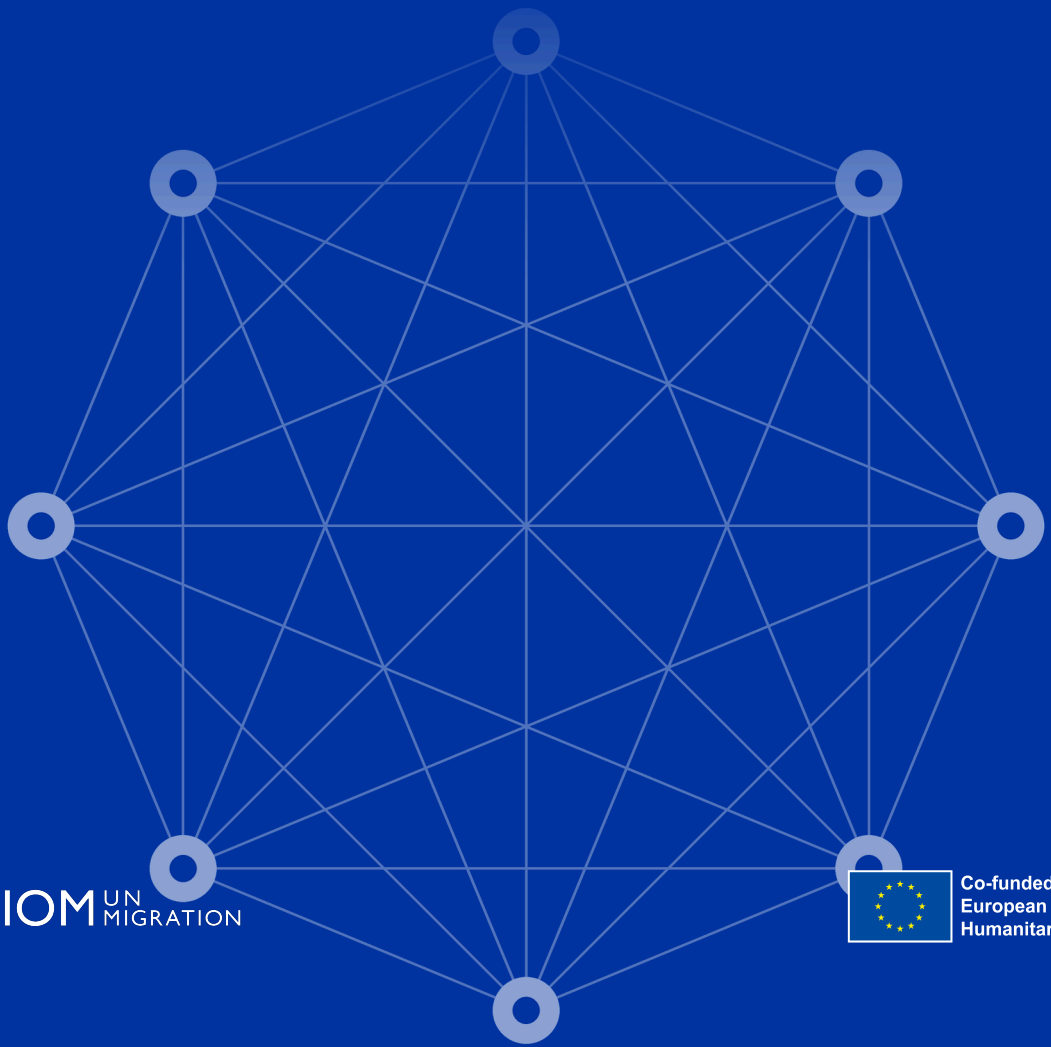
IDEHA TRUST FRAMEWORK

Implementation Guidelines



IOM UN MIGRATION

Co-funded by
European Union
Humanitarian Aid

Publisher: International Organization for Migration (IOM)
Regional Office for East Horn and Southern Africa
Sri Aurobindo Avenue, Off Mzima Spring Road
Lavington
Nairobi
Kenya

This publication was issued without formal editing by IOM. This publication was issued without IOM Publications Unit (PUB) approval for adherence to IOM's brand and style standards. This publication was issued without IOM Research Unit (RES) endorsement.

IDEHA Trust Framework

Implementation Guidelines

Ott Sarv, prepared for International Organization for Migration (IOM)

30 June 2026

CONTENTS

IDEHA-IG-GOV-FRM-001: FRAMEWORK INSTRUMENT DEVELOPMENT, VALIDATION AND CONTROLLED PUBLICATION

IDEHA-IG-GOV-SCH-001 Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for the preparation, validation, adoption readiness and controlled publication of Framework Instruments established under the Trust Framework.

2. This Guideline applies to Responsible Actors preparing Framework Instruments assigned to them under the applicable Framework provisions.

3. This Guideline establishes requirements for:

(a) preparation of Framework Instrument development records;

(b) allocation of requirements to the appropriate Framework Instrument;

(c) validation of normative content;

(d) identification of dependencies and references;

(e) preparation of publication information;

(f) maintenance of historical development records.

4. This Guideline does not:

(a) establish Framework Instrument categories;

(b) establish Decision Competence;

(c) assign Instrument Status;

(d) create Controlled Effects;

(e) establish Trust Service Categories or Trust Object Categories;

(f) replace requirements established by the Main Framework or Annexes.

FRAMEWORK INSTRUMENT DEVELOPMENT BASIS

Article 2

1. A Responsible Actor shall prepare a Framework Instrument only where an enabling provision permits or requires its development.

2. Before preparing a Framework Instrument, the Responsible Actor shall establish a development basis.

3. The development basis shall identify:

(a) the enabling Framework provision;

(b) the Framework Instrument category;

(c) the intended subject matter;

(d) the responsible drafting Actor;

(e) the affected Framework Instruments;

(f) the applicable Controlled Terms;

(g) the applicable Recognised Standards, where relevant.

Article 3

1. The Responsible Actor shall maintain a requirement allocation record during the preparation of a Framework Instrument.

2. The requirement allocation record shall identify:

(a) each requirement included in the draft;

(b) the normative basis for the requirement;

(c) the Framework Instrument responsible for the requirement;

(d) dependencies on other Framework Instruments;

(e) applicable Profiles and Technical Specifications.

3. A requirement shall not be included in a Framework Instrument where its normative ownership belongs to another Framework Instrument.

NORMATIVE CONTENT AND ALLOCATION

Article 4

1. A Framework Instrument shall contain only requirements necessary for the implementation of its assigned subject matter.

2. A Framework Instrument shall not repeat requirements already established by:

(a) the Main Framework;

(b) Annexes;

(c) another Framework Instrument.

3. Where a requirement is established by another Framework Instrument, the draft shall reference that requirement and specify only the additional implementation conditions necessary for its application.

Article 5

1. The Responsible Actor shall ensure that the draft Framework Instrument remains within its assigned scope.

2. The Responsible Actor shall verify that the draft does not:

(a) introduce a new category of Actor;

(b) introduce a new Trust Service Category;

(c) introduce a new Trust Object Category;

(d) establish a new Status;

(e) establish a new Qualified Status;

(f) modify Controlled Effects;

(g) assign Decision Competence.

3. Where the implementation of a requirement requires a new category, Status, Controlled Effect or Decision Competence, the matter shall be addressed through the applicable Main Framework amendment route.

CONTROLLED TERMS AND REFERENCES

Article 6

1. A Framework Instrument shall use Controlled Terms established by the Trust Framework.

2. A Framework Instrument shall not introduce a new capitalised term where an applicable Controlled Term already exists.

3. Where a new term is required for implementation purposes, the Responsible Actor shall determine whether:

(a) the term is an implementation expression limited to that Framework Instrument; or

(b) the term requires inclusion in the Controlled Terms through the applicable amendment process.

Article 7

1. A Framework Instrument shall identify dependencies on:

(a) Main Framework provisions;

(b) Annexes;

(c) other Framework Instruments;

(d) Profiles;

(e) Technical Specifications;

(f) Recognised Standards.

2. References shall identify the applicable scope and Version where required.

3. A reference to another Framework Instrument shall not incorporate requirements outside the identified scope.

DRAFT VALIDATION

Article 8

1. Before submission through the applicable adoption route, the Responsible Actor shall validate the draft Framework Instrument.

2. The validation shall confirm that:

(a) the draft remains within its enabling provision;

(b) the requirements are allocated to the correct normative layer;

(c) Controlled Terms are used consistently;

(d) dependencies are identified;

(e) referenced standards are identified;

(f) technical detail is assigned to Technical Specifications where required.

Article 9

1. The Responsible Actor shall perform a duplication assessment before submission.

2. The duplication assessment shall consider:

(a) duplication with the Main Framework;

(b) duplication with Annexes;

(c) duplication with other Framework Instruments;

(d) duplication of horizontal controls;

(e) duplication of technical requirements.

3. Where duplication is identified, the Responsible Actor shall:

(a) remove the duplicated requirement; or

(b) retain only the implementation condition necessary for applying the existing requirement.

STANDARDS AND TECHNICAL BOUNDARY

Article 10

1. Where a Framework Instrument requires the application of Recognised Standards, those standards shall be identified in accordance with the applicable standards-management requirements.

2. The standards reference shall identify:

(a) issuing organisation;

(b) reference identifier;

(c) title;

(d) applicable edition or Version;

(e) implementation purpose;

(f) applicable scope;

(g) approved adaptations or exclusions.

Article 11

1. A Framework Instrument shall not contain:

(a) technical schemas;

(b) message structures;

(c) protocol definitions;

(d) algorithm specifications;

(e) cryptographic parameters;

(f) interface definitions;

(g) test vectors;

(h) deployment configurations.

2. The matters referred to in paragraph 1 shall be established through Technical Specifications where required.

PUBLICATION AND LIFECYCLE RECORDS

Article 12

1. The Responsible Actor shall prepare the information required for controlled publication following adoption of a Framework Instrument.

2. The publication information shall include:

(a) Instrument Identifier;

(b) title;

(c) Version;

(d) Effective Date;

(e) applicable Annexes;

(f) applicable references.

Article 13

1. The Responsible Actor shall maintain records demonstrating the preparation and validation of a Framework Instrument.

2. The records shall include:

(a) development basis;

(b) requirement allocation record;

(c) duplication assessment;

(d) validation results;

(e) dependency assessment;

(f) standards assessment;

(g) draft Versions;

(h) publication information.

Article 14

1. Changes to a Framework Instrument shall be implemented through the applicable Change Control process.

2. The Responsible Actor shall maintain records identifying:

(a) the changed Framework Instrument;

(b) the new Version;

(c) affected dependencies;

(d) affected Standards;

(e) transition conditions.

3. Previous Versions shall remain identifiable for Historical State purposes.

APPLICABLE STANDARDS

Article 15

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Status;

(b) Qualified Status;

(c) Service Permission;

(d) Technical Exchange Permission;

(e) Controlled Reliance.

ANNEX I

Applicable standards

Reference	Application
ISO 15489-1:2016	Records management principles applicable to Framework Instrument development and lifecycle records
ISO 23081-1:2017	Metadata principles applicable to Framework Instrument lifecycle information
ISO 8601-1:2019	Date and time representation for Framework Instrument metadata

IDEHA-IG-GOV-SCH-001: SCHEME DEVELOPMENT AND OPERATIONS

IDEHA-IG-GOV-SCH-001

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for the establishment, operation, modification and closure of Schemes under the Trust Framework.

2. This Guideline applies to Responsible Actors assigned responsibility for preparing or operating a Scheme.

3. This Guideline shall apply within the scope established by the applicable Framework provisions.

4. This Guideline does not:

(a) establish Trust Service Categories;

(b) establish Trust Object Categories;

(c) assign Status or Qualified Status;

(d) establish Decision Competence;

(e) create Controlled Effects;

(f) replace requirements established by the Main Framework, Annexes or other Framework Instruments.

SCHEME ESTABLISHMENT

Article 2

1. A Responsible Actor preparing a Scheme shall establish a Scheme development record before submitting the Scheme for approval.

2. The Scheme development record shall contain:

(a) the Scheme identifier;

(b) the enabling Framework provision;

(c) the intended purpose and governed context;

(d) the participating Actors;

(e) the applicable Trust Services, Trust Objects or Sources;

(f) the applicable Profiles and Technical Specifications;

(g) the applicable Reliance Conditions;

(h) the applicable safeguards and limitations.

Article 3

1. A Scheme shall define its operational scope.

2. The Scheme scope shall identify:

(a) the governed purpose;

(b) the participating Actors;

(c) the applicable Federation Domains;

(d) the applicable Trust Services, Trust Objects or Sources;

(e) the permitted reliance context;

(f) applicable limitations.

3. A Scheme shall not extend the scope or effect of a Trust Service, Trust Object or Source beyond the conditions established by the applicable Framework Instruments.

SCHEME GOVERNANCE

Article 4

1. The Responsible Actor shall establish governance arrangements necessary for operation of the Scheme.

2. The governance arrangements shall identify:

(a) responsible governance functions;

(b) operational responsibilities;

(c) participation responsibilities;

(d) monitoring responsibilities;

(e) review responsibilities.

3. The governance arrangements shall remain within the Decision Competence and responsibility allocation established by the Trust Framework.

PARTICIPATION AND OPERATIONAL CONDITIONS

Article 5

1. Participation in a Scheme shall be recorded and maintained by the Responsible Actor.

2. The participation record shall identify:

(a) participating Actor;

(b) assigned Role where applicable;

(c) participation scope;

(d) effective date;

(e) restrictions or limitations.

3. Participation in a Scheme shall not by itself establish:

(a) Trust Service Status;

(b) Qualified Trust Service Status;

(c) Qualified Trust Object Status;

(d) Authorisation;

(e) Controlled Reliance.

Article 6

1. A Scheme may identify implementation conditions applicable within its scope.

2. Those conditions may include:

(a) applicable Profiles;

(b) applicable Technical Specifications;

(c) applicable Recognised Standards;

(d) applicable Assurance Conditions;

(e) applicable Security Conditions;

(f) applicable Accessibility Conditions.

3. A Scheme shall not redefine requirements established by the Main Framework or Annexes.

SCHEME OPERATION AND MONITORING

Article 7

1. The Responsible Actor shall maintain operational information necessary for Scheme operation.

2. Operational information shall include:

(a) current Version;

(b) applicable Profiles;

(c) applicable Technical Specifications;

(d) participating Actors;

(e) operational dependencies;

(f) applicable restrictions.

3. The Responsible Actor shall ensure that operational information remains consistent with the authoritative Framework Instruments.

Article 8

1. The Responsible Actor shall monitor whether the Scheme continues to operate within its approved scope.

2. Monitoring shall consider:

(a) changes affecting participating Actors;

(b) changes affecting Trust Services, Trust Objects or Sources;

(c) changes affecting Profiles or Technical Specifications;

(d) changes affecting Security Conditions;

(e) changes affecting Protected-Person Safeguards;

(f) changes affecting Reliance Conditions.

SCHEME MODIFICATION AND CLOSURE

Article 9

1. A proposed modification to a Scheme shall be assessed before implementation.

2. The assessment shall identify:

(a) affected Framework Instruments;

(b) affected participating Actors;

(c) affected Trust Services, Trust Objects or Sources;

(d) affected Profiles;

(e) affected Technical Specifications;

(f) transition requirements.

Article 10

1. Where a Scheme no longer operates within its approved scope, the Responsible Actor shall implement corrective measures.

2. Corrective measures may include:

(a) modification of operational conditions;

(b) restriction of Scheme scope;

(c) temporary Suspension;

(d) closure of the Scheme.

3. Closure shall identify:

(a) effective closure date;

(b) affected Actors;

(c) affected Trust Services, Trust Objects or Sources;

(d) transition arrangements;

(e) records retention requirements.

RECORDS AND EVIDENCE

Article 11

1. The Responsible Actor shall maintain records demonstrating:

(a) Scheme establishment;

(b) governance arrangements;

(c) participation decisions;

(d) operational changes;

(e) monitoring activities;

(f) Reviews;

(g) closure activities.

2. Records shall enable reconstruction of the Scheme lifecycle.

APPLICABLE STANDARDS

Article 12

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only within the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create Status, Qualified Status, Controlled Effects or Decision Competence.

ANNEX I

Applicable standards

Reference	Application
ISO/IEC 24760-2	Identity-management architecture considerations where a Scheme includes identity-related functions
ISO/IEC 29146	Access-management architecture considerations where a Scheme includes controlled access arrangements
ISO/IEC 27001	Security-management controls applicable to Scheme operation
ISO/IEC 27701	Privacy-management controls where personal data processing is performed within the Scheme

IDEHA-IG-GOV-PRF-001: PROFILE DEVELOPMENT AND CONTROLLED SELECTION IMPLEMENTATION

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for the preparation, selection, validation, publication and maintenance of Profiles established under the Trust Framework.

2. This Guideline applies to Responsible Actors preparing or maintaining Profiles assigned to them under the applicable Framework provisions.

3. This Guideline establishes requirements for:

(a) identifying the implementation context for a Profile;

(b) selecting applicable requirements, options and conditions;

(c) defining dependencies on Framework Instruments;

(d) validating Profile consistency;

(e) maintaining Profile lifecycle information.

4. This Guideline does not:

(a) establish new Trust Service Categories;

(b) establish new Trust Object Categories;

(c) assign Status or Qualified Status;

(d) create Controlled Effects;

(e) modify requirements established by the Main Framework or Annexes;

(f) replace Technical Specifications.

PROFILE DEVELOPMENT BASIS

Article 2

1. A Responsible Actor shall prepare a Profile only where an enabling provision permits or requires the selection of implementation requirements.

2. Before preparing a Profile, the Responsible Actor shall establish a Profile development basis.

3. The Profile development basis shall identify:

(a) the enabling Framework provision;

(b) the subject matter to which the Profile applies;

(c) the applicable Framework Instrument;

(d) the intended implementation context;

(e) the responsible drafting Actor;

(f) the applicable Trust Services, Trust Objects, Sources or other Controlled Matters.

Article 3

1. The Responsible Actor shall identify the purpose of the Profile.

2. The purpose shall specify:

(a) the implementation context;

(b) the applicable Actors;

(c) the applicable Trust Services, Trust Objects or Sources;

(d) the intended Assurance Conditions;

(e) the applicable Reliance Conditions.

3. A Profile shall not expand the purpose or scope established by the enabling Framework provision.

SELECTION OF REQUIREMENTS

Article 4

1. A Profile shall identify the requirements selected for its applicable implementation context.

2. A Profile may select:

(a) optional requirements;

(b) implementation classes;

(c) Assurance Conditions;

(d) Security Conditions;

(e) Accessibility Conditions;

(f) lifecycle conditions;

(g) technical implementation options.

3. A Profile shall identify the source Framework Instrument for each selected requirement.

Article 5

1. The Responsible Actor shall ensure that selected requirements remain consistent with:

(a) the Main Framework;

(b) applicable Annexes;

(c) applicable Implementation Guidelines;

(d) applicable Technical Specifications.

2. A Profile shall not:

(a) remove mandatory requirements;

(b) reduce applicable Security Conditions;

(c) remove Protected-Person Safeguards;

(d) alter Status requirements;

(e) change Decision Competence.

PROFILE CONTENT

Article 6

1. A Profile shall specify the implementation conditions applicable within its scope.

2. The Profile shall identify, where applicable:

(a) applicable Trust Service or Trust Object category;

(b) applicable Actors;

(c) applicable Source categories;

(d) applicable Assurance Conditions;

(e) applicable Security Conditions;

(f) applicable Accessibility Conditions;

(g) applicable Validation requirements;

(h) applicable lifecycle conditions.

3. The Profile shall identify requirements that remain subject to a Technical Specification.

Article 7

1. A Profile shall identify dependencies on:

(a) Framework Instruments;

(b) other Profiles;

(c) Technical Specifications;

(d) Recognised Standards.

2. Dependencies shall identify:

(a) the dependent instrument;

(b) the applicable scope;

(c) the applicable Version;

(d) the effect of the dependency.

Article 8

1. Where a Profile requires technical implementation choices, those choices shall be defined through the applicable Technical Specification.

2. A Profile shall identify the Technical Specification required for:

(a) data structures;

(b) formats;

(c) protocols;

(d) interfaces;

(e) algorithms;

(f) parameters;

(g) testing requirements.

3. A Profile shall not contain detailed technical requirements assigned to a Technical Specification.

ASSURANCE AND QUALIFICATION CONDITIONS

Article 9

1. Where a Profile specifies Assurance Conditions, it shall identify:

(a) the applicable Assurance Domains;

(b) the applicable Assurance Levels;

(c) the required evidence;

(d) the assessment conditions.

2. Where a Profile applies to Qualified Trust Services or Qualified Trust Objects, it shall identify the qualified conditions established by the applicable Framework provisions.

3. A Profile shall not establish Qualified Status.

Article 10

1. A Profile requiring Conformity Assessment shall identify:

(a) the subject of assessment;

(b) the applicable requirements;

(c) the required evidence;

(d) the assessment scope.

2. A Profile shall not determine the outcome of a Conformity Assessment.

3. A Profile shall not assign Qualified Status or another Status.

VALIDATION AND PUBLICATION

Article 11

1. Before publication, the Responsible Actor shall validate the Profile.

2. The validation shall confirm that:

(a) the Profile remains within its enabling provision;

(b) selected requirements are complete;

(c) dependencies are identified;

(d) terminology is consistent;

(e) no higher-ranking requirement is modified;

(f) no technical requirement has been incorrectly allocated.

Article 12

1. The Responsible Actor shall maintain records demonstrating:

(a) Profile development;

(b) requirement selection;

(c) dependency analysis;

(d) validation results;

(e) consultation where applicable;

(f) Version history.

PROFILE LIFECYCLE

Article 13

1. Changes to a Profile shall be assessed before implementation.

2. The assessment shall identify:

(a) affected Framework Instruments;

(b) affected Technical Specifications;

(c) affected Recognised Standards;

(d) affected implementations;

(e) transition requirements.

3. Previous Profile Versions shall remain identifiable for Historical State purposes.

Article 14

1. A Profile may be restricted, withdrawn or replaced where:

(a) requirements are no longer applicable;

(b) dependencies have changed;

(c) security conditions require modification;

(d) transition to a replacement Profile is completed.

2. Restriction, withdrawal or replacement shall not modify Status already established under the applicable Framework provisions unless determined through the applicable Decision Competence.

APPLICABLE STANDARDS

Article 15

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Status;

(b) Qualified Status;

(c) Service Permission;

(d) Technical Exchange Permission;

(e) Controlled Reliance.

ANNEX I

Applicable standards

Reference	Application
ISO/IEC 24760-2:2025	Identity-management architecture considerations where Profiles select identity-related implementation conditions
ISO/IEC 29146:2024	Access-management architecture considerations where Profiles select access-control conditions
ISO/IEC 27001:2022	Security-management controls applicable to Profile governance where required
ISO/IEC 27701:2025	Privacy-management controls where Profiles include personal-data processing conditions

IDEHA-IG-GOV-STD-001: STANDARDS SELECTION AND TECHNICAL REFERENCE MANAGEMENT IMPLEMENTATION

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for the evaluation, selection, registration, maintenance and transition of Recognised Standards and technical references used within the Trust Framework.

2. This Guideline applies to Responsible Actors performing standards-management functions assigned under the applicable Framework provisions.

3. This Guideline establishes requirements for:

(a) assessment of proposed standards and technical references;

(b) recording of recognised standards;

(c) identification of applicable editions and Versions;

(d) management of dependencies, adaptations and exclusions;

(e) transition between standards;

(f) maintenance of standards lifecycle information.

4. This Guideline does not:

(a) create technical requirements for Trust Services, Trust Objects or Sources;

(b) replace subject-specific requirements established by other Implementation Guidelines;

(c) define technical specifications, protocols, schemas, algorithms or parameters;

(d) create Status, Qualified Status or Controlled Effects through recognition of a standard.

STANDARDS EVALUATION BASIS

Article 2

1. A Responsible Actor proposing a standard or technical reference for recognition shall establish a standards evaluation record.

2. The standards evaluation record shall identify:

(a) the proposed standard or technical reference;

(b) the issuing organisation;

(c) the intended implementation function;

(d) the applicable Framework Instrument;

(e) the responsible evaluation Actor;

(f) the affected Trust Services, Trust Objects, Sources or other Controlled Matters.

Article 3

1. The evaluation of a proposed standard shall consider:

(a) suitability for the intended implementation purpose;

(b) technical maturity;

(c) security characteristics;

(d) interoperability considerations;

(e) lifecycle management arrangements;

(f) compatibility with applicable Framework requirements;

(g) availability of conformity evidence.

2. The evaluation shall identify whether the standard is:

(a) mandatory;

(b) conditionally applicable;

(c) an approved option;

(d) informative.

STANDARDS REFERENCE MANAGEMENT

Article 4

1. A Recognised Standard shall be recorded with sufficient information to identify its identity and applicability.

2. The standards record shall contain:

(a) issuing organisation;

(b) standard identifier;

(c) title;

(d) edition or Version;

(e) publication date where relevant;

(f) implementation purpose;

(g) applicable Framework Instrument;

(h) applicable scope;

(i) dependencies;

(j) transition information.

Article 5

1. Where only part of a standard applies, the applicable scope shall be identified.

2. The standards record shall identify, where applicable:

(a) applicable clauses;

(b) applicable annexes;

(c) applicable profiles;

(d) applicable conformance classes;

(e) applicable policy requirements;

(f) applicable implementation options.

3. A general reference to a standards family shall not establish an implementation requirement.

Article 6

1. Where a Recognised Standard requires adaptation for use within the Trust Framework, the adaptation shall be recorded.

2. The adaptation record shall identify:

(a) the affected standard provision;

(b) the reason for the adaptation;

(c) the applicable Framework requirement;

(d) the resulting implementation condition;

(e) the responsible approval function.

3. An adaptation shall not modify the scope or Controlled Effects established by the Main Framework.

STANDARDS DEPENDENCIES

Article 7

1. A Recognised Standard shall identify normative dependencies necessary for its implementation.

2. The dependency record shall identify:

(a) the dependent standard;

(b) the dependency purpose;

(c) the applicable Version;

(d) the effect of dependency failure.

3. A dependency shall not be interpreted as creating automatic applicability outside the identified implementation scope.

Article 8

1. Where multiple Recognised Standards apply to the same implementation function, the Responsible Actor shall identify their relationship.

2. The relationship shall specify:

(a) primary standard;

(b) supporting standards;

(c) optional standards;

(d) superseded standards;

(e) incompatible standards where applicable.

STANDARDS LIFECYCLE MANAGEMENT

Article 9

1. The Responsible Actor shall monitor Recognised Standards for:

(a) new editions;

(b) security concerns;

(c) technical obsolescence;

(d) interoperability impacts;

(e) withdrawal or replacement.

2. Monitoring results shall be recorded in the standards lifecycle record.

Article 10

1. A new edition or Version of a standard shall not automatically replace an existing Recognised Standard.

2. Before adoption of a replacement Version, the Responsible Actor shall assess:

(a) changes in requirements;

(b) security impacts;

(c) implementation impacts;

(d) conformity impacts;

(e) transition requirements.

Article 11

1. Where a Recognised Standard is replaced, the transition decision shall identify:

(a) the previous standard;

(b) the replacement standard;

(c) the effective date;

(d) the transition period;

(e) coexistence conditions;

(f) affected Framework Instruments;

(g) affected Technical Specifications.

2. The previous standard shall remain identifiable for Historical State purposes.

STANDARDS APPLICATION

Article 12

1. A subject-specific Framework Instrument applying a Recognised Standard shall identify:

(a) the Recognised Standard;

(b) the applicable implementation function;

(c) the applicable scope;

(d) the required conformity evidence.

2. A Recognised Standard shall apply only within the scope identified by the applicable Framework Instrument.

3. Recognition of a standard shall not by itself establish:

(a) Status;

(b) Qualified Status;

(c) Service Permission;

(d) Technical Exchange Permission;

(e) Authorisation;

(f) Controlled Reliance.

Article 13

1. Where a Recognised Standard defines conformity requirements, the applicable Framework Instrument shall identify the required conformity evidence.

2. Conformity evidence may include:

(a) certification;

(b) assessment reports;

(c) testing evidence;

(d) declarations;

(e) implementation records.

3. The existence of conformity evidence shall not replace any required Framework Decision or Status determination.

RECORDS AND PUBLICATION

Article 14

1. The Responsible Actor shall maintain the Standards Register.

2. The Standards Register shall contain:

(a) recognised standards;

(b) applicable Versions;

(c) lifecycle Status;

(d) implementation scope;

(e) dependencies;

(f) adaptations;

(g) transition information.

3. The Standards Register shall enable historical reconstruction of standards applicability.

APPLICABLE STANDARDS

Article 15

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the standards-management functions identified in that Annex.

3. The standards referenced in Annex I shall not determine the technical requirements of subject-specific implementations.

ANNEX I

Applicable standards

Reference	Application
ISO/IEC 17000:2020	Conformity assessment vocabulary and general principles
ISO/IEC 17065:2012	Requirements for bodies certifying products, processes and services where certification evidence is used
ISO/IEC 17021-1:2015	Requirements for bodies providing management-system audits and certification where applicable
ISO/IEC 17025:2017	Competence requirements for testing and calibration laboratories where applicable
ISO/IEC 27001:2022	Security-management considerations for standards lifecycle information

IDEHA-IG-ACT-PAR-001: PARTICIPATION, ROLES, MANDATES AND REPRESENTATION IMPLEMENTATION

IDEHA-IG-ACT-PAR-001

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for the registration, assignment, maintenance and lifecycle management of Participation, Roles, Mandates and representation relationships within the Trust Framework.

2. This Guideline applies to Responsible Actors managing Participation records, Role assignments, Mandates or representation relationships under an applicable Framework Instrument.

3. This Guideline establishes requirements for:

(a) recording Participation;

(b) assigning Roles;

(c) recording Mandates;

(d) managing representation relationships;

(e) maintaining lifecycle evidence;

(f) supporting Validation of authority and representation.

4. This Guideline does not:

(a) establish Actor categories;

(b) establish Participation rights;

(c) create Decision Competence;

(d) create Authorisation Outcomes;

(e) establish legal capacity or authority;

(f) replace requirements established by the Main Framework, applicable Schemes or applicable Profiles.

PARTICIPATION RECORDS

Article 2

1. A Responsible Actor shall maintain a Participation record for each Actor participating within an applicable Framework context.

2. The Participation record shall identify:

(a) the participating Actor;

(b) the applicable Scheme, Federation Domain or Framework context;

(c) the participation scope;

(d) the applicable effective period;

(e) the assigned Roles where applicable;

(f) restrictions or limitations;

(g) lifecycle Status.

3. A Participation record shall not by itself establish Authorisation to perform a specific Action.

Article 3

1. Before activating Participation, the Responsible Actor shall verify the information required by the applicable Scheme or Framework Instrument.

2. The verification shall consider, where applicable:

(a) Actor identity;

(b) organisational information;

(c) authority information;

(d) applicable Source information;

(e) required Assurance Conditions;

(f) applicable Security Conditions.

3. Evidence supporting Participation shall be maintained according to the applicable records-management requirements.

ROLE ASSIGNMENT

Article 4

1. A Responsible Actor assigning a Role shall record:

(a) the Actor receiving the Role;

(b) the Role identifier;

(c) the Role scope;

(d) the applicable context;

(e) the effective period;

(f) restrictions or conditions.

2. A Role assignment shall not be interpreted as creating permission to perform an Action.

3. A Role may be used as an input to an Authorisation Service where the applicable Authorisation Policy requires such input.

Article 5

1. Where a Role depends on qualifications, Attributes, Mandates or other conditions, the Responsible Actor shall identify those dependencies.

2. The Role record shall identify, where applicable:

(a) required evidence;

(b) validating Source;

(c) applicable Status;

(d) validity period;

(e) reassessment requirements.

3. A Role shall cease to be relied upon where the conditions supporting that Role are no longer valid.

MANDATES AND DELEGATED AUTHORITY

Article 6

1. A Mandate shall identify the authority granted by one Actor to another Actor within an identified scope.

2. A Mandate record shall contain:

(a) Mandating Actor;

(b) Mandated Actor;

(c) permitted scope;

(d) permitted Actions where applicable;

(e) limitations;

(f) effective period;

(g) revocation conditions;

(h) supporting evidence.

3. A Mandate shall not extend beyond the authority available to the Mandating Actor.

Article 7

1. A Responsible Actor shall verify the validity of a Mandate before relying on it.

2. The verification shall determine:

(a) identity of the Mandating Actor;

(b) identity of the Mandated Actor;

(c) existence of authority to grant the Mandate;

(d) scope compatibility;

(e) validity period;

(f) revocation or restriction Status.

3. Where a Mandate is used as an input to an Authorisation decision, the Mandate shall be evaluated together with the applicable Authorisation Policy.

REPRESENTATION RELATIONSHIPS

Article 8

1. A representation relationship shall identify the relationship between a Representing Actor and a Represented Person or Actor.

2. The representation record shall identify:

(a) representing Actor;

(b) represented Person or Actor;

(c) representation basis;

(d) permitted scope;

(e) effective period;

(f) limitations;

(g) evidence supporting the representation.

3. A representation relationship shall not alter the identity, Status or obligations of the represented Person or Actor.

Article 9

1. A Responsible Actor shall distinguish between:

(a) legal representation;

(b) organisational representation;

(c) delegated representation;

(d) operational assistance;

(e) emergency representation;

(f) other representation categories established by an applicable Profile.

2. The applicable Profile shall define the conditions under which each representation category may be used.

LIFECYCLE MANAGEMENT

Article 10

1. Participation, Role, Mandate and representation records shall maintain lifecycle information.

2. Lifecycle information shall include, where applicable:

(a) creation;

(b) activation;

(c) modification;

(d) suspension;

(e) expiration;

(f) revocation;

(g) withdrawal;

(h) historical state.

3. Previous states shall remain identifiable where required for Historical State determination.

Article 11

1. Changes affecting Participation, Roles, Mandates or representation shall be assessed before implementation where they may affect:

(a) Authorisation;

(b) Controlled Reliance;

(c) Trust Service operation;

(d) Source access;

(e) Federation participation.

2. The assessment shall identify:

(a) affected Actors;

(b) affected Services;

(c) affected Policies;

(d) transition requirements.

VALIDATION AND EVIDENCE

Article 12

1. Participation, Role, Mandate and representation information shall be capable of Verification and Validation where relied upon by another Framework Actor.

2. Verification shall determine:

(a) record integrity;

(b) identifier consistency;

(c) completeness of required information.

3. Validation shall determine:

(a) current Status;

(b) effective period;

(c) supporting evidence;

(d) applicable scope;

(e) historical validity where required.

Article 13

1. The Responsible Actor shall maintain evidence sufficient to reconstruct:

(a) the basis for Participation;

(b) Role assignment decisions;

(c) Mandate creation and modification;

(d) representation relationships;

(e) Validation decisions;

(f) lifecycle changes.

2. Evidence shall be protected against unauthorised alteration and disclosure.

SECURITY AND SAFEGUARDS

Article 14

1. Participation, Role, Mandate and representation information shall be protected according to its classification and sensitivity.

2. Access to such information shall be limited according to:

(a) assigned Role;

(b) Authorisation Policy;

(c) purpose;

(d) minimum necessary disclosure.

3. Special safeguards shall apply where the information concerns Protected Persons or representation involving vulnerable individuals.

APPLICABLE STANDARDS

Article 15

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Participation;

(b) Role;

(c) Mandate;

(d) Authorisation;

(e) Controlled Reliance.

ANNEX I

Applicable standards

Reference	Application
ISO/IEC 24760-1:2025	Identity concepts, identity information and relationship between identity information and Actors
ISO/IEC 24760-2:2025	Identity-management architecture considerations for Actor and representation relationships
ISO/IEC 24760-3:2025	Operational management of identity information and lifecycle activities
ISO/IEC 11179-3:2023	Metadata registration for Role, Mandate and relationship-related data elements
ISO/IEC 29146:2024	Access-management architecture where Role and Mandate information is evaluated for access decisions

IDEHA-IG-FED-DOM-001: FEDERATION DOMAIN AND CROSS-DOMAIN IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for the establishment, operation, maintenance and lifecycle management of Federation Domains and cross-domain arrangements under the Trust Framework.

2. This Guideline applies to Responsible Actors establishing or operating Federation Domains, Federation Agreements or cross-domain trust arrangements.

3. This Guideline establishes requirements for:

(a) Federation Domain registration;

(b) governance and responsibility allocation;

(c) participation management;

(d) cross-domain trust arrangements;

(e) operational coordination;

(f) lifecycle and transition management.

4. This Guideline does not:

(a) establish Federation Domains as new Actor categories;

(b) create Trust Service Categories;

(c) create Trust Object Categories;

(d) assign Status or Qualified Status;

(e) create Controlled Effects;

(f) replace requirements established by the Main Framework, Schemes, Profiles or Technical Specifications.

FEDERATION DOMAIN ESTABLISHMENT

Article 2

1. A Responsible Actor proposing a Federation Domain shall establish a Federation Domain development record.

2. The development record shall identify:

(a) the proposed Federation Domain Identifier;

(b) the responsible governance function;

(c) the purpose and scope;

(d) participating Actors;

(e) participating Federation Domains where applicable;

(f) applicable Trust Services, Trust Objects and Sources;

(g) applicable Schemes, Profiles and Technical Specifications.

3. The Federation Domain shall operate only within the scope established through the applicable Framework decision route.

Article 3

1. A Federation Domain shall define its operational boundaries.

2. The boundaries shall identify:

(a) participating jurisdictions, organisations or operational domains;

(b) permitted Trust Services;

(c) permitted Sources;

(d) permitted Trust Objects;

(e) permitted exchange relationships;

(f) applicable Reliance Conditions.

3. A Federation Domain shall not modify the Status, scope or obligations of participating Actors, Trust Services, Trust Objects or Sources.

FEDERATION GOVERNANCE

Article 4

1. A Federation Domain shall maintain governance arrangements sufficient for its operation.

2. The governance arrangements shall identify:

(a) responsible governance Actors;

(b) operational responsibilities;

(c) participation management responsibilities;

(d) security responsibilities;

(e) incident coordination responsibilities;

(f) Review responsibilities.

3. Governance arrangements shall remain consistent with the Decision Competence established by the Trust Framework.

Article 5

1. A Federation Domain shall maintain a record of participating Actors.

2. The participation record shall identify:

(a) Actor Identifier;

(b) participation scope;

(c) assigned Roles;

(d) applicable Trust Services, Trust Objects or Sources;

(e) effective period;

(f) restrictions or limitations.

3. Participation in a Federation Domain shall not by itself create:

(a) Trust Service Status;

(b) Qualified Trust Service Status;

(c) Authorisation;

(d) Controlled Reliance.

FEDERATION AGREEMENTS

Article 6

1. A Federation Agreement shall define the conditions under which participating Actors cooperate within a Federation Domain.

2. A Federation Agreement shall identify:

(a) participating Actors;

(b) responsibilities;

(c) permitted interactions;

(d) applicable Trust Services;

(e) applicable Sources;

(f) security conditions;

(g) safeguards;

(h) dispute and escalation arrangements.

3. A Federation Agreement shall not replace:

(a) Framework requirements;

(b) Source governance;

(c) Trust Service requirements;

(d) Authorisation decisions;

(e) data-sharing arrangements between Actors.

Article 7

1. Where a Federation Domain includes cross-domain interactions, the responsible Actors shall establish cross-domain trust arrangements.

2. Cross-domain trust arrangements shall identify:

(a) participating Federation Domains;

(b) trust anchors;

(c) applicable Trust Lists or equivalent Status information;

(d) Validation requirements;

(e) applicable Profiles;

(f) Technical Specifications.

3. Cross-domain trust shall not establish automatic acceptance of all Trust Services, Trust Objects or Sources.

CROSS-DOMAIN OPERATION

Article 8

1. A Federation Domain shall define the conditions for cross-domain reliance.

2. Those conditions shall identify, where applicable:

(a) accepted Trust Services;

(b) accepted Trust Objects;

(c) accepted Sources;

(d) required Validation;

(e) required Status verification;

(f) applicable Assurance Conditions;

(g) applicable Security Conditions.

3. A Relying Actor shall apply its Local Trust Acceptance Policy where required by the Main Framework.

Article 9

1. Federation Domains shall maintain information necessary for operational discovery.

2. Discovery information may include:

(a) Federation Domain Identifier;

(b) participating Actor identifiers;

(c) Trust Service identifiers;

(d) Source identifiers;

(e) Endpoint information;

(f) applicable Profiles;

(g) Technical Specification references.

3. Discovery information shall not disclose information beyond the permitted publication scope.

SECURITY AND CONTINUITY COORDINATION

Article 10

1. A Federation Domain shall establish coordination arrangements for:

(a) security events;

(b) Trust Service disruptions;

(c) Source availability issues;

(d) compromise events;

(e) continuity measures.

2. Coordination arrangements shall identify:

(a) responsible Actors;

(b) notification conditions;

(c) communication channels;

(d) evidence requirements;

(e) recovery coordination.

Article 11

1. A Federation Domain shall define transition arrangements where changes affect cross-domain operation.

2. Transition arrangements shall consider:

(a) changes to Trust Services;

(b) changes to Trust Objects;

(c) changes to Sources;

(d) changes to Standards;

(e) changes to Technical Specifications;

(f) cessation of participating Actors.

3. Transition arrangements shall preserve Historical State where required.

LIFECYCLE MANAGEMENT

Article 12

1. The Responsible Actor shall monitor whether the Federation Domain continues to operate within its approved scope.

2. Monitoring shall consider:

(a) participation changes;

(b) security events;

(c) changes to applicable Profiles;

(d) changes to applicable Standards;

(e) changes affecting Reliance Conditions.

3. Material changes shall be assessed before implementation.

Article 13

1. A Federation Domain may be restricted, suspended or closed where:

(a) operational conditions are no longer satisfied;

(b) security conditions are no longer sufficient;

(c) governance requirements cannot be maintained;

(d) transition to a replacement arrangement is completed.

2. Closure shall identify:

(a) effective closure date;

(b) affected Actors;

(c) affected Trust Services, Trust Objects and Sources;

(d) transition arrangements;

(e) records retention requirements.

RECORDS AND EVIDENCE

Article 14

1. The Responsible Actor shall maintain records demonstrating:

(a) Federation Domain establishment;

(b) governance arrangements;

(c) participation decisions;

(d) Federation Agreements;

(e) cross-domain trust arrangements;

(f) operational changes;

(g) lifecycle decisions.

2. Records shall enable reconstruction of the Federation Domain lifecycle.

APPLICABLE STANDARDS

Article 15

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Federation Domain Status;

(b) Trust Service Status;

(c) Qualified Status;

(d) Authorisation;

(e) Controlled Reliance.

ANNEX I

Applicable standards

Reference	Application
ISO/IEC 27001:2022	Information security management for Federation Domain governance and operation
ISO/IEC 27701:2025	Privacy information management where personal data is processed across Federation Domains
ISO/IEC 29146:2024	Access-management architecture where cross-domain access decisions are performed
ISO/IEC 24760-2:2025	Identity-management architecture considerations for cross-domain identity relationships
ETSI TS 119 612 V2.4.1	Trusted-list structures where Federation Domains rely on Trust List publication
ETSI TS 119 615 V1.4.1	Interpretation and use of Trust List information across domains

IDEHA-IG-SRC-ASO-001: SOURCE AND AUTHORITATIVE SOURCE IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for the recognition, registration, operation, maintenance and lifecycle management of Sources and Authoritative Sources within the Trust Framework.

2. This Guideline applies to Responsible Actors managing Sources, Authoritative Sources and Qualified Authoritative Sources within an applicable Framework context.

3. This Guideline establishes requirements for:

(a) Source identification;

(b) Source Scope definition;

(c) Source Basis management;

(d) Attribute provenance and quality management;

(e) Source verification;

(f) Correction and lifecycle management.

4. This Guideline does not:

(a) establish Sources as Trust Service Categories;

(b) create Trust Service Status;

(c) create Qualified Authoritative Source Status;

(d) establish legal authority of a Source;

(e) create Controlled Effects;

(f) replace requirements established by the Main Framework, Schemes, Profiles or Technical Specifications.

SOURCE REGISTRATION AND IDENTIFICATION

Article 2

1. A Responsible Actor managing a Source shall maintain a Source record.

2. The Source record shall identify:

(a) the Source Identifier;

(b) the Source Holder;

(c) the Source Steward;

(d) the Source Scope;

(e) the Source purpose;

(f) the Attributes maintained by the Source;

(g) the applicable jurisdiction or operational domain;

(h) the effective period of the Source recognition.

Article 3

1. A Source Identifier shall uniquely identify the Source within the applicable identifier scope.

2. A Source Identifier shall not:

(a) disclose personal information;

(b) encode Source classification;

(c) encode Status;

(d) encode jurisdictional meaning unless required by the applicable identifier scheme.

3. The Responsible Actor shall maintain the relationship between the Source Identifier and the Source metadata required for Validation.

SOURCE SCOPE AND ATTRIBUTES

Article 4

1. A Source shall define its Source Scope.

2. The Source Scope shall identify:

(a) the Attributes maintained by the Source;

(b) the Subjects to which the Attributes relate;

(c) the applicable geographic, organisational or operational scope;

(d) the applicable time period;

(e) the conditions under which the Source is authoritative.

3. A Source shall not be considered authoritative for Attributes outside its Source Scope.

Article 5

1. A Source maintaining Attributes shall maintain semantic definitions for those Attributes.

2. Attribute definitions shall identify:

(a) Attribute Identifier;

(b) Attribute meaning;

(c) value domain;

(d) datatype;

(e) permitted transformations;

(f) quality requirements;

(g) lifecycle conditions.

3. Attribute semantics shall remain separate from:

(a) Attribute values;

(b) Source identifiers;

(c) Subject identifiers;

(d) Trust Object identifiers.

AUTHORITATIVE SOURCE DESIGNATION

Article 6

1. An Authoritative Source shall be designated only where the applicable Framework Instrument establishes that the Source has authority for the identified Source Scope.

2. The designation shall identify:

(a) the Source Scope;

(b) the Attributes covered;

(c) the responsible Source Holder;

(d) the applicable conditions;

(e) the effective period.

3. Authoritative Source designation shall not establish Qualified Authoritative Source Status.

Article 7

1. A Qualified Authoritative Source shall satisfy the applicable Qualified Profile.

2. The Qualified Profile shall specify:

(a) Assurance Conditions;

(b) Security Conditions;

(c) Data Quality Conditions;

(d) Provenance requirements;

(e) correction and lifecycle requirements;

(f) Conformity Assessment requirements.

3. Qualified Authoritative Source Status shall apply only within the approved Source Scope.

SOURCE DATA QUALITY AND PROVENANCE

Article 8

1. A Source shall maintain information sufficient to establish the origin and lifecycle of Attributes.

2. Provenance information shall identify, where applicable:

(a) originating event;

(b) originating Source process;

(c) creation time;

(d) modification history;

(e) responsible Actor;

(f) transformation or derivation activity.

3. Derived Attributes shall identify:

(a) source Attributes;

(b) derivation method;

(c) applicable Version;

(d) responsible processing function.

Article 9

1. A Source shall establish Data Quality controls appropriate to its Source Scope.

2. Data Quality controls shall address, where applicable:

(a) accuracy;

(b) completeness;

(c) consistency;

(d) timeliness;

(e) uniqueness;

(f) validity.

3. Data Quality requirements shall be specified by the applicable Profile where different Source Scopes require different conditions.

SOURCE VERIFICATION AND RELIANCE

Article 10

1. A Source consumer shall verify that the Source information used is applicable to the intended purpose.

2. Verification shall determine:

(a) Source identity;

(b) Source Scope;

(c) Attribute coverage;

(d) Provenance availability;

(e) applicable Version;

(f) data freshness.

3. Validation of a Source shall determine, where applicable:

(a) Source Status;

(b) Authoritative Source Status;

(c) Qualified Authoritative Source Status;

(d) Historical State;

(e) applicable restrictions.

Article 11

1. A Relying Actor shall not assume that an Attribute is authoritative solely because it originates from a recognised Source.

2. Reliance shall consider:

(a) the Source Scope;

(b) Attribute definition;

(c) Freshness Condition;

(d) Provenance;

(e) Correction status;

(f) applicable Reliance Conditions.

3. A Source shall not determine the legal effect of an Attribute outside the Source Scope assigned to it.

CORRECTION AND LIFECYCLE MANAGEMENT

Article 12

1. A Source shall maintain procedures for:

(a) Attribute correction;

(b) supersession;

(c) historical preservation;

(d) withdrawal of incorrect information;

(e) notification where required.

2. Corrections shall preserve sufficient evidence to reconstruct:

(a) previous values;

(b) correction basis;

(c) responsible Actor;

(d) effective time;

(e) affected reliance decisions.

Article 13

1. Changes affecting a Source shall be assessed where they affect:

(a) Source Scope;

(b) Attribute meaning;

(c) Data Quality;

(d) Provenance;

(e) interoperability;

(f) Qualified Authoritative Source conditions.

2. Material changes shall be managed through the applicable Change Control process.

SECURITY AND ACCESS

Article 14

1. Sources shall protect information according to its classification and applicable disclosure conditions.

2. Access to Source information shall be controlled through:

(a) Authentication;

(b) Authorisation;

(c) Disclosure Conditions;

(d) purpose limitations;

(e) audit requirements.

3. Security requirements shall be applied according to the applicable Security Conditions.

RECORDS AND EVIDENCE

Article 15

1. The Responsible Actor shall maintain records demonstrating:

(a) Source registration;

(b) Source Scope;

(c) Attribute definitions;

(d) Provenance;

(e) Data Quality assessments;

(f) corrections;

(g) lifecycle changes;

(h) Qualification evidence where applicable.

2. Records shall enable reconstruction of the Source lifecycle and Historical State.

APPLICABLE STANDARDS

Article 16

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Source authority;

(b) Authoritative Source Status;

(c) Qualified Authoritative Source Status;

(d) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ISO/IEC 11179-1:2023	Metadata registry framework for Source Attributes and semantic definitions
ISO/IEC 11179-3:2023	Registration and identification of metadata items
ISO/IEC 11179-31:2023	Description of data elements, value domains and data-element concepts
ISO/IEC 11179-6:2023	Registration authority and metadata lifecycle management
ISO/IEC 24760-1:2025	Identity information concepts and relationships
ISO/IEC 24760-2:2025	Identity-management architecture considerations
ISO/IEC 24760-3:2025	Identity-management operational processes
ISO/IEC 25012:2008	Data quality model
ISO/IEC 25024:2015	Data quality measurement
ISO 15489-1:2016	Records management principles
ISO 23081-1:2017	Metadata for records management
ISO/IEC 27001:2022	Information security management controls
ISO/IEC 27701:2025	Privacy information management controls

IDEHA-IG-OBJ-GEN-001: TRUST OBJECT COMMON AND LIFECYCLE IMPLEMENTATION

Version: 0.2

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for the identification, creation, issuance, lifecycle management, protection, Validation support and historical reconstruction of Trust Objects.

2. This Guideline applies to Actors responsible for creating, issuing, managing, validating or relying upon Trust Objects within the scope established by the applicable Framework Instruments.

3. This Guideline establishes common implementation requirements for:

(a) Trust Object identification;

(b) Trust Object Metadata;

(c) Trust Object lifecycle management;

(d) Trust Object dependencies;

(e) Trust Object evidence;

(f) Historical State reconstruction.

4. This Guideline applies together with the applicable Trust Object specific Implementation Guideline.

5. This Guideline does not:

(a) establish Trust Object Categories;

(b) define the substantive meaning of a Trust Object Category;

(c) assign Status or Qualified Status;

(d) establish Controlled Effects;

(e) replace requirements of a Trust Object specific Profile;

(f) define technical formats, schemas, protocols or cryptographic parameters.

TRUST OBJECT IDENTIFICATION

Article 2

1. Each Trust Object shall be assigned a Trust Object Identifier.

2. The Trust Object Identifier shall:

(a) uniquely distinguish the Trust Object within its applicable scope;

(b) remain stable throughout the Trust Object lifecycle;

(c) not disclose personal information;

(d) not encode Trust Object Status, Assurance Level or Qualified Status.

3. The Trust Object Identifier shall remain separate from:

(a) Subject Identifiers;

(b) Actor Identifiers;

(c) Source Identifiers;

(d) Trust Service Identifiers;

(e) Serial Numbers.

4. The applicable Trust Object Profile shall define:

(a) identifier generation;

(b) uniqueness scope;

(c) non-reuse conditions;

(d) collision handling;

(e) lifecycle treatment.

Article 3

1. Where a Trust Object contains an issuer-assigned Serial Number, the Serial Number shall identify the issued object within the issuer scope.

2. A Serial Number shall:

(a) be unique within the issuer scope;

(b) not be reused;

(c) remain linked to the issuing Actor;

(d) remain separate from the Trust Object Identifier.

3. The relationship between a Trust Object Identifier and a Serial Number shall be defined by the applicable Trust Object Profile or Technical Specification.

TRUST OBJECT METADATA

Article 4

1. A Trust Object shall contain or reference Metadata necessary for identification, Validation and lifecycle management.

2. Metadata shall include, where applicable:

(a) Trust Object Identifier;

(b) Trust Object Category;

(c) Issuer or producing Actor;

(d) creation time;

(e) issuance time;

(f) Version;

(g) applicable Profile;

(h) applicable Technical Specification;

(i) Status reference;

(j) dependency references;

(k) Provenance information.

3. Metadata shall not be interpreted as creating Authenticity, Validity, Status or Controlled Reliance.

Article 5

1. The Issuer or producing Actor shall ensure that Trust Object Metadata remains consistent with the applicable Profile.

2. Changes to Metadata shall be controlled where they may affect:

(a) Identification;

(b) Validation;

(c) Status determination;

(d) Historical State;

(e) Controlled Reliance.

TRUST OBJECT CREATION AND ISSUANCE

Article 6

1. A Trust Object shall be created only by an Actor authorised to create that Trust Object within the applicable scope.

2. Creation shall include, where applicable:

(a) determination of the Subject or matter to which the Trust Object relates;

(b) evaluation of required evidence;

(c) application of the applicable Profile;

(d) creation of the Trust Object representation;

(e) recording of creation evidence.

3. The creation process shall preserve the relationship between:

(a) the Trust Object;

(b) the Issuer or producing Actor;

(c) the applicable Source Basis or evidence basis;

(d) the applicable protection mechanism.

Article 7

1. Issuance of a Trust Object shall include recording:

(a) issuance time;

(b) issuing Actor;

(c) applicable Service Scope;

(d) applicable Profile Version;

(e) applicable dependencies;

(f) issuance evidence.

2. The issuance record shall enable reconstruction of the conditions existing at the time of issuance.

TRUST OBJECT PROTECTION

Article 8

1. A Trust Object shall be protected according to its category, purpose and applicable Profile.

2. Protection mechanisms may include:

(a) Electronic Signature;

(b) Electronic Seal;

(c) encryption;

(d) integrity mechanisms;

(e) access controls;

(f) other recognised protection methods.

3. The protection mechanism shall remain separate from the Trust Object Category unless the Main Framework establishes a specific relationship.

Article 9

1. Where a Trust Object depends on another Trust Object, the dependency shall be identified.

2. Dependency information shall identify:

(a) dependent Trust Object;

(b) dependency purpose;

(c) required Status;

(d) applicable Validation conditions;

(e) dependency Version.

3. A dependent Trust Object shall not transfer its Status, Qualified Status or Controlled Effects to another Trust Object.

TRUST OBJECT LIFECYCLE

Article 10

1. The lifecycle of a Trust Object shall include, where applicable:

(a) creation;

(b) issuance;

(c) activation;

(d) use;

(e) Validation;

(f) Suspension;

(g) Revocation;

(h) replacement;

(i) supersession;

(j) expiration;

(k) archival;

(l) closure.

2. The applicable Trust Object Profile shall define the lifecycle states applicable to each Trust Object Category.

Article 11

1. Lifecycle changes affecting a Trust Object shall be recorded.

2. The lifecycle record shall identify:

(a) previous state;

(b) new state;

(c) effective time;

(d) responsible Actor;

(e) reason for change;

(f) supporting evidence.

3. Lifecycle records shall enable determination of the Trust Object state at a previous point in time.

VALIDATION AND HISTORICAL RECONSTRUCTION

Article 12

1. A Trust Object shall be capable of Verification and Validation according to its applicable Profile.

2. Verification shall determine:

(a) structural consistency;

(b) integrity of representation;

(c) presence of required Metadata;

(d) format compliance.

3. Validation shall determine, where applicable:

(a) Authenticity;

(b) Validity;

(c) Status;

(d) Qualified Status conditions;

(e) dependency validity;

(f) Historical State.

Article 13

1. Where a Trust Object is relied upon after changes to its dependencies, Validation shall consider the Historical State applicable at the relevant time.

2. Historical State determination shall consider:

(a) Trust Object Version;

(b) dependency Status;

(c) issuer or producing Actor Status;

(d) applicable Standards;

(e) applicable Profiles.

3. A current Status shall not automatically determine the historical Status of a Trust Object.

CORRECTION, REPLACEMENT AND PRESERVATION

Article 14

1. A Trust Object lifecycle process shall define conditions for:

(a) Correction;

(b) replacement;

(c) supersession;

(d) withdrawal;

(e) preservation.

2. Replacement or supersession shall create a new Trust Object Identifier unless the applicable Profile expressly provides another controlled mechanism.

3. Previous Trust Objects shall remain identifiable where required for Historical State determination.

Article 15

1. Trust Objects requiring long-term reliance shall be preserved according to the applicable Profile.

2. Preservation requirements may include:

(a) Validation evidence preservation;

(b) timestamp evidence;

(c) cryptographic transition management;

(d) historical dependency records;

(e) integrity verification.

RECORDS AND EVIDENCE

Article 16

1. The Responsible Actor shall maintain records sufficient to reconstruct:

(a) creation;

(b) issuance;

(c) protection;

(d) Validation;

(e) lifecycle changes;

(f) dependency changes;

(g) historical state.

2. Records shall be protected against unauthorised alteration and disclosure.

APPLICABLE STANDARDS

Article 17

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Trust Object Category;

(b) Status;

(c) Qualified Status;

(d) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ISO/IEC 24760-1:2025	Identity and identifier concepts where Trust Objects relate to Subjects or Actors
ISO/IEC 11179-3:2023	Metadata registration principles for Trust Object Metadata
ISO 15489-1:2016	Records management principles for lifecycle evidence
ISO 23081-1:2017	Metadata principles for lifecycle and provenance information
ISO/IEC 27001:2022	Security management controls applicable to Trust Object lifecycle management
ISO/IEC 27002:2022	Security controls applicable to Trust Object protection

IDEHA-IG-OBJ-EAA-001: ELECTRONIC ATTESTATION IMPLEMENTATION

IDEHA-IG-OBJ-GEN-001 Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for the creation, issuance, management, Validation support and lifecycle management of Electronic Attestations.

2. This Guideline applies to Trust Service Providers providing an Electronic Attestation Service and Actors creating, issuing, validating or relying upon Electronic Attestations.

3. This Guideline establishes requirements for:

(a) Attestation Issuer responsibilities;

(b) Attestation Statement implementation;

(c) Source Basis and evidence handling;

(d) Electronic Attestation creation and issuance;

(e) Electronic Attestation lifecycle management;

(f) Validation support.

4. This Guideline applies together with the applicable Electronic Attestation Profile.

5. This Guideline does not:

(a) establish Electronic Attestation as a new Trust Service Category;

(b) establish Qualified Electronic Attestation conditions;

(c) assign Qualified Trust Service Status;

(d) define Attribute semantics belonging to the Data Quality and Semantic Implementation Guideline;

(e) define technical formats, schemas or protocols assigned to Technical Specifications.

ELECTRONIC ATTESTATION SCOPE AND PROFILE

Article 2

1. An Electronic Attestation shall be created according to an applicable Electronic Attestation Profile.

2. The Electronic Attestation Profile shall identify:

(a) the purpose of the Electronic Attestation;

(b) the Subject or matter to which the Attestation Statement relates;

(c) the applicable Attributes or statements;

(d) the applicable Source Basis;

(e) the applicable Assurance Conditions;

(f) the applicable Security Conditions;

(g) the applicable Validation requirements.

3. An Electronic Attestation shall not contain statements outside the scope established by the applicable Profile.

ATTESTATION ISSUER

Article 3

1. An Attestation Issuer shall be identified within each Electronic Attestation.

2. The Attestation Issuer information shall identify:

(a) the issuing Trust Service Provider or Actor;

(b) the Electronic Attestation Service;

(c) the applicable Service Scope;

(d) the applicable Version;

(e) the applicable Profile.

3. The Attestation Issuer shall remain responsible for the creation and issuance process within its assigned scope.

4. The Attestation Issuer shall not assume responsibility for a Source beyond the Source Basis and verification activities performed.

SUBJECT AND ATTESTATION STATEMENT

Article 4

1. An Electronic Attestation shall identify the Subject or matter to which the Attestation Statement relates.

2. The Subject reference shall use an applicable Subject Identifier or another permitted reference defined by the applicable Profile.

3. A Subject Identifier shall:

(a) remain opaque;

(b) not disclose identity type;

(c) not disclose demographic information;

(d) not disclose Status or qualification information.

4. The Attestation Statement shall identify the Attribute, fact or relationship being attested.

Article 5

1. Attribute information included in an Electronic Attestation shall use controlled semantic definitions.

2. The Electronic Attestation shall identify, where applicable:

(a) Attribute Identifier;

(b) Attribute Version;

(c) value domain;

(d) Source Basis;

(e) Provenance information;

(f) applicable Freshness Condition.

3. Attribute values shall remain separate from:

(a) Attribute identifiers;

(b) Subject identifiers;

(c) Trust Object identifiers.

SOURCE BASIS AND EVIDENCE

Article 6

1. Where an Electronic Attestation is based on information obtained from a Source, the Source Basis shall be identified.

2. The Source Basis shall identify, where applicable:

(a) Source Identifier;

(b) Source Scope;

(c) Source Holder;

(d) Source Steward;

(e) relevant evidence;

(f) Provenance information.

3. An Electronic Attestation shall not be considered authoritative solely because it contains information originating from a Source.

Article 7

1. The Attestation Issuer shall evaluate the evidence basis before issuing an Electronic Attestation.

2. The evaluation shall determine, where applicable:

(a) Source applicability;

(b) Attribute scope;

(c) Provenance;

(d) Freshness;

(e) integrity of received information;

(f) applicable Assurance Conditions.

3. The evaluation result shall be retained as issuance evidence.

ELECTRONIC ATTESTATION CREATION AND ISSUANCE

Article 8

1. Before issuing an Electronic Attestation, the Attestation Issuer shall verify that:

(a) the issuance request is authorised;

(b) the Subject or matter is identified;

(c) the Attestation Statement is within scope;

(d) required evidence is available;

(e) applicable conditions are satisfied.

2. The Electronic Attestation shall contain or reference:

(a) Trust Object Identifier;

(b) Attestation Issuer;

(c) Attestation Statement;

(d) issuance time;

(e) applicable Profile;

(f) applicable protection information;

(g) Status information or Status reference where applicable.

Article 9

1. The Attestation Issuer shall protect the Electronic Attestation against unauthorised alteration.

2. Protection mechanisms may include:

(a) Electronic Signature;

(b) Electronic Seal;

(c) another approved integrity mechanism.

3. Where an Electronic Attestation is qualified, the applicable Qualified Object Profile shall identify the required qualified protection dependencies.

ELECTRONIC ATTESTATION LIFECYCLE

Article 10

1. The lifecycle of an Electronic Attestation shall include, where applicable:

(a) creation;

(b) issuance;

(c) activation;

(d) use;

(e) Validation;

(f) correction;

(g) replacement;

(h) suspension;

(i) revocation;

(j) expiration;

(k) withdrawal.

2. Lifecycle states shall be defined by the applicable Profile.

Article 11

1. The Attestation Issuer shall maintain Status information necessary for Validation.

2. Status information shall identify, where applicable:

(a) current Status;

(b) effective time;

(c) reason for Status change;

(d) responsible Actor;

(e) supporting evidence.

3. Status information shall enable determination of the Electronic Attestation state at a relevant time.

QUALIFIED ELECTRONIC ATTESTATIONS

Article 12

1. A Qualified Electronic Attestation shall satisfy the requirements established by the applicable Qualified Object Profile.

2. The Qualified Object Profile shall identify:

(a) required Qualified Trust Service Provider Status;

(b) required Qualified Trust Service Status;

(c) required Source Status where applicable;

(d) required protection mechanisms;

(e) required Assurance Conditions;

(f) required Validation conditions.

3. Qualified Status shall apply only within the scope established by the applicable Qualified Profile.

4. Qualification of a dependency shall not automatically transfer Qualified Status to the Electronic Attestation.

VALIDATION AND RELIANCE

Article 13

1. An Electronic Attestation shall support Validation according to its applicable Profile.

2. Validation shall determine, where applicable:

(a) Attestation Issuer identity;

(b) protection validity;

(c) Attribute integrity;

(d) Source Basis;

(e) Status;

(f) Historical State;

(g) applicable limitations.

3. A Relying Actor shall apply its Local Trust Acceptance Policy before Controlled Reliance.

Article 14

1. An Electronic Attestation shall not by itself establish:

(a) the underlying legal fact;

(b) eligibility;

(c) entitlement;

(d) Authorisation;

(e) a Source authority outside its assigned scope.

2. Reliance shall consider the purpose, scope and limitations of the Electronic Attestation.

CORRECTION AND REPLACEMENT

Article 15

1. The Attestation Issuer shall maintain procedures for:

(a) correction;

(b) replacement;

(c) supersession;

(d) revocation;

(e) withdrawal.

2. Replacement of an Electronic Attestation shall identify:

(a) predecessor Trust Object Identifier;

(b) replacement Trust Object Identifier;

(c) reason for replacement;

(d) effective time.

3. Previous Electronic Attestations shall remain identifiable where required for Historical State determination.

RECORDS AND EVIDENCE

Article 16

1. The Attestation Issuer shall maintain records sufficient to reconstruct:

(a) issuance basis;

(b) Source Basis;

(c) evidence evaluation;

(d) creation process;

(e) protection process;

(f) lifecycle changes;

(g) Validation history.

2. Records shall be protected according to the applicable Security Conditions.

APPLICABLE STANDARDS

Article 17

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Electronic Attestation Category;

(b) Qualified Trust Service Status;

(c) Qualified Trust Object Status;

(d) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 319 401:2024	General trust service provider implementation requirements
ETSI TS 119 461:2025	Identity proofing requirements where identity evidence is evaluated before issuance

Reference	Application
ISO/IEC 11179-3:2023	Attribute metadata registration and semantic identification
ISO/IEC 11179-31:2023	Data-element concepts, value domains and semantic descriptions
ISO/IEC 24760-1:2025	Identity information concepts and relationships
ISO/IEC 27001:2022	Security management controls applicable to attestation issuance
ISO/IEC 27701:2025	Privacy management controls where personal data is processed

IDEHA-IG-OBJ-CRT-001: CERTIFICATE AS SPECIALISED ELECTRONIC ATTESTATION IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Certificates issued as specialised Electronic Attestations within the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Certificate-related Electronic Attestation Services and Actors creating, issuing, validating or relying upon Certificates.

3. This Guideline establishes requirements for:

(a) Certificate identification;

(b) Certificate issuance;

(c) Certificate content;

(d) Certificate lifecycle management;

(e) Certificate Status management;

(f) Certificate Validation support.

4. This Guideline applies together with the applicable Certificate Profile and Technical Specification.

5. This Guideline does not:

(a) establish Certificate as a separate Trust Object Category;

(b) establish a new Trust Service Category;

(c) define X.509 technical structures;

(d) define cryptographic algorithms or parameters;

(e) assign Qualified Status;

(f) replace requirements established by the Main Framework, Electronic Attestation Implementation Guideline or applicable Qualified Object Profile.

CERTIFICATE SCOPE AND PURPOSE

Article 2

1. A Certificate shall be issued only within the scope established by the applicable Certificate Profile.

2. The Certificate Profile shall identify:

(a) Certificate purpose;

(b) Subject category;

(c) Certificate Holder;

(d) applicable Validation Data;

(e) applicable Assurance Conditions;

(f) applicable Security Conditions;

(g) applicable lifecycle conditions.

3. A Certificate shall not contain statements or bindings outside the scope established by the applicable Certificate Profile.

CERTIFICATE ISSUER AND RESPONSIBILITIES

Article 3

1. The Certificate Issuer shall be identified within each issued Certificate.

2. The Certificate Issuer information shall identify:

(a) the issuing Trust Service Provider;

(b) the issuing Electronic Attestation Service;

(c) the applicable Service Scope;

(d) the applicable Certificate Profile.

3. The Certificate Issuer shall remain responsible for:

(a) Certificate issuance;

(b) Certificate lifecycle management;

(c) Certificate Status information;

(d) Certificate issuance evidence.

4. The Certificate Issuer shall not create or alter the legal identity of the Subject through Certificate issuance.

SUBJECT IDENTIFICATION AND BINDING

Article 4

1. A Certificate shall identify the Subject to which the Certificate relates.

2. The Subject identification method shall be defined by the applicable Certificate Profile.

3. The Certificate Profile shall specify:

(a) Subject identification requirements;

(b) identity evidence requirements;

(c) Attribute verification requirements;

(d) representation requirements where applicable.

4. Subject identification information shall remain separate from:

(a) Certificate Identifier;

(b) Serial Number;

(c) Trust Service Identifier;

(d) Subject Identifier.

Article 5

1. Where a Certificate binds Validation Data to a Subject, the Certificate shall identify the Validation Data.

2. The binding shall include:

(a) Subject reference;

(b) Validation Data reference;

(c) Certificate validity period;

(d) Certificate policy information;

(e) applicable restrictions.

3. The binding shall remain within the purpose defined by the Certificate Profile.

CERTIFICATE CONTENT

Article 6

1. The Certificate shall contain or reference information necessary for:

(a) identification;

(b) Validation;

(c) lifecycle management;

(d) reliance within the applicable scope.

2. The Certificate content shall be defined by the applicable Technical Specification.

3. The Technical Specification shall define:

(a) data structure;

(b) encoding;

(c) mandatory fields;

(d) optional fields;

(e) extensions;

(f) policy identifiers;

(g) validation requirements.

Article 7

1. A Certificate shall contain a Certificate Identifier or equivalent identifier mechanism.

2. A Certificate Serial Number shall:

(a) uniquely identify the Certificate within the issuer scope;

(b) not be reused;

(c) remain associated with the issuing Actor.

3. The relationship between the Certificate Identifier and the Trust Object Identifier shall be defined by the applicable Profile.

CERTIFICATE ISSUANCE

Article 8

1. Before issuing a Certificate, the Certificate Issuer shall verify that:

(a) the issuance request is authorised;

(b) the Subject is identified;

(c) required evidence is available;

(d) required Attributes have been verified;

(e) applicable conditions are satisfied.

2. The Certificate Issuer shall maintain issuance evidence.

3. Issuance evidence shall include, where applicable:

(a) identity verification results;

(b) Attribute verification results;

(c) approval information;

(d) issuance time;

(e) Certificate Profile Version.

CERTIFICATE LIFECYCLE

Article 9

1. The lifecycle of a Certificate shall include, where applicable:

(a) request;

(b) approval;

(c) issuance;

(d) activation;

(e) suspension;

(f) revocation;

(g) expiration;

(h) renewal;

(i) replacement.

2. The Certificate Issuer shall maintain lifecycle information for each issued Certificate.

Article 10

1. Certificate Status information shall enable determination of whether a Certificate remains valid for its intended purpose.

2. Certificate Status information shall identify:

(a) Certificate Identifier;

(b) Status;

(c) effective time;

(d) reason for Status change where applicable;

(e) responsible Actor.

3. Certificate Status information shall support historical determination where required.

QUALIFIED CERTIFICATES

Article 11

1. A Qualified Certificate shall satisfy the requirements established by the applicable Qualified Object Profile.

2. The Qualified Object Profile shall identify:

(a) required Qualified Trust Service Provider Status;

(b) required Qualified Trust Service Status;

(c) required Certificate Profile;

(d) required Validation conditions;

(e) required Security Conditions.

3. Qualified Certificate Status shall apply only within the approved Qualified Scope.

4. Qualification of the Certificate Issuer shall not automatically qualify every issued Certificate.

CERTIFICATE VALIDATION

Article 12

1. Certificate Validation shall determine whether the Certificate satisfies the applicable Certificate Profile and Validation requirements.

2. Validation shall determine, where applicable:

(a) Certificate integrity;

(b) issuer identity;

(c) Subject binding;

(d) certificate chain validity;

(e) Certificate Status;

(f) policy applicability;

(g) Historical State.

3. Certificate Validation shall be performed according to the applicable Validation and Verification Service requirements.

Article 13

1. A Certificate shall not by itself establish:

(a) Authorisation;

(b) entitlement;

(c) legal capacity;

(d) eligibility;

(e) any fact outside the Certificate scope.

2. Reliance upon a Certificate shall consider:

(a) Certificate purpose;

(b) Certificate Profile;

(c) Status;

(d) Source Basis where applicable;

(e) applicable Reliance Conditions.

CERTIFICATE REPLACEMENT AND CESSATION

Article 14

1. The Certificate Issuer shall maintain procedures for:

(a) renewal;

(b) replacement;

(c) suspension;

(d) revocation;

(e) withdrawal.

2. Replacement of a Certificate shall identify:

(a) predecessor Certificate;

(b) replacement Certificate;

(c) effective time;

(d) reason for replacement.

3. Previous Certificates shall remain identifiable where required for Historical State determination.

RECORDS AND EVIDENCE

Article 15

1. The Certificate Issuer shall maintain records sufficient to reconstruct:

(a) issuance;

(b) identity verification;

(c) Certificate creation;

(d) Certificate Status changes;

(e) Validation history;

(f) replacement and revocation events.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 16

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Certificate Category;

(b) Qualified Status;

(c) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
RFC 5280	X.509 public key certificate structure, certificate path validation and certificate extensions
ETSI EN 319 411-1	General policy requirements for certificate-issuing Trust Service Providers
ETSI EN 319 411-2	Policy requirements for qualified certificate issuing Trust Service Providers
ETSI EN 319 412-1	Certificate profile requirements and common certificate data structures

Reference	Application
ETSI EN 319 412-2	Certificate profiles for natural persons
ETSI EN 319 412-3	Certificate profiles for legal persons
ETSI EN 319 412-5	Qualified certificate statements
ISO/IEC 24760-1:2025	Identity concepts and identity information relationships
ISO/IEC 27001:2022	Security management controls applicable to Certificate services

IDEHA-IG-OBJ-DSG-001: DIGITAL SIGNATURE AND CREATION DATA IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Digital Signature Creation Data, Digital Signature Validation Data, Digital Signature Creation Mechanisms and Digital Signature Creation Devices.

2. This Guideline applies to Actors responsible for generating, protecting, operating, assessing, managing or relying upon Digital Signature creation environments.

3. This Guideline establishes requirements for:

(a) generation and protection of Digital Signature Creation Data;

(b) management of Digital Signature Validation Data;

(c) operation of Digital Signature Creation Mechanisms;

(d) operation of Digital Signature Creation Devices;

(e) security boundaries protecting Digital Signature Creation Data;

(f) conformity assessment and assurance evidence;

(g) lifecycle management and compromise handling.

4. This Guideline applies together with:

(a) IDEHA-IG-SVC-DSG-001 Digital Signing Service Implementation;

(b) IDEHA-IG-SVC-SIG-001 Electronic Signature Service Implementation;

(c) IDEHA-IG-SVC-SEL-001 Electronic Seal Service Implementation;

(d) IDEHA-IG-SEC-CRY-001 Cryptographic Controls and Cryptographic Agility Implementation;

(e) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish requirements for:

(a) Electronic Signatures;

(b) Electronic Seals;

(c) Advanced Electronic Signatures;

(d) Advanced Electronic Seals;

(e) Qualified Electronic Signatures;

(f) Qualified Electronic Seals;

(g) Signatory identification;

(h) Seal Creator identification;

(i) signing intent;

(j) sealing intent;

(k) signature workflows;

(l) signature formats;

(m) signature Validation procedures.

DIGITAL SIGNATURE CREATION DATA

Article 2

1. Digital Signature Creation Data shall consist of cryptographic data uniquely associated with the creation of Digital Signatures.

2. Digital Signature Creation Data shall be generated and managed within an approved cryptographic environment.

3. The responsible Actor shall ensure that Digital Signature Creation Data:

(a) is generated using approved cryptographic mechanisms;

(b) remains confidential;

(c) remains protected against unauthorised extraction;

(d) remains protected against unauthorised duplication;

(e) is used only through authorised cryptographic operations.

4. Digital Signature Creation Data shall not be used for purposes outside the approved Digital Signature creation function.

Article 3

1. Generation of Digital Signature Creation Data shall ensure:

(a) practical uniqueness;

(b) sufficient unpredictability;

(c) appropriate cryptographic strength;

(d) protection of generation processes;

(e) traceability of lifecycle events.

2. The applicable Cryptographic Profile shall specify:

(a) permitted algorithms;

(b) cryptographic parameters;

(c) key-generation requirements;

(d) transition conditions.

DIGITAL SIGNATURE VALIDATION DATA

Article 4

1. Digital Signature Validation Data shall enable verification of a Digital Signature.

2. Digital Signature Validation Data shall correspond exclusively to the associated Digital Signature Creation Data.

3. The responsible Actor shall maintain evidence establishing the association between:

(a) Digital Signature Creation Data;

(b) Digital Signature Validation Data;

(c) Digital Signature Creation Device;

(d) applicable cryptographic mechanism.

4. The technical representation of Digital Signature Validation Data shall be defined by the applicable Technical Specification.

DIGITAL SIGNATURE CREATION MECHANISM

Article 5

1. A Digital Signature Creation Mechanism shall provide the cryptographic function used to generate Digital Signatures.

2. The Digital Signature Creation Mechanism shall identify:

(a) cryptographic operations;

(b) protected functions;

(c) required inputs;

(d) security assumptions;

(e) external dependencies.

3. The Digital Signature Creation Mechanism shall operate within an identified security boundary.

Article 6

1. A Digital Signature Creation Mechanism shall ensure that:

(a) Digital Signature Creation Data is used only by authorised functions;

(b) cryptographic operations are executed according to approved requirements;

(c) unauthorised modification of cryptographic functions is prevented;

(d) security-relevant events are recorded where required.

DIGITAL SIGNATURE CREATION DEVICE

Article 7

1. A Digital Signature Creation Device shall provide the protected environment in which Digital Signature Creation Data is generated, stored or used.

2. The Digital Signature Creation Device shall identify:

(a) Device Identifier;

(b) device category;

(c) security boundary;

(d) configuration Version;

(e) operational Status;

(f) conformity evidence where applicable.

3. The Device Identifier shall:

(a) remain stable during the applicable lifecycle;

(b) not disclose personal information;

(c) not encode Status;

(d) not encode qualification level.

Article 8

1. The Digital Signature Creation Device security boundary shall identify:

(a) protected components;

(b) trusted functions;

(c) cryptographic functions;

(d) administrative interfaces;

(e) external interfaces;

(f) dependencies.

2. The security boundary shall protect Digital Signature Creation Data against:

(a) unauthorised disclosure;

(b) unauthorised extraction;

(c) unauthorised duplication;

(d) unauthorised modification;

(e) unauthorised use.

DEVICE ACTIVATION AND CONTROLLED OPERATION

Article 9

1. A Digital Signature Creation Device shall support controlled activation of Digital Signature creation operations.

2. Activation controls shall ensure:

(a) authorised operation;

(b) protection of activation information;

(c) prevention of unauthorised activation;

(d) detection of abnormal activity.

3. Device activation requirements shall remain separate from:

(a) Authentication Service operation;

(b) Electronic Signature Service operation;

(c) Authorisation Service decisions.

REMOTE DIGITAL SIGNATURE CREATION DEVICES

Article 10

1. A remote Digital Signature Creation Device shall maintain a controlled security boundary between:

(a) Signatory interaction;

(b) activation functions;

(c) cryptographic functions;

(d) Digital Signature Creation Data.

2. A remote Digital Signature Creation Device shall identify:

(a) Cryptographic Module;

(b) Signature Activation Mechanism where applicable;

(c) Signature Activation Data where applicable;

(d) trusted communication channels;

(e) operational responsibilities.

3. The applicable Profile shall specify requirements for remote operation and sole control conditions where applicable.

QUALIFIED DIGITAL SIGNATURE CREATION DEVICES

Article 11

1. A Digital Signature Creation Device intended to obtain Qualified Status shall satisfy the applicable Qualified Object Profile.

2. The Qualified Object Profile shall specify:

(a) applicable Protection Profile;

(b) required assurance level;

(c) required conformity evidence;

(d) evaluated configuration;

(e) lifecycle conditions;

(f) operational limitations.

3. A cryptographic module, Hardware Security Module, secure element or other cryptographic component shall not by itself constitute a Qualified Digital Signature Creation Device.

Article 12

1. The minimum security evaluation level for a Qualified Digital Signature Creation Device shall be:

(a) Common Criteria Evaluation Assurance Level 4 augmented by applicable augmentation requirements; or

(b) an equivalent assurance level recognised through the applicable qualification route.

2. The security evaluation shall identify:

(a) Target of Evaluation;

(b) Security Target;

(c) Protection Profile;

(d) evaluated configuration;

(e) certification scope;

(f) applicable limitations.

3. A modification affecting the evaluated security boundary shall require reassessment where required by the applicable conformity route.

CRYPTOGRAPHIC MODULES AND COMPOSITE DEVICES

Article 13

1. Where a Digital Signature Creation Device includes a Cryptographic Module, the Cryptographic Module shall satisfy the applicable security requirements.

2. Where a Digital Signature Creation Device consists of multiple security components, the conformity evidence shall identify:

(a) each evaluated component;

(b) the relationship between components;

(c) the combined security boundary;

(d) applicable dependencies.

3. A composite Digital Signature Creation Device shall be assessed as the complete configuration intended for operation.

LIFECYCLE MANAGEMENT

Article 14

1. The lifecycle of Digital Signature Creation Data and Digital Signature Creation Devices shall include, where applicable:

(a) generation;

(b) registration;

(c) configuration;

(d) evaluation;

(e) activation;

(f) operation;

(g) maintenance;

(h) suspension;

(i) replacement;

(j) retirement;

(k) destruction.

2. Lifecycle events affecting security assurance shall be recorded.

Article 15

1. Changes affecting the security properties of a Digital Signature Creation Device shall be assessed before implementation.

2. The assessment shall consider:

(a) hardware changes;

(b) firmware changes;

(c) software changes;

(d) cryptographic changes;

(e) configuration changes;

(f) certification impact.

COMPROMISE MANAGEMENT

Article 16

1. Where Digital Signature Creation Data or a Digital Signature Creation Device is compromised or suspected to be compromised, the responsible Actor shall implement protective measures.

2. Protective measures shall include, where applicable:

(a) restriction of operation;

(b) preservation of evidence;

(c) investigation;

(d) replacement;

(e) reassessment.

3. The effect of compromise on previously created Digital Signatures shall be determined through the applicable Validation process.

RECORDS AND EVIDENCE

Article 17

1. The responsible Actor shall maintain records sufficient to reconstruct:

(a) Digital Signature Creation Data lifecycle;

(b) Digital Signature Creation Device identity;

(c) device configuration;

(d) security evaluation;

(e) cryptographic operations;

(f) compromise events.

2. Records shall identify the relationship between:

(a) Digital Signature Creation Data;

(b) Digital Signature Validation Data;

(c) Digital Signature Creation Mechanism;

(d) Digital Signature Creation Device.

APPLICABLE STANDARDS

Article 18

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Electronic Signature Status;

(b) Qualified Electronic Signature Status;

(c) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
EN 419 211 series	Protection Profiles for secure signature creation devices
EN 419 241-1	General security requirements for trustworthy systems supporting server signing
EN 419 241-2	Protection Profile for QSCD for server signing
EN 419 221-5	Protection Profile for cryptographic modules used in Trust Services
ISO/IEC 15408 series	Common Criteria security evaluation framework
ISO/IEC 18045	Common Criteria evaluation methodology
ISO/IEC 19790	Security requirements for cryptographic modules
ISO/IEC 24759	Cryptographic module testing requirements
ISO/IEC 11770 series	Key management requirements
ETSI TS 119 312	Cryptographic suites and mechanisms

IDEHA-IG-OBJ-SIG-001: ELECTRONIC SIGNATURE IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Electronic Signatures within the Trust Framework.

2. This Guideline applies to Actors creating, managing, validating or relying upon Electronic Signatures within the scope established by the applicable Framework Instruments.

3. This Guideline establishes requirements for:

(a) Electronic Signature creation context;

(b) Signatory attribution;

(c) signing act implementation;

(d) signing intent evidence;

(e) association between the Electronic Signature and signed data;

(f) Electronic Signature lifecycle management;

(g) Signature Evidence management.

4. This Guideline applies together with:

(a) IDEHA-IG-OBJ-DSG-001 Digital Signature Creation Data and Device Implementation;

(b) IDEHA-IG-SVC-DSG-001 Digital Signing Service Implementation;

(c) IDEHA-IG-SVC-SIG-001 Electronic Signature Service Implementation;

(d) IDEHA-IG-SVC-VVS-001 Validation and Verification Service Implementation;

(e) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) Digital Signature Creation Data requirements;

(b) Digital Signature Creation Device requirements;

(c) cryptographic algorithms;

(d) cryptographic parameters;

(e) signature format structures;

(f) Certificate issuance requirements;

(g) Certificate Service requirements.

Those matters shall be implemented through the applicable Framework Instruments.

ELECTRONIC SIGNATURE SCOPE

Article 2

1. An Electronic Signature shall be associated with identified electronic data and an identified signing context.

2. The Electronic Signature implementation shall identify:

(a) the signed data;

(b) the Signatory;

(c) the signing event;

(d) the Digital Signature where applicable;

(e) the applicable Electronic Signature Profile.

3. The Electronic Signature shall remain associated with the signed data throughout its lifecycle.

Article 3

1. The applicable Electronic Signature Profile shall define:

(a) the purpose of the Electronic Signature;

(b) the applicable Signatory requirements;

(c) the required evidence;

(d) the applicable Assurance Conditions;

(e) the applicable Security Conditions;

(f) the applicable Validation requirements.

2. An Electronic Signature Profile shall not modify the Electronic Signature Categories or Controlled Effects established by the Main Framework.

SIGNATORY IDENTIFICATION AND ATTRIBUTION

Article 4

1. The Electronic Signature implementation shall establish the relationship between the Electronic Signature and the Signatory.

2. The applicable Electronic Signature Profile shall specify:

(a) Signatory identification requirements;

(b) required Authentication conditions;

(c) required evidence;

(d) applicable identity binding requirements.

3. The Signatory reference shall remain separate from:

(a) Digital Signature Identifier;

(b) Trust Object Identifier;

(c) Certificate Identifier;

(d) Signature Value.

Article 5

1. The Electronic Signature shall provide evidence sufficient to determine the Signatory associated with the signing event.

2. Signatory attribution evidence shall identify, where applicable:

(a) Signatory reference;

(b) Authentication Event;

(c) signing service interaction;

(d) applicable Signature Profile;

(e) signing time;

(f) relevant limitations.

SIGNING ACT AND INTENT

Article 6

1. The Electronic Signature implementation shall establish evidence of the signing act.

2. The signing act evidence shall identify, where applicable:

(a) the Signatory action;

(b) the signed data presented for signing;

(c) the signing event;

(d) the creation request;

(e) the resulting Electronic Signature.

3. The applicable Profile shall define the required level of evidence.

Article 7

1. Where signing intent is required, the Electronic Signature implementation shall record evidence demonstrating that the Signatory intended to apply the Electronic Signature to the identified data.

2. Signing intent evidence may include:

(a) explicit confirmation;

(b) user interaction evidence;

(c) transaction confirmation;

(d) another approved indication.

3. Signing intent shall remain separate from:

(a) Authentication;

(b) Authorisation;

(c) Digital Signature creation;

(d) Certificate issuance.

SIGNED DATA ASSOCIATION

Article 8

1. An Electronic Signature shall remain bound to the electronic data to which it relates.

2. The binding shall enable determination of:

(a) the signed data;

(b) the Electronic Signature;

(c) the applicable Signature Profile;

(d) the relevant creation context.

3. Any subsequent alteration of the signed data shall be detectable according to the applicable Validation requirements.

Article 9

1. The applicable Technical Specification shall define:

(a) signed-data representation;

(b) signature container format;

(c) signature attributes;

(d) encoding;

(e) interoperability requirements.

2. This Guideline shall not define technical signature formats.

ADVANCED ELECTRONIC SIGNATURE IMPLEMENTATION

Article 10

1. An Advanced Electronic Signature shall satisfy the conditions established by the Main Framework.

2. The applicable Electronic Signature Profile shall specify implementation requirements for:

(a) unique association with the Signatory;

(b) identification of the Signatory;

(c) Signatory control over the signature creation process;

(d) detection of subsequent alteration of signed data.

3. The implementation evidence shall support Validation of the applicable Advanced Electronic Signature conditions.

QUALIFIED ELECTRONIC SIGNATURE IMPLEMENTATION

Article 11

1. A Qualified Electronic Signature shall satisfy the conditions established by the Main Framework and the applicable Qualified Object Profile.

2. The applicable Qualified Object Profile shall identify:

(a) required Advanced Electronic Signature conditions;

(b) required Qualified Certificate;

(c) required Qualified Digital Signature Creation Device;

(d) required Validation conditions;

(e) required preservation conditions where applicable.

3. The presence of:

(a) a Qualified Certificate;

(b) a Qualified Digital Signature Creation Device;

(c) a Qualified Trust Service Provider;

shall not individually establish a Qualified Electronic Signature.

4. Qualified Status shall apply only where all applicable qualified conditions are satisfied.

SIGNATURE EVIDENCE

Article 12

1. The Electronic Signature implementation shall maintain evidence sufficient to support Validation.

2. Signature Evidence shall identify, where applicable:

(a) signed data;

(b) Signatory;

(c) Digital Signature;

(d) Certificate dependency;

(e) creation time;

(f) signing event;

(g) applicable Profile;

(h) Validation dependencies.

3. Signature Evidence shall be protected against unauthorised alteration.

Article 13

1. Where long-term reliance is required, the Electronic Signature shall support preservation of evidence required for Historical Validation.

2. Preservation evidence may include:

(a) timestamps;

(b) Certificate information;

(c) Status information;

(d) Validation results;

(e) cryptographic transition information.

3. Preservation requirements shall be defined by the applicable Profile.

ELECTRONIC SIGNATURE LIFECYCLE

Article 14

1. The lifecycle of an Electronic Signature shall include, where applicable:

(a) creation;

(b) delivery;

(c) Validation;

(d) preservation;

(e) historical evaluation.

2. Lifecycle events affecting reliance shall be recorded.

Article 15

1. Changes affecting Electronic Signature dependencies shall be assessed where they may affect:

(a) attribution;

(b) Validation;

(c) Historical State;

(d) Controlled Reliance.

2. The assessment shall identify:

(a) affected Electronic Signatures;

(b) affected Certificates;

(c) affected Digital Signature Creation Devices;

(d) applicable transition measures.

ACCESSIBILITY AND SAFEGUARDS

Article 16

1. Electronic Signature implementations shall provide Accessible Alternatives where required by the applicable Safeguard Conditions.

2. The applicable Profile shall define:

(a) alternative signing methods;

(b) assisted signing arrangements;

(c) accessibility requirements;

(d) human support conditions.

3. Accessibility measures shall preserve the applicable Assurance Conditions.

RECORDS AND EVIDENCE

Article 17

1. The responsible Actor shall maintain records sufficient to reconstruct:

(a) signing request;

(b) Signatory identification;

(c) signing event;

(d) Digital Signature creation reference;

(e) Signature Evidence;

(f) lifecycle events.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 18

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Electronic Signature Category;

(b) Qualified Electronic Signature Status;

(c) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 319 102-1	Validation process requirements for electronic signatures

Reference	Application
ETSI EN 319 122-1	CAdES signature representation requirements
ETSI EN 319 132-1	XAdES signature representation requirements
ETSI EN 319 142-1	PAdES signature representation requirements
ETSI TS 119 182-1	JAdES signature representation requirements
ETSI EN 319 312	Cryptographic suites where applicable
ETSI EN 319 411-2	Qualified certificate service requirements where qualified certificates are used
ISO/IEC 29115	Authentication assurance considerations for Signatory identification
ISO/IEC 24760 series	Identity information and identity binding considerations

IDEHA-IG-OBJ-SEL-001: ELECTRONIC SEAL IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Electronic Seals within the Trust Framework.

2. This Guideline applies to Actors creating, managing, validating or relying upon Electronic Seals within the scope established by the applicable Framework Instruments.

3. This Guideline establishes requirements for:

(a) Electronic Seal creation context;

(b) Seal Creator attribution;

(c) organisational authority and control;

(d) sealing act implementation;

(e) association between the Electronic Seal and sealed data;

(f) Electronic Seal lifecycle management;

(g) Seal Evidence management.

4. This Guideline applies together with:

(a) IDEHA-IG-OBJ-DSG-001 Digital Signature Creation Data and Device Implementation;

(b) IDEHA-IG-SVC-DSG-001 Digital Signing Service Implementation;

(c) IDEHA-IG-SVC-SEL-001 Electronic Seal Service Implementation;

(d) IDEHA-IG-SVC-VVS-001 Validation and Verification Service Implementation;

(e) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) Digital Signature Creation Data requirements;

(b) Digital Signature Creation Device requirements;

(c) cryptographic algorithms;

(d) cryptographic parameters;

(e) certificate issuance requirements;

(f) Certificate Service requirements;

(g) seal format structures;

(h) Seal Validation procedures.

Those matters shall be implemented through the applicable Framework Instruments.

ELECTRONIC SEAL SCOPE

Article 2

1. An Electronic Seal shall be associated with identified electronic data and an identified Seal Creator.

2. The Electronic Seal implementation shall identify:

(a) the sealed data;

(b) the Seal Creator;

(c) the sealing event;

(d) the Digital Signature where applicable;

(e) the applicable Electronic Seal Profile.

3. The Electronic Seal shall remain associated with the sealed data throughout its lifecycle.

Article 3

1. The applicable Electronic Seal Profile shall define:

(a) the purpose of the Electronic Seal;

(b) the Seal Creator requirements;

(c) the required evidence;

(d) the applicable Assurance Conditions;

(e) the applicable Security Conditions;

(f) the applicable Validation requirements.

2. An Electronic Seal Profile shall not modify the Electronic Seal Categories or Controlled Effects established by the Main Framework.

SEAL CREATOR IDENTIFICATION AND ATTRIBUTION

Article 4

1. The Electronic Seal implementation shall establish the relationship between the Electronic Seal and the Seal Creator.

2. The applicable Electronic Seal Profile shall specify:

(a) Seal Creator identification requirements;

(b) organisational identification requirements;

(c) authority verification requirements;

(d) required evidence.

3. The Seal Creator reference shall remain separate from:

(a) Digital Signature Identifier;

(b) Trust Object Identifier;

(c) Certificate Identifier;

(d) Signature Value.

Article 5

1. The Electronic Seal shall provide evidence sufficient to determine the organisational Actor associated with the sealing event.

2. Seal Creator attribution evidence shall identify, where applicable:

(a) Seal Creator reference;

(b) initiating Actor;

(c) sealing authority;

(d) sealing event;

(e) applicable Electronic Seal Profile;

(f) sealing time;

(g) relevant limitations.

ORGANISATIONAL AUTHORITY AND CONTROL

Article 6

1. An Electronic Seal shall be created only where the Seal Creator has authority to apply the seal within the applicable scope.

2. The responsible Actor shall maintain evidence demonstrating:

(a) identity of the Seal Creator;

(b) authority to apply the Electronic Seal;

(c) scope of authority;

(d) validity period;

(e) applicable limitations.

3. Authority to apply an Electronic Seal shall remain separate from:

(a) Digital Signature creation;

(b) Authentication;

(c) Authorisation;

(d) legal effect of the sealed data.

Article 7

1. Where sealing is performed automatically, the responsible Actor shall maintain evidence demonstrating:

(a) the initiating system or process;

(b) the applicable policy;

(c) the authority permitting automated sealing;

(d) the sealed-data determination;

(e) the sealing event.

2. Automated sealing shall not remove the requirement to establish the Seal Creator.

SEALING ACT AND EVIDENCE

Article 8

1. The Electronic Seal implementation shall establish evidence of the sealing act.

2. Sealing act evidence shall identify, where applicable:

(a) the sealed data;

(b) the Seal Creator;

(c) the sealing request;

(d) the sealing event;

(e) the resulting Electronic Seal.

3. The applicable Profile shall define the required evidence level.

Article 9

1. The Electronic Seal shall remain bound to the electronic data to which it relates.

2. The binding shall enable determination of:

(a) the sealed data;

(b) the Electronic Seal;

(c) the applicable Electronic Seal Profile;

(d) the relevant creation context.

3. Any subsequent alteration of the sealed data shall be detectable according to the applicable Validation requirements.

Article 10

1. The applicable Technical Specification shall define:

(a) sealed-data representation;

(b) seal container format;

(c) seal attributes;

(d) encoding;

(e) interoperability requirements.

2. This Guideline shall not define technical seal formats.

ADVANCED ELECTRONIC SEAL IMPLEMENTATION

Article 11

1. An Advanced Electronic Seal shall satisfy the conditions established by the Main Framework.

2. The applicable Electronic Seal Profile shall specify implementation requirements for:

(a) unique association with the Seal Creator;

(b) identification of the Seal Creator;

(c) Seal Creator control over the seal creation process;

(d) detection of subsequent alteration of sealed data.

3. The implementation evidence shall support Validation of the applicable Advanced Electronic Seal conditions.

QUALIFIED ELECTRONIC SEAL IMPLEMENTATION

Article 12

1. A Qualified Electronic Seal shall satisfy the conditions established by the Main Framework and the applicable Qualified Object Profile.

2. The applicable Qualified Object Profile shall identify:

(a) required Advanced Electronic Seal conditions;

(b) required Qualified Certificate;

(c) required Qualified Digital Signature Creation Device;

(d) required Validation conditions;

(e) preservation requirements where applicable.

3. The presence of:

(a) a Qualified Certificate;

(b) a Qualified Digital Signature Creation Device;

(c) a Qualified Trust Service Provider;

shall not individually establish a Qualified Electronic Seal.

4. Qualified Status shall apply only where all applicable qualified conditions are satisfied.

SEAL EVIDENCE

Article 13

1. The Electronic Seal implementation shall maintain evidence sufficient to support Validation.

2. Seal Evidence shall identify, where applicable:

(a) sealed data;

(b) Seal Creator;

(c) Digital Signature;

(d) Certificate dependency;

(e) sealing time;

(f) sealing event;

(g) applicable Profile;

(h) Validation dependencies.

3. Seal Evidence shall be protected against unauthorised alteration.

Article 14

1. Where long-term reliance is required, the Electronic Seal shall support preservation of evidence required for Historical Validation.

2. Preservation evidence may include:

(a) timestamps;

(b) Certificate information;

(c) Status information;

(d) Validation results;

(e) cryptographic transition information.

3. Preservation requirements shall be defined by the applicable Profile.

ELECTRONIC SEAL LIFECYCLE

Article 15

1. The lifecycle of an Electronic Seal shall include, where applicable:

(a) creation;

(b) delivery;

(c) Validation;

(d) preservation;

(e) historical evaluation.

2. Lifecycle events affecting reliance shall be recorded.

Article 16

1. Changes affecting Electronic Seal dependencies shall be assessed where they may affect:

(a) attribution;

(b) Validation;

(c) Historical State;

(d) Controlled Reliance.

2. The assessment shall identify:

(a) affected Electronic Seals;

(b) affected Certificates;

(c) affected Digital Signature Creation Devices;

(d) applicable transition measures.

ACCESSIBILITY AND SAFEGUARDS

Article 17

1. Electronic Seal implementations used for organisational processes shall maintain accessibility and safeguard requirements where natural persons interact with the sealing process.

2. The applicable Profile shall define:

(a) human interaction requirements;

(b) approval conditions;

(c) accessibility requirements;

(d) assisted operation conditions.

3. Accessibility measures shall preserve applicable Assurance Conditions.

RECORDS AND EVIDENCE

Article 18

1. The responsible Actor shall maintain records sufficient to reconstruct:

(a) sealing request;

(b) Seal Creator identification;

(c) sealing authority;

(d) sealing event;

(e) Digital Signature creation reference;

(f) Seal Evidence;

(g) lifecycle events.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 19

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Electronic Seal Category;

(b) Qualified Electronic Seal Status;

(c) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 319 102-1	Validation process requirements for electronic signatures and seals
ETSI EN 319 122-1	CAdES seal representation requirements
ETSI EN 319 132-1	XAdES seal representation requirements
ETSI EN 319 142-1	PAdES seal representation requirements
ETSI TS 119 182-1	JAdES seal representation requirements
ETSI EN 319 411-1	General policy requirements for certificate-issuing Trust Service Providers where certificates are used
ETSI EN 319 411-2	Qualified certificate issuing requirements where qualified seals are used
RFC 5280	Certificate validation and public-key certificate processing
ISO/IEC 24760 series	Identity information and organisational identity relationship considerations
ISO/IEC 27001:2022	Security management controls applicable to seal creation processes

IG14: ELECTRONIC SIGNATURE SERVICE IMPLEMENTATION

IDEHA-IG-SVC-SIG-001 Version: 0.1

IDEHA-IG-OBJ-TST-001 Electronic Timestamp Implementation

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Electronic Timestamps and Qualified Electronic Timestamps within the Trust Framework.

2. This Guideline applies to Actors creating, managing, validating or relying upon Electronic Timestamps within the scope established by the applicable Framework Instruments.

3. This Guideline establishes requirements for:

(a) Electronic Timestamp object identification;

(b) binding of electronic data to an identified time;

(c) timestamp evidence;

(d) timestamp object lifecycle management;

(e) dependencies required for Validation;

(f) Qualified Electronic Timestamp object conditions.

4. This Guideline applies together with:

(a) IDEHA-IG-SVC-TST-001 Electronic Timestamp Service Implementation;

(b) IDEHA-IG-SVC-VVS-001 Validation and Verification Service Implementation;

(c) IDEHA-IG-OBJ-DSG-001 Digital Signature Creation Data and Device Implementation;

(d) IDEHA-IG-SEC-CRY-001 Cryptographic Controls and Cryptographic Agility Implementation;

(e) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) Electronic Timestamp Service operation;

(b) Trust Service Provider requirements;

(c) time-source operation procedures;

(d) clock synchronisation architecture;

(e) cryptographic algorithm selection;

(f) timestamp transport protocols;

(g) signature format timestamp integration.

Those matters shall be implemented through the applicable Framework Instruments.

ELECTRONIC TIMESTAMP SCOPE

Article 2

1. An Electronic Timestamp shall establish a binding between identified electronic data and an identified time.

2. The Electronic Timestamp shall identify:

(a) the referenced electronic data or data representation;

(b) the generated time value;

(c) the Timestamp Issuer;

(d) the applicable Timestamp Profile;

(e) the protection mechanism.

3. The Electronic Timestamp shall remain associated with the referenced electronic data throughout its lifecycle.

Article 3

1. The applicable Timestamp Profile shall define:

(a) the purpose of the Electronic Timestamp;

(b) the data reference method;

(c) the required time accuracy;

(d) the required evidence;

(e) the applicable Validation conditions;

(f) the applicable Security Conditions.

2. A Timestamp Profile shall not modify the Electronic Timestamp Category or Controlled Effects established by the Main Framework.

TIMESTAMP DATA BINDING

Article 4

1. An Electronic Timestamp shall identify the electronic data to which the time value applies.

2. The data binding shall enable determination of:

(a) the referenced electronic data;

(b) the applied data representation;

(c) the time value;

(d) the Timestamp Issuer;

(e) the applicable Profile.

3. The Electronic Timestamp shall not require disclosure of the original electronic data where a protected data reference is used.

Article 5

1. Where a digest or equivalent data reference is used, the applicable Technical Specification shall define:

(a) the data-reference representation;

(b) the permitted cryptographic mechanisms;

(c) the encoding;

(d) interoperability requirements.

2. A digest or data reference shall not by itself establish the legal meaning, ownership or validity of the referenced data.

TIME INFORMATION

Article 6

1. An Electronic Timestamp shall contain or reference an identified time value.

2. The time information shall identify, where applicable:

(a) generation time;

(b) time precision;

(c) time accuracy;

(d) applicable time reference;

(e) uncertainty information.

3. The interpretation of time information shall be defined by the applicable Timestamp Profile.

Article 7

1. The Electronic Timestamp shall provide evidence sufficient to determine the relationship between:

(a) the referenced electronic data;

(b) the identified time;

(c) the Timestamp Issuer;

(d) the applicable Timestamp Profile.

2. Timestamp evidence shall remain available for Validation according to the applicable lifecycle requirements.

TIMESTAMP PROTECTION

Article 8

1. An Electronic Timestamp shall be protected against unauthorised alteration.

2. Protection mechanisms shall ensure:

(a) integrity of the timestamp information;

(b) authenticity of the Timestamp Issuer;

(c) detection of modification.

3. The protection mechanism shall remain separate from the Timestamp Category.

Article 9

1. Where an Electronic Timestamp depends on another Trust Object, the dependency shall be identified.

2. Dependencies may include:

(a) Certificate;

(b) Electronic Signature;

(c) Electronic Seal;

(d) Trust List information;

(e) other Validation evidence.

3. A dependency shall not transfer its Status, Qualified Status or Controlled Effects to the Electronic Timestamp.

QUALIFIED ELECTRONIC TIMESTAMP

Article 10

1. A Qualified Electronic Timestamp shall satisfy the requirements established by the Main Framework and the applicable Qualified Object Profile.

2. The Qualified Object Profile shall identify:

(a) required Qualified Trust Service Provider Status;

(b) required Qualified Trust Service Status;

(c) required time conditions;

(d) required protection conditions;

(e) required Validation conditions;

(f) required evidence.

3. Qualification of the Electronic Timestamp Service shall not automatically qualify every Electronic Timestamp issued by that service.

4. Qualified Status shall apply only where all applicable qualified conditions are satisfied.

VALIDATION SUPPORT

Article 11

1. An Electronic Timestamp shall support Validation according to the applicable Validation requirements.

2. Validation support shall enable determination of:

(a) timestamp integrity;

(b) Timestamp Issuer identity;

(c) referenced data binding;

(d) time information;

(e) protection validity;

(f) Status information;

(g) Historical State.

3. Validation requirements shall be implemented through the Validation and Verification Service Implementation.

Article 12

1. An Electronic Timestamp shall not by itself establish:

(a) ownership of the referenced data;

(b) legal validity of the referenced data;

(c) Authorisation;

(d) approval;

(e) consent;

(f) any fact expressed by the referenced data.

2. Reliance upon an Electronic Timestamp shall consider:

(a) purpose;

(b) Profile;

(c) Status;

(d) Validation Result;

(e) applicable Reliance Conditions.

TIMESTAMP LIFECYCLE

Article 13

1. The lifecycle of an Electronic Timestamp shall include, where applicable:

(a) creation;

(b) issuance;

(c) Validation;

(d) preservation;

(e) historical evaluation.

2. Lifecycle information affecting reliance shall be recorded.

Article 14

1. Changes affecting Electronic Timestamp dependencies shall be assessed where they may affect:

(a) integrity;

(b) Validation;

(c) Historical State;

(d) Controlled Reliance.

2. The assessment shall identify:

(a) affected Electronic Timestamps;

(b) affected Certificates;

(c) affected cryptographic dependencies;

(d) applicable transition measures.

PRESERVATION AND LONG-TERM RELIANCE

Article 15

1. Where long-term reliance is required, the Electronic Timestamp shall support preservation of evidence necessary for Historical Validation.

2. Preservation evidence may include:

(a) timestamp evidence;

(b) Certificate information;

(c) Status information;

(d) Validation evidence;

(e) cryptographic transition information.

3. Long-term preservation requirements shall be defined by the applicable Profile.

RECORDS AND EVIDENCE

Article 16

1. The responsible Actor shall maintain records sufficient to reconstruct:

(a) timestamp creation;

(b) referenced data binding;

(c) Timestamp Issuer;

(d) timestamp dependencies;

(e) lifecycle events;

(f) Validation history.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 17

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Electronic Timestamp Category;

(b) Qualified Electronic Timestamp Status;

(c) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 319 422	Timestamp token and protocol profile requirements
RFC 3161	Time-Stamp Protocol
RFC 5816	ESSCertIDv2 update for timestamp token certificate identification
RFC 5280	Certificate validation where timestamp certificates are used
ETSI EN 319 102-1	Validation process requirements applicable to timestamps
ISO/IEC 18014-4	Traceability of time sources where applicable
ISO 8601-1:2019	Date and time representation

IDEHA-IG-SVC-TSP-001: TRUST SERVICE PROVIDER AND TRUST SERVICE COMMON IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements applicable to Trust Service Providers and Trust Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers responsible for providing one or more Trust Services within the scope established by the applicable Framework Instruments.

3. This Guideline establishes common implementation requirements for:

(a) Trust Service Provider governance;

(b) Trust Service inventory and separation;

(c) Trust Service operational management;

(d) service documentation and evidence;

(e) service lifecycle management;

(f) common security and continuity arrangements;

(g) dependencies between Trust Services.

4. This Guideline applies together with the applicable Trust Service-specific Implementation Guideline.

5. This Guideline does not establish:

(a) Trust Service Categories;

(b) Trust Service Provider Status;

(c) Qualified Trust Service Provider Status;

(d) Qualified Trust Service Status;

(e) Service Permission;

(f) Qualification decisions;

(g) Humanitarian Trust List governance;

(h) service-specific technical requirements.

Those matters shall be implemented through the applicable Framework Instruments.

TRUST SERVICE PROVIDER OPERATIONAL IDENTITY

Article 2

1. A Trust Service Provider shall maintain operational information identifying its Trust Service Provider functions.

2. The operational information shall identify:

(a) Trust Service Provider Identifier;

(b) organisational information;

(c) applicable Provider Scope;

(d) responsible governance functions;

(e) provided Trust Services;

(f) applicable Service Permissions;

(g) lifecycle information.

3. The Trust Service Provider Identifier shall remain separate from:

(a) Trust Service Identifier;

(b) Certificate Identifier;

(c) Service Digital Identity;

(d) Trust Object Identifier.

TRUST SERVICE INVENTORY AND SEPARATION

Article 3

1. A Trust Service Provider shall maintain an inventory of Trust Services provided under the Trust Framework.

2. The Trust Service inventory shall identify:

(a) Trust Service Identifier;

(b) Trust Service Category;

(c) Service Scope;

(d) applicable Profiles;

(e) applicable Technical Specifications;

(f) applicable Standards;

(g) operational Status.

3. Each Trust Service shall remain separately identifiable.

4. A Trust Service Provider shall not:

(a) merge separate Trust Services into one service identity;

(b) use one Service Identifier for different Trust Services;

(c) assume that qualification of one Trust Service applies to another Trust Service.

Article 4

1. A Trust Service Provider providing multiple Trust Services shall maintain separation between:

(a) service governance;

(b) service operation;

(c) service evidence;

(d) service dependencies;

(e) service lifecycle.

2. The separation shall be sufficient to determine the scope of each Trust Service independently.

TRUST SERVICE DOCUMENTATION

Article 5

1. A Trust Service Provider shall maintain documentation necessary for operation and reliance upon each Trust Service.

2. The documentation shall identify, where applicable:

(a) Trust Service description;

(b) Service Scope;

(c) applicable Profiles;

(d) applicable Technical Specifications;

(e) applicable Standards;

(f) operational limitations;

(g) security conditions;

(h) evidence requirements.

3. Service documentation shall remain consistent with the applicable Framework Instruments.

Article 6

1. A Trust Service Provider shall maintain service practice information sufficient to demonstrate how each Trust Service is operated.

2. The practice information shall include, where applicable:

(a) responsibilities;

(b) operational procedures;

(c) security controls;

(d) incident handling arrangements;

(e) continuity arrangements;

(f) evidence retention requirements.

3. Service practice information shall not modify requirements established by the Main Framework or applicable Profiles.

TRUST SERVICE OPERATION

Article 7

1. A Trust Service Provider shall operate each Trust Service within its assigned Service Scope.

2. The Trust Service Provider shall ensure that each Trust Service:

(a) performs only permitted functions;

(b) applies applicable Profiles;

(c) applies applicable Technical Specifications;

(d) maintains required evidence;

(e) supports applicable Validation requirements.

3. A Trust Service Provider shall not perform functions outside the approved scope of a Trust Service.

Article 8

1. A Trust Service Provider shall maintain records of Trust Service operations.

2. Operational records shall identify, where applicable:

(a) service requests;

(b) service outputs;

(c) processing events;

(d) Status changes;

(e) security events;

(f) lifecycle events.

3. Operational records shall enable reconstruction of relevant service activities.

DEPENDENCIES AND SUPPORTING FUNCTIONS

Article 9

1. A Trust Service Provider shall identify dependencies required for operation of each Trust Service.

2. Dependencies may include:

(a) Sources;

(b) Trust Objects;

(c) Certificates;

(d) Validation Services;

(e) Electronic Timestamp Services;

(f) Cryptographic mechanisms;

(g) supporting Actors.

3. Dependency information shall identify:

(a) dependency purpose;

(b) applicable scope;

(c) required Status;

(d) applicable Validation conditions.

4. A dependency shall not transfer its Status or Qualified Status to the Trust Service.

SECURITY AND CONFIDENTIALITY

Article 10

1. A Trust Service Provider shall implement security measures appropriate to the Trust Services provided.

2. Security measures shall address, where applicable:

(a) confidentiality;

(b) integrity;

(c) availability;

(d) authenticity;

(e) accountability;

(f) access control;

(g) monitoring.

3. Security requirements specific to a Trust Service shall be established by the applicable Trust Service-specific Implementation Guideline.

PERSONNEL AND SUPPORTING ACTORS

Article 11

1. A Trust Service Provider shall define responsibilities for persons and supporting Actors involved in Trust Service operation.

2. Responsibilities shall identify:

(a) assigned functions;

(b) access permissions;

(c) competence requirements;

(d) segregation requirements;

(e) accountability arrangements.

3. Supporting Actors shall operate only within the scope assigned by the Trust Service Provider.

INCIDENT RESPONSE AND CONTINUITY

Article 12

1. A Trust Service Provider shall maintain arrangements for:

(a) incident detection;

(b) incident response;

(c) service continuity;

(d) Recovery;

(e) evidence preservation.

2. Incident and continuity arrangements shall identify:

(a) responsible functions;

(b) notification conditions;

(c) affected Trust Services;

(d) Recovery conditions.

3. Service-specific incident requirements shall be established by the applicable Implementation Guideline.

TRUST SERVICE LIFECYCLE MANAGEMENT

Article 13

1. A Trust Service Provider shall manage the lifecycle of each Trust Service.

2. The lifecycle shall include, where applicable:

(a) preparation;

(b) activation;

(c) operation;

(d) modification;

(e) restriction;

(f) Suspension;

(g) withdrawal;

(h) cessation.

3. Lifecycle changes shall be recorded.

Article 14

1. Before implementing a material change affecting a Trust Service, the Trust Service Provider shall assess:

(a) affected Service Scope;

(b) affected Profiles;

(c) affected Technical Specifications;

(d) affected Standards;

(e) affected dependencies;

(f) impact on reliance.

2. Material changes shall be managed according to the applicable Change Control requirements.

QUALIFICATION SUPPORT

Article 15

1. Where a Trust Service Provider seeks Qualified Status for a Trust Service, it shall prepare evidence according to the applicable Qualified Profile.

2. Evidence shall identify:

(a) Trust Service scope;

(b) applicable requirements;

(c) conformity evidence;

(d) assessment results;

(e) limitations.

3. Preparation of qualification evidence shall not create Qualified Status.

4. Qualified Status shall arise only through the applicable Framework decision route.

RECORDS AND EVIDENCE

Article 16

1. A Trust Service Provider shall maintain records sufficient to reconstruct:

(a) Trust Service establishment;

(b) service operation;

(c) service dependencies;

(d) service changes;

(e) security events;

(f) qualification evidence where applicable.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 17

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Trust Service Category;

(b) Trust Service Status;

(c) Qualified Trust Service Status;

(d) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 319 401	General policy requirements for Trust Service Providers
ISO/IEC 27001:2022	Information security management controls applicable to Trust Service operation
ISO/IEC 27002:2022	Security control implementation guidance
ISO/IEC 27701:2025	Privacy information management where personal data processing is performed
ISO 22301:2019	Business continuity management where continuity requirements apply
ISO/IEC 20000-1:2018	Service management controls where service-management processes are applied

IDEHA-IG-SVC-IDN-001: IDENTIFICATION SERVICE IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Identification Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Identification Services and Actors performing Identification Service functions within the applicable Service Scope.

3. This Guideline establishes requirements for:

(a) Identity Proofing;

(b) Identity Registration;

(c) maintenance of Identity Registration Records;

(d) Identifier allocation and management;

(e) Identity Resolution;

(f) identity lifecycle management;

(g) Identification Results.

4. This Guideline applies together with:

(a) IDEHA-IG-SRC-ASO-001 Source and Authoritative Source Implementation;

(b) IDEHA-IG-DAT-SEM-001 Controlled Data Elements, Semantics and Data Quality Implementation;

(c) IDEHA-IG-BIO-GEN-001 Biometric Implementation Controls;

(d) IDEHA-IG-SVC-AUT-001 Authentication Service Implementation;

(e) IDEHA-IG-SVC-EAS-001 Electronic Attestation Service Implementation;

(f) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) civil registration authority;

(b) legal identity creation;

(c) Source authority;

(d) Electronic Attestation issuance;

(e) Authentication Service operation;

(f) Authorisation decisions;

(g) biometric technical formats;

(h) technical data exchange protocols.

Those matters shall be implemented through the applicable Framework Instruments.

IDENTIFICATION SERVICE SCOPE

Article 2

1. An Identification Service shall operate within an identified Service Scope.

2. The Service Scope shall identify:

(a) Subject categories;

(b) permitted Identification Service Functions;

(c) applicable Sources;

(d) applicable Profiles;

(e) applicable Assurance Conditions;

(f) applicable Security Conditions;

(g) applicable jurisdictions or operational domains.

3. An Identification Service shall not perform functions outside its approved Service Scope.

Article 3

1. The Identification Service shall distinguish between:

(a) identity evidence;

(b) identity information;

(c) Identity Registration Records;

(d) Identification Results;

(e) Identity Resolution Results.

2. The Identification Service shall maintain separation between:

(a) the registered identity representation;

(b) the evidence used to establish that representation;

(c) the Source providing the evidence;

(d) outputs produced by the Identification Service.

IDENTITY PROOFING

Article 4

1. Identity Proofing shall establish confidence that identity information relates to the identified Subject.

2. Identity Proofing shall evaluate:

(a) identity evidence;

(b) Source information;

(c) biographic information;

(d) biometric information where applicable;

(e) demographic information where applicable;

(f) other permitted evidence.

3. The applicable Profile shall define:

(a) accepted evidence types;

(b) evidence quality requirements;

(c) verification methods;

(d) assurance conditions;

(e) failure and exception handling.

Article 5

1. The Identification Service shall record evidence supporting an Identity Proofing result.

2. The evidence record shall identify, where applicable:

(a) evidence type;

(b) evidence Source;

(c) collection method;

(d) verification method;

(e) processing time;

(f) responsible Actor;

(g) outcome.

3. Evidence used for Identity Proofing shall remain attributable to its Source and shall not become a new Source solely through use by the Identification Service.

IDENTITY REGISTRATION

Article 6

1. Identity Registration shall establish and maintain an Identity Registration Record for a registered Subject.

2. An Identity Registration Record shall contain or reference, where applicable:

(a) biographic data;

(b) biometric data;

(c) demographic data;

(d) allocated Identification Number;

(e) family relationship information;

(f) contact details;

(g) identification document details;

(h) registration evidence;

(i) lifecycle information.

3. The applicable Profile shall define the permitted data elements, retention conditions and reuse conditions.

Article 7

1. The Identification Service shall ensure that Identity Registration Records maintain:

(a) provenance;

(b) Data Quality information;

(c) Source references;

(d) correction history;

(e) lifecycle information.

2. Information contained in an Identity Registration Record shall remain distinguishable according to its origin and purpose.

3. Derived information shall identify:

(a) source information;

(b) derivation method;

(c) responsible processing function;

(d) applicable Version.

IDENTIFICATION NUMBER

Article 8

1. An Identification Service assigning an Identification Number shall maintain an Identifier namespace.

2. An Identification Number shall:

(a) uniquely identify the Subject within the applicable namespace;

(b) remain stable during the applicable lifecycle;

(c) remain separate from identity Attributes;

(d) remain separate from Trust Object Identifiers.

3. An Identification Number shall not:

(a) disclose identity type;

(b) disclose demographic information;

(c) disclose jurisdictional meaning unless required by the identifier scheme;

(d) encode Status or qualification information.

4. The applicable Profile shall define:

(a) generation method;

(b) uniqueness scope;

(c) non-reuse conditions;

(d) lifecycle treatment.

IDENTITY RESOLUTION

Article 9

1. Identity Resolution shall determine whether identity information refers to:

(a) an existing Identity Registration Record;

(b) a different Identity Registration Record;

(c) an unresolved identity state.

2. Identity Resolution shall consider:

(a) available identity information;

(b) applicable matching rules;

(c) permitted biometric comparison where applicable;

(d) confidence thresholds;

(e) human review requirements.

3. Identity Resolution shall not create a legal identity or alter Source records.

Article 10

1. Where automated matching is used, the Identification Service shall maintain evidence of:

(a) matching method;

(b) algorithm Version;

(c) thresholds;

(d) input data;

(e) result;

(f) limitations.

2. The applicable Profile shall define requirements for:

(a) false match risk;

(b) false non-match risk;

(c) demographic performance;

(d) human review.

BIOGRAPHIC, BIOMETRIC AND DEMOGRAPHIC DATA

Article 11

1. The Identification Service shall process biographic, biometric and demographic data according to the applicable Profile.

2. The applicable Profile shall identify:

(a) permitted data elements;

(b) collection conditions;

(c) Source requirements;

(d) quality requirements;

(e) retention conditions;

(f) reuse conditions.

3. Biometric data shall be processed according to the applicable Biometric Implementation requirements.

4. Demographic data shall remain separate from:

(a) Identification Number;

(b) Subject Identifier;

(c) Trust Object Identifier.

IDENTITY REGISTRATION RECORD LIFECYCLE

Article 12

1. The Identification Service shall manage the lifecycle of Identity Registration Records.

2. Lifecycle management shall include, where applicable:

(a) creation;

(b) update;

(c) correction;

(d) suspension;

(e) recovery;

(f) closure;

(g) historical preservation.

3. Lifecycle events shall identify:

(a) responsible Actor;

(b) effective time;

(c) reason;

(d) supporting evidence.

Article 13

1. Corrections to Identity Registration Records shall preserve sufficient evidence to reconstruct:

(a) previous information;

(b) correction basis;

(c) responsible Actor;

(d) effective time.

2. A correction shall not remove historical information required for accountability or Historical State determination.

IDENTIFICATION RESULTS

Article 14

1. An Identification Service shall produce an Identification Result where an Identification Service Function produces an outcome intended for use by another Actor.

2. An Identification Result shall identify, where applicable:

(a) Subject reference;

(b) Identification Service;

(c) evaluated evidence basis;

(d) Assurance Conditions;

(e) evaluation time;

(f) limitations.

3. An Identification Result shall not:

(a) create legal identity;

(b) create Source authority;

(c) create Authorisation;

(d) create entitlement.

Article 15

1. An Identity Resolution Result shall identify, where applicable:

(a) evaluated records;

(b) resolution method;

(c) confidence information;

(d) limitations;

(e) evaluation time.

2. An Identity Resolution Result shall remain separate from an Identification Result.

REUSE AND DISCLOSURE

Article 16

1. Identity Registration Record information shall be reused only within the conditions established by the applicable Profile.

2. Reuse conditions shall consider:

(a) purpose;

(b) Service Scope;

(c) Source Basis;

(d) Freshness Condition;

(e) Assurance Conditions;

(f) disclosure restrictions.

3. The Identification Service shall not disclose Identity Registration Record information beyond the authorised scope.

SECURITY AND SAFEGUARDS

Article 17

1. The Identification Service shall protect Identity Registration Records and related evidence against:

(a) unauthorised access;

(b) unauthorised modification;

(c) unauthorised disclosure;

(d) loss of integrity.

2. Access shall be controlled through:

(a) Authentication;

(b) Authorisation;

(c) purpose restrictions;

(d) audit requirements.

3. Protected-Person Safeguards and Accessible Alternatives shall apply where required.

RECORDS AND EVIDENCE

Article 18

1. The Identification Service shall maintain records sufficient to reconstruct:

(a) Identity Proofing;

(b) Identity Registration;

(c) Identity Resolution;

(d) Identifier allocation;

(e) corrections;

(f) lifecycle changes;

(g) Identification Results.

2. Records shall identify:

(a) responsible Actor;

(b) Source Basis;

(c) processing method;

(d) applicable Profile Version.

APPLICABLE STANDARDS

Article 19

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) identity;

(b) Source authority;

(c) Identification Service Status;

(d) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ISO/IEC 24760-1:2025	Identity concepts, identity information and Identifier principles

Reference	Application
ISO/IEC 24760-2:2025	Identity-management architecture considerations
ISO/IEC 24760-3:2025	Identity-management operational processes
ETSI TS 119 461 V2.1.1	Identity proofing requirements where used for trust-service-related identity verification
ISO/IEC TS 29003:2018	Identity-proofing guidance
NIST SP 800-63A-4	Identity proofing and enrolment controls
ISO/IEC 11179-31:2023	Data-element concepts and semantic descriptions
ISO/IEC 25012:2008	Data quality model
ISO/IEC 25024:2015	Data quality measurement
ISO 15489-1:2016	Records management principles
ISO 23081-1:2017	Records metadata principles
ISO/IEC 24745:2022	Biometric information protection where biometric data is processed

IDEHA-IG-SVC-AUT-001: AUTHENTICATION SERVICE IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Authentication Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Authentication Services and Actors performing Authentication functions within the applicable Service Scope.

3. This Guideline establishes requirements for:

(a) Subject Authentication;

(b) System Authentication;

(c) Authentication Mechanisms;

(d) Authenticators;

(e) Authentication Events;

(f) Authentication Outcomes;

(g) session and reauthentication management.

4. This Guideline applies together with:

(a) IDEHA-IG-SVC-IDN-001 Identification Service Implementation;

(b) IDEHA-IG-SVC-AUZ-001 Authorisation Service Implementation;

(c) IDEHA-IG-OBJ-DSG-001 Digital Signature Creation Data and Device Implementation where cryptographic Authenticators are used;

(d) IDEHA-IG-SEC-CRY-001 Cryptographic Controls and Cryptographic Agility Implementation;

(e) IDEHA-IG-BIO-GEN-001 Biometric Implementation Controls where biometric Authenticators are used;

(f) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) identity;

(b) Identity Proofing;

(c) Identity Registration;

(d) Authorisation;

(e) Electronic Signature;

(f) Electronic Seal;

(g) Trust Object issuance;

(h) access policy decisions;

(i) cryptographic algorithm selection.

Those matters shall be implemented through the applicable Framework Instruments.

AUTHENTICATION SERVICE SCOPE

Article 2

1. An Authentication Service shall operate within an identified Service Scope.

2. The Service Scope shall identify:

(a) authenticated Subject or entity categories;

(b) permitted Authentication Mechanisms;

(c) supported Authenticators;

(d) applicable Assurance Conditions;

(e) applicable Security Conditions;

(f) applicable Profiles;

(g) applicable Technical Specifications.

3. An Authentication Service shall not perform functions outside its approved Service Scope.

Article 3

1. An Authentication Service shall distinguish between:

(a) Authentication;

(b) Authentication Mechanism;

(c) Authenticator;

(d) Authentication Event;

(e) Authentication Outcome.

2. The Authentication Service shall maintain separation between:

(a) identity information used for Authentication;

(b) Authentication evidence;

(c) Authentication decision;

(d) Authorisation decision.

3. A successful Authentication Event shall not by itself create Authorisation.

AUTHENTICATION MECHANISMS

Article 4

1. An Authentication Service shall use Authentication Mechanisms appropriate to the applicable Assurance Conditions.

2. An Authentication Mechanism shall define:

(a) authenticated entity;

(b) authentication method;

(c) required inputs;

(d) required evidence;

(e) security conditions;

(f) failure conditions.

3. The applicable Authentication Profile shall specify:

(a) permitted mechanisms;

(b) assurance level;

(c) factor requirements;

(d) replay resistance requirements;

(e) phishing resistance requirements where applicable.

Article 5

1. Authentication Mechanisms may include:

(a) knowledge factors;

(b) possession factors;

(c) inherence factors;

(d) cryptographic Authenticators;

(e) device-based Authenticators;

(f) service or system authentication mechanisms.

2. The applicable Profile shall determine the permitted combination of factors.

3. A biometric characteristic shall not by itself constitute an Authenticator unless explicitly permitted by the applicable Profile.

AUTHENTICATORS

Article 6

1. An Authenticator shall be uniquely associated with the authenticated Subject or entity within the applicable scope.

2. Authenticator information shall identify:

(a) Authenticator Identifier;

(b) associated Subject or entity reference;

(c) Authenticator type;

(d) activation conditions;

(e) lifecycle Status;

(f) effective period.

3. An Authenticator Identifier shall:

(a) remain opaque;

(b) not disclose identity type;

(c) not disclose personal information;

(d) remain separate from Subject Identifier and Trust Object Identifier.

Article 7

1. The Authentication Service shall manage the Authenticator lifecycle.

2. Lifecycle management shall include:

(a) issuance;

(b) binding;

(c) activation;

(d) use;

(e) suspension;

(f) replacement;

(g) revocation;

(h) recovery;

(i) termination.

3. Lifecycle events affecting Authentication assurance shall be recorded.

SUBJECT AUTHENTICATION

Article 8

1. Subject Authentication shall determine whether the identified Subject successfully demonstrates control of an approved Authenticator.

2. Subject Authentication shall evaluate:

(a) Authentication request;

(b) Authenticator status;

(c) Authentication mechanism;

(d) required factors;

(e) security conditions.

3. Subject Authentication shall not establish:

(a) identity;

(b) legal capacity;

(c) entitlement;

(d) Authorisation.

Article 9

1. Where Subject Authentication uses a cryptographic Authenticator, the Authentication Service shall verify:

(a) possession or control of the cryptographic material;

(b) integrity of the Authentication response;

(c) freshness of the Authentication Event;

(d) applicable certificate or key status where relevant.

2. Cryptographic key lifecycle requirements shall be established through the applicable Cryptographic Controls requirements.

SYSTEM AUTHENTICATION

Article 10

1. System Authentication shall determine whether a system, service, device or Endpoint is authenticated within the applicable scope.

2. System Authentication may apply to:

(a) information systems;

(b) services;

(c) applications;

(d) devices;

(e) workloads;

(f) gateways;

(g) Endpoints.

3. System Authentication shall identify:

(a) authenticated system or entity;

(b) authentication mechanism;

(c) credential or certificate reference;

(d) Authentication Event;

(e) applicable Security Conditions.

Article 11

1. A system Authentication Credential shall remain separate from:

(a) Subject Authentication credentials;

(b) Authorisation credentials;

(c) Trust Service Identifier;

(d) Trust Object Identifier.

2. A system successfully authenticated shall not automatically receive permission to access a resource.

3. Authorisation shall be determined through the applicable Authorisation Service.

BIOMETRIC AUTHENTICATION

Article 12

1. Where biometric information contributes to Authentication, the Authentication Service shall apply the applicable Biometric Implementation requirements.

2. Biometric Authentication shall consider:

(a) biometric sample quality;

(b) biometric reference protection;

(c) presentation attack detection;

(d) applicable performance requirements;

(e) accessibility conditions.

3. A biometric comparison result shall not independently establish identity or Authorisation.

AUTHENTICATION EVENTS

Article 13

1. Each Authentication Event shall be uniquely identifiable within the applicable scope.

2. An Authentication Event record shall identify:

(a) Authentication Event Identifier;

(b) authenticated Subject or entity;

(c) Authentication Mechanism;

(d) Authenticator used;

(e) Authentication time;

(f) result;

(g) Assurance Conditions achieved;

(h) limitations.

3. Authentication Event information shall be protected according to applicable Security Conditions.

Article 14

1. An Authentication Event shall remain associated with the conditions under which it occurred.

2. The Authentication Service shall record:

(a) successful Authentication;

(b) failed Authentication;

(c) rejected Authentication;

(d) restricted Authentication;

(e) step-up Authentication where applicable.

3. Authentication evidence shall be retained according to the applicable Profile.

AUTHENTICATION OUTCOMES

Article 15

1. An Authentication Service shall produce an Authentication Outcome following an Authentication Event.

2. An Authentication Outcome shall identify:

(a) authenticated Subject or entity;

(b) Authentication Service;

(c) Authentication Mechanism;

(d) achieved Assurance Conditions;

(e) Authentication time;

(f) validity period;

(g) limitations.

3. An Authentication Outcome shall remain separate from:

(a) Authorisation Outcome;

(b) Electronic Attestation;

(c) Electronic Signature.

Article 16

1. An Authentication Outcome shall support Verification and Validation.

2. Validation shall determine, where applicable:

(a) Authentication Service Status;

(b) Authenticator Status;

(c) Authentication Mechanism;

(d) Assurance Conditions;

(e) validity period;

(f) Historical State.

3. An Authentication Outcome shall not establish Authorisation.

SESSION AND REAUTHENTICATION MANAGEMENT

Article 17

1. Where an Authentication Service establishes a session, the session shall be associated with the applicable Authentication Outcome.

2. Session management shall define:

(a) session identifier;

(b) session validity period;

(c) inactivity conditions;

(d) reauthentication conditions;

(e) termination conditions.

3. A session shall not provide a higher assurance level than the Authentication Event that established it.

Article 18

1. Reauthentication shall be required where:

(a) the applicable Profile requires it;

(b) the session exceeds its permitted period;

(c) risk conditions change;

(d) the requested operation requires additional assurance.

2. Step-up Authentication shall establish a new Authentication Outcome or update the existing outcome according to the applicable Profile.

FAILURE, RECOVERY AND REPLACEMENT

Article 19

1. The Authentication Service shall maintain procedures for:

(a) failed Authentication;

(b) Authenticator recovery;

(c) Authenticator replacement;

(d) compromised Authenticator handling.

2. Recovery and replacement processes shall provide assurance equivalent to the intended Authentication use unless the applicable Profile establishes another condition.

SECURITY AND SAFEGUARDS

Article 20

1. The Authentication Service shall protect Authentication information against:

(a) unauthorised access;

(b) credential compromise;

(c) replay;

(d) impersonation;

(e) unauthorised disclosure.

2. Security controls shall include, where applicable:

(a) monitoring;

(b) anomaly detection;

(c) rate limitation;

(d) audit records;

(e) incident response.

RECORDS AND EVIDENCE

Article 21

1. The Authentication Service shall maintain records sufficient to reconstruct:

(a) Authentication Events;

(b) Authentication Outcomes;

(c) Authenticator lifecycle;

(d) failed Authentication attempts;

(e) recovery actions;

(f) security events.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 22

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) identity;

(b) Authorisation;

(c) Trust Object Status;

(d) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
NIST SP 800-63B-4	Authentication and Authenticator management requirements
ISO/IEC 29115:2013	Entity Authentication Assurance framework
ISO/IEC 9798-1:2010	Entity Authentication framework
ISO/IEC 9798-2:2019	Symmetric cryptographic Authentication mechanisms
ISO/IEC 9798-3:2019	Public-key cryptographic Authentication mechanisms
RFC 5280	Certificate validation where certificate-based Authentication is used
RFC 9525	Service identity verification in TLS
RFC 8446	TLS 1.3 protected communication
ISO/IEC 24745:2022	Biometric information protection
ISO/IEC 30107-1:2023	Presentation attack detection framework
ISO/IEC 30107-3:2023	Presentation attack detection testing
ISO/IEC 19795-1:2021	Biometric performance testing

IDEHA-IG-SVC-AUZ-001: AUTHORISATION SERVICE IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Authorisation Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Authorisation Services and Actors performing Authorisation functions within the applicable Service Scope.

3. This Guideline establishes requirements for:

(a) Authorisation Policy management;

(b) Authorisation request processing;

(c) policy evaluation;

(d) Authorisation decision generation;

(e) Authorisation Outcome management;

(f) enforcement coordination;

(g) lifecycle management of Authorisation decisions.

4. This Guideline applies together with:

(a) IDEHA-IG-SVC-AUT-001 Authentication Service Implementation;

(b) IDEHA-IG-ACT-PAR-001 Participation, Roles, Mandates and Representation Implementation;

(c) IDEHA-IG-SRC-ASO-001 Source and Authoritative Source Implementation;

(d) IDEHA-IG-SVC-FDX-001 Federated Data Exchange Service Implementation where Authorisation applies to data exchange;

(e) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) identity;

(b) Authentication;

(c) Identity Proofing;

(d) Identity Registration;

(e) Source authority;

(f) legal rights or entitlements;

(g) data-sharing agreements;

(h) cryptographic mechanisms;

(i) access-token formats;

(j) protocol bindings.

Those matters shall be implemented through the applicable Framework Instruments.

AUTHORISATION SERVICE SCOPE

Article 2

1. An Authorisation Service shall operate within an identified Service Scope.

2. The Service Scope shall identify:

(a) permitted Authorisation functions;

(b) Actor categories;

(c) Controlled Matters subject to evaluation;

(d) applicable Policies;

(e) applicable Profiles;

(f) applicable Assurance Conditions;

(g) applicable Security Conditions.

3. An Authorisation Service shall not perform functions outside its approved Service Scope.

Article 3

1. An Authorisation Service shall distinguish between:

(a) Authentication Outcome;

(b) Authorisation Request;

(c) Authorisation Policy;

(d) Authorisation Decision;

(e) Authorisation Outcome;

(f) Policy Enforcement.

2. A successful Authentication Event shall not by itself establish Authorisation.

3. An Authorisation Outcome shall not establish identity, Source authority, legal capacity or entitlement unless such matters are determined by another applicable Framework Instrument.

AUTHORISATION ARCHITECTURE

Article 4

1. An Authorisation Service shall maintain functions necessary for policy-based evaluation.

2. The functions may include:

(a) Policy Administration Function;

(b) Policy Decision Function;

(c) Policy Information Function;

(d) Policy Enforcement Function.

3. The applicable Profile shall define the functions required for each implementation context.

Article 5

1. The Policy Administration Function shall manage Authorisation Policies.

2. Policy administration shall include:

(a) creation;

(b) approval;

(c) publication;

(d) modification;

(e) suspension;

(f) withdrawal;

(g) version management.

3. Policy administration shall remain separate from Policy evaluation.

AUTHORISATION POLICIES

Article 6

1. An Authorisation Policy shall define conditions under which an Action may be permitted, denied or restricted.

2. An Authorisation Policy shall identify, where applicable:

(a) Policy Identifier;

(b) Policy Version;

(c) Policy Owner;

(d) applicable Actors;

(e) Controlled Matters;

(f) permitted Actions;

(g) purposes;

(h) required Attributes;

(i) obligations;

(j) restrictions;

(k) validity period.

3. An Authorisation Policy shall operate only within the scope assigned by the responsible Actor.

Article 7

1. An Authorisation Policy shall not:

(a) create a Subject identity;

(b) create a Role;

(c) create a Mandate;

(d) create a Source authority;

(e) create a legal entitlement.

2. Where a Policy requires Roles, Mandates, Attributes or Source information, those inputs shall be obtained from applicable authoritative functions.

AUTHORISATION REQUEST

Article 8

1. An Authorisation Request shall identify the requested Action and the Controlled Matter to which the Action applies.

2. An Authorisation Request shall contain, where applicable:

(a) requesting Actor;

(b) represented Subject where applicable;

(c) recipient;

(d) Controlled Matter;

(e) requested Action;

(f) Purpose;

(g) Authentication Outcome reference;

(h) Role or Mandate reference;

(i) applicable consent reference where applicable;

(j) contextual information.

3. The applicable Technical Specification shall define the technical representation of Authorisation Requests.

Article 9

1. Before evaluation, the Authorisation Service shall verify that the Authorisation Request is complete and within the Service Scope.

2. The verification shall determine:

(a) presence of required information;

(b) validity of references;

(c) applicability of the requested Action;

(d) applicability of the requested Controlled Matter.

POLICY EVALUATION

Article 10

1. The Policy Decision Function shall evaluate the Authorisation Request against the applicable Authorisation Policy.

2. The evaluation shall consider, where applicable:

(a) Actor Attributes;

(b) Subject Attributes;

(c) Role information;

(d) Mandate information;

(e) Source information;

(f) Authentication Assurance;

(g) Purpose;

(h) environmental conditions;

(i) security conditions.

3. The evaluation result shall be recorded as an Authorisation Decision.

Article 11

1. Where required information is unavailable, invalid or insufficient, the Authorisation Decision shall not result in an unauthorised Permit.

2. The Authorisation Service shall identify, where applicable:

(a) missing information;

(b) unavailable Sources;

(c) expired conditions;

(d) unresolved conflicts;

(e) policy limitations.

3. An inability to determine Authorisation shall remain distinguishable from a Deny decision.

ROLES, MANDATES AND DELEGATED AUTHORITY

Article 12

1. An Authorisation Service may evaluate Roles, Mandates and representation information as decision inputs.

2. The evaluation shall determine:

(a) existence of the Role or Mandate;

(b) applicable scope;

(c) validity period;

(d) restrictions;

(e) relationship to the requested Action.

3. A Role or Mandate used in an Authorisation decision shall not be expanded beyond its assigned scope.

Article 13

1. A delegated authority shall be evaluated against:

(a) delegating Actor;

(b) delegated Actor;

(c) delegated scope;

(d) permitted Actions;

(e) validity period;

(f) revocation conditions.

2. Delegation shall not permit an Actor to grant authority exceeding the authority available to that Actor.

CONSENT AND PURPOSE CONDITIONS

Article 14

1. Where consent is applicable, the Authorisation Service may evaluate consent information as an Authorisation input.

2. Consent information shall identify, where applicable:

(a) consenting Subject;

(b) receiving Actor;

(c) permitted data or Controlled Matter;

(d) purpose;

(e) validity period;

(f) withdrawal status;

(g) limitations.

3. Consent shall remain separate from:

(a) Authentication;

(b) Authorisation Policy;

(c) Authorisation Outcome.

4. The existence of consent shall not replace other required Authorisation conditions.

AUTHORISATION OUTCOME

Article 15

1. An Authorisation Service shall produce an Authorisation Outcome following evaluation.

2. An Authorisation Outcome shall identify:

(a) Authorisation Outcome Identifier;

(b) requesting Actor;

(c) represented Subject where applicable;

(d) Controlled Matter;

(e) Action;

(f) Purpose;

(g) decision;

(h) Policy Identifier and Version;

(i) evaluation time;

(j) validity period;

(k) obligations;

(l) restrictions;

(m) limitations.

3. An Authorisation Outcome shall remain separate from:

(a) Authentication Outcome;

(b) Electronic Attestation;

(c) Electronic Signature;

(d) Authorisation Policy.

Article 16

1. An Authorisation Outcome may contain obligations requiring enforcement by another Actor or function.

2. Obligations may include:

(a) restricted disclosure;

(b) additional verification;

(c) logging;

(d) human approval;

(e) purpose limitation;

(f) retention restrictions.

3. The Policy Enforcement Function shall verify that mandatory obligations can be satisfied before permitting the requested Action.

POLICY ENFORCEMENT

Article 17

1. Policy Enforcement shall apply the Authorisation Outcome to the requested operation.

2. The Policy Enforcement Function shall verify:

(a) Outcome integrity;

(b) Outcome validity;

(c) applicable scope;

(d) obligations;

(e) restrictions.

3. Policy Enforcement shall not modify the substantive Authorisation decision.

CONTINUOUS AUTHORISATION AND RE-EVALUATION

Article 18

1. An Authorisation Outcome shall remain valid only for the conditions and period established by the applicable Policy.

2. Re-evaluation shall occur where:

(a) the validity period expires;

(b) the Authentication Outcome changes;

(c) Role or Mandate information changes;

(d) Source Status changes;

(e) requested Action changes;

(f) Purpose changes;

(g) risk conditions materially change.

3. A cached Authorisation Outcome shall not be used beyond its permitted scope.

LIFECYCLE MANAGEMENT

Article 19

1. The lifecycle of an Authorisation Outcome shall include, where applicable:

(a) creation;

(b) activation;

(c) use;

(d) expiry;

(e) revocation;

(f) replacement;

(g) historical retention.

2. Lifecycle events shall identify:

(a) responsible Actor;

(b) effective time;

(c) reason;

(d) supporting evidence.

SECURITY AND RECORDS

Article 20

1. The Authorisation Service shall protect:

(a) Authorisation Policies;

(b) Authorisation Requests;

(c) Authorisation Decisions;

(d) Authorisation Outcomes;

(e) evaluation evidence.

2. Protection shall include:

(a) confidentiality;

(b) integrity;

(c) access control;

(d) accountability;

(e) auditability.

Article 21

1. The Authorisation Service shall maintain records sufficient to reconstruct:

(a) evaluated Request;

(b) applicable Policy;

(c) decision inputs;

(d) Authorisation Decision;

(e) Authorisation Outcome;

(f) enforcement result.

2. Records shall enable historical determination of the Authorisation conditions applicable at the relevant time.

APPLICABLE STANDARDS

Article 22

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) identity;

(b) Authentication;

(c) Authorisation;

(d) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ISO/IEC 29146:2024	Access-management architecture and distributed authorisation functions
ISO/IEC 10181-3:1996	Access-control framework concepts
NIST SP 800-162	Attribute Based Access Control implementation guidance
OASIS XACML 3.0	Policy language and decision model
XACML JSON Profile 1.1	JSON representation of policy requests and responses
XACML REST Profile 1.1	REST-based policy decision interface
XACML RBAC Profile 1.0	Role-based policy evaluation where applicable
XACML Administration and Delegation Profile 1.0	Policy administration and delegation where applicable
ISO/IEC TS 27560:2023	Consent records where consent is used as an Authorisation input
ISO/IEC 27701:2025	Privacy management controls where personal data access decisions are performed
ISO/IEC 27001:2022	Security management controls applicable to Authorisation Services

IDEHA-IG-SVC-DSG-001: DIGITAL SIGNING SERVICE IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Digital Signing Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Digital Signing Services and Actors operating Digital Signing Service functions within the applicable Service Scope.

3. This Guideline establishes requirements for:

(a) Digital Signing Service operation;

(b) signing request processing;

(c) Digital Signature creation orchestration;

(d) interaction with Digital Signature Creation Mechanisms and Devices;

(e) signing evidence management;

(f) service lifecycle management.

4. This Guideline applies together with:

(a) IDEHA-IG-OBJ-DSG-001 Digital Signature Creation Data and Device Implementation;

(b) IDEHA-IG-OBJ-SIG-001 Electronic Signature Implementation;

(c) IDEHA-IG-OBJ-SEL-001 Electronic Seal Implementation where applicable;

(d) IDEHA-IG-SVC-AUT-001 Authentication Service Implementation;

(e) IDEHA-IG-SVC-AUZ-001 Authorisation Service Implementation;

(f) IDEHA-IG-SVC-VVS-001 Validation and Verification Service Implementation;

(g) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) Digital Signature Creation Data requirements;

(b) Digital Signature Creation Device requirements;

(c) Qualified Digital Signature Creation Device requirements;

(d) Electronic Signature requirements;

(e) Electronic Seal requirements;

(f) Signatory identification requirements;

(g) signing intent requirements;

(h) signature format requirements;

(i) cryptographic algorithm selection.

Those matters shall be implemented through the applicable Framework Instruments.

DIGITAL SIGNING SERVICE SCOPE

Article 2

1. A Digital Signing Service shall operate within an identified Service Scope.

2. The Service Scope shall identify:

(a) permitted signing functions;

(b) supported Digital Signature Creation Mechanisms;

(c) supported Digital Signature Creation Devices;

(d) supported Signature Profiles;

(e) applicable Assurance Conditions;

(f) applicable Security Conditions;

(g) applicable Technical Specifications.

3. A Digital Signing Service shall not perform signing operations outside its approved Service Scope.

Article 3

1. A Digital Signing Service shall maintain separation between:

(a) signing request processing;

(b) Digital Signature creation;

(c) Electronic Signature creation;

(d) Electronic Seal creation;

(e) Validation activities.

2. A Digital Signing Service shall create Digital Signatures only.

3. The resulting Digital Signature shall become part of an Electronic Signature or Electronic Seal only through the applicable Framework Instrument.

SIGNING REQUEST PROCESSING

Article 4

1. A Digital Signing Service shall process signing requests according to the applicable Signing Profile.

2. A signing request shall identify, where applicable:

(a) requesting Actor;

(b) requested signing operation;

(c) data to be signed;

(d) Digital Signature Creation Mechanism;

(e) Digital Signature Creation Device;

(f) applicable Profile;

(g) required evidence.

3. The Digital Signing Service shall verify that the requested operation is within its Service Scope.

Article 5

1. Before creating a Digital Signature, the Digital Signing Service shall determine that:

(a) the request is valid;

(b) the required Digital Signature Creation Device is available;

(c) the Digital Signature Creation Data may be used;

(d) applicable Authentication conditions are satisfied;

(e) applicable Authorisation conditions are satisfied.

2. The Digital Signing Service shall not determine:

(a) legal effect of the signed data;

(b) existence of signing intent;

(c) validity of the resulting Electronic Signature.

Those matters belong to the applicable Electronic Signature Profile.

INTERACTION WITH DIGITAL SIGNATURE CREATION DEVICES

Article 6

1. A Digital Signing Service shall use Digital Signature Creation Mechanisms and Digital Signature Creation Devices according to the applicable Profile.

2. The Digital Signing Service shall maintain evidence of:

(a) selected Digital Signature Creation Device;

(b) selected Digital Signature Creation Mechanism;

(c) signing operation;

(d) creation result;

(e) applicable configuration.

3. The Digital Signing Service shall not alter the security boundary or evaluated configuration of a Digital Signature Creation Device.

Article 7

1. Where a Digital Signing Service operates with a remote Digital Signature Creation Device, it shall ensure that:

(a) the correct signing operation is selected;

(b) the intended data representation is provided;

(c) communication with the device is protected;

(d) creation evidence is generated.

2. Remote operation shall comply with the applicable remote signing Profile.

3. The Digital Signing Service shall not replace the requirements applicable to the Digital Signature Creation Device.

AUTHENTICATION AND AUTHORISATION DEPENDENCIES

Article 8

1. Where required by the applicable Profile, a Digital Signing Service shall require an Authentication Outcome before initiating a signing operation.

2. The Authentication Outcome shall identify, where applicable:

(a) authenticated Subject;

(b) Authentication Service;

(c) Authentication Assurance;

(d) validity period;

(e) limitations.

3. Authentication shall remain separate from the Digital Signature creation process.

Article 9

1. Where required by the applicable Profile, a Digital Signing Service shall require an Authorisation Outcome before initiating a signing operation.

2. The Authorisation Outcome shall identify, where applicable:

(a) permitted signing operation;

(b) Actor;

(c) Subject;

(d) scope;

(e) validity period;

(f) restrictions.

3. Authorisation shall remain separate from Digital Signature creation.

DIGITAL SIGNATURE CREATION OPERATION

Article 10

1. A Digital Signing Service shall create a Digital Signature using the approved Digital Signature Creation Mechanism.

2. The creation operation shall identify:

(a) data representation provided for signing;

(b) Digital Signature Creation Data reference;

(c) Digital Signature Creation Device reference;

(d) creation time;

(e) resulting Digital Signature.

3. The Digital Signing Service shall preserve the relationship between the signing request and the resulting Digital Signature.

Article 11

1. A Digital Signing Service shall produce creation evidence sufficient to reconstruct the Digital Signature creation operation.

2. Creation evidence shall include, where applicable:

(a) signing request identifier;

(b) Digital Signature identifier;

(c) Digital Signature Creation Device reference;

(d) Digital Signature Creation Mechanism reference;

(e) creation time;

(f) service Version;

(g) applicable Profile.

3. Creation evidence shall not expose Digital Signature Creation Data.

SERVICE EVIDENCE

Article 12

1. The Digital Signing Service shall maintain evidence sufficient to demonstrate operation of the service.

2. Service evidence shall identify:

(a) received request;

(b) evaluation performed;

(c) dependencies used;

(d) creation operation;

(e) resulting Digital Signature;

(f) service outcome.

3. Evidence shall be protected against unauthorised alteration.

QUALIFIED DIGITAL SIGNING SERVICE

Article 13

1. A Digital Signing Service intended to operate as a Qualified Trust Service shall satisfy the applicable Qualified Profile.

2. The Qualified Profile shall identify:

(a) required Trust Service Provider Status;

(b) required Trust Service Status;

(c) applicable Digital Signature Creation Device requirements;

(d) applicable service assurance conditions;

(e) required evidence.

3. Qualified Status of the Digital Signing Service shall not establish:

(a) Qualified Electronic Signature Status;

(b) Qualified Electronic Seal Status;

(c) Qualified Digital Signature Creation Device Status.

4. Each qualified condition shall be evaluated separately.

SERVICE LIFECYCLE MANAGEMENT

Article 14

1. The lifecycle of a Digital Signing Service shall include, where applicable:

(a) preparation;

(b) activation;

(c) operation;

(d) modification;

(e) restriction;

(f) Suspension;

(g) cessation.

2. Lifecycle events affecting signing operations shall be recorded.

Article 15

1. Changes affecting the Digital Signing Service shall be assessed before implementation.

2. The assessment shall consider:

(a) Digital Signature Creation Devices;

(b) Digital Signature Creation Mechanisms;

(c) supported Profiles;

(d) Authentication dependencies;

(e) Authorisation dependencies;

(f) Technical Specifications.

3. Material changes shall be managed according to applicable Change Control requirements.

INCIDENT MANAGEMENT

Article 16

1. A Digital Signing Service shall maintain procedures for:

(a) signing service interruption;

(b) Digital Signature Creation Device compromise;

(c) Digital Signature Creation Data compromise;

(d) failed signing operations;

(e) recovery.

2. Incident records shall identify affected signing operations where applicable.

3. The effect on created Digital Signatures shall be determined through applicable Validation processes.

RECORDS AND EVIDENCE

Article 17

1. The Digital Signing Service shall maintain records sufficient to reconstruct:

(a) signing requests;

(b) authentication and authorisation dependencies;

(c) Digital Signature creation operations;

(d) service decisions;

(e) incidents;

(f) lifecycle changes.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 18

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Electronic Signature Status;

(b) Qualified Electronic Signature Status;

(c) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 419 241-1	General security requirements for trustworthy systems supporting server signing
ETSI EN 419 241-2	Protection Profile for QSCD used for server signing
ETSI TS 119 431-1	Policy and security requirements for remote signature creation services
ETSI TS 119 432	Protocols and interfaces for remote signature creation
ETSI EN 319 102-1	Signature validation process where service evidence includes validation dependencies
ETSI EN 319 312	Cryptographic suites where applicable
ISO/IEC 27001:2022	Information security management controls applicable to Digital Signing Services
ISO/IEC 27701:2025	Privacy management controls where personal data is processed
ISO 22301:2019	Business continuity management where continuity requirements apply

IDEHA-IG-SVC-SIG-001: ELECTRONIC SIGNATURE SERVICE IMPLEMENTATION

Version: 0.1

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Electronic Signature Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Electronic Signature Services and Actors operating Electronic Signature Service functions within the applicable Service Scope.

3. This Guideline establishes requirements for:

(a) Electronic Signature request processing;

(b) Signatory interaction;

(c) signing workflow management;

(d) signing intent evidence;

(e) presentation and confirmation of data before signing;

(f) delivery of Electronic Signatures;

(g) Electronic Signature service evidence.

4. This Guideline applies together with:

(a) IDEHA-IG-OBJ-SIG-001 Electronic Signature Implementation;

(b) IDEHA-IG-OBJ-DSG-001 Digital Signature Creation Data and Device Implementation;

(c) IDEHA-IG-SVC-DSG-001 Digital Signing Service Implementation;

(d) IDEHA-IG-SVC-AUT-001 Authentication Service Implementation;

(e) IDEHA-IG-SVC-AUZ-001 Authorisation Service Implementation;

(f) IDEHA-IG-SVC-VVS-001 Validation and Verification Service Implementation;

(g) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) Digital Signature Creation Data requirements;

(b) Digital Signature Creation Device requirements;

(c) cryptographic algorithms;

(d) cryptographic parameters;

(e) Certificate issuance requirements;

(f) Digital Signature formats;

(g) Validation procedures.

Those matters shall be implemented through the applicable Framework Instruments.

ELECTRONIC SIGNATURE SERVICE SCOPE

Article 2

1. An Electronic Signature Service shall operate within an identified Service Scope.

2. The Service Scope shall identify:

(a) permitted Electronic Signature functions;

(b) supported Electronic Signature Profiles;

(c) supported signing workflows;

(d) applicable Authentication dependencies;

(e) applicable Authorisation dependencies;

(f) applicable Assurance Conditions;

(g) applicable Security Conditions.

3. An Electronic Signature Service shall not perform functions outside its approved Service Scope.

Article 3

1. An Electronic Signature Service shall maintain separation between:

(a) Electronic Signature workflow;

(b) Digital Signature creation;

(c) Authentication;

(d) Authorisation;

(e) Validation.

2. An Electronic Signature Service shall not create legal effects beyond those established by the applicable Framework Instruments.

ELECTRONIC SIGNATURE REQUEST PROCESSING

Article 4

1. An Electronic Signature Service shall process Electronic Signature requests according to the applicable Electronic Signature Profile.

2. An Electronic Signature request shall identify, where applicable:

(a) requesting Actor;

(b) Signatory;

(c) data to be signed;

(d) intended purpose;

(e) applicable Signature Profile;

(f) required evidence.

3. The Electronic Signature Service shall verify that the requested signing operation is within its Service Scope.

Article 5

1. Before initiating a signing operation, the Electronic Signature Service shall determine that:

(a) the Signatory is identified according to the applicable Profile;

(b) required Authentication conditions are satisfied;

(c) required Authorisation conditions are satisfied;

(d) the data to be signed is identified;

(e) the signing workflow is applicable.

2. The Electronic Signature Service shall not replace the Identification Service or Authentication Service.

SIGNATORY INTERACTION

Article 6

1. The Electronic Signature Service shall provide mechanisms enabling the Signatory to participate in the signing process.

2. The signing interaction shall ensure, where applicable:

(a) identification of the data to be signed;

(b) presentation of relevant signing information;

(c) confirmation of the signing operation;

(d) recording of the signing action.

3. The applicable Profile shall define the required level of interaction.

Article 7

1. The Electronic Signature Service shall ensure that the Signatory is able to understand the signing operation to the extent required by the applicable Profile.

2. The signing interface shall identify, where applicable:

(a) signed data;

(b) relevant transaction information;

(c) signing context;

(d) applicable limitations.

3. Presentation requirements shall remain separate from Digital Signature creation requirements.

SIGNING INTENT

Article 8

1. Where signing intent is required by the applicable Profile, the Electronic Signature Service shall capture evidence demonstrating that the Signatory intended to apply the Electronic Signature to the identified data.

2. Signing intent evidence may include:

(a) explicit confirmation;

(b) user interaction;

(c) transaction confirmation;

(d) another approved interaction mechanism.

3. Signing intent shall remain separate from:

(a) Authentication;

(b) Authorisation;

(c) Digital Signature creation.

Article 9

1. The Electronic Signature Service shall record signing intent evidence where required.

2. The evidence shall identify:

(a) Signatory;

(b) signed data reference;

(c) signing event;

(d) time of confirmation;

(e) applicable workflow.

3. Signing intent evidence shall be protected against unauthorised alteration.

AUTHENTICATION AND AUTHORISATION DEPENDENCIES

Article 10

1. Where required by the applicable Profile, the Electronic Signature Service shall obtain an Authentication Outcome before completing a signing operation.

2. The Authentication Outcome shall identify, where applicable:

(a) authenticated Subject;

(b) Authentication Service;

(c) Authentication Assurance;

(d) validity period;

(e) limitations.

3. Authentication shall remain separate from the Electronic Signature.

Article 11

1. Where required by the applicable Profile, the Electronic Signature Service shall obtain an Authorisation Outcome before completing a signing operation.

2. The Authorisation Outcome shall identify, where applicable:

(a) permitted signing operation;

(b) Actor;

(c) represented Subject;

(d) scope;

(e) validity period;

(f) restrictions.

3. Authorisation shall remain separate from the Electronic Signature.

DIGITAL SIGNATURE SERVICE DEPENDENCY

Article 12

1. An Electronic Signature Service shall use a Digital Signing Service or equivalent Digital Signature creation function where a Digital Signature is required.

2. The Electronic Signature Service shall maintain evidence of:

(a) Digital Signing Service used;

(b) Digital Signature creation operation;

(c) resulting Digital Signature;

(d) applicable Signature Profile.

3. The Electronic Signature Service shall not modify the Digital Signature creation environment.

Article 13

1. The Electronic Signature Service shall maintain the relationship between:

(a) Signatory;

(b) signing workflow;

(c) signed data;

(d) Digital Signature;

(e) resulting Electronic Signature.

2. The relationship shall support Validation according to the applicable Profile.

ELECTRONIC SIGNATURE DELIVERY

Article 14

1. The Electronic Signature Service shall deliver the resulting Electronic Signature according to the applicable Profile.

2. Delivery information shall identify, where applicable:

(a) Electronic Signature Identifier;

(b) recipient;

(c) delivery time;

(d) applied Profile;

(e) associated evidence.

3. The delivered Electronic Signature shall remain protected against unauthorised alteration.

QUALIFIED ELECTRONIC SIGNATURE SERVICE

Article 15

1. An Electronic Signature Service intended to provide Qualified Electronic Signatures shall satisfy the applicable Qualified Profile.

2. The Qualified Profile shall identify:

(a) required Qualified Trust Service Provider Status;

(b) required Qualified Trust Service Status;

(c) required Digital Signing Service conditions;

(d) required Qualified Digital Signature Creation Device dependency;

(e) required Qualified Certificate dependency;

(f) required evidence.

3. Qualification of the Electronic Signature Service shall not by itself establish Qualified Electronic Signature Status for every signature created through the service.

4. Qualified Electronic Signature Status shall be determined according to the applicable Qualified Object Profile.

SERVICE EVIDENCE

Article 16

1. The Electronic Signature Service shall maintain evidence sufficient to reconstruct:

(a) signing request;

(b) Signatory interaction;

(c) Authentication and Authorisation dependencies;

(d) signing intent where applicable;

(e) Digital Signature creation reference;

(f) resulting Electronic Signature.

2. Evidence shall be protected according to applicable Security Conditions.

LIFECYCLE MANAGEMENT

Article 17

1. The lifecycle of an Electronic Signature Service shall include, where applicable:

(a) preparation;

(b) activation;

(c) operation;

(d) modification;

(e) restriction;

(f) Suspension;

(g) cessation.

2. Lifecycle events affecting signing operations shall be recorded.

Article 18

1. Changes affecting an Electronic Signature Service shall be assessed before implementation.

2. The assessment shall consider:

(a) applicable Electronic Signature Profiles;

(b) Digital Signing Service dependencies;

(c) Authentication dependencies;

(d) Authorisation dependencies;

(e) Technical Specifications;

(f) Security Conditions.

3. Material changes shall be managed according to applicable Change Control requirements.

ACCESSIBILITY AND SAFEGUARDS

Article 19

1. An Electronic Signature Service shall provide Accessible Alternatives where required by the applicable Safeguard Conditions.

2. Accessible Alternatives shall preserve the applicable Assurance Conditions.

3. The applicable Profile shall define:

(a) assisted signing arrangements;

(b) alternative interaction methods;

(c) human support conditions;

(d) accessibility requirements.

RECORDS AND EVIDENCE

Article 20

1. The Electronic Signature Service shall maintain records sufficient to reconstruct:

(a) signing requests;

(b) Signatory interaction;

(c) signing intent evidence;

(d) Authentication dependencies;

(e) Authorisation dependencies;

(f) Digital Signature creation references;

(g) service lifecycle events.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 21

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Electronic Signature Status;

(b) Qualified Electronic Signature Status;

(c) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 319 401	General policy requirements for Trust Service Providers
ETSI EN 319 411-2	Qualified certificate issuing requirements where qualified signatures are supported
ETSI EN 319 102-1	Signature validation process requirements

Reference	Application
ETSI EN 319 122-1	CAdES representation requirements
ETSI EN 319 132-1	XAdES representation requirements
ETSI EN 319 142-1	PAdES representation requirements
ETSI TS 119 182-1	JAdES representation requirements
ETSI TS 119 431-1	Remote signing service requirements where applicable
ISO/IEC 29115	Authentication assurance considerations
ISO/IEC 24760 series	Identity information and identity binding considerations
ISO/IEC 27001:2022	Information security management controls
ISO/IEC 27701:2025	Privacy management controls where personal data is processed

IDEHA-IG-SVC-SEL-001: ELECTRONIC SEAL SERVICE IMPLEMENTATION

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Electronic Seal Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Electronic Seal Services and Actors operating Electronic Seal Service functions within the applicable Service Scope.

3. This Guideline establishes requirements for:

(a) Electronic Seal request processing;

(b) Seal Creator interaction and authority handling;

(c) sealing workflow management;

(d) automated and scheduled sealing operations;

(e) interaction with Digital Signing Services;

(f) Seal Evidence management;

(g) Electronic Seal Service lifecycle management.

4. This Guideline applies together with:

(a) IDEHA-IG-OBJ-SEL-001 Electronic Seal Implementation;

(b) IDEHA-IG-OBJ-DSG-001 Digital Signature Creation Data and Device Implementation;

(c) IDEHA-IG-SVC-DSG-001 Digital Signing Service Implementation;

(d) IDEHA-IG-SVC-AUT-001 Authentication Service Implementation;

(e) IDEHA-IG-SVC-AUZ-001 Authorisation Service Implementation;

(f) IDEHA-IG-SVC-VVS-001 Validation and Verification Service Implementation;

(g) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) Digital Signature Creation Data requirements;

(b) Digital Signature Creation Device requirements;

(c) cryptographic algorithms;

(d) cryptographic parameters;

(e) Electronic Seal object requirements;

(f) Advanced Electronic Seal requirements;

(g) Qualified Electronic Seal requirements;

(h) Seal Validation procedures.

Those matters shall be implemented through the applicable Framework Instruments.

ELECTRONIC SEAL SERVICE SCOPE

Article 2

1. An Electronic Seal Service shall operate within an identified Service Scope.

2. The Service Scope shall identify:

(a) permitted sealing functions;

(b) supported Electronic Seal Profiles;

(c) supported sealing workflows;

(d) supported Digital Signing Services;

(e) applicable Authentication dependencies;

(f) applicable Authorisation dependencies;

(g) applicable Assurance Conditions;

(h) applicable Security Conditions.

3. An Electronic Seal Service shall not perform sealing operations outside its approved Service Scope.

Article 3

1. An Electronic Seal Service shall maintain separation between:

(a) sealing workflow;

(b) Digital Signature creation;

(c) organisational authority evaluation;

(d) Authentication;

(e) Authorisation;

(f) Validation.

2. An Electronic Seal Service shall not determine legal effect of sealed data.

3. The resulting Electronic Seal shall acquire its applicable legal or evidential effect only according to the Main Framework and applicable Profile.

SEAL REQUEST PROCESSING

Article 4

1. An Electronic Seal Service shall process sealing requests according to the applicable Electronic Seal Profile.

2. A sealing request shall identify, where applicable:

(a) requesting Actor;

(b) Seal Creator;

(c) data to be sealed;

(d) intended purpose;

(e) applicable Seal Profile;

(f) required evidence.

3. The Electronic Seal Service shall verify that the requested sealing operation is within its Service Scope.

Article 5

1. Before initiating a sealing operation, the Electronic Seal Service shall determine that:

(a) the requesting Actor is identified;

(b) the Seal Creator is identified;

(c) required authority conditions are satisfied;

(d) the data to be sealed is identified;

(e) applicable workflow requirements are fulfilled.

2. The Electronic Seal Service shall not replace:

(a) Identification Service;

(b) Authentication Service;

(c) Authorisation Service.

SEAL CREATOR AND AUTHORITY HANDLING

Article 6

1. An Electronic Seal Service shall maintain evidence identifying the Seal Creator associated with the sealing operation.

2. Seal Creator information shall identify, where applicable:

(a) Seal Creator reference;

(b) organisational Actor;

(c) authority basis;

(d) effective period;

(e) limitations.

3. Seal Creator information shall remain separate from:

(a) Digital Signature Creation Data;

(b) Certificate Identifier;

(c) Electronic Seal Identifier;

(d) Trust Object Identifier.

Article 7

1. Where sealing requires organisational approval, the Electronic Seal Service shall verify the applicable approval or authority condition before initiating sealing.

2. Approval evidence may identify:

(a) approving Actor;

(b) approval event;

(c) approved data;

(d) applicable policy;

(e) approval time.

3. Approval evidence shall remain separate from the resulting Electronic Seal.

AUTOMATED AND SCHEDULED SEALING

Article 8

1. An Electronic Seal Service may support automated sealing where permitted by the applicable Profile.

2. Automated sealing shall identify:

(a) initiating system or process;

(b) sealing policy;

(c) authority permitting automated sealing;

(d) data selection rules;

(e) sealing event.

3. Automated sealing shall not remove the requirement to identify the Seal Creator.

Article 9

1. Scheduled sealing operations shall operate according to predefined conditions.

2. The Electronic Seal Service shall maintain evidence of:

(a) schedule definition;

(b) execution event;

(c) data selection;

(d) sealing operation;

(e) resulting Electronic Seal.

3. Changes to scheduled sealing conditions shall be managed through applicable Change Control requirements.

AUTHENTICATION AND AUTHORISATION DEPENDENCIES

Article 10

1. Where required by the applicable Profile, the Electronic Seal Service shall obtain an Authentication Outcome before completing a sealing operation.

2. The Authentication Outcome shall identify, where applicable:

(a) authenticated Actor;

(b) Authentication Service;

(c) Authentication Assurance;

(d) validity period;

(e) limitations.

3. Authentication shall remain separate from Electronic Seal creation.

Article 11

1. Where required by the applicable Profile, the Electronic Seal Service shall obtain an Authorisation Outcome before completing a sealing operation.

2. The Authorisation Outcome shall identify, where applicable:

(a) permitted sealing operation;

(b) Actor;

(c) scope;

(d) validity period;

(e) restrictions.

3. Authorisation shall remain separate from the Electronic Seal.

DIGITAL SIGNATURE CREATION DEPENDENCY

Article 12

1. An Electronic Seal Service shall use a Digital Signing Service or equivalent Digital Signature creation function where a Digital Signature is required for sealing.

2. The Electronic Seal Service shall maintain evidence of:

(a) Digital Signing Service used;

(b) Digital Signature creation operation;

(c) resulting Digital Signature;

(d) applicable Seal Profile.

3. The Electronic Seal Service shall not modify the Digital Signature Creation Device or Digital Signature Creation Data environment.

Article 13

1. The Electronic Seal Service shall maintain the relationship between:

(a) Seal Creator;

(b) sealing workflow;

(c) sealed data;

(d) Digital Signature;

(e) resulting Electronic Seal.

2. The relationship shall support Validation according to the applicable Profile.

SEAL DELIVERY AND EVIDENCE

Article 14

1. The Electronic Seal Service shall deliver the resulting Electronic Seal according to the applicable Profile.

2. Delivery information shall identify, where applicable:

(a) Electronic Seal Identifier;

(b) recipient;

(c) delivery time;

(d) applied Profile;

(e) associated evidence.

3. The delivered Electronic Seal shall remain protected against unauthorised alteration.

Article 15

1. The Electronic Seal Service shall maintain Seal Evidence sufficient to reconstruct:

(a) sealing request;

(b) Seal Creator;

(c) authority evaluation;

(d) Authentication and Authorisation dependencies;

(e) Digital Signature creation reference;

(f) resulting Electronic Seal.

2. Seal Evidence shall be protected according to applicable Security Conditions.

QUALIFIED ELECTRONIC SEAL SERVICE

Article 16

1. An Electronic Seal Service intended to provide Qualified Electronic Seals shall satisfy the applicable Qualified Profile.

2. The Qualified Profile shall identify:

(a) required Qualified Trust Service Provider Status;

(b) required Qualified Trust Service Status;

(c) required Digital Signing Service conditions;

(d) required Qualified Digital Signature Creation Device dependency;

(e) required Qualified Certificate dependency;

(f) required evidence.

3. Qualification of the Electronic Seal Service shall not by itself establish Qualified Electronic Seal Status for every seal created through the service.

4. Qualified Electronic Seal Status shall be determined according to the applicable Qualified Object Profile.

SERVICE LIFECYCLE MANAGEMENT

Article 17

1. The lifecycle of an Electronic Seal Service shall include, where applicable:

(a) preparation;

(b) activation;

(c) operation;

(d) modification;

(e) restriction;

(f) Suspension;

(g) cessation.

2. Lifecycle events affecting sealing operations shall be recorded.

Article 18

1. Changes affecting an Electronic Seal Service shall be assessed before implementation.

2. The assessment shall consider:

(a) Electronic Seal Profiles;

(b) Digital Signing Service dependencies;

(c) Authentication dependencies;

(d) Authorisation dependencies;

(e) Technical Specifications;

(f) Security Conditions.

3. Material changes shall be managed according to applicable Change Control requirements.

INCIDENT MANAGEMENT

Article 19

1. An Electronic Seal Service shall maintain procedures for:

(a) sealing service interruption;

(b) Digital Signature Creation Device compromise;

(c) Digital Signature Creation Data compromise;

(d) failed sealing operations;

(e) recovery.

2. Incident records shall identify affected sealing operations where applicable.

3. The effect on created Electronic Seals shall be determined through applicable Validation processes.

RECORDS AND EVIDENCE

Article 20

1. The Electronic Seal Service shall maintain records sufficient to reconstruct:

(a) sealing requests;

(b) Seal Creator identification;

(c) authority verification;

(d) Authentication and Authorisation dependencies;

(e) Digital Signature creation references;

(f) resulting Electronic Seals;

(g) service lifecycle events.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 21

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Electronic Seal Status;

(b) Qualified Electronic Seal Status;

(c) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 319 401	General policy requirements for Trust Service Providers
ETSI EN 319 411-2	Qualified certificate issuing requirements where qualified seals are supported
ETSI EN 319 102-1	Signature and seal validation process requirements
ETSI EN 319 122-1	CAdES seal representation requirements
ETSI EN 319 132-1	XAdES seal representation requirements
ETSI EN 319 142-1	PAdES seal representation requirements
ETSI TS 119 182-1	JAdES seal representation requirements
ETSI TS 119 431-1	Remote signing service requirements where applicable
ISO/IEC 24760 series	Identity and organisational identity relationship considerations
ISO/IEC 27001:2022	Information security management controls
ISO/IEC 27701:2025	Privacy management controls where personal data is processed
ISO 22301:2019	Business continuity management where continuity requirements apply

IDEHA-IG-SVC-TST-001: ELECTRONIC TIMESTAMP SERVICE IMPLEMENTATION

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Electronic Timestamp Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Electronic Timestamp Services and Actors operating Electronic Timestamp Service functions within the applicable Service Scope.

3. This Guideline establishes requirements for:

(a) Electronic Timestamp Service operation;

(b) timestamp request processing;

(c) Time-Stamping Unit operation;

(d) trusted time source management;

(e) timestamp issuance;

(f) timestamp service evidence;

(g) service lifecycle management.

4. This Guideline applies together with:

(a) IDEHA-IG-OBJ-TST-001 Electronic Timestamp Implementation;

(b) IDEHA-IG-SVC-VVS-001 Validation and Verification Service Implementation;

(c) IDEHA-IG-OBJ-DSG-001 Digital Signature Creation Data and Device Implementation;

(d) IDEHA-IG-SEC-CRY-001 Cryptographic Controls and Cryptographic Agility Implementation;

(e) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) Electronic Timestamp object categories;

(b) Qualified Electronic Timestamp object conditions;

(c) timestamp token formats;

(d) signature timestamp integration;

(e) signature or seal validation procedures;

(f) cryptographic algorithm selection.

Those matters shall be implemented through the applicable Framework Instruments.

ELECTRONIC TIMESTAMP SERVICE SCOPE

Article 2

1. An Electronic Timestamp Service shall operate within an identified Service Scope.

2. The Service Scope shall identify:

(a) permitted timestamp functions;

(b) supported Timestamp Profiles;

(c) supported Time-Stamping Units;

(d) applicable time sources;

(e) applicable Assurance Conditions;

(f) applicable Security Conditions;

(g) applicable Technical Specifications.

3. An Electronic Timestamp Service shall not issue Electronic Timestamps outside its approved Service Scope.

TIMESTAMP SERVICE ARCHITECTURE

Article 3

1. An Electronic Timestamp Service shall maintain operational separation between:

(a) time source management;

(b) Time-Stamping Unit operation;

(c) timestamp request processing;

(d) timestamp creation;

(e) timestamp evidence management.

2. The Electronic Timestamp Service shall identify the components involved in timestamp creation.

3. Component relationships shall be maintained as operational evidence.

Article 4

1. An Electronic Timestamp Service shall operate Time-Stamping Units within a controlled security environment.

2. The Time-Stamping Unit shall:

(a) receive authorised timestamp requests;

(b) obtain trusted time information;

(c) create Electronic Timestamps;

(d) protect timestamp creation functions;

(e) maintain required evidence.

3. The Time-Stamping Unit shall operate according to the applicable Timestamp Profile.

TIMESTAMP REQUEST PROCESSING

Article 5

1. An Electronic Timestamp Service shall process timestamp requests according to the applicable Timestamp Profile.

2. A timestamp request shall identify, where applicable:

(a) requesting Actor;

(b) data reference;

(c) requested timestamp function;

(d) applicable Timestamp Profile;

(e) required evidence.

3. The Electronic Timestamp Service shall verify that the requested operation is within its Service Scope.

Article 6

1. An Electronic Timestamp Service shall ensure that the timestamp request is processed without unauthorised modification.

2. Request processing shall maintain evidence of:

(a) request receipt;

(b) request evaluation;

(c) request acceptance or rejection;

(d) timestamp creation result.

3. The Electronic Timestamp Service shall not require disclosure of the original electronic data where a protected data reference is used.

TRUSTED TIME SOURCE MANAGEMENT

Article 7

1. An Electronic Timestamp Service shall use trusted time sources appropriate to the applicable Timestamp Profile.

2. The trusted time source arrangement shall establish:

(a) traceability to the applicable time reference;

(b) synchronisation conditions;

(c) monitoring conditions;

(d) accuracy conditions;

(e) failure handling conditions.

3. The Electronic Timestamp Service shall monitor the accuracy and availability of trusted time sources.

Article 8

1. The Electronic Timestamp Service shall establish procedures for loss of acceptable time synchronisation.

2. Where trusted time conditions are no longer satisfied, the Electronic Timestamp Service shall:

(a) prevent issuance where required;

(b) record the event;

(c) assess affected timestamps;

(d) initiate corrective measures.

3. The applicable Timestamp Profile shall define the conditions for service restoration.

TIME-STAMPING UNIT OPERATION

Article 9

1. A Time-Stamping Unit shall operate within an identified security boundary.

2. The security boundary shall identify:

(a) protected components;

(b) timestamp creation functions;

(c) cryptographic functions;

(d) administrative functions;

(e) external dependencies.

3. The Time-Stamping Unit shall protect timestamp creation material against:

(a) unauthorised disclosure;

(b) unauthorised use;

(c) unauthorised modification;

(d) unauthorised replacement.

Article 10

1. The Electronic Timestamp Service shall maintain evidence relating to each Time-Stamping Unit.

2. Evidence shall identify, where applicable:

(a) Time-Stamping Unit Identifier;

(b) configuration Version;

(c) cryptographic dependencies;

(d) operational Status;

(e) lifecycle events.

ELECTRONIC TIMESTAMP ISSUANCE

Article 11

1. An Electronic Timestamp Service shall create Electronic Timestamps according to the applicable Timestamp Profile.

2. The issuance process shall establish:

(a) data-reference binding;

(b) trusted time application;

(c) timestamp protection;

(d) issuance evidence.

3. The Electronic Timestamp Service shall maintain the relationship between:

(a) timestamp request;

(b) Time-Stamping Unit;

(c) trusted time source;

(d) resulting Electronic Timestamp.

Article 12

1. The Electronic Timestamp Service shall maintain issuance records sufficient to reconstruct timestamp creation.

2. Issuance records shall identify:

(a) request identifier;

(b) timestamp identifier;

(c) Time-Stamping Unit;

(d) creation time;

(e) applicable Timestamp Profile;

(f) service Version.

QUALIFIED ELECTRONIC TIMESTAMP SERVICE

Article 13

1. An Electronic Timestamp Service intended to provide Qualified Electronic Timestamps shall satisfy the applicable Qualified Profile.

2. The Qualified Profile shall identify:

(a) required Qualified Trust Service Provider Status;

(b) required Qualified Trust Service Status;

(c) required time-source conditions;

(d) required security conditions;

(e) required evidence;

(f) required conformity assessment.

3. Qualification of the Electronic Timestamp Service shall not automatically establish Qualified Status for every Electronic Timestamp issued.

4. Qualified Electronic Timestamp Status shall be determined according to the applicable Qualified Object Profile.

TIMESTAMP SERVICE EVIDENCE

Article 14

1. The Electronic Timestamp Service shall maintain evidence sufficient to demonstrate:

(a) request processing;

(b) trusted time conditions;

(c) Time-Stamping Unit operation;

(d) timestamp issuance;

(e) security events;

(f) lifecycle changes.

2. Evidence shall be protected against unauthorised alteration.

SERVICE LIFECYCLE MANAGEMENT

Article 15

1. The lifecycle of an Electronic Timestamp Service shall include, where applicable:

(a) preparation;

(b) activation;

(c) operation;

(d) modification;

(e) restriction;

(f) Suspension;

(g) cessation.

2. Lifecycle events affecting timestamp reliability shall be recorded.

Article 16

1. Changes affecting an Electronic Timestamp Service shall be assessed before implementation.

2. The assessment shall consider:

(a) Time-Stamping Units;

(b) trusted time sources;

(c) cryptographic dependencies;

(d) Timestamp Profiles;

(e) Technical Specifications;

(f) Security Conditions.

3. Material changes shall be managed according to applicable Change Control requirements.

INCIDENT MANAGEMENT AND CONTINUITY

Article 17

1. An Electronic Timestamp Service shall maintain procedures for:

(a) time-source failure;

(b) Time-Stamping Unit compromise;

(c) cryptographic compromise;

(d) service interruption;

(e) recovery.

2. Incident records shall identify affected Electronic Timestamps where applicable.

3. The effect on issued Electronic Timestamps shall be determined through the applicable Validation process.

RECORDS AND EVIDENCE

Article 18

1. The Electronic Timestamp Service shall maintain records sufficient to reconstruct:

(a) timestamp requests;

(b) trusted time conditions;

(c) Time-Stamping Unit operation;

(d) timestamp issuance;

(e) lifecycle events;

(f) incident events.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 19

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Electronic Timestamp Category;

(b) Qualified Electronic Timestamp Status;

(c) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 319 421	Policy and security requirements for Electronic Timestamp Services
ETSI EN 319 422	Timestamp protocol and token profile requirements
RFC 3161	Time-Stamp Protocol
RFC 5816	ESSCertIDv2 update for timestamp token certificate identification
ETSI EN 319 102-1	Validation process requirements applicable to timestamps
ISO/IEC 18014-4	Time source traceability and assurance considerations
ISO 8601-1:2019	Date and time representation
ISO/IEC 27001:2022	Information security management controls
ISO/IEC 27701:2025	Privacy management controls where personal data is processed
ISO 22301:2019	Business continuity management where continuity requirements apply

IDEHA-IG-SVC-EAS-001: ELECTRONIC ATTESTATION SERVICE IMPLEMENTATION

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Electronic Attestation Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Electronic Attestation Services and Actors operating Electronic Attestation Service functions within the applicable Service Scope.

3. This Guideline establishes requirements for:

(a) Electronic Attestation Service operation;

(b) attestation request processing;

(c) Attestation Issuer responsibilities;

(d) evidence evaluation before issuance;

(e) Source Basis handling;

(f) Electronic Attestation issuance;

(g) Electronic Attestation lifecycle management;

(h) issuance evidence management.

4. This Guideline applies together with:

(a) IDEHA-IG-OBJ-EAA-001 Electronic Attestation Implementation;

(b) IDEHA-IG-SRC-ASO-001 Source and Authoritative Source Implementation;

(c) IDEHA-IG-SVC-IDN-001 Identification Service Implementation where identity information is used;

(d) IDEHA-IG-DAT-SEM-001 Controlled Data Elements, Semantics and Data Quality Implementation;

(e) IDEHA-IG-SVC-VVS-001 Validation and Verification Service Implementation;

(f) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) Electronic Attestation Categories;

(b) Attribute semantic definitions;

(c) Source authority;

(d) Identification Service operation;

(e) Authentication Service operation;

(f) Authorisation decisions;

(g) attestation data formats;

(h) technical schemas;

(i) cryptographic algorithms.

Those matters shall be implemented through the applicable Framework Instruments.

ELECTRONIC ATTESTATION SERVICE SCOPE

Article 2

1. An Electronic Attestation Service shall operate within an identified Service Scope.

2. The Service Scope shall identify:

(a) permitted attestation functions;

(b) supported Attestation Profiles;

(c) supported Attestation Schemes;

(d) permitted Source Basis;

(e) applicable Assurance Conditions;

(f) applicable Security Conditions;

(g) applicable Technical Specifications.

3. An Electronic Attestation Service shall not issue Electronic Attestations outside its approved Service Scope.

Article 3

1. An Electronic Attestation Service shall maintain separation between:

(a) evidence collection;

(b) evidence evaluation;

(c) attestation creation;

(d) attestation issuance;

(e) attestation Status management.

2. An Electronic Attestation Service shall not:

(a) create Source authority;

(b) modify Attribute meaning;

(c) create underlying legal facts;

(d) replace the Source maintaining the attested information.

3. The Electronic Attestation Service shall remain responsible for the issuance process within its assigned Service Scope.

ATTESTATION REQUEST PROCESSING

Article 4

1. An Electronic Attestation Service shall process attestation requests according to the applicable Attestation Profile.

2. An attestation request shall identify, where applicable:

(a) requesting Actor;

(b) intended Subject;

(c) requested Attestation Profile;

(d) requested Attributes or statements;

(e) intended purpose;

(f) required evidence.

3. The Electronic Attestation Service shall verify that the requested attestation operation is within its Service Scope.

Article 5

1. Before issuing an Electronic Attestation, the Electronic Attestation Service shall determine that:

(a) the request is valid;

(b) the Subject or matter is identified;

(c) the required Source Basis is available;

(d) the requested Attributes are within scope;

(e) applicable issuance conditions are satisfied.

2. The Electronic Attestation Service shall maintain evidence of the evaluation performed before issuance.

ATTESTATION ISSUER RESPONSIBILITIES

Article 6

1. An Electronic Attestation Service shall identify the Attestation Issuer responsible for issuing an Electronic Attestation.

2. The Attestation Issuer information shall identify:

(a) issuing Trust Service Provider or Actor;

(b) Electronic Attestation Service;

(c) applicable Service Scope;

(d) applicable Attestation Profile.

3. The Attestation Issuer shall remain responsible for:

(a) issuance decision;

(b) attestation creation process;

(c) issuance evidence;

(d) lifecycle management.

4. The Attestation Issuer shall not assume responsibility for a Source beyond the evaluation performed according to the applicable Profile.

SOURCE BASIS AND EVIDENCE EVALUATION

Article 7

1. Where an Electronic Attestation relies on information from a Source, the Electronic Attestation Service shall identify the Source Basis.

2. The Source Basis shall identify, where applicable:

(a) Source Identifier;

(b) Source Scope;

(c) Source Holder;

(d) Source Steward;

(e) relevant evidence;

(f) Provenance information.

3. The Electronic Attestation Service shall use Source information only within the Source Scope applicable to the attestation.

Article 8

1. Before issuance, the Electronic Attestation Service shall evaluate the information used to create the Electronic Attestation.

2. The evaluation shall determine, where applicable:

(a) Source applicability;

(b) Attribute applicability;

(c) data integrity;

(d) Provenance;

(e) Freshness Conditions;

(f) applicable Assurance Conditions.

3. Evaluation results shall be retained as issuance evidence.

ATTRIBUTE HANDLING

Article 9

1. An Electronic Attestation Service shall use Attributes according to the applicable semantic definitions.

2. The Electronic Attestation Service shall ensure that:

(a) Attribute Identifier remains separate from Attribute value;

(b) Attribute Version is maintained where applicable;

(c) Attribute meaning remains unchanged;

(d) transformations are recorded.

3. The Electronic Attestation Service shall not create new semantic meaning through issuance.

Article 10

1. Where Attributes are derived, the Electronic Attestation Service shall identify:

(a) source Attributes;

(b) derivation method;

(c) responsible processing function;

(d) derivation Version;

(e) limitations.

2. Derived Attributes shall remain distinguishable from directly sourced Attributes.

ELECTRONIC ATTESTATION ISSUANCE

Article 11

1. An Electronic Attestation Service shall create Electronic Attestations according to the applicable Attestation Profile.

2. The issuance process shall establish:

(a) Subject or matter reference;

(b) Attestation Statement;

(c) Source Basis where applicable;

(d) Attestation Issuer;

(e) issuance time;

(f) applicable Profile;

(g) required protection.

3. The Electronic Attestation Service shall maintain the relationship between:

(a) request;

(b) evaluated evidence;

(c) issuance decision;

(d) resulting Electronic Attestation.

Article 12

1. The Electronic Attestation Service shall protect issued Electronic Attestations according to the applicable Profile.

2. Protection requirements may include:

(a) Electronic Signature;

(b) Electronic Seal;

(c) integrity protection;

(d) other approved mechanisms.

3. Technical protection formats shall be defined through the applicable Technical Specification.

QUALIFIED ELECTRONIC ATTESTATION SERVICE

Article 13

1. An Electronic Attestation Service intended to provide Qualified Electronic Attestations shall satisfy the applicable Qualified Profile.

2. The Qualified Profile shall identify:

(a) required Qualified Trust Service Provider Status;

(b) required Qualified Trust Service Status;

(c) required Source conditions where applicable;

(d) required protection conditions;

(e) required Assurance Conditions;

(f) required evidence.

3. Qualification of the Electronic Attestation Service shall not automatically qualify every Electronic Attestation issued by the service.

4. Qualified Electronic Attestation Status shall be determined according to the applicable Qualified Object Profile.

STATUS AND LIFECYCLE MANAGEMENT

Article 14

1. An Electronic Attestation Service shall maintain lifecycle information for issued Electronic Attestations.

2. Lifecycle information shall include, where applicable:

(a) creation;

(b) issuance;

(c) activation;

(d) use;

(e) correction;

(f) replacement;

(g) Suspension;

(h) Revocation;

(i) expiration;

(j) withdrawal.

3. Lifecycle events shall identify:

(a) responsible Actor;

(b) effective time;

(c) reason;

(d) supporting evidence.

Article 15

1. An Electronic Attestation Service shall maintain Status information necessary for Validation.

2. Status information shall identify, where applicable:

(a) Electronic Attestation Identifier;

(b) Status;

(c) effective time;

(d) reason;

(e) responsible Actor.

3. Status information shall support determination of Historical State where required.

CORRECTION AND REPLACEMENT

Article 16

1. The Electronic Attestation Service shall maintain procedures for:

(a) correction;

(b) replacement;

(c) supersession;

(d) withdrawal;

(e) Revocation.

2. Replacement of an Electronic Attestation shall identify:

(a) predecessor Electronic Attestation;

(b) replacement Electronic Attestation;

(c) reason;

(d) effective time.

3. Previous Electronic Attestations shall remain identifiable where required for Historical State determination.

SERVICE LIFECYCLE MANAGEMENT

Article 17

1. The lifecycle of an Electronic Attestation Service shall include, where applicable:

(a) preparation;

(b) activation;

(c) operation;

(d) modification;

(e) restriction;

(f) Suspension;

(g) cessation.

2. Lifecycle events affecting attestation issuance shall be recorded.

Article 18

1. Changes affecting an Electronic Attestation Service shall be assessed before implementation.

2. The assessment shall consider:

(a) Attestation Profiles;

(b) Source dependencies;

(c) Attribute dependencies;

(d) Technical Specifications;

(e) Security Conditions;

(f) Assurance Conditions.

3. Material changes shall be managed according to applicable Change Control requirements.

RECORDS AND EVIDENCE

Article 19

1. The Electronic Attestation Service shall maintain records sufficient to reconstruct:

(a) attestation requests;

(b) evidence evaluation;

(c) Source Basis;

(d) issuance decisions;

(e) issued Electronic Attestations;

(f) lifecycle events.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 20

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Electronic Attestation Category;

(b) Qualified Electronic Attestation Status;

(c) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 319 401	General policy requirements for Trust Service Providers
ETSI TS 119 461	Identity and Attribute verification requirements where applicable
ISO/IEC 11179-3:2023	Metadata registration and Attribute identification
ISO/IEC 11179-31:2023	Data-element concepts and value-domain descriptions
ISO/IEC 24760-1:2025	Identity information and identity relationship concepts
ISO/IEC 25012:2008	Data quality model
ISO/IEC 25024:2015	Data quality measurement
ISO/IEC 27001:2022	Information security management controls
ISO/IEC 27701:2025	Privacy management controls where personal data is processed
ISO 15489-1:2016	Records management principles

IDEHA-IG-SVC-VVS-001: VALIDATION AND VERIFICATION SERVICE IMPLEMENTATION

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Validation Services and Verification Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Validation and Verification Services and Actors performing Validation or Verification functions within the applicable Service Scope.

3. This Guideline establishes requirements for:

(a) Verification request processing;

(b) Validation request processing;

(c) evidence evaluation;

(d) dependency resolution;

(e) Status determination;

(f) Historical State determination;

(g) Verification Results, Validation Results and Status Responses.

4. This Guideline applies together with:

(a) IDEHA-IG-OBJ-DSG-001 Digital Signature Creation Data and Device Implementation;

(b) IDEHA-IG-OBJ-SIG-001 Electronic Signature Implementation;

(c) IDEHA-IG-OBJ-SEL-001 Electronic Seal Implementation;

(d) IDEHA-IG-OBJ-TST-001 Electronic Timestamp Implementation;

(e) IDEHA-IG-OBJ-EAA-001 Electronic Attestation Implementation;

(f) IDEHA-IG-SVC-AUT-001 Authentication Service Implementation;

(g) IDEHA-IG-SVC-AUZ-001 Authorisation Service Implementation;

(h) IDEHA-IG-PUB-HTL-001 Humanitarian Trust List, Status Publication, Registers, Catalogues and Federation Discovery Implementation.

5. This Guideline does not establish:

(a) Trust Object creation;

(b) Trust Service operation other than Validation and Verification functions;

(c) Certificate issuance;

(d) Status publication;

(e) Source authority;

(f) Authentication;

(g) Authorisation;

(h) cryptographic algorithm selection;

(i) technical object formats.

Those matters shall be implemented through the applicable Framework Instruments.

VALIDATION AND VERIFICATION SERVICE SCOPE

Article 2

1. A Validation and Verification Service shall operate within an identified Service Scope.

2. The Service Scope shall identify:

(a) permitted Validation functions;

(b) permitted Verification functions;

(c) supported Trust Object Categories;

(d) supported Trust Services;

(e) supported Status sources;

(f) applicable Profiles;

(g) applicable Assurance Conditions;

(h) applicable Security Conditions.

3. A Validation and Verification Service shall not perform functions outside its approved Service Scope.

Article 3

1. A Validation and Verification Service shall distinguish between:

(a) Verification;

(b) Validation;

(c) Verification Result;

(d) Validation Result;

(e) Status Response.

2. Verification shall determine whether information can be checked against available evidence.

3. Validation shall determine whether the applicable requirements for reliance are satisfied.

4. A Verification Result shall not automatically establish Validity, Status or Controlled Reliance.

VERIFICATION REQUESTS

Article 4

1. A Validation and Verification Service shall process Verification requests according to the applicable Profile.

2. A Verification request shall identify, where applicable:

(a) requesting Actor;

(b) matter to be verified;

(c) requested Verification function;

(d) applicable Profile;

(e) required evidence.

3. The Validation and Verification Service shall verify that the requested function is within its Service Scope.

Article 5

1. Verification shall evaluate the available information necessary to determine the requested fact.

2. Verification may include:

(a) structural checking;

(b) integrity checking;

(c) consistency checking;

(d) presence checking;

(e) comparison against available information.

3. Verification shall not determine matters requiring Status evaluation, Historical State evaluation or Controlled Reliance assessment.

VALIDATION REQUESTS

Article 6

1. A Validation request shall identify the Trust Object, Trust Service, Source, Authentication Outcome, Authorisation Outcome or other Controlled Matter subject to evaluation.

2. A Validation request shall identify, where applicable:

(a) relying Actor;

(b) intended purpose;

(c) evaluation time;

(d) applicable Profile;

(e) required Assurance Conditions.

3. The Validation and Verification Service shall determine the applicable evaluation requirements before performing Validation.

Article 7

1. Validation shall consider, where applicable:

(a) Authenticity;

(b) Integrity;

(c) Status;

(d) dependency validity;

(e) applicable Assurance Conditions;

(f) Historical State;

(g) limitations.

2. Validation shall evaluate only matters within the applicable Service Scope.

EVIDENCE EVALUATION

Article 8

1. A Validation and Verification Service shall evaluate evidence according to the applicable Validation Profile.

2. Evidence evaluation may include:

(a) Trust Object evidence;

(b) Certificate evidence;

(c) Status evidence;

(d) Source evidence;

(e) Authentication evidence;

(f) Authorisation evidence;

(g) timestamp evidence.

3. The Validation and Verification Service shall record evidence used for the evaluation.

Article 9

1. Evidence used during Validation shall remain attributable to its originating Actor or Source.

2. The Validation and Verification Service shall not become the owner of evidence solely because it evaluates that evidence.

3. Evidence transformation or derivation performed during Validation shall be recorded.

TRUST OBJECT VALIDATION

Article 10

1. Validation of a Trust Object shall determine whether the Trust Object satisfies applicable requirements.

2. Validation shall consider, where applicable:

(a) Trust Object identity;

(b) issuing Actor;

(c) protection mechanism;

(d) dependency information;

(e) Status;

(f) applicable Profile;

(g) Historical State.

3. Validation requirements shall be defined by the applicable Trust Object Profile.

Article 11

1. Digital Signature and Electronic Signature Validation shall determine, where applicable:

(a) signed data integrity;

(b) Digital Signature integrity;

(c) Validation Data applicability;

(d) Certificate dependencies;

(e) applicable Signature Profile;

(f) Historical State.

2. Electronic Seal Validation shall determine, where applicable:

(a) sealed data integrity;

(b) Digital Signature integrity;

(c) Seal Creator dependencies;

(d) Certificate dependencies;

(e) applicable Seal Profile.

3. The Validation and Verification Service shall not create Electronic Signatures or Electronic Seals.

Article 12

1. Electronic Timestamp Validation shall determine, where applicable:

(a) timestamp integrity;

(b) Timestamp Issuer;

(c) data reference binding;

(d) time information;

(e) Status information;

(f) Historical State.

2. The Validation and Verification Service shall not create Electronic Timestamps.

Article 13

1. Electronic Attestation Validation shall determine, where applicable:

(a) Attestation Issuer;

(b) integrity of the Attestation Statement;

(c) Source Basis;

(d) Attribute applicability;

(e) Status;

(f) Historical State.

2. Validation shall consider the applicable Attestation Profile.

CERTIFICATE AND STATUS VALIDATION

Article 14

1. Where Validation depends on Certificates, the Validation and Verification Service shall evaluate:

(a) certificate integrity;

(b) certificate chain;

(c) issuer information;

(d) certificate Status;

(e) applicable certificate policy;

(f) historical validity.

2. Certificate Validation shall be performed according to the applicable Certificate Profile.

Article 15

1. Where Validation requires Status information, the Validation and Verification Service shall determine:

(a) Status source;

(b) Status authenticity;

(c) Status applicability;

(d) effective time;

(e) historical Status where required.

2. Status information shall be evaluated separately from the identity of the Status source.

HUMANITARIAN TRUST LIST DEPENDENCY

Article 16

1. Where Validation depends on Humanitarian Trust List information, the Validation and Verification Service shall determine:

(a) applicable Trust List Version;

(b) authenticity of the Trust List;

(c) relevant Entry;

(d) published Status;

(e) effective time;

(f) historical information.

2. Humanitarian Trust List publication shall remain separate from Validation decisions.

3. The Validation and Verification Service shall not create Trust Service Status.

AUTHENTICATION AND AUTHORISATION OUTCOME VALIDATION

Article 17

1. Where Validation requires Authentication Outcomes, the Validation and Verification Service shall determine:

(a) issuing Authentication Service;

(b) Authentication Outcome integrity;

(c) Authentication Assurance;

(d) validity period;

(e) limitations.

2. Authentication Outcome Validation shall not create a new Authentication Event.

Article 18

1. Where Validation requires Authorisation Outcomes, the Validation and Verification Service shall determine:

(a) issuing Authorisation Service;

(b) Outcome integrity;

(c) Policy reference;

(d) validity period;

(e) scope;

(f) limitations.

2. Authorisation Outcome Validation shall not create a new Authorisation decision.

HISTORICAL STATE

Article 19

1. Where reliance requires evaluation at a previous time, the Validation and Verification Service shall determine the applicable Historical State.

2. Historical State determination shall consider:

(a) Trust Object Version;

(b) Status at the relevant time;

(c) dependency Status;

(d) applicable Standards;

(e) applicable Profiles.

3. Current Status shall not automatically determine Historical State.

VALIDATION RESULTS AND STATUS RESPONSES

Article 20

1. A Validation and Verification Service shall produce a result corresponding to the performed evaluation.

2. A Verification Result shall identify, where applicable:

(a) evaluated matter;

(b) checks performed;

(c) result;

(d) limitations.

3. A Validation Result shall identify, where applicable:

(a) evaluated matter;

(b) evidence used;

(c) evaluation time;

(d) Status information;

(e) Historical State;

(f) limitations.

Article 21

1. A Status Response shall identify:

(a) Status source;

(b) evaluated Status;

(c) effective time;

(d) applicable scope;

(e) limitations.

2. A Status Response shall remain separate from a Validation Result.

SERVICE LIFECYCLE MANAGEMENT

Article 22

1. The lifecycle of a Validation and Verification Service shall include, where applicable:

(a) preparation;

(b) activation;

(c) operation;

(d) modification;

(e) restriction;

(f) Suspension;

(g) cessation.

2. Lifecycle events affecting Validation reliability shall be recorded.

Article 23

1. Changes affecting Validation and Verification Services shall be assessed before implementation.

2. The assessment shall consider:

(a) supported Trust Objects;

(b) supported Trust Services;

(c) Status dependencies;

(d) Profiles;

(e) Technical Specifications;

(f) Standards.

3. Material changes shall be managed according to applicable Change Control requirements.

RECORDS AND EVIDENCE

Article 24

1. The Validation and Verification Service shall maintain records sufficient to reconstruct:

(a) Verification requests;

(b) Validation requests;

(c) evidence evaluated;

(d) evaluation results;

(e) Status Responses;

(f) Historical State determinations;

(g) lifecycle events.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 25

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Trust Object Status;

(b) Trust Service Status;

(c) Qualified Status;

(d) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
ETSI EN 319 102-1	Validation process requirements for electronic signatures and seals
ETSI TS 119 102-2	Validation report structures where applicable
ETSI TS 119 615	Trust List use and interpretation
ETSI TS 119 612	Trusted List structures where applicable
RFC 5280	Certificate path validation
RFC 6960	Online Certificate Status Protocol where applicable
RFC 3161	Timestamp validation where timestamp tokens are used
RFC 5816	Timestamp certificate identification update
ISO/IEC 27001:2022	Information security management controls
ISO/IEC 27701:2025	Privacy management controls where personal data is processed

IDEHA-IG-SVC-FDX-001: FEDERATED DATA EXCHANGE SERVICE IMPLEMENTATION

SUBJECT MATTER AND SCOPE

Article 1

1. This Guideline lays down implementation requirements for Federated Data Exchange Services operating under the Trust Framework.

2. This Guideline applies to Trust Service Providers providing Federated Data Exchange Services and Actors operating exchange functions within the applicable Service Scope.

3. This Guideline establishes requirements for:

(a) Federated Data Exchange Service operation;

(b) Participant onboarding;

(c) Controlled Gateway operation;

(d) Endpoint registration and management;

(e) Technical Exchange Route operation;

(f) request and response exchange lifecycle;

(g) Exchange Evidence management;

(h) service continuity and lifecycle management.

4. This Guideline applies together with:

(a) IDEHA-IG-FED-DOM-001 Federation Domain and Cross-Domain Implementation;

(b) IDEHA-IG-ACT-PAR-001 Participation, Roles, Mandates and Representation Implementation;

(c) IDEHA-IG-SVC-AUT-001 Authentication Service Implementation;

(d) IDEHA-IG-SVC-AUZ-001 Authorisation Service Implementation;

(e) IDEHA-IG-SRC-ASO-001 Source and Authoritative Source Implementation;

(f) IDEHA-IG-DAT-SEM-001 Controlled Data Elements, Semantics and Data Quality Implementation;

(g) IDEHA-IG-SEC-CRY-001 Cryptographic Controls and Cryptographic Agility Implementation;

(h) IDEHA-IG-ASR-GEN-001 Assurance, Conformity Assessment and Qualification Implementation.

5. This Guideline does not establish:

(a) data-sharing agreements between Actors;

(b) Source authority;

(c) substantive disclosure decisions;

(d) Authorisation Policies;

(e) identity information;

(f) data semantics;

(g) payload business meaning;

(h) message schemas;

(i) protocol bindings;

(j) cryptographic algorithm parameters.

Those matters shall be implemented through the applicable Framework Instruments.

FEDERATED DATA EXCHANGE SERVICE SCOPE

Article 2

1. A Federated Data Exchange Service shall operate within an identified Service Scope.

2. The Service Scope shall identify:

(a) participating Actors;

(b) Federation Domains;

(c) Technical Exchange Routes;

(d) Endpoints;

(e) supported exchange functions;

(f) applicable Security Conditions;

(g) applicable Technical Specifications.

3. A Federated Data Exchange Service shall not perform exchanges outside its approved Service Scope.

Article 3

1. A Federated Data Exchange Service shall maintain separation between:

(a) exchange routing;

(b) system Authentication;

(c) Authorisation enforcement;

(d) payload handling;

(e) Exchange Evidence creation.

2. A Federated Data Exchange Service shall not:

(a) become the Source Holder;

(b) determine the substantive right to disclose data;

(c) determine the entitlement of a receiving Actor;

(d) modify the meaning of exchanged data.

3. The Federated Data Exchange Service shall transport and process exchange information only within the authorised scope.

EXCHANGE ARCHITECTURE

Article 4

1. A Federated Data Exchange Service shall consist of controlled exchange functions supporting communication between authorised Actors.

2. The exchange architecture shall identify, where applicable:

(a) Data Exchange Provider;

(b) Controlled Gateway;

(c) Participant Actor;

(d) Endpoint;

(e) Technical Exchange Route;

(f) Federation Domain dependencies.

3. The relationship between exchange components shall be maintained as operational evidence.

Article 5

1. A Controlled Gateway shall provide the controlled point through which exchange communication is performed.

2. A Controlled Gateway shall perform, where applicable:

(a) system Authentication;

(b) route resolution;

(c) exchange policy enforcement;

(d) request and response handling;

(e) Exchange Evidence generation.

3. A Controlled Gateway shall not perform substantive evaluation of the data being exchanged unless separately authorised under another Framework Instrument.

PARTICIPANT ONBOARDING

Article 6

1. A Federated Data Exchange Service shall establish procedures for onboarding participating Actors.

2. Onboarding shall verify, where applicable:

(a) Actor identity;

(b) Participation status;

(c) Federation Domain membership;

(d) Endpoint information;

(e) required Security Conditions;

(f) required Technical Specifications.

3. Onboarding evidence shall be maintained throughout the participation lifecycle.

Article 7

1. A participating Actor shall maintain information required for exchange operation.

2. The information shall identify, where applicable:

(a) Actor Identifier;

(b) Participant status;

(c) associated Controlled Gateways;

(d) permitted Endpoints;

(e) applicable exchange scope;

(f) lifecycle information.

3. Participation in the Federated Data Exchange Service shall not create Authorisation to access specific data.

ENDPOINT MANAGEMENT

Article 8

1. A Federated Data Exchange Service shall maintain Endpoint information necessary for exchange operation.

2. Endpoint information shall identify:

(a) Endpoint Identifier;

(b) responsible Actor;

(c) service function;

(d) Technical Exchange Route;

(e) operational Status;

(f) applicable Technical Specification.

3. Endpoint information shall remain separate from:

(a) Subject Identifier;

(b) Trust Object Identifier;

(c) Source Identifier.

Article 9

1. Endpoint activation shall require verification that:

(a) the Endpoint belongs to the identified Actor;

(b) required Authentication mechanisms are available;

(c) required Security Conditions are satisfied;

(d) applicable Technical Specifications are supported.

2. Endpoint changes affecting exchange reliability shall be managed through applicable Change Control requirements.

TECHNICAL EXCHANGE ROUTE

Article 10

1. A Technical Exchange Route shall define the controlled path through which exchange communication occurs.

2. A Technical Exchange Route shall identify, where applicable:

(a) originating Endpoint;

(b) receiving Endpoint;

(c) Controlled Gateways;

(d) Federation Domain;

(e) applicable Security Conditions;

(f) applicable Technical Specifications.

3. A Technical Exchange Route shall not define the substantive purpose or legal basis of data exchange.

EXCHANGE REQUEST PROCESSING

Article 11

1. A Federated Data Exchange Service shall process exchange requests according to the applicable Exchange Profile.

2. An exchange request shall identify, where applicable:

(a) requesting Actor;

(b) receiving Actor;

(c) requested Endpoint;

(d) Controlled Matter;

(e) Authorisation Outcome reference;

(f) interaction identifier;

(g) applicable Technical Specification.

3. The Federated Data Exchange Service shall verify that the request is within the permitted exchange scope.

Article 12

1. Before transmitting a request, the Federated Data Exchange Service shall verify:

(a) requesting Participant status;

(b) Endpoint availability;

(c) Technical Exchange Route availability;

(d) required Authentication conditions;

(e) required Authorisation conditions.

2. Verification of exchange conditions shall not replace substantive Authorisation decisions.

RESPONSE PROCESSING

Article 13

1. A Federated Data Exchange Service shall process responses according to the applicable Exchange Profile.

2. Response processing shall maintain:

(a) response integrity;

(b) response attribution;

(c) interaction correlation;

(d) delivery evidence.

3. The Federated Data Exchange Service shall not alter the substantive content of received responses.

AUTHENTICATION AND CONFIDENTIALITY

Article 14

1. A Federated Data Exchange Service shall use System Authentication mechanisms appropriate to the applicable Security Conditions.

2. System Authentication shall identify, where applicable:

(a) Controlled Gateway;

(b) Endpoint;

(c) participating system;

(d) communication peer.

3. System Authentication shall remain separate from:

(a) Subject Authentication;

(b) Authorisation;

(c) data disclosure permission.

Article 15

1. Exchange communication shall provide protection against:

(a) unauthorised disclosure;

(b) unauthorised modification;

(c) impersonation;

(d) replay.

2. The applicable Technical Specification shall define:

(a) transport protection;

(b) payload protection;

(c) message integrity protection;

(d) cryptographic mechanisms.

3. Payload protection requirements shall apply independently from transport protection where required by the applicable Profile.

AUTHORISATION ENFORCEMENT DEPENDENCY

Article 16

1. A Federated Data Exchange Service shall enforce applicable Authorisation Outcomes before permitting exchange.

2. The enforcement shall verify, where applicable:

(a) Outcome integrity;

(b) validity period;

(c) permitted Actor;

(d) permitted receiving Actor;

(e) permitted Controlled Matter;

(f) obligations and restrictions.

3. The Federated Data Exchange Service shall not create Authorisation Outcomes.

EXCHANGE EVIDENCE

Article 17

1. A Federated Data Exchange Service shall create Exchange Evidence for controlled exchanges.

2. Exchange Evidence shall identify, where applicable:

(a) Exchange Evidence Identifier;

(b) requesting Actor;

(c) receiving Actor;

(d) Controlled Gateways;

(e) interaction identifier;

(f) request and response references;

(g) relevant timestamps;

(h) Authentication evidence references;

(i) Authorisation Outcome reference;

(j) exchange result.

3. Exchange Evidence shall not contain exchanged payload data unless required by the applicable Profile.

Article 18

1. Exchange Evidence shall be protected against unauthorised alteration.

2. Protection may include:

(a) integrity mechanisms;

(b) Electronic Signature;

(c) Electronic Seal;

(d) Electronic Timestamp;

(e) other approved mechanisms.

3. The applicable Profile shall determine required protection conditions.

FAILURE HANDLING AND CONTINUITY

Article 19

1. A Federated Data Exchange Service shall maintain procedures for:

(a) failed exchanges;

(b) unavailable Endpoints;

(c) communication failures;

(d) Authentication failures;

(e) Authorisation failures;

(f) recovery.

2. Failure records shall identify:

(a) affected exchange;

(b) failure condition;

(c) responsible component;

(d) recovery action.

Article 20

1. A Federated Data Exchange Service shall maintain continuity arrangements.

2. Continuity arrangements shall address:

(a) Controlled Gateway availability;

(b) configuration recovery;

(c) Endpoint recovery;

(d) exchange evidence preservation;

(e) restoration procedures.

SERVICE LIFECYCLE MANAGEMENT

Article 21

1. The lifecycle of a Federated Data Exchange Service shall include, where applicable:

(a) preparation;

(b) activation;

(c) operation;

(d) modification;

(e) restriction;

(f) Suspension;

(g) cessation.

2. Lifecycle events affecting exchange reliability shall be recorded.

Article 22

1. Changes affecting a Federated Data Exchange Service shall be assessed before implementation.

2. The assessment shall consider:

(a) Federation Domains;

(b) Controlled Gateways;

(c) Endpoints;

(d) Technical Exchange Routes;

(e) Security Conditions;

(f) Technical Specifications.

3. Material changes shall be managed according to applicable Change Control requirements.

RECORDS AND EVIDENCE

Article 23

1. The Federated Data Exchange Service shall maintain records sufficient to reconstruct:

(a) participant onboarding;

(b) Endpoint lifecycle;

(c) exchange requests;

(d) exchange responses;

(e) Authentication dependencies;

(f) Authorisation dependencies;

(g) Exchange Evidence;

(h) incidents.

2. Records shall be protected according to applicable Security Conditions.

APPLICABLE STANDARDS

Article 24

1. The standards applicable to this Guideline are set out in Annex I.

2. A standard referenced in Annex I shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Authorisation;

(b) Source authority;

(c) Trust Service Status;

(d) Controlled Effects.

ANNEX I

Applicable standards

Reference	Application
RFC 8446	TLS 1.3 protected communication
RFC 5280	Certificate validation where certificate-based system authentication is used
RFC 9525	Service identity verification in TLS
RFC 9110	HTTP semantics where HTTP exchange is used
RFC 9113	HTTP/2 where HTTP/2 exchange is used
RFC 9530	HTTP message digest integrity
RFC 9421	HTTP message signatures where message-level integrity is required
OpenAPI Specification 3.2.0	Service interface description where applicable
ISO/IEC 27001:2022	Information security management controls
ISO/IEC 27002:2022	Security control implementation guidance

Reference	Application
ISO/IEC 27701:2025	Privacy management controls where personal data is processed
ISO 22301:2019	Business continuity management where continuity requirements apply
ETSI TS 119 612	Trusted List structures where Trust List dependencies apply
ETSI TS 119 615	Trusted List interpretation where Trust List dependencies apply

IDEHA-IG-SVC-FDX-001: FEDERATED DATA EXCHANGE SERVICE IMPLEMENTATION

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Guideline establishes implementation requirements for a Federated Data Exchange Service recognised under the Framework.

1.2. This Guideline shall apply to each Trust Service Provider, requesting Actor, responding Actor, Source Holder, Source Steward, Relying Actor, Technical Exchange Route Operator, Intermediary, Endpoint operator and supporting Actor implementing, operating, assessing, supervising or using a Federated Data Exchange Service.

1.3. This Guideline shall govern, where assigned within the Service Scope:

(a) Federated Data Exchange Service implementation and operational activation;

(b) Provider, participating-Actor, Endpoint, Technical Exchange Route Operator, Intermediary and supporting-Actor responsibilities;

(c) federation-policy and configuration distribution;

(d) Humanitarian Trust List based discovery and address resolution;

(e) exchange-request intake and admissibility;

(f) Endpoint Authentication, route resolution and destination resolution;

(g) Authorisation and Policy Enforcement;

(h) request, response, Trust Object and Trust Service Output exchange;

(i) payload signing or sealing before encryption;

(j) Transport Confidentiality and Payload Confidentiality;

(k) Integrity, Authenticity, correlation, replay, duplication, Status and error controls;

(l) Exchange Evidence and Controlled Exchange Results;

(m) dependencies, incidents, Continuity, Recovery, qualification and service lifecycle.

1.4. This Guideline shall not:

(a) redefine the Federated Data Exchange Service, Exchange Evidence or Controlled Exchange Results;

(b) create a separate gateway, messaging, routing, directory, delivery or policy-distribution Trust Service Category;

(c) assign access, disclosure permission, acceptance of content, a substantive decision, Source Status, Trust Service Status or Controlled Reliance;

(d) transfer governance, Decision Competence or Status Publication responsibility for the Humanitarian Trust List to the Trust Service Provider or a technical operator;

(e) require a Source or responding system to store its substantive records within a gateway, route component or shared federation platform;

(f) convert a request, response, payload, message, log or transport record into an Electronic Attestation or another Trust Object by implication;

(g) prescribe payload semantics, business-data models, exact schemas, encodings, algorithms, parameter values, interfaces, product configurations or test vectors.

1.5. Compliance with this Guideline shall not, by itself, establish Trust Service Status, Service Permission, Technical Exchange Permission, Qualified Status, Source Status, Authorisation, access, disclosure, acceptance, External Legal Status, External Legal Effect or Controlled Reliance.

Article 2: Allocation between Scheme, Profile and Technical Specification

2.1. The applicable Scheme shall identify:

(a) the governed purpose and operational context;

(b) the participating Actor categories and Federation Domains;

(c) the permitted request, response, Trust Object and Trust Service Output categories;

(d) the permitted Source and responding-system categories;

(e) the applicable purpose, access, disclosure and Reliance Conditions;

(f) the applicable safeguards, Review Routes and Remedy Routes.

2.2. The applicable Federated Data Exchange Service Profile shall identify:

(a) the Trust Service Provider and Service Scope;

(b) the participating Actor, Endpoint, Technical Exchange Route and Federation Domain categories;

(c) the permitted exchange patterns and interaction classes;

(d) the supported request, response, payload and evidence categories;

(e) the Endpoint Authentication and Authorisation requirements;

(f) the route-resolution and destination-resolution conditions;

(g) the Humanitarian Trust List and Discovery Metadata dependencies;

(h) the federation-policy and configuration-package requirements;

(i) the payload signing or sealing requirements;

(j) the Transport Confidentiality and Payload Confidentiality requirements;

(k) the correlation, replay, duplication, sequencing, Status and error controls;

(l) the Exchange Evidence and Controlled Exchange Result requirements;

(m) the delivery-state, failure-state, timeout and retry conditions;

(n) the availability, Continuity and Recovery conditions;

(o) the security, monitoring, incident, Retention and historical-reconstruction conditions;

(p) the conformity and qualified conditions, where applicable.

2.3. The applicable exchange Profile shall define each permitted interaction pattern, request purpose, requesting and responding Role, payload class, response class, exchange state, time condition, restriction and caveat.

2.4. The applicable Endpoint Profile shall define the Endpoint identity, responsible Actor, permitted service functions, Authentication conditions, Authorisation conditions, Technical Exchange Route bindings, certificate or key dependencies, Status conditions and lifecycle controls.

2.5. The applicable Technical Specification shall define:

(a) request and response schemas;

(b) exchange envelopes;

(c) payload-package structures;

(d) Endpoint and Technical Exchange Route identifiers;

(e) correlation values;

(f) Status codes and error structures;

(g) signature, seal and encryption containers;

(h) transport and protocol bindings;

(i) interface behaviour;

(j) cryptographic parameter selections;

(k) conformance tests.

Article 3: Implementation Plan

3.1. Before operational activation, the Trust Service Provider shall maintain an approved Implementation Plan for the Federated Data Exchange Service.

3.2. The Implementation Plan shall identify:

(a) the Service Scope and Service Permission;

(b) the participating Actors and Federation Domains;

(c) the gateway, Endpoint and Technical Exchange Route arrangements;

(d) the federation-policy and configuration-distribution arrangements;

(e) the Humanitarian Trust List and Discovery Metadata dependencies;

(f) the Endpoint Authentication arrangements;

(g) the Authorisation and Policy Enforcement arrangements;

(h) the payload signing or sealing arrangements;

(i) the payload-encryption arrangements;

(j) the Transport Confidentiality arrangements;

(k) the Exchange Evidence and trusted-time arrangements;

(l) the dependency, incident, Continuity, Recovery and cessation arrangements;

(m) the applicable Scheme, Profile and Technical Specification Versions;

(n) the applicable conformity and qualified conditions.

3.3. The Implementation Plan shall identify each Actor having access to plaintext payload information and the authorised purpose, scope and conditions of that access.

3.4. The Implementation Plan shall identify each technical component that processes routing Metadata, Discovery Metadata, certificates, policy packages, configuration packages, payload packages, Exchange Evidence or operational logs.

3.5. The Implementation Plan shall remain consistent with the approved Service Scope and shall be updated following each material change.

3.6. The Implementation Plan shall not create Service Permission, Technical Exchange Permission, access, disclosure, Qualified Status or another Controlled Effect.

SECTION 2: SERVICE IDENTITY, RESPONSIBILITY AND FEDERATION COORDINATION

Article 4: Service identity and Service Scope

4.1. Each Federated Data Exchange Service shall have an independently identifiable service record.

4.2. The service record shall identify:

(a) the Trust Service Provider;

(b) the Trust Service Identifier and Version;

(c) the Service Scope;

(d) the applicable Scheme and Profile Versions;

(e) the supported Federation Domains;

(f) the supported participating-Actor and Endpoint categories;

(g) the supported interaction, request, response and payload classes;

(h) the recognised Technical Exchange Routes and route dependencies;

(i) the Exchange Evidence and Controlled Exchange Result classes;

(j) the Service Status, Service Permission and Qualified Scope, where applicable;

(k) the security, Continuity, lifecycle and cessation conditions.

4.3. A shared platform, gateway, network, Endpoint, Technical Exchange Route, product name, operational team or infrastructure component shall not merge the Federated Data Exchange Service with another Trust Service.

4.4. Each materially distinct Service Scope shall remain separately identifiable where differences affect purpose, Federation Domain, Actor category, Endpoint class, exchange pattern, protection, output, Assurance, qualified condition or responsibility.

4.5. Technical availability, discovery, registration, onboarding or testing shall not create Service Permission or Technical Exchange Permission.

Article 5: Responsibilities and separation of functions

5.1. The Trust Service Provider shall remain responsible for the Federated Data Exchange Service within the recognised Service Scope.

5.2. The Trust Service Provider shall identify the Actor responsible for:

(a) service governance and Service Permission compliance;

(b) federation-policy and configuration-package distribution;

(c) Endpoint registration and lifecycle administration;

(d) Technical Exchange Route registration and operational control;

(e) Humanitarian Trust List discovery and destination resolution;

(f) security monitoring and incident handling;

(g) exchange-state and error management;

(h) Exchange Evidence and Controlled Exchange Result production;

(i) Continuity, Recovery and cessation;

(j) records, Review and Remedy support.

5.3. A Technical Exchange Route Operator, Intermediary, gateway operator, relay operator or supporting Actor shall perform only the functions expressly assigned by the applicable Profile and Authorisation Outcome.

5.4. Operation of an Endpoint, gateway, directory, route, queue, broker, relay, policy-distribution or monitoring component shall not assign the Role, Mandate, Status or Decision Competence of the requesting Actor, responding Actor, Source Holder, Source Steward, Framework Body or Relying Actor.

5.5. A responding Actor shall retain responsibility for Source access, response generation, disclosure conditions and substantive content.

5.6. The Trust Service Provider shall not become the Source Holder, Source Steward, Attestation Issuer, policy owner or substantive decision-maker merely because the service routes, correlates, logs, protects or evidences an interaction.

5.7. Outsourcing or shared operation shall preserve the responsibility, evidence, security and lifecycle requirements assigned to each Actor and Service Scope.

Article 6: Service Permission and operational activation

6.1. A Federated Data Exchange Service shall enter operational use only where the applicable Service Permission and each required Technical Exchange Permission are effective for the intended scope.

6.2. Before activation, the Trust Service Provider shall verify:

(a) service recognition and Service Scope;

(b) participating-Actor and Endpoint eligibility;

(c) Technical Exchange Route registration and Status;

(d) applicable Scheme, Profile and Technical Specification Versions;

(e) Endpoint Authentication controls;

(f) Authorisation and Policy Enforcement controls;

(g) federation-policy and configuration-package controls;

(h) Humanitarian Trust List discovery controls;

(i) payload signing or sealing controls;

(j) Payload Confidentiality controls;

(k) Transport Confidentiality controls;

(l) Exchange Evidence and trusted-time controls;

(m) incident, Continuity and Recovery arrangements;

(n) required conformity and qualified conditions.

6.3. Operational activation shall be recorded before the first controlled exchange within the activated scope.

6.4. A component shall not be treated as operationally activated solely because it is reachable, configured, tested or published through Discovery Metadata.

6.5. A material activation condition that cannot be established shall prevent operation within the affected scope.

Article 7: Federation policy and configuration distribution

7.1. The Federated Data Exchange Service shall maintain or use a central policy component for controlled distribution of federation-policy and configuration packages.

7.2. The central policy component shall distribute only packages authorised by the responsible Framework Body or Actor within its assigned competence.

7.3. A federation-policy or configuration package shall identify:

(a) the issuing Actor;

(b) the package identifier and Version;

(c) the applicable Federation Domain and scope;

(d) the applicable Actors, Endpoints or Technical Exchange Routes;

(e) the applicable policy, Profile and Technical Specification references;

(f) the Effective Date and expiry or review time;

(g) the predecessor package, where applicable;

(h) the applicable restrictions and transition conditions.

7.4. Each federation-policy and configuration package shall be protected by an Electronic Seal attributable to the issuing Actor before distribution.

7.5. Where approval by an identified natural person is required, the package shall contain or reference the applicable Electronic Signature evidence.

7.6. Where proof of existence at an identified time is required, the protected package shall receive an Electronic Timestamp.

7.7. Before use, the Trust Service Provider shall verify and validate:

(a) the package identifier and Version;

(b) the issuing Actor;

(c) the Electronic Seal or Electronic Signature;

(d) the applicable Certificate and Status information;

(e) the Effective Date and scope;

(f) the applicable predecessor and transition relationship.

7.8. A central policy component shall not:

(a) create an Authorisation Outcome;

(b) define a Source Scope;

(c) assign Status;

(d) create Technical Exchange Permission;

(e) replace a responding Actor's disclosure decision.

7.9. A locally cached policy or configuration package shall remain derivative, freshness-controlled and traceable to the authoritative package.

Article 8: Humanitarian Trust List discovery and address resolution

8.1. The Federated Data Exchange Service shall use the Humanitarian Trust List and authorised Discovery Metadata as the trusted source for federation discovery and address resolution.

8.2. The Humanitarian Trust List shall contain or reference, where authorised:

(a) Actor identifiers;

(b) Trust Service Provider identifiers;

(c) Trust Service identifiers;

(d) service certificates or other digital identity information;

(e) Endpoint references;

(f) Federation Domain relationships;

(g) supported Profiles and Technical Specifications;

(h) current and historical Status information;

(i) applicable restrictions and Validity Periods.

8.3. Before using Humanitarian Trust List information, the Federated Data Exchange Service shall verify and validate:

(a) the authenticity and Integrity of the publication;

(b) the Scheme Operator Certificate or other authorised publication identity;

(c) the publication Version and sequence information;

(d) the applicable Entry;

(e) the Entry Status and Effective Date;

(f) the Discovery Metadata scope;

(g) the applicable Endpoint reference;

(h) the applicable Federation Domain;

(i) the applicable Freshness Condition.

8.4. A cached or locally replicated Humanitarian Trust List record shall remain derivative, freshness-controlled and traceable to the authoritative publication.

8.5. Inclusion of an Actor, Trust Service, Endpoint or Technical Exchange Route reference in the Humanitarian Trust List shall not create:

(a) Authorisation;

(b) access;

(c) disclosure permission;

(d) Technical Exchange Permission;

(e) Controlled Reliance.

8.6. The Trust Service Provider shall not operate, control, assign or alter Status through the Humanitarian Trust List.

8.7. A technical operator shall not acquire Decision Competence by hosting, caching, distributing or processing Humanitarian Trust List information.

SECTION 3: CONTROLLED EXCHANGE OPERATION AND PAYLOAD PROTECTION

Article 9: Exchange-request intake and admissibility

9.1. Each exchange request shall be independently identifiable and attributable to the requesting Actor and originating Endpoint.

9.2. The request shall contain or reference:

(a) the requesting Actor and originating Endpoint;

(b) the intended responding Actor or receiving Endpoint;

(c) the recognised purpose;

(d) the requested action;

(e) the requested Controlled Matter or payload class;

(f) the applicable Scheme, Profile and Technical Specification Versions;

(g) the Controlled Interaction identifier;

(h) the Authorisation Outcome reference, where required;

(i) the applicable policy and configuration-package references;

(j) the applicable restrictions, caveats and correlation information.

9.3. Before admitting the request, the Federated Data Exchange Service shall verify:

(a) the identity and current Status of the requesting Actor and originating Endpoint;

(b) the applicable Service Permission and Technical Exchange Permission;

(c) the current Technical Exchange Route and destination;

(d) the applicable Authorisation Outcome;

(e) the applicable policy and configuration package;

(f) the required payload-protection conditions;

(g) the applicable time and Freshness Conditions.

9.4. Request admission shall not create a right to receive a response or require disclosure by the responding Actor.

9.5. The service shall reject, restrict or hold a request where an applicable identity, Status, permission, Technical Exchange Route, security, freshness or policy condition cannot be established.

9.6. A held or rejected request shall receive the Status or error treatment assigned by the applicable Profile without unnecessary disclosure of Protection-Sensitive Information or Security-Sensitive Information.

Article 10: Endpoint Authentication and route resolution

10.1. Each participating Endpoint shall be uniquely identifiable within the applicable Federation Domain and Service Scope.

10.2. The Federated Data Exchange Service shall authenticate each participating Endpoint at the level and frequency assigned by the applicable Profile.

10.3. Endpoint Authentication shall establish the Endpoint identity and current Authentication Outcome but shall not, by itself, establish Authorisation, disclosure permission, Source Status or Controlled Reliance.

10.4. Certificate-based Endpoint Authentication shall use the certificate and validation arrangements assigned by the applicable Endpoint Profile and Technical Specification.

10.5. Route and destination resolution shall use authenticated Humanitarian Trust List information, authorised Discovery Metadata and current federation-policy and configuration packages.

10.6. The service shall detect and prevent:

(a) unauthorised route substitution;

(b) destination substitution;

(c) certificate substitution;

(d) Endpoint redirection;

(e) downgrade to an unauthorised protocol or protection arrangement.

10.7. A route-resolution result shall not create Technical Exchange Permission or require the responding Actor to disclose information.

10.8. Where an authorised current destination cannot be established, the service shall terminate or hold the interaction according to the applicable Profile.

Article 11: Authorisation, disclosure and Policy Enforcement

11.1. An Authorisation Service or local Policy Enforcement Function shall determine and enforce the applicable exchange permission where required by the Scheme or Profile.

11.2. An Authorisation decision shall remain separate from:

(a) Endpoint Authentication;

(b) Humanitarian Trust List discovery;

(c) route and destination resolution;

(d) technical availability;

(e) Source access;

(f) response generation;

(g) payload protection;

(h) content acceptance;

(i) Controlled Reliance.

11.3. The requesting Actor shall provide or reference the purpose, requested action, target, scope and context required for Authorisation evaluation.

11.4. The responding Actor shall enforce its own access and Disclosure Conditions before releasing a response or payload.

11.5. The Federated Data Exchange Service shall enforce the applicable Authorisation Outcome only within the identified interaction, purpose, Actor, Endpoint, payload class, Technical Exchange Route and Validity Period.

11.6. A previous Authorisation Outcome shall not be reused where the interaction, purpose, Actor, Endpoint, recipient, payload class, Technical Exchange Route, Status or time condition has materially changed.

11.7. The service shall not invent, extend or reinterpret an Authorisation Policy or Authorisation Outcome.

11.8. A successful exchange shall not establish that the exchange was lawful, necessary, accurate or acceptable beyond the conditions evidenced for that interaction.

Article 12: Request, response and Source separation

12.1. A responding Actor shall generate a response only after applying the applicable Source access, purpose, disclosure, data-minimisation, Freshness and Authorisation conditions.

12.2. A Source shall remain under the control of its Source Holder and Source Steward and shall not be required to reside within the Federated Data Exchange Service, gateway or Technical Exchange Route.

12.3. The service shall transport or mediate only the request, response, Trust Object, Trust Service Output or evidence assigned by the applicable exchange Profile.

12.4. A request shall not become an Electronic Attestation merely because it contains statements, identifiers, Attributes or supporting information.

12.5. A response shall not become an Electronic Attestation merely because it contains a statement or originates from a recognised Actor.

12.6. Where a response constitutes or contains an Electronic Attestation, that Electronic Attestation shall remain a separate Trust Object governed by its applicable Framework Instruments.

12.7. The service shall preserve the separation between:

(a) the request and its requester;

(b) the Source and responding Actor;

(c) the response and its substantive Issuer or producer;

(d) the exchanged payload and Exchange Evidence;

(e) the exchanged payload and Controlled Exchange Result.

12.8. Transformation, aggregation or derivation performed during exchange shall be expressly authorised, attributable and governed by the applicable Profile and shall not transfer Source Status to the resulting output.

Article 13: Payload-package protection

13.1. Each payload shall be placed within a payload package before transmission through a Technical Exchange Route.

13.2. The payload package shall contain or reference:

(a) the sending Actor;

(b) the intended receiving Actor;

(c) the originating and receiving Endpoints;

(d) the Controlled Interaction identifier;

(e) the recognised purpose;

(f) the applicable Profile and Technical Specification Versions;

(g) the payload identifier and payload digest;

(h) the applicable Authorisation Outcome reference;

(i) the creation time;

(j) the applicable restrictions and caveats.

13.3. Before Payload Confidentiality is applied, the sending Actor shall protect the plaintext payload package:

(a) by an Electronic Seal attributable to the sending Actor; or

(b) by an Electronic Signature where the payload package is attributable to a Signatory under the applicable Profile.

13.4. An existing Electronic Signature, Electronic Seal, Electronic Timestamp, Certificate or other object-level protection applied to a Trust Object or Trust Service Output contained in the payload package shall remain intact.

13.5. The sending Actor shall apply Payload Confidentiality to the signed or sealed payload package before that package enters the Technical Exchange Route.

13.6. Payload Confidentiality shall ensure that plaintext access is limited to:

(a) the authorised sending Actor;

(b) the authorised receiving Actor;

(c) each additional processing Actor expressly identified by the applicable Profile and Authorisation Outcome.

13.7. A Trust Service Provider, Technical Exchange Route Operator, Intermediary, gateway operator, relay operator, policy component or monitoring component shall not access the plaintext payload unless separately authorised as a processing Actor for the recognised purpose.

13.8. Decryption material shall not be disclosed to an unrelated Technical Exchange Route, Intermediary, support or monitoring component.

13.9. The receiving Actor shall:

(a) decrypt the payload package;

(b) verify and validate the Electronic Seal or Electronic Signature applied by the sending Actor;

(c) verify the payload digest and package Metadata;

(d) verify the applicable Certificate and Status information;

(e) reject or isolate the payload where the required protection cannot be established.

13.10. An Electronic Seal, Electronic Signature or encryption mechanism shall not, by itself, authorise collection, processing, exchange, disclosure, onward transfer or Retention.

Article 14: Transport protection, correlation and error handling

14.1. Each Technical Exchange Route shall use HTTPS over TLS 1.3 in accordance with Annex I and the applicable Technical Specification.

14.2. Plain HTTP shall not be used for a Controlled Interaction.

14.3. Transport protection shall provide:

(a) Transport Confidentiality;

(b) transport Integrity;

(c) mutual system Authentication;

(d) protection against unauthorised interception and redirection.

14.4. Transport protection shall remain separate from and shall not replace:

(a) the Electronic Seal or Electronic Signature applied to the payload package;

(b) Payload Confidentiality;

(c) object-level protection;

(d) Exchange Evidence protection.

14.5. Where the applicable Technical Specification uses HTTP message protection, the exchange envelope shall contain:

(a) a content digest;

(b) a signature over the selected request or response components;

(c) the applicable signature-creation time and validity information;

(d) the applicable certificate or key reference.

14.6. Each Controlled Interaction shall have an identifier sufficient to correlate its request, response, Status, evidence, retry and error states.

14.7. The service shall implement controls against:

(a) replay;

(b) unintended duplicate processing;

(c) incorrect sequencing;

(d) correlation collision;

(e) response substitution;

(f) route downgrade.

14.8. A retry shall preserve the relationship with the original interaction and shall not conceal whether an earlier request was processed, refused, failed or remained unresolved.

14.9. Duplicate detection shall not, by itself, determine that a substantive request or response is fraudulent, invalid or unacceptable.

14.10. The service shall assign each interaction the processing, transmission, receipt, refusal, timeout, failure or unable-to-determine state required by the applicable Profile.

14.11. Error information shall be sufficient for authorised diagnosis and Remedy without exposing unnecessary Source content, Protection-Sensitive Information or Security-Sensitive Information.

14.12. A technical success state shall not establish substantive acceptance, delivery of a substantive benefit, completion of a business process or Controlled Reliance.

14.13. An unresolved or ambiguous interaction state shall not be represented as successful delivery or substantive completion.

SECTION 4: SERVICE OUTPUTS, FEDERATION AND OPERATIONAL RESILIENCE

Article 15: Exchange Evidence, operational logs and trusted time

15.1. The Federated Data Exchange Service shall create Exchange Evidence for each Controlled Interaction.

15.2. Exchange Evidence shall contain or reference:

(a) the producing Federated Data Exchange Service;

(b) the requesting and responding Actors and Endpoints;

(c) the Controlled Interaction identifier;

(d) the request, response and payload-package references without unnecessary disclosure of content;

(e) the payload digest;

(f) the sending Actor's Electronic Seal or Electronic Signature reference;

(g) the payload-encryption reference;

(h) the relevant times;

(i) the Technical Exchange Route and security context;

(j) the applicable policy and configuration-package Versions;

(k) the Authentication and Authorisation references;

(l) the processing, transmission, receipt, refusal or failure state;

(m) the applicable restrictions and caveats.

15.3. Exchange Evidence shall remain separate from the exchanged payload and from each Trust Object or Trust Service Output carried through the interaction.

15.4. Exchange Evidence shall be protected by:

(a) an Electronic Seal attributable to the producing Federated Data Exchange Service; and

(b) an Electronic Timestamp establishing the protected evidence state at an identified time.

15.5. The applicable Profile shall identify where a Qualified Electronic Seal, Qualified Electronic Timestamp or another qualified dependency is required.

15.6. Operational logs shall:

(a) use trusted and synchronised time;

(b) record attributable security-relevant events;

(c) be protected against unauthorised alteration and deletion;

(d) preserve event ordering and correlation;

(e) exclude plaintext payload content unless expressly authorised.

15.7. Integrity-protected operational-log batches or evidence roots shall be periodically sealed and timestamped at the frequency assigned by the applicable Profile.

15.8. Exchange Evidence and operational-log evidence shall remain available for the Retention period assigned by the applicable Profile and shall support Historical State reconstruction.

15.9. Exchange Evidence shall not, by itself, create access, disclosure permission, acceptance of content, delivery of a substantive benefit, a local business decision or Controlled Reliance.

15.10. Delivery evidence shall remain a subordinate Exchange Evidence function and shall not constitute a separate Trust Service Category.

Article 16: Controlled Exchange Results

16.1. The Federated Data Exchange Service shall create a Controlled Exchange Result where the applicable Profile requires a separately identifiable result of the interaction.

16.2. A Controlled Exchange Result shall contain or reference:

(a) the producing Federated Data Exchange Service;

(b) the requesting and responding Actors or Endpoints;

(c) the Controlled Interaction identifier;

(d) the relevant request, response or payload-package reference;

(e) the Technical Exchange Route and security context;

(f) the result or delivery state;

(g) the evaluation time and Validity Period;

(h) the applicable restrictions and caveats.

16.3. A Controlled Exchange Result shall remain separate from Exchange Evidence, exchanged content and any local acceptance or business decision.

16.4. A Controlled Exchange Result shall not, by itself, create access, disclosure permission, acceptance of content, delivery of a substantive benefit or Controlled Reliance.

16.5. A Controlled Exchange Result shall be interpreted only against the interaction, evaluation time, Profile Version, Technical Exchange Route, evidence, restrictions and Validity Period identified for that Result.

16.6. Where a Controlled Exchange Result is issued as an Electronic Attestation, that Electronic Attestation shall remain a separate Trust Object governed by the applicable Attestation Profile.

16.7. Qualified Status shall apply to an individual Controlled Exchange Result only through the applicable object-instance qualification conditions.

Article 17: Cross-domain exchange and dependencies

17.1. Cross-domain exchange shall preserve:

(a) the identity and responsibility of each participating Actor and Endpoint;

(b) the Decision Competence of each Framework Body;

(c) the applicable Federation Agreement and Federation Trust Relationship;

(d) the Source, Trust Service, Technical Exchange Route, output and Status boundaries;

(e) the applicable policy, protection, evidence, Review and Remedy conditions.

17.2. Recognition, listing or discovery in one Federation Domain shall not transfer Service Permission, Technical Exchange Permission, Source Status, Qualified Status or Controlled Reliance to another Federation Domain.

17.3. A parent Federation Domain reference to a nested-domain publication shall not make the parent publication the authoritative source of the nested-domain Status.

17.4. The Trust Service Provider shall identify each material dependency of the Federated Data Exchange Service.

17.5. Dependencies shall include, where applicable:

(a) Identification and Authentication Services;

(b) Authorisation Services and Policy Enforcement Functions;

(c) Validation and Verification Services;

(d) Humanitarian Trust List and Discovery Metadata publications;

(e) central policy and configuration-distribution components;

(f) Sources and responding systems;

(g) Endpoints and Technical Exchange Routes;

(h) certificates, keys, protection mechanisms and devices;

(i) Electronic Signature, Electronic Seal and Electronic Timestamp Services;

(j) time, monitoring, logging, queueing and Recovery services;

(k) shared infrastructure and outsourced functions.

17.6. Each dependency record shall identify the responsible Actor, function, scope, Status, interface, failure mode, Continuity arrangement and evidence reference.

17.7. Shared infrastructure shall not merge the Federated Data Exchange Service with another Trust Service or transfer responsibility between Providers.

17.8. Failure, restriction, Suspension or Withdrawal of a dependency shall affect the service only within the identified dependent scope.

17.9. The service shall not continue an interaction where a required dependency cannot satisfy the applicable security, Status, Authorisation, protection or qualified condition.

17.10. Dependency substitution shall undergo Change Control and the assessment required by the applicable Profile before operational use.

Article 18: Security incidents, Continuity and Recovery

18.1. The Trust Service Provider shall monitor the Federated Data Exchange Service for:

(a) unauthorised access or disclosure;

(b) interception or alteration;

(c) replay or duplication;

(d) misrouting or destination substitution;

(e) Endpoint or gateway compromise;

(f) policy-package or configuration-package compromise;

(g) Humanitarian Trust List substitution or stale-data use;

(h) certificate, key or cryptographic compromise;

(i) Exchange Evidence or operational-log corruption;

(j) dependency failure;

(k) other Security Incidents.

18.2. Incident assessment shall identify:

(a) the affected Service Scope;

(b) the affected Actors, Endpoints, Technical Exchange Routes, interactions, payload classes, outputs and dependencies;

(c) whether plaintext or protected content was exposed;

(d) whether a policy, configuration or discovery package was affected;

(e) the affected Confidentiality, Integrity, Authenticity, availability, Status or qualified condition;

(f) the required containment, notification, Status, Review and Remedy actions.

18.3. Incident effects shall propagate only through identified dependencies and within the evidenced affected scope.

18.4. An Endpoint, gateway, Technical Exchange Route or policy-component incident shall not automatically suspend the entire Trust Service Provider or each unrelated Trust Service.

18.5. The Trust Service Provider shall maintain a Continuity Plan covering:

(a) alternative Endpoints and Technical Exchange Routes;

(b) policy and configuration recovery;

(c) Humanitarian Trust List and Discovery Metadata availability;

(d) queueing, retry and timeout controls;

(e) payload and evidence protection during interruption;

(f) Degraded Operation conditions;

(g) unresolved-interaction reconciliation;

(h) Recovery testing and return-to-service conditions.

18.6. Degraded Operation shall not bypass:

(a) Endpoint Authentication;

(b) Authorisation and disclosure conditions;

(c) policy and configuration validation;

(d) payload signing or sealing;

(e) Payload Confidentiality;

(f) Transport Confidentiality;

(g) Exchange Evidence and trusted-time requirements;

(h) Status or qualified-dependency conditions.

18.7. The service shall not represent an interaction as completed where processing, delivery or response state remains unresolved.

18.8. Recovery of technical operation shall not automatically reinstate Service Permission, Technical Exchange Permission, dependency Status or Qualified Status.

18.9. The Trust Service Provider shall complete the required Verification, assessment and approval before returning the affected scope to normal operation.

SECTION 5: ASSURANCE, LIFECYCLE AND STANDARDS

Article 19: Assurance, Conformity Assessment and qualification

19.1. The Federated Data Exchange Service shall be subject to the Assurance and Conformity Assessment requirements assigned by the applicable Framework Instruments and Profile.

19.2. The evidence package shall demonstrate, within the assessed scope:

(a) service identity, Service Scope and Service Permission;

(b) Provider, participating-Actor, Endpoint, Technical Exchange Route Operator and supporting-Actor responsibility;

(c) federation-policy and configuration-package controls;

(d) Humanitarian Trust List discovery and address-resolution controls;

(e) request admissibility and interaction classification;

(f) Endpoint Authentication and route-resolution controls;

(g) Authorisation, disclosure and Policy Enforcement controls;

(h) Source, request, response and payload separation;

(i) payload signing or sealing before encryption;

(j) Transport Confidentiality and Payload Confidentiality;

(k) Integrity, Authenticity, correlation, replay, duplication, Status and error controls;

(l) Exchange Evidence, operational-log and trusted-time controls;

(m) Controlled Exchange Result production;

(n) dependency, incident, Continuity and lifecycle controls.

19.3. Qualified Federated Data Exchange Service Status shall require the applicable decision-based qualification route and each required qualified dependency.

19.4. Qualified Trust Service Provider Status shall not, by itself, qualify the Federated Data Exchange Service.

19.5. Qualified Federated Data Exchange Service Status shall not transfer to:

(a) Exchange Evidence;

(b) a Controlled Exchange Result;

(c) a requesting Actor, responding Actor, Endpoint, Technical Exchange Route Operator or Intermediary;

(d) a Source, Trust Object, Trust Service Output or payload;

(e) a Technical Exchange Route, Certificate, key, mechanism or device;

(f) another Trust Service, output or component.

19.6. Each individual Exchange Evidence object or Controlled Exchange Result shall receive Qualified Status only through the applicable object-instance qualification conditions.

19.7. Framework qualification shall not, by itself, assign External Legal Status or External Legal Effect.

19.8. A material unresolved non-conformity shall prevent operation within the affected scope until the applicable corrective, restriction, Suspension or reassessment condition has been satisfied.

Article 20: Service lifecycle, change, transition and cessation

20.1. The Federated Data Exchange Service lifecycle shall include proposal, assessment, recognition, activation, operation, surveillance, restriction, Suspension, Correction, change, transition, Withdrawal, cessation and archival treatment.

20.2. The Trust Service Provider shall apply Change Control to each material change affecting:

(a) the Service Scope or Service Permission;

(b) a participating Actor, Endpoint, Technical Exchange Route, Federation Domain or interaction class;

(c) a request, response, payload or output class;

(d) the federation-policy or configuration-distribution model;

(e) the Humanitarian Trust List discovery or address-resolution model;

(f) the Authentication, Authorisation, disclosure or Policy Enforcement model;

(g) the payload signing, sealing or encryption model;

(h) the Transport Confidentiality model;

(i) the correlation, replay, duplication, Status or error model;

(j) an Exchange Evidence, operational-log or Controlled Exchange Result arrangement;

(k) a Source, Trust Service, protection or infrastructure dependency;

(l) the incident, Continuity or Recovery arrangement;

(m) the Qualified Scope or assessed conformity basis.

20.3. A material change shall undergo the assessment, testing, approval and publication required by the applicable Framework Instrument before operational use.

20.4. A transition between service Versions shall preserve:

(a) Controlled Interaction identifiers;

(b) request and response state;

(c) Authentication and Authorisation evidence;

(d) policy and configuration-package references;

(e) Humanitarian Trust List and Discovery Metadata references;

(f) Technical Exchange Route and Endpoint references;

(g) payload-package and protection references;

(h) Exchange Evidence and Controlled Exchange Results;

(i) Status and dependency references;

(j) Historical State.

20.5. Restriction, Suspension, Withdrawal or cessation of the Federated Data Exchange Service shall not automatically invalidate Exchange Evidence or Controlled Exchange Results created before the Effective Date of that action.

20.6. Earlier outputs shall remain subject to their own Validation basis, Status, dependencies, lifecycle and Historical State.

20.7. Before cessation, the Trust Service Provider shall implement an approved cessation plan covering:

(a) pending, queued and unresolved interactions;

(b) requesting and responding Actor, Endpoint and Technical Exchange Route dependencies;

(c) federation-policy and configuration-package continuity;

(d) Humanitarian Trust List and discovery dependencies;

(e) request, response, output and evidence delivery;

(f) unresolved-state reconciliation;

(g) continuing Validation and Status support;

(h) record Retention, preservation and transfer;

(i) dependency termination;

(j) affected participating-Actor and Relying Actor notification;

(k) incident, Review and Remedy continuity;

(l) final Service Status and publication actions.

20.8. Cessation of technical operation shall not remove continuing security, Confidentiality, Retention, Validation, Status, Review, Remedy or historical-reconstruction obligations.

20.9. Cessation shall not transfer Source responsibility, Authorisation responsibility, Humanitarian Trust List responsibility or Controlled Reliance responsibility to the Trust Service Provider or a successor service.

Article 21: Reference standards and specifications

21.1. The reference standards and specifications applicable to the implementation of this Guideline are set out in Annex I.

21.2. A reference identified in Annex I shall apply only within the implementation function, scope and condition identified in that Annex.

21.3. Exact algorithms, parameter sets, Certificate Profiles, signature and seal formats, timestamp profiles, payload schemas, protocol bindings and test conditions shall be selected through the applicable Profile and Technical Specification.

21.4. Standards governed principally by the following Framework Instruments shall apply through those instruments and shall not be repeated in Annex I:

(a) Electronic Signature and Electronic Seal standards;

(b) Electronic Timestamp standards;

(c) Certificate issuance and Validation standards;

(d) Humanitarian Trust List publication standards;

(e) cryptographic algorithm and post-quantum transition standards;

(f) general Trust Service Provider, security and Continuity standards.

21.5. Conformity with a reference standard or specification shall constitute evidence only for the requirements and scope mapped to that reference.

21.6. Conformity with a reference standard or specification shall not, by itself, create Service Permission, Technical Exchange Permission, Qualified Status, Authorisation, access, disclosure, acceptance or Controlled Reliance.

ANNEX I: REFERENCE STANDARDS AND SPECIFICATIONS

Reference	Implementation function	Applicability and controlled treatment
RFC 9846, The Transport Layer Security Protocol Version 1.3, 2026	Transport Confidentiality and mutually authenticated protected communication	Mandatory for Technical Exchange Routes. RFC 8446 is superseded for new implementations. The applicable Technical Specification shall define the permitted TLS configuration and shall prohibit unauthorised downgrade.
RFC 9110, HTTP Semantics, 2022	HTTP request and response semantics	Mandatory where HTTP-based exchange is selected. Only the https URI scheme shall be used for Controlled Interactions.
RFC 9525, Service Identity in TLS, 2023	Verification of system, service and Endpoint identity	Mandatory where service identity is represented through X.509 Certificates in TLS.
RFC 9530, Digest Fields, 2024	Integrity digests for HTTP content and representations	Mandatory for HTTP-based exchange envelopes carrying a payload or payload reference.
RFC 9421, HTTP Message Signatures, 2024	Protection of selected HTTP request and response components	Mandatory where the applicable Technical Specification uses HTTP-based exchange. It shall protect exchange-envelope and routing Metadata and shall not replace the Electronic Seal or Electronic Signature applied to the payload package.

Reference	Implementation function	Applicability and controlled treatment
RFC 7516, JSON Web Encryption, 2015	Payload Confidentiality for JSON-based payload packages	Conditionally mandatory where the applicable Technical Specification selects a JSON-based encrypted payload package.
RFC 5652, Cryptographic Message Syntax, as updated by RFC 8933 and RFC 9629	Payload Confidentiality for binary, document and format-neutral payload packages	Conditionally mandatory where the applicable Technical Specification selects CMS EnvelopedData. Cryptographic mechanisms and migration conditions shall be selected through the Cryptographic Controls and Cryptographic Agility instruments.
RFC 9052, CBOR Object Signing and Encryption: Structures and Process, 2022	Payload protection for CBOR-based payload packages	Conditionally mandatory where the applicable Technical Specification selects a CBOR-based payload package.
RFC 9053, CBOR Object Signing and Encryption: Initial Algorithms, 2022	Algorithm identifiers used with COSE	Applicable only together with the cryptographic mechanisms selected through the Cryptographic Controls and Cryptographic Agility instruments.
RFC 9457, Problem Details for HTTP APIs, 2023	Common technical error representation	Mandatory for HTTP-based error responses unless the applicable Technical Specification establishes a stricter compatible profile. Error responses shall not disclose unnecessary Protection-Sensitive Information or Security-Sensitive Information.
RFC 9562, Universally Unique IDentifiers, 2024	Controlled Interaction, request, response and evidence identifiers	Mandatory where UUIDs are selected by the applicable Technical Specification. An interaction identifier shall not serve as a Subject Identifier, Identification Number, Trust Service Identifier or access credential.

IDEHA-IG-ASR-QLF-001: ASSURANCE AND QUALIFICATION IMPLEMENTATION

Version: 0.1

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Guideline lays down implementation requirements for Assurance evaluation, Conformity Assessment and the preparation, maintenance and lifecycle support of qualification under the Framework.

1.2. This Guideline shall apply to each Framework Body, Conformity Assessment Body, Responsible Actor, applicant for qualification, Trust Service Provider, Source Holder, Source Steward, Issuer and supporting Actor involved in an Assurance evaluation, Conformity Assessment or qualification process.

1.3. This Guideline shall govern, where applicable:

(a) implementation planning;

(b) requirement and evidence mapping;

(c) Assurance evaluation;

(d) Conformity Assessment preparation and conduct;

(e) competence, independence and conflict controls;

(f) findings, non-conformities and corrective action;

(g) Conformity Assessment Results;

(h) qualification evidence packages;

(i) Object-Instance Qualification implementation;

(j) qualified dependencies and composite arrangements;

(k) Status Publication handoff;

(l) surveillance, reassessment and material-change treatment;

(m) lifecycle-action and reinstatement evidence;

(n) Historical State reconstruction.

1.4. This Guideline shall not:

(a) establish an Assurance Domain or Assurance Level;

(b) establish an eligible qualified category;

(c) establish or modify a qualification route;

(d) assign Decision Competence;

(e) assign recognition, Service Permission, Technical Exchange Permission or Qualified Status;

(f) create a Trust Service Category, Trust Object Category, Source category or Controlled Effect;

(g) treat an Assurance outcome or Conformity Assessment Result as a qualification decision;

(h) prescribe technical thresholds, scoring formulae, algorithms, parameter values, test vectors, schemas, interfaces or product configurations assigned to a Profile or Technical Specification;

(i) extend Qualified Status from one Status-Bearing Matter, Qualified Scope, Version, configuration, dependency or period to another.

1.5. Compliance with this Guideline shall not, by itself, establish an Assurance Level, positive Conformity Assessment Result, qualification decision, Qualified Status, recognition, operational activation, External Legal Status, External Legal Effect or permission for Controlled Reliance.

Article 2: Implementation Plan and responsibilities

2.1. Before an Assurance evaluation or Conformity Assessment begins, the Responsible Actor shall maintain an approved Implementation Plan.

2.2. Before an application for Decision-Based Qualification is submitted, the applicant shall ensure that the Implementation Plan covers the qualification process and the intended Qualified Scope.

2.3. The Implementation Plan shall identify:

(a) the Assurance Object or assessment subject;

(b) the intended assessment or qualification purpose;

(c) the applicable Profile and Version;

(d) the proposed scope;

(e) the applicable Framework requirements;

(f) the applicable Recognised Standards and Technical Specifications;

(g) the Responsible Actors;

(h) the Conformity Assessment Body, where applicable;

(i) the required evidence;

(j) the evaluation and assessment methods;

(k) the material dependencies;

(l) the expected schedule and decision gates;

(m) the surveillance and reassessment arrangements;

(n) the change, lifecycle and historical-evidence arrangements.

2.4. Where several Controlled Matters are evaluated together, the Implementation Plan shall identify each Controlled Matter and its scope separately.

2.5. A shared Provider, system, location, component, assessment activity or evidence source shall not merge the identity, scope, outcome or Qualified Status of separate Controlled Matters.

2.6. The Responsible Actor shall update the Implementation Plan where a material change affects the planned scope, requirements, evidence, methods, dependencies, schedule or intended qualification outcome.

2.7. An Implementation Plan shall not create an Assurance outcome, Conformity Assessment Result or Qualified Status.

Article 3: Requirement and evidence mapping

3.1. The Responsible Actor shall maintain a requirement and evidence map for each Assurance evaluation, Conformity Assessment and application for qualification.

3.2. The requirement and evidence map shall identify:

(a) each applicable requirement;

(b) the Framework Instrument and Version establishing the requirement;

(c) the Controlled Matter and scope to which the requirement applies;

(d) the evidence required to evaluate the requirement;

(e) the Actor responsible for producing or maintaining that evidence;

(f) the evidence source and Version;

(g) the applicable Freshness Condition;

(h) the evaluation or assessment method;

(i) the resulting finding or conclusion;

(j) each limitation, caveat or unresolved matter.

3.3. A reference to a Recognised Standard shall identify the exact edition, selected provisions, applicable scope and each approved adaptation or exclusion.

3.4. Evidence supporting one requirement or Controlled Matter shall not be treated as evidence of another requirement or Controlled Matter unless the requirement and evidence map expressly establishes that relationship.

3.5. Evidence derived from another record, assessment or result shall identify:

(a) the originating evidence;

(b) the derivation method;

(c) the responsible Actor;

(d) the derivation time;

(e) the applicable Version;

(f) each limitation introduced by the derivation.

3.6. A missing, stale, conflicting, inaccessible or unreliable item of evidence shall be recorded and reflected in the applicable evaluation, finding, conclusion or decision package.

3.7. An unresolved evidence gap shall not be represented as a satisfied requirement.

SECTION 2: ASSURANCE IMPLEMENTATION

Article 4: Assurance evaluation planning

4.1. Before an Assurance evaluation begins, the Responsible Actor shall prepare an evaluation plan.

4.2. The evaluation plan shall identify:

(a) the Assurance Object;

(b) each applicable Assurance Domain;

(c) the applicable Assurance Conditions;

(d) the Assurance Level or outcome class selected by the applicable Profile;

(e) the evidence requirements;

(f) the evaluation methods;

(g) the material dependencies;

(h) the evaluation time and Validity Period;

(i) the competence and independence requirements applicable to the evaluator;

(j) the treatment of uncertainty, conflicting evidence and unavailable dependencies;

(k) the human-review conditions, where applicable.

4.3. Assurance evaluation shall be performed separately for each applicable Assurance Domain.

4.4. Assignment of the same Assurance Level in different Assurance Domains shall not establish equivalence between those Domains.

4.5. A composite Assurance evaluation shall apply only the combination method established by the applicable Profile.

4.6. A qualified dependency shall be evaluated as a condition and shall not transfer Qualified Status or an Assurance Level to the Assurance Object.

4.7. The evaluation plan shall identify each condition requiring re-evaluation following a material change.

Article 5: Assurance evidence and evaluation conduct

5.1. Assurance evidence shall be attributable, relevant, sufficiently current, protected and traceable to the Assurance Object and Assurance Condition for which it is used.

5.2. The evaluator shall verify, where applicable:

(a) the evidence identity and source;

(b) the Actor responsible for the evidence;

(c) the evidence Version;

(d) the evidence creation and evaluation times;

(e) the evidence Integrity and Authenticity;

(f) the applicable Freshness Condition;

(g) the relationship between the evidence and the Assurance Object;

(h) each restriction or limitation.

5.3. Evaluation methods shall be appropriate to the Assurance Domain, Assurance Condition, evidence type and potential consequence of an incorrect outcome.

5.4. Evaluation methods shall include, where applicable:

(a) document and record review;

(b) observation;

(c) interview;

(d) testing;

(e) inspection;

(f) sampling;

(g) independent confirmation;

(h) technical Verification or Validation;

(i) historical-evidence reconstruction.

5.5. Sampling shall identify the population, sampling basis, sample size, selection method, period and limitation of the conclusion supported by the sample.

5.6. Technical testing alone shall not establish an Assurance outcome where organisational, governance, personnel, Source, lifecycle, security, safeguard or dependency conditions also apply.

5.7. An evaluator shall not issue a positive Assurance outcome where the evidence is insufficient to establish the required Assurance Conditions.

5.8. An unable-to-determine outcome shall remain distinguishable from a negative outcome.

Article 6: Assurance evaluation record

6.1. Each completed Assurance evaluation shall produce an evaluation record.

6.2. The evaluation record shall identify:

(a) the Assurance Object;

(b) the applicable Assurance Domains;

(c) the applicable Profile and Version;

(d) the Assurance Conditions evaluated;

(e) the evidence considered;

(f) the evaluation methods;

(g) the findings;

(h) the resulting Assurance Level or outcome class;

(i) each dependency;

(j) each limitation, caveat and unresolved matter;

(k) the evaluation time;

(l) the Validity Period;

(m) the evaluator and responsible Actor;

(n) the conditions requiring re-evaluation.

6.3. The evaluation record shall distinguish:

(a) evidence;

(b) evaluator findings;

(c) the Assurance outcome;

(d) recommendations;

(e) unresolved matters.

6.4. An Assurance evaluation record shall remain separate from a Conformity Assessment Result and qualification decision.

6.5. A change affecting the Assurance Object, applicable Profile, evidence basis, dependency, configuration or Assurance Condition shall trigger re-evaluation where required by the applicable Profile.

6.6. A superseded or corrected Assurance evaluation record shall remain identifiable for Historical State, Review and Remedy purposes.

SECTION 3: CONFORMITY ASSESSMENT IMPLEMENTATION

Article 7: Assessment request and scope confirmation

7.1. A request for Conformity Assessment shall identify:

(a) the assessment subject;

(b) the requesting Actor;

(c) the purpose of the assessment;

(d) the proposed assessment scope;

(e) the applicable requirements and Versions;

(f) the applicable Profile and Technical Specifications;

(g) the operational locations and Controlled Environments;

(h) the systems, components, mechanisms and devices included in the scope;

(i) the material third-party and outsourced dependencies;

(j) the intended period of applicability;

(k) the intended use of the Conformity Assessment Result.

7.2. Before accepting the request, the Conformity Assessment Body shall confirm:

(a) that the assessment subject and scope are sufficiently identified;

(b) that the applicable requirements are available and capable of assessment;

(c) that the Conformity Assessment Body has the required recognised scope, competence and resources;

(d) that independence and conflict requirements are satisfied;

(e) that the proposed assessment period is sufficient;

(f) that any required accreditation or equivalent competence evidence is current and applicable.

7.3. The confirmed assessment scope shall identify each assessed Controlled Matter separately.

7.4. Assessment of a Trust Service Provider shall remain separate from assessment of each Trust Service provided by that Trust Service Provider.

7.5. Assessment of a Trust Service shall remain separate from assessment of its outputs, Trust Objects, Sources, mechanisms, devices and dependencies.

7.6. An assessment covering several Controlled Matters shall produce separately identifiable findings and conclusions for each assessment subject and scope.

7.7. A change to the confirmed scope shall be recorded and accepted by the relevant Actors before the affected assessment activity proceeds.

7.8. A Conformity Assessment Body shall not issue a conclusion outside its recognised or accredited scope.

Article 8: Competence, independence and subcontracting

8.1. A Conformity Assessment Body shall assign personnel having the competence required for the assessment subject, assessment methods, Framework requirements, applicable standards and technical environment.

8.2. The Conformity Assessment Body shall maintain a competence record identifying:

(a) the required competence areas;

(b) the assigned personnel;

(c) relevant qualifications and experience;

(d) competence evaluation;

(e) continuing competence activities;

(f) each limitation on assigned functions.

8.3. The Conformity Assessment Body shall identify and manage actual, potential and perceived conflicts of interest before and during the assessment.

8.4. A person or organisational function shall not:

(a) assess its own operational performance where independent assessment is required;

(b) make a certification conclusion concerning a matter for which it has incompatible operational responsibility;

(c) assess a matter where prior consultancy or implementation activity impairs independence;

(d) participate in both the assessment and independent review where those functions are required to remain separate.

8.5. Where a conflict cannot be controlled, the affected person, function or Conformity Assessment Body shall not perform the assessment activity.

8.6. Subcontracting shall identify:

(a) the subcontracted activity;

(b) the subcontractor;

(c) the competence and independence requirements;

(d) the applicable standard;

(e) the evidence and reporting requirements;

(f) the access and confidentiality conditions.

8.7. The recognised Conformity Assessment Body shall retain responsibility for each subcontracted assessment activity and for the resulting Conformity Assessment Result.

8.8. A subcontractor shall not acquire Conformity Assessment Body recognition or Decision Competence by reason only of performing a subcontracted activity.

8.9. A certification conclusion made by a Conformity Assessment Body shall remain separate from the qualification decision made by the competent Framework Body.

Article 9: Assessment plan and conduct

9.1. The Conformity Assessment Body shall prepare an assessment plan before substantive assessment activity begins.

9.2. The assessment plan shall identify:

(a) the assessment subject and scope;

(b) the applicable requirements and Versions;

(c) the assessment team and assigned functions;

(d) the assessment methods;

(e) the operational locations and Controlled Environments;

(f) the systems, components, mechanisms, devices and dependencies to be examined;

(g) the allocated assessment time and resources;

(h) the sampling method, where applicable;

(i) the testing and inspection activities;

(j) the assessment schedule;

(k) the reporting and review arrangements;

(l) the treatment of confidential, personal, Protection-Sensitive and Security-Sensitive Information.

9.3. The allocated assessment time and resources shall be proportionate to the scope, complexity, risk, number of locations, number of Trust Services, dependency structure and intended Qualified Scope.

9.4. The assessment shall be conducted against the requirements and Versions applicable to the confirmed assessment scope.

9.5. The Conformity Assessment Body shall obtain sufficient evidence through examination, testing, inspection, observation, interview, sampling and record review to support each material finding.

9.6. Remote assessment methods shall be used only where they provide evidence sufficient for the requirement being assessed.

9.7. The Conformity Assessment Body shall verify the identity, source, Integrity, relevance and period of applicability of material evidence.

9.8. The assessed Actor shall provide authorised access to the personnel, records, systems, locations and evidence required for the assessment.

9.9. A limitation preventing complete assessment of a requirement shall be recorded and reflected in the relevant finding and conclusion.

9.10. The Conformity Assessment Body shall not infer conformity from the absence of detected evidence of non-conformity.

Article 10: Findings, non-conformities and corrective action

10.1. Each assessment finding shall identify:

(a) the assessment subject and affected scope;

(b) the applicable requirement and Version;

(c) the evidence examined;

(d) the assessment method;

(e) the finding;

(f) the actual or potential effect;

(g) the responsible assessor;

(h) the assessment time.

10.2. A non-conformity shall identify:

(a) the failed requirement;

(b) the affected Controlled Matter and scope;

(c) the evidence basis;

(d) the effect on Assurance, security, lifecycle, qualification or Controlled Reliance;

(e) the required corrective action;

(f) the completion period;

(g) the Verification and closure conditions.

10.3. A material non-conformity shall prevent a positive assessment conclusion for the affected scope.

10.4. Where the assessment supports Qualified Trust Service Provider Status or Qualified Trust Service Status, each non-conformity against a mandatory qualified requirement shall be closed before a positive certification conclusion is issued.

10.5. Corrective-action evidence shall identify:

(a) the correction performed;

(b) the root cause where required;

(c) the affected systems, records, processes or dependencies;

(d) the completion time;

(e) the responsible Actor;

(f) the Verification performed;

(g) the closure conclusion.

10.6. Closure of a non-conformity shall be verified by the Conformity Assessment Body or another Actor expressly authorised by the applicable assessment arrangement.

10.7. An observation or opportunity for improvement shall remain distinguishable from a non-conformity.

10.8. An observation or opportunity for improvement shall not be used to conceal or downgrade a failure to satisfy a mandatory requirement.

10.9. A finding or non-conformity shall not, by itself, restrict, suspend, withdraw or revoke Status.

Article 11: Conformity Assessment Result

11.1. A completed Conformity Assessment shall produce a Conformity Assessment Result.

11.2. The Conformity Assessment Result shall identify:

(a) the assessment subject;

(b) the assessed scope;

(c) the applicable requirements and Versions;

(d) the applicable Profile and Technical Specifications;

(e) the Conformity Assessment Body;

(f) the assessment team;

(g) the assessment period;

(h) the assessment methods;

(i) the evidence basis;

(j) each finding and non-conformity;

(k) each limitation and caveat;

(l) the corrective-action and closure status;

(m) the assessment conclusion;

(n) the issue date;

(o) the period of applicability;

(p) the conditions requiring surveillance or reassessment.

11.3. Where a certification arrangement is used, the Conformity Assessment Result shall contain or reference:

(a) the certification conclusion;

(b) any certificate issued by the Conformity Assessment Body;

(c) the certification scope;

(d) the issue and expiry dates;

(e) the applicable surveillance conditions.

11.4. A Conformity Assessment Result covering several Controlled Matters shall state a separate conclusion for each assessed matter and scope.

11.5. A positive Conformity Assessment Result shall not, by itself, assign recognition, Service Permission, Technical Exchange Permission, operational activation or Qualified Status.

11.6. The Conformity Assessment Body shall protect the Conformity Assessment Result against unauthorised alteration, deletion and disclosure.

11.7. The assessed Actor shall receive the complete Conformity Assessment Result and the evidence references necessary for submission to the competent Framework Body.

11.8. A corrected or superseded Conformity Assessment Result shall remain identifiable and linked to its predecessor.

SECTION 4: QUALIFICATION IMPLEMENTATION

Article 12: Decision-Based Qualification evidence package

12.1. An applicant for Decision-Based Qualification shall prepare a qualification evidence package for submission to the competent Framework Body.

12.2. The qualification evidence package shall identify:

(a) the eligible Status-Bearing Matter;

(b) its stable identifier, category and Version;

(c) the applicant and Responsible Actor;

(d) the applicable Qualified Profile and Version;

(e) the proposed Qualified Scope;

(f) the applicable Conformity Assessment Result;

(g) each non-conformity and its closure status;

(h) the material qualified dependencies;

(i) the evidence supporting each qualified condition;

(j) the applicable security, Continuity and lifecycle conditions;

(k) the proposed Effective Date and review date;

(l) the proposed surveillance and reassessment arrangements;

(m) the proposed restrictions and caveats;

(n) the publication information required following a qualification decision;

(o) the applicable Review Route.

12.3. A separate qualification evidence package shall be maintained for each:

(a) Trust Service Provider;

(b) Trust Service;

(c) Authoritative Source;

(d) creation mechanism or device;

(e) other matter subject to Decision-Based Qualification under the Framework.

12.4. A package covering several related matters shall preserve the separate identity, scope, evidence and requested outcome of each matter.

12.5. The proposed Qualified Scope shall not exceed the assessed scope.

12.6. The applicant shall identify each material limitation, uncertainty, dependency and unresolved matter in the qualification evidence package.

12.7. The competent Framework Body shall receive the complete evidence package before the qualification decision is prepared.

12.8. Submission, acceptance or technical completeness of the qualification evidence package shall not create Qualified Status.

Article 13: Object-Instance Qualification implementation

13.1. A Responsible Actor implementing Object-Instance Qualification shall maintain a controlled process for evaluating each eligible Trust Object or Trust Service Output against the applicable Qualified Object Profile.

13.2. The process shall verify, where applicable:

(a) the identity and category of the object or output;

(b) the applicable Qualified Object Profile and Version;

(c) the required issuing or producing Trust Service Status;

(d) the required qualified dependencies;

(e) the creation or issuance evidence;

(f) the required content and Metadata;

(g) the required protection mechanism;

(h) the applicable lifecycle and Status information;

(i) the applicable Validation requirements.

13.3. The process shall produce or reference a Validation Result confirming whether the applicable qualified conditions were satisfied.

13.4. The object-instance qualification record shall identify:

(a) the Trust Object or Trust Service Output;

(b) the Qualified Object Profile and Version;

(c) the issuing or producing Trust Service;

(d) each qualified dependency and its relevant Status;

(e) the evaluation time;

(f) the creation or issuance time;

(g) the evidence considered;

(h) the Validation Result;

(i) each limitation and caveat.

13.5. Object-Instance Qualification shall not require an individual Framework Decision unless the Framework expressly assigns such a decision.

13.6. Failure of an individual object or output to satisfy a qualified condition shall prevent Qualified Trust Object Status for that object or output and shall not, by itself, alter the Status of its Issuer, Trust Service Provider, Trust Service, Source, mechanism, device or dependency.

13.7. An object-instance qualification record shall remain available for Historical Validation during the applicable Retention period.

Article 14: Qualified dependencies and composite arrangements

14.1. Each qualified dependency shall be recorded and evaluated within the scope and time for which it is required.

14.2. The qualified-dependency record shall identify:

(a) the dependent Controlled Matter;

(b) the supporting Controlled Matter;

(c) the dependency type;

(d) the required Status and Qualified Scope;

(e) the applicable Version or configuration;

(f) the relevant time condition;

(g) the evidence and Status source;

(h) the effect of restriction, Suspension, Withdrawal, Revocation, expiry or unavailability.

14.3. Qualified Status assigned to a dependency shall not transfer to the dependent Controlled Matter.

14.4. A composite arrangement shall preserve separate identification of:

(a) each assessment subject;

(b) each Assurance Object;

(c) each qualified dependency;

(d) each applicable requirement;

(e) each finding;

(f) each assessment or qualification outcome.

14.5. The applicable Profile shall establish the rule for combining Assurance outcomes, assessment findings or dependency conditions.

14.6. A composite arrangement shall not derive an overall positive conclusion solely from the highest Assurance Level, strongest dependency or most favourable constituent result.

14.7. Failure or unavailability of a required qualified dependency shall prevent a positive qualified outcome within the affected dependent scope.

14.8. Substitution of a qualified dependency shall undergo the assessment and Change Control required by the applicable Profile before operational use.

14.9. Historical evaluation shall use the dependency Status, Version, configuration and scope applicable at the relevant past time.

Article 15: Decision and Status Publication handoff

15.1. Following a Framework Decision assigning, restricting, suspending, withdrawing, revoking or reinstating Qualified Status, the Responsible Actor shall prepare the authorised Status Publication information.

15.2. The Status Publication information shall identify:

(a) the qualified Status-Bearing Matter;

(b) its stable identifier and category;

(c) the Qualified Scope;

(d) the applicable Qualified Profile and Version;

(e) the Effective Date;

(f) the Validity Period or review date;

(g) each restriction and caveat;

(h) the Framework Decision reference;

(i) the responsible Framework Body;

(j) the applicable discovery or service identity information;

(k) the predecessor Status entry, where applicable.

15.3. The Responsible Actor shall transmit the authorised information to the function responsible for Status Publication.

15.4. Before publication, the publication function shall verify consistency between:

(a) the Framework Decision;

(b) the Status-Bearing Matter identifier;

(c) the Qualified Scope;

(d) the Qualified Profile and Version;

(e) the Effective Date;

(f) the published restrictions and caveats.

15.5. A technical operator shall not alter the qualified decision, Qualified Scope, Effective Date, restriction or lifecycle state contained in the authorised publication information.

15.6. Individual high-volume Trust Objects and Trust Service Outputs shall not receive Humanitarian Trust List Entries unless the Framework expressly requires individual publication.

15.7. Qualified Trust Object Status shall ordinarily be evidenced through the object or output, applicable Qualified Object Profile, issuing-service Status, dependency Status, Validation Result and authorised Status information.

15.8. A publication error shall be corrected through the applicable publication and Correction processes without altering the underlying Framework Decision.

SECTION 5: SURVEILLANCE AND QUALIFICATION LIFECYCLE

Article 16: Surveillance, reassessment and material change

16.1. Each matter subject to continuing Assurance, Conformity Assessment or Decision-Based Qualification shall have a surveillance and reassessment plan.

16.2. The plan shall identify:

(a) the subject and scope;

(b) the applicable requirements and Versions;

(c) the surveillance frequency;

(d) the surveillance methods;

(e) the evidence to be reviewed;

(f) the material-change triggers;

(g) the responsible Actors;

(h) the reporting and escalation arrangements;

(i) the conditions requiring full reassessment.

16.3. A Qualified Trust Service Provider and each Qualified Trust Service shall undergo at least one surveillance Conformity Assessment within each twelve-month period.

16.4. A shorter surveillance interval shall apply where required by the applicable Qualified Profile, Framework Decision, risk assessment, incident, dependency condition or previous finding.

16.5. Surveillance of several Trust Services during one assessment activity shall preserve separate evidence, findings and conclusions for each Trust Service and Qualified Scope.

16.6. Reassessment shall occur where a material change affects:

(a) the assessed or qualified scope;

(b) the applicable Profile, requirement or Recognised Standard;

(c) governance or organisational arrangements;

(d) operational locations or Controlled Environments;

(e) systems, components, mechanisms or devices;

(f) material third parties or outsourced functions;

(g) security, Continuity or safeguard conditions;

(h) Sources or other material dependencies;

(i) evidence, testing or monitoring arrangements;

(j) a Qualified Scope or qualified dependency.

16.7. The Responsible Actor shall notify the competent Framework Body and Conformity Assessment Body of a material change within the period assigned by the applicable Profile or Framework Decision.

16.8. Where prior assessment is required, the changed matter shall not operate under the earlier assessed or Qualified Scope until that assessment and the required decision are complete.

16.9. A surveillance finding shall be recorded and communicated to the competent Framework Body where lifecycle action or another Framework Decision is required.

16.10. A surveillance finding shall not, by itself, alter Qualified Status.

Article 17: Lifecycle action and reinstatement support

17.1. Where evidence indicates that a qualified condition is no longer satisfied or is materially at risk, the Responsible Actor shall prepare a lifecycle-action evidence package for the competent Framework Body.

17.2. The evidence package shall identify:

(a) the affected Status-Bearing Matter and Qualified Scope;

(b) the failed or threatened condition;

(c) the evidence basis;

(d) the relevant finding, non-conformity, incident or change;

(e) the affected dependencies;

(f) the affected outputs or Trust Objects;

(g) the immediate protective and corrective actions;

(h) the proposed restriction, Suspension, Withdrawal, Revocation or other treatment;

(i) the proposed Effective Date;

(j) the Status Publication and notification requirements;

(k) the treatment of Historical State;

(l) the applicable Review Route.

17.3. A lifecycle-action evidence package shall distinguish between:

(a) the Trust Service Provider;

(b) each Trust Service;

(c) each Source;

(d) each mechanism or device;

(e) each individual Trust Object or Trust Service Output.

17.4. A proposed lifecycle action shall remain limited to the affected matter and scope supported by the evidence.

17.5. Treatment of outputs created before the Effective Date of a lifecycle action shall be determined under the applicable Framework requirements and Historical State evidence.

17.6. An application for reinstatement shall include:

(a) the corrected condition;

(b) the corrective-action evidence;

(c) independent Verification where required;

(d) the reassessment result;

(e) the restored dependency conditions;

(f) the proposed reinstated scope;

(g) the proposed Effective Date;

(h) the required publication information.

17.7. Reinstatement of Qualified Trust Service Provider Status shall not, by itself, reinstate Qualified Trust Service Status.

17.8. Reinstatement of a Qualified Trust Service shall not, by itself, reinstate the Qualified Status of another Trust Service, Source, mechanism, device, Trust Object or Trust Service Output.

17.9. Corrective action, reassessment or submission of a reinstatement application shall not create reinstated Qualified Status before the applicable Framework Decision.

Article 18: Records and Historical State

18.1. Each Responsible Actor shall maintain the records required to reconstruct Assurance evaluation, Conformity Assessment and qualification within the applicable scope.

18.2. The records shall include, where applicable:

(a) Implementation Plans;

(b) requirement and evidence maps;

(c) Assurance evaluation plans and records;

(d) assessment requests and confirmed scopes;

(e) competence and independence records;

(f) assessment plans;

(g) evidence and sampling records;

(h) findings and non-conformities;

(i) corrective-action and closure records;

(j) Conformity Assessment Results;

(k) qualification evidence packages;

(l) Framework Decision references;

(m) object-instance qualification records;

(n) qualified-dependency records;

(o) Status Publication handoff records;

(p) surveillance and reassessment records;

(q) material-change records;

(r) lifecycle-action and reinstatement records;

(s) Review and Remedy records.

18.3. Records shall preserve the identity, Version, time, scope, evidence source, responsible Actor, dependency and applicable Framework Instrument for each material action and conclusion.

18.4. Records shall be protected against unauthorised access, alteration, deletion and disclosure.

18.5. Access to records shall be limited according to assigned Decision Competence, assessment responsibility, Review Route, Remedy Route and applicable Confidentiality conditions.

18.6. Historical State shall remain reconstructable for the period required for Validation, supervision, Review, Remedy, Controlled Reliance and External Legal Effect where applicable.

18.7. Correction of a record shall preserve the earlier record, the correction basis, the responsible Actor and the Effective Date of the correction.

18.8. A later evaluation, assessment, decision or publication shall not erase or silently replace earlier evidence or Historical State.

18.9. A corrected or superseded record shall remain linked to its predecessor and successor.

Article 19: Reference standards and specifications

19.1. The reference standards applicable to the implementation of this Guideline are set out in Annex I.

19.2. A reference identified in Annex I shall apply only within the implementation function, subject and scope identified in that Annex.

19.3. Service-specific, object-specific, Source-specific, device-specific and technical-testing standards shall be identified through the applicable subject-specific Implementation Guideline, Profile and Technical Specification.

19.4. A later edition, amendment or replacement of a standard identified in Annex I shall not apply automatically.

19.5. A later edition, amendment or replacement shall undergo standards evaluation and Change Control before it is assigned Framework effect.

19.6. Conformity with a standard identified in Annex I shall constitute evidence only for the requirements and scope mapped to that standard.

19.7. Conformity with a standard shall not, by itself, create an Assurance outcome, positive Conformity Assessment Result, qualification decision, Qualified Status, recognition, Service Permission, Technical Exchange Permission or Controlled Reliance.

ANNEX I: REFERENCE STANDARDS

Reference	Implementation function	Applicability and controlled treatment
ISO/IEC 17000:2020, Conformity assessment — Vocabulary and general principles	Common conformity-assessment concepts and functional relationships	Applicable as supporting terminology and principles where consistent with the Controlled Terms established by the Framework. Part II terminology shall prevail where the meanings differ.
ISO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services	Competence, impartiality, operation, review and certification requirements for Conformity Assessment Bodies	Mandatory where a Conformity Assessment Body makes a certification conclusion concerning a product, process or service.
ETSI EN 319 403-1 V2.3.1, 2020-06, Trust Service Provider Conformity Assessment — Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers	Additional requirements for assessment and certification of Trust Service Providers and Trust Services	Mandatory for a Conformity Assessment Body assessing a Trust Service Provider or Trust Service for Decision-Based Qualification, together with ISO/IEC 17065:2012.
ISO/IEC 17067:2013, Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes	Design and maintenance of continuing-certification arrangements	Mandatory where a conformity-assessment arrangement supporting continuing Decision-Based Qualification uses product, process or service certification.

Reference	Implementation function	Applicability and controlled treatment
		Scheme type 6 shall apply to Qualified Trust Service Provider and Qualified Trust Service assessment unless the applicable Qualified Profile establishes a stricter arrangement.
ISO/IEC 17011:2017, Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies	Accreditation-body competence, impartiality and consistent operation	Applicable where accreditation is used as evidence supporting recognition or continuing competence of a Conformity Assessment Body.
ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories	Testing, sampling and calibration performed by a laboratory	Mandatory for subcontracted or relied-upon laboratory activities where the applicable Profile requires accredited testing or calibration.
ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements	Audit and certification of management systems	Mandatory where a management-system audit is subcontracted or used as distinct conformity evidence.
ISO/IEC 17020:2026, Conformity assessment — Requirements for bodies performing inspection	Inspection activities used as conformity evidence	Mandatory where inspection is subcontracted or relied upon as a distinct assessment activity.
ISO 19011:2026, Guidelines for auditing management systems	Audit-programme management, audit planning, audit conduct and auditor competence	Applicable as supporting guidance where management-system audit methods form part of the assessment plan. It shall not replace ISO/IEC 17065, ETSI EN 319 403-1 or another mandatory conformity-assessment standard.

IDEHA-IG-SEC-CNF-001: SECURITY AND CONFIDENTIALITY IMPLEMENTATION

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Guideline lays down implementation requirements for security and Confidentiality under the Framework.

1.2. This Guideline shall apply to each Framework Body, Participating Actor, Trust Service Provider, Source Holder, Source Steward, Issuer, Relying Actor, Responsible Actor, Technical Exchange Route Operator, Intermediary, supporting Actor and technical operator responsible for implementing or operating a Controlled Matter, Controlled Environment, Trust Service, Source, Trust Object, Trust Service Output, mechanism, device, Authenticator, Endpoint, Technical Exchange Route, Register, Catalogue or Humanitarian Trust List component.

1.3. This Guideline shall govern, where applicable:

(a) security governance, responsibility and Accountability;

(b) security scope, inventory and dependency identification;

(c) trust-boundary and Controlled Environment implementation;

(d) security risk assessment and treatment;

(e) information classification and handling;

(f) Transport Confidentiality, Payload Confidentiality, storage confidentiality, processing confidentiality and disclosure control;

(g) plaintext access and Intermediary exclusion;

(h) access control and privileged functions;

(i) Integrity, Authenticity and Accountability controls;

(j) protected functions and Security-Sensitive Information;

(k) secure acquisition, development, configuration and change;

(l) vulnerability management;

(m) security monitoring, logging and evidence;

(n) Security Incident readiness and handoff;

(o) security testing, exceptions and lifecycle evidence.

1.4. This Guideline shall not:

(a) redefine the security architecture or structural relationships established by the Main Framework and Annex H;

(b) establish a security category, Trust Service Category, Trust Object Category, Status category, qualification route or Controlled Effect;

(c) assign recognition, Service Permission, Technical Exchange Permission, Status, Qualified Status, access, disclosure permission, Authorisation or Controlled Reliance;

(d) replace a Framework Decision or a decision retained by a Responsible Actor within its assigned responsibility;

(e) treat encryption, Authentication, successful testing, technical isolation or technical inaccessibility as Authorisation or disclosure permission;

(f) prescribe exact algorithms, key sizes, protocol Versions, cipher suites, schemas, interfaces, configuration values, product settings or test vectors;

(g) govern operational Security Incident response, containment, notification, Continuity, Degraded Operation, Recovery, reinstatement or incident closure.

1.5. Cryptographic policy, cryptographic mechanisms, key lifecycle, cryptographic agility and post-quantum transition shall be governed by IDEHA-IG-SEC-CRY-001.

1.6. Operational Security Incident response, Continuity, Degraded Operation, Recovery, reinstatement and closure shall be governed by IDEHA-IG-SEC-INC-001.

1.7. Compliance with this Guideline shall not, by itself, establish operational activation, Authorisation, disclosure permission, Qualified Status, External Legal Status, External Legal Effect or permission for Controlled Reliance.

Article 2: Application through Schemes, Profiles and Technical Specifications

2.1. The applicable Scheme shall identify:

(a) the governed purpose and operational context;

(b) the participating Actors and affected persons;

(c) the Controlled Matters and interactions within scope;

(d) the applicable risk context;

(e) the required safeguards;

(f) the applicable Review and Remedy arrangements.

2.2. The applicable Profile shall identify:

(a) the security scope and Responsible Actors;

(b) the Controlled Matters, Controlled Environments and trust boundaries;

(c) the applicable information classes;

(d) the Confidentiality, Integrity, Authenticity, Availability and Accountability requirements;

(e) the applicable access and privileged-function requirements;

(f) the protected functions and Security-Sensitive Information;

(g) the required security controls and evidence;

(h) the testing, Assurance and Conformity Assessment requirements;

(i) the incident-readiness and handoff requirements;

(j) the exception, change, Review and lifecycle conditions.

2.3. The applicable Technical Specification shall define the exact implementation and testing requirements, including:

(a) algorithms and parameters;

(b) technical formats and interfaces;

(c) protocol options;

(d) configuration values;

(e) control settings;

(f) test inputs and expected results;

(g) technical conformance criteria.

2.4. A subject-specific Implementation Guideline shall establish only the additional security requirements necessary for its subject matter and shall not repeat the horizontal controls established by this Guideline.

2.5. A Profile, Technical Specification, test report, risk decision, exception record, monitoring record or security evidence artefact shall not alter a category, Decision Competence, Status or Controlled Effect established by the Main Framework.

Article 3: Security and Confidentiality Implementation Plan

3.1. A Responsible Actor shall maintain a Security and Confidentiality Implementation Plan for each implementation within its responsibility.

3.2. The Implementation Plan shall identify:

(a) the governed purpose and implementation scope;

(b) the applicable Federation Domain;

(c) the Controlled Matters and Controlled Environments within scope;

(d) each Responsible Actor, supporting Actor, technical operator and material dependency;

(e) the organisational, physical, technical and Federation Boundaries;

(f) the information classes and applicable Confidentiality requirements;

(g) the security risks, treatment decisions and residual risks;

(h) the access, Integrity, Authenticity, Availability and Accountability controls;

(i) the protected functions and Security-Sensitive Information;

(j) the monitoring, logging, vulnerability-management and evidence arrangements;

(k) the Security Incident readiness and handoff arrangements;

(l) the testing, Assurance and Conformity Assessment requirements;

(m) the exception, Change Control, Review, Remedy, Retention and lifecycle arrangements.

3.3. The Implementation Plan shall distinguish:

(a) governance responsibility from technical operation;

(b) security-control operation from Decision Competence;

(c) Transport Confidentiality from Payload Confidentiality;

(d) storage confidentiality from processing confidentiality;

(e) Confidentiality from Authorisation and disclosure permission;

(f) Authentication from access permission;

(g) Integrity from Authenticity;

(h) service security from object-level protection;

(i) security monitoring from Security Incident response;

(j) technical Recovery from Status or permission reinstatement.

3.4. The Responsible Actor shall approve the Implementation Plan before operational activation within the affected scope.

3.5. Approval of the Implementation Plan shall not replace a Framework Decision, Service Permission, Technical Exchange Permission, Source-access decision, Authorisation Outcome or qualification decision required by the Framework.

3.6. The Responsible Actor shall update the Implementation Plan where a material change affects the scope, risk, Actors, dependencies, information classification, controls, evidence, monitoring, Assurance or incident readiness.

SECTION 2: GOVERNANCE, SCOPE AND RISK

Article 4: Security governance, responsibility and Accountability

4.1. Each Responsible Actor shall assign security responsibility for every Controlled Matter and security function within its scope.

4.2. The responsibility record shall identify:

(a) the accountable organisational function;

(b) the operational security function;

(c) the Controlled Matter and function within scope;

(d) the supporting Actors and technical operators;

(e) the approval, escalation and Review routes;

(f) the evidence and reporting obligations.

4.3. A Trust Service Provider shall retain responsibility for the security of each Trust Service within its Provider Scope and Service Scope.

4.4. A Source Holder and Source Steward shall retain their respective security responsibilities for the Source and Source Scope assigned by the applicable Source Profile.

4.5. A Technical Exchange Route Operator, Intermediary, supporting Actor or technical operator shall remain responsible for its assigned security functions without acquiring the Role, Status, responsibility or Decision Competence of another Actor.

4.6. Outsourcing, shared infrastructure or delegation of technical operation shall not remove the responsibility assigned to the Responsible Actor.

4.7. Security responsibilities shall remain identifiable during:

(a) normal operation;

(b) maintenance;

(c) privileged or emergency access;

(d) incident handoff;

(e) transition;

(f) cessation.

4.8. The Responsible Actor shall review the responsibility allocation following each material organisational, technical or dependency change.

Article 5: Controlled Matter inventory, trust boundaries and Controlled Environments

5.1. A Responsible Actor shall maintain an inventory of the Controlled Matters and material dependencies within its security scope.

5.2. The inventory shall identify, where applicable:

(a) Actors, Roles and Mandates;

(b) Trust Service Providers and Trust Services;

(c) Sources and Source Scopes;

(d) Trust Objects and Trust Service Outputs;

(e) mechanisms, devices and Authenticators;

(f) Endpoints, Technical Exchange Routes and Intermediaries;

(g) Registers, Catalogues, Humanitarian Trust List components and publication channels;

(h) information stores, processing environments and evidence repositories;

(i) external services, supporting Actors and material dependencies;

(j) applicable Status, Version and lifecycle information.

5.3. The Responsible Actor shall identify each organisational, physical, technical and Federation Boundary crossed by a Controlled Interaction or information flow.

5.4. A trust-boundary record shall identify:

(a) the originating and receiving Actors;

(b) the Controlled Matters crossing the boundary;

(c) the applicable Authentication and Authorisation conditions;

(d) the applicable Confidentiality, Integrity, Authenticity and evidence requirements;

(e) the permitted processing and disclosure scope;

(f) each Intermediary and technical operator;

(g) the monitoring and incident-handoff arrangements.

5.5. The Responsible Actor shall identify each Controlled Environment required for:

(a) a protected function;

(b) a qualified dependency;

(c) Restricted Information;

(d) Protection-Sensitive Information;

(e) Security-Sensitive Information;

(f) an elevated Assurance condition.

5.6. The inventory, trust-boundary record and Controlled Environment record shall remain current and traceable to the applicable Profile and Version.

5.7. Inclusion in an inventory, architecture record or trust-boundary record shall not create recognition, access, Service Permission, Technical Exchange Permission or Authorisation.

Article 6: Security risk assessment and treatment

6.1. A Responsible Actor shall assess security risks before operational activation and throughout the implementation lifecycle.

6.2. The risk assessment shall identify, where applicable:

(a) the Controlled Matters, Actors, persons and operations exposed to harm;

(b) threats, vulnerabilities and adverse conditions;

(c) Confidentiality, Integrity, Authenticity, Availability, Accountability and protection impacts;

(d) risks arising from aggregation, inference, correlation, linkability and onward transfer;

(e) risks arising from shared infrastructure, outsourcing and cross-domain dependencies;

(f) risks affecting Trust Services, Sources, Trust Objects, mechanisms, devices, Endpoints and Technical Exchange Routes;

(g) risks affecting Assurance, Conformity Assessment and Qualified Status;

(h) risks affecting Correction, Review, Remedy and Historical State;

(i) likelihood, consequence, uncertainty and the evidence basis.

6.3. A risk-treatment record shall identify:

(a) the selected controls;

(b) the Responsible Actor for each control;

(c) the implementation and verification time;

(d) the expected residual risk;

(e) the monitoring and reassessment requirements;

(f) the escalation and incident-handoff conditions.

6.4. A material risk affecting a mandatory dependency shall be addressed before that dependency supports a positive Assurance, Verification, Validation, qualification or Controlled Reliance outcome.

6.5. Residual risk shall be accepted only by the Actor or Framework Body holding the applicable responsibility or Decision Competence.

6.6. A residual-risk decision shall identify:

(a) the affected scope;

(b) the evidence basis;

(c) the controls applied;

(d) the duration and review date;

(e) the limitations;

(f) the continuing obligations.

6.7. Risk acceptance shall not create Authorisation, disclosure permission, Qualified Status or permission for Controlled Reliance.

Article 7: Shared infrastructure, supplier and dependency security

7.1. A Responsible Actor shall identify and assess each material security dependency before relying on shared infrastructure, an outsourced function, a supplier, a supporting Actor or another Federation Domain.

7.2. A dependency record shall identify:

(a) the dependent and supporting Controlled Matters;

(b) the responsible and supporting Actors;

(c) the assigned security function and scope;

(d) the service, information and trust boundaries;

(e) the applicable Profile, Technical Specification and Version;

(f) the evidence, monitoring and notification obligations;

(g) the restriction, transition and termination conditions.

7.3. A contractual, operational or Federation arrangement shall allocate:

(a) access and privileged-function responsibilities;

(b) Confidentiality, Integrity, Authenticity and Availability responsibilities;

(c) logging, monitoring and evidence responsibilities;

(d) vulnerability, update and remediation responsibilities;

(e) Security Incident notification and cooperation responsibilities;

(f) return, transfer, Retention and Deletion responsibilities;

(g) Assurance and Conformity Assessment access rights;

(h) transition and exit responsibilities.

7.4. A supporting Actor shall provide the evidence required to demonstrate performance of its assigned security functions.

7.5. Shared infrastructure shall not merge the Status, Service Scope, Qualified Scope, security responsibility or lifecycle of the Controlled Matters using that infrastructure.

7.6. A security weakness or Security Incident affecting shared infrastructure shall affect a dependent Controlled Matter only according to the identified dependency, relevant time, evidence and affected scope.

7.7. Termination of a dependency shall include:

(a) secure transition;

(b) access removal;

(c) information return or transfer;

(d) Retention and Deletion treatment;

(e) evidence preservation;

(f) verification of completed exit actions.

SECTION 3: INFORMATION PROTECTION AND ACCESS

Article 8: Information classification and handling

8.1. A Responsible Actor shall classify information according to the harm capable of arising from unauthorised access, use, combination, alteration, loss, disclosure or Retention.

8.2. The classification process shall identify:

(a) information authorised for public disclosure;

(b) information subject to restricted operational or supervisory access;

(c) Restricted Information;

(d) Protection-Sensitive Information;

(e) Security-Sensitive Information;

(f) each narrower class established by the applicable Profile.

8.3. A classification record shall identify:

(a) the information class;

(b) the responsible Actor;

(c) the authorised purposes and recipients;

(d) the applicable access and disclosure controls;

(e) the storage, transmission and processing controls;

(f) the logging and monitoring controls;

(g) the Retention, archival and Deletion conditions;

(h) the review and reclassification triggers.

8.4. Information that is not individually sensitive shall be classified according to the additional risk created by aggregation, combination, inference, correlation or linkability.

8.5. A Humanitarian Trust List Entry, Register Entry, Catalogue Entry, Status Response, error message, log or evidence record shall contain only information authorised for its assigned access or publication class.

8.6. Information shall retain its applicable handling requirements when copied, transformed, cached, backed up, archived or transferred.

8.7. Reclassification shall preserve:

(a) the earlier classification;

(b) the reason and evidence basis;

(c) the responsible Actor;

(d) the Effective Date;

(e) the effect on access, disclosure, Retention and existing copies.

Article 9: Confidentiality control implementation

9.1. A Responsible Actor shall implement Confidentiality controls throughout:

(a) collection and creation;

(b) issuance;

(c) transmission and receipt;

(d) processing;

(e) storage and backup;

(f) disclosure;

(g) Retention and archival;

(h) Deletion and destruction.

9.2. The implementation shall distinguish:

(a) Transport Confidentiality;

(b) Payload Confidentiality;

(c) storage confidentiality;

(d) processing confidentiality;

(e) disclosure control.

9.3. The applicable Profile shall identify the Confidentiality layer required for each information class, interaction, trust boundary, processing activity and lifecycle state.

9.4. A Confidentiality-control record shall identify:

(a) the protected information and scope;

(b) the authorised Actors and purposes;

(c) the protection and termination points;

(d) the mechanism, dependency and responsible Actor;

(e) the Validation, monitoring and evidence requirements;

(f) the failure, restriction and incident-handoff conditions.

9.5. Confidentiality controls shall preserve data minimisation and shall not require disclosure of additional information merely to operate the control.

9.6. Confidentiality protection shall not replace:

(a) Integrity;

(b) Authenticity;

(c) Authentication;

(d) Authorisation;

(e) Status;

(f) Validation;

(g) Controlled Reliance requirements.

9.7. Encryption, isolation or technical inaccessibility shall not, by itself, authorise collection, processing, exchange, disclosure, onward transfer or Retention.

9.8. Each failure of a required Confidentiality control shall receive the restriction and incident-handoff treatment assigned by the applicable Profile.

Article 10: Payload Confidentiality and plaintext access

10.1. Where Payload Confidentiality is required, the originating Actor shall protect the payload before it enters the Technical Exchange Route.

10.2. Plaintext access shall be limited to:

(a) the authorised originating Actor;

(b) the authorised receiving Actor;

(c) each additional processing Actor expressly identified by the applicable Profile and Authorisation Outcome.

10.3. A Technical Exchange Route Operator, Intermediary, gateway operator, relay operator or Federated Data Exchange Service Provider shall not access plaintext payload content solely because that Actor carries, routes, stores, monitors or evidences the exchange.

10.4. Decryption material shall not be made available to an Intermediary or unrelated component unless:

(a) the applicable Profile assigns that Actor a processing function;

(b) the applicable Authorisation Outcome covers the processing;

(c) the required safeguards and evidence apply.

10.5. The payload-protection record shall identify:

(a) the originating and receiving Actors;

(b) the protected payload and associated Metadata;

(c) the encryption and decryption responsibilities;

(d) the authorised processing points;

(e) the applicable key or credential dependency;

(f) the Integrity and Authenticity controls;

(g) the failure and incident-handoff conditions.

10.6. Discovery Metadata, routing Metadata and Exchange Evidence shall be limited to the information necessary and authorised for routing, security, Accountability and error handling.

10.7. Transport Confidentiality shall not replace Payload Confidentiality where Payload Confidentiality is required.

10.8. Payload Confidentiality shall not replace an Electronic Signature, Electronic Seal, Electronic Timestamp or other object-level protection required for independent Verification or Validation.

10.9. Payload signing, sealing and encryption for the Federated Data Exchange Service shall be implemented in accordance with IDEHA-IG-SVC-FDX-001 and the applicable Profile and Technical Specification.

Article 11: Access control and privileged functions

11.1. A Responsible Actor shall limit access to a Controlled Matter, Trust Service, Source, Endpoint, mechanism, device, administrative function or evidence repository to authorised Actors and the minimum scope necessary for the assigned purpose.

11.2. The access-control arrangement shall address, where applicable:

(a) Identification and Authentication;

(b) Authorisation;

(c) least privilege;

(d) separation of duties;

(e) privileged access;

(f) emergency access;

(g) periodic access Review;

(h) restriction and removal of access;

(i) auditable access evidence.

11.3. An access record shall identify:

(a) the Actor and applicable Role;

(b) the purpose;

(c) the Controlled Matter;

(d) the permitted action and scope;

(e) the Effective Date;

(f) the expiry or review date;

(g) the approval basis;

(h) the evidence reference.

11.4. Privileged access shall be:

(a) separately authorised;

(b) limited to the assigned function;

(c) time-limited where practicable;

(d) monitored;

(e) periodically reviewed.

11.5. Emergency access shall be limited to the emergency scope, recorded, monitored, reviewed and terminated when the emergency condition ends.

11.6. A successful Authentication Outcome shall not, by itself, create Authorisation, disclosure permission or access to another Controlled Matter.

11.7. Administrative, maintenance or support access shall not assign the Role, Status or Decision Competence of the Actor responsible for the controlled function.

11.8. Access shall be removed without undue delay where the applicable Role, Mandate, employment, contract, purpose, dependency or Authorisation condition ends or changes.

11.9. Access Reviews shall identify and correct excessive, conflicting, dormant, unauthorised or no longer necessary access.

SECTION 4: INTEGRITY, PROTECTED FUNCTIONS AND OPERATIONAL SECURITY

Article 12: Integrity, Authenticity and Accountability

12.1. A Responsible Actor shall protect a Controlled Matter against unauthorised alteration, substitution, deletion, corruption, replay and incorrect lifecycle transition.

12.2. The applicable Profile shall identify the Integrity, Authenticity and Accountability controls required for each:

(a) Trust Object and Trust Service Output;

(b) request, response and message;

(c) record and evidence artefact;

(d) decision and Status publication;

(e) policy and configuration package;

(f) lifecycle event.

12.3. A statement-bearing Trust Object or Trust Service Output crossing an organisational or Federation Boundary shall receive the object-level protection required by the applicable Framework Instruments and Profile.

12.4. Transport protection shall not replace an Electronic Signature, Electronic Seal, Electronic Timestamp, Certificate or other object-level evidence required for independent Verification or Validation.

12.5. A material action, access, disclosure, change, decision and lifecycle transition shall be attributable to the responsible Actor, service, mechanism, device or system where Accountability requires that attribution.

12.6. A Controlled Interaction shall include replay, duplication, sequencing and correlation controls where the applicable Profile identifies those risks.

12.7. Integrity, Authenticity and Accountability evidence shall be protected against unauthorised alteration and retained according to the applicable Profile and Retention requirements.

12.8. Successful Integrity or Authenticity Verification shall not, by itself, establish correctness, lawfulness, Authorisation, acceptance or Controlled Reliance.

Article 13: Protected functions and Security-Sensitive Information

13.1. A Responsible Actor shall identify each protected function and item of Security-Sensitive Information within its scope.

13.2. Protected functions and Security-Sensitive Information shall include, where applicable:

(a) Digital Signature Creation Data and protected creation functions;

(b) Digital Signature Validation Data and trust anchors;

(c) encryption and decryption keys;

(d) Authentication secrets and recovery material;

(e) privileged administrative credentials;

(f) creation mechanisms and devices;

(g) security policies and configurations;

(h) vulnerability and Security Incident information;

(i) certificate, Status and Validation dependencies;

(j) monitoring, detection and response configurations.

13.3. The protected-function record shall identify:

(a) the responsible Actor;

(b) the authorised functions and users;

(c) the applicable Controlled Environment;

(d) the access and separation-of-duties controls;

(e) the monitoring and evidence requirements;

(f) the restriction, compromise and incident-handoff conditions.

13.4. Access to a protected function or item of Security-Sensitive Information shall be separately authorised, logged, monitored and reviewed.

13.5. Digital Signature Creation Data and Digital Signature Creation Devices shall be governed by IDEHA-IG-OBJ-DSG-001.

13.6. Cryptographic mechanisms, key lifecycle, trust-anchor controls, cryptographic agility and post-quantum transition shall be governed by IDEHA-IG-SEC-CRY-001.

13.7. A remote or shared protected-function arrangement shall preserve the control, activation, separation and evidence requirements assigned by the applicable Profile.

13.8. Compromise or suspected compromise of a protected function, Authenticator, mechanism, device, credential or item of Security-Sensitive Information shall trigger the handoff required by Article 17.

Article 14: Secure design, acquisition, development, configuration and change

14.1. A Responsible Actor shall integrate security and Confidentiality requirements into:

(a) design;

(b) acquisition;

(c) development;

(d) configuration;

(e) deployment;

(f) operation and maintenance;

(g) retirement.

14.2. Security design shall identify:

(a) the governed purpose and security assumptions;

(b) the trust boundaries and Controlled Environments;

(c) the threat and risk model;

(d) the information flows and processing points;

(e) the required access, Confidentiality, Integrity, Authenticity and evidence controls;

(f) the failure, exception and incident-handoff behaviour;

(g) the testing and acceptance criteria.

14.3. Acquisition, development and configuration controls shall address, where applicable:

(a) separation of development, testing and operational environments;

(b) source, build and configuration Integrity;

(c) supplier, dependency and component review;

(d) secure default configuration;

(e) removal or restriction of unnecessary functions and access;

(f) secret and credential protection;

(g) code, configuration and change Review;

(h) security testing before operational use.

14.4. A material security change shall undergo the assessment, testing, approval and evidence requirements assigned by the applicable Profile before operational use.

14.5. Emergency change shall remain subject to:

(a) recorded scope and approval;

(b) compensating controls;

(c) proportionate testing;

(d) post-implementation Review;

(e) rollback arrangements.

14.6. Technical availability or successful deployment shall not, by itself, establish operational activation, Service Permission, Technical Exchange Permission or permission for Controlled Reliance.

Article 15: Vulnerability management and remediation

15.1. A Responsible Actor shall maintain a vulnerability-management process for each system, Trust Service, Source, mechanism, device, Endpoint, Technical Exchange Route and material dependency within its scope.

15.2. The process shall include:

(a) vulnerability identification and intake;

(b) validation and affected-scope determination;

(c) risk assessment and prioritisation;

(d) remediation, mitigation or restriction;

(e) testing and Verification;

(f) notification and controlled disclosure where required;

(g) evidence and closure.

15.3. A vulnerability assessment shall consider the possible effect on:

(a) Trust Service Provider Status, Trust Service Status and Service Permission;

(b) Trust Object Status and Validation;

(c) Source Status and Source Verification;

(d) mechanisms, devices and Authenticators;

(e) Technical Exchange Permission and Endpoint operation;

(f) Assurance, Conformity Assessment and Qualified Status;

(g) dependent Actors and Federation Domains.

15.4. A Responsible Actor shall apply an urgent restriction or compensating control where continued operation creates an unacceptable risk.

15.5. Vulnerability information shall be restricted where premature or unnecessary disclosure would increase the risk.

15.6. Closure shall require evidence that the assigned remediation or mitigation is effective within the affected scope.

15.7. A vulnerability that indicates actual or suspected compromise shall be handed to the process governed by IDEHA-IG-SEC-INC-001 without undue delay.

15.8. Vulnerability closure shall not, by itself, reinstate a Status, permission or Qualified Status affected by a separate Framework Decision.

Article 16: Security monitoring, logging and evidence

16.1. A Responsible Actor shall monitor the security state of the Controlled Matters and dependencies within its scope.

16.2. Monitoring shall address, where applicable:

(a) access and privileged activity;

(b) Authentication and Authorisation events;

(c) configuration and policy changes;

(d) Trust Service, Source, mechanism, device, Endpoint and Technical Exchange Route state;

(e) Confidentiality, Integrity and Authenticity control operation;

(f) vulnerability and remediation state;

(g) unusual, failed, repeated or unauthorised activity;

(h) dependency, Status and qualified-condition changes.

16.3. Logging shall be limited to information necessary and authorised for security, Accountability, evidence and error handling.

16.4. Logs and monitoring records shall not contain plaintext payload content, Digital Signature Creation Data, Authentication secrets or other Restricted Information beyond what is necessary and authorised for the assigned purpose.

16.5. Security logs and evidence shall preserve:

(a) trusted time and event sequence;

(b) Actor, service, mechanism, device or system attribution;

(c) the event and affected scope;

(d) Integrity and Authenticity;

(e) access controls;

(f) Version and configuration context;

(g) Retention and Historical State.

16.6. The applicable Profile shall identify the logs or evidence sets requiring an Electronic Seal, Electronic Timestamp or periodic evidence aggregation.

16.7. Monitoring and evidence shall support detection, assessment, Assurance, Conformity Assessment, Review, Remedy and Historical Validation.

16.8. A monitoring alert shall not, by itself, establish a Security Incident, Status change, non-conformity, fault or adverse finding against an Actor or person.

Article 17: Security Incident readiness and handoff

17.1. A Responsible Actor shall maintain readiness to detect, initially assess and hand off a suspected Security Incident to the process governed by IDEHA-IG-SEC-INC-001.

17.2. Readiness arrangements shall identify:

(a) detection sources and monitoring responsibilities;

(b) initial assessment and triage responsibilities;

(c) incident-classification and severity inputs;

(d) escalation, notification and contact routes;

(e) evidence-preservation requirements;

(f) affected-Actor and Federation Domain coordination routes;

(g) Protection-Sensitive Information and Security-Sensitive Information handling;

(h) the transition to containment, Continuity, Degraded Operation and Recovery.

17.3. A suspected-incident record shall identify:

(a) the known affected scope;

(b) the detection and occurrence times where known;

(c) the available evidence;

(d) the reporting source;

(e) the initial protective controls;

(f) the responsible handoff function.

17.4. A Responsible Actor shall preserve evidence before taking an action capable of destroying or materially altering that evidence, unless immediate action is necessary to prevent serious harm.

17.5. An incident-readiness exercise shall test:

(a) communication;

(b) escalation;

(c) evidence preservation;

(d) cross-Actor handoff;

(e) Federation Domain coordination.

17.6. An incident-readiness exercise shall not require unauthorised access to live Protected-Person data.

17.7. Detection or notification of a suspected Security Incident shall not, by itself, suspend or withdraw Trust Service Provider Status, Trust Service Status, Source Status, Trust Object Status, Qualified Status or Technical Exchange Permission.

17.8. Operational containment, Status evaluation, notification, Continuity, Degraded Operation, Recovery, reinstatement and closure shall be governed by IDEHA-IG-SEC-INC-001 and the applicable Framework Decision.

SECTION 5: ASSURANCE, EXCEPTIONS AND LIFECYCLE

Article 18: Security testing, Assurance and Conformity Assessment

18.1. A Responsible Actor shall test security and Confidentiality controls:

(a) before operational activation;

(b) after each material change affecting the assessed scope;

(c) at the interval required by the applicable Profile;

(d) following a material vulnerability or Security Incident where reassessment is required.

18.2. Testing shall address, where applicable:

(a) access and privileged-function controls;

(b) Authentication and Authorisation enforcement;

(c) Transport Confidentiality and Payload Confidentiality;

(d) storage and processing confidentiality;

(e) Integrity, Authenticity and object-level protection;

(f) protected functions and Security-Sensitive Information;

(g) configuration, supplier, dependency and change controls;

(h) monitoring, logging and evidence;

(i) vulnerability handling and incident handoff.

18.3. The test plan shall identify:

(a) the tested scope;

(b) the applicable Profile and Technical Specification Versions;

(c) the test environment;

(d) the methods and inputs;

(e) the expected results and acceptance criteria;

(f) the Responsible Actors;

(g) the required evidence.

18.4. Testing in an operational environment shall protect persons, live information, Trust Services, Sources, dependencies and ongoing Controlled Interactions from unauthorised effect.

18.5. A test result shall identify each limitation, deviation, unresolved finding and residual risk.

18.6. A material unresolved security non-conformity shall prevent positive Conformity Assessment or operational use within the affected scope until the applicable corrective, restriction or acceptance condition is satisfied.

18.7. Security Assurance and Conformity Assessment shall be implemented in accordance with IDEHA-IG-ASR-QLF-001 and the applicable Assurance or Qualified Profile.

18.8. Successful testing or positive Conformity Assessment shall not, by itself, assign Qualified Status, Service Permission, Technical Exchange Permission or Controlled Reliance.

Article 19: Security exceptions and temporary controls

19.1. A Responsible Actor shall use a security exception only where:

(a) the applicable requirement cannot be satisfied within the required time;

(b) the unresolved condition does not create an unacceptable risk;

(c) a time-limited remediation or transition plan is available.

19.2. A security-exception record shall identify:

(a) the affected requirement and Controlled Matter;

(b) the reason and evidence basis;

(c) the affected scope and persons;

(d) the risk and potential Controlled Effect;

(e) the compensating controls;

(f) the approving Actor;

(g) the Effective Date and expiry date;

(h) the monitoring and Review conditions;

(i) the remediation or transition plan;

(j) the incident-handoff condition.

19.3. A security exception shall be approved only by the Actor or Framework Body holding the applicable responsibility or Decision Competence.

19.4. An exception shall remain limited to the identified:

(a) scope;

(b) duration;

(c) Version;

(d) configuration.

19.5. An exception shall not:

(a) waive a Protected-Person Safeguard;

(b) create access or disclosure permission;

(c) extend Qualified Status;

(d) bypass a mandatory Framework Decision;

(e) permit continued operation where the residual risk is unacceptable.

19.6. The Responsible Actor shall withdraw the exception where the approval conditions cease to be satisfied or the residual risk becomes unacceptable.

19.7. Expiry, withdrawal or remediation of an exception shall be recorded and verified.

Article 20: Records, Review, Remedy and lifecycle

20.1. A Responsible Actor shall retain the security-governance, inventory, boundary, risk, classification, access, control, testing, vulnerability, monitoring, exception and readiness records required by the applicable Profile and Retention requirements.

20.2. Records shall preserve:

(a) Integrity;

(b) Authenticity;

(c) Provenance;

(d) Version;

(e) time;

(f) the responsible Actor;

(g) access controls;

(h) Historical State.

20.3. Records shall remain available to the authorised Framework Body, Conformity Assessment Body, Review function or Remedy function within the applicable scope.

20.4. A security record shall not disclose Protection-Sensitive Information or Security-Sensitive Information beyond the authorised purpose and requester scope.

20.5. A material security change shall follow the applicable Change Control, Versioning, transition and Historical State requirements.

20.6. Restriction, Suspension, Withdrawal or cessation of a Trust Service, Source, mechanism, device, Endpoint, Technical Exchange Route or dependency shall not remove continuing Confidentiality, evidence, Retention, Review, Remedy or historical-reconstruction obligations.

20.7. An affected Actor or person shall have access to the applicable Correction, Complaint, Review and Remedy Routes.

20.8. Review shall distinguish between:

(a) the security-risk or control evaluation;

(b) the technical test result;

(c) the Conformity Assessment Result;

(d) a Framework Decision or Status action;

(e) the Relying Actor's separate acceptance and Controlled Reliance decision.

20.9. Correction of a security record shall preserve the earlier record and identify the correcting Actor, reason, evidence, Effective Date and effect.

20.10. A Remedy shall apply only within the competence and affected scope identified by the applicable Review outcome and shall not create recognition, Status, permission or Qualified Status by implication.

Article 21: Reference standards and specifications

21.1. The reference standards applicable to the implementation of this Guideline are set out in Annex I.

21.2. A reference identified in Annex I shall apply only within the implementation function, subject and scope identified in that Annex.

21.3. The applicable Profile shall identify the controls selected from a referenced standard and their application to the relevant Controlled Matters, Controlled Environments and risks.

21.4. Exact algorithms, parameter sets, cryptographic mechanisms, protocol configurations, test conditions and product settings shall be established through the applicable Profile and Technical Specification.

21.5. Standards governed principally by the following Framework Instruments shall apply through those instruments and shall not be repeated in Annex I:

(a) cryptographic mechanisms, key management, cryptographic modules and post-quantum transition under IDEHA-IG-SEC-CRY-001;

(b) Security Incident response, Continuity and Recovery under IDEHA-IG-SEC-INC-001;

(c) Trust Service Provider common controls under IDEHA-IG-SVC-TSP-001;

(d) subject-specific Trust Service, Trust Object, Source and Technical Exchange requirements.

21.6. A later edition, amendment or replacement of a standard identified in Annex I shall not apply automatically.

21.7. A later edition, amendment or replacement shall undergo standards evaluation and Change Control before it is assigned Framework effect.

21.8. Conformity with a referenced standard shall constitute evidence only for the requirements and scope mapped to that reference.

21.9. Conformity with a referenced standard shall not, by itself, establish operational activation, Service Permission, Technical Exchange Permission, Authorisation, Qualified Status or Controlled Reliance.

ANNEX I: REFERENCE STANDARDS

Reference	Implementation function	Applicability and controlled treatment
ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, including ISO/IEC 27001:2022/Amd 1:2024	Information security management system	Applicable to establishment, implementation, maintenance and continual improvement of security governance. Certification shall be required only where the applicable Profile or qualification condition expressly requires it.
ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls	Information security control selection and implementation	Applicable as the principal horizontal control reference. The applicable Profile shall identify the controls selected, excluded or supplemented for the relevant scope.
ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks	Security risk assessment and treatment	Applicable to the risk-assessment, treatment, monitoring and reassessment processes governed by Article 6.
ISO/IEC 27701:2025, Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance	Privacy management for personal data	Applicable where the implementation processes personal data or maintains privacy-management responsibilities. It shall not create an access, disclosure or processing basis.
ISO/IEC 29100:2024, Information technology — Security techniques — Privacy framework	Privacy roles, principles and safeguarding considerations	Applicable as a supporting reference for classification, confidentiality, data minimisation, linkability and privacy-risk treatment. Part II terminology shall prevail where meanings differ.
ISO/IEC 27036-2:2022, Cybersecurity — Supplier relationships — Part 2: Requirements	Supplier and acquirer security requirements	Applicable to material supplier, outsourcing and supporting-Actor relationships governed by Article 7.
ISO/IEC 27036-3:2023, Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security	Supply-chain security	Applicable to acquisition, development, component, dependency and supply-chain controls governed by Articles 7 and 14.

Reference	Implementation function	Applicability and controlled treatment
ISO/IEC 27040:2024, Information technology — Security techniques — Storage security	Storage confidentiality, Integrity and lifecycle protection	Applicable where information, evidence, backups or cryptographic dependencies are stored in ICT storage environments.
ISO/IEC 27034-1:2011, Information technology — Security techniques — Application security — Part 1: Overview and concepts, including ISO/IEC 27034-1:2011/ Cor 1:2014	Application-security governance and secure development	Applicable to application acquisition, development, operation and retirement under Article 14. Exact technical controls shall remain Profile and Technical Specification matters.
ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	Cloud-service security controls	Conditionally applicable where a cloud service forms part of the implementation. A successor edition shall not apply until published, assessed and recognised through the standards-management route.
ISO/IEC 27018:2025, Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information in public clouds acting as PII processors	Protection of personal data in public-cloud processing	Conditionally applicable where a public-cloud provider processes personal data on behalf of a Responsible Actor. It shall be applied together with the applicable Profile, Authorisation and Confidentiality requirements.

IDEHA-IG-SEC-CRY-001: CRYPTOGRAPHIC CONTROLS AND CRYPTOGRAPHIC AGILITY IMPLEMENTATION

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Guideline lays down implementation requirements for cryptographic controls and cryptographic agility under the Framework.

1.2. This Guideline shall apply to each Responsible Actor, Framework Body, Trust Service Provider, Source Holder, Source Steward, Issuer, Technical Exchange Route Operator, Intermediary, supporting Actor and technical operator responsible for implementing, operating, assessing or relying upon cryptographic protection.

1.3. This Guideline shall govern, where applicable:

(a) cryptographic governance and responsibility;

(b) cryptographic inventories and dependency records;

(c) protection-lifetime and cryptographic-risk assessment;

(d) selection and controlled use of Recognised Standards and cryptographic mechanisms;

(e) algorithm and parameter identification;

(f) random-bit generation and entropy management;

(g) key, secret and cryptographic-material lifecycle management;

(h) cryptographic modules and protected execution environments;

(i) trust anchors and cryptographic Validation dependencies;

(j) cryptographic agility and transition readiness;

(k) algorithm restriction, deprecation, replacement and emergency transition;

(l) post-quantum migration;

(m) hybrid and composite cryptographic arrangements;

(n) cryptographic compromise handoff;

(o) testing, conformity evidence and Historical State.

1.4. This Guideline shall not:

(a) redefine Digital Signature Creation Data, Digital Signature Validation Data, Digital Signature Creation Mechanisms or Digital Signature Creation Devices;

(b) establish the conditions for an Electronic Signature, Electronic Seal, Electronic Timestamp, Certificate or Electronic Attestation;

(c) establish a Trust Service Category, Trust Object Category, Status category, qualification route or Controlled Effect;

(d) assign recognition, Service Permission, Technical Exchange Permission, Authorisation, Status or Qualified Status;

(e) prescribe exact algorithms, parameter sets, key lengths, encodings, protocol bindings, certificate extensions, signature formats, product configurations or test vectors;

(f) replace the security architecture established by the Main Framework and Annex H;

(g) replace operational Security Incident response, containment, notification, Continuity, Recovery, reinstatement or closure;

(h) treat the availability or use of a cryptographic mechanism as proof of Authorisation, lawfulness, correctness, acceptance or Controlled Reliance.

1.5. Digital Signature Creation Data, Digital Signature Creation Mechanisms and Digital Signature Creation Devices shall be implemented in accordance with IDEHA-IG-OBJ-DSG-001.

1.6. Horizontal security and Confidentiality controls shall be implemented in accordance with IDEHA-IG-SEC-CNF-001.

1.7. Operational response to cryptographic compromise shall be governed by IDEHA-IG-SEC-INC-001.

1.8. Assurance, Conformity Assessment and qualification evidence shall be governed by IDEHA-IG-ASR-QLF-001.

1.9. Compliance with this Guideline shall not, by itself, establish cryptographic suitability for an unidentified purpose, Qualified Status, operational activation, External Legal Status, External Legal Effect or permission for Controlled Reliance.

Article 2: Application through Schemes, Profiles and Technical Specifications

2.1. The applicable Scheme shall identify:

(a) the governed purpose and operational context;

(b) the participating Actors and Federation Domains;

(c) the Controlled Matters and interactions requiring cryptographic protection;

(d) the information and evidence protection periods;

(e) the consequences of cryptographic failure;

(f) the applicable safeguards, Review Routes and Remedy Routes.

2.2. The applicable Profile shall identify:

(a) the cryptographic functions required within its scope;

(b) the permitted mechanism and algorithm categories;

(c) the required security strength;

(d) the applicable protection lifetime;

(e) the permitted key and secret lifecycle models;

(f) the required module, mechanism or device assurance;

(g) the permitted backup, Recovery, escrow and replacement arrangements;

(h) the applicable agility and transition requirements;

(i) the post-quantum and hybrid requirements, where applicable;

(j) the required testing, evidence and reassessment conditions.

2.3. The applicable Technical Specification shall define:

(a) exact algorithms and parameter sets;

(b) key and output lengths;

(c) algorithm and parameter identifiers;

(d) key, signature, ciphertext and certificate representations;

(e) cryptographic container and protocol bindings;

(f) algorithm-negotiation behaviour;

(g) key-derivation, key-agreement and key-encapsulation constructions;

(h) hybrid and composite constructions;

(i) module and interface requirements;

(j) test vectors and conformance criteria;

(k) migration and interoperability behaviour.

2.4. A deployment instruction shall define environment-specific:

(a) cryptographic module configuration;

(b) key and trust-anchor locations;

(c) access and administration assignments;

(d) operational rotation schedules;

(e) monitoring settings;

(f) backup and Recovery procedures;

(g) emergency transition procedures.

2.5. A subject-specific Implementation Guideline shall identify only the additional cryptographic requirements required for its subject matter and shall not repeat the horizontal controls established by this Guideline.

2.6. A Scheme, Profile, Technical Specification, test result or deployment instruction shall not create a category, Status, permission, qualification route or Controlled Effect not established by the Main Framework.

Article 3: Cryptographic Implementation Plan

3.1. A Responsible Actor shall maintain an approved Cryptographic Implementation Plan for each implementation within its responsibility.

3.2. The Implementation Plan shall identify:

(a) the implementation and cryptographic scope;

(b) the Responsible Actors and supporting Actors;

(c) the applicable Scheme, Profile and Technical Specification Versions;

(d) the cryptographic functions and protected information;

(e) the protection lifetime and required security strength;

(f) the cryptographic inventory;

(g) the permitted cryptographic mechanisms;

(h) the key, secret and cryptographic-material lifecycle arrangements;

(i) the cryptographic modules, mechanisms, devices and Controlled Environments;

(j) the trust anchors and Validation dependencies;

(k) the cryptographic agility arrangements;

(l) the post-quantum migration arrangements;

(m) the permitted hybrid or composite arrangements;

(n) the monitoring, testing and evidence arrangements;

(o) the compromise, transition and incident-handoff arrangements;

(p) the Retention and Historical State requirements.

3.3. The Implementation Plan shall distinguish:

(a) cryptographic policy from technical implementation;

(b) a key or secret from the mechanism, device or module using it;

(c) cryptographic protection from Authorisation;

(d) encryption from disclosure permission;

(e) Integrity from Authenticity;

(f) key establishment from entity Authentication;

(g) algorithm support from permission to use that algorithm;

(h) technical Recovery from reinstatement of Status or permission;

(i) current algorithm acceptability from historical Validation acceptability.

3.4. The Responsible Actor shall approve the Implementation Plan before operational activation within the affected scope.

3.5. The Responsible Actor shall update the Implementation Plan following a material change affecting the cryptographic scope, protection lifetime, algorithm, parameter, key, module, device, trust anchor, protocol, dependency, transition plan or post-quantum risk.

3.6. Approval of the Implementation Plan shall not create Service Permission, Technical Exchange Permission, Qualified Status or permission for Controlled Reliance.

SECTION 2: CRYPTOGRAPHIC INVENTORY AND MECHANISM SELECTION

Article 4: Cryptographic inventory

4.1. A Responsible Actor shall maintain a cryptographic inventory covering each cryptographic asset, use and dependency within its scope.

4.2. The cryptographic inventory shall identify, where applicable:

(a) the Controlled Matter protected;

(b) the cryptographic function;

(c) the algorithm and parameter identifier;

(d) the key, secret or cryptographic-material category;

(e) the responsible and operating Actors;

(f) the cryptographic module, mechanism, device or software component;

(g) the applicable certificate, trust anchor or Validation dependency;

(h) the applicable protocol, format and Technical Specification Version;

(i) the information-protection lifetime;

(j) the key or secret validity and use period;

(k) the implementation and operational locations;

(l) each supporting Actor and external dependency;

(m) the current use classification;

(n) the replacement and migration route;

(o) the evidence and monitoring references.

4.3. The inventory shall include cryptographic use that is:

(a) directly implemented;

(b) embedded within a product or service;

(c) provided by a supporting Actor;

(d) inherited through a protocol, library, platform, module or device;

(e) used for archived or historically retained information;

(f) inactive but capable of reactivation.

4.4. The Responsible Actor shall identify each cryptographic dependency not under its direct control and the Actor responsible for its migration, replacement or withdrawal.

4.5. An unrecorded cryptographic mechanism shall not be used for a controlled production function unless an urgent exception has been approved under the applicable security-exception process.

4.6. The inventory shall be updated following:

(a) activation of a new cryptographic function;

(b) replacement or rotation;

(c) module, mechanism, device or software change;

(d) algorithm or parameter transition;

(e) certificate or trust-anchor change;

(f) identification of an unknown or inherited dependency;

(g) compromise, restriction or deprecation.

4.7. Inclusion in the inventory shall not establish recognition, approval, suitability, Status or permission to use the recorded mechanism.

Article 5: Protection lifetime and required security strength

5.1. Before selecting a cryptographic mechanism, the Responsible Actor shall determine the period during which the protected matter requires Confidentiality, Integrity, Authenticity, Accountability or evidential reliability.

5.2. The protection-lifetime assessment shall consider:

(a) the information sensitivity and classification;

(b) the expected Retention period;

(c) the period of intended Controlled Reliance;

(d) the expected lifecycle of the relevant system, mechanism or device;

(e) the time required to replace the implementation;

(f) the time required to migrate retained information and evidence;

(g) the expected cryptanalytic and technological threat horizon;

(h) the consequence of retrospective decryption, forgery or trust-anchor compromise;

(i) the need for Historical Validation.

5.3. The required security strength shall be sufficient for the complete protection lifetime and migration period.

5.4. A mechanism shall not be selected merely because it is currently interoperable where its expected security lifetime is shorter than the required protection period.

5.5. Long-lived Confidentiality requirements shall consider the risk that encrypted information may be collected and retained for later decryption.

5.6. Long-lived Authenticity and Integrity requirements shall consider the risk of future forgery affecting:

(a) trust anchors;

(b) Certificates;

(c) Electronic Signatures and Electronic Seals;

(d) Electronic Timestamps;

(e) Electronic Attestations;

(f) policy and configuration packages;

(g) preserved evidence.

5.7. The applicable Profile shall identify the required security-strength category and the date or condition by which migration shall be completed.

5.8. The protection-lifetime assessment shall be reviewed following a material change in cryptanalytic knowledge, implementation capability, standards status or threat assessment.

Article 6: Approved cryptographic mechanisms and controlled catalogue

6.1. A cryptographic mechanism shall be used for a controlled production function only where it is:

(a) identified in the Standards Register;

(b) permitted by the applicable Profile;

(c) implemented through the applicable Technical Specification;

(d) suitable for the required function, security strength and protection lifetime;

(e) supported by the required conformity and Validation evidence.

6.2. The Responsible Actor shall maintain or use a controlled cryptographic-mechanism catalogue.

6.3. The catalogue shall identify:

(a) the mechanism and algorithm identifier;

(b) the applicable standard and edition;

(c) the cryptographic function;

(d) the permitted parameter categories;

(e) the permitted implementation contexts;

(f) the minimum and maximum permitted use periods;

(g) each restriction and caveat;

(h) the predecessor and successor mechanisms;

(i) the transition and coexistence conditions;

(j) the testing and conformity requirements.

6.4. The catalogue shall distinguish mechanisms that are:

(a) permitted for new protection;

(b) permitted only for Verification or Historical Validation;

(c) restricted to an identified transitional scope;

(d) prohibited for new or continuing use;

(e) permitted only for testing or migration preparation.

6.5. A mechanism permitted for Verification or Historical Validation shall not thereby be permitted for new creation, encryption, signing, sealing, timestamping, Authentication or key establishment.

6.6. A mechanism shall not be represented as approved merely because it:

(a) is implemented by a product;

(b) is enabled by default;

(c) appears in a protocol negotiation;

(d) is included in a certificate or file format;

(e) has previously been used within the same Federation Domain.

6.7. A draft standard, candidate algorithm, experimental construction or vendor-defined mechanism shall not be used within a qualified or production scope unless the applicable Profile expressly permits controlled testing and excludes production reliance.

6.8. The Standards Register and cryptographic-mechanism catalogue shall preserve earlier use classifications and Effective Dates for Historical Validation.

Article 7: Algorithm identification, negotiation and downgrade protection

7.1. Each cryptographic operation shall identify the algorithm and parameter set used in a manner sufficient for deterministic Verification and Validation.

7.2. An algorithm identifier shall not rely on:

(a) an unstated default;

(b) an implementation-specific assumption;

(c) the ordering of an undocumented list;

(d) an ambiguous or reused identifier.

7.3. The applicable Technical Specification shall define:

(a) algorithm identifiers;

(b) parameter identifiers;

(c) identifier encoding;

(d) algorithm-agility fields;

(e) mandatory processing behaviour;

(f) unsupported-algorithm behaviour.

7.4. Algorithm negotiation shall:

(a) permit only mechanisms authorised by the applicable Profile;

(b) bind the selected mechanism to the protected interaction;

(c) prevent unauthorised substitution;

(d) prevent silent downgrade;

(e) produce evidence of the offered and selected mechanisms where material.

7.5. Failure to establish an authorised common mechanism shall result in secure failure and shall not trigger an undocumented fallback.

7.6. A legacy mechanism shall not be selected solely because a participating component does not support the required replacement mechanism.

7.7. Where coexistence is permitted, the applicable Profile shall identify:

(a) the permitted mechanism combinations;

(b) the affected Actors and systems;

(c) the beginning and end of the coexistence period;

(d) the required evidence;

(e) the final cutover condition.

7.8. Algorithm aliases, equivalent identifiers and external catalogue mappings shall be controlled and traceable to one authoritative mechanism entry.

SECTION 3: KEY, SECRET AND CRYPTOGRAPHIC-MODULE LIFECYCLE

Article 8: Generation, entropy and random-bit generation

8.1. A key, secret, nonce, seed or other random-dependent cryptographic value shall be generated using an approved random-bit generation arrangement.

8.2. The generation arrangement shall identify:

(a) the random-bit generator;

(b) the entropy source;

(c) the cryptographic module or environment;

(d) the health and failure tests;

(e) the responsible Actor;

(f) the applicable standard and Technical Specification;

(g) the evidence retained.

8.3. Generation shall provide the unpredictability and security strength required by the applicable Profile.

8.4. The Responsible Actor shall ensure that:

(a) entropy sources are appropriate to the operational environment;

(b) deterministic generators are correctly seeded and reseeded;

(c) generator state is protected;

(d) repeated or predictable output is detected where practicable;

(e) generator failure results in secure failure.

8.5. A virtualised, shared, remote or constrained environment shall be assessed for risks affecting entropy availability, generator state separation and output independence.

8.6. A generated key shall be subject to the required validity, structural and pairwise-consistency checks before use.

8.7. Generation evidence shall not disclose a private key, secret, seed or generator state.

8.8. A generation process that cannot establish the required entropy or generator condition shall not produce material represented as suitable for controlled use.

Article 9: Key establishment, provisioning, distribution and derivation

9.1. Key establishment, provisioning, distribution, agreement, encapsulation and derivation shall use mechanisms permitted by the applicable Profile and Technical Specification.

9.2. The applicable arrangement shall identify:

(a) the participating Actors and systems;

(b) the key or secret purpose;

(c) the originating and receiving environments;

(d) the Authentication and Authorisation conditions;

(e) the mechanism and parameter identifiers;

(f) the confirmation requirements;

(g) the protection and evidence requirements;

(h) the failure and retry behaviour.

9.3. A key or secret shall be bound to:

(a) its intended cryptographic function;

(b) its authorised Actor, system, service or device;

(c) its applicable scope;

(d) its permitted use period;

(e) its applicable algorithm and parameter set.

9.4. Key derivation shall identify:

(a) the input material;

(b) the derivation function;

(c) the context and purpose information;

(d) the output-key separation rules;

(e) the applicable Version.

9.5. Derived keys used for different functions, Actors, sessions, purposes or directions shall be cryptographically separated.

9.6. Key-distribution and key-establishment messages shall be protected against:

(a) unauthorised disclosure;

(b) substitution;

(c) replay;

(d) redirection;

(e) unknown-key-share conditions;

(f) unauthorised downgrade.

9.7. Where a key-encapsulation mechanism is used, the implementation shall apply the decapsulation-failure, key-confirmation and context-binding requirements assigned by the applicable Technical Specification.

9.8. A key or secret shall not be accepted merely because transport of the material succeeded.

Article 10: Storage, use, access, backup and Recovery

10.1. A key, secret or other cryptographic material shall be stored and used only within the Controlled Environment and purpose assigned by the applicable Profile.

10.2. Access shall be limited according to:

(a) the cryptographic function;

(b) the responsible Role;

(c) least privilege;

(d) separation of duties;

(e) the applicable activation and Authorisation conditions.

10.3. Private keys, secret keys, Digital Signature Creation Data, Authentication secrets and recovery material shall be protected against:

(a) unauthorised disclosure;

(b) extraction;

(c) duplication;

(d) substitution;

(e) unauthorised use;

(f) rollback to an earlier state.

10.4. Separate keys shall be used for materially different functions, including where applicable:

(a) Electronic Signature creation;

(b) Electronic Seal creation;

(c) Electronic Timestamp protection;

(d) Authentication;

(e) payload encryption;

(f) transport protection;

(g) policy or configuration-package protection;

(h) Humanitarian Trust List protection;

(i) Exchange Evidence protection.

10.5. A single key shall be used for more than one function only where the applicable Profile expressly permits that use and the risk, certificate, module and lifecycle conditions remain compatible.

10.6. Backup or Recovery of private or secret material shall be permitted only where:

(a) the applicable Profile permits it;

(b) equivalent or stronger protection is maintained;

(c) the authorised custody and access model is preserved;

(d) creation, access, restoration and destruction are evidenced.

10.7. A backup, escrow, reconstruction or Recovery arrangement shall not be used where it would defeat:

(a) the required control of Digital Signature Creation Data;

(b) the non-exportability requirement of an Authenticator or device;

(c) the assigned qualified condition;

(d) the required separation of duties.

10.8. Recovery of technical access to a key or secret shall not, by itself, reinstate a Status, permission, Certificate, Authenticator or Trust Service.

10.9. Plaintext key material shall not be recorded in operational logs, monitoring data, evidence records or support tickets.

Article 11: Rotation, replacement, restriction, Revocation and destruction

11.1. A Responsible Actor shall define lifecycle conditions for each key, secret, certificate-dependent key pair and trust anchor.

11.2. Lifecycle conditions shall identify:

(a) generation or provisioning;

(b) activation;

(c) permitted use;

(d) rotation or renewal;

(e) restriction or Suspension;

(f) Revocation;

(g) replacement;

(h) expiry;

(i) destruction;

(j) preservation of non-secret evidence.

11.3. Rotation and replacement shall occur before:

(a) the permitted use period ends;

(b) the mechanism becomes unsuitable;

(c) the required security strength is no longer met;

(d) a dependency expires or is withdrawn;

(e) continued use creates an unacceptable risk.

11.4. Replacement shall preserve the relationship between:

(a) the earlier and replacement keys;

(b) the applicable Certificates;

(c) the affected mechanisms, devices and Trust Services;

(d) the Effective Dates;

(e) the affected historical evidence.

11.5. Restriction, Suspension or Revocation shall prevent further use within the affected scope from the applicable Effective Date.

11.6. A revoked, destroyed or rendered-unusable private key, secret or Digital Signature Creation Data shall not be reactivated.

11.7. Secure destruction shall:

(a) apply to each active, backup, cached, replicated and recoverable copy;

(b) address residual material in modules, memory, storage and support systems;

(c) be verified;

(d) produce evidence without preserving the destroyed secret.

11.8. Destruction of secret material shall not destroy the public, Status, lifecycle and evidence information required for Historical Validation.

Article 12: Cryptographic modules, mechanisms and protected environments

12.1. A cryptographic module, mechanism, device or protected execution environment shall be selected according to:

(a) the cryptographic function;

(b) the sensitivity of the protected material;

(c) the required security strength;

(d) the operational environment;

(e) the applicable Assurance and qualified conditions.

12.2. The implementation record shall identify:

(a) the module, mechanism, device or environment;

(b) the security boundary;

(c) the hardware, firmware and software Versions;

(d) the approved configuration;

(e) the supported cryptographic mechanisms;

(f) the assigned keys, secrets and functions;

(g) the conformity or certification evidence;

(h) the operational and lifecycle restrictions.

12.3. A cryptographic module shall maintain:

(a) role and service separation;

(b) authorised activation;

(c) protection of critical security parameters;

(d) approved-state control;

(e) self-tests and error handling;

(f) secure update and configuration control;

(g) evidence of material security events.

12.4. A failed self-test, Integrity check or approved-state condition shall result in secure failure within the affected function.

12.5. A software implementation outside a certified cryptographic module shall require the risk, protection and testing evidence assigned by the applicable Profile.

12.6. Certification of a cryptographic module shall not, by itself:

(a) qualify a Digital Signature Creation Device;

(b) qualify a Trust Service;

(c) qualify a Trust Service Provider;

(d) establish the suitability of every supported mechanism;

(e) assign Qualified Status to an output.

12.7. Qualified Digital Signature Creation Devices and their minimum assurance requirements shall be governed by IDEHA-IG-OBJ-DSG-001.

12.8. A material change to a cryptographic module, mechanism, device, firmware, software, configuration or operating environment shall undergo Change Control and reassessment before continued use within the earlier assessed scope.

Article 13: Trust anchors, Certificates and Validation dependencies

13.1. A Responsible Actor shall maintain a controlled record of each trust anchor and cryptographic Validation dependency within its scope.

13.2. The record shall identify:

(a) the trust anchor or dependency;

(b) the responsible Actor;

(c) the permitted purpose and scope;

(d) the algorithm and parameter identifiers;

(e) the applicable Certificate or public-key information;

(f) the activation and expiry times;

(g) the Status and publication source;

(h) the predecessor and successor relationship;

(i) the distribution and update method;

(j) the Historical State requirements.

13.3. Trust-anchor distribution and update packages shall be protected against unauthorised modification and substitution.

13.4. A trust anchor shall be accepted only for the purpose, scope, Federation Domain, Profile and period assigned to it.

13.5. Replacement or rollover shall preserve:

(a) continuity of Validation;

(b) predecessor and successor relationships;

(c) overlap or transition conditions;

(d) protection against unauthorised substitution;

(e) historical evidence.

13.6. Removal of a trust anchor from current use shall not remove the information required to validate earlier Certificates, Trust Objects, Trust Service Outputs or evidence.

13.7. A Certificate, Humanitarian Trust List Entry or trust-anchor record shall not be accepted solely because its cryptographic protection verifies.

13.8. Validation shall also establish the applicable Status, scope, time, policy, dependency and Historical State.

SECTION 4: CRYPTOGRAPHIC AGILITY AND POST-QUANTUM TRANSITION

Article 14: Cryptographic agility

14.1. A Responsible Actor shall implement cryptographic agility proportionate to the scale, criticality, protection lifetime and replacement complexity of the implementation.

14.2. Cryptographic agility shall enable controlled replacement or adaptation of:

(a) algorithms;

(b) parameter sets;

(c) keys and secrets;

(d) certificates and trust anchors;

(e) modules, mechanisms and devices;

(f) protocols and cryptographic containers;

(g) cryptographic libraries and interfaces;

(h) Validation rules.

14.3. The implementation shall avoid unnecessary hard-coding of:

(a) algorithm identifiers;

(b) parameter sets;

(c) key lengths;

(d) certificate profiles;

(e) trust anchors;

(f) permitted mechanism lists.

14.4. Agility controls shall include, where applicable:

(a) machine-processable mechanism catalogues;

(b) configurable permitted-mechanism lists;

(c) explicit Version and algorithm identifiers;

(d) modular cryptographic interfaces;

(e) controlled negotiation;

(f) dual-operation and coexistence capability;

(g) migration and rollback testing;

(h) visibility of current cryptographic use;

(i) removal of prohibited mechanisms.

14.5. Cryptographic agility shall not permit an unauthorised component, administrator, peer or downgrade process to select a weaker mechanism.

14.6. An agility mechanism shall fail securely where the selected cryptographic configuration is not authorised or cannot be validated.

14.7. Agility shall preserve interoperability only within the conditions authorised by the applicable Profile and Technical Specification.

14.8. A capability to support several algorithms shall not create permission to use every supported algorithm.

Article 15: Restriction, deprecation and cryptographic transition

15.1. A Responsible Actor shall maintain a transition plan for each mechanism expected to become unsuitable before the end of the implementation or protection lifetime.

15.2. The transition plan shall identify:

(a) the current and replacement mechanisms;

(b) the affected keys, Certificates, systems, Trust Services, Trust Objects and dependencies;

(c) the reason and evidence basis;

(d) the target architecture;

(e) the migration sequence;

(f) the coexistence period;

(g) the testing and conformity requirements;

(h) the Effective Dates;

(i) the final end of permitted use;

(j) the rollback and emergency conditions;

(k) the historical-evidence treatment.

15.3. Restriction or deprecation shall identify whether the affected mechanism remains permitted for:

(a) new protection;

(b) existing protected information;

(c) Verification;

(d) Historical Validation;

(e) migration processing;

(f) controlled testing.

15.4. A transition shall prevent:

(a) silent downgrade;

(b) unplanned fallback;

(c) reuse of revoked or retired material;

(d) loss of historical Validation evidence;

(e) reintroduction of a prohibited mechanism through a dependency.

15.5. Where re-protection is required, the migration record shall preserve:

(a) the original protected matter;

(b) the original cryptographic evidence;

(c) the migration action;

(d) the replacement protection;

(e) the responsible Actor;

(f) the migration time.

15.6. Emergency restriction may take effect before completion of ordinary transition activities where continued use creates an unacceptable risk.

15.7. Emergency technical restriction shall not, by itself, alter governance Status, Service Permission, Qualified Status or the validity of an earlier Trust Object.

Article 16: Quantum-risk assessment and migration planning

16.1. A Responsible Actor shall assess the effect of quantum computing on each public-key cryptographic dependency within its scope.

16.2. The assessment shall consider:

(a) the information-protection lifetime;

(b) the time required to replace systems, devices, protocols and dependencies;

(c) the time required to migrate retained data and evidence;

(d) the time required to obtain confidence, interoperability and conformity evidence for replacement mechanisms;

(e) the risk of retrospective decryption;

(f) the risk of future signature or trust-anchor forgery;

(g) the effect on qualified and historically relied-upon matters;

(h) supplier and cross-domain dependencies.

16.3. The quantum-risk record shall identify:

(a) the affected cryptographic asset or process;

(b) the current quantum-vulnerable mechanism;

(c) the protected matter and required protection period;

(d) the migration priority;

(e) the target mechanism category;

(f) the responsible Actor;

(g) the target completion date;

(h) the dependencies and blockers;

(i) the required testing and evidence.

16.4. The migration plan shall address:

(a) inventory completion;

(b) target-state definition;

(c) pilot and interoperability testing;

(d) certificate, key and trust-anchor transition;

(e) module, mechanism and device availability;

(f) protocol and format transition;

(g) hybrid or coexistence arrangements where required;

(h) Validation and Historical State;

(i) final removal of quantum-vulnerable mechanisms.

16.5. A long-lived Confidentiality use shall be prioritised where the protected information may remain sensitive after a cryptographically relevant quantum capability could become available.

16.6. A long-lived trust anchor, archival signature or evidence-protection use shall be prioritised where future forgery could invalidate or undermine retained evidence.

16.7. A draft, candidate or non-standardised post-quantum mechanism shall not be used for production or qualified protection merely because migration urgency exists.

Article 17: Post-quantum and hybrid cryptographic arrangements

17.1. A post-quantum mechanism shall be used only where:

(a) it is identified in the Standards Register;

(b) the applicable Profile permits its use;

(c) the applicable Technical Specification defines its integration;

(d) the required module, certificate, format, protocol and Validation support exists;

(e) the required testing and conformity evidence is available.

17.2. A hybrid or composite arrangement shall identify:

(a) each component mechanism;

(b) the function of each component;

(c) the combination rule;

(d) the key and lifecycle relationship;

(e) the security property intended to be preserved;

(f) the Validation rule;

(g) the downgrade and failure behaviour;

(h) the transition and retirement condition.

17.3. A hybrid arrangement shall not be constructed through an undocumented or ad hoc combination of algorithms.

17.4. The applicable Technical Specification shall establish whether successful Validation requires:

(a) every component mechanism to validate;

(b) an identified minimum set of component mechanisms to validate;

(c) another formally defined combination rule.

17.5. A component key shall not be reused across unrelated hybrid arrangements where that reuse would create unintended dependency, Revocation or compromise propagation.

17.6. The implementation shall bind the component algorithms, keys, ciphertexts or signatures to the same cryptographic context and protected matter.

17.7. Hybrid negotiation shall be protected against downgrade to:

(a) a traditional-only mechanism;

(b) an unauthorised post-quantum mechanism;

(c) an incomplete component set;

(d) a weaker parameter set.

17.8. Hybrid operation shall preserve separately identifiable evidence for each component mechanism and the combined result.

17.9. Compromise, restriction or failure of one component shall be evaluated according to the documented combination rule and shall not be concealed by the successful operation of another component.

17.10. A hybrid arrangement shall be removed when its transitional or risk-reduction purpose no longer applies and the applicable Profile requires migration to a post-quantum-only arrangement.

Article 18: Cryptographic compromise and incident handoff

18.1. Compromise or suspected compromise of a key, secret, random-bit generator, cryptographic module, trust anchor, algorithm implementation or protected cryptographic process shall be treated as a Security Incident.

18.2. The Responsible Actor shall identify without undue delay:

(a) the affected cryptographic material and mechanism;

(b) the known or suspected compromise period;

(c) the affected systems, Trust Services, Sources, Trust Objects, outputs and interactions;

(d) the affected Certificates and trust anchors;

(e) the affected protection and Validation functions;

(f) the required restriction, rotation, replacement, Revocation or destruction action;

(g) the required notification and incident handoff;

(h) the effect on Historical State.

18.3. Immediate cryptographic containment may include:

(a) prevention of further use;

(b) removal from permitted-mechanism lists;

(c) key or certificate Revocation;

(d) trust-anchor restriction;

(e) algorithm-negotiation restriction;

(f) activation of a replacement mechanism.

18.4. Technical containment shall not, by itself, assign or alter Status, Qualified Status, Service Permission or Technical Exchange Permission.

18.5. The effect on an earlier Trust Object, Trust Service Output, Certificate, interaction or evidence record shall be determined according to:

(a) the relevant creation or issuance time;

(b) the known affected period;

(c) the cryptographic evidence;

(d) the applicable Status and Historical State;

(e) the applicable Profile.

18.6. Recovery of a cryptographic function shall not automatically reinstate an earlier Status, permission, qualified condition or trust-anchor acceptance.

18.7. Operational containment, notification, Continuity, Recovery, reinstatement and closure shall proceed under IDEHA-IG-SEC-INC-001.

SECTION 5: ASSURANCE, EVIDENCE AND STANDARDS

Article 19: Testing, Assurance and Conformity Assessment

19.1. Cryptographic controls shall be tested:

(a) before operational activation;

(b) following a material cryptographic change;

(c) before and during a cryptographic transition;

(d) at the interval required by the applicable Profile;

(e) following a material vulnerability or Security Incident where reassessment is required.

19.2. Testing shall address, where applicable:

(a) algorithm and parameter processing;

(b) random-bit generation;

(c) key generation and establishment;

(d) key separation and use restrictions;

(e) module approved-state operation;

(f) self-tests and error handling;

(g) certificate and trust-anchor processing;

(h) algorithm negotiation and downgrade resistance;

(i) rotation, replacement and Revocation;

(j) backup, Recovery and destruction;

(k) hybrid and post-quantum processing;

(l) interoperability and Historical Validation.

19.3. The test plan shall identify:

(a) the tested scope;

(b) the applicable Profile and Technical Specification Versions;

(c) the algorithms and parameter sets;

(d) the module, mechanism, device or software Version;

(e) the methods, inputs and expected results;

(f) the acceptance criteria;

(g) the Responsible Actors;

(h) the evidence retained.

19.4. Testing shall include negative and failure cases sufficient to demonstrate secure failure.

19.5. Known-answer, pairwise-consistency, entropy, health, interoperability and migration tests shall be performed where required by the applicable standard or Profile.

19.6. A material unresolved cryptographic non-conformity shall prevent operational use within the affected scope.

19.7. Module, mechanism, device and implementation certification shall be accepted only within the evaluated configuration and certification scope.

19.8. Successful cryptographic testing or certification shall not, by itself, establish:

(a) the suitability of the mechanism for every use;

(b) Qualified Status;

(c) Service Permission;

(d) Technical Exchange Permission;

(e) Authorisation;

(f) Controlled Reliance.

19.9. Assurance and Conformity Assessment shall be implemented in accordance with IDEHA-IG-ASR-QLF-001.

Article 20: Records and Historical State

20.1. A Responsible Actor shall retain records sufficient to reconstruct cryptographic protection and lifecycle conditions within the applicable scope.

20.2. Records shall include, where applicable:

(a) the Cryptographic Implementation Plan;

(b) the cryptographic inventory;

(c) protection-lifetime and risk assessments;

(d) mechanism-catalogue entries;

(e) algorithm and parameter identifiers;

(f) generation and entropy evidence;

(g) key establishment, provisioning and derivation evidence;

(h) module, mechanism, device and configuration evidence;

(i) trust-anchor and Certificate dependencies;

(j) rotation, replacement, restriction, Revocation and destruction records;

(k) transition and migration records;

(l) post-quantum and hybrid-arrangement records;

(m) testing and Conformity Assessment evidence;

(n) compromise and incident-handoff records.

20.3. Cryptographic records shall not contain secret material beyond what is strictly necessary and authorised for the assigned function.

20.4. Historical State shall preserve, where required:

(a) the algorithm and parameter set;

(b) the applicable standard and Technical Specification Version;

(c) the key, Certificate and trust-anchor Status;

(d) the module, mechanism, device and configuration;

(e) the use and protection periods;

(f) the applicable mechanism use classification;

(g) the Validation rules applicable at the relevant time.

20.5. A mechanism prohibited for new use may remain available in an isolated Validation environment where required to validate historical evidence.

20.6. A historical Validation environment shall prevent the prohibited mechanism from being used for new protection.

20.7. Correction of a cryptographic record shall preserve:

(a) the earlier record;

(b) the correction basis;

(c) the responsible Actor;

(d) the Effective Date;

(e) the affected scope.

20.8. A later mechanism, parameter, certificate, trust anchor or Validation rule shall not silently replace the Historical State applicable to an earlier protected matter.

Article 21: Reference standards and technical references

21.1. The reference standards and technical references applicable to the implementation of this Guideline are set out in Annex I.

21.2. A reference identified in Annex I shall apply only within the implementation function, scope and condition identified in that Annex.

21.3. The applicable Profile and Technical Specification shall select the exact mechanism, parameter set, identifier, format, protocol integration and test condition.

21.4. Subject-specific standards for Electronic Signatures, Electronic Seals, Electronic Timestamps, Certificates, Electronic Attestations, Authentication, Technical Exchange and Digital Signature Creation Devices shall apply through their respective Framework Instruments and shall not be repeated in Annex I.

21.5. A later edition, amendment or replacement of a reference identified in Annex I shall not apply automatically.

21.6. A later edition, amendment or replacement shall undergo standards evaluation and Change Control before it is assigned Framework effect.

21.7. Conformity with a reference standard or technical reference shall constitute evidence only for the requirements and scope mapped to that reference.

21.8. Conformity with a reference shall not, by itself, establish operational activation, Service Permission, Technical Exchange Permission, Authorisation, Qualified Status or Controlled Reliance.

ANNEX I: REFERENCE STANDARDS AND TECHNICAL REFERENCES

Reference	Implementation function	Applicability and controlled treatment
ETSI TS 119 312 V2.1.1, 2026-06, Electronic Signatures and Trust Infrastructures — Cryptographic Suites	Cryptographic suites for Electronic Signatures, Electronic Seals, Certificates, Electronic Timestamps and related Trust Services	Mandatory within its applicable subject scope. Exact suites and parameters shall be selected through the applicable Profile and Technical Specification.
ETSI TS 119 322 V1.2.1, 2024-12, Electronic Signatures and Trust Infrastructure — Schema for machine-readable cryptographic algorithms and cipher-suite catalogues	Machine-processable cryptographic-mechanism catalogue	Applicable where the cryptographic-mechanism catalogue is distributed or processed in machine-readable form.
ECCG Agreed Cryptographic Mechanisms, Version 2.0, April 2025	Current European technical reference for agreed cryptographic mechanisms used in evaluated ICT products	Applicable as the recognised mechanism-selection baseline where the applicable Profile requires alignment with European cybersecurity certification practice. Draft Version 3 shall not apply until formally adopted and recognised through the standards-management route.
ISO/IEC 11770-1:2010, Information technology — Security techniques — Key management — Part 1: Framework	General key-management framework and lifecycle model	Mandatory as the horizontal key-management reference. Subject-specific mechanisms shall be selected from the applicable further parts or another Recognised Standard.
ISO/IEC 11770-2:2018, IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques	Symmetric-key establishment mechanisms	Conditionally applicable where symmetric key-establishment mechanisms are selected.
ISO/IEC 11770-3:2021, including ISO/IEC 11770-3:2021/Amd 1:2025, Information security — Key management — Part 3: Mechanisms using asymmetric techniques	Asymmetric key agreement, transport and establishment	Conditionally applicable where the selected mechanism falls within its scope. Exact mechanism selection remains a Profile and Technical Specification matter.
ISO/IEC 11770-5:2020, Information security — Key management — Part 5: Group key management	Group-key establishment and rekeying	Conditionally applicable where a controlled group-key arrangement is selected.
ISO/IEC 11770-6:2016, Information technology — Security techniques — Key	Key-derivation functions	Applicable where keys are derived from secret input material. Context and purpose separation

Reference	Implementation function	Applicability and controlled treatment
management — Part 6: Key derivation		shall be defined by the applicable Technical Specification.
ISO/IEC 18031:2025, Information technology — Security techniques — Random bit generation	Random-bit generation model and security requirements	Mandatory for random-bit generation used in controlled cryptographic functions unless the applicable Profile selects an equivalent recognised standard.
ISO/IEC 20543:2019, Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408	Random-bit generator testing and analysis	Applicable where independent random-bit generator testing is required.
ISO/IEC 19790:2025, Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules	Cryptographic-module security requirements	Mandatory where a Profile requires an evaluated cryptographic module. The required security level and configuration shall be selected by the applicable Profile.
ISO/IEC 24759:2025, Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules	Cryptographic-module conformity testing	Mandatory together with ISO/IEC 19790:2025 where module testing under that framework is required.
ISO/IEC 17825:2024, Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	Testing of resistance to non-invasive attacks	Conditionally applicable where side-channel and related non-invasive attack resistance is required by the applicable Profile.
NIST FIPS 203, 2024, Module-Lattice-Based Key-Encapsulation Mechanism Standard	Post-quantum key encapsulation using ML-KEM	Conditionally applicable where a post-quantum key-encapsulation mechanism is selected. The parameter set and protocol integration shall be defined by the applicable Profile and Technical Specification.
NIST FIPS 204, 2024, Module-Lattice-Based Digital Signature Standard	Post-quantum Digital Signatures using ML-DSA	Conditionally applicable where a post-quantum Digital Signature mechanism is selected and the applicable Certificate, format, device and Validation support is available.
NIST FIPS 205, 2024, Stateless Hash-Based Digital Signature Standard	Post-quantum Digital Signatures using SLH-DSA	Conditionally applicable where a stateless hash-based Digital Signature mechanism is selected and the applicable Certificate,

Reference	Implementation function	Applicability and controlled treatment
		format, device and Validation support is available.
NIST SP 800-227, 2025, Recommendations for Key-Encapsulation Mechanisms	Secure implementation and use of key-encapsulation mechanisms	Applicable where a key-encapsulation mechanism, including ML-KEM, is used.
NIST CSWP 39-upd1, 2026, Considerations for Achieving Crypto Agility: Strategies and Practices	Cryptographic-agility planning and implementation	Applicable as supporting guidance for Article 14 and cryptographic-transition planning.
ETSI TR 103 619 V1.1.1, 2020-07, Migration strategies and recommendations to Quantum Safe schemes	Quantum-safe inventory, migration planning and execution	Applicable as supporting guidance for the migration process governed by Article 16.
ETSI TR 104 016 V1.1.1, 2024-10, Quantum-Safe Cryptography — A Repeatable Framework for Quantum-Safe Migrations	Repeatable quantum-safe migration framework	Applicable as supporting guidance for planning, prioritisation and execution of quantum-safe migration.
ETSI TR 103 966 V1.1.1, 2024-10, Quantum-Safe Cryptography — Deployment Considerations for Hybrid Schemes	Design and deployment considerations for traditional and post-quantum hybrid schemes	Applicable as supporting guidance where a hybrid arrangement is permitted under Article 17.

IDEHA-IG-SEC-INC-001: SECURITY INCIDENT, CONTINUITY AND RECOVERY IMPLEMENTATION

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Guideline lays down implementation requirements for Security Incident readiness, assessment, response, Continuity, Degraded Operation, Recovery and post-incident improvement under the Framework.

1.2. This Guideline shall apply to each Responsible Actor, Framework Body, Trust Service Provider, Source Holder, Source Steward, Issuer, Relying Actor, Technical Exchange Route Operator, Intermediary, supporting Actor and technical operator responsible for a Controlled Matter, Controlled Environment, Trust Service, Source, Trust Object, Trust Service Output, mechanism, device, Authenticator, Endpoint, Technical Exchange Route, Register, Catalogue or Humanitarian Trust List component.

1.3. This Guideline shall govern, where applicable:

(a) Security Incident readiness;

(b) detection and initial assessment;

(c) incident classification;

(d) incident coordination and escalation;

(e) evidence preservation;

(f) containment and corrective action;

(g) notification and communication;

(h) Continuity arrangements;

(i) Degraded Operation;

(j) Recovery and restoration;

(k) reinstatement support;

(l) post-incident Review and improvement.

1.4. This Guideline shall not:

(a) redefine Security Incident, Continuity, Degraded Operation, Recovery, Reinstatement, Status, Suspension, Withdrawal, Revocation or Controlled Effects established by the Main Framework;

(b) replace preventive security controls established by IDEHA-IG-SEC-CNF-001;

(c) replace cryptographic controls established by IDEHA-IG-SEC-CRY-001;

(d) assign Status, Qualified Status, Service Permission, Technical Exchange Permission, Authorisation or Controlled Reliance;

(e) determine the legal consequences of a Security Incident;

(f) replace a Framework Decision required for restriction, Suspension, Withdrawal, Revocation, reinstatement or qualification action;

(g) prescribe exact technical response tools, forensic products, communication platforms, protocol bindings or recovery technologies.

1.5. Security controls, cryptographic controls, access controls, confidentiality controls and vulnerability controls shall continue to apply during Security Incident response, Degraded Operation and Recovery unless a formally approved exception applies.

1.6. Compliance with this Guideline shall not, by itself, establish a Security Incident classification, Status change, qualification action, Remedy outcome or permission for Controlled Reliance.

Article 2: Application through Schemes, Profiles and Technical Specifications

2.1. The applicable Scheme shall identify:

(a) the governed operational context;

(b) the participating Actors;

(c) the affected Federation Domains;

(d) the applicable Review Routes and Remedy Routes;

(e) the coordination and notification expectations.

2.2. The applicable Security Incident, Continuity and Recovery Profile shall identify:

(a) incident categories and severity conditions;

(b) Responsible Actors;

(c) notification thresholds;

(d) evidence requirements;

(e) coordination arrangements;

(f) Degraded Operation conditions;

(g) Recovery objectives;

(h) restoration conditions;

(i) reinstatement evidence;

(j) testing and exercise requirements;

(k) historical reconstruction requirements.

2.3. The applicable Technical Specification shall define:

(a) technical monitoring interfaces;

(b) event formats;

(c) notification formats;

(d) communication protocols;

(e) recovery automation interfaces;

(f) technical test procedures.

2.4. Subject-specific Implementation Guidelines shall establish additional incident, Continuity and Recovery requirements only where required by their subject matter.

2.5. A Security Incident process, technical event, monitoring alert, continuity action or recovery activity shall not create a Framework Decision, Status change, Authorisation or Controlled Effect.

Article 3: Security Incident and Continuity Implementation Plan

3.1. A Responsible Actor shall maintain a Security Incident and Continuity Implementation Plan for each Controlled Matter within its responsibility.

3.2. The Implementation Plan shall identify:

(a) the scope of the plan;

(b) Responsible Actors;

(c) supporting Actors;

(d) Security Incident roles;

(e) communication and escalation routes;

(f) affected Controlled Matters;

(g) dependencies;

(h) evidence sources;

(i) detection and monitoring arrangements;

(j) initial assessment procedures;

(k) containment procedures;

(l) Continuity arrangements;

(m) Degraded Operation conditions;

(n) Recovery procedures;

(o) reinstatement support;

(p) testing and exercise arrangements;

(q) Review and improvement processes.

3.3. The Implementation Plan shall distinguish:

(a) preventive security controls from incident response;

(b) an operational event from a Security Incident;

(c) technical containment from Status restriction;

(d) Recovery from reinstatement;

(e) reinstatement support from a Framework Decision;

(f) incident evidence from substantive business records;

(g) availability restoration from Controlled Reliance restoration.

3.4. The Responsible Actor shall review and update the Implementation Plan following:

(a) a material Security Incident;

(b) a material dependency change;

(c) a material architectural change;

(d) a major exercise result;

(e) a material vulnerability.

3.5. Approval of an Implementation Plan shall not create a right to continue operation where mandatory security, Status, permission or qualified conditions are not satisfied.

SECTION 2: INCIDENT READINESS AND ASSESSMENT

Article 4: Incident readiness

4.1. A Responsible Actor shall maintain readiness to detect, assess, coordinate and respond to Security Incidents affecting its scope.

4.2. Readiness arrangements shall identify:

(a) incident detection sources;

(b) monitoring responsibilities;

(c) incident contacts;

(d) escalation routes;

(e) evidence-preservation responsibilities;

(f) affected-Actor communication routes;

(g) decision and approval routes;

(h) external coordination requirements where applicable.

4.3. The Responsible Actor shall maintain current contact information for:

(a) internal incident functions;

(b) supporting Actors;

(c) affected Framework Bodies;

(d) Conformity Assessment Bodies where required;

(e) other Actors identified by the applicable Profile.

4.4. Incident-readiness arrangements shall consider:

(a) Trust Services;

(b) Sources;

(c) Trust Objects;

(d) Trust Service Outputs;

(e) Humanitarian Trust List information;

(f) Endpoints;

(g) Technical Exchange Routes;

(h) cryptographic dependencies;

(i) protected functions;

(j) Protected-Person Safeguards.

4.5. Incident-readiness exercises shall verify:

(a) communication;

(b) escalation;

(c) evidence preservation;

(d) coordination;

(e) Continuity;

(f) Recovery;

(g) reinstatement support.

4.6. Exercise results shall identify:

(a) scope;

(b) date;

(c) participants;

(d) findings;

(e) corrective actions;

(f) responsible Actor;

(g) completion date.

Article 5: Detection and initial assessment

5.1. A Responsible Actor shall assess detected events to determine whether they may constitute a Security Incident.

5.2. Initial assessment shall identify:

(a) affected Controlled Matter;

(b) affected Actor;

(c) affected system, service, Source, Trust Object, Endpoint or dependency;

(d) detection source;

(e) occurrence time where known;

(f) detection time;

(g) available evidence;

(h) potential Confidentiality, Integrity, Authenticity, Availability or Accountability impact;

(i) required immediate protective measures.

5.3. An event shall remain distinguishable from a Security Incident until sufficient information exists to classify it.

5.4. Lack of complete information shall not prevent protective action where delay may increase harm.

5.5. Initial assessment shall not:

(a) assign Status;

(b) establish liability;

(c) determine legal effect;

(d) determine Remedy outcome.

5.6. Where an event cannot be ruled out as a Security Incident, the Responsible Actor shall apply the protective and coordination measures required by the applicable Profile.

Article 6: Incident classification

6.1. A Responsible Actor shall classify Security Incidents according to the applicable Incident Profile.

6.2. Classification shall consider:

(a) affected Controlled Matters;

(b) affected persons;

(c) affected Actors;

(d) Confidentiality impact;

(e) Integrity impact;

(f) Authenticity impact;

(g) Availability impact;

(h) Accountability impact;

(i) geographic or Federation Domain scope;

(j) duration;

(k) dependency impact;

(l) potential effect on Status, Qualification or Controlled Reliance.

6.3. Incident severity shall identify:

(a) classification basis;

(b) evidence supporting classification;

(c) affected scope;

(d) required response level;

(e) notification obligations.

6.4. Incident severity shall be reviewed where new evidence materially changes the assessed impact.

6.5. Classification shall not automatically result in:

(a) Suspension;

(b) Withdrawal;

(c) Revocation;

(d) Status change;

(e) Remedy outcome.

Those actions require the applicable Framework process.

SECTION 3: INCIDENT RESPONSE AND COORDINATION

Article 7: Incident response roles and coordination

7.1. A Responsible Actor shall assign incident-response roles.

7.2. Incident-response roles shall identify:

(a) incident coordinator;

(b) technical responders;

(c) evidence-preservation function;

(d) communication function;

(e) Framework coordination function;

(f) Recovery coordination function.

7.3. Roles shall remain separate from Framework Decision Competence unless expressly assigned.

7.4. A technical responder shall not acquire Decision Competence merely by controlling technical recovery.

7.5. A Framework Body shall be notified where the incident may affect:

(a) Status;

(b) Qualified Status;

(c) Service Permission;

(d) Technical Exchange Permission;

(e) Humanitarian Trust List publication;

(f) Controlled Reliance.

Article 8: Evidence preservation

8.1. A Responsible Actor shall preserve evidence necessary to understand, assess, respond to and review a Security Incident.

8.2. Evidence preservation shall identify:

(a) affected systems and Controlled Matters;

(b) relevant times;

(c) event records;

(d) configuration state;

(e) access records;

(f) authentication records;

(g) cryptographic evidence;

(h) dependency information;

(i) response actions.

8.3. Evidence shall preserve:

(a) Integrity;

(b) Authenticity;

(c) provenance;

(d) access history;

(e) time information;

(f) chain of custody where applicable.

8.4. Evidence preservation shall avoid unnecessary collection of personal data or Protected-Person Information.

8.5. Evidence shall be protected against:

(a) unauthorised access;

(b) alteration;

(c) deletion;

(d) disclosure.

8.6. Incident evidence shall remain separate from:

(a) substantive Source records;

(b) Trust Objects;

(c) Trust Service Outputs;

(d) Authorisation Outcomes.

Article 9: Containment and corrective action

9.1. A Responsible Actor shall implement containment measures appropriate to the incident scope and risk.

9.2. Containment measures may include:

(a) isolation;

(b) restriction of access;

(c) credential restriction;

(d) key or certificate restriction;

(e) Endpoint restriction;

(f) Technical Exchange Route restriction;

(g) service restriction;

(h) temporary processing limitation.

9.3. Containment shall preserve evidence required for:

(a) Review;

(b) Remedy;

(c) Assurance;

(d) Conformity Assessment;

(e) Historical State.

9.4. Corrective actions shall identify:

(a) affected scope;

(b) root cause where determined;

(c) correction performed;

(d) responsible Actor;

(e) verification method;

(f) completion date;

(g) remaining risks.

9.5. Containment or corrective action shall not:

(a) create Authorisation;

(b) create Status;

(c) reinstate Qualified Status;

(d) replace a Framework Decision.

Article 10: Notification and communication

10.1. A Responsible Actor shall notify the Actors and Framework Bodies identified by the applicable Incident Profile.

10.2. Notification shall identify, where applicable:

(a) incident identifier;

(b) affected scope;

(c) classification;

(d) known impact;

(e) protective measures;

(f) required actions;

(g) communication contact;

(h) update schedule.

10.3. Notification shall contain sufficient information for coordination while protecting:

(a) Security-Sensitive Information;

(b) Protection-Sensitive Information;

(c) personal data;

(d) operationally sensitive information.

10.4. Notification shall not disclose information beyond the recipient's authorised purpose and scope.

10.5. A notification shall be corrected where new material information changes:

(a) impact;

(b) affected scope;

(c) required action;

(d) Recovery conditions.

SECTION 4: CONTINUITY, DEGRADED OPERATION AND RECOVERY

Article 11: Continuity arrangements

11.1. A Responsible Actor shall maintain Continuity arrangements for each critical Controlled Matter.

11.2. Continuity arrangements shall identify:

(a) critical functions;

(b) Recovery objectives;

(c) dependencies;

(d) alternative operating conditions;

(e) responsible Actors;

(f) communication routes;

(g) evidence preservation requirements.

11.3. Continuity arrangements shall consider:

(a) Trust Services;

(b) Sources;

(c) Trust Objects;

(d) Technical Exchange Routes;

(e) Humanitarian Trust List availability;

(f) cryptographic dependencies;

(g) supporting Actors.

11.4. A Continuity arrangement shall not bypass:

(a) Authorisation;

(b) Confidentiality;

(c) Integrity;

(d) Authenticity;

(e) required Status checks;

(f) qualified conditions.

Article 12: Degraded Operation

12.1. A Responsible Actor may operate in Degraded Operation only where:

(a) the condition is identified by the applicable Profile;

(b) the residual risk is assessed;

(c) the permitted scope is defined;

(d) responsible approval is obtained;

(e) monitoring remains active.

12.2. Degraded Operation shall identify:

(a) permitted functions;

(b) prohibited functions;

(c) affected Actors;

(d) duration;

(e) compensating controls;

(f) exit conditions.

12.3. Degraded Operation shall not permit:

(a) unauthorised disclosure;

(b) bypass of Authorisation;

(c) bypass of payload protection;

(d) creation of unvalidated Trust Objects;

(e) unrecorded privileged actions.

12.4. Degraded Operation records shall identify all actions performed during the degraded period.

12.5. A Degraded Operation condition shall end when:

(a) normal operation is restored; or

(b) the permitted period expires; or

(c) risk exceeds the approved condition.

Article 13: Recovery and restoration

13.1. Recovery shall restore affected functions according to the applicable Recovery Plan.

13.2. Recovery shall verify:

(a) system Integrity;

(b) configuration correctness;

(c) dependency availability;

(d) security-control operation;

(e) monitoring capability;

(f) evidence availability.

13.3. Recovery shall not restore:

(a) expired Status;

(b) revoked credentials;

(c) withdrawn Trust Services;

(d) removed permissions.

13.4. Before return to normal operation, the Responsible Actor shall verify:

(a) security conditions;

(b) Authorisation conditions;

(c) dependency conditions;

(d) operational readiness;

(e) evidence continuity.

13.5. Restoration shall be recorded.

SECTION 5: REASSESSMENT, IMPROVEMENT AND LIFECYCLE

Article 14: Reassessment and reinstatement support

14.1. A Responsible Actor shall determine whether reassessment is required following a Security Incident.

14.2. Reassessment shall be considered where the incident affects:

(a) Assurance conditions;

(b) Conformity Assessment scope;

(c) Qualified Scope;

(d) Security boundary;

(e) cryptographic protection;

(f) Trust Service operation;

(g) Source reliability;

(h) Technical Exchange Permission.

14.3. Reassessment evidence shall identify:

(a) incident reference;

(b) affected scope;

(c) corrective actions;

(d) verification performed;

(e) remaining risks;

(f) required decisions.

14.4. A Responsible Actor seeking reinstatement of an affected Status or permission shall submit evidence according to the applicable Framework process.

14.5. Recovery completion, technical correction or incident closure shall not automatically reinstate:

(a) Service Permission;

(b) Technical Exchange Permission;

(c) Status;

(d) Qualified Status;

(e) Controlled Reliance.

14.6. Reinstatement shall occur only through the applicable Framework Decision or lifecycle process.

Article 15: Post-incident review and improvement

15.1. A Responsible Actor shall conduct a post-incident Review following each material Security Incident.

15.2. The Review shall consider:

(a) detection effectiveness;

(b) assessment accuracy;

(c) response effectiveness;

(d) evidence handling;

(e) communication effectiveness;

(f) Continuity performance;

(g) Recovery performance;

(h) dependency performance;

(i) control effectiveness;

(j) required improvements.

15.3. The Review record shall identify:

(a) lessons learned;

(b) corrective actions;

(c) responsible Actor;

(d) completion date;

(e) verification method.

15.4. Improvements shall be incorporated into:

(a) security controls;

(b) risk assessments;

(c) Implementation Plans;

(d) Continuity arrangements;

(e) training and exercises;

(f) Profiles or Technical Specifications where required.

15.5. A post-incident Review shall not replace a Complaint, Review Route or Remedy Route available to affected persons or Actors.

Article 16: Records and Historical State

16.1. A Responsible Actor shall retain records sufficient to reconstruct the Security Incident lifecycle.

16.2. Records shall include, where applicable:

(a) detection records;

(b) initial assessment;

(c) classification;

(d) evidence preservation;

(e) coordination records;

(f) notification records;

(g) containment actions;

(h) Continuity actions;

(i) Degraded Operation records;

(j) Recovery actions;

(k) reassessment evidence;

(l) reinstatement support;

(m) post-incident Review.

16.3. Records shall preserve:

(a) Integrity;

(b) Authenticity;

(c) provenance;

(d) access history;

(e) relevant time information;

(f) affected scope.

16.4. Records shall remain protected against unauthorised alteration, disclosure and deletion.

16.5. Historical State shall remain reconstructable for:

(a) Validation;

(b) Assurance;

(c) Conformity Assessment;

(d) supervision;

(e) Review;

(f) Remedy;

(g) Controlled Reliance.

16.6. Correction of an incident record shall preserve:

(a) the earlier record;

(b) correction basis;

(c) responsible Actor;

(d) Effective Date;

(e) affected scope.

Article 17: Reference standards and specifications

17.1. The reference standards applicable to this Guideline are set out in Annex I.

17.2. A reference identified in Annex I shall apply only within the implementation function and scope identified in that Annex.

17.3. Exact incident tools, communication protocols, recovery automation interfaces and technical procedures shall be defined through the applicable Profile and Technical Specification.

17.4. Security governance, security controls and cryptographic controls shall apply through IDEHA-IG-SEC-CNF-001 and IDEHA-IG-SEC-CRY-001.

17.5. A later edition, amendment or replacement of a reference identified in Annex I shall not apply automatically.

17.6. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that reference.

17.7. Conformity with a referenced standard shall not, by itself, establish Security Incident classification, Status change, qualification action, Service Permission, Technical Exchange Permission or Controlled Reliance.

ANNEX I: REFERENCE STANDARDS

Reference	Implementation function	Applicability and controlled treatment
ISO/IEC 27035-1:2023, Information security incident management — Part 1: Principles and process	Security Incident management principles	Applicable as the principal Security Incident management reference.
ISO/IEC 27035-2:2016, Information security incident management — Part 2: Guidelines to plan and prepare for incident response	Incident preparedness and planning	Applicable for readiness, roles, procedures and response preparation.
ISO/IEC 27035-3:2020, Information security incident management — Part 3: Guidelines for ICT incident response operations	ICT incident response operations	Applicable for technical incident response activities.
ISO/IEC 27031:2025, Cybersecurity — ICT readiness for business continuity	ICT continuity and recovery readiness	Applicable for ICT continuity planning, recovery capability and restoration readiness.

Reference	Implementation function	Applicability and controlled treatment
ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements	Business continuity management	Applicable where a formal business continuity management system is implemented or required by the applicable Profile.
ISO 22320:2018, Security and resilience — Emergency management — Requirements for incident response	Incident-response coordination	Applicable where multi-Actor emergency coordination arrangements are required.
ISO 22361:2022, Security and resilience — Crisis management — Guidance	Crisis-management guidance	Applicable as supporting guidance for significant cross-domain incidents.
ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls	Security controls supporting incident prevention, detection and response	Applied through IDEHA-IG-SEC-CNF-001. Repeated controls shall not be duplicated here.
ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks	Risk reassessment after incidents	Applicable for post-incident risk reassessment and improvement.
ISO 19011:2018, Guidelines for auditing management systems	Post-incident review and audit methods	Applicable where formal audit activities are performed.

IDEHA-IG-GOV-SUP-001: SUPERVISION AND CORRECTIVE ACTION IMPLEMENTATION

Article 1: Subject matter and scope

1.1. This Guideline lays down implementation requirements for supervisory activities, compliance monitoring, findings management, corrective action and follow-up verification under the Framework.

1.2. This Guideline shall apply to Framework Bodies, supervisory functions, Responsible Actors, Trust Service Providers, Source Holders, Source Stewards, Issuers, Conformity Assessment Bodies, supporting Actors and other Actors subject to supervision under the applicable Framework Instrument.

1.3. This Guideline shall govern, where applicable:

(a) supervisory planning;

(b) supervisory scope definition;

(c) evidence requests and evidence review;

(d) supervisory activities and monitoring;

(e) findings identification and classification;

(f) corrective action planning;

(g) remediation monitoring;

(h) escalation recommendations;

(i) closure verification;

(j) supervisory records and Historical State.

1.4. This Guideline shall not:

(a) establish Framework governance roles;

(b) assign Decision Competence;

(c) create supervisory authority;

(d) assign Status, Qualified Status, Service Permission or Technical Exchange Permission;

(e) determine sanctions, legal consequences or External Legal Effect;

(f) replace Assurance evaluation, Conformity Assessment or qualification processes;

(g) replace Security Incident response;

(h) replace Complaint, Review or Remedy Routes.

1.5. Supervision shall operate within the competence, scope and authority established by the Main Framework and applicable Annexes.

1.6. A supervisory activity, finding, corrective action or recommendation shall not, by itself, create a Framework Decision or Controlled Effect.

Article 2: Supervision planning and scope

2.1. A supervisory function shall maintain a supervision plan for each supervised scope.

2.2. The supervision plan shall identify:

(a) the supervised Actor;

(b) the supervised Controlled Matters;

(c) the applicable Framework Instruments;

(d) the applicable Profiles and Versions;

(e) the supervisory objectives;

(f) the supervision frequency;

(g) the supervisory methods;

(h) the evidence requirements;

(i) the reporting arrangements;

(j) the escalation conditions;

(k) the follow-up arrangements.

2.3. The supervision plan shall consider:

(a) the nature and criticality of the supervised Service, Source, Trust Object, Trust Service Output or dependency;

(b) the applicable Assurance Conditions;

(c) previous findings;

(d) Security Incidents;

(e) material changes;

(f) dependency risks;

(g) complaints, Review outcomes and Remedy outcomes where relevant.

2.4. Supervision scope shall identify separately:

(a) Trust Service Provider;

(b) individual Trust Service;

(c) Source;

(d) Trust Object or Trust Service Output;

(e) mechanism or device;

(f) Endpoint or Technical Exchange Route;

(g) supporting Actor.

2.5. Supervision of a Trust Service Provider shall not automatically constitute supervision of each Trust Service operated by that Provider.

2.6. Supervision of one Trust Service shall not automatically establish compliance of another Trust Service.

2.7. The supervision plan shall be reviewed following:

(a) material change;

(b) repeated findings;

(c) Security Incident;

(d) significant dependency failure;

(e) change in applicable Framework requirements.

Article 3: Supervisory methods

3.1. Supervisory activities may include:

(a) document review;

(b) evidence review;

(c) interviews;

(d) inspection;

(e) observation;

(f) technical verification;

(g) sampling;

(h) remote assessment;

(i) onsite activity where required.

3.2. The supervisory function shall select methods proportionate to:

(a) the supervised scope;

(b) the risk;

(c) the applicable Assurance Conditions;

(d) previous findings;

(e) available evidence.

3.3. Supervisory methods shall identify:

(a) purpose;

(b) scope;

(c) evidence examined;

(d) responsible supervisory function;

(e) date and duration;

(f) limitations.

3.4. Remote supervisory methods may be used where they provide sufficient evidence for the supervisory objective.

3.5. A supervisory function shall not infer compliance solely from:

(a) absence of complaints;

(b) absence of known incidents;

(c) existence of certification;

(d) existence of a previous positive finding.

3.6. A supervisory activity shall remain separate from:

(a) Conformity Assessment;

(b) qualification decision;

(c) Status assignment;

(d) Remedy decision.

Article 4: Supervisory evidence

4.1. A supervised Actor shall provide evidence necessary for the supervisory activity within the applicable scope.

4.2. Evidence provided for supervision shall identify:

(a) the source;

(b) responsible Actor;

(c) creation time;

(d) Version;

(e) applicable scope;

(f) Integrity and Authenticity information where required.

4.3. The supervisory function shall evaluate:

(a) relevance;

(b) completeness;

(c) reliability;

(d) consistency;

(e) applicability period.

4.4. Evidence shall be protected against:

(a) unauthorised access;

(b) alteration;

(c) deletion;

(d) disclosure.

4.5. The supervisory function shall limit collection of information to what is necessary for the supervisory purpose.

4.6. Protection-Sensitive Information and Security-Sensitive Information shall be handled according to the applicable Security Conditions.

4.7. Evidence used for supervision shall remain attributable to its originating Actor.

4.8. A supervisory function shall not become the owner of evidence solely because it reviews or stores that evidence.

Article 5: Supervisory findings

5.1. A supervisory function shall record findings identified during supervision.

5.2. A finding shall identify:

(a) supervised Actor;

(b) affected Controlled Matter;

(c) applicable requirement;

(d) evidence basis;

(e) observation;

(f) impact;

(g) severity;

(h) required action;

(i) responsible Actor;

(j) due date.

5.3. Findings may include:

(a) conformity confirmation;

(b) observation;

(c) improvement opportunity;

(d) non-conformity;

(e) material non-conformity.

5.4. A finding shall distinguish between:

(a) evidence;

(b) supervisory evaluation;

(c) recommended action;

(d) Framework Decision requiring separate competence.

5.5. A finding shall not:

(a) assign Status;

(b) withdraw Status;

(c) suspend Service Permission;

(d) create liability;

(e) determine Remedy.

Article 6: Non-conformity management

6.1. A non-conformity shall identify the failed requirement and affected scope.

6.2. A non-conformity record shall include:

(a) requirement reference;

(b) affected Actor;

(c) affected Controlled Matter;

(d) evidence basis;

(e) impact assessment;

(f) corrective action requirement;

(g) completion deadline;

(h) verification method.

6.3. A material non-conformity shall be escalated where it may affect:

(a) Qualified Status;

(b) Service Permission;

(c) Technical Exchange Permission;

(d) Source Status;

(e) Trust Object reliance;

(f) Protected-Person Safeguards.

6.4. A non-conformity shall remain open until:

(a) corrective action is completed;

(b) evidence is provided;

(c) verification is performed;

(d) closure is recorded.

6.5. A supervised Actor shall not close its own non-conformity without the required independent verification where applicable.

6.6. Closure of a non-conformity shall not automatically restore:

(a) Status;

(b) Qualified Status;

(c) Service Permission;

(d) Technical Exchange Permission.

Article 7: Corrective action plans

7.1. Where corrective action is required, the responsible Actor shall prepare a corrective action plan.

7.2. The corrective action plan shall identify:

(a) identified deficiency;

(b) root cause where applicable;

(c) corrective action;

(d) responsible Actor;

(e) implementation date;

(f) verification evidence;

(g) residual risk;

(h) preventive improvement.

7.3. Corrective action shall address both:

(a) immediate correction;

(b) prevention of recurrence.

7.4. The supervisory function shall evaluate whether the proposed corrective action is proportionate to:

(a) the finding;

(b) the risk;

(c) the affected scope;

(d) the potential impact.

7.5. A corrective action plan shall not replace:

(a) incident response;

(b) Conformity Assessment;

(c) qualification reassessment;

(d) Framework Decision.

Article 8: Follow-up verification

8.1. A supervisory function shall verify completion of corrective actions according to the corrective action plan.

8.2. Verification shall determine:

(a) completion;

(b) evidence sufficiency;

(c) effectiveness;

(d) remaining risks;

(e) need for additional action.

8.3. Follow-up verification shall identify:

(a) verification date;

(b) verified scope;

(c) evidence examined;

(d) verification method;

(e) conclusion.

8.4. Where corrective action is insufficient, the supervisory function shall:

(a) maintain the finding;

(b) require additional corrective action;

(c) escalate according to competence.

8.5. Repeated or systemic findings shall trigger supervisory review of:

(a) risk;

(b) supervision frequency;

(c) need for escalation;

(d) need for reassessment.

Article 9: Escalation and recommendations

9.1. A supervisory function shall escalate matters where:

(a) corrective action is not completed;

(b) repeated findings occur;

(c) a material risk remains;

(d) Qualified Conditions may no longer be satisfied;

(e) Protected-Person Safeguards may be affected.

9.2. Escalation information shall identify:

(a) affected scope;

(b) evidence basis;

(c) supervisory findings;

(d) corrective action history;

(e) recommended next steps.

9.3. Recommendations shall remain separate from Framework Decisions.

9.4. The competent Framework Body shall determine any action requiring Decision Competence.

9.5. A supervisory function shall not:

(a) assign Status;

(b) revoke Status;

(c) suspend Status;

(d) create a qualification decision.

Article 10: Supervision of material changes

10.1. A supervised Actor shall notify material changes affecting the supervised scope where required by the applicable Framework Instrument.

10.2. Material changes may include:

(a) organisational changes;

(b) Service Scope changes;

(c) Source changes;

(d) technical architecture changes;

(e) cryptographic changes;

(f) dependency changes;

(g) security boundary changes;

(h) qualification-impacting changes.

10.3. The supervisory function shall determine whether:

(a) additional supervision is required;

(b) reassessment is required;

(c) corrective action is required;

(d) escalation is required.

10.4. A material change shall not automatically alter Status or Qualified Status.

Article 11: Supervisory records

11.1. A supervisory function shall maintain records sufficient to reconstruct supervisory activities.

11.2. Records shall include:

(a) supervision plans;

(b) evidence requests;

(c) evidence received;

(d) supervisory activities;

(e) findings;

(f) corrective action plans;

(g) verification results;

(h) escalation records;

(i) closure decisions.

11.3. Records shall preserve:

(a) Integrity;

(b) Authenticity;

(c) provenance;

(d) Version;

(e) time;

(f) responsible Actor.

11.4. Supervisory records shall remain available for:

(a) Review;

(b) Remedy;

(c) Assurance;

(d) Conformity Assessment;

(e) Historical State determination.

11.5. Correction of supervisory records shall preserve:

(a) previous record;

(b) correction basis;

(c) responsible Actor;

(d) Effective Date

Article 12: Reference standards and specifications

12.1. The reference standards applicable to this Guideline are set out in Annex I.

12.2. Standards shall apply only within the implementation function identified in Annex I.

12.3. Exact supervisory methods, evidence formats and reporting structures may be established through applicable Profiles and Technical Specifications.

12.4. Conformity with a referenced standard shall not create:

(a) supervisory authority;

(b) Status;

(c) Qualified Status;

(d) Controlled Effects.

ANNEX I: REFERENCE STANDARDS

Reference	Implementation function	Applicability
ISO 19011:2018, Guidelines for auditing management systems	Supervisory audit methods	Applicable as guidance for planning, conducting and documenting supervisory reviews.
ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems	Management-system audit competence where supervisory activities use such methods	Applicable only where management-system audit functions are performed.
ISO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services	Certification relationship distinction	Applicable only to distinguish certification activities from supervision.
ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks	Risk-based supervisory planning	Applicable where supervision evaluates security-risk treatment.
ISO/IEC 27001:2022, Information security management systems — Requirements	Security-management evidence review	Applicable where supervised Actors operate an information security management system.
ISO/IEC 27701:2025, Privacy information management systems	Privacy-management supervision	Applicable where supervision includes personal-data processing controls.

IDEHA-IG-RMR-GEN-001: PROTECTED-PERSON SAFEGUARDS, COMPLAINT, CORRECTION, REVIEW AND REMEDY IMPLEMENTATION

Article 1: Subject matter and scope

1.1. This Guideline lays down implementation requirements for Protected-Person Safeguards, accessibility, complaint handling, correction requests, Review Routes and Remedy Routes under the Framework.

1.2. This Guideline shall apply to each Framework Body, Responsible Actor, Trust Service Provider, Source Holder, Source Steward, Issuer, Relying Actor, supporting Actor and technical operator whose implementation affects a Protected Person.

1.3. This Guideline shall govern, where applicable:

(a) safeguard implementation planning;

(b) accessibility and Accessible Alternatives;

(c) non-exclusion measures;

(d) adverse-effect assessment;

(e) complaint intake and handling;

(f) correction requests;

(g) Review Route implementation;

(h) Remedy Route implementation;

(i) affected-person communication;

(j) records, evidence and improvement.

1.4. This Guideline shall not:

(a) create rights, obligations, entitlements or legal remedies beyond those established by the Main Framework;

(b) replace judicial, administrative or external legal procedures;

(c) assign Decision Competence;

(d) determine Status, Qualified Status, Service Permission or Technical Exchange Permission;

(e) replace Security Incident response;

(f) replace supervision, Assurance, Conformity Assessment or qualification processes;

(g) determine compensation, sanctions or external legal consequences.

1.5. Compliance with this Guideline shall not, by itself, establish a Remedy outcome, Framework Decision, External Legal Status, External Legal Effect or permission for Controlled Reliance.

Article 2: Application through Schemes, Profiles and Technical Specifications

2.1. The applicable Scheme shall identify:

(a) the affected persons and operational context;

(b) the participating Actors;

(c) the relevant services, Sources, Trust Objects or Trust Service Outputs;

(d) the applicable safeguards;

(e) the Review and Remedy arrangements.

2.2. The applicable Profile shall identify:

(a) the Protected-Person Safeguards applicable to the implementation;

(b) accessibility requirements;

(c) Accessible Alternatives;

(d) non-exclusion measures;

(e) adverse-effect assessment requirements;

(f) communication requirements;

(g) complaint and correction processes;

(h) Review Route conditions;

(i) Remedy Route conditions;

(j) evidence and record requirements.

2.3. The applicable Technical Specification shall define:

(a) accessibility interfaces;

(b) communication formats;

(c) technical support mechanisms;

(d) accessibility testing requirements;

(e) technical implementation details.

2.4. A safeguard, accessibility measure, complaint, correction, Review or Remedy process shall not modify:

(a) Trust Service Categories;

(b) Trust Object Categories;

(c) Status;

(d) Qualified Status;

(e) Decision Competence;

(f) Controlled Effects.

Article 3: Safeguard Implementation Plan

3.1. A Responsible Actor shall maintain a Protected-Person Safeguard Implementation Plan where its implementation may affect Protected Persons.

3.2. The Implementation Plan shall identify:

(a) affected persons and groups;

(b) affected services, Sources, Trust Objects or Trust Service Outputs;

(c) potential adverse effects;

(d) accessibility requirements;

(e) Accessible Alternatives;

(f) communication arrangements;

(g) complaint and correction routes;

(h) Review Routes;

(i) Remedy Routes;

(j) responsible Actors;

(k) monitoring and improvement arrangements.

3.3. The Implementation Plan shall distinguish:

(a) accessibility from identity verification;

(b) assistance from representation;

(c) complaint handling from Security Incident response;

(d) correction from modification of authoritative records;

(e) Review from supervision;

(f) Remedy from qualification or Status decisions.

3.4. The Responsible Actor shall review the Implementation Plan following:

(a) material service changes;

(b) adverse-effect findings;

(c) repeated complaints;

(d) accessibility failures;

(e) material changes affecting Protected Persons.

3.5. Approval of a Safeguard Implementation Plan shall not create access, entitlement, Status or Authorisation.

Article 4: Accessibility requirements

4.1. A Responsible Actor shall implement accessibility measures appropriate to the affected service, Source, Trust Object, Trust Service Output or interaction.

4.2. Accessibility measures shall consider:

(a) different communication needs;

(b) different levels of digital capability;

(c) assistive technology compatibility;

(d) language and communication barriers;

(e) temporary or permanent limitations affecting interaction;

(f) environmental and operational constraints.

4.3. Accessibility requirements shall be proportionate to:

(a) the purpose of the implementation;

(b) the potential adverse effect;

(c) the available safeguards;

(d) the operational context.

4.4. A lack of accessibility shall not result in unnecessary exclusion where a lawful and secure alternative interaction method can be provided.

4.5. Accessibility measures shall preserve applicable:

(a) Security Conditions;

(b) Assurance Conditions;

(c) Integrity requirements;

(d) Authenticity requirements.

Article 5: Accessible Alternatives

5.1. Where a primary interaction method may create exclusion, the Responsible Actor shall provide an Accessible Alternative where required by the applicable Profile.

5.2. An Accessible Alternative may include:

(a) assisted interaction;

(b) alternative communication channels;

(c) human-supported processes;

(d) alternative verification methods;

(e) alternative presentation formats;

(f) additional support mechanisms.

5.3. An Accessible Alternative shall identify:

(a) the applicable service function;

(b) the alternative process;

(c) the responsible Actor;

(d) the security conditions;

(e) the evidence requirements;

(f) the limitations.

5.4. An Accessible Alternative shall not:

(a) reduce mandatory safeguards;

(b) create an unauthorised exception;

(c) transfer responsibility to the Protected Person.

5.5. The use of an Accessible Alternative shall be recorded where required for Accountability, Review or Remedy.

Article 6: Non-exclusion implementation

6.1. A Responsible Actor shall assess whether an implementation may exclude a Protected Person from accessing a lawful service, exercising a Framework right or using an available interaction route.

6.2. The assessment shall consider:

(a) accessibility barriers;

(b) identity and Authentication barriers;

(c) geographic or infrastructure limitations;

(d) language barriers;

(e) economic or operational constraints;

(f) security measures creating disproportionate exclusion.

6.3. Where a risk of exclusion is identified, the Responsible Actor shall:

(a) assess alternatives;

(b) implement mitigation where appropriate;

(c) document the decision;

(d) monitor the outcome.

6.4. A security requirement shall not be removed solely to avoid exclusion where the requirement protects a necessary Assurance or Security Condition.

6.5. A Responsible Actor shall seek proportionate solutions preserving both:

(a) inclusion;

(b) trust and security requirements.

Article 7: Adverse-effect assessment

7.1. A Responsible Actor shall perform an adverse-effect assessment where an implementation may materially affect a Protected Person.

7.2. The assessment shall identify:

(a) affected persons;

(b) affected service or process;

(c) potential adverse effects;

(d) causes and contributing factors;

(e) existing safeguards;

(f) mitigation measures;

(g) responsible Actor;

(h) review date.

7.3. Adverse effects may include:

(a) exclusion;

(b) inability to access a service;

(c) incorrect identity association;

(d) incorrect Attribute use;

(e) inability to correct information;

(f) inability to exercise a Review or Remedy Route.

7.4. The Responsible Actor shall document the assessment outcome.

7.5. The assessment shall not determine legal liability or external legal effect.

Article 8: Adverse-effect mitigation

8.1. Where adverse effects are identified, the Responsible Actor shall implement proportionate mitigation.

8.2. Mitigation may include:

(a) Accessible Alternatives;

(b) additional human review;

(c) correction procedures;

(d) improved communication;

(e) additional verification;

(f) process modification.

8.3. Mitigation shall identify:

(a) responsible Actor;

(b) implementation date;

(c) evidence;

(d) effectiveness review.

8.4. Repeated adverse effects shall trigger review of:

(a) service design;

(b) Profile requirements;

(c) operational procedures;

(d) safeguards.

Article 9: Complaint intake

9.1. A Responsible Actor shall provide a Complaint Route accessible to affected persons.

9.2. The Complaint Route shall identify:

(a) submission method;

(b) required information;

(c) communication method;

(d) expected response time;

(e) responsible function.

9.3. A complaint shall identify, where available:

(a) complainant reference;

(b) affected service or process;

(c) issue description;

(d) supporting information;

(e) requested outcome.

9.4. A Responsible Actor shall provide reasonable assistance where a person cannot independently submit a complaint.

9.5. A complaint shall not require unnecessary disclosure of personal or sensitive information.

Article 10: Complaint assessment and handlin

10.1. A Responsible Actor shall assess each complaint within the applicable scope.

10.2. Assessment shall determine:

(a) subject matter;

(b) affected Controlled Matter;

(c) responsible Actor;

(d) applicable process;

(e) required action.

10.3. A complaint shall be classified as:

(a) information request;

(b) correction request;

(c) Review request;

(d) Remedy request;

(e) another applicable category.

10.4. The Responsible Actor shall communicate:

(a) acknowledgement;

(b) assessment result;

(c) required next steps;

(d) outcome or escalation.

10.5. Complaint handling shall preserve:

(a) confidentiality;

(b) Integrity;

(c) evidence;

(d) Accountability.

Article 11: Correction requests

11.1. A Responsible Actor shall provide a Correction Route where inaccurate, incomplete or outdated information affects a Protected Person.

11.2. A Correction Route shall distinguish:

(a) correction of an operational record;

(b) correction of a derived record;

(c) correction request to an authoritative Source;

(d) correction of a Trust Object or Trust Service Output.

11.3. A Responsible Actor shall not modify an authoritative Source record unless authorised to do so.

11.4. A correction request shall identify:

(a) affected information;

(b) requested correction;

(c) evidence supporting the request;

(d) responsible Actor.

11.5. A correction decision shall identify:

(a) action taken;

(b) evidence considered;

(c) Effective Date;

(d) limitations.

11.6. Historical records shall remain identifiable where required for Accountability, Validation or Remedy.

Article 12: Review Routes

12.1. A Responsible Actor shall provide access to the applicable Review Route established by the Main Framework.

12.2. A Review request shall identify:

(a) requester;

(b) affected matter;

(c) contested action or decision;

(d) reasons for review;

(e) supporting evidence.

12.3. The Review process shall:

(a) identify the responsible Review function;

(b) consider available evidence;

(c) provide an impartial evaluation;

(d) record the outcome.

12.4. A Review outcome shall identify:

(a) reviewed matter;

(b) evidence considered;

(c) findings;

(d) corrective actions;

(e) further Remedy options.

12.5. A Review function shall not exceed its assigned competence.

Article 13: Remedy Routes

13.1. A Responsible Actor shall implement Remedy Routes according to the applicable Framework provisions.

13.2. Remedy may include:

(a) correction;

(b) restoration of an affected process;

(c) additional review;

(d) modification of an operational action;

(e) other measures permitted by the Framework.

13.3. A Remedy outcome shall identify:

(a) affected person;

(b) affected matter;

(c) remedy measure;

(d) responsible Actor;

(e) implementation date;

(f) evidence.

13.4. Remedy shall be limited to the competence and scope established by the Framework.

13.5. Remedy shall not:

(a) assign Status;

(b) create Qualified Status;

(c) create Authorisation;

(d) replace a Framework Decision.

Article 14: Communication with affected persons

14.1. Communication with affected persons shall be:

(a) understandable;

(b) accessible;

(c) proportionate;

(d) timely.

14.2. Communication shall identify:

(a) the matter concerned;

(b) available actions;

(c) responsible Actor;

(d) applicable timelines;

(e) available Review and Remedy Routes.

14.3. Communication shall avoid unnecessary disclosure of:

(a) Security-Sensitive Information;

(b) Protection-Sensitive Information;

(c) third-party confidential information.

Article 15: Records

15.1. A Responsible Actor shall maintain records sufficient to reconstruct:

(a) safeguard assessments;

(b) accessibility measures;

(c) adverse-effect assessments;

(d) complaints;

(e) correction requests;

(f) Review requests;

(g) Remedy requests;

(h) outcomes and corrective actions.

15.2. Records shall preserve:

(a) Integrity;

(b) Authenticity;

(c) provenance;

(d) time;

(e) responsible Actor;

(f) affected scope.

15.3. Records shall be protected according to applicable Security Conditions.

15.4. Correction of records shall preserve:

(a) earlier record;

(b) correction basis;

(c) responsible Actor;

(d) Effective Date.

Article 16: Improvement and monitoring

16.1. A Responsible Actor shall monitor:

(a) complaint trends;

(b) correction trends;

(c) adverse effects;

(d) accessibility issues;

(e) Review outcomes;

(f) Remedy outcomes.

16.2. Monitoring results shall inform:

(a) service improvement;

(b) safeguard improvement;

(c) Profile updates;

(d) training;

(e) operational changes.

16.3. Repeated adverse effects shall trigger review of the underlying implementation.

16.4. Improvement actions shall identify:

(a) responsible Actor;

(b) implementation date;

(c) evidence;

(d) effectiveness review.

Article 17: Reference standards and specifications

17.1. The reference standards applicable to this Guideline are set out in Annex I.

17.2. A reference shall apply only within the implementation function identified in Annex I.

17.3. Exact accessibility interfaces, communication formats and technical support mechanisms shall be defined through applicable Profiles and Technical Specifications.

17.4. Conformity with a referenced standard shall not create:

(a) rights;

(b) obligations;

(c) Status;

(d) Qualified Status;

(e) Controlled Effects.

ANNEX I: REFERENCE STANDARDS

Reference	Implementation function	Applicability
ISO 10002:2018, Quality management — Customer satisfaction — Guidelines	Complaint handling processes	Applicable for complaint intake, classification, handling and improvement processes.

Reference	Implementation function	Applicability
for complaints handling in organizations		
ISO 10003:2018, Quality management — Customer satisfaction — Guidelines for dispute resolution external to organizations	External dispute resolution guidance	Applicable where external dispute-resolution mechanisms are implemented.
ISO 9241-171:2008, Ergonomics of human-system interaction — Part 171: Guidance on software accessibility	Software accessibility	Applicable for accessible software interaction design.
ISO 9241-210:2019, Human-centred design for interactive systems	Human-centred design	Applicable for service design affecting Protected Persons.
ISO/IEC 40500:2012, W3C Web Content Accessibility Guidelines 2.0	Web accessibility guidance	Applicable where web-based interfaces are used.
ISO/IEC 30071-1:2019, Information technology — Development of user interface accessibility	Accessibility management	Applicable for accessibility governance and implementation.
ISO/IEC 29184:2020, Online privacy notices and consent	Communication and transparency	Applicable where online privacy communication and consent information are provided.
ISO/IEC 27701:2025, Privacy information management systems	Privacy-related safeguards	Applicable where personal data processing affects Protected Persons.

IDEHA-IG-BIO-GEN-001: BIOMETRIC IMPLEMENTATION CONTROLS

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Guideline lays down implementation requirements for biometric data processing under the Framework.

1.2. This Guideline shall apply to each Responsible Actor, Identification Service Provider, Authentication Service Provider, Source Holder, Source Steward, Trust Service Provider, Issuer, Relying Actor and supporting Actor processing biometric information within an approved scope.

1.3. This Guideline shall govern, where applicable:

(a) biometric modality selection;

(b) biometric collection and capture;

(c) capture environment requirements;

(d) biometric quality assessment;

(e) biometric reference creation;

(f) biometric template protection;

(g) biometric comparison and performance evaluation;

(h) presentation attack detection;

(i) biometric algorithm governance;

(j) demographic performance monitoring;

(k) biometric lifecycle management;

(l) biometric evidence management;

(m) biometric interoperability.

1.4. This Guideline shall not:

(a) establish identity;

(b) establish legal identity;

(c) determine Identity Proofing requirements;

(d) create Identification Results;

(e) create Authentication Outcomes;

(f) establish Source authority;

(g) determine whether a person shall be enrolled;

(h) define legal grounds for biometric processing;

(i) prescribe a mandatory biometric modality for all implementations.

1.5. Identity Registration Records containing biometric information shall be governed by IDEHA-IG-SVC-IDN-001.

1.6. Biometric use as an Authentication factor shall be governed by IDEHA-IG-SVC-AUT-001.

1.7. Biometric information contained within Electronic Attestations shall be governed by IDEHA-IG-SVC-EAS-001 and IDEHA-IG-OBJ-EAA-001.

1.8. Security, Confidentiality, access control and incident requirements shall be governed by IDEHA-IG-SEC-CNF-001 and IDEHA-IG-SEC-INC-001.

1.9. Compliance with this Guideline shall not, by itself, establish identity, Authentication, Authorisation, Status, Qualified Status, Service Permission or Controlled Reliance.

Article 2: Application through Schemes, Profiles and Technical Specifications

2.1. The applicable Scheme shall identify:

(a) the operational purpose for biometric processing;

(b) the affected persons;

(c) the responsible Actors;

(d) the permitted biometric use cases;

(e) the applicable safeguards.

2.2. The applicable Biometric Profile shall identify:

(a) permitted biometric modalities;

(b) collection conditions;

(c) capture requirements;

(d) quality requirements;

(e) presentation attack detection requirements;

(f) template protection requirements;

(g) matching-performance requirements;

(h) algorithm governance requirements;

(i) retention and deletion conditions;

(j) interoperability requirements.

2.3. The applicable Technical Specification shall define:

(a) biometric data formats;

(b) image or sample encoding;

(c) template encoding;

(d) compression;

(e) biometric exchange structures;

(f) technical interfaces;

(g) algorithm parameters;

(h) testing procedures.

2.4. A biometric reference shall remain separate from:

(a) Identity Identifier;

(b) Identification Number;

(c) Subject Identifier;

(d) Trust Object Identifier;

(e) Authentication Outcome.

2.5. A biometric comparison result shall not, by itself, establish identity, entitlement or Authorisation.

Article 3: Biometric Implementation Plan

3.1. A Responsible Actor shall maintain a Biometric Implementation Plan where biometric information is collected, stored, compared or reused.

3.2. The Implementation Plan shall identify:

(a) biometric purpose;

(b) affected persons;

(c) responsible Actor;

(d) biometric modalities;

(e) collection processes;

(f) capture environments;

(g) storage arrangements;

(h) protection mechanisms;

(i) matching processes;

(j) performance evaluation;

(k) retention and deletion;

(l) interoperability requirements;

(m) incident and compromise handling.

3.3. The Implementation Plan shall distinguish:

(a) biometric sample from biometric template;

(b) biometric reference from biometric comparison result;

(c) biometric matching from identity determination;

(d) biometric Authentication from identity registration;

(e) biometric protection from Authorisation.

3.4. The Responsible Actor shall review the Implementation Plan following:

(a) introduction of a new modality;

(b) algorithm change;

(c) material performance change;

(d) security incident;

(e) material lifecycle change.

SECTION 2: BIOMETRIC MODALITY GOVERNANCE

Article 4: Modality selection

4.1. A Responsible Actor shall select biometric modalities according to the intended purpose and operational context.

4.2. Modality selection shall consider:

(a) reliability;

(b) accessibility;

(c) availability;

(d) environmental conditions;

(e) population characteristics;

(f) performance requirements;

(g) risk of misuse;

(h) interoperability requirements.

4.3. A modality-selection record shall identify:

(a) selected modality;

(b) purpose;

(c) justification;

(d) affected population;

(e) limitations;

(f) review conditions.

4.4. No biometric modality shall be considered universally suitable for all purposes.

4.5. A Responsible Actor shall consider non-biometric or alternative methods where biometric collection may create disproportionate exclusion or adverse effects.

Article 5: Biometric modality lifecycle

5.1. Each biometric modality shall have lifecycle management.

5.2. Lifecycle information shall identify:

(a) introduction;

(b) approved use cases;

(c) applicable algorithms;

(d) performance evidence;

(e) restrictions;

(f) retirement conditions.

5.3. A retired modality shall remain identifiable for Historical State where previously created biometric references require evaluation.

5.4. Retirement of a modality shall include:

(a) migration conditions;

(b) retention treatment;

(c) deletion conditions;

(d) interoperability arrangements

SECTION 3: COLLECTION AND CAPTURE CONTROLS

Article 6: Biometric collection

6.1. Biometric collection shall be performed according to the applicable Biometric Profile.

6.2. Collection shall identify:

(a) biometric modality;

(b) collection purpose;

(c) collection event;

(d) collection Actor;

(e) collection environment;

(f) applicable quality requirements.

6.3. The collection process shall maintain evidence sufficient to establish:

(a) when collection occurred;

(b) which modality was collected;

(c) which equipment was used;

(d) which process was applied.

6.4. Collection evidence shall not contain unnecessary biometric content beyond the authorised purpose.

Article 7: Capture environment

7.1. A biometric capture environment shall provide conditions appropriate for the selected modality.

7.2. The capture environment shall consider:

(a) lighting;

(b) positioning;

(c) background conditions;

(d) sensor performance;

(e) operator assistance;

(f) environmental interference.

7.3. The Responsible Actor shall define capture-quality requirements.

7.4. Capture equipment shall be identified and maintained according to the applicable Profile.

7.5. Material changes to capture equipment shall be assessed before continued use.

Article 8: Biometric quality assessment

8.1. Each collected biometric sample shall be assessed according to applicable quality requirements.

8.2. Quality assessment shall consider:

(a) completeness;

(b) usability;

(c) distortion;

(d) environmental effects;

(e) capture errors;

(f) modality-specific characteristics.

8.3. Quality results shall identify:

(a) quality assessment method;

(b) result;

(c) threshold;

(d) processing decision.

8.4. A failed quality assessment shall not automatically determine identity failure.

8.5. The applicable Profile shall define whether:

(a) recapture;

(b) alternative modality;

(c) human review;

(d) another process

is required.

SECTION 4: BIOMETRIC REFERENCE PROTECTION

Article 9: Biometric reference creation

9.1. A biometric reference shall be created only within the approved scope.

9.2. A biometric reference record shall identify:

(a) reference identifier;

(b) biometric modality;

(c) creation process;

(d) creation time;

(e) responsible Actor;

(f) algorithm Version;

(g) protection method;

(h) lifecycle Status.

9.3. A biometric reference identifier shall:

(a) remain opaque;

(b) not disclose identity information;

(c) not encode demographic information;

(d) remain separate from Subject Identifiers.

9.4. A biometric reference shall not be considered the biometric source sample.

Article 10: Template protection

10.1. Biometric references shall be protected against:

(a) unauthorised access;

(b) unauthorised disclosure;

(c) unauthorised modification;

(d) unauthorised reconstruction;

(e) unauthorised reuse.

10.2. Protection mechanisms may include:

(a) encryption;

(b) transformation;

(c) secure storage;

(d) access control;

(e) template-protection mechanisms.

10.3. A biometric reference shall not be stored in plaintext unless expressly permitted by the applicable Profile.

10.4. A biometric reference shall not be reusable across unrelated purposes without an approved purpose and protection assessment.

10.5. Protection mechanisms shall preserve:

(a) performance requirements;

(b) interoperability requirements;

(c) lifecycle requirements.

SECTION 5: BIOMETRIC COMPARISON AND PERFORMANCE

Article 11: Biometric comparison

11.1. A biometric comparison process shall identify:

(a) input biometric information;

(b) biometric reference used;

(c) comparison method;

(d) algorithm Version;

(e) result;

(f) confidence or score where applicable.

11.2. A biometric comparison result shall remain separate from:

(a) identity;

(b) Authentication;

(c) Authorisation.

11.3. Automated biometric comparison shall operate according to approved thresholds and review procedures.

11.4. A comparison failure shall not automatically create adverse consequences without the applicable review or alternative process where required.

Article 12: Performance evaluation

12.1. A Responsible Actor shall evaluate biometric-system performance according to the applicable Profile.

12.2. Performance evaluation shall consider:

(a) false match rate;

(b) false non-match rate;

(c) failure to acquire rate;

(d) failure to enrol rate;

(e) processing time;

(f) population impact.

12.3. Performance evaluation shall identify:

(a) dataset or evaluation population;

(b) methodology;

(c) algorithm Version;

(d) testing conditions;

(e) limitations.

12.4. Performance results shall not be generalised beyond the evaluated scope.

Article 13: Demographic performance monitoring

13.1. Where biometric systems may produce different performance outcomes across populations, the Responsible Actor shall monitor demographic performance.

13.2. Monitoring shall consider:

(a) identified performance differences;

(b) possible causes;

(c) mitigation measures;

(d) accessibility impact.

13.3. Demographic performance monitoring shall respect applicable safeguards and shall not create discriminatory profiling.

13.4. Results shall be used to improve:

(a) algorithms;

(b) capture processes;

(c) training;

(d) alternative processes.

SECTION 6: PRESENTATION ATTACK DETECTION AND REMOTE COLLECTION

Article 14: Presentation attack detection

14.1. Where biometric presentation attacks create a material risk, the Responsible Actor shall implement presentation attack detection controls.

14.2. Presentation attack detection shall identify:

(a) applicable modality;

(b) attack classes addressed;

(c) detection method;

(d) testing evidence;

(e) limitations.

14.3. Presentation attack detection shall be evaluated according to the applicable Profile.

14.4. Failure of presentation attack detection shall not automatically determine fraud, identity failure or adverse action without applicable review procedures.

Article 15: Remote biometric collection

15.1. Remote biometric collection shall apply additional controls appropriate to the risk.

15.2. Remote collection controls shall address:

(a) device integrity;

(b) capture environment uncertainty;

(c) presentation attacks;

(d) communication protection;

(e) evidence collection;

(f) operator assistance where required.

15.3. Remote biometric collection shall maintain evidence sufficient to reconstruct:

(a) device used;

(b) collection time;

(c) collection process;

(d) quality assessment;

(e) outcome.

15.4. Remote collection shall not reduce required Assurance Conditions without an approved Profile condition.

SECTION 7: LIFECYCLE, SECURITY AND RECORDS

Article 16: Biometric lifecycle management

16.1. Biometric information lifecycle shall include:

(a) collection;

(b) quality assessment;

(c) reference creation;

(d) storage;

(e) use;

(f) update;

(g) restriction;

(h) deletion.

16.2. Lifecycle events shall identify:

(a) responsible Actor;

(b) Effective Date;

(c) reason;

(d) evidence.

16.3. Biometric information shall not be retained beyond the applicable purpose and Retention conditions.

16.4. Deletion shall address:

(a) active storage;

(b) backup copies;

(c) replicated copies;

(d) temporary processing copies.

Article 17: Biometric compromise handling

17.1. A biometric compromise shall be treated as a Security Incident.

17.2. The Responsible Actor shall assess:

(a) affected biometric references;

(b) affected persons;

(c) affected systems;

(d) affected purposes;

(e) possible misuse.

17.3. Response measures may include:

(a) restricting use;

(b) replacing protection mechanisms;

(c) changing authentication methods;

(d) increasing monitoring;

(e) notifying affected persons.

17.4. Unlike cryptographic keys, biometric characteristics cannot generally be replaced. The response shall therefore prioritise protection, limitation and alternative safeguards.

Article 18: Records and evidence

18.1. A Responsible Actor shall maintain records sufficient to reconstruct biometric lifecycle.

18.2. Records shall include:

(a) modality selection;

(b) collection events;

(c) capture equipment;

(d) quality results;

(e) reference creation;

(f) algorithm Versions;

(g) performance evaluations;

(h) presentation attack detection testing;

(i) lifecycle changes;

(j) deletion evidence.

18.3. Records shall preserve:

(a) Integrity;

(b) Authenticity;

(c) provenance;

(d) Version;

(e) time;

(f) responsible Actor.

18.4. Records shall be protected according to IDEHA-IG-SEC-CNF-001.

Article 19: Reference standards and specifications

19.1. The reference standards applicable to this Guideline are set out in Annex I.

19.2. Standards shall apply only within the implementation function identified in Annex I.

19.3. Exact biometric formats, encodings, algorithms and interface specifications shall be defined through applicable Technical Specifications.

19.4. Conformity with a referenced standard shall not establish identity, Authentication, Authorisation, Status or Controlled Effects.

ANNEX I: REFERENCE STANDARDS

Reference	Implementation function	Applicability
ISO/IEC 2382-37:2022, Information technology — Vocabulary — Biometrics	Biometric terminology	Principal terminology reference.
ISO/IEC 19794 series	Biometric data interchange formats	Applicable where biometric data interchange formats are required.
ISO/IEC 39794 series	Extensible biometric data interchange formats	Applicable where modern extensible biometric formats are selected.
ISO/IEC 30107-1:2023, Presentation attack detection — Part 1: Framework	Presentation attack detection concepts	Applicable for PAD implementation governance.
ISO/IEC 30107-3:2023, Presentation attack detection — Part 3: Testing and reporting	PAD testing and reporting	Applicable where PAD testing is required.
ISO/IEC 29794 series	Biometric sample quality	Applicable for biometric quality assessment.
ISO/IEC 19795-1:2021, Biometric performance testing and reporting — Part 1: Principles and framework	Performance testing methodology	Applicable for biometric performance evaluation.
ISO/IEC 24745:2022, Information security, cybersecurity and privacy protection — Biometric information protection	Biometric template protection	Principal reference for biometric information protection.
ISO/IEC 30136:2018, Performance testing of biometric template protection schemes	Template protection evaluation	Applicable where biometric template protection performance is evaluated.
ISO/IEC 29109 series	Conformance testing methodology for biometric data interchange formats	Applicable where interchange-format conformity testing is required.
ISO/IEC 27001:2022	Security management controls	Applicable through IDEHA-IG-SEC-CNF-001.
ISO/IEC 27701:2025	Privacy information management	Applicable where biometric information processing includes personal data governanc

IDEHA-IG-CHG-GEN-001: CHANGE CONTROL, VERSIONING, MIGRATION AND TRANSITION IMPLEMENTATION

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Guideline lays down implementation requirements for controlled change, Version management, migration, transition, compatibility and Historical State preservation under the Framework.

1.2. This Guideline shall apply to each Responsible Actor, Framework Body, Trust Service Provider, Source Holder, Source Steward, Issuer, Relying Actor, supporting Actor and technical operator implementing, operating, maintaining or transitioning a Controlled Matter.

1.3. This Guideline shall govern, where applicable:

(a) change identification;

(b) change classification;

(c) impact assessment;

(d) change approval and implementation;

(e) Version management;

(f) migration planning;

(g) transition management;

(h) compatibility assessment;

(i) deprecation and withdrawal;

(j) cessation support;

(k) Historical State preservation.

1.4. This Guideline shall not:

(a) establish Framework amendment procedures;

(b) assign Decision Competence;

(c) create or modify Framework rules;

(d) assign Status, Qualified Status, Service Permission or Technical Exchange Permission;

(e) determine External Legal Status or External Legal Effect;

(f) replace security change requirements established by IDEHA-IG-SEC-CNF-001;

(g) replace cryptographic migration requirements established by IDEHA-IG-SEC-CRY-001;

(h) replace Security Incident-driven changes established by IDEHA-IG-SEC-INC-001;

(i) replace qualification reassessment requirements established by IDEHA-IG-ASR-QLF-001.

1.5. A change shall be implemented only within the authority, scope and responsibility assigned by the applicable Framework Instrument.

1.6. A change approval, migration completion, Version release or technical deployment shall not, by itself, create:

(a) Authorisation;

(b) Status;

(c) Qualified Status;

(d) Service Permission;

(e) Controlled Reliance.

Article 2: Application through Schemes, Profiles and Technical Specifications

2.1. The applicable Scheme shall identify:

(a) the governed operational context;

(b) the participating Actors;

(c) the affected Controlled Matters;

(d) the applicable governance and approval routes;

(e) the applicable Review and Remedy conditions.

2.2. The applicable Profile shall identify:

(a) the change categories;

(b) the material-change criteria;

(c) the approval conditions;

(d) the required impact assessment;

(e) the Versioning rules;

(f) migration requirements;

(g) transition conditions;

(h) compatibility requirements;

(i) deprecation conditions;

(j) evidence requirements.

2.3. The applicable Technical Specification shall define:

(a) technical Version identifiers;

(b) schema and interface changes;

(c) compatibility requirements;

(d) migration mechanisms;

(e) technical validation procedures;

(f) test requirements.

2.4. A change to a Technical Specification shall not automatically change:

(a) a Framework rule;

(b) a Scheme;

(c) a Profile;

(d) a Status;

(e) a Qualified Scope.

2.5. A later Version shall remain identifiable from the earlier Version for Historical State determination.

Article 3: Change Implementation Plan

3.1. A Responsible Actor shall maintain a Change Implementation Plan for each material change.

3.2. The Change Implementation Plan shall identify:

(a) the change owner;

(b) the affected Controlled Matter;

(c) the reason for change;

(d) the current Version;

(e) the target Version;

(f) the applicable Framework Instruments;

(g) the affected Actors;

(h) the dependencies;

(i) the impact assessment;

(j) the migration approach;

(k) the transition period;

(l) testing requirements;

(m) communication requirements;

(n) rollback conditions;

(o) Historical State treatment.

3.3. The Change Implementation Plan shall distinguish:

(a) corrective change from enhancement;

(b) emergency change from planned change;

(c) technical change from Framework change;

(d) migration from replacement;

(e) Version update from creation of a new Controlled Matter.

3.4. A Change Implementation Plan shall be reviewed where:

(a) scope changes;

(b) dependencies change;

(c) risks change;

(d) implementation timing changes;

(e) transition conditions change.

SECTION 2: CHANGE GOVERNANCE AND ASSESSMENT

Article 4: Change identification and classification

4.1. A Responsible Actor shall classify each proposed change before implementation.

4.2. Change classification shall identify:

(a) change identifier;

(b) change owner;

(c) affected Controlled Matter;

(d) affected Version;

(e) reason;

(f) urgency;

(g) impact category;

(h) approval route.

4.3. Changes may be classified as:

(a) corrective change;

(b) preventive change;

(c) maintenance change;

(d) enhancement change;

(e) migration change;

(f) emergency change;

(g) retirement change.

4.4. A change shall be considered material where it may affect:

(a) Service Scope;

(b) Qualified Scope;

(c) Status;

(d) Assurance Conditions;

(e) Security Conditions;

(f) interoperability;

(g) dependencies;

(h) Trust Object creation or Validation;

(i) Source processing;

(j) Protected-Person Safeguards.

4.5. A material change shall undergo impact assessment before implementation.

4.6. A non-material change shall remain recorded according to the applicable Profile.

Article 5: Change impact assessment

5.1. A Responsible Actor shall assess the impact of each material change.

5.2. The impact assessment shall identify:

(a) affected Actors;

(b) affected Controlled Matters;

(c) affected Versions;

(d) affected Dependencies;

(e) affected Trust Services;

(f) affected Trust Objects;

(g) affected Sources;

(h) affected Technical Exchange Routes;

(i) affected Security Conditions;

(j) affected Assurance Conditions;

(k) affected Qualified Conditions;

(l) affected Protected Persons.

5.3. The impact assessment shall consider:

(a) security;

(b) Confidentiality;

(c) Integrity;

(d) Authenticity;

(e) Availability;

(f) interoperability;

(g) accessibility;

(h) operational continuity;

(i) Historical State;

(j) Review and Remedy.

5.4. The impact assessment shall identify:

(a) required testing;

(b) required approvals;

(c) required communication;

(d) required migration;

(e) rollback conditions.

5.5. A change shall not be implemented where the impact assessment identifies an unresolved unacceptable risk unless the applicable exception process permits it.

5.6. A change affecting Qualified Status shall be handled according to IDEHA-IG-ASR-QLF-001.

Article 6: Change approval and implementation

6.1. A material change shall require approval by the Actor or Framework Body holding the applicable responsibility.

6.2. Approval shall identify:

(a) approved scope;

(b) approved Version;

(c) effective date;

(d) implementation conditions;

(e) testing requirements;

(f) rollback conditions.

6.3. Implementation shall occur according to the approved Change Implementation Plan.

6.4. A change shall be verified after implementation.

6.5. Verification shall identify:

(a) implemented Version;

(b) affected scope;

(c) test results;

(d) outstanding issues;

(e) completion status.

6.6. Implementation evidence shall be retained.

6.7. Successful implementation shall not automatically establish:

(a) compliance;

(b) qualification;

(c) Status;

(d) Authorisation.

Those matters require separate evaluation where applicable.

SECTION 3: VERSION MANAGEMENT AND LIFECYCLE

Article 7: Version identification

7.1. Each Framework Instrument, Profile, Technical Specification, Trust Object, Trust Service Output, configuration package, policy package, mechanism, device and material implementation component shall have a Version identifier where required by the applicable Profile.

7.2. A Version identifier shall:

(a) uniquely identify the applicable state;

(b) remain immutable after publication;

(c) support Historical State determination;

(d) identify predecessor and successor relationships.

7.3. Version identifiers shall not be reused for materially different content.

7.4. A Version change shall identify:

(a) previous Version;

(b) new Version;

(c) Effective Date;

(d) change description;

(e) compatibility conditions.

Article 8: Version lifecycle management

8.1. A Version lifecycle shall include, where applicable:

(a) draft;

(b) approved;

(c) active;

(d) restricted;

(e) deprecated;

(f) withdrawn;

(g) archived.

8.2. Lifecycle transitions shall identify:

(a) responsible Actor;

(b) decision basis;

(c) Effective Date;

(d) affected scope;

(e) transition conditions.

8.3. A withdrawn Version shall remain identifiable where required for:

(a) Validation;

(b) Historical State;

(c) Review;

(d) Remedy;

(e) audit.

8.4. An archived Version shall not be used for new creation unless expressly permitted.

8.5. A deprecated Version shall identify:

(a) remaining permitted use;

(b) end-of-use date;

(c) replacement Version;

(d) migration requirements.

SECTION 4: MIGRATION AND TRANSITION MANAGEMENT

Article 9: Migration planning

9.1. A Responsible Actor shall prepare a migration plan where a change requires movement from one Version, mechanism, system, service or dependency to another.

9.2. The migration plan shall identify:

(a) current state;

(b) target state;

(c) migration scope;

(d) affected Actors;

(e) affected dependencies;

(f) migration sequence;

(g) testing;

(h) transition period;

(i) rollback conditions;

(j) completion criteria.

9.3. Migration shall preserve:

(a) Accountability;

(b) Integrity;

(c) Authenticity;

(d) Historical State;

(e) evidence continuity.

9.4. Migration shall not silently alter:

(a) Source authority;

(b) Trust Object meaning;

(c) Status;

(d) Qualified Scope;

(e) Controlled Reliance conditions.

Article 10: Transition management

10.1. A transition period may be established where old and new Versions operate together.

10.2. A transition arrangement shall identify:

(a) coexistence period;

(b) permitted Versions;

(c) affected Actors;

(d) compatibility rules;

(e) security requirements;

(f) termination condition.

10.3. During transition, a Responsible Actor shall prevent:

(a) unauthorised downgrade;

(b) uncontrolled Version mixing;

(c) ambiguous interpretation;

(d) loss of historical evidence.

10.4. A transition shall define the final condition under which the previous Version is:

(a) restricted;

(b) deprecated;

(c) withdrawn.

10.5. Transition completion shall be recorded.

Article 11: Compatibility management

11.1. A Responsible Actor shall assess compatibility before introducing a new Version.

11.2. Compatibility assessment shall identify:

(a) technical compatibility;

(b) semantic compatibility;

(c) security compatibility;

(d) operational compatibility;

(e) dependency compatibility.

11.3. A compatible Version shall not automatically be considered equivalent.

11.4. Where semantic meaning changes, a new Version or separate Controlled Matter shall be created.

11.5. Compatibility claims shall identify:

(a) tested scope;

(b) limitations;

(c) supported Versions;

(d) unsupported conditions.

SECTION 5: DEPRECATION, WITHDRAWAL AND CESSATION

Article 12: Deprecation

12.1. A Responsible Actor may deprecate a Version, mechanism, service function or dependency.

12.2. Deprecation shall identify:

(a) reason;

(b) affected scope;

(c) remaining permitted use;

(d) replacement;

(e) end date.

12.3. Deprecated elements shall not be used for new creation unless expressly permitted.

12.4. Deprecation shall preserve historical Validation capability where required.

Article 13: Withdrawal and cessation

13.1. Withdrawal shall identify:

(a) withdrawn element;

(b) effective date;

(c) affected Actors;

(d) replacement arrangements;

(e) evidence preservation requirements.

13.2. Cessation shall identify:

(a) pending operations;

(b) dependent Actors;

(c) retained records;

(d) transition obligations;

(e) final Status.

13.3. Withdrawal or cessation shall not invalidate earlier actions where Historical State requires continued recognition.

13.4. Cessation shall preserve:

(a) evidence;

(b) Validation capability;

(c) Review capability;

(d) Remedy capability.

SECTION 6: RECORDS AND HISTORICAL STATE

Article 14: Change records

14.1. A Responsible Actor shall maintain records sufficient to reconstruct change lifecycle.

14.2. Records shall include:

(a) change requests;

(b) classifications;

(c) impact assessments;

(d) approvals;

(e) implementation evidence;

(f) testing results;

(g) migration records;

(h) transition records;

(i) Version history;

(j) rollback events;

(k) withdrawal records.

14.3. Records shall preserve:

(a) Integrity;

(b) Authenticity;

(c) provenance;

(d) Version;

(e) time;

(f) responsible Actor.

14.4. Records shall be protected according to applicable Security Conditions.

Article 15: Historical State preservation

15.1. A Responsible Actor shall preserve information necessary to determine the state of a Controlled Matter at a previous time.

15.2. Historical State records shall identify:

(a) applicable Version;

(b) applicable Profile;

(c) applicable Technical Specification;

(d) applicable Dependencies;

(e) applicable Standards;

(f) applicable Status;

(g) effective period.

15.3. A current Version shall not automatically determine the state of an earlier interaction.

15.4. Migration shall preserve the relationship between:

(a) predecessor;

(b) successor;

(c) transition condition;

(d) effective time.

15.5. Historical State information shall remain available for:

(a) Validation;

(b) Assurance;

(c) Conformity Assessment;

(d) Review;

(e) Remedy.

SECTION 7: REFERENCE STANDARDS

Article 16: Reference standards and specifications

16.1. The reference standards applicable to this Guideline are set out in Annex I.

16.2. Standards shall apply only within the implementation function identified in Annex I.

16.3. Exact Version numbering schemes, technical identifiers, migration formats and interface behaviours shall be defined through applicable Profiles and Technical Specifications.

16.4. Conformity with a referenced standard shall not create:

(a) Status;

(b) Qualified Status;

(c) Service Permission;

(d) Controlled Effects.

ANNEX I: REFERENCE STANDARDS

Reference	Implementation function	Applicability
ISO/IEC/IEEE 24748-1:2024, Systems and software engineering — Life cycle management — Part 1: Guide for life cycle management	Lifecycle and transition planning	Applicable for structured lifecycle planning.
ISO/IEC/IEEE 15288:2023, Systems and software engineering — System life cycle processes	System lifecycle management	Applicable where changes affect complex systems or infrastructure.
ISO/IEC/IEEE 12207:2017, Systems and software engineering — Software life cycle processes	Software lifecycle changes	Applicable for software-related change management.
ISO/IEC 20000-1:2018, Information technology — Service management system requirements	Service change management	Applicable where formal service management processes are implemented.
ISO/IEC 27001:2022, Information security management systems — Requirements	Security-related change governance	Applicable where changes affect information-security management systems.
ISO/IEC 27002:2022, Information security controls	Change-control security controls	Applicable through selected controls identified in the applicable Profile.

Reference	Implementation function	Applicability
ISO/IEC 27005:2022, Information security risk management	Change impact risk assessment	Applicable for change-related risk assessment.
ITIL 4 Change Enablement Practice	Operational change governance guidance	Applicable as supporting operational guidance where adopted by the Responsible Actor.

IDEHA-IG-PUB-HTL-001: HUMANITARIAN TRUST LIST, STATUS PUBLICATION, REGISTERS, CATALOGUES

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Guideline lays down implementation requirements for Humanitarian Trust List operation, Status Publication, Registers, Catalogues and federation discovery under the Framework.

1.2. This Guideline shall apply to Framework Bodies, Status Publishers, Trust Service Providers, Responsible Actors, Trust Service operators, Source Holders, Source Stewards, Federation Domain operators, Discovery Metadata operators and supporting Actors responsible for publishing, maintaining, consuming or validating published trust information.

1.3. This Guideline shall govern, where applicable:

(a) Humanitarian Trust List publication;

(b) Status Publication implementation;

(c) Trust Service discovery;

(d) Actor and Endpoint discovery;

(e) Register management;

(f) Catalogue management;

(g) federation discovery metadata;

(h) publication integrity and authenticity;

(i) Status update lifecycle;

(j) correction, withdrawal and historical publication;

(k) discovery and Validation evidence.

1.4. This Guideline shall not:

(a) create Trust Service Categories;

(b) create Trust Object Categories;

(c) assign Status;

(d) assign Qualified Status;

(e) make qualification decisions;

(f) establish Decision Competence;

(g) create Service Permission;

(h) create Technical Exchange Permission;

(i) create Authorisation;

(j) determine Source authority;

(k) determine External Legal Status or External Legal Effect.

1.5. The Humanitarian Trust List shall publish authorised Status information and discovery information only.

1.6. Status creation, qualification decisions, Service Permission decisions and Framework Decisions shall remain with the competent Framework Body or responsible Actor identified by the Main Framework.

1.7. Compliance with this Guideline shall not, by itself, establish trust, recognition, Status, Qualified Status, Authorisation or Controlled Reliance.

Article 2: Application through Schemes, Profiles and Technical Specifications

2.1. The applicable Scheme shall identify:

(a) the governed trust context;

(b) the participating Actors;

(c) the Status-Bearing Matters;

(d) the applicable Federation Domains;

(e) the discovery purposes;

(f) the applicable safeguards.

2.2. The applicable Status Publication Profile shall identify:

(a) publication scope;

(b) Status information categories;

(c) publication frequency;

(d) update conditions;

(e) correction procedures;

(f) withdrawal procedures;

(g) historical publication requirements;

(h) integrity and authenticity requirements.

2.3. The applicable Discovery Profile shall identify:

(a) discovery information categories;

(b) Actor discovery;

(c) Trust Service discovery;

(d) Endpoint discovery;

(e) Technical Exchange Route discovery;

(f) Federation Domain discovery;

(g) applicable freshness requirements.

2.4. The applicable Technical Specification shall define:

(a) Trust List structure;

(b) Register structure;

(c) Catalogue structure;

(d) discovery metadata formats;

(e) publication interfaces;

(f) integrity-protection formats;

(g) exchange formats;

(h) validation procedures.

2.5. A published Entry shall remain separate from:

(a) the underlying Framework Decision;

(b) the Status-Bearing Matter;

(c) the Trust Service operation;

(d) the Trust Object;

(e) the Source record;

(f) the Authorisation decision.

Article 3: Publication Implementation Plan

3.1. A Status Publisher shall maintain a Publication Implementation Plan.

3.2. The Publication Implementation Plan shall identify:

(a) the publication scope;

(b) responsible Actors;

(c) publication functions;

(d) Humanitarian Trust List structure;

(e) Registers and Catalogues;

(f) discovery metadata;

(g) publication processes;

(h) integrity and authenticity protection;

(i) update processes;

(j) correction processes;

(k) withdrawal processes;

(l) historical publication arrangements;

(m) evidence and assurance requirements.

3.3. The Publication Implementation Plan shall distinguish:

(a) Status decision from Status publication;

(b) discovery from Authorisation;

(c) publication from Validation;

(d) Register entry from Source authority;

(e) Catalogue entry from Service Permission.

3.4. The Publication Implementation Plan shall be reviewed following:

(a) publication-model changes;

(b) Status-model changes;

(c) material technical changes;

(d) Security Incident;

(e) dependency changes.

SECTION 2: HUMANITARIAN TRUST LIST PUBLICATION MODEL

Article 4: Humanitarian Trust List purpose and scope

4.1. The Humanitarian Trust List shall provide a trusted publication mechanism for authorised trust information.

4.2. The Humanitarian Trust List may contain:

(a) Status information;

(b) Trust Service information;

(c) Trust Service Provider information;

(d) Actor discovery information;

(e) Endpoint discovery information;

(f) Federation Domain information;

(g) Certificate and trust information;

(h) publication metadata.

4.3. The Humanitarian Trust List shall identify:

(a) the publishing Framework Body or authorised Status Publisher;

(b) the publication Version;

(c) the Effective Date;

(d) the publication period;

(e) the applicable Scheme;

(f) the applicable Profile.

4.4. The Humanitarian Trust List shall not:

(a) create Status;

(b) replace a Framework Decision;

(c) replace Source records;

(d) replace Authorisation;

(e) create entitlement.

Article 5: Humanitarian Trust List structure

5.1. The Humanitarian Trust List shall maintain separately identifiable Entries.

5.2. Each Entry shall identify, where applicable:

(a) Entry Identifier;

(b) Status-Bearing Matter;

(c) category;

(d) Status;

(e) Effective Date;

(f) expiry or review date;

(g) publication source;

(h) applicable scope;

(i) restrictions;

(j) caveats.

5.3. An Entry shall identify the relationship between:

(a) published information;

(b) underlying decision;

(c) responsible Actor;

(d) supporting evidence.

5.4. An Entry shall not include information beyond the authorised publication scope.

5.5. Publication of an Entry shall not transfer responsibility from the responsible Actor to the Status Publisher.

Article 6: Publication integrity and authenticity

6.1. A Humanitarian Trust List publication shall be protected against unauthorised alteration.

6.2. Publication protection shall establish:

(a) publication origin;

(b) publication Integrity;

(c) publication Version;

(d) publication time;

(e) sequence continuity.

6.3. A Humanitarian Trust List package shall be protected using an Electronic Seal attributable to the authorised publishing Actor.

6.4. Where required by the applicable Profile, publication evidence shall include an Electronic Timestamp.

6.5. Publication protection shall not establish:

(a) the correctness of the published Status decision;

(b) the authority of the underlying decision;

(c) the legality of reliance.

6.6. The receiving Actor shall validate:

(a) publication authenticity;

(b) publication Integrity;

(c) publication Version;

(d) Effective Date;

(e) Status scope;

(f) historical applicability.

SECTION 3: STATUS PUBLICATION LIFECYCLE

Article 7: Status Publication creation

7.1. Status Publication shall occur only following an authorised Status decision or authorised publication event.

7.2. The publication process shall verify:

(a) decision reference;

(b) Status-Bearing Matter identity;

(c) Status category;

(d) Qualified Scope where applicable;

(e) Effective Date;

(f) restrictions;

(g) caveats.

7.3. The Status Publisher shall not modify the substantive decision.

7.4. Publication metadata shall identify:

(a) publication Actor;

(b) publication time;

(c) publication Version;

(d) applicable Technical Specification.

Article 8: Status update, correction and withdrawal

8.1. Status updates shall identify:

(a) previous Status;

(b) new Status;

(c) effective time;

(d) reason;

(e) responsible Actor.

8.2. Corrections shall preserve:

(a) original publication;

(b) correction basis;

(c) correction time;

(d) responsible Actor.

8.3. Withdrawal shall identify:

(a) withdrawn Entry;

(b) effective date;

(c) reason;

(d) successor Entry where applicable.

8.4. A withdrawn Entry shall remain available where required for:

(a) Historical State;

(b) Validation;

(c) Review;

(d) Remedy.

Article 9: Historical Status and publication state

9.1. The Humanitarian Trust List shall preserve historical publication states.

9.2. Historical publication information shall identify:

(a) Entry Version;

(b) Status at the relevant time;

(c) Effective Date;

(d) withdrawal or replacement events;

(e) applicable publication Version.

9.3. A current Humanitarian Trust List publication shall not automatically determine historical Status.

9.4. Historical publication state shall support:

(a) Validation;

(b) Assurance;

(c) Conformity Assessment;

(d) Review;

(e) Remedy.

SECTION 4: REGISTERS AND CATALOGUES

Article 10: Registers

10.1. A Register shall maintain controlled records of recognised Framework objects, Actors, Services or information categories assigned by the applicable Framework Instrument.

10.2. A Register Entry shall identify:

(a) Register Identifier;

(b) Entry Identifier;

(c) responsible Actor;

(d) recorded information;

(e) Version;

(f) lifecycle Status;

(g) Effective Date.

10.3. A Register shall maintain:

(a) creation;

(b) update;

(c) correction;

(d) withdrawal;

(e) historical preservation.

10.4. A Register Entry shall not create:

(a) Source authority;

(b) Status;

(c) Authorisation;

(d) Qualification.

Article 11: Catalogues

11.1. A Catalogue shall provide controlled discovery information for recognised items within an assigned scope.

11.2. A Catalogue may contain:

(a) Service information;

(b) technical capability information;

(c) Profile information;

(d) Version information;

(e) compatibility information.

11.3. A Catalogue Entry shall identify:

(a) Catalogue Identifier;

(b) Entry Identifier;

(c) responsible Actor;

(d) Version;

(e) Effective Date;

(f) lifecycle Status.

11.4. Catalogue information shall remain separate from:

(a) Status;

(b) Qualification;

(c) Authorisation;

(d) Source authority.

SECTION 5: FEDERATION DISCOVERY IMPLEMENTATION

Article 12: Federation discovery metadata

12.1. Federation discovery metadata shall support discovery of recognised federation participants and technical capabilities.

12.2. Discovery metadata may identify:

(a) Actor Identifier;

(b) Trust Service Identifier;

(c) Endpoint reference;

(d) Technical Exchange Route reference;

(e) Federation Domain;

(f) supported Profiles;

(g) supported Technical Specifications;

(h) certificate references.

12.3. Discovery metadata shall identify:

(a) responsible Actor;

(b) publication time;

(c) Version;

(d) lifecycle Status.

12.4. Discovery metadata shall not establish:

(a) access;

(b) disclosure permission;

(c) Authorisation;

(d) Technical Exchange Permission.

12.5. Discovery information shall be validated before use in a controlled exchange context.

Article 13: Address resolution and service discovery

13.1. Where the Humanitarian Trust List provides address-resolution functionality, the resolution process shall identify:

(a) requested service;

(b) responsible Actor;

(c) Endpoint;

(d) Technical Exchange Route;

(e) applicable Version.

13.2. Address resolution shall use current and validated discovery information.

13.3. Address resolution shall not:

(a) bypass Authorisation;

(b) bypass Endpoint Authentication;

(c) replace Source access decisions;

(d) create reliance rights.

13.4. A resolved Endpoint shall remain subject to:

(a) Authentication;

(b) Authorisation;

(c) Security Conditions;

(d) exchange policies.

SECTION 6: ASSURANCE, LIFECYCLE AND RECORDS

Article 14: Assurance and Conformity Assessment

14.1. A Status Publisher shall maintain evidence sufficient to demonstrate:

(a) publication processes;

(b) integrity protection;

(c) authenticity protection;

(d) lifecycle management;

(e) correction procedures;

(f) historical preservation.

14.2. Assurance and Conformity Assessment shall be performed according to IDEHA-IG-ASR-QLF-001 where applicable.

14.3. Positive Conformity Assessment shall not create Status.

14.4. Publication integrity shall not replace the underlying Framework Decision.

Article 15: Records and evidence

15.1. A Status Publisher shall maintain records sufficient to reconstruct:

(a) publication events;

(b) Status updates;

(c) corrections;

(d) withdrawals;

(e) discovery metadata changes;

(f) Register changes;

(g) Catalogue changes.

15.2. Records shall preserve:

(a) Integrity;

(b) Authenticity;

(c) provenance;

(d) Version;

(e) time;

(f) responsible Actor.

15.3. Records shall be protected according to IDEHA-IG-SEC-CNF-001.

15.4. Correction of records shall preserve:

(a) earlier record;

(b) correction basis;

(c) responsible Actor;

(d) Effective Date.

Article 16: Reference standards and specifications

16.1. The reference standards applicable to this Guideline are set out in Annex I.

16.2. Standards shall apply only within the implementation function identified in Annex I.

16.3. Exact publication structures, metadata formats, interfaces and validation procedures shall be defined through applicable Technical Specifications.

16.4. Conformity with a referenced standard shall not create:

(a) Status;

(b) Qualified Status;

(c) Service Permission;

(d) Controlled Effects.

ANNEX I: REFERENCE STANDARDS

Reference	Implementation function	Applicability
ETSI TS 119 612 V2.3.1, Trusted Lists	Trusted List structure and publication model	Applicable as the baseline reference for trusted-list structure and publication semantics.
ETSI TS 119 615 V1.1.1, Trusted Lists — Protocols for obtaining trusted lists	Trusted List access and retrieval	Applicable where trusted-list retrieval protocols are implemented.
ETSI EN 319 102-1, Electronic Signatures and Trust Infrastructures — Procedures for signature validation	Validation of signed publication objects where applicable	Applicable where validation processes depend on signed trust information.
RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile	Certificate validation dependencies	Applicable where Certificates support publication authenticity or discovery identity.

Reference	Implementation function	Applicability
ISO/IEC 9594-8:2020, Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks	Directory and certificate-related discovery concepts	Applicable as a supporting reference where directory-style discovery is implemented.
ISO/IEC 27001:2022, Information security management systems — Requirements	Publication security governance	Applicable through IDEHA-IG-SEC-CNF-001.
ISO/IEC 27002:2022, Information security controls	Publication security controls	Applicable through selected controls identified in the applicable Profile.
ISO 15489-1:2016, Records management	Publication records and lifecycle evidence	Applicable for publication record managemen

IDEHA-IG-SVC-IDN-001 IDENTIFICATION SERVICE IDENTITY VERIFICATION AND PROOFING IMPLEMENTATION

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1. This Guideline lays down implementation requirements for Identity Verification and Identity Proofing performed by a Trust Service Provider providing an Identification Service.

2. This Guideline applies to Trust Service Providers providing Identification Services and Actors performing, supporting or relying upon Identity Verification within an assigned Service Scope.

3. This Guideline establishes requirements for:

(a) evaluation of Evidence Artefacts;

(b) assessment of Evidence Strength;

(c) assessment of Evidence Validity;

(d) Identity Existence Assessment;

(e) Identity Fraud Risk Assessment;

(f) Identity Verification determination;

(g) application of Identification Assurance Profiles;

(h) creation of Identification Results.

4. This Guideline applies together with:

(a) the applicable Identification Service Profile;

(b) IDEHA-IG-SRC-ASO-001 Source and Authoritative Source Implementation;

(c) IDEHA-IG-DAT-SEM-001 Controlled Data Elements, Semantics and Data Quality Implementation;

(d) IDEHA-IG-BIO-GEN-001 Biometric Implementation Controls;

(e) IDEHA-IG-RMR-GEN-001 Protected-Person Safeguards, Complaint, Correction, Review and Remedy Implementation.

5. This Guideline does not establish:

(a) Identity Registration Record structure;

(b) Identification Number allocation;

(c) Identity Registration lifecycle;

(d) Authentication Service requirements;

(e) Authorisation Service requirements;

(f) Electronic Attestation issuance requirements;

(g) biometric technical specifications;

(h) technical document formats, interfaces or protocols.

6. Identity Verification performed under this Guideline shall support the Identification Service functions assigned through the applicable Framework Instruments.

7. Identity Verification shall not determine substantive humanitarian, administrative, programme or operational decisions unless such determination is separately assigned through an applicable Framework Instrument.

Article 2: Identification Service Identity Verification model

1. Identity Verification is a function performed within an Identification Service through which a Trust Service Provider evaluates whether available information and Evidence Artefacts provide sufficient confidence that a Claimed Identity Representation relates to the Subject.

2. Identity Verification shall be performed against the applicable Identification Assurance Profile.

3. Identity Verification shall evaluate:

(a) the Claimed Identity Representation;

(b) Evidence Artefacts;

(c) Source Basis where applicable;

(d) identity-related Attributes;

(e) biometric information where applicable;

(f) identity fraud indicators;

(g) applicable Assurance Conditions.

4. Identity Verification shall consist of the following assessment functions:

(a) Evidence Strength Assessment;

(b) Evidence Validity Assessment;

(c) Identity Existence Assessment;

(d) Identity Fraud Risk Assessment;

(e) Identity Verification Assessment.

5. The Identification Service shall determine an Identification Assurance Level based on the applicable Identification Assurance Profile.

6. The result of Identity Verification shall be recorded as an Identification Result.

7. Identity Verification shall not:

(a) create an Identity Registration Record;

(b) allocate an Identification Number;

(c) perform Authentication;

(d) perform Authorisation;

(e) determine eligibility or entitlement.

Article 3: Claimed Identity Representation

1. A Claimed Identity Representation is information presented or referenced for the purpose of establishing an identification basis concerning a Subject.

2. A Claimed Identity Representation may include:

(a) biographic information;

(b) demographic information;

(c) biometric information;

(d) Identifier references;

(e) Identification Document references;

(f) relationship information;

(g) other identity-related information permitted by the applicable Identification Profile.

3. A Claimed Identity Representation shall be evaluated against:

(a) Evidence Artefacts;

(b) Source Basis where applicable;

(c) applicable Assurance Conditions.

4. A Claimed Identity Representation shall not be considered verified solely because:

(a) the information is internally consistent;

(b) the information is self-asserted;

(c) the information is obtained through an unauthenticated source.

5. A Claimed Identity Representation shall remain separate from:

(a) Identity Registration Record;

(b) Identification Result;

(c) Authentication Outcome;

(d) Authorisation Outcome.

SECTION 2: EVIDENCE EVALUATION

Article 4: Evidence Artefacts

1. An Evidence Artefact is information or an object evaluated by an Identification Service to support Identity Verification.

2. Evidence Artefacts may include:

(a) Identification Document Evidence;

(b) civil registration evidence;

(c) Electronic Attestation Evidence;

(d) Source records;

(e) biometric evidence;

(f) demographic evidence;

(g) relationship evidence;

(h) institutional evidence;

(i) historical evidence.

3. The applicable Identification Assurance Profile shall define the permitted Evidence Artefact categories and minimum requirements.

4. Each Evidence Artefact shall be evaluated according to:

(a) origin;

(b) integrity;

(c) authenticity;

(d) validity;

(e) relevance;

(f) freshness;

(g) relationship to the Subject.

5. The Identification Service shall record the Evidence Artefacts evaluated during Identity Verification.

6. An Evidence Artefact shall not by itself:

(a) establish an Identity Registration Record;

(b) establish Authentication;

(c) establish Authorisation;

(d) create Source Status;

(e) create Authoritative Source Status.

7. Evidence Artefacts shall remain attributable to their originating Source, Issuer or responsible Actor.

Article 5: Evidence Strength Assessment

1. Evidence Strength Assessment shall determine the strength of an Evidence Artefact for the purpose of Identity Verification.

2. Evidence Strength Assessment shall consider:

(a) information contained within the Evidence Artefact;

(b) uniqueness of information;

(c) resistance to alteration or duplication;

(d) security features;

(e) issuance controls;

(f) identity binding performed during issuance;

(g) cryptographic protection where applicable.

3. Evidence Strength shall be assessed according to the following levels:

(a) Level 1: Basic Evidence;

(b) Level 2: Verified Evidence;

(c) Level 3: Strong Evidence;

(d) Level 4: Very Strong Evidence.

4. The applicable Identification Assurance Profile shall define the minimum Evidence Strength required for each Identification Assurance Level.

5. Evidence Strength shall be assessed separately for each Evidence Artefact.

6. The existence of a higher-strength Evidence Artefact shall not remove the requirement to assess Evidence Validity.

Article 6: Evidence Validity Assessment

1. Evidence Validity Assessment shall determine whether an Evidence Artefact is genuine, valid and suitable for the intended Identity Verification purpose.

2. Evidence Validity Assessment shall consider:

(a) authenticity;

(b) integrity;

(c) validity period;

(d) Status information;

(e) alteration or substitution indicators;

(f) physical security features;

(g) cryptographic security features where applicable.

3. Where an Evidence Artefact originates from a Source or Issuer, the Identification Service shall evaluate the applicable Source Basis or Issuer information.

4. The applicable Identification Assurance Profile shall define:

(a) validity checks;

(b) permitted verification methods;

(c) escalation conditions;

(d) human review requirements.

5. Evidence Validity Assessment shall remain separate from:

(a) Subject identity determination;

(b) Authentication;

(c) Authorisation.

Article 7: Identity Existence Assessment

1. Identity Existence Assessment shall determine whether available information demonstrates continuity or existence of the Claimed Identity Representation over an identified period where required by the applicable Identification Assurance Profile.

2. Identity Existence Assessment may consider:

(a) historical Source information;

(b) records maintained by recognised organisations;

(c) lifecycle events;

(d) previous verified interactions;

(e) historical Evidence Artefacts.

3. Identity Existence Assessment shall evaluate whether available information demonstrates continuity associated with the Claimed Identity Representation.

4. Identity Existence Assessment shall not determine:

(a) eligibility;

(b) entitlement;

(c) programme participation;

(d) legal status.

5. The applicable Identification Assurance Profile shall define:

(a) when Identity Existence Assessment is required;

(b) acceptable evidence;

(c) assessment period;

(d) minimum conditions.

SECTION 2: EVIDENCE EVALUATION

Article 8: Identity Fraud Risk Assessment

1. Identity Fraud Risk Assessment shall determine whether indicators exist that the Claimed Identity Representation may not relate to the Subject presenting or associated with that representation.

2. Identity Fraud Risk Assessment shall consider, where applicable:

(a) conflicting identity information;

(b) inconsistent Evidence Artefacts;

(c) duplicate identity indicators;

(d) synthetic identity indicators;

(e) impersonation indicators;

(f) presentation attack indicators;

(g) unusual identity lifecycle patterns;

(h) other indicators identified by the applicable Identification Assurance Profile.

3. Identity Fraud Risk Assessment shall evaluate risk indicators and shall not determine:

(a) fraud;

(b) misconduct;

(c) liability;

(d) criminal responsibility.

4. Where Identity Fraud Risk Assessment identifies material uncertainty or elevated risk, the Identification Service shall apply the applicable Identification Assurance Profile requirements.

5. Additional measures may include:

(a) additional Evidence Artefacts;

(b) additional Source Basis evaluation;

(c) biometric assessment;

(d) human review;

(e) another Identification Verification method.

6. The outcome of Identity Fraud Risk Assessment shall be recorded as part of the Identity Verification assessment evidence.

SECTION 3: IDENTITY VERIFICATION DETERMINATION

Article 9: Identity Verification Assessment

1. Identity Verification Assessment shall determine whether the evaluated information satisfies the requirements of the applicable Identification Assurance Profile.

2. Identity Verification Assessment shall consider:

(a) Evidence Strength Assessment;

(b) Evidence Validity Assessment;

(c) Identity Existence Assessment where applicable;

(d) Identity Fraud Risk Assessment;

(e) biometric evidence assessment where applicable;

(f) Source Basis;

(g) applicable Assurance Conditions.

3. The Identification Service shall record:

(a) Evidence Artefacts evaluated;

(b) assessment methods applied;

(c) Identification Assurance Profile applied;

(d) resulting Identification Assurance Level;

(e) limitations and caveats;

(f) human review activities where applicable.

4. Identity Verification Assessment shall result in:

(a) an Identification Result satisfying the applicable Assurance Conditions; or

(b) a determination that the applicable Assurance Conditions have not been satisfied.

5. Where the applicable Assurance Conditions are not satisfied, the Identification Service shall record the reason and applicable next steps.

6. An Identity Verification Assessment shall not:

(a) create an Identity Registration Record;

(b) allocate an Identification Number;

(c) establish Authentication;

(d) establish Authorisation.

Article 10: Identification Assurance Levels

1. Identification Assurance Levels shall define the confidence achieved through the Identity Verification process.

2. The Identification Assurance Levels are:

(a) Low Assurance;

(b) Substantial Assurance;

(c) High Assurance;

(d) Very High Assurance.

3. Each Identification Assurance Level shall be implemented through an Identification Assurance Profile established in Annex III.

4. An Identification Assurance Profile shall define the minimum conditions required for the corresponding Identification Assurance Level.

5. Identification Assurance Levels shall be determined based on:

(a) Evidence Strength;

(b) Evidence Validity;

(c) Identity Existence Assessment where applicable;

(d) Identity Fraud Risk Assessment;

(e) biometric evidence assessment where applicable;

(f) human review conditions where applicable.

6. An Identification Assurance Level shall apply only to the Identification Result produced by the Identification Service.

7. An Identification Assurance Level shall not transfer to:

(a) Authentication Outcomes;

(b) Authorisation Outcomes;

(c) Sources;

(d) Evidence Artefacts;

(e) Trust Objects;

(f) Electronic Attestations.

Article 11: Identification Verification Profiles

1. An Identification Verification Profile shall define the implementation conditions applicable to an Identification Assurance Level.

2. An Identification Verification Profile shall specify:

(a) intended purpose;

(b) applicable Identification Assurance Level;

(c) permitted Evidence Artefact categories;

(d) minimum Evidence Strength requirements;

(e) minimum Evidence Validity requirements;

(f) Identity Existence Assessment requirements;

(g) Identity Fraud Risk Assessment requirements;

(h) biometric evidence requirements where applicable;

(i) Source Basis requirements;

(j) human review requirements;

(k) Accessible Alternative requirements;

(l) limitations and caveats.

3. Identification Verification Profiles shall be established in Annex III.

4. An Identification Verification Profile shall not:

(a) create a new Identification Service category;

(b) establish Authentication requirements;

(c) establish Authorisation requirements;

(d) assign Source Status;

(e) assign Authoritative Source Status;

(f) assign Qualified Status.

5. The Identification Service shall apply the Identification Verification Profile corresponding to:

(a) the intended purpose;

(b) the required Identification Assurance Level;

(c) the applicable Scheme and Service Scope.

6. A Trust Service Provider providing an Identification Service shall not apply an Identification Verification Profile providing a lower Assurance Level than required by the applicable Framework Instrument.

SECTION 4: IDENTIFICATION VERIFICATION IMPLEMENTATION CONDITIONS

Article 12: Remote Identity Verification

1. A Trust Service Provider providing remote Identity Verification shall apply the requirements established by the applicable Remote Identity Verification Profile.

2. Remote Identity Verification shall ensure that:

(a) the Subject presenting the Evidence Artefact is associated with the Claimed Identity Representation;

(b) the Evidence Artefact presented is genuine;

(c) the Evidence Artefact has not been altered or substituted;

(d) the communication channel satisfies applicable Security Conditions;

(e) manipulation and replay risks are evaluated.

3. Remote Identity Verification may include:

(a) remote examination of Identification Document Evidence;

(b) cryptographic verification of electronic document features;

(c) biometric comparison;

(d) live interaction;

(e) Source verification;

(f) other methods permitted by the applicable Identification Verification Profile.

4. Remote Identity Verification shall apply controls against:

(a) presentation attacks;

(b) injection attacks;

(c) replay attacks;

(d) synthetic representations;

(e) unauthorised substitution.

5. Where automated remote Identity Verification cannot establish sufficient confidence, the Identification Service shall apply:

(a) additional Evidence Artefacts;

(b) human review;

(c) an Accessible Alternative;

(d) another permitted Identification Verification route.

6. Remote Identity Verification shall not rely solely on:

(a) a copied image of an Evidence Artefact;

(b) self-asserted identity information;

(c) an unverified contact point;

(d) an isolated biometric comparison result.

SECTION 4: IDENTIFICATION VERIFICATION IMPLEMENTATION CONDITIONS

Article 13: Biometric Evidence Assessment

1. Where biometric information is used during Identity Verification, the Identification Service shall apply the requirements established by the applicable Biometric Profile.

2. Biometric Evidence Assessment shall determine whether biometric information provides appropriate support for the applicable Identification Assurance Level.

3. Biometric Evidence Assessment shall consider:

(a) biometric modality;

(b) biometric sample quality;

(c) biometric reference source;

(d) biometric comparison purpose;

(e) presentation attack risks;

(f) protection of biometric information;

(g) applicable Security Conditions.

4. The Identification Service shall distinguish between:

(a) biometric sample;

(b) biometric reference;

(c) biometric template;

(d) biometric quality result;

(e) biometric comparison result;

(f) biometric decision result.

5. A biometric comparison result shall not, by itself:

(a) establish identity;

(b) create an Identity Registration Record;

(c) create an Authentication Outcome;

(d) create an Authorisation Outcome.

6. Biometric information shall be processed according to:

(a) the applicable Biometric Profile;

(b) applicable Security Conditions;

(c) applicable Protected-Person Safeguards;

(d) applicable retention and lifecycle requirements.

7. Technical requirements concerning:

(a) biometric data formats;

(b) biometric encoding;

(c) biometric algorithms;

(d) biometric capture conditions;

(e) biometric performance thresholds;

(f) presentation attack detection implementation shall be established through the applicable Technical Specification.

Article 14: Source Basis and Authoritative Source reliance

1. Where Identity Verification relies upon information originating from a Source, the Identification Service shall identify the applicable Source Basis.

2. The Source Basis shall identify, where applicable:

(a) Source Identifier;

(b) Source Scope;

(c) relevant Attribute or record category;

(d) Source Status;

(e) Authoritative Source Status where applicable;

(f) Qualified Authoritative Source Status where applicable;

(g) time of evaluation;

(h) applicable restrictions and limitations.

3. A Trust Service Provider providing an Identification Service shall rely on Source information only within:

(a) the recognised Source Scope;

(b) the applicable Source Profile;

(c) the permitted purpose;

(d) the applicable Reliance Conditions.

4. Authoritative Source Status shall not be assumed solely because:

(a) information originates from a public authority;

(b) information is stored in a recognised system;

(c) information is frequently relied upon;

(d) information is transmitted through a recognised Technical Exchange Route.

5. A Source Basis shall remain separate from:

(a) an Identification Result;

(b) an Identity Registration Record;

(c) an Authentication Outcome;

(d) an Authorisation Outcome.

6. Where multiple Sources provide conflicting information, the Identification Service shall apply the conflict-resolution requirements established by the applicable Identification Verification Profile.

7. Resolution of conflicting Source information shall not alter Source Status unless determined through the applicable Framework Decision route.

SECTION 5: SAFEGUARDS AND IDENTIFICATION RESULTS

Article 15: Human review and Protected-Person Safeguards

1. The Identification Service shall provide human review where required by the applicable Identification Verification Profile.

2. Human review shall be required where:

(a) automated evaluation cannot produce a reliable result;

(b) Evidence Artefacts contain unresolved conflicts;

(c) Identity Fraud Risk Assessment identifies material uncertainty;

(d) biometric evaluation produces an unresolved result;

(e) a Protected-Person Safeguard requires additional consideration;

(f) the Subject requests review through an applicable Review Route.

3. Human review shall consider:

(a) Evidence Artefacts;

(b) assessment results;

(c) Source Basis;

(d) limitations and uncertainty;

(e) applicable Safeguards.

4. The Identification Service shall ensure that:

(a) inability to satisfy one Identity Verification route does not automatically result in exclusion;

(b) Accessible Alternatives are available where required;

(c) Correction Routes are available;

(d) Review Routes are available;

(e) Remedy Routes are available.

5. A negative Identity Verification result shall not, by itself:

(a) establish fraud;

(b) establish misconduct;

(c) establish ineligibility;

(d) remove rights or access outside the Identification Service scope.

6. Where Identity Verification may produce an Adverse Protected-Person Effect, the Identification Service shall apply the safeguards established by the applicable Scheme or Profile.

7. Human review shall not replace the requirement for sufficient evidence, applicable Security Conditions or Assurance Conditions.

Article 16: Identification Result

1. An Identification Result shall record the outcome of Identity Verification performed by an Identification Service.

2. An Identification Result shall identify or reference:

(a) the Trust Service Provider;

(b) the Identification Service;

(c) the Subject or Claimed Identity Representation;

(d) the applied Identification Verification Profile;

(e) the Identification Assurance Level;

(f) Evidence Artefacts evaluated;

(g) Source Basis where applicable;

(h) assessment time;

(i) validity conditions;

(j) limitations and caveats.

3. The Identification Result shall contain sufficient information to determine the basis of the Identity Verification outcome.

4. An Identification Result may be used as an input to:

(a) Identity Registration;

(b) Authentication Services;

(c) Authorisation Services;

(d) Electronic Attestation Services;

(e) other permitted Trust Service functions.

5. Use of an Identification Result by another Trust Service shall remain subject to:

(a) applicable Reliance Conditions;

(b) the receiving Actor's Trust Acceptance Policy;

(c) applicable Assurance Conditions.

6. An Identification Result shall not:

(a) create an Identity Registration Record;

(b) allocate an Identification Number;

(c) authenticate a Subject;

(d) authorise an action;

(e) establish eligibility or entitlement.

7. Where an Identification Result is represented as an Electronic Attestation, the resulting Electronic Attestation shall constitute a separate Trust Object.

Article 17: Records and evidence

1. A Trust Service Provider providing an Identification Service shall maintain records sufficient to reconstruct the Identity Verification process.

2. Records shall include, where applicable:

(a) Claimed Identity Representation;

(b) Evidence Artefacts evaluated;

(c) Evidence Strength Assessment;

(d) Evidence Validity Assessment;

(e) Identity Existence Assessment;

(f) Identity Fraud Risk Assessment;

(g) Identity Verification Assessment;

(h) applied Identification Verification Profile;

(i) Identification Assurance Level;

(j) Source Basis;

(k) Identification Result;

(l) human review activities;

(m) Correction, Review and Remedy actions.

3. Records shall enable determination of the basis of an Identification Result at the relevant time.

4. Records shall be protected according to applicable:

(a) Security Conditions;

(b) Confidentiality requirements;

(c) retention requirements;

(d) Protected-Person Safeguards.

5. Records shall not contain information beyond the scope required for the Identity Verification purpose.

SECTION 6: STANDARDS AND TECHNICAL REFERENCES

Article 18: Applicable standards

1. The standards applicable to this Guideline are set out in Annex V.

2. A standard referenced in Annex V shall apply only for the implementation function identified in that Annex.

3. Conformity with a referenced standard shall constitute evidence only for the requirements mapped to that standard.

4. A referenced standard shall not create:

(a) Identification Service Status;

(b) Trust Service Provider Status;

(c) Authoritative Source Status;

(d) Qualified Status;

(e) Controlled Effects.

ANNEX I: EVIDENCE STRENGTH MATRIX

1. General requirements

1. The Evidence Strength Matrix defines the criteria used to determine the strength of an Evidence Artefact for Identity Verification.

2. Evidence Strength shall be assessed separately for each Evidence Artefact.

3. Evidence Strength shall be determined based on the characteristics of the Evidence Artefact and the assurance of the process through which the Evidence Artefact was created, issued or maintained.

4. The Evidence Strength Matrix shall be applied together with:

(a) the Evidence Validity Matrix;

(b) the applicable Identification Assurance Profile;

(c) the applicable Source Basis requirements.

2. Evidence Strength Level 1: Basic Evidence

An Evidence Artefact may achieve Level 1 where it contains sufficient information to establish a basic identification reference.

The assessment may consider:

Requirement	Description
Identity information	Contains one or more identity-related Attributes
Identifier information	Contains an Identifier or reference number where applicable
Personal information	Contains basic biographic or demographic information
Origin	Issued or provided by an identifiable Actor
Availability	Can be presented or accessed for evaluation

Level 1 Evidence does not provide strong assurance that:

(a) the Evidence Artefact has strong resistance against alteration;

(b) the Evidence Artefact was issued following strong identity proofing;

(c) the Evidence Artefact remains valid at the time of evaluation.

3. Evidence Strength Level 2: Verified Evidence

An Evidence Artefact may achieve Level 2 where it satisfies Level 1 and includes additional controls.

The assessment may consider:

Requirement	Description
Unique association	Contains information uniquely associated with the Subject
Issuance process	Issuer applied identity-related verification controls

Requirement	Description
Protection features	Contains physical or digital protection features
Issuer recognition	Issuer can be identified and verified
Controlled issuance	Issuance process applies defined controls

Level 2 Evidence provides increased confidence but does not necessarily provide strong Subject binding.

4. Evidence Strength Level 3: Strong Evidence

An Evidence Artefact may achieve Level 3 where it satisfies Level 2 and includes stronger identity binding.

The assessment may consider:

Requirement	Description
Strong identity binding	Issuer verified the relationship between Subject and Evidence Artefact
Secure issuance	Issuance process applies enhanced identity verification
Protected representation	Physical or cryptographic protection prevents unauthorised alteration
Subject association	Evidence includes photograph, biometric reference or equivalent binding information
Integrity protection	Integrity can be verified

Level 3 Evidence provides strong confidence that the Evidence Artefact relates to the identified Subject.

5. Evidence Strength Level 4: Very Strong Evidence

An Evidence Artefact may achieve Level 4 where it satisfies Level 3 and provides the highest available identity binding.

The assessment may consider:

Requirement	Description
Biometric binding	Includes biometric information linked to the Subject
Cryptographic protection	Digital information is protected using cryptographic mechanisms
Verified issuer	Issuing organisation can be cryptographically verified
Authoritative comparison	Issuer compared the Subject against authoritative identity information
Controlled issuance	Issuance process provides very high confidence

Level 4 Evidence provides the highest Evidence Strength available under this Guideline.

ANNEX II: EVIDENCE VALIDITY MATRIX

1. General requirements

1. The Evidence Validity Matrix defines the controls used to determine whether an Evidence Artefact is genuine, valid and suitable for Identity Verification.
2. Evidence Validity Assessment shall consider the state of the Evidence Artefact at the time of evaluation.
3. The applicable Identification Assurance Profile shall define the minimum Evidence Validity Level required.

2. Evidence Validity Level 1: Basic Validity

The evaluator shall determine whether:

(a) the Evidence Artefact appears consistent;

(b) required information is present;

(c) obvious alteration indicators are absent;

(d) the representation corresponds to the expected format.

3. Evidence Validity Level 2: Verified Validity

The evaluator shall determine whether:

(a) Level 1 conditions are satisfied;

(b) visible security features appear genuine;

(c) validity period remains applicable;

(d) available issuer information can be confirmed;

(e) the Evidence Artefact has not been visibly altered.

4. Evidence Validity Level 3: Strong Validity

The evaluator shall determine whether:

(a) Level 2 conditions are satisfied;

(b) advanced security features are verified;

(c) replay or substitution risks are addressed;

(d) cryptographic protection is validated where available;

(e) issuer validation information remains valid.

5. Evidence Validity Level 4: Very Strong Validity

The evaluator shall determine whether:

(a) Level 3 conditions are satisfied;

(b) advanced physical security features are verified;

(c) cryptographic security features are validated;

(d) issuer authenticity is confirmed;

(e) controlled evaluation conditions are applied where required.

ANNEX III: IDENTIFICATION ASSURANCE PROFILES

1. General requirements

1. Identification Assurance Profiles define the evidence and assessment combinations required to achieve an Identification Assurance Level.

2. Each Identification Assurance Profile shall identify:

(a) purpose;

(b) required Evidence Strength;

(c) required Evidence Validity;

(d) Identity Existence requirements;

(e) Identity Fraud Risk Assessment requirements;

(f) biometric requirements;

(g) human review requirements;

(h) Accessible Alternative requirements.

2. Low Assurance Identification Profile

IDEHA-IDV-L

Purpose:

Identity Verification where limited assurance is sufficient and where the consequences of incorrect identification are limited.

Minimum conditions:

Condition	Requirement
Evidence Strength	Level 1 or above
Evidence Validity	Level 1 or above
Identity Existence	Optional
Fraud assessment	Required
Human review	According to risk
Biometric evidence	Optional

Limitations:

(a) shall not be used where High Assurance or Very High Assurance is required;

(b) shall not support Controlled Reliance requiring stronger assurance.

3. Substantial Assurance Identification Profile

IDEHA-IDV-S

Purpose:

Identity Verification requiring increased confidence and controlled reuse.

Minimum conditions:

Condition	Requirement
Evidence Strength	Level 2 or above
Evidence Validity	Level 2 or above
Identity Existence	Required where defined
Fraud assessment	Required
Human review	Risk-based
Source Basis	Required where Source information is used

ANNEX III: IDENTIFICATION ASSURANCE PROFILES

4. High Assurance Identification Profile

IDEHA-IDV-H

Purpose:

Identity Verification where a high level of confidence is required and where incorrect identification may create material adverse consequences.

Minimum conditions:

Condition	Requirement
Evidence Strength	Level 3 or above
Evidence Validity	Level 3 or above
Identity Existence	Required
Fraud assessment	Required
Source Basis	Required where Source information is used
Biometric evidence	Required where defined by the applicable purpose
Human review	Required for unresolved conflicts or elevated risk

Evidence requirements:

(a) at least one Strong Evidence Artefact;

or

(b) multiple independent Evidence Artefacts meeting the applicable combination rules.

The Identification Service shall verify:

(a) the relationship between the Evidence Artefacts and the Subject;

(b) the validity of the Evidence Artefacts;

(c) the applicable Source Basis;

(d) the absence of unresolved material conflicts.

The Identification Result shall contain:

(a) applied Identification Profile;

(b) High Assurance Identification Level;

(c) evaluated Evidence Artefacts;

(d) assessment results;

(e) limitations and caveats.

Restrictions:

(a) shall not be reduced to lower assurance evidence where High Assurance is required;

(b) shall apply additional safeguards where Protected-Person risks exist.

5. Very High Assurance Identification Profile

IDEHA-IDV-VH

Purpose:

Identity Verification where the highest level of confidence is required and where incorrect identification may create significant adverse consequences.

Minimum conditions:

Condition	Requirement
Evidence Strength	Level 4
Evidence Validity	Level 4
Identity Existence	Required
Fraud assessment	Required
Source Basis	Required where Source information is used
Biometric evidence	Required where applicable
Human review	Required where automated evaluation is insufficient

Evidence requirements:

The Identification Service shall use:

(a) Very Strong Evidence Artefacts;

(b) authoritative Source information where applicable;

(c) cryptographically protected evidence where available;

(d) biometric or equivalent Subject binding where required.

The Identification Service shall verify:

(a) Evidence Artefact authenticity;

(b) Evidence Artefact integrity;

(c) issuer or Source authenticity;

(d) Subject association;

(e) lifecycle validity;

(f) fraud risk indicators.

Very High Assurance shall require enhanced controls for:

(a) evidence collection;

(b) evidence evaluation;

(c) human review;

(d) auditability;

(e) record preservation.

Restrictions:

(a) shall only be used where justified by the intended purpose;

(b) shall not become the default requirement for all Identification Services;

(c) shall apply Protected-Person Safeguards and Accessible Alternatives where required.

ANNEX IV: EVIDENCE ARTEFACT CATALOGUE

1. General requirements

1. The Evidence Artefact Catalogue identifies categories of Evidence Artefacts that may be evaluated during Identity Verification.

2. The Catalogue does not establish that an Evidence Artefact satisfies a particular Assurance Level.

3. The applicable Identification Assurance Profile shall determine whether an Evidence Artefact category may be used and the required Evidence Strength and Evidence Validity.

2. Identification Document Evidence

Identification Document Evidence includes documents issued by recognised Actors for the purpose of identifying a Subject.

Examples include:

Category	Examples
National identification documents	National identity documents issued by recognised authorities
Travel identification documents	Machine-readable travel documents where applicable
Functional identification documents	Documents issued for specific recognised functions
Humanitarian identification documents	Documents issued within recognised humanitarian identification processes

Assessment shall consider:

(a) issuing Actor;

(b) issuance process;

(c) security features;

(d) validity period;

(e) Subject association;

(f) lifecycle Status.

3. Civil Registration Evidence

Civil Registration Evidence includes records maintained by recognised civil registration Sources.

Examples include:

Category	Examples
Birth registration evidence	Evidence establishing birth-related information
Death registration evidence	Evidence establishing death-related information
Family relationship evidence	Evidence establishing recognised relationships

Assessment shall consider:

(a) Source Status;

(b) Source Scope;

(c) provenance;

(d) correction processes;

(e) freshness.

4. Electronic Attestation Evidence

Electronic Attestation Evidence includes Electronic Attestations issued by recognised Attestation Issuers.

Assessment shall consider:

(a) Attestation Issuer;

(b) Electronic Attestation Status;

(c) protection mechanism;

(d) Validation Result;

(e) Source Basis;

(f) Validity Period.

5. Biometric Evidence

Biometric Evidence includes biometric information used to support Identity Verification.

Categories include:

(a) biometric sample;

(b) biometric reference;

(c) biometric template;

(d) biometric comparison result.

Assessment shall consider:

(a) biometric quality;

(b) biometric protection;

(c) presentation attack controls;

(d) applicable Biometric Profile.

6. Demographic Evidence

Demographic Evidence includes information describing characteristics associated with a Subject.

Examples include:

(a) name;

(b) date of birth;

(c) place of birth;

(d) nationality or citizenship information where applicable;

(e) address information where applicable.

Demographic Evidence shall not be considered sufficient alone for High Assurance or Very High Assurance unless the applicable Profile expressly permits it.

7. Relationship Evidence

Relationship Evidence supports verification of a relationship between Subjects, Actors or entities.

Examples include:

(a) family relationships;

(b) guardianship;

(c) representation;

(d) organisational relationships.

Assessment shall consider:

(a) Source Basis;

(b) relationship validity;

(c) effective period;

(d) lifecycle Status.

8. Institutional Evidence

Institutional Evidence includes information issued or maintained by recognised organisations.

Examples include:

(a) employment records;

(b) education records;

(c) membership records;

(d) service participation records.

Assessment shall consider:

(a) organisation recognition;

(b) issuance controls;

(c) identity verification performed by the organisation;

(d) record lifecycle.

9. Historical Evidence

Historical Evidence includes information demonstrating continuity of identity-related information over time.

Examples include:

(a) historical records;

(b) previous Identification Results;

(c) historical Source information;

(d) verified interactions.

Historical Evidence shall not replace current Evidence Validity requirements where current verification is required.

ANNEX V: APPLICABLE STANDARDS

Reference	Application
ISO/IEC 24760-1	Identity concepts, terminology and identity information relationships
ISO/IEC 24760-2	Identity-management architecture considerations applicable to Identification Services
ISO/IEC 24760-3	Identity-management operational processes
ETSI TS 119 461	Identity proofing requirements applicable to trust-service-related identity verification
ISO/IEC TS 29003	Identity proofing assurance considerations
ISO/IEC 11179 series	Metadata and semantic registration for identity-related information

Reference	Application
ISO/IEC 25012	Data quality model applicable to identity information
ISO/IEC 25024	Data quality measurement applicable to identity information
ISO/IEC 19795 series	Biometric performance testing where biometric comparison is used
ISO/IEC 30107 series	Presentation attack detection where biometric presentation is used
ISO/IEC 24745	Biometric information protection
ICAO Doc 9303	Machine-readable travel document requirements where applicable
ISO 15489-1	Records management principles
ISO/IEC 27001	Information security management controls
ISO/IEC 27701	Privacy information management controls

UNTITLED

UC-01: CROSS-SOURCE IDENTITY RESOLUTION AND DEDUPLICATION USE-CASE IMPLEMENTATION GUIDELINE

Version: 0.1 Latest update UTC: 2026-07-25T07:19:54Z

One governance model. Federated data and services. Clearly allocated responsibility.

This Guideline coordinates existing Framework Instruments for a specific cross-source matching use case. It does not create a separate Deduplication Trust Service.

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Guideline establishes use-case-specific requirements for Identity Resolution and duplicate detection involving two or more separately governed Sources.

1.2. This Guideline shall apply where the proposed processing concerns:

(a) identity-record duplicate detection;

(b) determination that records concern the same Subject or different Subjects;

(c) household, case or referral duplicate detection;

(d) detection of potentially repeated assistance, payments, benefits, services or interventions;

(e) one-to-one, one-to-many, many-to-many, transactional, periodic or bulk matching;

(f) biometric or non-biometric matching;

(g) matching within or across Federation Domains.

1.3. This Guideline shall coordinate the use of existing Trust Services, Sources, Profiles, agreement routes, Technical Specifications and Framework Decisions.

1.4. This Guideline shall not:

(a) create a new Trust Service Category;

(b) create a universal identity register;

(c) require centralisation of Source records;

(d) assign Authoritative Source Status;

(e) establish access, disclosure or reuse permission;

(f) assign Service Permission or Technical Exchange Permission;

(g) assign Qualified Status;

(h) establish eligibility, entitlement, fraud, misconduct or exclusion;

(i) approve operational activation.

Article 2: Controlling Framework Instruments

2.1. This Guideline shall apply together with the current approved versions of:

(a) , Trust Service Provider and Trust Service Common IDEHA-IG-SVC-TSP-001 Implementation;

(b) , Identification Service Implementation; IDEHA-IG-SVC-IDN-001

(c) , Authentication Service Implementation; IDEHA-IG-SVC-AUT-001

(d) , Authorisation Service Implementation; IDEHA-IG-SVC-AUZ-001

(e) , Federated Data Exchange Service Implementation; IDEHA-IG-SVC-FDX-001

(f) , Source and Authoritative Source Implementation; IDEHA-IG-SRC-ASO-001

(g) , Controlled Data Elements, Semantics and Data Quality IDEHA-IG-DAT-SEM-001 Implementation;

(h) , Biometric Implementation Controls, where biometric IDEHA-IG-BIO-GEN-001 information is processed;

(i) , Assurance, Conformity Assessment and Qualification IDEHA-IG-ASR-GEN-001 Implementation;

(j) the applicable participation, Federation Domain, security, Confidentiality, incident, Continuity, Correction, Review and Remedy instruments.

2.2. A service-specific Implementation Guideline shall govern the internal operation, evidence, assurance and lifecycle of the Trust Service to which it applies.

2.3. This Guideline shall govern only the use-case-specific assembly, purpose, Source participation, matching scope, output treatment, reuse conditions and activation sequence.

2.4. Where this Guideline and a service-specific Implementation Guideline address the same matter, the more specific service requirement shall govern the internal operation of that service.

2.5. A Scheme, Profile, Technical Specification or use-case decision shall not reduce a mandatory requirement established by the Main Framework or a controlling Implementation Guideline.

Article 3: Trust Service classification

3.1. Identity Resolution and duplicate detection shall remain functions of the Identification Service.

3.2. The native matching output shall be an Identity Resolution Result or another Identification Result permitted by the applicable Identification Service Profile.

3.3. The Federated Data Exchange Service shall support the controlled exchange of authorised requests, matching representations, responses, Trust Service Outputs and Exchange Evidence.

3.4. The Authentication Service shall authenticate participating Subjects, Actors, systems or Endpoints within its approved Service Scope.

3.5. The Authorisation Service or an assigned Policy Enforcement Function shall determine or enforce the permission applicable to matching, Source access, exchange and disclosure.

3.6. The Electronic Attestation Service shall apply only where an Identity Resolution Result or related statement is issued as an Electronic Attestation.

3.7. The Validation and Verification Service shall apply where a Source, Status, Trust Service, Trust Service Output, Trust Object or dependency requires Validation or Verification.

3.8. Digital Signing, Electronic Signature, Electronic Seal and Electronic Timestamp Services shall apply only where required by the applicable Profile, Technical Specification or evidence conditions.

3.9. The use of several Trust Services within one implementation shall not merge their Service Scopes, outputs, Status, evidence or responsibility.

Source governance

Separate local Authentication Service record decision Identification Service Identity Resolution Result Identity Resolution Authorisation Service Separate programme Policy decision or assistance decision

Federated Data Exchange Service

Article 4: Separation from infrastructure migration

4.1. Cross-source deduplication, data-quality improvement and migration from BRaVE 2 to BRaVE 3 shall remain separately governed workstreams.

4.2. A migration or hosting decision shall not determine:

(a) the deduplication object;

(b) the matching purpose;

(c) the Source model;

(d) Authoritative Source Status;

(e) the permitted matching data;

(f) biometric processing;

(g) disclosure, return or reuse rights;

(h) the required Trust Services;

(i) assurance or Qualified Status.

4.3. Placement within the same database, tenant, subscription, Resource Group or hosting environment shall not merge Source responsibility or decision competence.

4.4. Separation into different databases, tenants or Resource Groups shall not, by itself, establish federated governance or require a particular matching architecture.

4.5. Infrastructure cost and migration urgency shall not override the governance, Source, protection, agreement, assurance or activation requirements established by this Guideline.

SECTION 2: USE-CASE DECISION GATES

Article 5: Decision-gate sequence

5.1. The Responsible Actors shall complete the following gates in sequence:

(a) Gate 1: use-case and deduplication object;

(b) Gate 2: Actors, Sources and responsibility;

(c) Gate 3: data, document and biometric model;

(d) Gate 4: Trust Service, exchange and output configuration;

(e) Gate 5: agreement, assurance and testing readiness;

(f) Gate 6: operational activation.

5.2. A later gate shall not be completed where a mandatory decision from an earlier gate remains unresolved.

5.3. Detailed technical design shall not be approved before Gates 1 and 2 are complete.

5.4. Production data shall not be processed before the relevant agreement, permission, assurance and testing conditions are effective.

5.5. Operational matching shall not begin before Gate 6 is complete.

Gate 1 Gate 2 Gate 3 Gate 4 Gate 5 Gate 6 Use case Actors and Sources Data and biometrics Services and outputs Assurance and testing Activation

Article 6: Gate 1: use-case definition

6.1. The competent Framework Body shall approve a Use-Case Decision File.

6.2. The Use-Case Decision File shall identify:

(a) the recognised purpose;

(b) the object being deduplicated;

(c) the participating population;

(d) the participating Sources;

(e) the matching pattern;

(f) the intended outputs;

(g) the intended operational consequence;

(h) prohibited uses;

(i) the Responsible Actors;

(j) the applicable safeguards;

(k) unresolved conditions.

6.3. The deduplication object shall be identified as one or more of:

(a) a natural person;

(b) an Identity Registration Record;

(c) another identity-related record;

(d) a household or relationship;

(e) a case;

(f) a referral;

(g) an assistance event;

(h) a payment or transfer;

(i) a service or intervention;

(j) another defined record or event category.

6.4. The same Subject appearing in more than one Source shall not, by itself, constitute duplicate assistance or duplicate service delivery.

6.5. Where the concern is repeated assistance, the use case shall distinguish:

(a) determination that records concern the same Subject;

(b) determination that the relevant assistance or service event has occurred;

(c) the substantive programme decision.

6.6. An Identity Resolution Result shall not, by itself, establish:

(a) eligibility;

(b) entitlement;

(c) fraud;

(d) misconduct;

(e) exclusion;

(f) recovery of assistance;

(g) denial of a service.

6.7. The matching pattern shall identify whether processing is:

(a) one-to-one;

(b) one-to-many;

(c) many-to-many;

(d) transactional;

(e) periodic batch processing;

(f) full-population bulk processing;

(g) event-triggered processing.

6.8. Bulk or full-population matching shall require an express necessity, proportionality and protection assessment.

Article 7: Gate 2: Actors, Sources and responsibility

7.1. Each material function shall have an identifiable Responsible Actor.

7.2. The Actor and Responsibility Matrix shall identify responsibility for:

(a) use-case governance;

(b) Source operation;

(c) Source stewardship;

(d) semantic governance;

(e) Identification Service provision;

(f) matching operation;

(g) Federated Data Exchange Service provision;

(h) Authorisation Policy management;

(i) Policy Enforcement;

(j) candidate-match review;

(k) same-Subject or different-Subject confirmation;

(l) local record action;

(m) programme or assistance decisions;

(n) assurance and conformity assessment;

(o) security and incident management;

(p) Correction, Complaint, Review and Remedy;

(q) cessation and transition.

7.3. Each database, dataset, tenant, register, repository or defined part thereof used for matching shall be identified as a Source.

7.4. Each Source shall be governed through an applicable Source Profile.

7.5. The Source Profile shall identify:

(a) the Source and Source Identifier;

(b) the Source Holder;

(c) the Source Steward;

(d) the recognised purpose;

(e) the Source Scope;

(f) the maintained information and record categories;

(g) semantic and Data Quality requirements;

(h) Provenance and Freshness Conditions;

(i) permitted transformations and derivations;

(j) Access Conditions;

(k) Disclosure Conditions;

(l) permitted Trust Service uses and outputs;

(m) retention and lifecycle conditions;

(n) Correction, Review and Remedy Routes;

(o) applicable Assurance Conditions.

7.6. A Source shall have Authoritative Source Status only through Source Designation by a Framework Body acting within its decision competence.

7.7. A Source Designation shall identify the Attribute, event, record category, population, purpose and scope for which the Source is authoritative.

7.8. Neither an IOM Source nor a partner Source shall be treated as universally authoritative merely because it contains more records, hosts the matching service or operates within the primary BRaVE environment.

7.9. A copy, export, matching index, normalised representation, biometric template, comparison score or Identity Resolution Result shall not inherit Authoritative Source Status.

7.10. Authoritative Source Status shall not, by itself, create access, disclosure, exchange or Controlled Reliance.

Article 8: Gate 3: data, document and biometric model

8.1. The use case shall have an approved semantic and data-quality model before matching rules are implemented.

8.2. Each Attribute used for matching shall identify:

(a) an Attribute Identifier;

(b) meaning;

(c) datatype;

(d) value domain;

(e) permitted value states;

(f) permitted transformations;

(g) Source Basis;

(h) Data Quality requirements;

(i) Provenance requirements;

(j) Freshness Conditions;

(k) permitted matching use;

(l) disclosure status;

(m) lifecycle and Correction conditions.

8.3. The semantic model shall distinguish, where applicable:

(a) legal, recorded, preferred, former and alternative names;

(b) nationality, citizenship, country of origin and habitual residence;

(c) sex recorded by a Source and gender-related information;

(d) exact, estimated, approximate, disputed and partially known values;

(e) identity, household, case, referral and assistance relationships;

(f) Source values and derived values.

8.4. The Source representation shall remain preserved.

8.5. A normalised, transliterated, tokenised or otherwise derived matching representation shall remain separately identifiable and shall retain its Provenance and transformation Version.

8.6. The applicable Technical Specification shall define:

(a) character encoding and Unicode treatment;

(b) original-script preservation;

(c) transliteration and normalisation;

(d) dates, times, time zones and partial dates;

(e) country, language and script codes;

(f) document categories and formats;

(g) document-number syntax;

(h) machine-readable travel-document treatment;

(i) technical schemas and validation rules.

8.7. Where biometric information is processed, the Biometric Implementation Plan shall identify:

(a) the biometric purpose;

(b) biometric modalities;

(c) affected population;

(d) participating Sources;

(e) whether raw samples, templates, protected references or a combination are processed;

(f) where templates are generated;

(g) biometric formats;

(h) capture and quality requirements;

(i) the matching algorithm and Version;

(j) candidate and confirmation thresholds;

(k) false-match and false-non-match treatment;

(l) human-review conditions;

(m) storage and processing locations;

(n) return, retention and deletion conditions;

(o) reuse and onward-disclosure restrictions;

(p) compromise, Recovery and re-enrolment procedures.

8.8. Raw samples, templates, protected references, comparison scores and identity determinations shall remain separately identifiable.

8.9. A biometric comparison score or threshold crossing shall not, by itself, constitute a confirmed same-Subject determination.

8.10. Raw biometric material shall remain with the originating Source unless central processing or transfer is separately justified, authorised and protected.

Article 9: Gate 4: Trust Service and output configuration

9.1. The use case shall operate under an approved Identification Service Profile and Identity Resolution Profile.

9.2. The Profiles shall identify:

(a) the Identity Provider;

(b) the Service Scope;

(c) participating Sources;

(d) Subject and record categories;

(e) population scope;

(f) permitted Attributes and biometric modalities;

(g) matching methods;

(h) algorithm and Version;

(i) candidate and outcome classes;

(j) thresholds;

(k) Assurance Conditions;

(l) human-review requirements;

(m) retention and deletion;

(n) permitted outputs;

(o) permitted result uses;

(p) Complaint, Correction, Review and Remedy Routes.

9.3. The applicable Federated Data Exchange Service Profile shall identify:

(a) participating Actors;

(b) Federation Domains;

(c) Endpoints;

(d) Technical Exchange Routes;

(e) exchange patterns;

(f) payload classes;

(g) Security Conditions;

(h) Exchange Evidence;

(i) Continuity and Recovery conditions.

9.4. The applicable Authorisation Policy shall identify:

(a) permitted Requesting Actors;

(b) permitted Responding Actors;

(c) approved purposes;

(d) participating Sources;

(e) permitted matching functions;

(f) permitted payload classes;

(g) permitted recipients;

(h) time and validity conditions;

(i) disclosure restrictions;

(j) reuse and onward-disclosure restrictions.

9.5. The Matching Output and Reuse Matrix shall identify what is returned to each participating Actor or Source.

9.6. The Matrix shall distinguish:

(a) Source Attributes;

(b) normalised or tokenised matching representations;

(c) raw biometric samples;

(d) biometric templates or protected references;

(e) comparison scores;

(f) candidate lists;

(g) confirmed Identity Resolution Results;

(h) unable-to-determine results;

(i) technical failures;

(j) assistance or service information;

(k) Exchange Evidence.

9.7. For each output, the Matrix shall identify:

(a) the producing Actor or Trust Service;

(b) the permitted recipient;

(c) the permitted purpose;

(d) disclosure mode;

(e) storage permission;

(f) retention period;

(g) reuse permission;

(h) onward-disclosure permission;

(i) permitted local action;

(j) required protection;

(k) Correction and Review Route.

9.8. The minimum-result principle shall apply.

9.9. A participating Source shall ordinarily receive only the result required for the approved purpose and shall not receive another Source's complete record.

9.10. Technical possession of an output shall not create a right to store, reuse, disclose or rely upon that output.

IOM local decision IOM Policy IOM Source Enforcement Federated Data Identification Service Candidate or confirmed Partner local decision Exchange Service Controlled matching Identity Resolution Result Partner Policy Partner Source Enforcement Separate programme decision

Article 10: Gate 5: agreement, assurance and testing readiness

10.1. The applicable Data Sharing Agreement or equivalent agreement route shall expressly cover the approved use case.

10.2. General data-sharing language shall not be presumed to authorise:

(a) full-population matching;

(b) one-to-many biometric matching;

(c) shared matching indexes;

(d) transfer of raw biometric samples;

(e) exchange of biometric templates;

(f) cross-border processing;

(g) matching-provider access;

(h) return of underlying Source data;

(i) cross-programme reuse;

(j) onward disclosure.

10.3. The use-case agreement schedule shall identify:

(a) purpose;

(b) participating Actors and Sources;

(c) Roles and responsibilities;

(d) permitted data elements;

(e) biometric processing;

(f) matching pattern;

(g) processing and storage locations;

(h) providers and subprocessors;

(i) permitted outputs;

(j) return and reuse rights;

(k) retention and deletion;

(l) security and incident obligations;

(m) Correction, Complaint, Review and Remedy;

(n) termination and cessation treatment.

10.4. The Responsible Actors shall determine the applicable Assurance Conditions.

10.5. The assurance assessment shall consider:

(a) population size;

(b) matching pattern;

(c) biometric processing;

(d) Source quality;

(e) cross-border scope;

(f) false-match and false-non-match consequences;

(g) automation;

(h) possible adverse effects;

(i) reliance by another Actor;

(j) provider-chain risk;

(k) security and Continuity risk.

10.6. The competent Framework Body shall determine separately whether Qualified Status is required for:

(a) the Trust Service Provider;

(b) the Identification Service;

(c) an Authoritative Source;

(d) an Identity Resolution Result;

(e) an Electronic Attestation;

(f) another eligible controlled object.

10.7. Qualified Status assigned to one object shall not transfer to another object.

10.8. Qualified Status shall not, by itself, create access, disclosure, exchange or Controlled Reliance.

10.9. A controlled pilot shall be completed before operational rollout.

10.10. Testing shall cover:

(a) Source mapping;

(b) semantic interoperability;

(c) multilingual and script handling;

(d) document processing;

(e) date and demographic treatment;

(f) biometric format compatibility;

(g) biometric quality;

(h) algorithm performance;

(i) false matches and false non-matches;

(j) demographic-performance variation;

(k) candidate review;

(l) Authentication and Authorisation;

(m) Policy Enforcement;

(n) payload protection;

(o) output minimisation;

(p) retention and deletion;

(q) Correction, Review and Remedy;

(r) Continuity and Recovery.

10.11. A material security, protection, agreement, assurance or remedy non-conformity shall prevent activation of the affected scope.

Article 11: Gate 6: operational activation

11.1. Operational activation shall require a recorded Framework Decision.

11.2. Before activation, the competent Framework Body shall verify:

(a) approval of the Use-Case Decision File;

(b) approval of the Actor and Responsibility Matrix;

(c) effective Source Profiles;

(d) effective Source Designations where required;

(e) approval of the Identification Service and Identity Resolution Profiles;

(f) approval of the Federated Data Exchange Service Profile;

(g) approval of the Authorisation Policy;

(h) approval of the Matching Output and Reuse Matrix;

(i) completion of the Biometric Implementation Plan where applicable;

(j) effectiveness of the agreement and legal basis;

(k) recognition of the required Trust Services;

(l) effectiveness of Service Permission;

(m) effectiveness of Technical Exchange Permission;

(n) completion of testing and conformity assessment;

(o) resolution of material non-conformities;

(p) readiness of incident, Continuity and Recovery arrangements;

(q) readiness of Correction, Complaint, Review and Remedy Routes.

11.3. The activation decision shall identify:

(a) participating Actors and Sources;

(b) the activated Service Scope;

(c) matching patterns;

(d) permitted Attributes and biometric objects;

(e) permitted outputs;

(f) restrictions;

(g) Effective Date;

(h) Validity Period;

(i) review date;

(j) Change Control conditions;

(k) Suspension and cessation conditions.

11.4. Technical reachability, system configuration, onboarding, catalogue listing, testing or publication shall not constitute operational activation.

Operational matching begins only after the activation decision records the approved scope, permissions, evidence, restrictions and review conditions.

SECTION 3: MATCHING OUTCOMES AND SUBSEQUENT DECISIONS

Article 12: Matching outcome classes

12.1. The Identity Resolution Profile shall distinguish:

(a) no candidate identified;

(b) candidate relationship;

(c) confirmed same-Subject determination;

(d) confirmed different-Subject determination;

(e) unable-to-determine result;

(f) data-quality failure;

(g) biometric-quality failure;

(h) technical failure.

12.2. A candidate match shall not constitute a confirmed Identity Resolution Result.

12.3. A technical or quality failure shall not be represented as a non-match.

12.4. An unable-to-determine result shall not be represented as a confirmed different-Subject determination.

12.5. A match, non-match or similarity score shall not constitute a finding of fraud, misconduct, entitlement or ineligibility.

12.6. An Identity Resolution Result shall identify or reference:

(a) the producing Identification Service;

(b) the matching purpose;

(c) the evaluated Sources;

(d) the matching method and Version;

(e) the outcome class;

(f) the applicable threshold class;

(g) quality and Assurance information;

(h) evaluation time;

(i) Validity Period;

(j) limitations and caveats;

(k) human-review requirements.

A candidate match is an input to an authorised confirmation process. It shall not directly trigger record merging, exclusion, recovery action or denial of assistance.

Article 13: Local record actions

13.1. A decision to link, merge, separate, restrict, correct, retain or delete Source records shall remain separate from the Identity Resolution Result.

13.2. An Identity Resolution Result shall not directly alter a Source record.

13.3. A local record-action decision shall identify:

(a) the affected Source and records;

(b) the action;

(c) the purpose;

(d) the supporting Identity Resolution Result;

(e) additional evidence;

(f) the Responsible Actor;

(g) the Effective Date and Status;

(h) the effect on Identifiers and dependent records;

(i) the Correction, Review and Remedy Routes.

13.4. A record merge shall preserve sufficient Provenance and Historical State to reconstruct the earlier records and decisions.

13.5. A record-separation action shall identify dependent records and corrective actions.

13.6. Correction of one Source shall not automatically correct another Source.

Article 14: Programme and assistance decisions

14.1. A programme, assistance, eligibility, entitlement, payment, referral or service decision shall remain separate from Identity Resolution.

14.2. The responsible programme Actor shall determine whether and how an Identity Resolution Result supports the substantive decision.

14.3. A confirmed same-Subject determination shall not establish that:

(a) assistance has already been received;

(b) two assistance events are equivalent;

(c) assistance was unauthorised;

(d) assistance is recoverable;

(e) a Subject shall be excluded.

14.4. A final significant adverse decision based substantially on automated matching shall be reviewed by a natural person.

Candidate relationship

Authorised review

Confirmed Identity Resolution Result

Separate Source Separate programme or No further action record decision assistance decision

Source lifecycle Programme lifecycle and evidence and remedy

SECTION 4: PROTECTION, LIFECYCLE AND CHANGE

Article 15: Return, reuse and onward disclosure

15.1. Matching outputs shall be used only for the purpose, Actor, programme, Source Scope, Federation Domain and period approved through the applicable instruments.

15.2. Cross-programme, cross-country, cross-Scheme or cross-domain reuse shall require a separately approved basis.

15.3. A result created for Source data-quality improvement shall not be reused for eligibility, fraud investigation, enforcement or exclusion unless a separately authorised basis applies.

15.4. Return or disclosure of an underlying Attribute, document image, raw biometric sample, template or comparison score shall require express authorisation.

15.5. Reuse shall preserve:

(a) Provenance;

(b) Source Basis;

(c) algorithm and Profile Version;

(d) limitations and caveats;

(e) Historical State;

(f) Validity Period.

15.6. A Trust Service Provider or technical provider shall not reuse Source information, biometric information, matching representations or results for product development, model training, benchmarking or another purpose unless a separately authorised basis applies.

Article 16: Protected-Person Safeguards

16.1. The use case shall be designed to prevent unjustified exclusion, misidentification, surveillance, retaliation, stigma or denial of assistance.

16.2. An Accessible Alternative shall be provided where biometric, document, device, connectivity, language, literacy or disability conditions create an unjustified barrier.

16.3. Failure to provide a biometric or satisfy one technical route shall not, by itself, determine identity, eligibility, entitlement, fraud, misconduct or exclusion.

16.4. A Protected Person shall receive information appropriate to the operational context concerning:

(a) the matching purpose;

(b) participating organisations;

(c) information and biometric modalities used;

(d) possible outcomes;

(e) possible operational consequences;

(f) retention and reuse;

(g) Correction, Complaint, Review and Remedy Routes.

16.5. Consent shall not be treated as the sole governance basis where dependency, power imbalance or inability to refuse affects voluntariness.

16.6. The use case shall include controls against function creep and unauthorised population expansion.

Article 17: Correction, Complaint, Review and Remedy

17.1. Each participating Actor shall provide an accessible route for correction of information and decisions within its responsibility.

17.2. The use case shall provide a Complaint and Review Route for:

(a) false matches;

(b) false non-matches;

(c) disputed candidate relationships;

(d) incorrect record linking or merging;

(e) biometric quality findings;

(f) unauthorised disclosure or reuse;

(g) adverse programme decisions based on the result.

17.3. A contested result shall be subject to human review before a final significant Adverse Protected-Person Effect.

17.4. Remedy shall address, where applicable:

(a) correction of the Identity Resolution Result;

(b) separation of records;

(c) correction of dependent Source records;

(d) reassessment of programme decisions;

(e) notification to affected Actors;

(f) restriction or deletion of unauthorised copies;

(g) restoration of access or assistance;

(h) preservation of evidence.

Article 18: Change Control

18.1. A material change shall be assessed before implementation.

18.2. Material changes shall include:

(a) addition of a Source;

(b) population expansion;

(c) a new purpose;

(d) a new matching pattern;

(e) a new Attribute;

(f) a semantic change;

(g) a new biometric modality;

(h) an algorithm or threshold change;

(i) a provider or hosting change;

(j) a cross-border processing change;

(k) a new output or recipient;

(l) expanded reuse;

(m) changed retention;

(n) a changed operational consequence.

18.3. Change assessment shall identify the affected:

(a) Framework Decisions;

(b) Profiles;

(c) Technical Specifications;

(d) agreement conditions;

(e) permissions;

(f) assurance and Qualified Status;

(g) testing;

(h) protection and remedy requirements.

18.4. A material change outside the activated scope shall require a new or amended activation decision.

Article 19: Incident, restriction, Suspension and cessation

19.1. The Responsible Actors shall maintain procedures for:

(a) unauthorised access or disclosure;

(b) biometric compromise;

(c) algorithm failure;

(d) excessive false matches or false non-matches;

(e) semantic or Source-quality failure;

(f) provider-chain incidents;

(g) loss of evidence;

(h) unauthorised reuse.

19.2. Restriction or Suspension shall identify:

(a) the affected scope;

(b) the reason;

(c) the evidence;

(d) the Effective Date;

(e) temporary controls;

(f) the review interval;

(g) exit conditions.

19.3. Suspension of a Trust Service shall not automatically invalidate every historical output unless the applicable Framework Decision assigns that effect.

19.4. Cessation shall address:

(a) termination of exchange;

(b) provider transition;

(c) return or deletion of Source and biometric information;

(d) preservation of evidence;

(e) continuing Validation, Review and Remedy;

(f) notification to affected Actors;

(g) Historical State.

ANNEX A: MANDATORY IMPLEMENTATION PACKAGE

Instrument	Use-case-specific function
Use-Case Decision File	Defines the object, purpose, population, pattern, outputs and intended consequence
Scheme	Establishes the governed context and participating Actors
Actor and Responsibility Matrix	Allocates each material function and decision
Source Profiles	Define each Source, scope, semantics, quality, access, disclosure and lifecycle
Source Designation decisions	Assign Authoritative Source Status where required
Controlled data-element registry	Defines permitted Attributes, value domains and semantic Versions

Instrument	Use-case-specific function
Source mapping specification	Maps local Source data to the controlled semantic model
Identification Service Profile	Defines the Identification Service Scope
Identity Resolution Profile	Defines matching methods, thresholds, outcomes and human review
Biometric Implementation Plan	Defines modalities, raw samples, templates, algorithms, quality and protection
Federated Data Exchange Service Profile	Defines Actors, Endpoints, routes, payloads and Exchange Evidence
Authorisation Policy	Defines permitted matching, access, exchange and disclosure
Data Sharing Agreement use-case schedule	Defines the agreement and processing conditions
Matching Output and Reuse Matrix	Defines return, storage, retention, reuse and onward disclosure
Technical Specifications	Define schemas, formats, standards, interfaces and validation rules
Assurance and qualification record	Defines assurance, conformity and Qualified Status
Pilot and test report	Records testing, limitations, non-conformities and residual risk
Activation decision	Records the approved operational scope and restrictions
Correction, Review and Remedy procedure	Provides challenge and corrective routes
Incident and cessation plan	Defines incident, Suspension, transition, deletion and evidence preservation

ANNEX B: INITIAL DECISION WORKSHOP

The following questions shall be resolved before detailed solution design is approved:

What object is being deduplicated?

What is the recognised purpose?

Is the concern identity duplication, assistance duplication or both?

Which Sources participate?

Who is the Source Holder for each Source?

Who is the Source Steward for each Source?

Which Source is authoritative for each relevant Attribute, event or decision?

Is matching one-to-one, one-to-many, many-to-many, periodic or bulk?

Which Attributes are permitted?

Which semantic definitions, value domains and code lists apply?

Which document categories and recognition rules apply?

Are biometrics used?

Are raw samples, templates, protected references or a combination processed?

Where are templates generated and stored?

Which algorithms, Versions and thresholds apply?

Who reviews candidate matches?

Who confirms same-Subject or different-Subject results?

What result is returned to each Actor or Source?

Are underlying Attributes, samples, templates or scores returned?

What storage and retention rights apply?

What reuse and onward-disclosure rights apply?

Who can link, merge, correct, restrict or separate local records?

Who makes any programme or assistance decision?

Which cross-border and provider-chain conditions apply?

Which Trust Services and permissions are required?

What assurance and Qualified Status are required?

What testing and acceptance criteria apply?

Which unresolved conditions prevent progression?

ANNEX C: MATCHING OUTPUT AND REUSE MATRIX

Output or information	Producing Actor or Service	Permitted recipient	Purpose	Disclosure mode	Storage	Ret
Source Attribute						
Normalised matching representation						
Raw biometric sample						
Biometric template						
Comparison score						
Candidate relationship						

Output or information	Producing Actor or Service	Permitted recipient	Purpose	Disclosure mode	Storage	Ret
Confirmed same-Subject result						
Confirmed different-Subject result						
Unable-to-determine result						
Assistance or service information						
Exchange Evidence						

ANNEX D: BIOMETRIC CONFIGURATION DECISION RECORD

Purpose and scope

- ☐ Biometric purpose identified
- ☐ Population identified
- ☐ Participating Sources identified
- ☐ Biometric modality identified
- ☐ One-to-one, one-to-many or bulk comparison identified
- ☐ Necessity and proportionality recorded
- ☐ Accessible Alternative identified

Biometric objects

- ☐ Raw samples used
- ☐ Templates used
- ☐ Protected references used
- ☐ Local template generation defined
- ☐ Shared template generation defined
- ☐ Storage locations defined
- ☐ Processing locations defined
- ☐ Return conditions defined
- ☐ Retention and deletion defined

Algorithm and performance

- ☐ Algorithm identified
- ☐ Provider identified
- ☐ Algorithm Version identified
- ☐ Feature-extraction Version identified
- ☐ Template format identified
- ☐ Quality measure identified
- ☐ Candidate threshold identified

- ☐ Confirmation threshold identified
- ☐ False-match criterion identified
- ☐ False-non-match criterion identified
- ☐ Demographic-performance testing completed
- ☐ Human-review range identified

Protection and lifecycle

- ☐ Template protection defined
- ☐ Presentation-attack detection defined
- ☐ Cross-border processing defined
- ☐ Provider access defined
- ☐ Compromise procedure defined
- ☐ Re-enrolment procedure defined
- ☐ Algorithm migration procedure defined
- ☐ Historical-result treatment defined
- ☐ Incident notification defined
- ☐ Correction, Review and Remedy defined

ANNEX E: DECISION-GATE READINESS CHECKLIST

Gate 1: Use case

- ☐ Deduplication object defined
- ☐ Purpose defined
- ☐ Intended consequence defined
- ☐ Identity and assistance decisions separated
- ☐ Matching pattern defined
- ☐ Population scope defined
- ☐ Use-Case Decision File approved

Gate 2: Actors and Sources

- ☐ Participating Actors identified
- ☐ Responsibilities allocated
- ☐ Source Holders identified
- ☐ Source Stewards identified
- ☐ Source Profiles approved
- ☐ Authoritative Source Scopes designated where required
- ☐ Technical and governance boundaries separated

Gate 3: Data and biometrics

- ☐ Controlled data elements defined
- ☐ Source mappings completed
- ☐ Unicode and multilingual treatment defined
- ☐ Date and demographic treatment defined
- ☐ Document-recognition rules defined
- ☐ Data Quality and Freshness Conditions defined
- ☐ Raw sample and template model defined
- ☐ Algorithms, Versions and thresholds defined
- ☐ Human-review conditions defined

Gate 4: Services and outputs

- ☐ Identification Service Profile approved
- ☐ Identity Resolution Profile approved
- ☐ Federated Data Exchange Service Profile approved

- ☐ Authorisation Policy approved
- ☐ Endpoints and Technical Exchange Routes identified
- ☐ Matching Output and Reuse Matrix approved
- ☐ Local record-action procedure approved
- ☐ Programme-decision separation confirmed

Gate 5: Agreement, assurance and testing

- ☐ Agreement route covers the use case
- ☐ Cross-border assessment complete
- ☐ Provider chain recorded
- ☐ Protected-Person Safeguards complete
- ☐ Assurance assessment complete
- ☐ Qualification decision complete
- ☐ Conformity Assessment complete
- ☐ Pilot and testing complete
- ☐ Material non-conformities resolved

Gate 6: Activation

- ☐ Service Permission effective
- ☐ Technical Exchange Permission effective
- ☐ Incident and Continuity arrangements ready
- ☐ Correction, Review and Remedy Routes ready
- ☐ Activation decision recorded
- ☐ Review date established
- ☐ Change Control active

> ⚠ Implementation condition
>
> Operational implementation shall not proceed where the deduplication object, Sources, responsibilities, semantic model, biometric model, output rights, reuse conditions, agreement basis, assurance requirements or activation conditions remain unresolved.