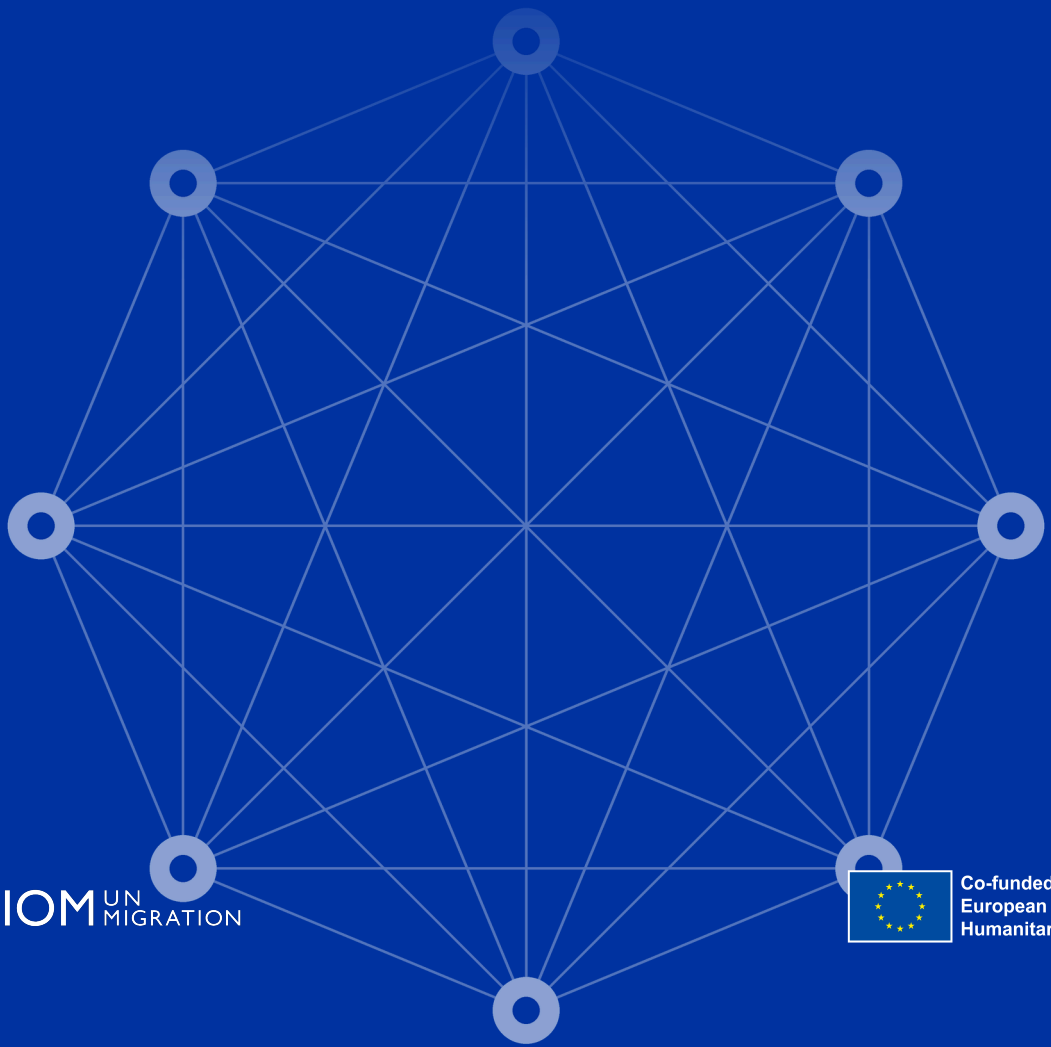
IDEHA TRUST FRAMEWORK

The governance, trust, assurance and controlled-exchange architecture for the IDEHA ecosystem



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

The governance, trust, assurance and controlled-exchange architecture for the IDEHA ecosystem

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

30 June 2026

CONTENTS

i Document identity

- **Programme:** Interoperable Data Ecosystem for Humanitarian Assistance (IDEHA)
- **Document type:** Framework
- **Prepared for:** International Organization for Migration (IOM)
- **Publishing year:** 2026
- **Status:** Initial draft
- **Confidentiality status:** Confidential

! Use statement and licence

Governance and assurance reference for IDEHA participation, controlled interaction, source recognition, attestation-based exchange, federated data exchange, safeguards, review and remedy.

PART I: GENERAL PROVISIONS AND CONSTITUTIONAL FRAMEWORK

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter

1.1. This Framework lays down rules on:

(a) governance and Participation within and between humanitarian Federation Domains;

(b) recognition, Status, qualification and supervision of Actors, Trust Service Providers, Trust Services, Trust Objects, Sources, mechanisms, devices, Technical Exchange Routes and Framework Instruments;

(c) creation, issuance, exchange, Verification, Validation, lifecycle management and Controlled Reliance of Controlled Matters;

(d) Status Publication, the Humanitarian Trust List, Registers, Catalogues and federation discovery;

(e) security, continuity, Review, Correction, Remedy and Change Control.

1.2. This Framework establishes common trust conditions for controlled interactions within and between Federation Domains.

1.3. This Framework governs trust functions and Controlled Effects and shall not determine the substantive humanitarian, administrative, programme or operational outcome for which a Controlled Matter is used.

Article 2: Scope

2.1. This Framework applies to a Controlled Matter only within the purpose, Federation Domain, Scheme, Profile, Role, scope, Validity Period and conditions assigned through the applicable Framework Instrument or Framework Decision.

2.2. This Framework supports organisational, national, regional, programme, purpose-specific, hybrid and Nested Federation arrangements.

2.3. This Framework shall not establish:

(a) a central humanitarian identity authority;

(b) a universal register of natural persons;

(c) central ownership of data held by Participating Actors;

(d) general authority over decisions retained by a Participating Actor or Federation Domain.

2.4. A matter shall not fall within the scope of this Framework by reason only of technical connection, operational use, publication, reference, contractual association or similarity to a Controlled Matter.

2.5. This Framework shall apply without prejudice to applicable law and External Instruments.

Article 3: Nature and effect of the Framework

3.1. This Framework is a contractually applied governance instrument for federated data exchange for humanitarian institutions.

3.2. An Actor shall be bound by this Framework only through accession, a Federation Agreement or another Recognised Instrument assigning that effect.

3.3. Accession or recognition shall create only the obligations, Status and Controlled Effects assigned within its scope.

3.4. Recognition, Status, qualification or a Framework Decision under this Framework shall not, by itself, confer public-law authority, External Legal Status or External Legal Effect.

3.5. External Legal Status or External Legal Effect shall arise only under the applicable legal order or External Instrument and within the scope assigned by it.

Article 4: Federation Domains

4.1. This Framework shall operate through Federation Domains connected by recognised Federation Trust Relationships.

4.2. Each Federation Domain shall maintain the governance, Participation, Source, Trust Service, policy, Technical Exchange and Controlled Reliance boundaries assigned to it.

4.3. A Nested Federation shall comply with the conditions applicable to the parent and nested Federation Domains.

4.4. A Federation Trust Relationship shall be established through a Federation Agreement or another Recognised Instrument.

4.5. Recognition in one Federation Domain shall not, by itself, create recognition, Status, Service Permission, Technical Exchange Permission or Controlled Reliance in another Federation Domain.

SECTION 2: CONSTITUTIONAL GOVERNANCE

Article 5: Framework Steward

5.1. The International Organization for Migration shall act as Framework Steward.

5.2. The Framework Steward shall maintain:

(a) the constitutional integrity and authoritative text of the Framework;

(b) the Framework architecture and instrument hierarchy;

(c) the controlled evolution and publication of the Framework;

(d) consistency between Main Parts, Annexes and subordinate Framework Instruments;

(e) the governance route for changes to controlled categories and instrument codes.

5.3. The Framework Steward shall not exercise Decision Competence assigned to another Framework Body unless a Recognised Instrument expressly assigns that competence.

5.4. The Framework Steward shall not acquire operational responsibility for a Trust Service, Source, Technical Exchange Route or local decision by reason only of stewardship.

Article 6: Framework Bodies and Framework Functions

6.1. The Framework shall operate through Framework Bodies assigned identified Framework Functions and Decision Competence.

6.2. A Framework Body shall act only within the scope assigned by the Framework or another Recognised Instrument.

6.3. Governance, recognition, qualification, supervision, Status Publication, Review and Remedy shall remain separate from Trust Service operation, Source responsibility, Technical Exchange operation and local Controlled Reliance.

6.4. The same Actor shall perform more than one Framework Function only where each function, scope, responsibility, evidence requirement and conflict control is assigned separately.

6.5. Part IV shall govern Framework Bodies, Decision Competence, Framework Decisions, supervision and Status Publication.

Article 7: Decision Competence and Framework Decisions

7.1. A Framework Body shall adopt a Framework Decision only within assigned Decision Competence.

7.2. A Framework Decision shall identify:

(a) the deciding Framework Body;

(b) the affected Controlled Matter;

(c) the applicable Framework Instrument and Version;

(d) the evidence basis;

(e) the assigned scope and conditions;

(f) the Effective Date;

(g) the Controlled Effect;

(h) the applicable Review Route.

7.3. A Framework Decision shall have effect only within the scope and conditions assigned to it.

7.4. A Framework Decision shall be recorded in a Decision File before its Controlled Effect begins.

SECTION 3: FRAMEWORK INSTRUMENTS

Article 8: Framework Instrument categories

8.1. The Framework Instrument categories are:

(a) Main Parts;

(b) Annexes;

(c) Implementation Guidelines;

(d) Schemes;

(e) Profiles;

(f) Technical Specifications;

(g) Body Instruments.

8.2. A document, procedure, record or technical artefact shall become a Framework Instrument only through the recognition route assigned by the Framework.

8.3. Each Framework Instrument shall identify its Instrument Identifier, purpose, scope, responsible Actor, Instrument Status, Version and Effective Date.

8.4. A new Framework Instrument category shall be established only by amendment of this Article and the corresponding entry in the Instrument Code Catalogue.

8.5. A subordinate Framework Instrument shall not create a new Trust Service Category, Trust Object Category, Status category, qualification route or Controlled Effect.

Article 9: Schemes and Profiles

9.1. A Scheme shall establish a governed arrangement for an identified purpose, context and participating scope.

9.2. A Scheme shall identify:

(a) the recognised purpose;

(b) the participating Federation Domains and Actors;

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

(d) the applicable policies, safeguards and Reliance Conditions;

(e) the applicable Profiles and implementation instruments;

(f) the governance, lifecycle, Review and Remedy arrangements.

9.3. A Profile shall select requirements and conditions for an identified Actor, Trust Service, Trust Object, Source, mechanism, device, Technical Exchange Route or process.

9.4. A Scheme or Profile shall not, by itself, assign Participation, Trust Service Provider Status, Trust Service Status, Source Status, Service Permission, Technical Exchange Permission, Qualified Status, access, disclosure or Controlled Reliance.

9.5. The approval, publication, restriction, suspension, withdrawal and change of a Scheme or Profile shall follow the governance route assigned by the Framework.

Article 10: Hierarchy and conflict of Framework Instruments

10.1. Main Parts shall prevail over Annexes and subordinate Framework Instruments.

10.2. Annexes shall prevail over Implementation Guidelines, Schemes, Profiles, Technical Specifications and Body Instruments within their subject matter.

10.3. A subordinate Framework Instrument shall not alter, extend or restrict a rule, category, Decision Competence or Controlled Effect established by a higher-ranking Framework Instrument.

10.4. A Body Instrument shall remain within its enabling provision and assigned Decision Competence.

10.5. Where Framework Instruments conflict, the higher-ranking Framework Instrument shall prevail to the extent of the conflict.

10.6. A conflict shall be recorded and resolved through the applicable Change Control and Review routes.

Article 11: Technology neutrality and implementation boundaries

11.1. Main Parts and Annexes shall remain neutral as to specific standards, protocols, formats, products and deployment models.

11.2. An Implementation Guideline shall assign implementation requirements and identify the Recognised Standards applicable to its subject matter where required.

11.3. A Scheme shall establish the governed context and shall refer to the applicable Implementation Guidelines and Profiles.

11.4. A Profile shall select the requirements, options and conditions applicable within its scope.

11.5. A Technical Specification shall assign schemas, protocols, formats, algorithms, parameters, interfaces, configurations, test conditions and other detailed technical requirements.

11.6. A deployment instruction shall address an environment-specific implementation and shall not form part of the Framework unless recognised as a Framework Instrument.

11.7. Technical conformity, testing, connection or availability shall not, by itself, create recognition, Service Permission, Technical Exchange Permission, access, disclosure, Qualified Status or Controlled Reliance.

SECTION 4: ACCESSION, APPLICATION AND INTERPRETATION

Article 12: Accession and application

12.1. An accession instrument shall identify:

(a) the Actor;

(b) the applicable Federation Domain;

(c) the Participation Scope and Assigned Roles;

(d) the applicable Schemes and Profiles;

(e) the Effective Date and Validity Period;

(f) the conditions, restrictions and lifecycle requirements;

(g) the applicable Review and Remedy Routes.

12.2. Accession shall not, by itself, assign Source Status, Trust Service Provider Status, Trust Service Status, Service Permission, Technical Exchange Permission, access, disclosure, Qualified Status or Controlled Reliance.

12.3. A Participating Actor shall perform each assigned function in accordance with the applicable Framework Instruments and Federation Agreement.

12.4. Withdrawal from Participation shall not remove obligations concerning Confidentiality, evidence, Retention, Review, Remedy or earlier Controlled Reliance where those obligations continue under an applicable Framework Instrument.

Article 13: Interpretation and External Instruments

13.1. This Framework shall be interpreted according to its wording, purpose, structure, hierarchy and the definitions in Part II.

13.2. Interpretation shall preserve the separation between Actors, Roles, Trust Service Providers, Trust Services, Trust Objects, Trust Service Outputs, Sources, Technical Exchange Routes, policies and Controlled Reliance.

13.3. A provision shall not be interpreted as creating a Controlled Effect that it does not expressly assign.

13.4. Recognition under an External Instrument shall not assign Status under this Framework unless the competent Framework Body assigns that Status through the applicable Framework route.

13.5. Recognition under this Framework shall not, by itself, assign External Legal Status or External Legal Effect.

13.6. Where an External Instrument imposes a stricter safeguard, the responsible Actor shall apply that safeguard within its applicable scope unless it conflicts with a higher-ranking applicable obligation.

PART II: DEFINITIONS AND CONTROLLED TERMS

Article 14: Application of definitions

14.1. For the purposes of the Framework, the definitions in this Part shall apply.

14.2. A definition shall determine the meaning of a term and shall not, by itself, assign Status, recognition, permission, qualification, Controlled Reliance or another Controlled Effect.

14.3. A term defined in this Part shall retain the same meaning throughout the Trust Framework unless a provision expressly assigns a narrower meaning for an identified scope.

14.4. A capitalised term not defined in this Part shall not be treated as a Controlled Term.

14.5. Controlled Term means a term assigned a specific meaning by this Part.

Article 15: Framework, governance and controlled matters

15.1. Framework means the iDEHA Trust Framework.

15.2. Framework Steward means the Actor assigned responsibility for the constitutional integrity, controlled evolution and authoritative publication of the Framework.

15.3. Framework Body means a governed body or organisational arrangement assigned one or more Framework Functions.

15.4. Framework Function means a governance, recognition, qualification, supervision, publication, Review, Remedy or other function assigned under the Framework.

15.5. Controlled Framework Function means a Framework Function subject to assigned Decision Competence, conditions, evidence, lifecycle and Controlled Effects.

15.6. Decision Competence means the competence assigned to a Framework Body or Actor to adopt an identified decision within an assigned scope.

15.7. Framework Decision means a decision adopted within assigned Decision Competence under the Framework.

15.8. Controlled Effect means an effect expressly assigned by the Framework or an applicable Framework Instrument.

15.9. Controlled Matter means an Actor, Role, Trust Service Provider, Trust Service, Trust Object, Trust Service Output, Source, mechanism, device, Technical Exchange Route, Framework Instrument, record, Entry, decision, Status or other matter governed by the Framework.

15.10. Status-Bearing Matter means a Controlled Matter to which the Framework assigns Status.

15.11. Recognised Instrument means an instrument assigned recognition under the Framework.

15.12. External Instrument means a legal, contractual, organisational, technical or other instrument originating outside the Framework.

15.13. External Legal Status means status, validity, authority, qualification or recognition assigned under an external legal order.

15.14. External Legal Effect means legal effect arising under an external legal order or External Instrument.

Article 16: Federation terms

16.1. Federation Domain means a governed trust environment in which recognised Actors, Trust Service Providers, Trust Services, Sources, policies and Technical Exchange arrangements operate under assigned conditions.

16.2. Federation Boundary means the organisational, functional, geographic, technical or jurisdictional boundary of a Federation Domain.

16.3. Federation Agreement means a Recognised Instrument governing Participation, interaction, responsibilities, policies, recognition or Cross-Domain Reliance between Federation Domains.

16.4. Federation Trust Relationship means a recognised relationship between Federation Domains for an assigned purpose and scope.

16.5. Nested Federation means a Federation Domain operating within, through or in a recognised relationship with another Federation Domain.

16.6. Cross-Domain Reliance means Controlled Reliance by an Actor in one Federation Domain on a Controlled Matter originating in another Federation Domain.

16.7. Federation Trust Policy means a Framework Instrument or recognised policy establishing common minimum trust conditions within or between Federation Domains.

Article 17: Actors, participation, roles and mandates

17.1. Actor means a natural person, legal entity, organisation, body, organisational unit, system or automated function capable of performing an activity under the Framework.

17.2. Recognised Actor means an Actor assigned recognition for an identified purpose and scope.

17.3. Participating Actor means a Recognised Actor assigned Participation.

17.4. Subject means the natural person, legal entity, organisation, object, record, event, Status, relationship, Attribute or other matter to which a Trust Object, Trust Service Output, Identifier or record relates.

17.5. Affected Person means a natural person whose rights, interests, access, Participation, Status, Controlled Reliance, Review Route or Remedy Route is affected or capable of being affected by a Controlled Effect.

17.6. Protected Person means an Affected Person to whom additional safeguards apply because of humanitarian context, vulnerability, dependency, exclusion risk, protection risk or another recognised safeguard basis.

17.7. Requesting Actor means an Actor initiating a Controlled Interaction.

17.8. Responding Actor means an Actor receiving or responding to a controlled request.

17.9. Relying Actor means an Actor undertaking Controlled Reliance within an assigned Reliance Condition.

17.10. Representative means an Actor acting for another Actor within an assigned Mandate Scope.

17.11. Represented Person means a natural person for whom a Representative acts.

17.12. Role means a function assigned to an Actor.

17.13. Assigned Role means a Role assigned through an authorised Framework route.

17.14. Role Scope means the purpose, function, condition and limitation of an Assigned Role.

17.15. Mandate means authority assigned to an Actor to act for, represent, support or bind another Actor.

17.16. Mandate Scope means the purpose, action, condition, limitation, time and subject matter of a Mandate.

17.17. Participation means recognised involvement within an assigned Participation Scope.

17.18. Participation Scope means the purpose, Federation Domain, Scheme, Role, Trust Service, Controlled Interaction, condition and limitation within which Participation applies.

17.19. Responsible Actor means an Actor assigned responsibility for a Controlled Matter, Framework Function, action, decision, Trust Service, process or obligation.

17.20. Issuer means the Actor to which an issued Trust Object or Trust Service Output is attributable.

17.21. Attestation Issuer means the Issuer to which an Electronic Attestation is attributable.

17.22. Signatory means the natural person to whom an Electronic Signature is attributable.

17.23. Seal Creator means the legal entity to which an Electronic Seal is attributable.

17.24. Source Holder means the Actor maintaining, operating, controlling or responsible for a Source.

17.25. Source Steward means the Actor assigned governance responsibility for the mandate, semantics, quality, provenance, Correction and lifecycle of a Source.

17.26. Trust Service Provider means a Provider recognised to provide one or more Trust Services.

17.27. Identity Provider means a Trust Service Provider recognised to provide an Identification Service within an assigned Service Scope.

17.28. Intermediary means an Actor facilitating an interaction between other Actors without acquiring their Role, Mandate, Status or responsibility.

Article 18: Trust Service terms

18.1. Provider means an Actor providing, operating, supporting or responsible for a service, function or controlled capability.

18.2. Provider Scope means the scope within which a Provider is recognised to provide one or more Trust Services.

18.3. Trust Service means a service recognised under the Framework for an identified Trust Service Function.

18.4. Trust Service Category means a category of Trust Service established by Part IX.

18.5. Trust Service Function means a function assigned to a Trust Service.

18.6. Trust Service Output means a result, object, response or evidence produced by a Trust Service.

18.7. Service Scope means the purpose, function, operation, outputs, Actors, Federation Domain, Scheme, Profile, conditions and limitations of a Trust Service.

18.8. Trust Service Provider Status means Status assigned to an identified Trust Service Provider within an assigned Provider Scope.

18.9. Qualified Trust Service Provider Status means Qualified Status assigned to an identified Trust Service Provider within an identified Qualified Scope.

18.10. Trust Service Status means Status assigned to an identified Trust Service within an assigned Service Scope.

18.11. Qualified Trust Service Status means Qualified Status assigned to an identified Trust Service within an identified Qualified Scope.

18.12. Service Permission means a Controlled Effect authorising an identified Trust Service to operate within an assigned Service Scope.

18.13. Qualified Trust Service Provider means a Trust Service Provider assigned Qualified Trust Service Provider Status within an identified Provider Scope.

18.14. Qualified Trust Service means a Trust Service assigned Qualified Trust Service Status within an identified Service Scope.

18.15. Identification Service means a Trust Service recognised to establish, verify, maintain or resolve an identification basis concerning a Subject.

18.16. Authentication Service means a Trust Service recognised to confirm an asserted identity, Role, origin, device, session, transaction, service, Trust Object or Controlled Interaction.

18.17. Authorisation Service means a Trust Service recognised to determine whether an action, access, disclosure, exchange, service use or Controlled Interaction is permitted.

18.18. Digital Signing Service means a Trust Service recognised to create Digital Signatures through controlled use of Digital Signature Creation Data and an identified creation mechanism or device.

18.19. Electronic Signature Service means a Trust Service recognised to create or manage Electronic Signatures attributable to natural persons.

18.20. Electronic Seal Service means a Trust Service recognised to create or manage Electronic Seals attributable to legal entities.

18.21. Electronic Timestamp Service means a Trust Service recognised to create or manage Electronic Timestamps.

18.22. Electronic Attestation Service means a Trust Service recognised to create, issue or manage Electronic Attestations and, where the applicable Profile so provides, Certificates.

18.23. Validation and Verification Service means a Trust Service recognised to verify identified properties, validate identified Controlled Matters or provide authorised Status Responses.

18.24. Federated Data Exchange Service means a Trust Service recognised to provide controlled exchange between recognised Actors or Federation Domains through Technical Exchange Routes.

Article 19: Trust Objects and Trust Service Outputs

19.1. Trust Object means an independently identifiable electronic or recorded artefact assigned a Trust Object Category and lifecycle under Part VI.

19.2. Trust Object Category means a category of Trust Object established by Part VI.

19.3. Trust Object Status means Status assigned to an identified Trust Object.

19.4. Trust Object Identifier means an Identifier assigned to distinguish a Trust Object within its applicable scope.

19.5. Serial Number means an issuer-scoped value assigned to distinguish one issued Trust Object from another.

19.6. Attribute means a characteristic, Status, Role, relationship, entitlement, eligibility, authorisation, permission, fact, event or other statement associated with a Subject.

19.7. Controlled Record means a record assigned a controlled identity, purpose, lifecycle and evidence function under the Framework.

19.8. Evidence Artefact means a Controlled Matter supporting proof of an action, state, dependency, result, decision or other Controlled Matter.

19.9. Signature Evidence means evidence supporting the creation, attribution, Validation or lifecycle of an Electronic Signature.

19.10. Seal Evidence means evidence supporting the creation, attribution, Validation or lifecycle of an Electronic Seal.

19.11. Identification Result means a Trust Service Output recording the result of an Identification Service other than an Identity Resolution Result.

19.12. Identity Resolution Result means a Trust Service Output recording a determination concerning relationships between identity records within an assigned scope.

19.13. Authentication Outcome means a Trust Service Output recording the result of an Authentication Service.

19.14. Authorisation Outcome means a Trust Service Output recording the result of an Authorisation Service.

19.15. Verification Result means a Trust Service Output recording the result of Verification.

19.16. Validation Result means a Trust Service Output recording the result of Validation.

19.17. Status Response means a Trust Service Output providing authorised Status information concerning an identified Status-Bearing Matter.

19.18. Exchange Evidence means a Trust Service Output evidencing the processing, transmission, receipt, refusal or failure of a Controlled Interaction.

19.19. Controlled Exchange Result means a Trust Service Output recording the outcome of a Federated Data Exchange Service interaction.

19.20. A Trust Service Output is a Trust Object only where Part VI assigns it a Trust Object Category and lifecycle.

19.21. Qualified Trust Object Status means Qualified Status of an individual Trust Object established through Object-Instance Qualification.

Article 20: Digital Signatures, Electronic Signatures, Electronic Seals, Electronic Timestamps and Certificates

20.1. Digital Signature means electronic data created through a Digital Signature Creation Process and associated with other electronic data to support Integrity verification and origin binding.

20.2. Digital Signature Creation Process means the controlled process through which Digital Signature Creation Data is used to create a Digital Signature.

20.3. Digital Signature Creation Data means unique data used to create a Digital Signature.

20.4. Digital Signature Validation Data means data used to validate a Digital Signature.

20.5. Digital Signature Creation Mechanism means configured hardware, software, a remote service or a protected execution arrangement used with Digital Signature Creation Data.

20.6. Digital Signature Creation Device means an identified implementation of a Digital Signature Creation Mechanism assigned an independent lifecycle and Status.

20.7. Qualified Digital Signature Creation Device means a Digital Signature Creation Device assigned Qualified Status under an applicable Qualified Profile and Framework Decision.

20.8. Electronic Signature means data in electronic form attached to or logically associated with other data in electronic form and used by a natural person to sign.

20.9. Advanced Electronic Signature means an Electronic Signature satisfying the requirements established for advanced Electronic Signatures in Part VI.

20.10. Qualified Electronic Signature means an Advanced Electronic Signature satisfying the requirements established for qualified Electronic Signatures in Part VI.

20.11. Electronic Seal means data in electronic form attached to or logically associated with other data in electronic form to evidence legal-entity origin and Integrity.

20.12. Advanced Electronic Seal means an Electronic Seal satisfying the requirements established for advanced Electronic Seals in Part VI.

20.13. Qualified Electronic Seal means an Advanced Electronic Seal satisfying the requirements established for qualified Electronic Seals in Part VI.

20.14. Electronic Timestamp means data in electronic form binding other data in electronic form to an identified time.

20.15. Qualified Electronic Timestamp means an Electronic Timestamp satisfying the requirements established for qualified Electronic Timestamps in Part VI.

20.16. Certificate means an Electronic Attestation linking Digital Signature Validation Data or another controlled value to a Subject.

20.17. Electronic Signature Certificate means a Certificate linking Digital Signature Validation Data to a natural person.

20.18. Electronic Seal Certificate means a Certificate linking Digital Signature Validation Data to a legal entity.

20.19. Qualified Certificate means a Certificate satisfying the requirements established for qualified Certificates in Part VI.

Article 21: Electronic Attestation terms

21.1. Electronic Attestation means data in electronic form containing an Attestation Statement attributable to an Attestation Issuer.

21.2. Attestation Statement means the fact, Attribute, Status, relationship, event, assessment, decision or other statement contained in an Electronic Attestation.

21.3. Attestation Profile means a Profile assigning the content, evidence basis, Assurance, protection, Status, lifecycle and Reliance Conditions applicable to an Electronic Attestation Trust Object Category.

21.4. Advanced Electronic Attestation means an Electronic Attestation satisfying the requirements established for advanced Electronic Attestations in Part VI.

21.5. Qualified Electronic Attestation means an Advanced Electronic Attestation satisfying the requirements established for qualified Electronic Attestations in Part VI.

21.6. Attestation Scheme means a Scheme governing the use of one or more Electronic Attestation Trust Object Categories for an identified purpose and context.

Article 22: Identification, Authentication and Authorisation terms

22.1. Identifier means a data value used to distinguish, reference or link a Subject, Actor, Controlled Matter, Trust Service, Source or record.

22.2. Identification means establishment, determination or verification of an identification basis relating to a Subject.

22.3. Identity Proofing means evaluation of evidence to establish confidence in an asserted identity.

22.4. Identity Registration means creation or recognition of an identity record within an assigned Service Scope of an Identification Service.

22.5. Identity Resolution means determination that records, Identifiers or representations concern the same Subject or concern different Subjects within an assigned scope.

22.6. Authentication means confirmation of an asserted identity, Role, origin, device, session, transaction, service, Trust Object or Controlled Interaction.

22.7. Authentication Mechanism means a mechanism recognised to support Authentication.

22.8. Authenticator means a Controlled Matter used through an Authentication Mechanism.

22.9. Authentication Event means an event in which Authentication is performed.

22.10. Authorisation means determination of whether an action, access, disclosure, exchange, service use or Controlled Interaction is permitted.

22.11. Authorisation Policy means a controlled policy governing Authorisation for an identified purpose and scope.

22.12. Policy Decision Function means the function of an Authorisation Service that evaluates an applicable policy.

22.13. Policy Enforcement Function means the function applying an Authorisation Outcome to a requested action or Controlled Interaction.

Article 23: Source and Authoritative Source terms

23.1. Source means an information basis recognised under the Framework for an identified purpose.

23.2. Source Scope means the purpose, information, Attributes, Subjects, functions, conditions and limitations for which a Source is recognised.

23.3. Source Profile means a Profile assigning the mandate, Source Scope, semantic, quality, provenance, security, lifecycle, Correction and evidence conditions applicable to a Source.

23.4. Source Status means Status assigned to an identified Source.

23.5. Source Basis means the identified Source, record, evidence reference, Source Scope and Version supporting a Trust Service Output or Trust Object.

23.6. Source Designation means assignment of Authoritative Source Status through a Framework Decision.

23.7. Authoritative Source means a Source assigned Authoritative Source Status for an identified Source Scope.

23.8. Authoritative Source Status means Status under which a Source is recognised as authoritative for an identified Source Scope.

23.9. Qualified Authoritative Source means an Authoritative Source assigned Qualified Authoritative Source Status within an identified Qualified Scope.

23.10. Qualified Authoritative Source Status means Qualified Status assigned to an Authoritative Source within an identified Source Scope.

23.11. Source Verification means evaluation of specified properties of a Source or Source Basis through Verification.

23.12. Freshness Condition means a condition governing whether a Controlled Matter is sufficiently current for an identified purpose.

23.13. Provenance means the traceable origin, custody, generation, transformation, Correction, supersession and lifecycle history of a Controlled Matter.

23.14. Data Quality means the degree to which data satisfies the accuracy, completeness, consistency, validity, currentness, timeliness, uniqueness, traceability and other conditions assigned by the applicable Profile.

Article 24: Reliance, policy and controlled interaction terms

24.1. Reliance means use of a Controlled Matter as a basis for an action, decision, service or Controlled Effect.

24.2. Controlled Reliance means Reliance governed by the Framework within an assigned purpose, scope and Reliance Condition.

24.3. Reliance Condition means a condition governing Controlled Reliance.

24.4. Reliance Limit means a restriction on the purpose, scope, value, time, Actor, transaction or Controlled Effect of Controlled Reliance.

24.5. Trust Acceptance Policy means a controlled policy establishing the conditions under which a Relying Actor accepts a Controlled Matter for a specified purpose and Controlled Reliance.

24.6. Local Trust Acceptance Policy means a Trust Acceptance Policy established by a Relying Actor for its own service, decision or Controlled Reliance.

24.7. Access Condition means a condition governing access to a Controlled Matter or Trust Service.

24.8. Disclosure Condition means a condition governing whether, how, to whom and for what purpose a Controlled Matter is disclosed or made available.

24.9. Controlled Interaction means an interaction between Actors, Trust Services, Sources, Trust Objects, Trust Service Outputs or technical components governed by the Framework.

24.10. Technical Exchange Route means a recognised technical means through which a Controlled Interaction occurs.

24.11. Technical Exchange Permission means a Controlled Effect authorising use of an identified Technical Exchange Route for an assigned purpose and scope.

24.12. Endpoint means a controlled technical point through which an Actor, Trust Service, Source or Technical Exchange Route is reached.

24.13. Technical Exchange Route Operator means the Actor responsible for operating an identified Technical Exchange Route.

24.14. Discovery Metadata means Metadata used to locate, identify or resolve a recognised Actor, Trust Service Provider, Trust Service, Source, Federation Domain, Endpoint or Technical Exchange Route.

Article 25: Assurance, Conformity Assessment and qualification terms

25.1. Assurance means confidence supported by evidence, controls, assessment and applicable conditions.

25.2. Assurance Object means the Controlled Matter to which Assurance is assigned.

25.3. Assurance Domain means the subject area within which Assurance is evaluated.

25.4. Assurance Condition means a condition required for an Assurance outcome.

25.5. Assurance Level means the degree of Assurance assigned within an Assurance Domain.

25.6. Low Assurance Level means limited confidence that the Assurance Object satisfies the applicable Assurance Conditions.

25.7. Substantial Assurance Level means substantial confidence that the Assurance Object satisfies the applicable Assurance Conditions.

25.8. High Assurance Level means high confidence that the Assurance Object satisfies the applicable Assurance Conditions.

25.9. Conformity Assessment means evaluation of a Controlled Matter against assigned conformity requirements.

25.10. Conformity Assessment Body means an Actor recognised to perform Conformity Assessment within an assigned scope.

25.11. Conformity Assessment Result means a Controlled Record documenting the outcome of a Conformity Assessment.

25.12. Decision-Based Qualification means qualification through a Framework Decision following the applicable Conformity Assessment route.

25.13. Object-Instance Qualification means qualification of an individual Trust Object or eligible Trust Service Output through satisfaction and Validation of an applicable Qualified Object Profile.

25.14. Qualification means a Framework-controlled determination or object-instance evaluation that an eligible Status-Bearing Matter satisfies the applicable qualified conditions.

25.15. Qualified Profile means a Profile assigning the conditions applicable to Qualified Status for an identified category and scope.

25.16. Qualified Status means Status assigned or established through the qualification route applicable to an eligible Status-Bearing Matter.

25.17. Qualified Scope means the purpose, category, function, configuration, condition and limitation within which Qualified Status applies.

25.18. Qualified Object Profile means a Qualified Profile applicable to an identified Trust Object Category or to an eligible Trust Service Output assigned that Category.

Article 26: Status and lifecycle terms

26.1. Status means a Framework-controlled state, classification, recognition or condition assigned to a Status-Bearing Matter.

26.2. Active Status means Status under which a Controlled Matter remains available for its permitted function.

26.3. Restricted Status means Status under which a Controlled Matter remains available only within an assigned limitation.

26.4. Suspended Status means Status under which an assigned function or Controlled Effect is temporarily unavailable or restricted.

26.5. Withdrawn Status means Status under which recognition, permission or future use has been removed.

26.6. Revoked Status means Status under which an assigned permission, recognition or Controlled Effect has been terminated from an identified time.

26.7. Superseded Status means Status under which a later Controlled Matter or Version has replaced the earlier matter.

26.8. Archived Status means Status under which a Controlled Matter is retained for historical, evidential, audit, Review or Remedy purposes.

26.9. Transitional Status means Status governing movement from one controlled state, Framework Instrument or Version to another.

26.10. Effective Date means the date and time from which a Controlled Matter, Version, Status, recognition, decision or change has effect.

26.11. Validity Period means the period during which a Status, permission, Trust Object, Trust Service Output, decision or Controlled Effect remains capable of application.

26.12. Lifecycle Condition means a condition governing creation, issuance, activation, operation, restriction, suspension, withdrawal, revocation, replacement, retention, archival or closure.

26.13. Restriction Condition means a condition limiting use, access, disclosure, exchange, publication, Verification, Validation, Controlled Reliance, retention or preservation.

26.14. Correction means an authorised action addressing an error, omission, inconsistency or defect.

26.15. Replacement means creation or recognition of a Controlled Matter taking the place of another for future use.

26.16. Suspension means temporary restriction or prevention of an assigned function, Status, permission or Controlled Effect.

26.17. Withdrawal means removal of recognition, Status, permission or future use.

26.18. Revocation means termination of an assigned Status, permission or Controlled Effect from an identified time.

26.19. Expiry means cessation because an assigned Validity Period has ended.

26.20. Reinstatement means restoration through an authorised route.

26.21. Retention means continued preservation for an assigned period and purpose.

26.22. Deletion means authorised removal or destruction subject to applicable evidence, Review and Remedy requirements.

26.23. Historical State means the Status, Version, dependencies and conditions of a Controlled Matter at an identified past time.

Article 27: Security, incident and continuity terms

27.1. Confidentiality means protection against unauthorised access, observation or disclosure.

27.2. Transport Confidentiality means Confidentiality applied to data while transmitted through a Technical Exchange Route.

27.3. Payload Confidentiality means Confidentiality applied to the content of a Controlled Interaction so that only authorised processing Actors have access to the plaintext content.

27.4. Integrity means protection against unauthorised alteration, corruption, substitution or loss.

27.5. Authenticity means confidence in an asserted origin or identity.

27.6. Availability means accessibility and usability when required.

27.7. Accountability means the ability to attribute and review an action, decision or state.

27.8. Security Condition means a condition protecting Confidentiality, Integrity, Availability, Authenticity, resilience or controlled access.

27.9. Security Incident means an event affecting or capable of materially affecting the Confidentiality, Integrity, Availability, Authenticity, resilience, Status, Assurance or Controlled Effect of a Controlled Matter.

27.10. Restricted Information means information subject to a Restriction Condition.

27.11. Protection-Sensitive Information means information whose access, use, disclosure, combination or loss is capable of creating a protection risk.

27.12. Security-Sensitive Information means information whose access, use, disclosure, alteration or loss is capable of compromising security, resilience, continuity or incident response.

27.13. Controlled Environment means an execution or operational context assigned Framework requirements for security, access, evidence and supervision.

27.14. Continuity means controlled maintenance of an assigned function under disruption.

27.15. Degraded Operation means continued operation under restricted conditions.

27.16. Recovery means restoration of required conditions following disruption or a Security Incident.

Article 28: Review, Correction and Remedy terms

28.1. Complaint means a request by an Actor or Affected Person for examination of an alleged error, breach, adverse effect or failure.

28.2. Complaint Route means the Framework-controlled route through which a Complaint is submitted and determined.

28.3. Review means structured reassessment of a Controlled Matter, decision, Status, result or Controlled Effect.

28.4. Review Route means the Framework-controlled route through which Review is sought or conducted.

28.5. Correction Route means the Framework-controlled route through which Correction is requested or performed.

28.6. Remedy means a Framework-controlled measure addressing an adverse, incorrect, invalid, unsafe or non-conforming state or Controlled Effect.

28.7. Remedy Route means the Framework-controlled route through which Remedy is sought or applied.

28.8. Interim Measure means a temporary measure applied before final Review or Remedy to control a material risk.

28.9. Remedy Closure means controlled completion of a Remedy process.

28.10. Accessible Alternative means an alternative route, process or mechanism enabling an Affected Person to exercise a function or right where the primary route creates an unjustified barrier.

28.11. Protected-Person Safeguard means a condition or measure protecting a Protected Person from exclusion, disproportionate harm or an Adverse Protected-Person Effect.

28.12. Adverse Protected-Person Effect means an adverse Controlled Effect affecting a Protected Person.

Article 29: Framework Instruments, records and publication terms

29.1. Framework Instrument means a controlled instrument recognised under the Framework.

29.2. Main Part means an operative Part establishing constitutional rules, Controlled Terms, recognised categories, Decision Competence, Status, Controlled Effects or essential boundaries.

29.3. Annex means a Framework Instrument establishing structural models, classifications, relationships and horizontal application rules required by the Main Parts.

29.4. Implementation Guideline means a Framework Instrument assigning implementation requirements and operational conditions for an identified object, Trust Service, governance function or horizontal control.

29.5. Scheme means a Framework Instrument establishing a governed arrangement for an identified purpose, context and participating scope.

29.6. Profile means a Framework Instrument selecting requirements and conditions for an identified Actor, Trust Service, Trust Object, Source, mechanism, device, route or process.

29.7. Technical Specification means a Framework Instrument assigning detailed technical requirements, formats, interfaces, parameters, schemas, configurations or test conditions.

29.8. Body Instrument means a Framework Instrument adopted by a Framework Body within its Decision Competence.

29.9. Instrument Status means Status assigned to a Framework Instrument.

29.10. Instrument Identifier means a stable identifier assigned to a Framework Instrument independently of its Version and Instrument Status.

29.11. Register means a governance-controlled record set recording identified Controlled Matters and their lifecycle information.

29.12. Catalogue means a governance-controlled record set organising or listing recognised categories, types or Controlled Matters.

29.13. Entry means a controlled record within a Register, Catalogue, Humanitarian Trust List, log or other controlled record set.

29.14. Humanitarian Trust List means the governance-controlled publication through which authorised Status and Discovery Metadata are published for Status-Bearing Matters whose publication is authorised.

29.15. Humanitarian Trust List Entry means an Entry published by the responsible Framework Body concerning an identified Status-Bearing Matter whose publication is authorised.

29.16. Status Publication means controlled publication of authorised Status information by the responsible Framework Body.

29.17. Decision File means a Controlled Record or set of Controlled Records evidencing a Framework Decision and its basis, scope, conditions, time and Controlled Effect.

29.18. Metadata means data describing the identity, category, provenance, Status, scope, Version, time, dependencies or other characteristics of a Controlled Matter.

29.19. Recognised Standard means a standard or technical reference assigned recognition through an authorised Framework route.

29.20. Standards Register means the Register recording Recognised Standards, editions, selected options, deviations and transition Status.

29.21. Trust Service Catalogue means the Catalogue recording the Trust Service Categories established by Part IX.

29.22. Trust Object Catalogue means the Catalogue recording the Trust Object Categories established by Part VI.

29.23. Instrument Code Catalogue means the Catalogue recording instrument-type, controlled-group and function codes used for Instrument Identifiers.

Article 30: Change, Version and transition terms

30.1. Version means an identified immutable state of a Controlled Matter.

30.2. Change Control means the Framework-controlled rules governing change to a Controlled Matter.

30.3. Change Classification means classification of a proposed change according to its nature, scope, risk and Controlled Effect.

30.4. Transition means controlled movement between states, Versions, requirements or implementation arrangements.

30.5. Transition Period means the assigned period for a Transition.

30.6. Migration means controlled transfer or transformation from one Version, system, format or arrangement to another.

30.7. Compatibility means the ability of identified Versions or implementations to interact within defined conditions.

30.8. Coexistence means authorised simultaneous operation of identified Versions during an assigned Transition Period.

30.9. Rollback means controlled restoration of an earlier approved Version or state.

30.10. Deprecation means Status indicating that new use of an identified matter is being restricted or ended in preparation for retirement or withdrawal.

30.11. Retirement means controlled cessation of operational use of an identified matter while preserving required historical evidence.

PART III: GENERAL PRINCIPLES

Version: 0.1

SECTION 1: CATEGORY, STATUS AND CONTROLLED EFFECT

Article 31: Application of general principles

31.1. The principles in this Part shall apply to every Controlled Matter and Controlled Interaction within the scope of the Framework.

31.2. A Framework Instrument shall apply these principles within its assigned scope and shall not disapply them unless a Main Part expressly provides otherwise.

31.3. A Framework Decision shall be interpreted consistently with the principles in this Part.

Article 32: Functional and category separation

32.1. Each Controlled Matter shall be governed according to its category, function, identity, scope, responsibility, evidence and lifecycle.

32.2. The following categories shall remain separate unless a Main Part expressly establishes a relationship between them:

(a) Actor and Role;

(b) Trust Service Provider and Trust Service;

(c) Trust Service and Trust Service Output;

(d) Trust Service Output and Trust Object;

(e) Source and Trust Service;

(f) Source and Electronic Attestation;

(g) Trust Object and Technical Exchange Route;

(h) Status information and the Status being reported;

(i) Validation and Controlled Reliance.

32.3. A Trust Service Output shall constitute a Trust Object only where Part VI assigns it a Trust Object Category and lifecycle.

32.4. Representation of a Trust Service Output in an Electronic Attestation shall create a separate Electronic Attestation and shall not reclassify the original output.

32.5. A dependency, common Provider, shared component, common Endpoint or technical route shall not merge the identity, Status, responsibility or Controlled Effect of separate Controlled Matters.

Article 33: Status and Qualified Status limitation

33.1. Status shall apply only to the identified Status-Bearing Matter and within the assigned scope.

33.2. Status assigned to one Controlled Matter shall not, by itself, transfer to another Controlled Matter.

33.3. Qualified Status assigned to a Trust Service Provider shall not qualify a Trust Service, Trust Service Output, Trust Object, Source, mechanism, device or dependency.

33.4. Qualified Status assigned to a Trust Service shall not qualify its Provider, outputs, Trust Objects, Sources, mechanisms, devices or dependencies.

33.5. Qualified Status assigned to a Trust Object, Source, mechanism or device shall not qualify another Controlled Matter.

33.6. A dependency on a qualified Controlled Matter shall constitute a condition and shall not transfer Qualified Status.

Article 34: Controlled Effects and non-inference

34.1. A Controlled Effect shall arise only where the Framework or an applicable Framework Instrument expressly assigns that effect.

34.2. Participation, recognition, Status Publication, inclusion in a Register or Catalogue, technical connection, testing, availability, successful Authentication, a positive Verification Result or a positive Validation Result shall not, by itself, create:

(a) access;

(b) disclosure;

(c) Authorisation;

(d) Service Permission;

(e) Technical Exchange Permission;

(f) Controlled Reliance;

(g) Qualified Status;

(h) an underlying humanitarian, programme or operational decision.

34.3. Absence of an express prohibition shall not create a Controlled Effect.

34.4. A subordinate Framework Instrument shall not create a Controlled Effect reserved to a Main Part or Framework Decision.

Article 35: Case neutrality

35.1. A Trust Service, Trust Object and Trust Service Output shall be classified according to its stable function and not according to the sector, programme or use case in which it is used.

35.2. The subject matter of an Attestation Statement shall not alter the Trust Object Category of Electronic Attestation or the Electronic Attestation Service category.

35.3. A Scheme shall govern the use context and shall not create a use-case-specific Trust Service Category.

35.4. A Profile shall select requirements for an existing category and shall not change that category.

35.5. A change in business purpose shall require evaluation of the applicable Scheme, Profile, policy and Reliance Conditions and shall not, by itself, change the object or service category.

SECTION 2: RESPONSIBILITY, EVIDENCE AND LIFECYCLE

Article 36: Responsibility and local decision competence

36.1. Each Actor shall remain responsible for the functions, decisions, systems, information and Controlled Effects assigned to it.

36.2. Federation, delegation, outsourcing, automation, technical exchange or use of a shared service shall not remove assigned responsibility.

36.3. A Framework Body shall not acquire operational responsibility for a Trust Service, Source, Technical Exchange Route or local decision by reason only of governance, supervision, qualification or Status Publication.

36.4. A Relying Actor shall remain responsible for its decision to accept and rely on a Controlled Matter.

36.5. A Responding Actor shall remain responsible for disclosure and service-response decisions within its assigned scope.

36.6. Where responsibility is shared, the applicable Framework Instrument shall identify the responsible Actors, boundaries, evidence and treatment of shared failures.

Article 37: Evidence and provenance

37.1. A material recognition, Status, qualification, Service Permission, Technical Exchange Permission, lifecycle action or Controlled Reliance shall be supported by evidence where required by the applicable Framework Instrument.

37.2. Evidence shall be attributable, relevant, sufficiently current, protected and traceable to the Controlled Matter and purpose for which it is used.

37.3. Provenance shall preserve the origin, custody, generation, transformation, Correction, supersession and lifecycle history required for the applicable purpose.

37.4. Evidence supporting one Controlled Matter shall not, by itself, establish the Status or condition of another Controlled Matter.

37.5. A material limitation, conflict, uncertainty or unavailable dependency shall be recorded and reflected in the resulting decision, Status, Trust Service Output or Reliance Condition.

Article 38: Dependencies and lifecycle

38.1. A dependency shall be identified where the operation, Status, Assurance, Validation or Controlled Reliance of one Controlled Matter depends on another.

38.2. A dependency record shall identify:

(a) the dependent matter;

(b) the supporting matter;

(c) the dependency type;

(d) the required Status and conditions;

(e) the lifecycle and propagation rules;

(f) the effect of unavailability, restriction, suspension, withdrawal or expiry.

38.3. A lifecycle action shall apply only to the affected Controlled Matter and scope unless an identified dependency or Framework Decision establishes a broader effect.

38.4. Suspension or withdrawal of a dependency shall not retrospectively invalidate an earlier Trust Object, Trust Service Output or decision unless the applicable Framework Instrument or Framework Decision expressly assigns that effect on a supported evidence basis.

38.5. Historical State shall remain reconstructable where required for Validation, Review, Remedy or Controlled Reliance.

SECTION 3: SECURITY, SAFEGUARDS, FEDERATION AND RELIANCE

Article 39: Security and Confidentiality

39.1. Responsible Actors shall protect Confidentiality, Integrity, Availability, Authenticity, Accountability, resilience and continuity according to the assigned scope and risks.

39.2. Transport Confidentiality, Payload Confidentiality, storage confidentiality, processing confidentiality, Integrity, Authenticity and Authorisation shall remain distinct controls.

39.3. Technical security shall not, by itself, create access, disclosure, Authorisation, Service Permission, Technical Exchange Permission or Controlled Reliance.

39.4. A shared security component shall not merge the Status or responsibility of the Controlled Matters that use it.

39.5. Security controls shall remain proportionate to the protected matter, Assurance Conditions, protection risks and consequences of failure.

Article 40: Protected-Person Safeguards and accessibility

40.1. The operation of the Framework shall not create unjustified exclusion of an Affected Person or Protected Person.

40.2. Where a digital process, Identifier, document, biometric, Authenticator, device or connectivity requirement creates an unjustified barrier, the applicable Framework Instrument shall provide an Accessible Alternative.

40.3. Failure or inability to satisfy one technical route shall not, by itself, determine identity, eligibility, entitlement, fraud, misconduct or final exclusion.

40.4. A process capable of producing an Adverse Protected-Person Effect shall include proportionate safeguards, explainability, Correction, Review and Remedy.

40.5. A final significant adverse decision based substantially on automated processing shall be subject to review by a natural person where required by the applicable Scheme or Profile.

40.6. Safeguards shall preserve the Integrity, evidence and accountability required for the controlled process.

Article 41: Federation and policy separation

41.1. A Federation Trust Policy shall establish the common minimum trust conditions applicable within or between Federation Domains.

41.2. A Local Trust Acceptance Policy shall establish the conditions under which a Relying Actor accepts a Controlled Matter for its own service, decision or Controlled Reliance.

41.3. A Federation Trust Policy shall not require a Relying Actor to accept a Controlled Matter where its applicable Local Trust Acceptance Policy and Reliance Conditions are not satisfied.

41.4. A Local Trust Acceptance Policy shall not reduce a mandatory condition established by the Framework, a Federation Agreement or an applicable Scheme.

41.5. An Authorisation Service shall evaluate an applicable Authorisation Policy and shall not acquire ownership of the policy or the underlying decision competence by reason only of evaluation.

41.6. Recognition, Status or policy in one Federation Domain shall not automatically create equivalent recognition, Status or acceptance in another Federation Domain.

Article 42: Controlled Reliance

42.1. A Relying Actor shall undertake Controlled Reliance only where:

(a) the Relying Actor holds the required Role and, where applicable, Mandate;

(b) the purpose and scope are authorised;

(c) the relevant Status and mandatory dependencies are current;

(d) the required Verification and Validation are complete;

(e) the applicable Federation Trust Policy and Local Trust Acceptance Policy are satisfied;

(f) the applicable Reliance Conditions, Reliance Limits, caveats and safeguards are observed.

42.2. Successful Validation shall establish only the result within the applicable evaluation scope and shall not require Controlled Reliance.

42.3. Controlled Reliance shall not transfer responsibility for the relying decision to the Issuer, Source Holder, Trust Service Provider, Framework Body or Technical Exchange Route Operator.

42.4. A Relying Actor shall maintain evidence sufficient to reconstruct the purpose, basis, applicable policies, Controlled Matters used, decision and outcome of material Controlled Reliance.

42.5. Where Controlled Reliance is capable of producing an Adverse Protected-Person Effect, the Relying Actor shall preserve access to the applicable Review and Remedy Routes.

PART IV: GOVERNANCE, SUPERVISION AND DECISION COMPETENCE

Version: 0.1

SECTION 1: GOVERNANCE ARCHITECTURE AND COMPETENCE

Article 43: Governance structure

43.1. The Framework shall operate through the Framework Steward and Framework Bodies assigned identified Framework Functions.

43.2. The governance structure shall distinguish:

(a) stewardship and Framework maintenance;

(b) recognition and Decision-Based Qualification;

(c) supervision and corrective action;

(d) Status Publication and federation discovery;

(e) Review and Remedy;

(f) operational functions performed by Participating Actors and Trust Service Providers.

43.3. Governance of a Controlled Matter shall not transfer operational responsibility for that Controlled Matter to the Framework Steward or a Framework Body.

43.4. The Humanitarian Trust List, governance Registers and governance Catalogues shall remain under the responsibility of the competent Framework Body.

Article 44: Framework Bodies and Framework Functions

44.1. A Framework Body shall be established or recognised through a Framework Instrument identifying:

(a) its Framework Functions;

(b) its Decision Competence;

(c) its composition and accountability;

(d) its independence and conflict controls;

(e) its records and evidence obligations;

(f) its Review and reporting arrangements;

(g) its lifecycle and succession arrangements.

44.2. A Framework Body shall perform only the Framework Functions assigned to it.

44.3. A Framework Function shall not be inferred from participation, technical capability, operational practice or absence of objection.

44.4. A Framework Body shall maintain the competence, resources and procedures required for its assigned functions.

Article 45: Decision Competence

45.1. A Framework Body shall adopt a Framework Decision only within its assigned Decision Competence.

45.2. Decision Competence shall identify:

(a) the decision category;

(b) the eligible Controlled Matters;

(c) the territorial, organisational and functional scope;

(d) the applicable evidence and procedure;

(e) the available Controlled Effects;

(f) the Review Route.

45.3. Cooperation, delegation, outsourcing, technical operation or cross-domain coordination shall not transfer Decision Competence unless a Recognised Instrument expressly assigns that transfer.

45.4. A delegation of Decision Competence shall identify the delegating and receiving Framework Bodies, scope, duration, conditions, evidence, oversight and termination route.

45.5. A Framework Decision adopted outside assigned Decision Competence shall not have Controlled Effect under the Framework.

Article 46: Framework Decisions

46.1. A Framework Decision shall be reasoned, attributable, evidence-based and limited to the assigned scope.

46.2. A Framework Decision shall identify:

(a) the deciding Framework Body;

(b) the affected Controlled Matter;

(c) the applicable Framework Instrument and Version;

(d) the evidence considered;

(e) the findings;

(f) the Controlled Effect;

(g) the Effective Date and Validity Period;

(h) the restrictions, conditions and caveats;

(i) the publication requirements;

(j) the Review Route.

46.3. A Framework Decision shall be recorded in a Decision File before its Controlled Effect begins.

46.4. A Framework Decision shall not have broader effect than the evidence and Decision Competence support.

46.5. A later decision shall identify its relationship with each earlier decision that it restricts, suspends, withdraws, replaces or supersedes.

SECTION 2: RECOGNITION, QUALIFICATION AND SUPERVISION

Article 47: Recognition decisions

47.1. A Framework Body shall assign recognition only where the applicable eligibility, evidence, Assurance, security, lifecycle and safeguard conditions are satisfied.

47.2. A recognition decision shall identify:

(a) the recognised Controlled Matter;

(b) the recognition category;

(c) the assigned scope;

(d) the applicable conditions and restrictions;

(e) the Effective Date and review date;

(f) the evidence basis;

(g) the required Register, Catalogue or Humanitarian Trust List treatment.

47.3. Recognition of one Controlled Matter shall not recognise another Controlled Matter.

47.4. Recognition shall not, by itself, create Service Permission, Technical Exchange Permission, access, disclosure, Qualified Status or Controlled Reliance.

Article 48: Decision-Based Qualification

48.1. A Framework Body shall assign Qualified Status through Decision-Based Qualification only to a category made eligible by Part X.

48.2. Decision-Based Qualification shall apply separately to:

(a) a Trust Service Provider;

(b) a Trust Service;

(c) an Authoritative Source;

(d) a creation mechanism or device;

(e) another category expressly made eligible by a Main Part.

48.3. A qualification decision shall satisfy Article 142 and shall identify the Qualified Scope and applicable Qualified Profile.

48.4. Object-Instance Qualification of an individual Trust Object or eligible Trust Service Output shall be governed by Part X and shall not require an individual Framework Decision unless a Main Part expressly assigns such a decision.

48.5. Qualified Status assigned through one qualification decision shall not transfer to another Controlled Matter.

Article 49: Supervision

49.1. A Framework Body assigned a supervision Framework Function shall monitor continuing compliance within its assigned scope.

49.2. Supervision shall be proportionate to the Controlled Matter, risks, Assurance Conditions, dependencies and potential Controlled Effects.

49.3. Supervision shall include, where applicable:

(a) review of Status and continuing eligibility;

(b) surveillance of qualified conditions;

(c) examination of records, evidence and reports;

(d) investigation of incidents and Complaints;

(e) verification of corrective actions;

(f) initiation of restriction, suspension or withdrawal procedures.

49.4. A Framework Body performing a supervision Framework Function shall not assume operational responsibility for the supervised Controlled Matter.

49.5. A supervision finding shall be recorded and communicated to the competent Framework Body where a Framework Decision is required.

Article 50: Corrective action and lifecycle decisions

50.1. A Framework Body shall require corrective action where a Controlled Matter fails or is at material risk of failing an applicable condition.

50.2. A corrective-action decision shall identify:

(a) the affected Controlled Matter and scope;

(b) the failed or threatened condition;

(c) the evidence basis;

(d) the required action;

(e) the completion period;

(f) the Verification and closure conditions;

(g) the consequence of non-completion.

50.3. A Framework Body shall restrict, suspend, withdraw, revoke or refuse reinstatement only where the applicable conditions and evidence support that Controlled Effect.

50.4. A lifecycle decision shall remain limited to the affected Controlled Matter and scope unless an identified dependency supports a broader effect.

50.5. An urgent Interim Measure shall remain temporary and subject to Review.

SECTION 3: STATUS PUBLICATION, REGISTERS AND GOVERNANCE EVIDENCE

Article 51: Humanitarian Trust List and Status Publication

51.1. The Humanitarian Trust List shall be a governance-controlled publication of authorised Status and Discovery Metadata.

51.2. The competent Framework Body shall own and control:

(a) the publication policy;

(b) eligibility for listing;

(c) the Status and scope published;

(d) the distinction between public, restricted and operational information;

(e) publication, Correction, suspension, withdrawal and historical retention;

(f) the authenticity and Integrity of the publication.

51.3. A technical operator shall support publication only within the instructions and controls of the competent Framework Body and shall not acquire Decision Competence, Trust Service Provider Status or ownership of the Humanitarian Trust List by reason only of that support.

51.4. Status Publication shall communicate an authorised Framework Decision and shall not create the Status being published.

51.5. Status information and Discovery Metadata shall have separate change authority and lifecycle treatment.

51.6. Discovery Metadata shall not create Service Permission, Technical Exchange Permission, access, disclosure or Controlled Reliance.

51.7. Individual high-volume Trust Objects shall not ordinarily receive Humanitarian Trust List Entries and shall use Validation and authorised Status Responses where applicable.

Article 52: Registers and Catalogues

52.1. The competent Framework Body shall maintain the Registers and Catalogues required by the Framework.

52.2. Governance-controlled Catalogues shall include, where applicable:

(a) the Trust Service Catalogue;

(b) the Trust Object Catalogue;

(c) the Instrument Code Catalogue;

(d) Scheme and Profile Catalogues;

(e) another Catalogue established through the Framework Instrument architecture.

52.3. Governance-controlled Registers shall include, where applicable:

(a) the Standards Register;

(b) qualification and decision records;

(c) mechanism and device records;

(d) another Register established through the Framework Instrument architecture.

52.4. An Entry shall identify its responsible Framework Body, Controlled Matter, purpose, Status where applicable, scope, evidence reference, Version, Effective Date and lifecycle.

52.5. Inclusion in a Register or Catalogue shall not, by itself, create recognition, Status, permission, operational activation or Controlled Reliance.

52.6. A new code, category or Entry shall follow the decision route assigned by the enabling Framework Instrument.

Article 53: Decision Files, records and transparency

53.1. A Framework Body shall maintain a Decision File for each material Framework Decision.

53.2. A Decision File shall contain or reference:

(a) Decision Competence;

(b) the affected Controlled Matter;

(c) the applicable requirements and Versions;

(d) the evidence and assessment basis;

(e) the findings and reasons;

(f) the Controlled Effect and scope;

(g) the Effective Date and lifecycle conditions;

(h) publication and notification actions;

(i) the Review Route.

53.3. Governance records shall be protected against unauthorised access, alteration, deletion and disclosure.

53.4. The competent Framework Body shall publish sufficient information to enable affected Actors and persons to understand a material Framework Decision, subject to Confidentiality, protection and security restrictions.

53.5. Historical decisions, Status and Versions shall remain reconstructable where required for Validation, Review, Remedy or Controlled Reliance.

SECTION 4: INDEPENDENCE, REVIEW AND CROSS-DOMAIN GOVERNANCE

Article 54: Independence and conflicts of interest

54.1. Framework Bodies and persons performing governance, assessment, supervision, Review and Remedy functions shall identify and manage actual, potential and perceived conflicts of interest.

54.2. A person or organisational function shall not:

(a) approve its own eligibility where independent approval is required;

(b) assign its own Qualified Status;

(c) independently assess or supervise its own performance;

(d) adopt and independently review the same Framework Decision.

54.3. Conflict controls shall include, where required, separation of personnel, decisions, systems, evidence, recusal, independent Review or enhanced supervision.

54.4. A function shall be refused, reassigned, restricted or suspended where a conflict cannot be controlled consistently with the Framework.

54.5. Conflict assessments and controls shall be recorded and reviewed after a material change.

Article 55: Review and cross-domain coordination

55.1. A Framework Decision shall be subject to the Review Route assigned by the Framework or applicable Framework Instrument.

55.2. The reviewing function shall examine Decision Competence, procedure, evidence, scope, Controlled Effect, proportionality, safeguards and consistency with the Framework.

55.3. The reviewing function shall remain sufficiently independent from the original decision-making function.

55.4. Where a governance matter affects more than one Federation Domain, the responsible Framework Bodies shall coordinate evidence, Status Publication, lifecycle action and communication while preserving the Decision Competence of each Federation Domain.

55.5. A Framework Body in one Federation Domain shall not alter a decision or Status assigned within another Federation Domain unless a Federation Agreement expressly assigns that competence.

55.6. Review and coordination records shall identify the participating Framework Bodies, retained Decision Competence, evidence exchanged, outcomes and unresolved matters.

PART V: ACTORS, PARTICIPATION, ROLES AND MANDATES

SECTION 1: RECOGNITION, PARTICIPATION, ROLES AND MANDATES

Article 56: Recognition of Actors

56.1. An Actor shall perform a Framework Function, Assigned Role or controlled activity only where the applicable recognition and eligibility conditions are satisfied.

56.2. An Actor-recognition decision shall identify:

(a) the Actor;

(b) the recognised purpose and scope;

(c) the applicable Federation Domain and Scheme;

(d) the eligible Roles and functions;

(e) the evidence and Assurance Conditions;

(f) the Effective Date and lifecycle;

(g) the Review Route.

56.3. Recognition of an Actor shall not, by itself, assign Participation, a Role, Mandate, Trust Service Provider Status, Trust Service Status, Source Status, access, disclosure or Controlled Reliance.

56.4. An Actor shall notify the competent Framework Body of a material change affecting its identity, eligibility, capability or continuing compliance.

56.5. A material change shall be reviewed before the Actor continues a function affected by that change where continuing recognition depends on the changed condition.

Article 57: Participation

57.1. Participation shall arise through accession, a Federation Agreement, a Framework Decision or another Recognised Instrument assigning that effect.

57.2. A Participation instrument or decision shall identify:

(a) the Participating Actor;

(b) the Participation Scope;

(c) the applicable Federation Domain and Scheme;

(d) the Assigned Roles and authorised Controlled Interactions;

(e) the applicable Framework Instruments;

(f) the conditions, restrictions and evidence obligations;

(g) the Effective Date, Validity Period and lifecycle;

(h) the Review and Remedy Routes.

57.3. A Participating Actor shall comply with the Framework Instruments applicable to its Participation Scope.

57.4. Participation in one Federation Domain shall not establish Participation in another Federation Domain.

57.5. Participation shall be restricted, suspended, withdrawn or allowed to expire only through the applicable lifecycle route.

57.6. Participation shall not, by itself, assign a Role, Service Permission, Technical Exchange Permission, access, disclosure or Controlled Reliance.

Article 58: Roles and Role Scope

58.1. A Role shall be assigned through an authorised Framework route.

58.2. A Role assignment shall identify:

(a) the Actor and Assigned Role;

(b) the Role Scope and recognised purpose;

(c) the applicable Federation Domain and Scheme;

(d) the permitted and prohibited functions;

(e) the conditions, restrictions and evidence obligations;

(f) the Effective Date, Validity Period and lifecycle;

(g) the Review Route.

58.3. An Actor shall perform an Assigned Role only within its Role Scope.

58.4. Each Role performed by the same Actor shall retain its own scope, responsibility, conditions, evidence and lifecycle.

58.5. Role recognition shall not, by itself, create access, disclosure, Authorisation, Service Permission, Technical Exchange Permission or Controlled Reliance.

58.6. Role information shall be published only where the competent Framework Body authorises publication.

Article 59: Mandates and representation

59.1. An Actor shall act for, represent, support or bind another Actor only within an assigned Mandate.

59.2. A Mandate shall identify:

(a) the mandating Actor and Representative;

(b) the Represented Person or Actor;

(c) the purpose and permitted acts;

(d) the Subjects and Controlled Matters concerned;

(e) the recipients or services for which the Mandate applies;

(f) the conditions, restrictions and evidence requirements;

(g) the Effective Date, Validity Period and lifecycle;

(h) the Review and Remedy Routes.

59.3. A Representative shall verify that the Mandate remains active and applicable before performing an act that depends on it.

59.4. A restriction, suspension, withdrawal, revocation or expiry of a Mandate shall be communicated to each Actor and Trust Service materially affected by that change.

59.5. A Mandate and each material lifecycle change shall be recorded in a form sufficient for Verification and historical reconstruction.

59.6. A Mandate concerning a Protected Person shall include safeguards against conflict, coercion and misuse and shall preserve an Accessible Alternative where required.

Article 60: Responsible Actors

60.1. Each Framework Function, Controlled Matter, Trust Service, Source, Technical Exchange Route, Controlled Interaction and material obligation shall have an identifiable Responsible Actor.

60.2. A Responsible Actor shall:

(a) perform its assigned function within scope;

(b) comply with the applicable Framework Instruments;

(c) maintain required evidence and records;

(d) preserve applicable security and safeguard conditions;

(e) report material failures and changes;

(f) cooperate with supervision, Review and Remedy.

60.3. Where responsibility is shared, the applicable Framework Instrument shall identify each Responsible Actor, the allocated functions, the boundaries between them and the treatment of shared failures.

60.4. Delegation, outsourcing, automation or use of an Intermediary shall not remove assigned responsibility.

60.5. An ambiguity or gap in responsibility shall be referred to the competent Framework Body and shall not reduce protection available to an Affected Person or Protected Person.

SECTION 2: INTERACTION AND ATTRIBUTION ROLES

Article 61: Requesting and Responding Actors

61.1. A Requesting Actor shall initiate a Controlled Interaction only where the applicable Participation, Role, Mandate, purpose, Authorisation, Access Conditions, Disclosure Conditions and evidence requirements are satisfied.

61.2. A request shall identify:

(a) the Requesting Actor;

(b) the intended Responding Actor or Trust Service;

(c) the recognised purpose;

(d) the requested action or Controlled Matter;

(e) the applicable policy, restrictions and correlation information;

(f) the evidence required by the applicable Profile.

61.3. A Responding Actor shall respond only where:

(a) the Requesting Actor is identified, authenticated and authorised as required;

(b) the requested action is within the Responding Actor's Assigned Role and responsibility;

(c) the applicable Federation Trust Policy and the Responding Actor's Authorisation Policy are satisfied;

(d) the applicable Access Conditions, Disclosure Conditions and safeguards are satisfied;

(e) the response can be produced with the required protection and evidence.

61.4. Inclusion of the Requesting Actor, Issuer or Trust Service in the Humanitarian Trust List shall not require the Responding Actor to disclose information or provide a service.

61.5. The Requesting Actor and Responding Actor shall maintain the evidence required to reconstruct a material Controlled Interaction.

Article 62: Relying Actors

62.1. A Relying Actor shall undertake Controlled Reliance only in accordance with Article 42 and the applicable Reliance Conditions.

62.2. A Relying Actor shall determine whether a Controlled Matter is acceptable for the identified purpose under its Local Trust Acceptance Policy.

62.3. A Relying Actor shall evaluate:

(a) the category and identity of the Controlled Matter;

(b) the relevant Status and mandatory dependencies;

(c) the required Verification and Validation;

(d) the applicable Assurance and Qualified Status;

(e) the Reliance Limits, caveats and Validity Period;

(f) the applicable safeguards and Review Route.

62.4. A positive Validation Result or authorised Status Response shall not require a Relying Actor to accept or rely on the evaluated matter.

62.5. A Relying Actor shall remain responsible for the operational decision or service outcome based on Controlled Reliance.

62.6. Where Controlled Reliance is capable of producing an Adverse Protected-Person Effect, the Relying Actor shall preserve natural-person review and the applicable Review and Remedy Routes where required by the Scheme or Profile.

Article 63: Issuers and Attestation Issuers

63.1. An Issuer shall be responsible for each issued Trust Object or Trust Service Output attributable to it within the assigned scope.

63.2. An Issuer shall ensure that the issued matter satisfies the applicable identity, content, protection, evidence, Status and lifecycle requirements.

63.3. An Attestation Issuer shall ensure that an Electronic Attestation identifies the Attestation Statement, Attestation Issuer, Subject where applicable, Source Basis or other evidence basis where required, protection, Status and Reliance Conditions.

63.4. Issuer responsibility shall not transfer to a Relying Actor by reason only of Controlled Reliance.

63.5. Reliance by another Actor shall not transfer responsibility for the relying decision to the Issuer.

63.6. A material error affecting an issued matter shall trigger the applicable Correction, Replacement, Suspension, Withdrawal, Revocation or notification procedure.

Article 64: Signatories and Seal Creators

64.1. A Signatory shall be the natural person to whom an Electronic Signature is attributable.

64.2. The applicable Profile shall establish the evidence required to link the Signatory, signing act, signed data, Digital Signature, creation mechanism or device and expression of intent.

64.3. A Seal Creator shall be the legal entity to which an Electronic Seal is attributable.

64.4. The applicable Profile shall establish the evidence required to link the Seal Creator, authorised sealing process, sealed data, Digital Signature and creation mechanism or device.

64.5. A Signatory or Seal Creator shall exercise the control required by the applicable Profile over the signing or sealing process.

64.6. Attribution of an Electronic Signature or Electronic Seal shall not, by itself, establish Authorisation, correctness of content or Controlled Reliance beyond the assigned purpose.

SECTION 3: SOURCE, PROVIDER AND INTERMEDIARY ROLES

Article 65: Source Holders and Source Stewards

65.1. A Source Holder shall maintain and operate a Source within the recognised Source Scope and applicable Source Profile.

65.2. A Source Steward shall govern the mandate, semantics, Data Quality, provenance, Correction and lifecycle of a Source within its assigned scope.

65.3. The same Actor shall perform both functions only where the respective responsibilities, evidence and controls remain identifiable.

65.4. Performance of the Source Holder or Source Steward function shall not, by itself, assign Authoritative Source Status, Qualified Authoritative Source Status, Trust Service Provider Status or Service Permission.

65.5. A Source Holder and Source Steward shall cooperate with applicable Correction, Review, supervision and incident processes.

Article 66: Trust Service Providers and Identity Providers

66.1. A Trust Service Provider shall provide one or more Trust Services only within an assigned Provider Scope and in accordance with Part VIII.

66.2. Trust Service Provider Status shall remain separate from the Status and Service Permission of each Trust Service provided by that Provider.

66.3. Qualified Trust Service Provider Status shall remain separate from Qualified Trust Service Status and Qualified Trust Object Status.

66.4. An Identity Provider shall be a Trust Service Provider recognised to provide an Identification Service within an assigned Service Scope.

66.5. Recognition as an Identity Provider shall not, by itself, authorise performance of Identity Registration, Identity Resolution, Authentication, Authorisation or another function outside the recognised Identification Service Scope.

66.6. Provision of more than one Trust Service by the same Trust Service Provider shall not merge the identity, Status, evidence or responsibility of those Trust Services.

Article 67: Intermediaries, outsourcing and technical operators

67.1. An Intermediary shall perform only the facilitation function assigned through its Role, Mandate, Provider Scope or another Recognised Instrument.

67.2. An Intermediary shall preserve:

(a) the identity and responsibility of the originating and receiving Actors;

(b) the Integrity, attribution and dependency context of each Controlled Matter;

(c) the applicable Confidentiality and Disclosure Conditions;

(d) the evidence and safeguards required for the Controlled Interaction.

67.3. An Intermediary shall not alter the meaning, purpose, Status or Controlled Effect of a Controlled Matter.

67.4. An Intermediary shall not access a payload protected by Payload Confidentiality unless access is expressly authorised for the recognised purpose and recorded.

67.5. Outsourcing shall not remove the responsibility assigned to the Responsible Actor.

67.6. A technical operator supporting a Framework Body, Humanitarian Trust List, Register or Catalogue shall not acquire Decision Competence, authority to assign Status or Trust Service Provider Status by reason only of that support.

67.7. Transformation that changes meaning, attribution or dependency context shall create a separately identifiable Controlled Matter where required by the applicable Framework Instrument.

Article 68: Multiple roles, conflicts and actor lifecycle

68.1. An Actor shall perform more than one Role only where the applicable Framework Instruments permit the combination and each Role retains separate scope, responsibility, evidence and lifecycle.

68.2. The Actor and competent Framework Body shall identify and manage actual, potential and perceived conflicts of interest arising from combined Roles.

68.3. An Actor shall not:

(a) approve its own eligibility where independent approval is required;

(b) assign its own Qualified Status;

(c) independently assess or supervise its own performance;

(d) adopt and independently review the same Framework Decision.

68.4. A Role combination shall be refused, restricted, suspended or terminated where the conflict cannot be controlled consistently with the Framework.

68.5. Recognition, Participation, Assigned Roles and Mandates shall be subject to their applicable lifecycle conditions.

68.6. An Actor shall cease exercising a suspended, withdrawn, revoked or expired function from the Effective Date of that lifecycle action.

68.7. Records shall remain sufficient to reconstruct recognition, Participation, Role assignment, Mandate, lifecycle action, responsibility and material Controlled Interactions.

PART VI: TRUST OBJECTS

SECTION 1: GENERAL PROVISIONS

Article 69: Scope and general requirements

69.1. This Part establishes the Trust Object Categories recognised under the Framework.

69.2. A Trust Object shall be governed according to its category, purpose, scope, protection, evidence, Status and lifecycle.

69.3. A Trust Object shall be independently identifiable within its applicable scope.

69.4. Creation, issuance, possession, presentation, Verification, Validation or technical availability of a Trust Object shall not, by itself, create Authorisation, Controlled Reliance or another Controlled Effect.

69.5. A Trust Service Output shall constitute a Trust Object only where this Part assigns it a Trust Object Category and lifecycle.

69.6. A Trust Object shall not change category by reason only of its representation, transport, storage or use in another process.

Article 70: Identifiers, Serial Numbers and Metadata

70.1. A Trust Object shall contain or reference a Trust Object Identifier sufficient to distinguish it within its applicable scope.

70.2. An issued Trust Object shall contain or reference an issuer-scoped Serial Number where the applicable Profile requires one.

70.3. An Identifier or Serial Number shall constitute Metadata and shall not, by itself, establish authenticity, validity, ownership, authority, Status or Controlled Reliance.

70.4. Trust Object Metadata shall identify, where applicable:

(a) the Trust Object Category;

(b) the Issuer or responsible Trust Service;

(c) the Version;

(d) the creation or issuance time;

(e) the applicable Profile;

(f) the Status reference;

(g) the Validity Period;

(h) the dependencies and evidence references.

70.5. Metadata shall be protected against unauthorised alteration where alteration could affect Verification, Validation, Status or Controlled Reliance.

Article 71: Status and lifecycle of Trust Objects

71.1. A Trust Object shall be subject to the lifecycle assigned by the Framework and the applicable Profile.

71.2. The lifecycle shall identify, where applicable:

(a) creation;

(b) issuance;

(c) activation;

(d) presentation;

(e) Verification and Validation;

(f) restriction;

(g) suspension;

(h) withdrawal or revocation;

(i) replacement or supersession;

(j) retention, preservation and archival;

(k) expiry and closure.

71.3. Trust Object Status shall apply only to the identified Trust Object and assigned scope.

71.4. A lifecycle action affecting one Trust Object shall affect another Trust Object only where the applicable dependency relationship or Framework Instrument establishes that effect.

71.5. Historical Status and Version information shall remain reconstructable where required for Validation, Review, Remedy or Controlled Reliance.

Article 72: Qualified Trust Object Status

72.1. Each Trust Object Category established by this Part shall be eligible for Qualified Trust Object Status where an applicable Qualified Object Profile defines meaningful qualified conditions for that category.

72.2. An individual Trust Object shall have Qualified Trust Object Status only where:

(a) it satisfies the applicable Qualified Object Profile;

(b) it is created or issued through the Trust Service Status required by that Profile;

(c) each required qualified dependency is valid within its assigned scope;

(d) the required creation, issuance and Validation evidence is available;

(e) Validation confirms satisfaction of the applicable qualified conditions.

72.3. Qualified Trust Object Status shall arise through satisfaction and Validation of the applicable Qualified Object Profile and shall not require an individual Framework Decision unless the Framework expressly assigns such a decision.

72.4. Qualified Trust Object Status shall apply only to the identified Trust Object and Qualified Scope.

72.5. Qualified Trust Object Status shall not transfer to:

(a) the Issuer;

(b) the Subject;

(c) the Trust Service Provider;

(d) the Trust Service;

(e) the Source Basis;

(f) a mechanism, device or dependent Trust Object.

SECTION 2: DIGITAL SIGNATURES, CREATION DATA AND CREATION DEVICES

Article 73: Digital Signatures

73.1. A Digital Signature shall be associated with identified electronic data for the purpose of supporting Integrity Verification and origin binding within an assigned scope.

73.2. A Digital Signature shall identify or reference:

(a) the signed data or an unambiguous representation of that data;

(b) the Digital Signature Validation Data or Certificate required for Validation;

(c) the Digital Signature Creation Mechanism or Device category;

(d) the applicable algorithm and parameter identifiers;

(e) the creation evidence required by the applicable Profile.

73.3. A Digital Signature shall not disclose or directly identify Digital Signature Creation Data.

73.4. A Digital Signature shall not, by itself, constitute an Electronic Signature or Electronic Seal.

73.5. A Digital Signature shall have Qualified Trust Object Status only where Article 72 and the applicable Qualified Profile for Digital Signatures are satisfied.

Article 74: Digital Signature Creation Data and Validation Data

74.1. Digital Signature Creation Data shall be unique within the assigned creation process and protected throughout its lifecycle.

74.2. Digital Signature Creation Data shall:

(a) be protected against disclosure;

(b) be protected against unauthorised alteration and use;

(c) be activated only through an authorised creation process;

(d) remain subject to the control model assigned by the applicable Profile;

(e) be destroyed, revoked or rendered unusable when required by the applicable lifecycle condition.

74.3. Digital Signature Validation Data shall be made available only to the extent necessary for authorised Verification and Validation.

74.4. Validation Data shall remain linked to the applicable Status, Certificate, algorithm, parameter and lifecycle information.

74.5. Compromise or suspected compromise of creation data shall trigger the applicable containment, Status, revocation, replacement and notification procedures.

Article 75: Digital Signature Creation Mechanisms and Devices

75.1. A Digital Signature Creation Mechanism or Device shall be independently identifiable and governed within an assigned function, configuration and operational environment.

75.2. A Digital Signature Creation Mechanism or Device shall ensure that Digital Signature Creation Data:

(a) remains confidential;

(b) is protected against unauthorised use;

(c) is used only within the authorised creation process;

(d) cannot be derived through ordinary operation of the mechanism or device;

(e) is subject to auditable lifecycle controls.

75.3. A Qualified Digital Signature Creation Device shall have Qualified Status only where the applicable Qualified Profile, Conformity Assessment and Framework Decision assign that Status.

75.4. Qualified Status shall apply only to the identified device, configuration, Version, function and operational environment.

75.5. Qualified Status assigned to a mechanism or device shall not, by itself, qualify a Trust Service, Digital Signature, Electronic Signature, Electronic Seal or Trust Service Provider.

SECTION 3: ELECTRONIC SIGNATURES

Article 76: Electronic Signatures and Advanced Electronic Signatures

76.1. An Electronic Signature shall be attached to or logically associated with identified electronic data and attributable to a Signatory.

76.2. An Electronic Signature shall record or reference the evidence required to establish the association between:

(a) the Signatory;

(b) the signing act;

(c) the signed data;

(d) the applicable Digital Signature;

(e) the applicable creation mechanism or device.

76.3. An Advanced Electronic Signature shall:

(a) be uniquely linked to the Signatory;

(b) be capable of identifying the Signatory within the assigned scope;

(c) be created using Digital Signature Creation Data used for the Electronic Signature that the Signatory controls with a high level of confidence under the applicable Profile;

(d) be linked to the signed data so that any subsequent change is detectable;

(e) contain or reference the evidence required for Validation.

76.4. An Electronic Signature shall not create Authorisation, consent to unrelated processing or Controlled Reliance beyond the assigned signing purpose.

Article 77: Qualified Electronic Signatures

77.1. A Qualified Electronic Signature shall:

(a) satisfy Article 76.3;

(b) be created through a Qualified Digital Signature Creation Device or another qualified creation arrangement permitted by the applicable Qualified Profile;

(c) be based on a valid Qualified Certificate whose Profile is applicable to Electronic Signatures where required by the applicable Qualified Profile;

(d) satisfy the applicable Qualified Electronic Signature Profile;

(e) be capable of Validation as satisfying the qualified conditions.

77.2. Qualified Status of a Qualified Electronic Signature shall apply only to the identified Electronic Signature.

77.3. Qualified Status of the Certificate, creation device, Digital Signing Service or Electronic Signature Service shall constitute a dependency condition and shall not transfer to the Electronic Signature.

77.4. Framework qualification shall not, by itself, assign External Legal Effect to the Qualified Electronic Signature.

SECTION 4: ELECTRONIC SEALS

Article 78: Electronic Seals and Advanced Electronic Seals

78.1. An Electronic Seal shall be attached to or logically associated with identified electronic data and attributable to a Seal Creator.

78.2. An Electronic Seal shall record or reference the evidence required to establish the association between:

(a) the Seal Creator;

(b) the authorised sealing process;

(c) the sealed data;

(d) the applicable Digital Signature;

(e) the applicable creation mechanism or device.

78.3. An Advanced Electronic Seal shall:

(a) be uniquely linked to the Seal Creator;

(b) be capable of identifying the Seal Creator within the assigned scope;

(c) be created using Digital Signature Creation Data used for the Electronic Seal and controlled by the Seal Creator with a high level of confidence under the applicable Profile;

(d) be linked to the sealed data so that any subsequent change is detectable;

(e) contain or reference the evidence required for Validation.

78.4. An Electronic Seal shall evidence origin and Integrity and shall not, by itself, establish the correctness, lawfulness or acceptance of the sealed content.

Article 79: Qualified Electronic Seals

79.1. A Qualified Electronic Seal shall:

(a) satisfy Article 78.3;

(b) be created through a Qualified Digital Signature Creation Device or another qualified creation arrangement permitted by the applicable Qualified Profile;

(c) be based on a valid Qualified Certificate whose Profile is applicable to Electronic Seals where required by the applicable Qualified Profile;

(d) satisfy the applicable Qualified Electronic Seal Profile;

(e) be capable of Validation as satisfying the qualified conditions.

79.2. Qualified Status of a Qualified Electronic Seal shall apply only to the identified Electronic Seal.

79.3. Qualified Status of the Certificate, creation device, Digital Signing Service or Electronic Seal Service shall constitute a dependency condition and shall not transfer to the Electronic Seal.

79.4. Framework qualification shall not, by itself, assign External Legal Effect to the Qualified Electronic Seal.

SECTION 5: ELECTRONIC TIMESTAMPS

Article 80: Electronic Timestamps

80.1. An Electronic Timestamp shall bind identified electronic data to an identified time.

80.2. An Electronic Timestamp shall identify or reference:

(a) the data or an unambiguous representation of the data;

(b) the time value;

(c) the applicable time source;

(d) the accuracy and uncertainty where required;

(e) the Issuer or Electronic Timestamp Service;

(f) the protection and Validation evidence.

80.3. An Electronic Timestamp shall evidence the association between the data and time and shall not, by itself, establish the correctness or lawfulness of the data.

Article 81: Qualified Electronic Timestamps

81.1. A Qualified Electronic Timestamp shall:

(a) bind the identified data to an identified time so that any undetectable change is prevented under the applicable Qualified Profile;

(b) use a time source satisfying the applicable qualified accuracy and traceability requirements;

(c) be protected by the qualified Electronic Signature, Electronic Seal or other qualified protection required by the applicable Qualified Profile;

(d) be issued through an Electronic Timestamp Service having Qualified Trust Service Status where required by the applicable Qualified Profile;

(e) be capable of Validation as satisfying the qualified conditions.

81.2. Qualified Status of a Qualified Electronic Timestamp shall apply only to the identified Electronic Timestamp.

81.3. Qualified Status of a time source, protection object or Electronic Timestamp Service shall not transfer to the Electronic Timestamp.

SECTION 6: CERTIFICATES

Article 82: Certificates

82.1. A Certificate shall link Digital Signature Validation Data or another controlled value to an identified Subject.

82.2. A Certificate shall identify or reference:

(a) the Subject;

(b) the Issuer;

(c) the validation data or controlled value;

(d) the applicable Profile for Certificates;

(e) the Validity Period;

(f) the Status reference;

(g) the Serial Number;

(h) the applicable restrictions and intended scope.

82.3. A Certificate shall constitute a specialised Electronic Attestation and shall remain subject to the requirements applicable to its Certificate category.

82.4. A Certificate shall not, by itself, create identity, Role, Authorisation, ownership or Controlled Reliance beyond the certified association.

Article 83: Qualified Certificates

83.1. A Qualified Certificate shall:

(a) satisfy the applicable Qualified Profile for Certificates;

(b) be issued through the Trust Service Status required by that Profile;

(c) contain or reference the required Subject, Issuer, validation, Status, validity, restriction and serial-number information;

(d) be protected through the qualified protection required by the applicable Qualified Profile;

(e) be capable of Validation as satisfying the qualified conditions.

83.2. A Qualified Certificate for Electronic Signatures shall link Digital Signature Validation Data to a natural person.

83.3. A Qualified Certificate for Electronic Seals shall link Digital Signature Validation Data to a legal entity.

83.4. Qualified Status of a Qualified Certificate shall apply only to the identified Certificate and shall not transfer to the Subject, Issuer, Trust Service or Trust Object using the Certificate.

SECTION 7: ELECTRONIC ATTESTATIONS

Article 84: Electronic Attestations and Advanced Electronic Attestations

84.1. An Electronic Attestation shall contain an Attestation Statement attributable to an identified Attestation Issuer.

84.2. An Electronic Attestation shall be governed according to the function of attesting a statement and not according to the sector, programme or use case to which the statement relates.

84.3. An Electronic Attestation shall identify or reference:

(a) the Attestation Issuer;

(b) the Subject, where applicable;

(c) the Attestation Statement;

(d) the Source Basis or other evidence basis, where required;

(e) the Trust Object Identifier and issuer-scoped Serial Number;

(f) the issuance time;

(g) the Validity Period or Freshness Condition;

(h) the applicable Assurance information;

(i) the Status reference;

(j) the restrictions, caveats and Reliance Limits;

(k) the applicable protection object.

84.4. An Advanced Electronic Attestation shall:

(a) be uniquely attributable to the Attestation Issuer;

(b) identify the Attestation Issuer within the assigned scope;

(c) protect the Attestation Statement and material Metadata against undetected alteration;

(d) contain or reference the evidence required by the applicable Attestation Profile assigning advanced conditions;

(e) be capable of Validation against the applicable Profile and Status information.

84.5. An Electronic Attestation shall not, by itself, create the underlying fact, Status, relationship, decision, eligibility or entitlement expressed by the Attestation Statement.

Article 85: Qualified Electronic Attestations

85.1. A Qualified Electronic Attestation shall:

(a) satisfy Article 84.4;

(b) satisfy the applicable Qualified Profile for Electronic Attestations;

(c) be issued through an Electronic Attestation Service having Qualified Trust Service Status where required by that Profile;

(d) use each qualified Source, Certificate, Electronic Signature, Electronic Seal, Electronic Timestamp or other dependency required by that Profile;

(e) be capable of Validation as satisfying the qualified conditions.

85.2. Qualified Status of a Qualified Electronic Attestation shall apply only to the identified Electronic Attestation.

85.3. Qualified Status of the Attestation Issuer, Trust Service, Source or protection object shall constitute a dependency condition and shall not transfer to the Electronic Attestation.

85.4. The subject matter of the Attestation Statement shall not alter the qualified object category.

SECTION 8: IDENTIFICATION SERVICE OUTPUTS

Article 86: Identification Results and Identity Resolution Results

86.1. An Identification Result shall record the outcome of an Identification Service other than Identity Resolution.

86.2. An Identity Resolution Result shall record a determination concerning relationships between identity records within an assigned scope.

86.3. An Identification Result or Identity Resolution Result shall identify or reference:

(a) the Identification Service;

(b) the identification or resolution purpose;

(c) the evidence and Source Basis used;

(d) the method and Version;

(e) the result and confidence or Assurance information;

(f) the time and Validity Period;

(g) the limitations, caveats and human-review conditions.

86.4. An Identity Resolution Result shall not, by itself, establish identity, registration, eligibility, entitlement, fraud or misconduct.

86.5. Issuance of an Identification Result or Identity Resolution Result as an Electronic Attestation shall create a separate Electronic Attestation.

86.6. Qualified Status shall apply to an Identification Result or Identity Resolution Result only where Article 72 and the applicable Qualified Object Profile are satisfied.

SECTION 9: AUTHENTICATION AND AUTHORISATION OUTPUTS

Article 87: Authentication Outcomes and Authorisation Outcomes

87.1. An Authentication Outcome shall record whether an asserted identity, Role, origin, device, session, transaction, service, Trust Object or Controlled Interaction has been authenticated within an assigned scope.

87.2. An Authorisation Outcome shall record whether an identified action, access, disclosure, exchange, service use or Controlled Interaction is permitted within an assigned scope.

87.3. An Authentication Outcome or Authorisation Outcome shall identify or reference:

(a) the producing Trust Service;

(b) the evaluated assertion or requested action;

(c) the evaluation context;

(d) the applicable Profile or policy and Version;

(e) the evidence and Status information used;

(f) the result;

(g) the time and Validity Period;

(h) the restrictions, obligations and caveats.

87.4. A successful Authentication Outcome shall not, by itself, create Authorisation.

87.5. An Authorisation Outcome shall not, by itself, execute or enforce the authorised action.

87.6. Qualified Status shall apply to an Authentication Outcome or Authorisation Outcome only where Article 72 and the applicable Qualified Object Profile are satisfied.

SECTION 10: VALIDATION AND STATUS OUTPUTS

Article 88: Verification Results, Validation Results and Status Responses

88.1. A Verification Result shall record the outcome of checking identified information, evidence, Status or relationships against defined conditions.

88.2. A Validation Result shall record whether an identified Controlled Matter satisfies the applicable validation basis and Reliance Conditions at an identified time.

88.3. A Status Response shall provide authorised Status information concerning an identified Status-Bearing Matter.

88.4. Each Verification Result, Validation Result or Status Response shall identify or reference:

(a) the producing Validation and Verification Service;

(b) the evaluated matter;

(c) the evaluation basis and Profile Version;

(d) the evidence and Status information used;

(e) the evaluation time;

(f) the result;

(g) the Validity Period;

(h) the restrictions and caveats.

88.5. A Verification Result, Validation Result or Status Response shall not create or alter the underlying Status, Source, Trust Object, Authorisation or Controlled Reliance.

88.6. Qualified Status shall apply to a Verification Result, Validation Result or Status Response only where Article 72 and the applicable Qualified Object Profile are satisfied.

SECTION 11: FEDERATED DATA EXCHANGE OUTPUTS

Article 89: Exchange Evidence and Controlled Exchange Results

89.1. Exchange Evidence shall evidence the processing, transmission, receipt, refusal or failure of a Controlled Interaction.

89.2. A Controlled Exchange Result shall record the outcome of a Federated Data Exchange Service interaction.

89.3. Exchange Evidence or a Controlled Exchange Result shall identify or reference:

(a) the Federated Data Exchange Service;

(b) the requesting and responding endpoints or Actors;

(c) the interaction identifier;

(d) the message or payload reference without unnecessary disclosure of content;

(e) the relevant times;

(f) the route and security context;

(g) the result or delivery state;

(h) the applicable limitations and caveats.

89.4. Exchange Evidence or a Controlled Exchange Result shall not, by itself, create access, disclosure permission, acceptance of content or Controlled Reliance.

89.5. Qualified Status shall apply to Exchange Evidence or a Controlled Exchange Result only where Article 72 and the applicable Qualified Object Profile are satisfied.

SECTION 12: DEPENDENCIES, CORRECTION AND PRESERVATION

Article 90: Trust Object dependencies, Correction and historical validity

90.1. A Trust Object dependency shall identify the dependent Trust Object, supporting Controlled Matter, dependency type, applicable condition and lifecycle effect.

90.2. A dependency shall not transfer identity, Status, responsibility, Assurance or Qualified Status.

90.3. A signed, sealed, timestamped or otherwise integrity-protected Trust Object shall not be altered after issuance.

90.4. An error or changed condition shall be addressed through Correction of the underlying record and, where applicable:

(a) replacement;

(b) supersession;

(c) suspension;

(d) withdrawal;

(e) revocation;

(f) issuance of a corrective Trust Object;

(g) publication of an applicable Status or caveat.

90.5. Correction of an underlying Source, decision or record shall not alter an existing Trust Object.

90.6. A later lifecycle action shall not automatically invalidate a Trust Object that satisfied the requirements applicable at its creation or issuance time.

90.7. Historical evidence, Status, Version and dependency information shall remain available where required for Validation, Review, Remedy or Controlled Reliance.

PART VII: SOURCES AND AUTHORITATIVE SOURCES

SECTION 1: GENERAL PROVISIONS

Article 91: Subject matter and category boundaries

91.1. This Part establishes the requirements applicable to Sources, Authoritative Sources and Qualified Authoritative Sources.

91.2. A Source shall remain separate from:

(a) a Trust Service Provider;

(b) a Trust Service;

(c) a Trust Service Output;

(d) a Trust Object;

(e) a Technical Exchange Route;

(f) a Humanitarian Trust List Entry.

91.3. Recognition, use, technical availability or publication of a Source shall not, by itself, assign Authoritative Source Status, Qualified Authoritative Source Status, access, disclosure permission, Service Permission, Technical Exchange Permission or Controlled Reliance.

91.4. Source Status shall apply only to the identified Source and Source Scope.

91.5. A Framework Instrument shall not treat a copy, extract, replica, transformation, aggregation or derivative as the originating Source unless a separate recognition decision identifies that matter as a Source.

Article 92: Recognition of Sources and Source Profiles

92.1. A Framework Body shall recognise a Source only where the applicable Source Profile and evidence identify:

(a) the Source;

(b) the Source Holder;

(c) the Source Steward, where assigned;

(d) the recognised purpose;

(e) the Source Scope;

(f) the information maintained by the Source;

(g) the applicable quality, semantic, provenance and Freshness Conditions;

(h) the access and Disclosure Conditions;

(i) the Correction, Review and Remedy Routes;

(j) the lifecycle conditions.

92.2. A Framework Decision recognising a Source shall identify the Source Status, Source Scope, Effective Date, applicable restrictions and review date.

92.3. A recognised Source shall be governed by an applicable Source Profile.

92.4. A Source Profile shall select the requirements applicable to the identified Source and shall not, by itself, assign Source Status, Authoritative Source Status or Qualified Status.

92.5. Technical schemas, formats, interfaces, validation rules and implementation parameters applicable to a Source shall be established through the applicable Technical Specification.

Article 93: Source Holders and Source Stewards

93.1. A Source Holder shall maintain the Source within the recognised Source Scope and in accordance with the applicable Source Profile.

93.2. A Source Holder shall ensure that Source information and material changes are attributable, traceable and subject to the applicable quality, security, Correction and lifecycle controls.

93.3. A Source Steward shall govern, within its assigned scope:

(a) semantic definitions;

(b) classifications, taxonomies and controlled vocabularies;

(c) Data Quality requirements;

(d) provenance requirements;

(e) Correction conditions;

(f) lifecycle conditions;

(g) proposals for changes to the Source Profile.

93.4. Where the same Actor performs the functions of Source Holder and Source Steward, the respective responsibilities and controls shall remain separately identifiable.

93.5. Performance of the Source Holder or Source Steward function shall not, by itself, assign Trust Service Provider Status, Authoritative Source Status or Qualified Status.

SECTION 2: AUTHORITATIVE AND QUALIFIED SOURCE STATUS

Article 94: Source Designation and Authoritative Source Status

94.1. A Source shall have Authoritative Source Status only where a Framework Body acting within its Decision Competence assigns that Status through Source Designation.

94.2. A Framework Decision assigning Source Designation shall identify:

(a) the Source and Source Holder;

(b) the authoritative Source Scope;

(c) the information for which the Source is authoritative;

(d) the recognised purpose;

(e) the evidence supporting the designation;

(f) the applicable Assurance, quality, semantic, provenance and Freshness Conditions;

(g) the Effective Date and review date;

(h) the restrictions, caveats and Reliance Limits;

(i) the Correction, restriction, suspension and withdrawal conditions.

94.3. Authoritative Source Status shall apply only within the Source Scope assigned by the Framework Decision.

94.4. Information outside the authoritative Source Scope shall not be treated as authoritative by reason only of its inclusion in the same Source.

94.5. A copy, extract, replica, transformation, aggregation or derivative shall not inherit Authoritative Source Status.

94.6. Authoritative Source Status shall not, by itself, create access, disclosure permission, Authorisation, Service Permission, Technical Exchange Permission or Controlled Reliance.

Article 95: Qualified Authoritative Source Status

95.1. An Authoritative Source shall have Qualified Authoritative Source Status only where:

(a) an applicable Qualified Profile for the Authoritative Source is in force;

(b) the Source satisfies the applicable Assurance, quality, provenance, security and lifecycle conditions;

(c) the required Conformity Assessment has been completed;

(d) each material non-conformity has been resolved;

(e) the evidence basis has been recorded;

(f) a Framework Body acting within its Decision Competence assigns that Status in accordance with Articles 142 and 146.

95.2. Qualified Authoritative Source Status shall apply only to the identified Source and Qualified Scope.

95.3. Qualified Authoritative Source Status shall not transfer to:

(a) the Source Holder;

(b) the Source Steward;

(c) a Trust Service using the Source;

(d) a Trust Service Output based on the Source;

(e) a Trust Object referring to the Source;

(f) a copy, extract, transformation, aggregation or derivative.

95.4. A material change affecting the Qualified Scope, provenance, quality, semantics, security or lifecycle of the Source shall trigger reassessment before Qualified Authoritative Source Status continues to apply to the changed matter.

95.5. The competent Framework Body shall publish authorised Qualified Authoritative Source Status through the Humanitarian Trust List or another governance-controlled publication mechanism where publication is authorised.

SECTION 3: SOURCE SCOPE, QUALITY AND EVIDENCE

Article 96: Source Scope and authoritative content

96.1. A Source Scope shall identify the precise boundary within which Source Status applies.

96.2. The Source Scope shall identify, where applicable:

(a) the information, Attributes or record categories;

(b) the Subject or object categories;

(c) the population scope;

(d) the geographic scope;

(e) the organisational scope;

(f) the temporal scope;

(g) the recognised purpose;

(h) the applicable limitations.

96.3. Overlapping Source Scopes shall be recognised only where the applicable Source Profiles and Framework Decisions define the relationship between those Sources.

96.4. Where Sources provide conflicting information, the applicable Scheme or Profile shall define the comparison, escalation, human Review and resolution conditions.

96.5. Resolution of conflicting Source information shall not alter the Source Status of either Source unless a Framework Decision assigns that Controlled Effect.

Article 97: Data Quality, semantics and provenance

97.1. A Source Holder shall maintain Data Quality in accordance with the applicable Source Profile.

97.2. The applicable Source Profile shall define the required conditions concerning:

(a) accuracy;

(b) completeness;

(c) consistency;

(d) validity;

(e) uniqueness;

(f) currentness and timeliness;

(g) traceability;

(h) semantic consistency;

(i) Correction.

97.3. Estimated, approximate, incomplete, disputed, unverified, derived or unknown values shall remain distinguishable from confirmed values.

97.4. Provenance shall identify, where applicable:

(a) the origin of the information;

(b) the method and time of creation or collection;

(c) the responsible Actor or system;

(d) each material transformation;

(e) each Correction;

(f) each supersession or replacement;

(g) the applicable Version and Status.

97.5. A Source Steward shall ensure that changes to semantic definitions, classifications, taxonomies, controlled vocabularies and code lists are versioned and traceable.

97.6. A change to a semantic definition shall not retrospectively change the meaning of information created under an earlier Version.

Article 98: Freshness, derivation and historical state

98.1. A Source used for an identified purpose shall satisfy the applicable Freshness Condition.

98.2. A Freshness Condition shall identify the event, time, review interval or maximum age relevant to the purpose for which the Source information is used.

98.3. A derived value shall identify:

(a) the Source values on which it depends;

(b) the derivation rule;

(c) the rule Version;

(d) the time of derivation;

(e) the responsible Actor or system.

98.4. A derived value shall not inherit Authoritative Source Status unless the applicable Framework Decision expressly assigns that Status to the identified derivation and Source Scope.

98.5. Historical Source Status, Version, provenance and semantic information shall remain reconstructable where required for Validation, Review, Remedy or Controlled Reliance.

SECTION 4: ACCESS, USE AND OUTPUTS

Article 99: Access and disclosure

99.1. Access to a Source shall occur only where:

(a) the Requesting Actor is identified and authenticated as required;

(b) the requested purpose is authorised;

(c) the applicable Access Conditions are satisfied;

(d) the applicable Disclosure Conditions are satisfied;

(e) the request is limited to the information necessary for the authorised purpose;

(f) the applicable security and Protected-Person Safeguards are satisfied.

99.2. A Source Holder shall enforce the applicable Access Conditions and Disclosure Conditions.

99.3. Technical availability of a Source or Endpoint shall not constitute access, disclosure or Technical Exchange Permission.

99.4. A Source Holder shall retain evidence of material access, disclosure, refusal and restriction decisions according to the applicable Framework Instrument.

99.5. Cross-domain access shall remain subject to Article 103 and the applicable Federation Agreement.

Article 100: Use of Sources by Trust Services and Relying Actors

100.1. A Trust Service shall use a Source only within the recognised Source Scope and the Service Scope assigned to that Trust Service.

100.2. Before using Source information, a Trust Service Provider shall evaluate, where applicable:

(a) the Source Status;

(b) the Source Scope;

(c) the applicable Authoritative Source Status or Qualified Authoritative Source Status;

(d) the Freshness Condition;

(e) Data Quality and semantic conditions;

(f) Provenance;

(g) restrictions, caveats and dependencies.

100.3. The applicable Profile shall determine whether a Trust Service Output or Trust Object requires:

(a) a recognised Source;

(b) an Authoritative Source;

(c) a Qualified Authoritative Source;

(d) more than one independent Source;

(e) another evidence basis;

(f) no Source dependency.

100.4. Use of a Source by a Trust Service shall not convert the Source into a Trust Service Output or Trust Object.

100.5. Use of Source information shall not remove the responsibility of a Relying Actor to apply the applicable Trust Acceptance Policy and Reliance Conditions.

100.6. A Local Trust Acceptance Policy shall not alter the Source Status assigned by a Framework Body.

Article 101: Source Verification and representation of Source information

101.1. Where Source Verification produces a Trust Service Output, it shall be performed within the Service Scope of a Validation and Verification Service.

101.2. A Verification Result concerning a Source or Source Basis shall remain separate from the Source and Source Status.

101.3. A Verification Result shall not, by itself, assign, extend, restrict, suspend or withdraw Source Status.

101.4. Where Source information or a Verification Result is represented in an Electronic Attestation, that Electronic Attestation shall constitute a separate Trust Object issued through an Electronic Attestation Service.

101.5. Issuance of an Electronic Attestation shall not convert the underlying Source, Source record or Verification Result into an Electronic Attestation.

101.6. The applicable Profile shall define the Source references, evidence, Assurance information, caveats and Reliance Limits included in or associated with the resulting Trust Service Output or Trust Object.

SECTION 5: CORRECTION, LIFECYCLE AND CROSS-DOMAIN USE

Article 102: Correction, restriction, suspension and withdrawal

102.1. A recognised Source shall have an accessible Correction Route appropriate to its purpose, scope and potential Controlled Effects.

102.2. A Source Holder shall record each material Correction, including:

(a) the information corrected;

(b) the reason for the Correction;

(c) the evidence basis;

(d) the corrected information;

(e) the Effective Date;

(f) the responsible Actor;

(g) the effect on dependent Controlled Matters.

102.3. Correction of Source information shall not alter an existing signed, sealed, timestamped or otherwise integrity-protected Trust Object or Trust Service Output.

102.4. Where corrected Source information affects an existing Trust Object or Trust Service Output, the responsible Actor shall apply the applicable replacement, supersession, restriction, suspension, withdrawal, revocation, notification or re-evaluation procedure.

102.5. A Framework Body shall restrict, suspend or withdraw Source Status only where the applicable evidence and lifecycle conditions support that Controlled Effect.

102.6. Restriction, suspension or withdrawal of Source Status shall affect dependent Trust Services, Trust Service Outputs and Trust Objects only through an identified dependency and within the affected scope.

102.7. Restriction, suspension or withdrawal of Source Status shall not automatically invalidate a Trust Object or Trust Service Output created before the Effective Date of that action.

102.8. The competent Framework Body shall publish authorised Source Status changes through the applicable governance-controlled publication mechanism.

Article 103: Cross-domain recognition and use

103.1. Cross-domain recognition and use of a Source shall be governed by the applicable Federation Agreement, Scheme, Profile and conditions governing recognition of the Source.

103.2. Cross-domain use shall identify:

(a) the originating Federation Domain;

(b) the receiving Federation Domain;

(c) the Source Status and Source Scope;

(d) the applicable Federation Trust Relationship;

(e) the permitted purpose;

(f) the Access Conditions, Disclosure Conditions and Reliance Conditions;

(g) the Correction, Review and Remedy Routes.

103.3. Recognition, Authoritative Source Status or Qualified Authoritative Source Status in one Federation Domain shall not automatically create equivalent Status in another Federation Domain.

103.4. The competent Framework Body in the receiving Federation Domain shall determine recognition within its Decision Competence, and each Relying Actor shall determine acceptance under its applicable Trust Acceptance Policy.

103.5. Participating Federation Domains shall coordinate material Correction, restriction, suspension, withdrawal, incident and Status Publication information affecting cross-domain use.

103.6. Cross-domain coordination shall not transfer Decision Competence between Federation Domains unless a Federation Agreement expressly assigns that Decision Competence.

PART VIII: TRUST SERVICE PROVIDERS

SECTION 1: RECOGNITION AND TRUST SERVICE PROVIDER STATUS

Article 104: Subject matter and provider boundaries

104.1. This Part establishes the requirements applicable to Trust Service Providers.

104.2. A Trust Service Provider shall remain separate from:

(a) each Trust Service provided by that Trust Service Provider;

(b) each Trust Service Output;

(c) each Trust Object;

(d) each Source;

(e) each mechanism, device, system and component;

(f) each subcontractor or dependent Provider.

104.3. Trust Service Provider Status shall apply only to the identified Trust Service Provider and Provider Scope.

104.4. Recognition, qualification, restriction, suspension or withdrawal of a Trust Service Provider shall not automatically assign the corresponding Status to a Trust Service, Trust Service Output, Trust Object, Source, mechanism or device.

104.5. Provision of more than one Trust Service by the same Trust Service Provider shall not merge those Trust Services, their Service Scopes, outputs, evidence, dependencies or lifecycle.

Article 105: Recognition and Provider Scope

105.1. A Framework Body shall recognise a Trust Service Provider only where the applicable Profile and evidence identify:

(a) the legal or organisational identity of the Provider;

(b) the Provider Scope;

(c) the Trust Service Categories for which recognition is sought;

(d) the governance and management arrangements;

(e) the responsible persons and organisational functions;

(f) the operational locations and Controlled Environments;

(g) the systems, mechanisms, devices and components to be used;

(h) the material third-party and outsourced dependencies;

(i) the security, continuity and incident arrangements;

(j) the evidence and record-management arrangements;

(k) the Complaint, Review and Remedy Routes;

(l) the cessation and transition arrangements.

105.2. A Framework Decision recognising a Trust Service Provider shall identify the Trust Service Provider Status, Provider Scope, Effective Date, applicable restrictions and review date.

105.3. Provider recognition shall not, by itself, recognise or activate a Trust Service.

105.4. Provider recognition shall not, by itself, assign Service Permission, Technical Exchange Permission, access, disclosure, Controlled Reliance or Qualified Status.

105.5. A material change affecting the Provider Scope shall be assessed before the existing Trust Service Provider Status continues to apply to the changed matter.

Article 106: Qualified Trust Service Provider Status

106.1. A Trust Service Provider shall have Qualified Trust Service Provider Status only where:

(a) an applicable Qualified Profile for the Trust Service Provider is in force;

(b) the Provider satisfies the applicable governance, organisational, operational, security, continuity and Assurance Conditions;

(c) the required Conformity Assessment has been completed;

(d) each material non-conformity has been resolved;

(e) the evidence basis has been recorded;

(f) a Framework Body acting within its Decision Competence assigns that Status in accordance with Articles 142 and 143.

106.2. Qualified Trust Service Provider Status shall apply only to the identified Trust Service Provider and Qualified Scope.

106.3. Qualified Trust Service Provider Status shall not transfer to:

(a) a Trust Service;

(b) a Trust Service Output;

(c) a Trust Object;

(d) a Source;

(e) a mechanism, device, system or component;

(f) a subcontractor or dependency.

106.4. Qualified Trust Service Provider Status within the relevant Provider Scope shall be a required condition for Qualified Trust Service Status and shall not, by itself, assign that Status.

106.5. A material change affecting the Qualified Scope shall trigger reassessment before Qualified Trust Service Provider Status continues to apply to the changed matter.

106.6. The competent Framework Body shall publish authorised Qualified Trust Service Provider Status through the Humanitarian Trust List.

SECTION 2: REQUIREMENTS APPLICABLE TO TRUST SERVICE PROVIDERS

Article 107: General obligations and service independence

107.1. A Trust Service Provider shall provide each Trust Service in accordance with:

(a) the Framework;

(b) the applicable Scheme;

(c) the applicable Profile;

(d) the applicable Implementation Guideline;

(e) the applicable Technical Specification;

(f) the assigned Trust Service Status, Service Permission and Service Scope.

107.2. A Trust Service Provider shall maintain governance, policies, procedures and controls proportionate to the Trust Services provided, their dependencies, risks and Assurance Conditions.

107.3. For each Trust Service, the Trust Service Provider shall maintain separate identification of:

(a) the service identifier and Trust Service Category;

(b) the Service Scope and Service Permission;

(c) the native Trust Service Outputs;

(d) the responsible organisational function;

(e) the applicable Schemes and Profiles;

(f) the systems, mechanisms, devices and components used;

(g) the Sources and other dependencies;

(h) the evidence and lifecycle records.

107.4. Shared systems, personnel, mechanisms, devices, components or locations shall not merge the identity, Status or responsibility of separate Trust Services.

107.5. A Trust Service Provider shall ensure that information supplied to Framework Bodies, Conformity Assessment Bodies, Participating Actors and Relying Actors is accurate, current and attributable.

107.6. A Trust Service Provider shall maintain an accessible Complaint Route and Correction Route for matters within its responsibility.

Article 108: Governance, personnel and organisational resources

108.1. A Trust Service Provider shall maintain an organisational structure capable of supporting the Trust Services within the recognised Provider Scope.

108.2. A Trust Service Provider shall assign responsibility for:

(a) Trust Service governance;

(b) security and risk management;

(c) operational control;

(d) change and configuration control;

(e) evidence and records;

(f) incident response and continuity;

(g) complaints, Correction, Review and Remedy;

(h) conformity and supervision cooperation.

108.3. Personnel performing Trust Service functions shall possess the competence, reliability, experience and qualifications required for their assigned functions.

108.4. A Trust Service Provider shall apply separation of duties where concentration of functions would create an unacceptable risk.

108.5. Access to creation data, personal data, Restricted Information, security-sensitive functions and Trust Service records shall be limited to authorised personnel.

108.6. A Trust Service Provider shall maintain sufficient financial, technical, organisational and operational resources for the Trust Services provided.

108.7. Personnel and organisational changes shall be managed so that security, continuity, evidence, accountability and the conditions supporting Service Permission are preserved.

Article 109: Systems, mechanisms, devices and controlled environments

109.1. A Trust Service Provider shall identify the systems, mechanisms, devices, components and Controlled Environments used to provide each Trust Service.

109.2. Those matters shall be:

(a) suitable for the assigned function;

(b) protected according to the applicable Security Conditions;

(c) configured and operated according to the applicable Framework Instruments;

(d) subject to controlled change and Version management;

(e) monitored throughout their lifecycle;

(f) supported by evidence sufficient for supervision and Conformity Assessment.

109.3. Status assigned to a mechanism, device, system, component or Controlled Environment shall remain separate from Trust Service Provider Status and Trust Service Status.

109.4. Qualified Status assigned to a creation mechanism or device shall not, by itself, qualify the Trust Service Provider, Trust Service or Trust Object produced through it.

109.5. A Trust Service Provider shall assess a material change to a system, mechanism, device, component or Controlled Environment before continued operation under the existing Trust Service Provider Status, Trust Service Status, Service Permission or Qualified Status.

109.6. Detailed technical requirements shall be established through the applicable Implementation Guideline, Profile and Technical Specification.

Article 110: Third parties, outsourcing and dependencies

110.1. A Trust Service Provider shall remain responsible for a Trust Service where another Actor performs a supporting or outsourced function.

110.2. Before using a material third party or outsourced function, the Trust Service Provider shall record:

(a) the function to be performed;

(b) the responsible Actors and retained responsibilities;

(c) the applicable security, Assurance and lifecycle conditions;

(d) the evidence, audit and access rights;

(e) the incident and notification obligations;

(f) the continuity, termination and transition arrangements;

(g) the effect of failure, restriction, suspension or withdrawal.

110.3. A third party shall not acquire Trust Service Provider Status or Qualified Trust Service Provider Status by reason only of performing a supporting or outsourced function.

110.4. Status assigned to a third party or its component shall not transfer to the Trust Service Provider or Trust Service.

110.5. A Trust Service Provider shall monitor each material dependency throughout its lifecycle.

110.6. A change, incident or lifecycle action affecting a dependency shall affect the Trust Service Provider or Trust Service only within the dependency scope established by the applicable Framework Instrument.

Article 111: Records, evidence and transparency

111.1. A Trust Service Provider shall maintain records and evidence sufficient to establish the proper operation and lifecycle of each Trust Service.

111.2. Records shall identify, where applicable:

(a) the Trust Service and its Version;

(b) the applicable Service Scope and Service Permission;

(c) the responsible organisational function;

(d) material requests and Trust Service Outputs;

(e) the systems, mechanisms, devices, components and dependencies used;

(f) the applicable Status and Assurance information;

(g) material changes;

(h) Security Incidents and corrective actions;

(i) Complaints, Reviews and Remedies;

(j) restriction, suspension, withdrawal, cessation and transition actions.

111.3. Records shall be protected against unauthorised access, alteration, deletion and disclosure.

111.4. The applicable Framework Instrument shall define retention, access, disclosure, preservation and deletion conditions.

111.5. A Trust Service Provider shall provide evidence to the competent Framework Body, Conformity Assessment Body, supervision function or reviewing function within the assigned competence of that function.

111.6. Transparency information supplied to Participating Actors or Relying Actors shall identify the Trust Service Provider, Trust Service, applicable Service Scope, material restrictions, applicable Profiles, Complaint Route and Status reference.

Article 112: Notification of material changes and incidents

112.1. A Trust Service Provider shall notify the competent Framework Body of a material change affecting:

(a) Trust Service Provider Status or Provider Scope;

(b) Trust Service Status, Service Permission or Service Scope;

(c) a qualified condition;

(d) a material dependency;

(e) a security or continuity condition;

(f) an operational location or Controlled Environment;

(g) a material system, mechanism, device or component;

(h) the cessation or transfer of a Trust Service.

112.2. A Trust Service Provider shall notify the competent Framework Body of a material Security Incident or non-conformity within the period defined by the applicable Framework Instrument.

112.3. A notification shall identify:

(a) the affected Provider, Trust Service and Controlled Matters;

(b) the nature and scope of the change, incident or non-conformity;

(c) the known or reasonably anticipated effect;

(d) the immediate controls applied;

(e) the affected dependencies and Federation Domains;

(f) the required corrective, continuity and lifecycle actions;

(g) the next reporting or review time.

112.4. Notification shall not, by itself, restrict, suspend or withdraw Trust Service Provider Status, Trust Service Status, Service Permission or Qualified Status.

112.5. The Trust Service Provider shall notify affected Actors and persons where the applicable Framework Instrument requires that notification.

SECTION 3: SUPERVISION AND PROVIDER LIFECYCLE

Article 113: Supervision and conformity cooperation

113.1. A Trust Service Provider shall cooperate with the competent Framework Body, Conformity Assessment Body, supervision function and reviewing function.

113.2. Cooperation shall include, within the assigned scope:

(a) provision of records and evidence;

(b) access to relevant systems, locations and personnel;

(c) support for testing, assessment and investigation;

(d) implementation and Verification of corrective actions;

(e) notification of material changes and incidents;

(f) support for Status Publication and lifecycle decisions.

113.3. Supervision or Conformity Assessment shall not transfer operational responsibility for a Trust Service to the supervising or assessing Actor.

113.4. A Trust Service Provider shall not obstruct, conceal or materially delay an authorised assessment, supervision action, Review or Remedy.

113.5. A supervision or assessment finding shall not, by itself, change Trust Service Provider Status unless a Framework Decision assigns that Controlled Effect.

Article 114: Restriction, suspension, withdrawal and reinstatement

114.1. A Framework Body shall restrict, suspend or withdraw Trust Service Provider Status only where the applicable evidence and lifecycle conditions support that Controlled Effect.

114.2. A lifecycle decision shall identify:

(a) the affected Trust Service Provider and Provider Scope;

(b) the evidence basis;

(c) the Effective Date;

(d) the affected Trust Services and dependencies;

(e) the required corrective, continuity and transition actions;

(f) the Humanitarian Trust List treatment;

(g) the Review Route.

114.3. Restriction, suspension or withdrawal of Trust Service Provider Status shall affect a Trust Service only where Trust Service Provider Status is a required dependency for that Trust Service and only within the affected Provider Scope.

114.4. Restriction, suspension or withdrawal of Trust Service Provider Status shall not automatically invalidate Trust Service Outputs or Trust Objects created before the Effective Date of that action.

114.5. A Framework Body shall reinstate Trust Service Provider Status only where the applicable corrective, assessment, evidence and decision conditions are satisfied.

114.6. Reinstatement of Trust Service Provider Status shall not, by itself, reinstate Trust Service Status, Service Permission or Qualified Trust Service Status.

Article 115: Cessation and transition

115.1. A Trust Service Provider ceasing one or more Trust Services shall implement the cessation and transition arrangements established by the applicable Framework Instruments.

115.2. Before cessation, the Trust Service Provider shall:

(a) notify the competent Framework Body and affected Participating Actors;

(b) protect and preserve required records and evidence;

(c) maintain required Status and Validation information;

(d) protect creation data, cryptographic material, personal data and Restricted Information;

(e) apply the approved transfer, replacement, migration or termination procedure;

(f) support the required Humanitarian Trust List and Register updates through the competent Framework Body;

(g) protect affected persons and Relying Actors from avoidable harm.

115.3. Cessation of a Trust Service Provider or Trust Service shall not automatically invalidate Trust Objects or Trust Service Outputs created before the Effective Date of cessation.

115.4. The applicable Profile shall define the effect of cessation on continuing Validation, Status Responses, preservation, transition and Controlled Reliance.

115.5. A Trust Service Provider shall retain continuing obligations after cessation where required for security, Confidentiality, evidence, Validation, Review, Remedy or historical reconstruction.

115.6. Transfer of records, systems, functions or operational responsibility shall not transfer Trust Service Provider Status, Qualified Trust Service Provider Status, Trust Service Status or Service Permission.

115.7. A successor Trust Service Provider or Trust Service shall obtain its own recognition, Status and Service Permission before operational use.

115.8. Completion of cessation shall be recorded and shall remain subject to the applicable Review Route.

PART IX: TRUST SERVICES

SECTION 1: GENERAL PROVISIONS

Article 116: Trust Service Categories

116.1. The Trust Service Categories recognised under the Framework are:

(a) Identification Service;

(b) Authentication Service;

(c) Authorisation Service;

(d) Digital Signing Service;

(e) Electronic Signature Service;

(f) Electronic Seal Service;

(g) Electronic Timestamp Service;

(h) Electronic Attestation Service;

(i) Validation and Verification Service;

(j) Federated Data Exchange Service.

116.2. Each Trust Service Category shall be defined according to its stable function and native Trust Service Outputs and not according to a sector, programme or use case.

116.3. A Scheme shall select the Trust Services required for its purpose without altering their classification.

116.4. A Profile shall select the conditions applicable to a Trust Service without creating a new Trust Service Category.

116.5. A new Trust Service Category shall require amendment of this Part and the corresponding definitions in Part II.

116.6. The Trust Service Catalogue shall record the Categories established by this Article and shall not create or remove a Category.

Article 117: Recognition, Service Scope and Service Permission

117.1. A Framework Body shall recognise each Trust Service separately.

117.2. A Trust Service-recognition decision shall identify:

(a) the Trust Service Provider;

(b) the Trust Service Category;

(c) the service identifier;

(d) the Service Scope;

(e) the native Trust Service Outputs;

(f) the applicable Schemes and Profiles;

(g) the material dependencies;

(h) the applicable Assurance Conditions;

(i) the Effective Date and Validity Period;

(j) the lifecycle conditions;

(k) the restrictions and caveats.

117.3. A Trust Service shall operate only where the applicable Framework Decision assigns Service Permission within the recognised Service Scope.

117.4. Recognition or technical availability shall not, by itself, assign Service Permission or operational activation.

117.5. Recognition or Service Permission assigned to one Trust Service shall not apply to another Trust Service provided by the same or another Trust Service Provider.

117.6. Trust Service recognition shall not, by itself, create access, disclosure permission, Technical Exchange Permission, Controlled Reliance or Qualified Status.

Article 118: Qualified Trust Service Status

118.1. Each Trust Service Category established by Article 116 shall be eligible for Qualified Trust Service Status.

118.2. A Trust Service shall have Qualified Trust Service Status only where:

(a) the Trust Service Provider has Qualified Trust Service Provider Status for the relevant Provider Scope;

(b) an applicable service-specific Qualified Profile is in force;

(c) the Trust Service satisfies the applicable functional, operational, security, continuity and Assurance Conditions;

(d) the required Conformity Assessment has been completed;

(e) each material non-conformity has been resolved;

(f) the evidence basis has been recorded;

(g) a Framework Body acting within its Decision Competence assigns that Status.

118.3. Qualified Trust Service Status shall apply only to the identified Trust Service and Qualified Scope.

118.4. Qualified Trust Service Status shall not transfer to the Trust Service Provider outside the Qualified Scope assigned to that Trust Service Provider, another Trust Service, a Trust Service Output, Trust Object, Source, mechanism, device or component.

118.5. Each Trust Service provided through a composite or shared implementation shall be assessed and qualified independently.

Article 119: Trust Service independence, dependencies and lifecycle

119.1. Each Trust Service shall retain its independent identity, Trust Service Status, Service Scope, native outputs, evidence, responsibility and lifecycle.

119.2. Use of a common Trust Service Provider, system, component, mechanism, device, Source or Technical Exchange Route shall not merge separate Trust Services.

119.3. A Trust Service dependency shall identify the dependent Trust Service, supporting Controlled Matter, dependency type, applicable condition and lifecycle effect.

119.4. Loss, restriction, suspension or withdrawal of the Trust Service Provider Status required for a Trust Service shall trigger restriction, suspension or review of the dependent Service Permission within the affected Provider Scope.

119.5. Paragraph 119.4 shall not transfer Trust Service Provider Status to the Trust Service or Trust Service Status to the Provider.

119.6. Restriction, suspension or withdrawal affecting one Trust Service shall affect another Trust Service only where an identified dependency or Framework Decision establishes that effect.

119.7. A Trust Service shall be subject to applicable restriction, suspension, withdrawal, cessation, transition and historical-treatment conditions.

119.8. Cessation of a Trust Service shall not automatically invalidate Trust Objects or Trust Service Outputs created before the Effective Date of cessation.

119.9. Where a Trust Service Output is issued as an Electronic Attestation, the Electronic Attestation shall constitute a separate Trust Object produced by an Electronic Attestation Service.

SECTION 2: IDENTIFICATION SERVICE

Article 120: Identification Service

120.1. An Identification Service shall establish, verify, maintain or resolve an identification basis concerning an identified Subject within an assigned Service Scope.

120.2. The Identification Service Functions shall include, where assigned:

(a) Identity Proofing;

(b) Identity Registration;

(c) person or organisation binding;

(d) Identifier assignment and management;

(e) Identity Resolution;

(f) duplicate detection;

(g) identity-record linking and separation;

(h) identity lifecycle management;

(i) reproofing, recovery and closure.

120.3. The native Trust Service Outputs of an Identification Service shall be Identification Results and Identity Resolution Results.

120.4. An Identification Service shall not issue an Electronic Attestation unless the same or another Trust Service Provider separately provides an Electronic Attestation Service for that issuance.

120.5. An Identification Result or Identity Resolution Result shall not, by itself, create Authorisation, eligibility, entitlement, a finding of fraud, access, disclosure permission or a local registration decision outside the assigned Service Scope.

120.6. The applicable Profile shall define the permitted evidence, Sources, identification functions, Assurance Conditions, output classes, human-review conditions, accessibility safeguards and lifecycle requirements.

SECTION 3: AUTHENTICATION SERVICE

Article 121: Authentication Service

121.1. An Authentication Service shall confirm an asserted identity, Role, origin, device, session, transaction, service, Trust Object or Controlled Interaction within an assigned Service Scope.

121.2. An Authentication Service shall use Authentication Mechanisms governed by the applicable Profile.

121.3. The native Trust Service Output of an Authentication Service shall be an Authentication Outcome.

121.4. An Authentication Outcome shall identify the asserted matter, Authentication Mechanism, context, result, Assurance information, time, Validity Period, restrictions and caveats.

121.5. A successful Authentication Outcome shall not, by itself, create Authorisation, access, disclosure permission, Controlled Reliance, eligibility, entitlement or Trust Service recognition.

121.6. The applicable Profile shall define the permitted Authentication Mechanisms, Assurance Conditions, risk controls, outcome classes, accessibility safeguards and lifecycle requirements.

SECTION 4: AUTHORISATION SERVICE

Article 122: Authorisation Service

122.1. An Authorisation Service shall determine whether an identified action, access, disclosure, exchange, service use or Controlled Interaction is permitted within an assigned Service Scope.

122.2. An Authorisation Service shall evaluate, where applicable:

(a) Authorisation Policies;

(b) Roles and Mandates;

(c) Attributes and Status information;

(d) purpose and context;

(e) Access Conditions;

(f) Disclosure Conditions;

(g) security and safeguard conditions;

(h) Reliance Conditions.

122.3. Responsibility for defining a policy shall remain with the Actor or Framework Body assigned that responsibility.

122.4. The Policy Decision Function shall evaluate the applicable policy and shall not alter that policy.

122.5. The native Trust Service Output of an Authorisation Service shall be an Authorisation Outcome.

122.6. An Authorisation Outcome shall not, by itself, execute or enforce the authorised action.

122.7. The Policy Enforcement Function shall apply the Authorisation Outcome to the requested action where the applicable Framework Instrument assigns that function.

SECTION 5: DIGITAL SIGNING SERVICE

Article 123: Digital Signing Service

123.1. A Digital Signing Service shall create Digital Signatures through controlled use of Digital Signature Creation Data and an identified Digital Signature Creation Mechanism or Device.

123.2. A Digital Signing Service shall support local or remote creation only within the assigned Service Scope and control model.

123.3. A Digital Signing Service shall ensure that creation data is protected, activated and used according to Part VI and the applicable Profile.

123.4. The native Trust Service Outputs of a Digital Signing Service shall be a Digital Signature and the creation evidence required for Validation.

123.5. A Digital Signature produced by a Digital Signing Service shall not, by itself, constitute an Electronic Signature or Electronic Seal.

123.6. Use of a Qualified Digital Signature Creation Device shall constitute a dependency condition and shall not, by itself, qualify the Digital Signing Service or Digital Signature.

123.7. The applicable Profile shall define the creation control model, permitted mechanisms and devices, evidence, remote-operation conditions, key lifecycle, compromise handling and Validation requirements.

SECTION 6: ELECTRONIC SIGNATURE SERVICE

Article 124: Electronic Signature Service

124.1. An Electronic Signature Service shall create or manage Electronic Signatures attributable to natural persons within an assigned Service Scope.

124.2. An Electronic Signature Service shall establish the association between the Signatory, signing act, signed data, applicable Digital Signature, creation mechanism or device and required evidence of intent or approval.

124.3. Where an Electronic Signature Service depends on a Digital Signing Service, each Trust Service shall retain its independent identity, Status, responsibility and evidence.

124.4. The native Trust Service Outputs of an Electronic Signature Service shall be an Electronic Signature and Signature Evidence.

124.5. The applicable Profile shall define the Signatory control model, signing intent, permitted creation arrangements, evidence, Validation and lifecycle requirements.

124.6. Framework recognition or qualification shall not, by itself, assign External Legal Effect to an Electronic Signature.

SECTION 7: ELECTRONIC SEAL SERVICE

Article 125: Electronic Seal Service

125.1. An Electronic Seal Service shall create or manage Electronic Seals attributable to legal entities within an assigned Service Scope.

125.2. An Electronic Seal Service shall establish the association between the Seal Creator, authorised sealing process, sealed data, applicable Digital Signature, creation mechanism or device and organisational-control evidence.

125.3. Where an Electronic Seal Service depends on a Digital Signing Service, each Trust Service shall retain its independent identity, Status, responsibility and evidence.

125.4. The native Trust Service Outputs of an Electronic Seal Service shall be an Electronic Seal and Seal Evidence.

125.5. The applicable Profile shall define the organisational control model, authorised sealing process, permitted creation arrangements, evidence, Validation and lifecycle requirements.

125.6. Framework recognition or qualification shall not, by itself, assign External Legal Effect to an Electronic Seal.

SECTION 8: ELECTRONIC TIMESTAMP SERVICE

Article 126: Electronic Timestamp Service

126.1. An Electronic Timestamp Service shall bind identified electronic data to an identified time within an assigned Service Scope.

126.2. An Electronic Timestamp Service shall use a time source and time-control process satisfying the applicable Profile.

126.3. The native Trust Service Output of an Electronic Timestamp Service shall be an Electronic Timestamp.

126.4. An Electronic Timestamp Service shall ensure that the time value, data reference, accuracy, uncertainty, protection and Validation evidence satisfy the applicable Profile.

126.5. The applicable Profile shall define the time-source, accuracy, protection, evidence, Validity Period, continuity and qualified-dependency requirements.

SECTION 9: ELECTRONIC ATTESTATION SERVICE

Article 127: Electronic Attestation Service

127.1. An Electronic Attestation Service shall create, issue and manage Electronic Attestations within an assigned Service Scope.

127.2. An Electronic Attestation Service shall operate independently of the sector, programme or use case to which an Attestation Statement relates.

127.3. The native Trust Service Output of an Electronic Attestation Service shall be an Electronic Attestation.

127.4. A Certificate shall be issued as a specialised Electronic Attestation under an applicable Profile for Certificates.

127.5. The applicable Profile shall determine whether an Electronic Attestation requires a Source, Authoritative Source, Qualified Authoritative Source, other evidence basis or no Source dependency.

127.6. An Electronic Attestation Service shall maintain the issuance, Status, Correction, replacement, suspension, withdrawal, revocation and preservation information required by the applicable Profile.

127.7. An Electronic Attestation Service shall not acquire responsibility for an underlying business, eligibility, entitlement, assessment or programme decision by reason only of issuing an Electronic Attestation representing that decision.

SECTION 10: VALIDATION AND VERIFICATION SERVICE

Article 128: Validation and Verification Service

128.1. A Validation and Verification Service shall verify identified properties, validate identified Controlled Matters or provide authorised Status information within an assigned Service Scope.

128.2. The native Trust Service Outputs of a Validation and Verification Service shall be Verification Results, Validation Results and Status Responses.

128.3. A Validation and Verification Service shall identify the evaluated matter, evaluation basis, applicable Profile and Version, evidence and Status information used, evaluation time, result, Validity Period, restrictions and caveats.

128.4. Where evaluation depends on governance Status, the Validation and Verification Service shall use Status information authorised or published by the responsible Framework Body, including the Humanitarian Trust List where applicable.

128.5. Operation of a Validation and Verification Service shall not transfer governance or publication responsibility for the Humanitarian Trust List to the Trust Service Provider.

128.6. A Verification Result, Validation Result or Status Response shall not create or alter the underlying Status, Source, Trust Object, Authorisation or Controlled Reliance.

SECTION 11: FEDERATED DATA EXCHANGE SERVICE

Article 129: Federated Data Exchange Service

129.1. A Federated Data Exchange Service shall provide controlled exchange of requests, responses, Trust Objects, Trust Service Outputs and Exchange Evidence between recognised Actors or Federation Domains within an assigned Service Scope.

129.2. A Federated Data Exchange Service shall provide, according to the applicable Profile:

(a) identification and Authentication of participating endpoints;

(b) route and destination resolution;

(c) Transport Confidentiality;

(d) Payload Confidentiality where required;

(e) Integrity and Authenticity protection;

(f) request and response correlation;

(g) replay and duplicate-message controls;

(h) exchange-status and error handling;

(i) Exchange Evidence;

(j) continuity and recovery controls.

129.3. The native Trust Service Outputs of a Federated Data Exchange Service shall be Exchange Evidence and Controlled Exchange Results.

129.4. A Federated Data Exchange Service shall use Humanitarian Trust List and federation-discovery information only as authorised by the responsible Framework Body.

129.5. A Federated Data Exchange Service shall not operate, control or assign Status through the Humanitarian Trust List.

129.6. A Federated Data Exchange Service shall not, by itself, create access, disclosure permission, acceptance of content, a business decision, Source Status, Trust Service Status or Controlled Reliance.

129.7. An Authorisation Service or local Policy Enforcement Function shall determine and enforce the applicable exchange permission where required.

PART X: ASSURANCE, CONFORMITY ASSESSMENT AND QUALIFICATION

SECTION 1: ASSURANCE

Article 130: General provisions on Assurance

130.1. Assurance, Conformity Assessment and Qualification shall constitute separate Framework Functions.

130.2. An Assurance outcome shall not, by itself, constitute a Conformity Assessment Result, qualification decision, Qualified Status, recognition, operational activation or permission for Controlled Reliance.

130.3. A Conformity Assessment Result shall not, by itself, assign Qualified Status.

130.4. Qualified Status shall arise only through the qualification route applicable to the identified category of Status-Bearing Matter.

Article 131: Assurance Objects and Assurance Domains

131.1. Assurance shall be assigned to an identified Assurance Object within an identified Assurance Domain.

131.2. An Assurance Object shall be a Controlled Matter identified by the applicable Profile.

131.3. An Assurance Domain shall identify the subject area within which confidence is evaluated.

131.4. Assurance assigned in one Assurance Domain shall not automatically apply in another Assurance Domain.

131.5. Assurance assigned to one Assurance Object shall not transfer to another Assurance Object.

131.6. The applicable Profile shall identify the Assurance Object, Assurance Domain, Assurance Conditions, evidence basis and evaluation method.

Article 132: Assurance Levels

132.1. The Framework shall recognise:

(a) Low Assurance Level;

(b) Substantial Assurance Level;

(c) High Assurance Level.

132.2. The applicable Profile shall define the requirements for each Assurance Level within the relevant Assurance Domain.

132.3. Assignment of the same Assurance Level in different Assurance Domains shall not establish equivalence between those Domains.

132.4. A High Assurance Level shall not, by itself, create Qualified Status.

Article 133: Assurance Conditions and evidence

133.1. An Assurance outcome shall be based on evidence appropriate to the Assurance Object, Assurance Domain and recognised purpose.

133.2. Assurance evidence shall be:

(a) relevant to the Assurance Condition being evaluated;

(b) attributable to an identified Actor, Source, process or system;

(c) sufficiently current for the evaluation purpose;

(d) protected against unauthorised alteration;

(e) traceable to the applicable evaluation;

(f) retained according to the applicable lifecycle conditions.

133.3. The applicable Profile shall define the required evidence, permitted evidence sources, evaluation method, Freshness Conditions, conflict treatment, human-review conditions and Assurance outcome classes.

133.4. An Assurance outcome shall identify each material limitation, caveat and dependency affecting that outcome.

Article 134: Assurance dependencies and composite evaluations

134.1. Where an Assurance outcome depends on another Controlled Matter, the dependency shall be identified and evaluated.

134.2. A composite Assurance evaluation shall identify:

(a) each constituent Assurance Object;

(b) each applicable Assurance Domain;

(c) each dependency;

(d) the combination rule;

(e) the effect of an unavailable, suspended or non-conforming dependency;

(f) the resulting Assurance outcome.

134.3. A composite Assurance Level shall be determined according to the applicable Profile and shall not be inferred solely from the highest or lowest constituent Assurance Level.

134.4. A qualified dependency shall constitute a condition and shall not transfer Qualified Status to the dependent Assurance Object.

134.5. A material change affecting a dependency shall trigger reassessment where required by the applicable Profile.

SECTION 2: CONFORMITY ASSESSMENT

Article 135: Conformity Assessment

135.1. Conformity Assessment shall determine whether an identified assessment subject satisfies the requirements assigned by the Framework and applicable Framework Instruments.

135.2. A Conformity Assessment shall identify the assessment subject, assessed scope, applicable requirements and Versions, evidence examined, assessment methods, findings, limitations, assessment date and period of applicability.

135.3. Conformity Assessment shall remain separate from recognition, qualification, supervision and operational execution.

135.4. Technical testing alone shall not constitute a complete Conformity Assessment where organisational, governance, lifecycle, security or safeguard requirements also apply.

Article 136: Competence and independence of Conformity Assessment Bodies

136.1. An Actor shall perform Conformity Assessment only where recognised as a Conformity Assessment Body for the relevant scope.

136.2. A Conformity Assessment Body shall possess the competence, resources, methods and independence required by the applicable Framework Instrument.

136.3. A Conformity Assessment Body shall identify and manage conflicts of interest.

136.4. An Actor shall not assess a matter for which its operational responsibility impairs the independence of the assessment.

136.5. Use of a subcontractor shall not remove the responsibility of the recognised Conformity Assessment Body.

Article 137: Scope and conduct of Conformity Assessment

137.1. A Conformity Assessment shall be conducted against the requirements and Versions applicable to the identified assessment subject.

137.2. The assessment scope shall identify, where applicable:

(a) the Provider Scope;

(b) the Service Scope;

(c) the Trust Object Category;

(d) the Source Scope;

(e) the mechanism or device;

(f) the operational locations;

(g) the systems and components;

(h) the material dependencies;

(i) the applicable Schemes, Profiles and Technical Specifications.

137.3. The assessment shall include sufficient examination, testing, observation and evidence review to support the findings.

137.4. A limitation preventing a complete assessment shall be recorded and reflected in the Conformity Assessment Result.

137.5. A Conformity Assessment shall not extend beyond the assessed scope.

Article 138: Conformity Assessment Results

138.1. A Conformity Assessment shall produce a Conformity Assessment Result.

138.2. A Conformity Assessment Result shall identify:

(a) the assessment subject;

(b) the assessed scope;

(c) the applicable requirements and Versions;

(d) the assessment methods;

(e) the evidence basis;

(f) each finding and non-conformity;

(g) each limitation and caveat;

(h) the assessment conclusion;

(i) the issue date and period of applicability;

(j) the responsible Conformity Assessment Body.

138.3. A positive Conformity Assessment Result shall not, by itself, assign recognition, Service Permission, operational activation or Qualified Status.

138.4. A Conformity Assessment Result shall be protected and retained according to the applicable Framework Instrument.

Article 139: Surveillance and reassessment

139.1. An assessment subject shall be subject to surveillance or reassessment where required by the Framework, the applicable Profile or the qualification decision.

139.2. Reassessment shall occur where a material change affects the assessed scope, applicable requirements, organisational arrangements, Trust Service, Trust Object, Source, mechanism, device, dependency, security, continuity or safeguard conditions.

139.3. Surveillance shall be proportionate to the assessed subject, Assurance Conditions, risk and Qualified Status.

139.4. A surveillance finding capable of affecting recognition, qualification, restriction, suspension or withdrawal shall be communicated to the responsible Framework Body.

Article 140: Non-conformity

140.1. A non-conformity shall identify a failure to satisfy an applicable requirement.

140.2. A material non-conformity shall prevent a positive assessment conclusion where the failed requirement is necessary for the assigned Status or Qualified Scope.

140.3. A non-conformity record shall identify the affected subject and scope, failed requirement, evidence basis, actual or potential effect, required corrective action, correction period, Verification condition and closure condition.

140.4. Failure to correct a material non-conformity shall trigger the applicable restriction, suspension, withdrawal or reassessment procedure.

SECTION 3: QUALIFIED PROFILES AND QUALIFICATION ROUTES

Article 141: Qualified Profiles

141.1. Qualified Status shall be assigned or established only under an applicable Qualified Profile.

141.2. A Qualified Profile shall identify:

(a) the eligible status-bearing category;

(b) the Qualified Scope;

(c) the applicable Assurance Domains and Assurance Levels;

(d) the functional and operational requirements;

(e) the security and continuity requirements;

(f) the required dependencies;

(g) the applicable qualification route;

(h) the Conformity Assessment or object-Validation requirements;

(i) the surveillance and reassessment requirements;

(j) the lifecycle, restriction, suspension and withdrawal conditions;

(k) the evidence and publication requirements.

141.3. A Qualified Profile shall not, by itself, assign Qualified Status.

141.4. A Qualified Profile applicable to one status-bearing category shall not qualify another category.

Article 142: Decision-based qualification

142.1. Decision-based qualification shall apply to:

(a) Trust Service Providers;

(b) Trust Services;

(c) Authoritative Sources;

(d) creation mechanisms and devices;

(e) another governance Status expressly assigned to that route by the Framework.

142.2. A Framework Body shall assign Qualified Status through decision-based qualification only where:

(a) an applicable Qualified Profile is in force;

(b) the required Conformity Assessment has been completed;

(c) each material non-conformity has been resolved;

(d) the evidence basis has been recorded;

(e) the Qualified Scope has been identified.

142.3. A qualification decision shall identify the qualified Status-Bearing Matter, Qualified Profile and Version, Conformity Assessment Result, Qualified Scope, Effective Date, Validity Period or review date, restrictions, surveillance requirements, lifecycle conditions and Review Route.

142.4. A qualification decision shall not extend beyond the assessed and approved scope.

142.5. Qualified Status under the Framework shall not, by itself, create External Legal Status or External Legal Effect.

Article 143: Qualified Trust Service Provider Status

143.1. Qualified Trust Service Provider Status shall apply only to the identified Trust Service Provider and the Qualified Scope assigned to that Trust Service Provider.

143.2. Qualified Trust Service Provider Status shall be assessed and decided independently from the Qualified Status of each Trust Service provided by that Provider.

143.3. Qualified Trust Service Provider Status shall not transfer to a Trust Service, Trust Service Output, Trust Object, Source, mechanism, device, subcontractor or dependency.

143.4. A material change affecting the Qualified Scope assigned to the Trust Service Provider shall be assessed before Qualified Status continues to apply to that change.

Article 144: Qualified Trust Service Status

144.1. Qualified Trust Service Status shall apply only to the identified Trust Service and the Qualified Scope assigned to that Trust Service.

144.2. Each Trust Service shall be assessed and qualified independently.

144.3. Qualified Trust Service Status shall not transfer to the Trust Service Provider outside the Qualified Scope assigned to that Trust Service Provider, another Trust Service, a Trust Service Output, Trust Object, Source, mechanism or device.

144.4. Where a qualified Trust Service depends on another Controlled Matter, the applicable Qualified Profile shall identify the required Status of that dependency.

144.5. Qualified Status of a dependency shall not qualify the dependent Trust Service.

Article 145: Object-instance qualification

145.1. Object-instance qualification shall apply to individual Trust Objects and Trust Service Outputs eligible for Qualified Status under Part VI.

145.2. An individual Trust Object or eligible Trust Service Output shall have Qualified Status only where:

(a) it satisfies the applicable Qualified Object Profile;

(b) it is created or issued through the Trust Service Status required by that Profile;

(c) each required qualified dependency is valid within its assigned scope;

(d) it contains or references the required creation, issuance and lifecycle evidence;

(e) Validation confirms satisfaction of the applicable qualified conditions.

145.3. Object-instance qualification shall not require an individual Framework Decision unless the Framework expressly assigns such a decision.

145.4. Qualified Status of an individual object or output shall be evidenced through the object or output, applicable Profile, issuing-service Status, dependency Status, Validation Result and authorised Status information.

145.5. Qualified Status shall apply only to the identified object or output and shall not transfer to its Issuer, Subject, Trust Service Provider, Trust Service, Source Basis, protection object or dependency.

145.6. Each Trust Object Category established by Part VI shall be eligible for object-instance qualification where a Qualified Object Profile defines meaningful qualified conditions for that Category.

Article 146: Qualified Authoritative Source Status

146.1. Qualified Authoritative Source Status shall apply only to the identified Authoritative Source and the Qualified Scope assigned to that Authoritative Source.

146.2. Qualified Authoritative Source Status shall remain separate from the Qualified Status of the Source Holder, Source Steward, Trust Service or Trust Object using that Source.

146.3. A copy, extract, replica, transformation, aggregation or derivative shall require a separate qualification decision where Qualified Status is sought.

146.4. A material change affecting the Source Scope, provenance, quality, semantics or lifecycle shall be assessed before Qualified Status continues to apply to that change.

Article 147: Qualified creation mechanisms and devices

147.1. A creation mechanism or device shall have Qualified Status only where:

(a) the category is eligible for qualification;

(b) an applicable Qualified Profile is in force;

(c) the required Conformity Assessment has been completed;

(d) the mechanism or device is uniquely identified;

(e) the qualified configuration and scope are recorded;

(f) a Framework Body assigns Qualified Status.

147.2. A qualification decision for a mechanism or device shall identify the responsible Provider, model and unique identifier, hardware, software and firmware Versions, approved configuration, assigned function, qualified operational environment, evidence basis, Effective Date and lifecycle conditions.

147.3. Qualified Status assigned to a mechanism or device shall not transfer to another instance or configuration, the Trust Service using it, the Trust Service Provider, or a Trust Object or Trust Service Output produced through it.

147.4. A material change to a qualified mechanism or device shall be assessed before Qualified Status continues to apply.

Article 148: Publication and lifecycle of Qualified Status

148.1. A Framework Body shall publish authorised decision-based Qualified Status information through the Humanitarian Trust List or another governance-controlled publication mechanism.

148.2. Publication shall communicate the qualification decision and shall not create Qualified Status.

148.3. Individual Trust Objects shall not ordinarily receive Humanitarian Trust List Entries.

148.4. Qualified Status of an individual Trust Object shall be determined through Validation and the applicable authorised Status Response where lifecycle Status is required.

148.5. Published decision-based Qualified Status information shall identify the qualified Status-Bearing Matter, Qualified Scope, applicable Qualified Profile and Version, Effective Date, Validity Period or review date, restrictions and decision reference.

148.6. A Framework Body shall restrict, suspend or withdraw decision-based Qualified Status where the applicable qualified conditions are no longer satisfied.

148.7. Restriction, suspension or withdrawal shall apply only to the affected Qualified Scope unless an identified dependency requires a broader effect.

148.8. Historical Qualified Status information shall remain available where required for Validation, Review, Remedy and Controlled Reliance.

PART XI: SECURITY, INCIDENT RESPONSE AND CONTINUITY

SECTION 1: SECURITY GOVERNANCE AND CONTROLS

Article 149: Scope and application

149.1. This Part establishes the security, incident-response, continuity and Recovery requirements applicable to Controlled Matters and Controlled Interactions under the Framework.

149.2. Each Responsible Actor shall apply this Part within its assigned Role, Mandate, Provider Scope, Service Scope, Source Scope, Federation Domain or other recognised scope.

149.3. The applicable Implementation Guideline, Profile and Technical Specification shall assign the detailed controls, parameters, evidence and testing requirements necessary to satisfy this Part.

149.4. Compliance with this Part shall not, by itself, assign recognition, Status, Service Permission, Technical Exchange Permission, Authorisation, Controlled Reliance or Qualified Status.

Article 150: Security governance and risk management

150.1. A Responsible Actor shall establish and maintain security governance proportionate to the Controlled Matters, risks, Assurance Conditions and humanitarian consequences within its assigned scope.

150.2. Security governance shall identify:

(a) the Controlled Matters and dependencies protected;

(b) the responsible Roles and decision routes;

(c) the applicable Security Conditions and Protected-Person Safeguards;

(d) the risk-assessment, treatment and acceptance arrangements;

(e) the monitoring, testing and evidence requirements;

(f) the incident, continuity and Recovery arrangements;

(g) the review and Change Control arrangements.

150.3. A material security risk affecting a mandatory dependency shall be addressed before that dependency supports a positive Assurance, Verification, Validation, qualification or Controlled Reliance outcome.

150.4. Residual risk shall be accepted only by the Actor or Framework Body holding the applicable Decision Competence.

150.5. A residual-risk decision shall identify the affected scope, evidence basis, controls, duration, review date and continuing obligations.

150.6. Shared infrastructure, outsourcing or federation shall not transfer security responsibility from the Responsible Actor to another Actor unless the Framework expressly assigns that responsibility.

Article 151: Confidentiality

151.1. A Responsible Actor shall protect Confidentiality throughout collection, creation, issuance, transmission, receipt, processing, storage, disclosure, retention, archival and Deletion.

151.2. Confidentiality controls shall distinguish:

(a) Transport Confidentiality;

(b) Payload Confidentiality;

(c) storage confidentiality;

(d) processing confidentiality;

(e) disclosure control.

151.3. Access to Restricted Information, Protection-Sensitive Information and Security-Sensitive Information shall be limited to authorised Actors and the minimum information necessary for the assigned purpose.

151.4. Storage or processing outside the direct control of the originating or receiving Actor shall remain subject to the applicable Confidentiality, access, evidence and deletion controls.

151.5. Logs, monitoring records, error information and operational evidence shall not contain plaintext payload content or other Restricted Information beyond what is necessary and authorised for their assigned purpose.

151.6. Confidentiality protection shall not replace Integrity, Authenticity, Authorisation, Status, Validation or Controlled Reliance requirements.

151.7. Encryption or technical inaccessibility shall not, by itself, authorise collection, processing, exchange, disclosure or retention.

Article 152: Payload Confidentiality and controlled exchange

152.1. Where Payload Confidentiality is required, the payload shall be protected before it enters the Technical Exchange Route.

152.2. Plaintext access shall be limited to the authorised originating Actor, the authorised receiving Actor and each additional processing Actor expressly identified by the applicable Profile and Authorisation Outcome.

152.3. A Technical Exchange Route Operator, Intermediary or Federated Data Exchange Service Provider shall not access the plaintext payload unless that Actor is separately authorised as a processing Actor for the assigned purpose.

152.4. Decryption material shall not be made available to a Technical Exchange Route Operator, Intermediary or unrelated component unless the applicable Profile expressly assigns that Actor a processing function and the required safeguards apply.

152.5. Discovery Metadata, routing Metadata and exchange evidence shall be limited to the information necessary for routing, security, accountability and error handling.

152.6. Transport Confidentiality shall not replace Payload Confidentiality where Payload Confidentiality is required.

152.7. Payload Confidentiality shall not replace the object-level protection required for a Trust Object or Trust Service Output.

Article 153: Integrity, Authenticity and Accountability

153.1. A Responsible Actor shall protect a Controlled Matter against unauthorised alteration, substitution, deletion, corruption, replay and incorrect lifecycle transition.

153.2. A statement-bearing Trust Object or Trust Service Output exchanged across an organisational or Federation Boundary shall be protected by the Electronic Signature, Electronic Seal or other object-level protection required by Part VI and the applicable Profile.

153.3. Transport protection shall not replace the Electronic Signature, Electronic Seal, Electronic Timestamp, Certificate or other object-level evidence required for independent Verification or Validation.

153.4. 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.

153.5. Evidence supporting Integrity, Authenticity or Accountability shall be protected against unauthorised alteration and retained for the period assigned by the applicable Framework Instrument.

153.6. A Controlled Interaction shall include replay, duplication and correlation controls where the applicable Profile identifies those risks.

Article 154: Access control and protected functions

154.1. Access to a Controlled Matter, Trust Service, Source, Endpoint, creation mechanism, device or administrative function shall be limited to authorised Actors and the minimum scope necessary for the assigned purpose.

154.2. A Responsible Actor shall apply, where applicable:

(a) Identification and Authentication;

(b) Authorisation;

(c) least-privilege access;

(d) separation of duties;

(e) privileged-access control;

(f) periodic access review;

(g) prompt restriction or removal of access;

(h) auditable access records.

154.3. Privileged access shall be separately authorised, monitored and reviewed.

154.4. Emergency access shall be limited to the emergency scope, recorded, reviewed and terminated when the emergency condition ends.

154.5. A successful Authentication Outcome shall not, by itself, create Authorisation or access to another Controlled Matter.

154.6. Operation or support of a protected function shall not assign the Role, Status or Decision Competence of the Actor responsible for that function.

Article 155: Creation data, Validation Data and cryptographic material

155.1. Digital Signature Creation Data, Digital Signature Validation Data, encryption keys, Authentication secrets and other Security-Sensitive Information used for cryptographic protection shall be governed throughout their lifecycle.

155.2. Lifecycle controls shall address, where applicable:

(a) generation;

(b) activation;

(c) storage;

(d) use;

(e) backup and Recovery;

(f) rotation and replacement;

(g) restriction, Suspension and Revocation;

(h) secure destruction.

155.3. Digital Signature Creation Data shall be used only through the authorised Digital Signing Service and the assigned Digital Signature Creation Mechanism or Device.

155.4. A remote or shared creation arrangement shall preserve the control, activation and evidence requirements assigned by the applicable Profile to the Signatory, Seal Creator or other authorised Actor.

155.5. Digital Signature Validation Data shall remain linked to the applicable Certificate, Status, algorithm, parameter, Version and lifecycle information required for Validation.

155.6. Compromise or suspected compromise of creation data, cryptographic material, an Authenticator, creation mechanism or device shall be treated as a Security Incident.

155.7. Detailed cryptographic controls shall be established through the applicable Implementation Guideline, Profile and Technical Specification.

Article 156: Protection-Sensitive and Security-Sensitive Information

156.1. A Responsible Actor shall identify information whose access, use, combination, alteration, loss or disclosure is capable of creating a protection or security risk.

156.2. Protection-Sensitive Information and Security-Sensitive Information shall be subject to assigned controls concerning:

(a) access;

(b) disclosure;

(c) onward transfer;

(d) aggregation;

(e) logging;

(f) retention;

(g) Deletion;

(h) incident response.

156.3. Public or federation-wide publication shall not disclose Protection-Sensitive Information or Security-Sensitive Information unless an applicable Framework Instrument expressly authorises that disclosure.

156.4. A Humanitarian Trust List Entry, Register Entry or Catalogue Entry shall contain only the information authorised for its publication or access class.

156.5. A Responsible Actor shall assess the risk created by combining information that is not individually sensitive where the combination can create a protection or security risk.

156.6. Retention shall remain limited to the assigned purpose and period, subject to continuing evidence, Review and Remedy requirements.

SECTION 2: MONITORING AND INCIDENT RESPONSE

Article 157: Security monitoring and vulnerability management

157.1. A Responsible Actor shall monitor systems, Trust Services, Sources, mechanisms, devices, Technical Exchange Routes and material dependencies for security events, weaknesses and vulnerabilities.

157.2. Vulnerability management shall include:

(a) identification;

(b) assessment;

(c) prioritisation;

(d) remediation or mitigation;

(e) verification;

(f) notification and disclosure where required;

(g) closure.

157.3. A material vulnerability shall be assessed for its effect on:

(a) Trust Service Provider Status;

(b) Trust Service Status and Service Permission;

(c) Trust Object Status and Validation;

(d) Source Status;

(e) a creation mechanism or device;

(f) Assurance and Qualified Status;

(g) dependent Actors and Federation Domains.

157.4. A Responsible Actor shall apply an urgent control where continued operation creates an unacceptable risk.

157.5. Vulnerability information shall be restricted where premature or unnecessary disclosure would increase the risk.

157.6. Closure of a vulnerability shall require evidence that the assigned remediation or mitigation is effective within the affected scope.

Article 158: Security Incident detection, recording and notification

158.1. A Responsible Actor shall detect, assess, record and respond to a Security Incident without undue delay.

158.2. A Security Incident record shall identify:

(a) the affected Controlled Matters;

(b) the known time, duration and scope;

(c) the known or suspected cause;

(d) the affected Actors, persons, dependencies and Federation Domains;

(e) the actual or potential effect on Confidentiality, Integrity, Availability, Authenticity, Assurance, Status, Qualified Status or Controlled Effects;

(f) the containment, continuity, notification and Recovery actions taken.

158.3. The Responsible Actor shall notify the competent Framework Body and each other Actor required by the applicable Profile, Scheme or Federation Agreement.

158.4. Notification shall be proportionate to the Security Incident and shall not disclose Restricted Information beyond what the recipient requires to act.

158.5. Where a Security Incident is capable of producing an Adverse Protected-Person Effect, the Responsible Actor shall provide accessible information and the applicable protection, Correction, Review and Remedy Routes.

158.6. Inability to determine the full scope of a Security Incident shall not delay urgent containment or protective action.

158.7. Notification shall not, by itself, assign restriction, Suspension, Withdrawal, Revocation or another lifecycle Status.

Article 159: Containment and dependency evaluation

159.1. A Responsible Actor shall contain a Security Incident within the affected scope and shall avoid unnecessary effects on unrelated Controlled Matters.

159.2. Containment actions shall remain proportionate to the known risk and shall preserve the evidence required for investigation, Validation, Review and Remedy.

159.3. The incident evaluation shall identify:

(a) the originating cause;

(b) the affected systems, Trust Services, Trust Objects, Trust Service Outputs, Sources, mechanisms, devices and records;

(c) the period of exposure;

(d) each affected dependency;

(e) each affected Federation Domain;

(f) the required lifecycle actions.

159.4. A material Security Incident affecting a mandatory dependency shall prevent a new positive Assurance, Verification, Validation, qualification or Controlled Reliance outcome where that dependency cannot be established as valid and current.

159.5. A Security Incident shall not automatically invalidate an earlier Trust Object, Trust Service Output, decision or Controlled Reliance unless the applicable dependency, effective time or Framework Decision assigns that effect.

159.6. Cross-domain containment shall preserve the separate Decision Competence and authoritative records of each affected Federation Domain.

159.7. Each containment and propagation decision shall preserve the Historical State required for later evaluation.

Article 160: Effect on Status, Assurance and Qualified Status

160.1. A Framework Body shall restrict, suspend, withdraw, revoke or reinstate Status only within its assigned Decision Competence and on a supported evidence basis.

160.2. A Security Incident affecting a Trust Service Provider shall not automatically affect each Trust Service provided by that Provider.

160.3. A Security Incident affecting a Trust Service shall not automatically invalidate each Trust Service Output or Trust Object produced through that Service.

160.4. A Security Incident affecting a Source, mechanism or device shall affect another Controlled Matter only through an identified dependency or Framework Decision.

160.5. A Security Incident affecting a qualified Status-Bearing Matter shall trigger evaluation of the exact Qualified Scope and each qualified condition affected.

160.6. Where a qualified condition is no longer satisfied, the competent Framework Body or applicable object-instance qualification process shall apply the required restriction, Suspension, Withdrawal, Revocation or loss of Qualified Status.

160.7. The responsible Framework Body shall publish each authorised Status change through the Humanitarian Trust List or another applicable governance-controlled publication mechanism.

160.8. A Trust Service Provider, technical operator or publication-support Actor shall not assign or alter Status by reason only of supporting notification, Validation or publication.

SECTION 3: CONTINUITY AND RECOVERY

Article 161: Continuity arrangements

161.1. A Responsible Actor shall maintain Continuity arrangements proportionate to the assigned function, risks, Assurance Conditions and humanitarian consequences of disruption.

161.2. Continuity arrangements shall address:

(a) alternative personnel, facilities, systems and communication routes;

(b) backup, restoration and Recovery of Controlled Records and evidence;

(c) continuation or orderly Suspension of critical functions and Trust Services;

(d) Status Publication and notification during disruption;

(e) dependencies on other Actors, Sources, Trust Services and Federation Domains;

(f) Accessible Alternatives for Affected Persons and Protected Persons;

(g) transition and cessation arrangements.

161.3. A continuity arrangement shall preserve category separation, Decision Competence, Confidentiality, Integrity and Protected-Person Safeguards.

161.4. A continuity arrangement shall not activate an unrecognised Trust Service, Source, Technical Exchange Route, mechanism or device.

161.5. A shared continuity dependency shall be assessed for its effect on each dependent Controlled Matter separately.

161.6. A Responsible Actor shall test and review Continuity arrangements at intervals proportionate to the assigned risks and Assurance Conditions.

Article 162: Degraded Operation

162.1. Degraded Operation shall occur only where the applicable Profile and authorised continuity decision permit continued operation under restricted conditions.

162.2. A decision to enter Degraded Operation shall identify:

(a) the affected function, Trust Service or Controlled Matter;

(b) the reason;

(c) the restricted scope;

(d) the temporary controls;

(e) the permitted outputs and Controlled Interactions;

(f) the Assurance and Status effects;

(g) the start time, review interval and exit condition.

162.3. Degraded Operation shall not conceal an unavailable, stale, invalid, suspended or indeterminate mandatory dependency.

162.4. A High Assurance or qualified outcome shall not be produced where a mandatory condition for that outcome is not satisfied.

162.5. A Trust Service Output produced during Degraded Operation shall identify the applicable limitation or caveat where required by the Profile.

162.6. Degraded Operation shall end when its authorised period expires or its conditions are no longer satisfied.

Article 163: Recovery, Reinstatement and closure

163.1. Recovery shall restore the security, operation, evidence, Status and lifecycle conditions required for the affected function or Controlled Matter.

163.2. Before normal operation resumes, the Responsible Actor shall establish:

(a) containment of the cause;

(b) Correction of the failed control or an authorised compensating control;

(c) Integrity and currentness of affected systems, records, Status and dependencies;

(d) security of creation data and cryptographic material;

(e) completion of required testing, Validation, reassessment or Conformity Assessment;

(f) the effect on earlier outputs and Controlled Reliance;

(g) the monitoring required after Recovery.

163.3. Reinstatement of Status shall require the decision or process applicable to the matter whose Status was restricted, suspended, withdrawn or revoked.

163.4. Restoration of technical operation shall remain separate from Reinstatement of Status, Service Permission or Qualified Status.

163.5. A Security Incident shall be closed only where the Recovery evidence is complete, required corrective actions are verified, residual risks are accepted within assigned Decision Competence and affected Actors and persons have received required information.

163.6. Incident closure shall not remove continuing monitoring, Review, Remedy, Retention or historical-reconstruction obligations.

PART XII: REVIEW, CORRECTION AND REMEDY

SECTION 1: GENERAL PROVISIONS AND ACCESS

Article 164: Scope and general requirements

164.1. This Part establishes the Complaint, Correction, Review, Interim Measure and Remedy requirements applicable under the Framework.

164.2. An Actor or Affected Person affected by a Framework Decision, Status, Trust Service, Trust Service Output, Trust Object, Source record, Status Publication, Controlled Interaction or Controlled Reliance shall have access to the applicable route established by the Framework.

164.3. Complaint, Correction, Review and Remedy shall remain separate functions and shall not be treated as interchangeable.

164.4. Submission of a Complaint, Correction request or Review request shall not, by itself, suspend or invalidate the affected Controlled Matter or Controlled Effect.

164.5. A Responsible Actor or Framework Body shall apply an Interim Measure where continued operation or reliance creates a material risk that cannot await final determination.

164.6. Review and Remedy shall preserve the Decision Competence and responsibility of each affected Actor and Framework Body.

Article 165: Accessible routes and Protected-Person Safeguards

165.1. Complaint, Correction, Review and Remedy Routes shall be accessible, understandable, timely and proportionate to the affected matter.

165.2. An Affected Person shall not be required to identify the technical component, Trust Service, Trust Service Provider or responsible Federation Domain before submitting a request.

165.3. Appropriate assistance, representation and Accessible Alternatives shall be available where the primary digital route creates an unjustified barrier.

165.4. Failure or inability to satisfy an Identifier, document, biometric, Authentication, device or connectivity requirement shall not prevent access to a Complaint, Correction, Review or Remedy Route.

165.5. A final decision capable of producing a significant Adverse Protected-Person Effect shall be subject to review by a natural person where required by the applicable Scheme or Profile.

165.6. Use of a Complaint, Correction, Review or Remedy Route shall not create retaliation, unjustified exclusion or loss of an unrelated service.

165.7. A Representative shall act only within an assigned Mandate Scope, and the affected person shall receive information directly where appropriate and safe.

165.8. Protection-Sensitive Information and Security-Sensitive Information used in a remedial process shall remain subject to the applicable access and Disclosure Conditions.

SECTION 2: COMPLAINTS AND CORRECTION

Article 166: Complaints and intake

166.1. Each Responsible Actor and Framework Body shall provide a Complaint Route for matters within its assigned responsibility or Decision Competence.

166.2. A Complaint shall be acknowledged and recorded within the period assigned by the applicable Framework Instrument.

166.3. A Complaint record shall identify:

(a) the complainant or authorised Representative;

(b) the affected matter;

(c) the alleged error, breach, adverse effect or failure;

(d) the requested outcome;

(e) the evidence supplied;

(f) the responsible Actor or Framework Body;

(g) the applicable time limits and current state.

166.4. A recipient lacking responsibility or Decision Competence shall refer the Complaint to the competent Actor or Framework Body without requiring the complainant to restart the process.

166.5. One accessible entry route shall be available where resolution requires action by more than one Actor, Trust Service Provider or Federation Domain.

166.6. The Responsible Actor shall communicate material progress, delay and the final outcome in an accessible form.

166.7. A Complaint outcome shall identify the findings, reasons, assigned actions, implementation responsibility and further Review or Remedy Route.

Article 167: Correction of records and Source information

167.1. A Responsible Actor shall correct an inaccurate, incomplete, inconsistent, improperly attributed or unlawfully maintained record within its assigned responsibility.

167.2. A Correction record shall identify:

(a) the affected record or information;

(b) the error, omission or inconsistency;

(c) the evidence basis;

(d) the corrected information;

(e) the Effective Date;

(f) the responsible Actor;

(g) the effect on dependent Controlled Matters.

167.3. Correction of Source information shall be governed by Part VII and the applicable Source Profile.

167.4. Correction shall preserve the Historical State required for accountability, Validation, Review and Remedy.

167.5. Corrected information shall not be represented as having existed in the corrected form before the Effective Date of the Correction.

167.6. A material Correction shall trigger evaluation of affected Trust Service Outputs, Trust Objects, decisions, publications and Controlled Reliance where an identified dependency exists.

Article 168: Correction of Trust Objects and Trust Service Outputs

168.1. A signed, sealed, timestamped or otherwise integrity-protected Trust Object or Trust Service Output shall not be altered after creation or issuance.

168.2. An error affecting such a matter shall be addressed through one or more of the following actions:

(a) Replacement;

(b) supersession;

(c) restriction;

(d) Suspension;

(e) Withdrawal;

(f) Revocation;

(g) issuance of a corrective Trust Object or Trust Service Output;

(h) publication of an applicable Status or caveat.

168.3. A corrective Trust Object or Trust Service Output shall identify the affected earlier matter and the relationship between them.

168.4. Correction of a Trust Object or Trust Service Output shall not, by itself, correct the underlying Source, decision or local record.

168.5. Correction of the underlying Source, decision or local record shall not alter an existing Trust Object or Trust Service Output.

168.6. The responsible Issuer or Trust Service Provider shall notify affected Relying Actors where the Correction can materially affect Validation or Controlled Reliance and the applicable Profile requires notification.

Article 169: Correction of Status Publication, Registers and Catalogues

169.1. The responsible Framework Body shall correct inaccurate or incomplete Status information published through the Humanitarian Trust List or another governance-controlled publication mechanism.

169.2. A change to Discovery Metadata shall remain separate from a change to Status, scope or Decision Competence.

169.3. A correction to a Humanitarian Trust List Entry shall identify:

(a) the affected Entry;

(b) the inaccurate or incomplete information;

(c) the corrected information;

(d) the supporting Framework Decision or evidence reference;

(e) the Effective Date;

(f) the treatment of historical publication.

169.4. A technical operator or publication-support Actor shall not assign, alter or remove Status without an authorised Framework Decision.

169.5. The responsible Framework Body shall correct an inaccurate Register Entry or Catalogue Entry and shall preserve the distinction between record correction and assignment of a new Controlled Effect.

169.6. Historical Status, Version and publication information shall remain reconstructable after Correction.

SECTION 3: REVIEW AND INTERIM MEASURES

Article 170: Review of Framework Decisions

170.1. A Framework Decision shall be subject to the Review Route assigned by the Framework or applicable Framework Instrument.

170.2. Review shall examine:

(a) Decision Competence;

(b) the applicable requirements and Versions;

(c) evidence and procedure;

(d) the assigned scope;

(e) the Controlled Effect;

(f) restrictions and caveats;

(g) proportionality;

(h) Protected-Person Safeguards;

(i) consistency with the Framework.

170.3. The reviewing function shall be sufficiently independent from the original decision-making function.

170.4. The reviewing function shall not exercise Decision Competence beyond the scope assigned to it.

170.5. A Review outcome shall be reasoned, recorded and communicated to the affected Actor or person.

170.6. A Review outcome shall identify whether the original decision is confirmed, corrected, varied, withdrawn or returned for a new decision within the competent route.

170.7. Review under the Framework shall not remove an applicable external right of complaint, review or remedy.

Article 171: Review of Status, services, Sources, objects and Controlled Reliance

171.1. Trust Service Provider Status, Trust Service Status, Source Status, Trust Object Status, mechanism or device Status and Qualified Status shall be reviewed independently.

171.2. Review of a Trust Service Provider shall not automatically determine the Status of each Trust Service provided by that Provider.

171.3. Review of a Trust Service shall not automatically determine the Status or validity of each Trust Service Output or Trust Object produced through that Service.

171.4. Review of Qualified Status shall examine the exact qualified Status-Bearing Matter, Qualified Scope, Qualified Profile, evidence and dependencies.

171.5. Review of a Trust Object or Trust Service Output shall remain separate from Review of its Issuer, Source Basis, Trust Service and Relying Actor decision.

171.6. Review of a local acceptance or Controlled Reliance decision shall remain with the Relying Actor or other Actor holding the applicable decision responsibility, subject to the applicable Framework requirements.

171.7. A Review outcome shall identify each resulting continuation, Correction, reassessment, restriction, Suspension, Withdrawal, Revocation, Replacement or Remedy.

Article 172: Interim Measures

172.1. A Responsible Actor or Framework Body shall apply an Interim Measure where delay creates a material risk to security, continuity, evidence, an Affected Person or proper Controlled Reliance.

172.2. An Interim Measure shall:

(a) identify the affected Controlled Matter or Controlled Effect;

(b) state the evidence and risk basis;

(c) remain limited to the necessary scope;

(d) identify the Effective Date;

(e) identify the review interval and expiry condition;

(f) remain subject to Review and Remedy.

172.3. An Interim Measure shall not be treated as a final determination.

172.4. The responsible Actor or Framework Body shall remove, replace or confirm the Interim Measure through the applicable final route when its conditions are determined.

172.5. An Interim Measure affecting Status shall be published by the responsible Framework Body where Status Publication is required.

SECTION 4: REMEDY AND CLOSURE

Article 173: Remedy outcomes and implementation

173.1. A Remedy shall address an adverse, incorrect, invalid, unsafe or non-conforming state or Controlled Effect.

173.2. A Remedy shall include, where appropriate:

(a) Correction;

(b) re-evaluation or reassessment;

(c) Replacement or reissuance;

(d) restoration of access or Participation;

(e) removal of an unjustified restriction;

(f) restriction, Suspension, Withdrawal or Revocation;

(g) notification to affected Actors or persons;

(h) correction of Status Publication;

(i) prevention of recurrence;

(j) another measure assigned by the applicable Framework Instrument.

173.3. A Remedy shall identify the affected matter, responsible Actor, required action, Effective Date, implementation evidence, continuing limitations and further Review Route.

173.4. A Remedy shall not assign a Status, permission, entitlement or Controlled Effect outside the applicable Decision Competence.

173.5. The responsible Actor shall implement the Remedy and preserve evidence of completion.

173.6. A Remedy addressing a systemic or repeated failure shall include the corrective and preventive actions required to reduce recurrence.

Article 174: Cross-domain Review and Remedy

174.1. Where a matter affects more than one Federation Domain, the responsible Actors and Framework Bodies shall coordinate Review, Correction and Remedy through the applicable Federation Agreement.

174.2. Cross-domain coordination shall identify:

(a) the originating and receiving Federation Domains;

(b) the affected Actors, Trust Services, Trust Objects, Trust Service Outputs, Sources and decisions;

(c) the Decision Competence retained by each domain;

(d) the evidence to be exchanged;

(e) the applicable Confidentiality and Protected-Person Safeguards;

(f) the required Status and publication updates;

(g) the communication route for the affected Actor or person.

174.3. A Framework Body in one Federation Domain shall not alter a decision or Status assigned within another Federation Domain unless the applicable Federation Agreement assigns that Decision Competence.

174.4. An affected Actor or person shall have one accessible entry route where the matter requires coordination across Federation Domains.

174.5. Cross-domain coordination shall not delay an urgent Interim Measure within the Decision Competence of an affected domain.

Article 175: Closure, evidence and continuing rights

175.1. A Responsible Actor or Framework Body shall maintain records sufficient to establish the conduct and outcome of each material Complaint, Correction, Review and Remedy.

175.2. A closure record shall identify:

(a) the affected matter;

(b) the evidence considered;

(c) the findings;

(d) the decision or Remedy;

(e) the implementation evidence;

(f) the remaining limitations;

(g) the communication to affected Actors or persons;

(h) the closure date;

(i) continuing monitoring or Review conditions.

175.3. Remedy Closure shall occur only where the assigned actions have been completed, their effect has been verified and each continuing obligation is recorded.

175.4. Closure shall not remove continuing rights, Retention duties, monitoring obligations or future Review where new evidence, non-implementation or a continuing adverse effect is established.

175.5. Historical evidence shall remain available for the period assigned by the applicable Framework Instrument.

175.6. Finality under the Framework shall not remove an applicable external right of complaint, review or remedy.

PART XIII: CHANGE CONTROL, VERSIONING AND TRANSITIONAL PROVISIONS

SECTION 1: CHANGE CONTROL

Article 176: General provisions on change

176.1. A Controlled Matter shall be changed only through the applicable Change Control route.

176.2. Change Control shall preserve:

(a) the identity and category of the Controlled Matter;

(b) the applicable Decision Competence;

(c) the distinction between Status, permission, technical availability and Controlled Effect;

(d) dependency traceability;

(e) Historical State;

(f) security, continuity and Protected-Person Safeguards;

(g) Review and Remedy Routes.

176.3. A change shall not have Controlled Effect before approval through the applicable route and the assigned Effective Date.

176.4. Technical, administrative or editorial implementation of an unapproved change shall not create recognition, Status, permission, qualification or operational activation.

176.5. A subordinate Framework Instrument shall not change a category, Decision Competence or Controlled Effect established by a Main Part.

Article 177: Change Classification

177.1. A proposed change shall be assigned a Change Classification according to its nature, scope, risk and Controlled Effect.

177.2. Change Classification shall distinguish, where applicable:

(a) editorial change;

(b) corrective change;

(c) compatible functional change;

(d) material functional change;

(e) security change;

(f) emergency change;

(g) breaking change;

(h) Deprecation, Retirement or Withdrawal.

177.3. Change Classification shall determine the applicable approval, assessment, testing, notification, Migration and Transition requirements.

177.4. A change shall not be classified as editorial where it alters meaning, scope, category, responsibility, Status, dependency, policy, Reliance Condition or Controlled Effect.

177.5. The classification decision and evidence basis shall be recorded.

Article 178: Change proposal and impact assessment

178.1. A change proposal shall identify:

(a) the affected Controlled Matter;

(b) the current and proposed Versions;

(c) the purpose and reason for the change;

(d) the affected requirements and functions;

(e) the affected Actors, Trust Services, Trust Objects, Trust Service Outputs, Sources, mechanisms, devices, Technical Exchange Routes and Framework Instruments;

(f) the dependency, Assurance, security, continuity, safeguard, Review and Remedy effects;

(g) the Compatibility, Migration and Transition effects;

(h) the proposed Effective Date;

(i) the evidence and approval route.

178.2. A material change shall be subject to impact assessment before approval.

178.3. The impact assessment shall determine:

(a) whether reassessment or Conformity Assessment is required;

(b) whether Status, Qualified Status or Service Permission is affected;

(c) whether reissuance, re-enrolment, regeneration or replacement is required;

(d) whether existing Trust Objects and Trust Service Outputs remain valid;

(e) whether Compatibility, Coexistence, Migration or Transition is required;

(f) whether cross-domain notification or coordination is required;

(g) whether an Adverse Protected-Person Effect can arise.

178.4. A limitation or uncertainty affecting the impact assessment shall be recorded and reflected in the approval decision.

Article 179: Approval, implementation and entry into effect

179.1. A change shall be approved only by the Actor or Framework Body holding the applicable Decision Competence.

179.2. A change-approval decision shall identify:

(a) the approved change;

(b) the affected scope;

(c) the approved Version;

(d) the evidence basis;

(e) the Effective Date;

(f) the Transition conditions;

(g) the required publication and notification;

(h) the Rollback conditions.

179.3. A material change shall not enter operational use before the Responsible Actor verifies implementation, testing, security, evidence and acceptance conditions.

179.4. Implementation evidence shall remain linked to the approval decision.

179.5. Publication of a change shall not, by itself, create operational activation, Service Permission or Qualified Status.

SECTION 2: VERSIONING, IDENTIFIERS AND STANDARDS

Article 180: Versioning

180.1. A Framework Instrument, Trust Service, Trust Object type, Source Profile, mechanism, device, schema and material configuration shall have a Version where change affects meaning, operation, Compatibility, evidence, Status or Controlled Effect.

180.2. A Version shall identify an immutable state of the versioned matter.

180.3. A new Version shall not overwrite or silently alter an earlier Version.

180.4. Version information shall be sufficient to determine:

(a) the applicable requirements;

(b) the applicable semantics;

(c) the applicable technical behaviour;

(d) the applicable Status and permissions;

(e) the period of application;

(f) the relationship with preceding and succeeding Versions.

180.5. Version equivalence shall not be presumed.

180.6. The Framework Steward shall maintain the authoritative Version history of the Main Parts and Annexes.

Article 181: Instrument Identifiers and code governance

181.1. Each Framework Instrument shall have a stable Instrument Identifier.

181.2. An Instrument Identifier shall remain separate from:

(a) the Version;

(b) the Instrument Status;

(c) the Effective Date;

(d) the publication location;

(e) a GitBook slug or navigation title.

181.3. The Instrument Identifier model shall distinguish:

(a) the instrument type;

(b) the controlled group;

(c) the function or subject code;

(d) the sequence identifier.

181.4. Instrument-type, controlled-group and function codes shall be recorded in the Instrument Code Catalogue.

181.5. A Framework Body shall assign a new function code within an existing controlled group only through the applicable governance decision.

181.6. A new instrument type or controlled group shall require amendment of the applicable Framework Instrument architecture.

181.7. A new Trust Service Category shall require amendment of Parts II and IX.

181.8. A new Trust Object Category shall require amendment of Parts II and VI.

181.9. A retired Instrument Identifier or code shall remain reserved and shall not be reused.

181.10. The Instrument Code Catalogue shall remain extensible through the controlled routes established by this Article and shall not create a new category or Controlled Effect by itself.

Article 182: Changes to Framework Instruments and Recognised Standards

182.1. A change to an Annex, Implementation Guideline, Scheme, Profile, Technical Specification or Body Instrument shall be managed according to its instrument type, hierarchy and Controlled Effect.

182.2. A subordinate Framework Instrument shall not alter a rule, category or Decision Competence established by a higher-ranking Framework Instrument.

182.3. A change to a Recognised Standard, technical reference or implementation dependency shall be assessed before recognition or incorporation.

182.4. The assessment shall identify:

(a) the earlier and proposed editions or Versions;

(b) the affected requirements and implementations;

(c) Compatibility and interoperability;

(d) security and Assurance effects;

(e) conformity-testing requirements;

(f) Migration and Transition conditions;

(g) Deprecation and Retirement dates.

182.5. Publication of a later standard edition shall not automatically alter the Recognised Standard recorded in the Standards Register.

182.6. The Standards Register shall record the recognised edition, selected options, deviations, Effective Date, Transition Status and replacement relationship.

Article 183: Changes to Controlled Matters and Qualified Scope

183.1. A material change to a Trust Service Provider shall be assessed for its effect on Provider Scope, Trust Service Provider Status and each affected Trust Service.

183.2. A material change to a Trust Service shall be assessed independently for that Trust Service, Service Scope, Service Permission, Assurance and Qualified Status.

183.3. A material change to a Trust Object Category, Trust Service Output Category or applicable Profile shall be assessed for its effect on existing objects, outputs, Validation, Status and Controlled Reliance.

183.4. A material change to a Source shall be assessed for its effect on Source Scope, Source Status, Data Quality, Provenance, semantics and dependent Controlled Matters.

183.5. A material change to a creation mechanism or device shall be assessed for its effect on its identity, function, configuration, operational environment, evidence and Qualified Status.

183.6. A material change affecting a Qualified Scope shall be assessed before Qualified Status continues to apply to the changed matter.

183.7. A change to one Controlled Matter shall not automatically change the Status, Version or Qualified Status of another Controlled Matter.

SECTION 3: COMPATIBILITY, MIGRATION AND TRANSITION

Article 184: Compatibility and Coexistence

184.1. Compatibility shall be determined against identified Versions, functions, interfaces, object categories and interaction requirements.

184.2. A Compatibility determination shall identify:

(a) the matters and Versions compared;

(b) the supported interactions and Trust Object Categories;

(c) the limitations and prohibited combinations;

(d) the applicable period;

(e) the evidence and test basis.

184.3. Coexistence shall occur only where the applicable Framework Instrument defines:

(a) the permitted Version combinations;

(b) routing and Discovery Metadata conditions;

(c) Verification and Validation conditions;

(d) downgrade and substitution protections;

(e) Status and evidence treatment;

(f) the end of Coexistence.

184.4. Compatibility shall not establish equivalence of Assurance, Qualified Status or Controlled Effect.

184.5. Technical interoperability shall not, by itself, create Service Permission, Technical Exchange Permission or Controlled Reliance.

Article 185: Migration

185.1. Migration shall preserve the identity, category, Provenance, lifecycle and Historical State of each affected Controlled Matter.

185.2. A Migration plan shall identify:

(a) the source and target Versions;

(b) the affected data, Trust Objects, Trust Service Outputs, Trust Services, Sources and dependencies;

(c) the transformation and Validation rules;

(d) the security, Confidentiality and safeguard controls;

(e) the testing and acceptance criteria;

(f) the Transition Period;

(g) the Rollback conditions;

(h) the treatment of failures and exceptions;

(i) the evidence to be retained.

185.3. A migrated Trust Object, Source record, Status record or other Controlled Record shall remain traceable to its earlier state.

185.4. Migration shall not silently change the meaning, category, Issuer, Subject, Status, Qualified Status, Reliance Condition or Controlled Effect of a matter.

185.5. Where a transformation creates a new Trust Object, Trust Service Output or Source, the new matter shall receive its own identity, lifecycle and Status treatment.

Article 186: Emergency change

186.1. An emergency change shall occur only where delay creates an unacceptable security, continuity, protection or operational risk.

186.2. An emergency-change decision shall identify:

(a) the emergency condition;

(b) the affected scope;

(c) the temporary or permanent change;

(d) the Responsible Actor;

(e) the immediate controls;

(f) the evidence retained;

(g) the review and regularisation period;

(h) the Rollback condition.

186.3. An emergency change shall remain subject to subsequent assessment, approval and documentation through the ordinary Change Control route.

186.4. Emergency implementation shall not create broader Status, permission, Qualified Status or Controlled Effect than the emergency decision assigns.

186.5. An emergency change affecting another Federation Domain shall be communicated without undue delay through the applicable federation route.

Article 187: Rollback

187.1. A material change shall have a Rollback arrangement where Rollback is technically and operationally feasible.

187.2. A Rollback decision shall identify:

(a) the failed or withdrawn change;

(b) the target earlier Version or state;

(c) the affected data, Trust Objects, Trust Service Outputs, Trust Services, Sources and dependencies;

(d) the security, Confidentiality and evidence controls;

(e) the treatment of matters created during the changed Version;

(f) the required Status and publication updates.

187.3. Rollback shall not remove or rewrite historical evidence of the changed Version.

187.4. Where Rollback is not feasible, the Responsible Actor shall apply an approved containment, Replacement, Migration or cessation arrangement.

187.5. Rollback to an earlier technical state shall not, by itself, reinstate earlier Status, Service Permission or Qualified Status.

Article 188: Transition and transitional provisions

188.1. A Transition shall identify the period and conditions under which an earlier and later requirement, Version or implementation arrangement applies.

188.2. A Transition plan shall identify:

(a) the affected Controlled Matters;

(b) the start and end dates;

(c) the permitted Coexistence;

(d) the Migration milestones;

(e) the required Conformity Assessment, testing and acceptance evidence;

(f) the Status and publication treatment;

(g) the communication obligations;

(h) the closure criteria.

188.3. An earlier Version shall not remain in operational use after the end of its Transition Period unless an authorised extension identifies the scope, reason, safeguards and expiry.

188.4. A Transition shall not reduce a mandatory Security Condition, Protected-Person Safeguard, Review Route or Remedy Route.

188.5. A Trust Object or Trust Service Output created under an earlier Version shall remain governed by the applicable lifecycle and Transition provisions.

Article 189: Historical State and non-retroactivity

189.1. The Framework shall preserve the Historical State required to evaluate an action, decision, Trust Object, Trust Service Output, Source, Status, Qualified Status or Controlled Reliance at the time it occurred.

189.2. Historical reconstruction shall identify:

(a) the applicable Framework Instruments and Versions;

(b) the applicable Status and permissions;

(c) the applicable dependencies;

(d) the evidence and Validation basis;

(e) the applicable restrictions, caveats and Reliance Conditions.

189.3. A later change shall not retrospectively invalidate an earlier matter that satisfied the requirements applicable at the relevant time unless a Framework Decision expressly assigns that effect on a supported evidence basis and within assigned Decision Competence.

189.4. Correction of an historical record shall preserve the earlier record and identify the Correction and its Effective Date.

189.5. A later recognition, qualification or standard edition shall not be represented as having applied before its Effective Date.

Article 190: Deprecation, Retirement and Withdrawal

190.1. A Framework Instrument, Version, Recognised Standard, service implementation, mechanism, device or technical component shall be deprecated, retired or withdrawn only through the applicable Change Control route.

190.2. The applicable decision shall identify:

(a) the affected matter;

(b) the reason;

(c) the publication date;

(d) the end of new use;

(e) the end of operational use;

(f) the replacement or Migration route;

(g) the treatment of existing Trust Objects and Trust Service Outputs;

(h) the continuing Validation, Status and preservation arrangements.

190.3. Deprecation shall not, by itself, withdraw existing Status or invalidate an existing Controlled Matter.

190.4. A retired or withdrawn matter shall remain identifiable for Historical State, Validation, Review and Remedy purposes.

190.5. A retired Instrument Identifier, category code or function code shall remain reserved in the applicable Catalogue.

Article 191: Cross-domain change propagation

191.1. A change affecting more than one Federation Domain shall be communicated through the applicable federation governance route.

191.2. Cross-domain change information shall identify:

(a) the originating Federation Domain;

(b) the affected Controlled Matters and Versions;

(c) the Effective Date;

(d) Compatibility, Migration and Transition conditions;

(e) security, continuity and safeguard effects;

(f) Status and Humanitarian Trust List effects;

(g) required action by receiving Federation Domains;

(h) Review and escalation routes.

191.3. A receiving Federation Domain shall assess the change within its assigned Decision Competence and Local Trust Acceptance Policy.

191.4. Recognition of a change in one Federation Domain shall not automatically create recognition, Compatibility, operational activation, Technical Exchange Permission, Controlled Reliance or Qualified Status in another Federation Domain.

191.5. Cross-domain propagation shall preserve the authoritative record and Historical State of each affected Federation Domain.

Article 192: Change closure

192.1. A material change shall be closed only where:

(a) approved implementation is complete;

(b) required testing and Conformity Assessment are complete;

(c) Migration and Transition actions are complete;

(d) Status Publication, Register, Catalogue and Humanitarian Trust List updates are complete;

(e) residual risks are accepted within assigned Decision Competence;

(f) affected Actors and persons have received required information;

(g) Historical State and evidence are preserved;

(h) outstanding Review and Remedy matters are recorded.

192.2. A closure record shall identify the implemented Version, Effective Date, evidence basis, remaining limitations and continuing monitoring conditions.

192.3. Change closure shall not remove continuing surveillance, security, Review, Remedy, Retention or historical-reconstruction obligations.

192.4. Closure of a change in one Federation Domain shall not determine closure in another Federation Domain unless the applicable Federation Agreement assigns that effect.

ANNEX A: FUNCTIONAL ARCHITECTURE AND TRUST MODEL

IDEHA-ANN-FED-GEN-001 Version: 0.1

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Annex establishes the common architecture and federation relationship model required by Parts I, III, IV and V.

1.2. This Annex applies to each Federation Domain, Nested Federation, Federation Trust Relationship, Framework Body, Actor, Source, Trust Service Provider, Trust Service, Trust Object, Trust Service Output, Technical Exchange Route and Controlled Interaction governed by the Framework.

1.3. This Annex shall be applied together with the category, Status, Decision Competence and Controlled Effect rules established by the Main Parts.

1.4. This Annex shall not:

(a) create a Trust Service Category or Trust Object Category;

(b) assign recognition, Status, Qualified Status, Service Permission or Technical Exchange Permission;

(c) authorise access, disclosure or Controlled Reliance;

(d) prescribe a standard, protocol, format, product or deployment model;

(e) determine a substantive humanitarian, administrative, programme or operational outcome.

1.5. An Implementation Guideline, Scheme, Profile, Technical Specification or Body Instrument shall preserve the architecture and category boundaries established by this Annex.

Article 2: Architecture layers and category boundaries

2.1. The common architecture shall comprise the following functional layers:

(a) Framework governance, supervision, publication, Review and Remedy;

(b) federation, Participation, Roles, Mandates and responsibility;

(c) Source and Trust Service provision;

(d) Trust Service Outputs and Trust Objects;

(e) Controlled Interaction, Verification, Validation, Authorisation and Controlled Reliance.

2.2. The layers referred to in paragraph 2.1 shall describe functional relationships and shall not constitute separate Status categories or Controlled Effects.

2.3. Each Controlled Matter shall retain the category assigned by the Main Parts.

2.4. Performance of functions in more than one layer by the same Actor, system or technical component shall not merge:

(a) the functions performed;

(b) the Roles or responsibilities assigned;

(c) the Status of the affected Controlled Matters;

(d) the evidence and lifecycle applicable to those matters;

(e) the Decision Competence retained by a Framework Body or Actor.

2.5. A technical implementation shall support the architecture without converting:

(a) a Source into a Trust Service;

(b) a Trust Service into a Technical Exchange Route;

(c) a Trust Service Output into a Trust Object unless Part VI assigns that category;

(d) a Humanitarian Trust List or Register into a Trust Service;

(e) Verification, Validation or Authorisation into Controlled Reliance.

2.6. A dependency between layers shall be recorded without transferring identity, Status, responsibility, Assurance, Qualified Status or Controlled Effect.

SECTION 2: FEDERATION ARCHITECTURE

Article 3: Federation Domains and Federation Boundaries

3.1. A Federation Domain shall constitute the governed trust environment within which recognised Actors, Sources, Trust Service Providers, Trust Services, policies and Technical Exchange arrangements operate under assigned conditions.

3.2. Each Federation Domain shall be uniquely identifiable and shall record:

(a) its governance arrangements;

(b) its Federation Boundary;

(c) its participating Actors and recognised Roles;

(d) its applicable Federation Trust Policy;

(e) its recognised Sources, Trust Service Providers and Trust Services;

(f) its applicable Technical Exchange arrangements;

(g) its Status Publication, Review and Remedy arrangements.

3.3. A Federation Boundary shall identify the organisational, functional, geographic, technical or jurisdictional limits relevant to the Federation Domain.

3.4. A Federation Domain shall retain responsibility for decisions and Controlled Effects assigned within its boundary.

3.5. A Federation Domain shall not acquire ownership, authority or control over another Federation Domain by reason only of federation, technical connection, common governance support or participation in a shared Scheme.

3.6. Crossing a Federation Boundary shall not, by itself, create recognition, Service Permission, Technical Exchange Permission, access, disclosure, Qualified Status or Controlled Reliance.

3.7. Changes to a Federation Domain or Federation Boundary shall be managed under Part XIII and shall preserve the Historical State required for Validation, Review and Remedy.

Article 4: Nested Federation and Federation Trust Relationships

4.1. A Nested Federation shall operate under a recognised relationship between the parent and nested Federation Domains.

4.2. A Federation Trust Relationship shall be established through a Federation Agreement or another Recognised Instrument identifying:

(a) the participating Federation Domains;

(b) the recognised purpose and scope;

(c) the governance and Decision Competence retained by each Federation Domain;

(d) the recognition and Status conditions;

(e) the applicable policies and Reliance Conditions;

(f) the Technical Exchange and discovery conditions;

(g) the security, incident and continuity arrangements;

(h) the Review, Remedy, change and termination arrangements.

4.3. A parent Federation Domain shall not acquire the Decision Competence, operational responsibility, Source responsibility or local reliance responsibility of a nested Federation Domain unless a Recognised Instrument expressly assigns that competence or responsibility.

4.4. Recognition or Status in a parent Federation Domain shall not automatically extend to a nested Federation Domain, and recognition or Status in a nested Federation Domain shall not automatically extend to the parent Federation Domain.

4.5. A Federation Trust Relationship shall not be transitive beyond the Federation Domains and scope identified in the applicable Federation Agreement.

4.6. A parent Federation Domain shall reference the authoritative governance and Status Publication arrangements of a nested Federation Domain without duplicating local operational responsibility where the applicable Federation Agreement so provides.

4.7. Termination, restriction or suspension of a Federation Trust Relationship shall affect earlier Controlled Reliance only where the applicable Framework Decision, Reliance Condition or dependency rule assigns that effect.

SECTION 3: GOVERNANCE AND RESPONSIBILITY ARCHITECTURE

Article 5: Framework Bodies, Framework Functions and Decision Competence

5.1. Framework governance shall remain separate from Trust Service operation, Source responsibility, Technical Exchange operation and local Controlled Reliance.

5.2. Each Framework Body shall be assigned:

(a) one or more Framework Functions;

(b) the Decision Competence applicable to each function;

(c) the Controlled Matters within its scope;

(d) the evidence and record requirements;

(e) the conflict-control and independence requirements;

(f) the lifecycle and Review conditions.

5.3. A Framework Body shall adopt a Framework Decision only within the Decision Competence assigned to it.

5.4. Recognition, Decision-Based Qualification, supervision, Status Publication, Review and Remedy shall remain separately identifiable Framework Functions.

5.5. A technical operator, service provider or Intermediary supporting a Framework Body shall not acquire:

(a) Decision Competence;

(b) authority to assign or alter Status;

(c) authority to assign Qualified Status;

(d) governance ownership of the Humanitarian Trust List, Register or Catalogue supported by it;

(e) responsibility for a local Controlled Reliance decision.

5.6. A Framework Decision shall be recorded in a Decision File before its Controlled Effect begins.

5.7. A Framework Body shall retain the evidence required to reconstruct the Decision Competence, evidence basis, scope, Effective Date, Controlled Effect and Review Route of each material Framework Decision.

Article 6: Actors, Roles, Mandates and Responsible Actors

6.1. Participation, an Assigned Role, a Mandate and responsibility shall remain separate Controlled Matters.

6.2. A Participating Actor shall perform a function only within its Participation Scope, Role Scope, Mandate Scope and applicable Framework Instruments.

6.3. Each material function, decision, Trust Service, Source, Technical Exchange Route and Controlled Interaction shall have an identifiable Responsible Actor.

6.4. Where responsibility is shared, the applicable Framework Instrument shall identify:

(a) each Responsible Actor;

(b) the function and scope allocated to each Actor;

(c) the boundary between the allocated responsibilities;

(d) the treatment of shared dependencies and failures;

(e) the evidence, escalation and Review arrangements.

6.5. Performance of more than one Role by the same Actor shall not merge the scope, responsibility, evidence or lifecycle of those Roles.

6.6. A Mandate shall not create a Role, Status, permission or Controlled Effect beyond the Mandate Scope.

6.7. An Intermediary or Technical Exchange Route Operator shall not acquire the Role, Status, Mandate or responsibility of the Requesting Actor, Responding Actor, Issuer, Source Holder, Trust Service Provider or Relying Actor by reason only of facilitating a Controlled Interaction.

6.8. An ambiguity or gap in responsibility shall be referred to the competent Framework Body and shall not reduce the protection available to an Affected Person or Protected Person.

Article 7: Federation Trust Policy, Local Trust Acceptance Policy and local decision

competence

7.1. A Federation Trust Policy shall establish common minimum trust conditions within or between Federation Domains.

7.2. A Local Trust Acceptance Policy shall establish the conditions under which a Relying Actor accepts a Controlled Matter for an identified purpose and Controlled Reliance.

7.3. A Participating Actor shall retain Decision Competence over its local operational, disclosure, service and Controlled Reliance decisions unless a Recognised Instrument expressly assigns that competence elsewhere.

7.4. A Federation Trust Policy shall not require a Relying Actor to accept a Controlled Matter where the applicable Local Trust Acceptance Policy, Authorisation Policy, Reliance Condition or safeguard condition is not satisfied.

7.5. A Local Trust Acceptance Policy shall not reduce a mandatory condition or safeguard established by the Framework, a Federation Agreement or an applicable higher-ranking Framework Instrument.

7.6. An Authorisation Service shall evaluate the applicable Authorisation Policy without acquiring responsibility for defining that policy unless an applicable Framework Instrument assigns that function.

7.7. A Policy Enforcement Function shall apply an Authorisation Outcome to the requested action or Controlled Interaction without converting that Outcome into a local acceptance or Controlled Reliance decision.

7.8. Humanitarian Trust List inclusion, successful Verification, positive Validation or an Authorisation Outcome shall not, by itself, require acceptance or Controlled Reliance.

7.9. The applicable Federation Agreement, Scheme or Profile shall identify the rule for resolving an identified conflict between Federation Trust Policy, Authorisation Policy and Local Trust Acceptance Policy.

SECTION 4: TRUST ARCHITECTURE

Article 8: Sources, Trust Service Providers, Trust Services and Trust Objects

8.1. A Source shall provide an information basis recognised for an identified purpose and Source Scope.

8.2. A Trust Service Provider shall provide one or more independently recognised Trust Services within its Provider Scope.

8.3. Each Trust Service shall retain its own:

(a) Trust Service Category;

(b) Service Scope and Service Permission;

(c) Trust Service Status and Qualified Status, where assigned;

(d) native Trust Service Outputs;

(e) dependencies, evidence and lifecycle;

(f) Responsible Actor.

8.4. A Trust Service Output shall remain separate from the Trust Service that produced it.

8.5. A Trust Service Output shall become a Trust Object only where Part VI assigns the applicable Trust Object Category and the output satisfies the requirements for that category.

8.6. A Trust Object shall retain its identity, category, Issuer, Subject where applicable, Metadata, Status, dependencies and lifecycle independently from the Trust Service Provider and Trust Service associated with it.

8.7. An Electronic Attestation shall remain case-neutral and shall be governed according to its function as a statement-bearing Trust Object rather than the humanitarian, administrative, programme or operational use of its Attestation Statement.

8.8. A Source, Trust Service Provider, Trust Service, Trust Service Output and Trust Object shall be assessed and governed independently.

8.9. Recognition, Assurance or Qualified Status assigned to one matter shall not transfer to another matter by reason only of issuance, use, dependency, common ownership or common technical implementation.

Article 9: Technical Exchange Routes, Policy Enforcement and controlled interaction

9.1. A Technical Exchange Route shall provide the recognised technical means through which a Controlled Interaction occurs.

9.2. A Federated Data Exchange Service shall provide the controlled exchange functions assigned by Part IX without acquiring the local decision competence of a Requesting Actor, Responding Actor or Relying Actor.

9.3. Discovery Metadata published under governance control shall support location and resolution of recognised Actors, Trust Service Providers, Trust Services, Sources, Endpoints and Technical Exchange Routes.

9.4. Discovery of an Endpoint or Technical Exchange Route shall not create Technical Exchange Permission, access, disclosure, Service Permission or Controlled Reliance.

9.5. A Requesting Actor shall initiate a Controlled Interaction only where the applicable Participation, Role, Mandate, purpose, Authorisation, Access Conditions, Disclosure Conditions and evidence requirements are satisfied.

9.6. A Responding Actor shall respond only where the conditions established by Part V, Article 61, and the applicable policies, safeguards and Framework Instruments are satisfied.

9.7. A Policy Enforcement Function shall enforce the applicable Authorisation Outcome at the point assigned by the applicable Framework Instrument.

9.8. Transport Confidentiality, Payload Confidentiality and object-level Integrity and Authenticity protection shall remain separate controls.

9.9. A Technical Exchange Route Operator or Federated Data Exchange Service Provider shall not acquire ownership or unrestricted access to exchanged information by reason only of carrying or routing that information.

9.10. Technical availability, successful routing or completion of exchange shall not, by itself, establish the validity, correctness, acceptance or Controlled Reliance of an exchanged Controlled Matter.

Article 10: Verification, Validation, Authorisation and Controlled Reliance sequence

10.1. The evaluation of a Controlled Matter shall preserve the separation between discovery, Verification, Validation, Authorisation, acceptance and Controlled Reliance.

10.2. The evaluation model shall distinguish, where applicable:

(a) resolution of the relevant Actor, Trust Service Provider, Trust Service, Source, Endpoint or Federation Domain through authorised Discovery Metadata;

(b) Verification of identity, origin, attribution, Integrity or another identified property;

(c) Validation of the Controlled Matter, Status, applicable Profile and mandatory dependencies;

(d) evaluation of Authorisation for the requested action, access, disclosure or exchange;

(e) evaluation of acceptance under the Relying Actor's Local Trust Acceptance Policy;

(f) Controlled Reliance within the applicable Reliance Conditions and Reliance Limits.

10.3. The applicable Profile shall identify which steps are required and the order in which they apply without merging their respective functions or outputs.

10.4. A positive Verification Result shall not constitute a Validation Result, Authorisation Outcome or Controlled Reliance decision.

10.5. A positive Validation Result shall not constitute an Authorisation Outcome or require acceptance by a Relying Actor.

10.6. An Authorisation Outcome shall not constitute acceptance or Controlled Reliance.

10.7. A Relying Actor shall remain responsible for the local operational decision or service outcome based on Controlled Reliance.

10.8. The Responsible Actors shall retain the evidence required to reconstruct each material step and its result.

SECTION 5: CROSS-DOMAIN ARCHITECTURE

Article 11: Cross-Domain Reliance and retention of responsibility

11.1. Cross-Domain Reliance shall occur only within a recognised Federation Trust Relationship and the applicable Federation Agreement, Scheme, Profile and Reliance Conditions.

11.2. The originating Federation Domain shall retain responsibility for the governance, Status and evidence of Controlled Matters assigned within its Decision Competence.

11.3. The receiving Federation Domain shall retain responsibility for:

(a) local Authorisation;

(b) local acceptance under the applicable Local Trust Acceptance Policy;

(c) local Controlled Reliance;

(d) the resulting operational or service decision;

(e) applicable Review and Remedy Routes.

11.4. A Federation Agreement shall identify the recognition, mapping, Validation, policy, security, incident, Correction, Review and Remedy conditions required for Cross-Domain Reliance.

11.5. Recognition, Status, Assurance or Qualified Status in the originating Federation Domain shall not automatically create equivalent recognition, Status, Assurance or Qualified Status in the receiving Federation Domain.

11.6. The receiving Federation Domain shall evaluate the Controlled Matter within its own assigned Decision Competence and applicable policy conditions.

11.7. The participating Federation Domains shall coordinate material Correction, Suspension, Withdrawal, Revocation, incident and change information affecting Cross-Domain Reliance.

11.8. An Affected Person or Actor shall have access to an identifiable Review and Remedy route where coordination between Federation Domains is required.

11.9. Cross-Domain Reliance shall not transfer responsibility for the originating matter, receiving decision or supporting Trust Service beyond the scope assigned to each Responsible Actor.

SECTION 6: BOUNDARY RULES

Article 12: Non-centralisation, category separation and non-transfer of Status

12.1. The architecture established by this Annex shall not create:

(a) a central humanitarian identity authority;

(b) a universal register of natural persons;

(c) central ownership of data held by Participating Actors;

(d) general authority over local decisions retained by a Participating Actor or Federation Domain.

12.2. The Humanitarian Trust List, Registers and Catalogues shall remain governance-controlled publication or record mechanisms and shall not constitute Trust Services.

12.3. The address-book function shall be performed through authorised Discovery Metadata published or referenced through the Humanitarian Trust List and shall not constitute a separate Trust Service.

12.4. The following categories shall remain separate:

(a) Actor and Role;

(b) Source and Trust Service;

(c) Trust Service Provider and Trust Service;

(d) Trust Service and Trust Service Output;

(e) Trust Service Output and Trust Object;

(f) Technical Exchange Route and Federated Data Exchange Service;

(g) Status Publication and Status assignment;

(h) Verification, Validation, Authorisation and Controlled Reliance.

12.5. A dependency shall not transfer identity, responsibility, Status, Assurance, Qualified Status, permission or Controlled Effect.

12.6. Qualified Status shall apply only to the identified Status-Bearing Matter and Qualified Scope under the applicable qualification route.

12.7. Automation, common infrastructure, shared operation or federation shall not displace the responsibility of the Actor or Framework Body to which the Framework assigns the relevant function or decision.

12.8. A subordinate Framework Instrument shall not alter the architecture, categories or Controlled Effects established by the Main Parts and this Annex.

ANNEX B: FRAMEWORK INSTRUMENT, IDENTIFIER AND CODE MODEL

IDEHA-ANN-GOV-FRM-001 Version: 0.1

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Annex establishes the Framework Instrument hierarchy, Instrument Identifier model, controlled code model, record-identifier model, Version and lineage requirements, and rules for stable legal references.

1.2. This Annex applies to each Framework Instrument and to each governance-controlled Register, Catalogue, Decision File and Humanitarian Trust List record for which an identifier is assigned under the Framework.

1.3. This Annex shall be applied together with Parts I, IV and XIII.

1.4. This Annex shall not:

(a) create a Trust Service Category, Trust Object Category, Source category, Status category or qualification route;

(b) assign recognition, Instrument Status, Qualified Status, permission or Controlled Effect;

(c) determine the substantive requirements of a Trust Service, Trust Object, Source, Scheme or Profile;

(d) prescribe a technical protocol, data format, algorithm, product or deployment model.

1.5. An identifier or code shall identify or classify a Controlled Matter and shall not, by itself, create recognition, Status, authority, permission or Controlled Effect.

SECTION 2: FRAMEWORK INSTRUMENT ARCHITECTURE

Article 2: Framework Instrument hierarchy

2.1. The Framework Instrument hierarchy shall comprise:

(a) Main Parts;

(b) Annexes;

(c) Implementation Guidelines;

(d) Schemes;

(e) Profiles;

(f) Technical Specifications;

(g) Body Instruments.

2.2. Main Parts shall prevail over Annexes and subordinate Framework Instruments.

2.3. Annexes shall prevail over Implementation Guidelines, Schemes, Profiles, Technical Specifications and Body Instruments within their subject matter.

2.4. Implementation Guidelines, Schemes, Profiles, Technical Specifications and Body Instruments shall operate within their enabling provisions and assigned scopes.

2.5. Instruments referred to in paragraph 2.4 shall not form a separate order of precedence solely by reason of their instrument type.

2.6. Where more than one subordinate Framework Instrument applies, applicability shall be determined by:

(a) the enabling provision;

(b) the recognised purpose and scope;

(c) the referenced Instrument Identifier and Version;

(d) the Effective Date;

(e) the hierarchy and conflict rules established by Part I.

2.7. A document, record or technical artefact shall not become a Framework Instrument solely because another Framework Instrument refers to it.

Article 3: Function and permitted content of Framework Instrument categories

3.1. A Main Part shall establish constitutional rules, Controlled Terms, recognised categories, Decision Competence, Status, Controlled Effects and essential boundaries.

3.2. An Annex shall establish stable structural models, classifications, relationships and horizontal application rules required by the Main Parts.

3.3. An Implementation Guideline shall assign implementation requirements and operational conditions for an identified object, Trust Service, governance function or horizontal control and shall identify applicable Recognised Standards where required.

3.4. A Scheme shall establish a governed arrangement for an identified purpose, context and participating scope.

3.5. A Profile shall select requirements, options, Assurance Conditions, dependencies and lifecycle conditions for an existing Actor, Trust Service, Trust Object, Source, mechanism, device, Technical Exchange Route or process.

3.6. A Technical Specification shall assign detailed schemas, protocols, formats, algorithms, parameters, interfaces, configurations, test conditions and implementation requirements.

3.7. A Body Instrument shall record or assign a decision, approval, recognition, designation, qualification, restriction, Suspension, Withdrawal, Review outcome or other matter within the Decision Competence of the adopting Framework Body.

3.8. A Framework Instrument shall not contain material reserved to a higher-ranking Framework Instrument.

3.9. A subordinate Framework Instrument shall not create:

(a) a new Framework Instrument category;

(b) a new Trust Service Category or Trust Object Category;

(c) a new Status category or qualification route;

(d) new Decision Competence;

(e) a Controlled Effect not established by the Main Parts.

Article 4: Enabling relationships and subordinate-instrument boundaries

4.1. Each subordinate Framework Instrument shall identify the Main Part, Annex or other enabling provision under which it is adopted or recognised.

4.2. A Scheme shall identify the applicable Implementation Guidelines and Profiles.

4.3. A Profile shall identify the applicable Implementation Guidelines, Technical Specifications and mandatory dependencies.

4.4. A Technical Specification shall implement only the options, conditions and scope selected by its enabling Profile or other applicable Framework Instrument.

4.5. A Body Instrument shall identify the enabling provision and Decision Competence under which it is adopted.

4.6. A Framework Instrument shall reference another Framework Instrument by its stable Instrument Identifier and the applicable Version or Version-resolution rule.

4.7. Publication of a later Version shall not automatically amend a fixed reference to an earlier Version.

4.8. Incorporation by reference shall not transfer the Status, hierarchy, responsibility or Controlled Effect of the referenced instrument to the referring instrument.

4.9. A subordinate Framework Instrument shall not expand its own scope through a reference to another instrument.

4.10. A conflict between Framework Instruments shall be recorded and resolved under Part I and Part XIII before the conflicting provision is relied upon for a new Controlled Effect.

SECTION 3: INSTRUMENT IDENTIFIER MODEL

Article 5: Instrument Identifier structure

5.1. Each Framework Instrument shall have one stable Instrument Identifier.

5.2. An Instrument Identifier shall use the following structure:

IDEHA-TYPE-GROUP-FUNCTION-SEQUENCE

5.3. The elements referred to in paragraph 5.2 shall identify:

(a) IDEHA, as the Framework identifier root;

(b) TYPE, as the instrument-type code;

(c) GROUP, as the controlled subject-group code;

(d) FUNCTION, as the function or subject code within the controlled group;

(e) SEQUENCE, as the fixed sequence identifier.

5.4. Each Instrument Identifier shall contain uppercase Latin letters, Arabic numerals and hyphen separators only.

5.5. Each Framework Instrument shall have one primary controlled group and one primary function code.

5.6. Additional subject matter, dependencies and applicable functions shall be recorded in the instrument Metadata and the Instrument Code Catalogue and shall not be added to the Instrument Identifier.

5.7. An Instrument Identifier shall remain separate from:

(a) the Version;

(b) the Instrument Status;

(c) the Effective Date;

(d) the publication location;

(e) a GitBook slug or navigation title;

(f) the legal title of the Framework Instrument.

5.8. A change to a title, publication location, navigation label or file name shall not change the Instrument Identifier.

5.9. A Roman numeral assigned to a Main Part and a letter assigned to an Annex shall remain legal structural designations and shall not replace the Instrument Identifier.

Article 6: Initial instrument-type codes

6.1. The initial instrument-type codes shall be:

(a) MP for a Main Part;

(b) ANN for an Annex;

(c) IG for an Implementation Guideline;

(d) SCH for a Scheme;

(e) PRF for a Profile;

(f) TS for a Technical Specification;

(g) BI for a Body Instrument.

6.2. A code referred to in paragraph 6.1 shall identify the instrument type only and shall not indicate hierarchy within that type, Version, Status or priority.

6.3. A new instrument-type code shall be established only through amendment of Part I and this Annex.

6.4. A retired instrument-type code shall remain reserved and shall not be reassigned.

Article 7: Controlled group and function-code model

7.1. The initial controlled group codes shall be:

(a) GOV for Framework governance, Framework Instruments and Decision Competence;

(b) FED for federation, Federation Domains, Federation Agreements, federation policy and Cross-Domain Reliance;

(c) ACT for Actors, Participation, Roles, Mandates and representation;

(d) OBJ for Trust Objects and eligible Trust Service Outputs;

(e) SRC for Sources, Authoritative Sources, Source Verification, Data Quality, semantics and Provenance;

(f) TSP for Trust Service Providers and Provider governance;

(g) SVC for Trust Services and Trust Service Functions;

(h) ASR for Assurance, Conformity Assessment and qualification;

(i) PUB for the Humanitarian Trust List, Status Publication, Registers, Catalogues and federation discovery;

(j) SEC for security, Confidentiality, incidents and Continuity;

(k) RMR for Review, Correction and Remedy;

(l) CHG for Change Control, Versioning, Migration and Transition;

(m) DAT for controlled data elements, semantics, data models and Data Quality implementation;

(n) BIO for biometric capture, samples, templates, comparison, quality and devices.

7.2. The code GEN shall identify an instrument applying to the whole of a controlled group where no narrower function code is appropriate.

7.3. The initial core function codes for the SVC group shall be:

(a) IDN for the Identification Service;

(b) AUT for the Authentication Service;

(c) AUZ for the Authorisation Service;

(d) DSG for the Digital Signing Service;

(e) SIG for the Electronic Signature Service;

(f) SEL for the Electronic Seal Service;

(g) TST for the Electronic Timestamp Service;

(h) EAS for the Electronic Attestation Service;

(i) VVS for the Validation and Verification Service;

(j) FDX for the Federated Data Exchange Service.

7.4. The initial core function codes for the OBJ group shall be:

(a) DSG for Digital Signatures;

(b) SIG for Electronic Signatures;

(c) SEL for Electronic Seals;

(d) TST for Electronic Timestamps;

(e) CRT for Certificates;

(f) EAS for Electronic Attestations;

(g) IDN for Identification Results;

(h) IDR for Identity Resolution Results;

(i) AUT for Authentication Outcomes;

(j) AUZ for Authorisation Outcomes;

(k) VER for Verification Results;

(l) VAL for Validation Results;

(m) STR for Status Responses;

(n) EXE for Exchange Evidence;

(o) CXR for Controlled Exchange Results.

7.5. The Instrument Code Catalogue shall record subordinate Trust Service function codes and their parent Trust Service Category. The initial subordinate function mappings shall include:

(a) IPF for identity proofing under IDN;

(b) REG for identity registration under IDN;

(c) IDR for identity resolution under IDN;

(d) ILM for identity lifecycle management under IDN;

(e) PEV for policy evaluation under AUZ;

(f) STS for Status evaluation under VVS;

(g) DLV for delivery evidence under FDX.

7.6. The initial common function codes for the remaining controlled groups shall be recorded in the Instrument Code Catalogue and shall include, at minimum:

(a) FRM, DEC and SUP within GOV for Framework Instruments, Framework Decisions and supervision;

(b) DOM, AGR, POL and XDR within FED for Federation Domains, Federation Agreements, federation policy and Cross-Domain Reliance;

(c) PAR, ROL, MAN, REP and RLY within ACT for Participation, Roles, Mandates, representation and Relying Actors;

(d) ASO, SVR, DQS and PRV within SRC for Authoritative Sources, Source Verification, Data Quality and semantics, and Provenance;

(e) CFA and QLF within ASR for Conformity Assessment and qualification;

(f) HTL, REG, CAT, DSC and STP within PUB for the Humanitarian Trust List, Registers, Catalogues, discovery and Status Publication;

(g) CNF, CRY, INC and CON within SEC for Confidentiality, cryptographic controls, incidents and Continuity;

(h) REV, COR and REM within RMR for Review, Correction and Remedy;

(i) VRS, MIG, TRN and RBK within CHG for Versioning, Migration, Transition and Rollback;

(j) ELM, SEM and QTY within DAT for data elements, semantics and quality;

(k) CAP, SMP, TPL, MAT, QLT, PAD and DEV within BIO for capture, samples, templates, matching, quality, presentation attack detection and devices.

7.7. A function code shall identify subject matter or a subordinate function and shall not, by itself, create a Trust Service Category, Trust Object Category or Controlled Effect.

7.8. A function code for a subordinate function of a Trust Service shall remain mapped in the Instrument Code Catalogue to the Trust Service Category established by Part IX.

7.9. Identical function codes shall be used across different controlled groups only where the Instrument Code Catalogue records an intentional semantic relationship and the complete code path remains unambiguous.

7.10. A new function code within an existing controlled group shall be assigned through the governance route established by Article 12 and shall not require amendment of this Annex where it does not create a new category, group or Controlled Effect.

Article 8: Sequence identifiers, uniqueness and reservation

8.1. SEQUENCE shall comprise three Arabic numerals beginning with 001.

8.2. A sequence identifier shall be unique within the applicable combination of TYPE, GROUP and FUNCTION.

8.3. A sequence identifier shall not indicate Version, Status, priority, Assurance Level or chronological order outside its code path.

8.4. A sequence identifier shall not contain a letter suffix.

8.5. An Instrument Identifier shall not be reused after Retirement, Withdrawal, supersession or archival of the Framework Instrument.

8.6. A replacement or successor Framework Instrument shall receive a new Instrument Identifier where it constitutes a new instrument rather than a new Version of the same instrument.

8.7. The Instrument Code Catalogue shall record each allocated, reserved, retired and prohibited identifier range.

8.8. The following forms are examples of conforming Instrument Identifiers:

(a) IDEHA-IG-SVC-EAS-001;

(b) IDEHA-PRF-OBJ-EAS-001;

(c) IDEHA-TS-BIO-CAP-001;

(d) IDEHA-SCH-SVC-IDN-001.

8.9. The examples in paragraph 8.8 shall illustrate syntax only and shall not assign Instrument Status or recognition to an instrument.

SECTION 4: GOVERNANCE RECORD IDENTIFIERS

Article 9: Record identifiers for Registers, Catalogues, Decision Files and Humanitarian Trust List records

9.1. A Register, Catalogue, Decision File or Humanitarian Trust List record shall have a stable record identifier where required for governance, evidence, publication or historical reconstruction.

9.2. The initial record-type codes shall be:

(a) REG for a Register;

(b) CAT for a Catalogue;

(c) DF for a Decision File;

(d) HTL for a Humanitarian Trust List record set or Entry.

9.3. A record identifier shall use the structure applicable to the record type and shall identify, at minimum:

(a) the Framework root;

(b) the record type;

(c) the responsible governance domain or controlled group;

(d) the function or subject;

(e) a unique sequence.

9.4. A record-type code shall not constitute a Framework Instrument type code unless Part I is amended to establish that record type as a Framework Instrument category.

9.5. An Entry shall identify the parent Register, Catalogue or Humanitarian Trust List record set to which it belongs.

9.6. A Decision File shall identify the Framework Decision, deciding Framework Body, affected Controlled Matter and Effective Date to which it relates.

9.7. A Humanitarian Trust List Entry identifier shall remain separate from the identifier of the Status-Bearing Matter described by the Entry.

9.8. Correction, replacement or supersession of an Entry shall preserve its predecessor relationship and Historical State.

9.9. Inclusion in a record set or assignment of a record identifier shall not, by itself, create recognition, Status, permission, qualification or Controlled Effect.

SECTION 5: VERSION, STATUS AND LINEAGE

Article 10: Version, Instrument Status and Effective Date

10.1. Version, Instrument Status and Effective Date shall be recorded as separate properties of a Framework Instrument.

10.2. A Version shall identify an immutable state of the Framework Instrument.

10.3. Instrument Status shall identify the Framework-controlled lifecycle condition of the Framework Instrument.

10.4. The Effective Date shall identify the date and time from which the applicable Version or Instrument Status has effect.

10.5. Recognition of a new Version shall not automatically alter the Instrument Status of an earlier Version.

10.6. A change of Instrument Status shall not require a new Version where the text and substantive content of the Framework Instrument remain unchanged.

10.7. A change affecting meaning, scope, requirements, dependencies, responsibility, Status conditions or Controlled Effects shall require a new Version.

10.8. A Framework Instrument shall not have operative effect before:

(a) the applicable recognition or approval decision;

(b) assignment of Instrument Status;

(c) recording of the Effective Date;

(d) authoritative publication through the assigned route.

10.9. The Framework Steward shall preserve the authoritative Version and Instrument Status history of the Main Parts and Annexes.

10.10. The Responsible Actor shall preserve the corresponding history for each subordinate Framework Instrument within its responsibility.

Article 11: Predecessor, successor, replacement and supersession relationships

11.1. A Framework Instrument shall identify its predecessor and successor relationships where applicable.

11.2. A relationship shall distinguish:

(a) amendment of the same Framework Instrument through a new Version;

(b) Replacement by a new Framework Instrument;

(c) supersession by one or more successor instruments;

(d) consolidation of more than one predecessor instrument;

(e) division of one predecessor instrument into more than one successor instrument;

(f) Retirement or Withdrawal without replacement.

11.3. A successor Framework Instrument shall not inherit recognition, Instrument Status, Qualified Status or Controlled Effect from a predecessor unless the applicable Framework Decision expressly assigns the corresponding effect.

11.4. Supersession shall not delete or rewrite the predecessor Framework Instrument or its Historical State.

11.5. A predecessor shall remain identifiable for interpretation, Validation, Review, Remedy and evaluation of earlier Controlled Reliance.

11.6. A replacement or supersession record shall identify:

(a) the predecessor Instrument Identifier and Version;

(b) the successor Instrument Identifier and Version;

(c) the relationship type;

(d) the Effective Date;

(e) the Transition conditions;

(f) the effect on existing dependencies and references.

11.7. A reference to a superseded Framework Instrument shall continue to identify that historical instrument unless the referring instrument is amended or a recognised Version-resolution rule applies.

SECTION 6: CODE GOVERNANCE AND REFERENCES

Article 12: Allocation, change, retirement and non-reuse of codes

12.1. The Framework Steward shall maintain the Instrument Code Catalogue.

12.2. Each Instrument Code Catalogue Entry shall identify:

(a) the code;

(b) the code type;

(c) the controlled group and parent code, where applicable;

(d) the authoritative label and meaning;

(e) the Framework category or function to which it relates;

(f) the permitted instrument or record types;

(g) the Effective Date and Status;

(h) the predecessor, successor and retirement relationships;

(i) the decision reference.

12.3. A code shall be allocated only where:

(a) an existing code does not accurately perform the required function;

(b) the meaning and parent relationship are unambiguous;

(c) the code does not create a category or Controlled Effect not established by the Framework;

(d) the allocation decision is recorded.

12.4. The meaning of an allocated code shall not be changed to represent a different function or category.

12.5. Where the required meaning changes materially, a new code shall be allocated and the earlier code shall be deprecated, retired or superseded through the applicable Change Control route.

12.6. A retired, withdrawn or superseded code shall remain reserved and shall not be reused.

12.7. A new function code within an existing controlled group shall be assigned by the competent Framework Body only where the code does not create a new instrument type, controlled group, Trust Service Category, Trust Object Category, Status category, qualification route or Controlled Effect.

12.8. A new instrument type shall require amendment of Part I and this Annex. A new controlled group shall require amendment of this Annex and of each Main Part whose controlled categories are affected.

12.9. A new Trust Service Category shall require amendment of Parts II and IX before a corresponding function code is assigned.

12.10. A new Trust Object Category shall require amendment of Parts II and VI before a corresponding function code is assigned.

12.11. The Instrument Code Catalogue shall preserve the complete history of allocated, reserved, deprecated, retired, superseded and prohibited codes.

Article 13: Stable legal references and cross-instrument citation

13.1. A legal reference to a Framework Instrument shall identify the stable Instrument Identifier.

13.2. Where the applicable Version is material, the reference shall identify:

(a) the fixed Version; or

(b) the recognised Version-resolution rule.

13.3. A reference to a provision in another Framework Instrument shall identify:

(a) the Instrument Identifier;

(b) the Article;

(c) the paragraph;

(d) the point and sub-point, where applicable;

(e) the Version where required under paragraph 13.2.

13.4. A reference within the same Framework Instrument shall identify the Article and, where required, the paragraph, point and sub-point.

13.5. A reference to an Annex shall use the Annex title or letter together with the Article and paragraph reference and shall not incorporate the Annex letter into the Article number.

13.6. A GitBook link, slug, navigation title, file name or publication location shall support navigation only and shall not replace a legal reference.

13.7. The expressions above, below, previous section and following section shall not be used where a stable legal reference is available.

13.8. Each material cross-reference shall be verified before the referring Framework Instrument acquires operative effect.

13.9. A broken, ambiguous or unresolved cross-reference shall be corrected through Change Control and shall not be interpreted as creating a broader requirement or Controlled Effect.

13.10. Supersession, Migration or relocation of a Framework Instrument shall preserve the ability to resolve historical legal references.

ANNEX C: TRUST OBJECT CLASSIFICATION AND RELATIONSHIP MODEL

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

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Annex establishes the Trust Object classification and relationship model required by Parts II, VI, IX and X.

1.2. This Annex applies to each Trust Object Category established by Part VI and to each Trust Service Output for which Part VI assigns a Trust Object Category and lifecycle.

1.3. This Annex shall be applied together with the category, Status, qualification, dependency, Validation and lifecycle rules established by the Main Parts.

1.4. This Annex shall not:

(a) create a new Trust Object Category or Trust Service Category;

(b) assign recognition, Status, Qualified Status, Authorisation or Controlled Reliance;

(c) convert a Trust Service Output, Source, record or Evidence Artefact into a Trust Object where Part VI does not assign that category;

(d) prescribe a technical format, schema, algorithm, product, protocol or deployment model;

(e) determine the substantive truth, lawfulness, eligibility, entitlement or acceptance of information represented by a Trust Object.

1.5. An Implementation Guideline, Scheme, Profile, Technical Specification or Body Instrument shall preserve the classifications and category boundaries established by this Annex.

Article 2: Trust Object Categories

2.1. The Trust Object Categories established by Part VI shall comprise:

(a) Digital Signature;

(b) Electronic Signature;

(c) Electronic Seal;

(d) Electronic Timestamp;

(e) Certificate;

(f) Electronic Attestation;

(g) Identification Result;

(h) Identity Resolution Result;

(i) Authentication Outcome;

(j) Authorisation Outcome;

(k) Verification Result;

(l) Validation Result;

(m) Status Response;

(n) Exchange Evidence;

(o) Controlled Exchange Result.

2.2. Each Trust Object Category shall be defined according to its stable function and shall remain independent of the sector, programme, Scheme or use case in which the Trust Object is used.

2.3. The Trust Object Catalogue shall record the Categories established by paragraph 2.1 and shall not create, merge, remove or reclassify a Category.

2.4. A Trust Object shall remain separate from:

(a) the Trust Service Provider responsible for the producing Trust Service;

(b) the producing Trust Service;

(c) the Source or evidence basis used;

(d) a Technical Exchange Route through which it is transmitted;

(e) a Humanitarian Trust List Entry or other Status publication;

(f) a local Authorisation, acceptance or Controlled Reliance decision.

2.5. A Trust Service Output shall constitute a Trust Object only where Part VI assigns that output a Trust Object Category, independent identity and lifecycle.

2.6. Representation, encoding, transport, storage, presentation, copying or use in another process shall not change the Trust Object Category.

2.7. A Trust Object shall retain its category where it supports, protects, references or depends on another Trust Object.

Article 3: Object identity, Metadata and lineage

3.1. Each Trust Object shall be independently identifiable within its applicable scope.

3.2. An issued Trust Object shall contain or reference an issuer-scoped Serial Number where the applicable Profile requires one.

3.3. A Trust Object Identifier or Serial Number shall constitute Metadata and shall not, by itself, establish Authenticity, validity, ownership, authority, Status, qualification or Controlled Reliance.

3.4. Trust Object Metadata shall identify, where applicable:

(a) the Trust Object Category;

(b) the Issuer or producing Trust Service;

(c) the Subject, where applicable;

(d) the applicable Profile and Version;

(e) the creation or issuance time;

(f) the Validity Period or Freshness Condition;

(g) the Status reference;

(h) the protection, evidence and dependency references;

(i) the predecessor, successor, replacement or corrective relationship.

3.5. A Version shall identify an immutable state of a Trust Object or Trust Object structure and shall not overwrite an earlier Version.

3.6. A predecessor, successor, replacement, supersession or corrective relationship shall identify each related Trust Object and the Effective Date of the relationship.

3.7. A retired Trust Object Identifier or Serial Number shall not be reassigned within the scope in which uniqueness is required.

3.8. Reference to another Controlled Matter shall not transfer the identity, Status, responsibility, Assurance, Qualified Status or Controlled Effect of that matter to the Trust Object.

SECTION 2: DIGITAL SIGNATURE

Article 4: Digital Signature relationship model

4.1. A Digital Signature shall be the native Trust Service Output of a Digital Signing Service and shall support Integrity Verification and origin binding for identified electronic data.

4.2. A Digital Signature shall identify or reference:

(a) the signed data or an unambiguous representation of that data;

(b) the applicable Digital Signature Validation Data or Certificate;

(c) the applicable Digital Signature Creation Mechanism or Device category;

(d) the algorithm and parameter identifiers required for Validation;

(e) the creation evidence required by the applicable Profile;

(f) the producing Digital Signing Service and the applicable Version of that Service.

4.3. A Digital Signature shall not disclose or directly identify Digital Signature Creation Data.

4.4. A Digital Signature shall remain separate from an Electronic Signature and Electronic Seal.

4.5. A Digital Signature shall support an Electronic Signature or Electronic Seal only where the applicable Profile establishes that dependency.

4.6. Qualified Status assigned to the Digital Signing Service, Certificate, creation mechanism or device shall constitute a dependency condition and shall not transfer to the Digital Signature.

4.7. Restriction, Suspension, Withdrawal or Revocation of a dependency shall affect the Digital Signature only within the scope and time established by the applicable Profile, Status information and Validation basis.

SECTION 3: ELECTRONIC SIGNATURE

Article 5: Electronic Signature relationship model

5.1. An Electronic Signature shall be attributable to a Signatory and shall establish the association between the Signatory, signing act and signed data within the assigned scope.

5.2. An Electronic Signature shall contain or reference:

(a) the Signatory;

(b) the signing purpose and evidence of intent or approval required by the applicable Profile;

(c) the signed data;

(d) the applicable Digital Signature;

(e) the applicable creation mechanism or device;

(f) the Signature Evidence required for Validation;

(g) the producing Electronic Signature Service and the applicable Version of that Service.

5.3. The Digital Signature referred to in paragraph 5.2, point (d), shall remain a separate Trust Object and dependency.

5.4. An Advanced Electronic Signature shall satisfy the linking, identification, Signatory-control, Integrity and Validation-evidence conditions established by Part VI and the applicable Profile.

5.5. A Qualified Electronic Signature shall satisfy the applicable Qualified Object Profile and each required qualified dependency without receiving Qualified Status by transfer from that dependency.

5.6. Signature Evidence shall constitute an Evidence Artefact and shall become a separate Trust Object only where Part VI assigns it a Trust Object Category.

5.7. An Electronic Signature shall not, by itself, create Authorisation, consent to unrelated processing, acceptance of unrelated content or Controlled Reliance outside the assigned signing purpose.

5.8. A lifecycle action affecting an Electronic Signature shall not alter the signed data or another Trust Object to which the Electronic Signature is attached or logically associated.

SECTION 4: ELECTRONIC SEAL

Article 6: Electronic Seal relationship model

6.1. An Electronic Seal shall be attributable to a Seal Creator and shall establish the association between that legal entity, the authorised sealing process and the sealed data within the assigned scope.

6.2. An Electronic Seal shall contain or reference:

(a) the Seal Creator;

(b) the authorised sealing purpose and organisational-control evidence;

(c) the sealed data;

(d) the applicable Digital Signature;

(e) the applicable creation mechanism or device;

(f) the Seal Evidence required for Validation;

(g) the producing Electronic Seal Service and the applicable Version of that Service.

6.3. The Digital Signature referred to in paragraph 6.2, point (d), shall remain a separate Trust Object and dependency.

6.4. An Advanced Electronic Seal shall satisfy the linking, identification, organisational-control, Integrity and Validation-evidence conditions established by Part VI and the applicable Profile.

6.5. A Qualified Electronic Seal shall satisfy the applicable Qualified Object Profile and each required qualified dependency without receiving Qualified Status by transfer from that dependency.

6.6. Seal Evidence shall constitute an Evidence Artefact and shall become a separate Trust Object only where Part VI assigns it a Trust Object Category.

6.7. An Electronic Seal shall evidence origin and Integrity and shall not, by itself, establish the correctness, lawfulness, approval or acceptance of the sealed content.

6.8. A lifecycle action affecting an Electronic Seal shall not alter the sealed data or another Trust Object to which the Electronic Seal is attached or logically associated.

SECTION 5: ELECTRONIC TIMESTAMP

Article 7: Electronic Timestamp relationship model

7.1. An Electronic Timestamp shall bind identified electronic data to an identified time.

7.2. An Electronic Timestamp shall contain or reference:

(a) the data or an unambiguous representation of the data;

(b) the time value;

(c) the applicable time source;

(d) the accuracy and uncertainty required by the applicable Profile;

(e) the Issuer or producing Electronic Timestamp Service;

(f) the protection and Validation evidence;

(g) the applicable Status and Validity Period.

7.3. An Electronic Timestamp shall remain separate from the data and Trust Object that it protects.

7.4. An Electronic Timestamp shall evidence the association between the identified data and time and shall not, by itself, establish the correctness, lawfulness or acceptance of the data.

7.5. A Qualified Electronic Timestamp shall satisfy the applicable Qualified Object Profile and the required qualified time-source, protection and service dependencies.

7.6. Qualified Status of a time source, protection object or Electronic Timestamp Service shall not transfer to the Electronic Timestamp.

7.7. A lifecycle action affecting an Electronic Timestamp shall affect another Trust Object only where the applicable dependency relationship and Validation basis establish that effect.

SECTION 6: CERTIFICATE

Article 8: Certificate relationship model

8.1. A Certificate shall link Digital Signature Validation Data or another controlled value to an identified Subject.

8.2. A Certificate shall contain or reference:

(a) the Subject;

(b) the Issuer;

(c) the validation data or controlled value;

(d) the applicable Profile for Certificates;

(e) the Validity Period;

(f) the Status reference;

(g) the issuer-scoped Serial Number;

(h) the restrictions and intended scope;

(i) the protection and Validation evidence.

8.3. A Certificate shall constitute a specialised Electronic Attestation for issuance purposes and shall retain its separate Certificate category and lifecycle.

8.4. The Electronic Attestation relationship referred to in paragraph 8.3 shall not merge the Certificate category with a general Electronic Attestation category or remove any Certificate-specific requirement.

8.5. A Certificate shall not, by itself, create identity, Role, Authorisation, ownership, eligibility, entitlement or Controlled Reliance beyond the certified association.

8.6. A Qualified Certificate for Electronic Signatures shall link Digital Signature Validation Data to a natural person under the applicable Qualified Profile.

8.7. A Qualified Certificate for Electronic Seals shall link Digital Signature Validation Data to a legal entity under the applicable Qualified Profile.

8.8. Qualified Status of a Certificate shall not transfer to the Subject, Issuer, Trust Service, Digital Signature, Electronic Signature, Electronic Seal or another Trust Object using that Certificate.

8.9. Suspension, Withdrawal, Revocation, Expiry, replacement or supersession of a Certificate shall be reflected through the applicable Status and Validation mechanisms without altering an earlier issued Certificate.

SECTION 7: ELECTRONIC ATTESTATION

Article 9: Electronic Attestation relationship model

9.1. An Electronic Attestation shall contain an Attestation Statement attributable to an identified Attestation Issuer.

9.2. The Electronic Attestation category shall remain independent of the sector, programme, Scheme or use case to which the Attestation Statement relates.

9.3. An Electronic Attestation shall contain or reference:

(a) the Attestation Issuer;

(b) the Subject, where applicable;

(c) the Attestation Statement;

(d) the Source Basis or other evidence basis, where required;

(e) the Trust Object Identifier and issuer-scoped Serial Number;

(f) the issuance time;

(g) the Validity Period or Freshness Condition;

(h) the applicable Assurance information;

(i) the Status reference;

(j) the restrictions, caveats and Reliance Limits;

(k) the applicable Electronic Signature, Electronic Seal or other protection object;

(l) the producing Electronic Attestation Service and the applicable Version of that Service.

9.4. An Advanced Electronic Attestation shall satisfy the attribution, Issuer-identification, Integrity, evidence and Validation conditions established by Part VI and the applicable Attestation Profile.

9.5. A Qualified Electronic Attestation shall satisfy the applicable Qualified Object Profile and each required qualified Trust Service, Source, Certificate, protection and time dependency.

9.6. Qualified Status of the Attestation Issuer, Trust Service, Source, Certificate, Electronic Signature, Electronic Seal, Electronic Timestamp or other dependency shall not transfer to the Electronic Attestation.

9.7. An Electronic Attestation shall not, by itself, create the fact, Attribute, Status, relationship, decision or other matter expressed by the Attestation Statement.

9.8. Issuance of an Identification Result, Identity Resolution Result, Authentication Outcome, Authorisation Outcome, Verification Result, Validation Result, Status Response or Controlled Exchange Result as an Electronic Attestation shall create a separate Electronic Attestation with its own identifier, Issuer, protection, Status and lifecycle.

9.9. The source or decision Actor responsible for the underlying statement shall retain that responsibility unless the applicable Framework Instrument expressly assigns another responsibility.

SECTION 8: IDENTIFICATION RESULT

Article 10: Identification Result relationship model

10.1. An Identification Result shall record the outcome of an Identification Service other than Identity Resolution.

10.2. An Identification Result shall contain or reference:

(a) the producing Identification Service;

(b) the identification purpose;

(c) the evidence and Source Basis used;

(d) the method and Version;

(e) the result and confidence or Assurance information;

(f) the evaluation time and Validity Period;

(g) the limitations, caveats and human-review conditions.

10.3. An Identification Result shall not, by itself, create Authorisation, eligibility, entitlement, access, disclosure permission or a local registration decision outside the assigned scope.

10.4. Where a local registration, Correction or refusal decision follows an Identification Result, that decision shall remain a separate Controlled Matter attributable to the responsible Actor.

10.5. Qualified Status shall apply to an Identification Result only where the applicable Qualified Object Profile and Validation conditions are satisfied.

10.6. Issuance of an Identification Result as an Electronic Attestation shall be governed by Article 9.8.

SECTION 9: IDENTITY RESOLUTION RESULT

Article 11: Identity Resolution Result relationship model

11.1. An Identity Resolution Result shall record a determination concerning relationships between identity records within an assigned scope.

11.2. An Identity Resolution Result shall contain or reference:

(a) the producing Identification Service;

(b) the resolution purpose and search scope;

(c) the evidence and Source Basis used;

(d) the matching method and Version;

(e) the candidate or relationship result and confidence or Assurance information;

(f) the evaluation time and Validity Period;

(g) the limitations, caveats and human-review conditions.

11.3. An Identity Resolution Result shall remain a native output of the Identification Service and shall not be classified as an Electronic Attestation Service output.

11.4. An Identity Resolution Result shall not, by itself, establish identity, registration, eligibility, entitlement, fraud, misconduct, access or Authorisation outside the assigned scope.

11.5. Where a local linking, separation, deduplication, registration, Correction or refusal decision follows an Identity Resolution Result, that decision shall remain a separate Controlled Matter attributable to the responsible Actor.

11.6. Qualified Status shall apply to an Identity Resolution Result only where the applicable Qualified Object Profile and Validation conditions are satisfied.

11.7. Issuance of an Identity Resolution Result as an Electronic Attestation shall be governed by Article 9.8.

SECTION 10: AUTHENTICATION OUTCOME

Article 12: Authentication Outcome relationship model

12.1. An Authentication Outcome shall record whether an asserted identity, Role, origin, device, session, transaction, service, Trust Object or Controlled Interaction has been authenticated within an assigned scope.

12.2. An Authentication Outcome shall contain or reference:

(a) the producing Authentication Service;

(b) the asserted matter;

(c) the Authentication Mechanism;

(d) the evaluation context;

(e) the evidence and Status information used;

(f) the result and Assurance information;

(g) the evaluation time and Validity Period;

(h) the restrictions and caveats.

12.3. A successful Authentication Outcome shall not, by itself, create Authorisation, access, disclosure permission, eligibility, entitlement or Controlled Reliance.

12.4. An Authentication Outcome shall remain separate from the Authenticator, Authentication Mechanism and Subject to which it relates.

12.5. Qualified Status shall apply to an Authentication Outcome only where the applicable Qualified Object Profile and Validation conditions are satisfied.

12.6. Issuance of an Authentication Outcome as an Electronic Attestation shall be governed by Article 9.8.

SECTION 11: AUTHORISATION OUTCOME

Article 13: Authorisation Outcome relationship model

13.1. An Authorisation Outcome shall record whether an identified action, access, disclosure, exchange, service use or Controlled Interaction is permitted within an assigned scope.

13.2. An Authorisation Outcome shall contain or reference:

(a) the producing Authorisation Service;

(b) the requested action;

(c) the evaluation context;

(d) the applicable Authorisation Policy and Version;

(e) the evidence and Status information used;

(f) the result;

(g) the evaluation time and Validity Period;

(h) the restrictions, obligations and caveats.

13.3. An Authorisation Outcome shall not, by itself, execute or enforce the authorised action.

13.4. A Policy Enforcement Function shall remain separate from the Authorisation Outcome and shall apply that Outcome only within the assigned enforcement scope.

13.5. An Authorisation Outcome shall not create Controlled Reliance beyond the action, purpose, scope and Validity Period identified in that Outcome.

13.6. Qualified Status shall apply to an Authorisation Outcome only where the applicable Qualified Object Profile and Validation conditions are satisfied.

13.7. Issuance of an Authorisation Outcome as an Electronic Attestation shall be governed by Article 9.8.

SECTION 12: VERIFICATION RESULT

Article 14: Verification Result relationship model

14.1. A Verification Result shall record the outcome of checking identified information, evidence, Status or relationships against defined conditions.

14.2. A Verification Result shall contain or reference:

(a) the producing Validation and Verification Service;

(b) the verified matter;

(c) the verification basis and applicable Profile Version;

(d) the evidence and Status information used;

(e) the evaluation time;

(f) the result;

(g) the Validity Period;

(h) the restrictions and caveats.

14.3. A Verification Result shall remain separate from the verified matter and shall not create or alter the underlying Status, Source, Trust Object, Authorisation or Controlled Reliance.

14.4. A Verification Result shall not be treated as a Validation Result or Status Response unless Part VI and the applicable Profile assign that separate category.

14.5. Qualified Status shall apply to a Verification Result only where the applicable Qualified Object Profile and Validation conditions are satisfied.

14.6. Issuance of a Verification Result as an Electronic Attestation shall be governed by Article 9.8.

SECTION 13: VALIDATION RESULT

Article 15: Validation Result relationship model

15.1. A Validation Result shall record whether an identified Controlled Matter satisfies the applicable validation basis and Reliance Conditions at an identified time.

15.2. A Validation Result shall contain or reference:

(a) the producing Validation and Verification Service;

(b) the validated matter;

(c) the validation basis and applicable Profile Version;

(d) the evidence, dependencies and Status information used;

(e) the evaluation time;

(f) the result;

(g) the Validity Period;

(h) the restrictions and caveats.

15.3. A Validation Result shall remain separate from the validated matter and shall not create or alter the underlying Status, Source, Trust Object, Authorisation or Controlled Reliance.

15.4. A Validation Result shall be interpreted according to the evaluation time, validation basis, evidence, dependencies, Status information and Validity Period recorded for that Result.

15.5. Qualified Status shall apply to a Validation Result only where the applicable Qualified Object Profile and Validation conditions are satisfied.

15.6. Issuance of a Validation Result as an Electronic Attestation shall be governed by Article 9.8.

SECTION 14: STATUS RESPONSE

Article 16: Status Response relationship model

16.1. A Status Response shall provide authorised Status information concerning an identified Status-Bearing Matter.

16.2. A Status Response shall contain or reference:

(a) the producing Validation and Verification Service;

(b) the Status-Bearing Matter;

(c) the governance record or authorised Status information;

(d) the applicable Status scope;

(e) the evaluation or response time;

(f) the Status value;

(g) the Validity Period;

(h) the restrictions and caveats.

16.3. A Status Response shall disclose only the Status information authorised for the requester, purpose, Status-Bearing Matter and Disclosure Condition.

16.4. A Status Response shall remain separate from the governance record and shall not create, alter, suspend, withdraw, revoke or reinstate the underlying Status.

16.5. Qualified Status shall apply to a Status Response only where the applicable Qualified Object Profile and Validation conditions are satisfied.

16.6. Issuance of a Status Response as an Electronic Attestation shall be governed by Article 9.8.

SECTION 15: EXCHANGE EVIDENCE

Article 17: Exchange Evidence relationship model

17.1. Exchange Evidence shall evidence the processing, transmission, receipt, refusal or failure of a Controlled Interaction.

17.2. Exchange Evidence 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 message or payload reference without unnecessary disclosure of content;

(e) the relevant times;

(f) the Technical Exchange Route and security context;

(g) the processing, delivery or failure state;

(h) the restrictions and caveats.

17.3. Exchange Evidence shall remain separate from the exchanged payload and from each Trust Object or Trust Service Output carried through the interaction.

17.4. 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.

17.5. Qualified Status shall apply to Exchange Evidence only where the applicable Qualified Object Profile and Validation conditions are satisfied.

SECTION 16: CONTROLLED EXCHANGE RESULT

Article 18: Controlled Exchange Result relationship model

18.1. A Controlled Exchange Result shall record the outcome of a Federated Data Exchange Service interaction.

18.2. 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 reference;

(e) the Technical Exchange Route and security context;

(f) the result or delivery state;

(g) the evaluation time and Validity Period;

(h) the restrictions and caveats.

18.3. A Controlled Exchange Result shall remain separate from Exchange Evidence, the exchanged content and any local acceptance or business decision.

18.4. A Controlled Exchange Result shall not, by itself, create access, disclosure permission, acceptance of content, delivery of a substantive benefit or Controlled Reliance.

18.5. Qualified Status shall apply to a Controlled Exchange Result only where the applicable Qualified Object Profile and Validation conditions are satisfied.

18.6. Issuance of a Controlled Exchange Result as an Electronic Attestation shall be governed by Article 9.8.

SECTION 17: TRUST SERVICE OUTPUT RELATIONSHIPS

Article 19: Native Trust Service Outputs and separate object representation

19.1. Annex D shall establish the native Trust Service Outputs of each Trust Service Category.

19.2. This Annex shall determine which native Trust Service Outputs have an independent Trust Object Category and lifecycle under Part VI.

19.3. Creation evidence, Signature Evidence, Seal Evidence, logs, audit records and other Evidence Artefacts shall not become separate Trust Objects unless Part VI assigns them a Trust Object Category.

19.4. Where a native Trust Service Output is represented by an Electronic Attestation, the representation shall constitute a separate Electronic Attestation and shall not reclassify, replace or merge with the original output.

19.5. The separate Electronic Attestation referred to in paragraph 19.4 shall identify or reference:

(a) the original Trust Service Output;

(b) the Attestation Issuer;

(c) the Attestation Statement;

(d) the applicable evidence and Source Basis;

(e) its own Trust Object Identifier and issuer-scoped Serial Number where required;

(f) its own protection, Status and lifecycle.

19.6. A Trust Object shall be qualified independently from the producing Trust Service, supporting Evidence Artefacts and dependent Trust Objects.

19.7. Packaging several Trust Objects or Trust Service Outputs in one technical container shall not merge their categories, Status, lifecycle or qualification.

19.8. Transmission through a Federated Data Exchange Service shall not change the category, Issuer, Status or lifecycle of the transmitted Trust Object or Trust Service Output.

SECTION 18: DEPENDENCIES

Article 20: Trust Object dependency model

20.1. A Trust Object dependency shall identify the relationship between a dependent Trust Object and a supporting Controlled Matter.

20.2. A dependency shall identify, where applicable:

(a) the dependent Trust Object;

(b) the supporting Controlled Matter;

(c) the dependency type;

(d) whether the dependency is mandatory, conditional or optional;

(e) the required Status, Assurance or Qualified Status;

(f) the applicable scope and Validity Period;

(g) the evidence and Validation basis;

(h) the lifecycle and failure effect.

20.3. Dependency types shall include, where applicable:

(a) Issuer dependency;

(b) Source or evidence dependency;

(c) protection-object dependency;

(d) Certificate dependency;

(e) time dependency;

(f) Status dependency;

(g) Trust Service dependency;

(h) creation mechanism or device dependency;

(i) Validation dependency;

(j) Technical Exchange Route dependency.

20.4. A dependency shall not transfer identity, Status, responsibility, Assurance, Qualified Status or Controlled Effect.

20.5. Loss, restriction, Suspension, Withdrawal, Revocation, Expiry or unavailability of a dependency shall affect the dependent Trust Object only within the scope and time established by the applicable Profile and Validation basis.

20.6. Historical evaluation shall use the dependency Status, Version and evidence applicable at the relevant time.

20.7. A Profile shall define the combination and failure rules applicable where a Trust Object depends on more than one supporting Controlled Matter.

SECTION 19: ADVANCED AND QUALIFIED OBJECT CLASSES

Article 21: Advanced and qualified Trust Object classes

21.1. The advanced Trust Object classes established by Part VI shall comprise:

(a) Advanced Electronic Signature;

(b) Advanced Electronic Seal;

(c) Advanced Electronic Attestation.

21.2. An advanced object class shall satisfy the category-specific linking, identification, control, Integrity, evidence and Validation conditions established by Part VI and the applicable Profile.

21.3. Qualified Trust Object Status shall be available for a Trust Object Category only where the applicable Qualified Object Profile defines meaningful qualified conditions for that Category.

21.4. Object-Instance Qualification shall require:

(a) satisfaction of the applicable Qualified Object Profile;

(b) the Trust Service Status required by that Profile;

(c) validity of each required qualified dependency;

(d) availability of the required creation or issuance evidence;

(e) Validation confirming the qualified conditions.

21.5. An individual Trust Object shall not require a separate Framework Decision for Qualified Status unless the Main Parts expressly assign that decision.

21.6. Qualified Status shall apply only to the identified Trust Object and Qualified Scope and shall not transfer to its Issuer, Subject, Trust Service Provider, Trust Service, Source Basis, mechanism, device or dependency.

21.7. Qualified Status assigned under the Framework shall not, by itself, assign External Legal Status or External Legal Effect.

SECTION 20: LIFECYCLE

Article 22: Trust Object lifecycle, Correction and historical validity

22.1. The lifecycle of a Trust Object shall identify, where applicable:

(a) creation;

(b) issuance;

(c) activation;

(d) presentation;

(e) Verification and Validation;

(f) restriction;

(g) Suspension;

(h) Withdrawal or Revocation;

(i) replacement or supersession;

(j) Retention, preservation and archival;

(k) Expiry and closure.

22.2. A signed, sealed, timestamped or otherwise Integrity-protected Trust Object shall not be altered after issuance.

22.3. An error or changed condition shall be addressed through Correction of the underlying record and, where applicable:

(a) replacement;

(b) supersession;

(c) restriction;

(d) Suspension;

(e) Withdrawal;

(f) Revocation;

(g) issuance of a corrective Trust Object;

(h) publication of an applicable Status or caveat.

22.4. Correction of an underlying Source, decision or record shall not alter an existing Trust Object.

22.5. Cessation, restriction, Suspension or Withdrawal of a Trust Service shall not automatically invalidate Trust Objects created before the Effective Date of that lifecycle action.

22.6. A later lifecycle action shall not retrospectively invalidate a Trust Object that satisfied the requirements applicable at its creation or issuance time unless the applicable Framework Decision expressly assigns that effect on a supported evidence basis.

22.7. Individual high-volume Trust Objects shall ordinarily use Status Responses and Validation rather than individual Humanitarian Trust List Entries.

22.8. Historical evidence, Status, Version, dependencies and relationships shall remain reconstructable where required for Validation, Review, Remedy or Controlled Reliance.

ANNEX D: TRUST SERVICE PROVIDER AND TRUST SERVICE CLASSIFICATION MODEL

IDEHA-ANN-SVC-GEN-001 Version: 0.1

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter and scope

1.1. This Annex establishes the common classification and relationship model for Trust Service Providers and the Trust Service Categories established by Part IX.

1.2. The Trust Service Categories governed by this Annex are:

(a) Identification Service;

(b) Authentication Service;

(c) Authorisation Service;

(d) Digital Signing Service;

(e) Electronic Signature Service;

(f) Electronic Seal Service;

(g) Electronic Timestamp Service;

(h) Electronic Attestation Service;

(i) Validation and Verification Service;

(j) Federated Data Exchange Service.

1.3. This Annex shall be applied together with Parts II, III, VIII, IX and X and Annex C.

1.4. This Annex shall not:

(a) create a Trust Service Category, Trust Object Category or qualification route;

(b) assign Trust Service Provider Status, Trust Service Status, Service Permission or Qualified Status;

(c) assign access, disclosure permission, Technical Exchange Permission or Controlled Reliance;

(d) prescribe a standard, protocol, algorithm, product, interface or deployment model;

(e) classify the Humanitarian Trust List, Status Publication, federation discovery, a Register or a Catalogue as a Trust Service.

1.5. A Scheme, Profile, Implementation Guideline, Technical Specification or Body Instrument shall preserve the Trust Service classification and provider-service boundaries established by this Annex.

SECTION 2: TRUST SERVICE PROVIDER AND SERVICE BOUNDARIES

Article 2: Trust Service Provider, Provider Scope and separate Trust Service identity

2.1. A Trust Service Provider shall be recognised within an assigned Provider Scope to provide one or more Trust Services.

2.2. Each Trust Service provided by a Trust Service Provider shall retain its independent:

(a) service identifier;

(b) Trust Service Category;

(c) Service Scope;

(d) Trust Service Status;

(e) Service Permission;

(f) native Trust Service Outputs;

(g) Assurance Conditions;

(h) dependencies;

(i) evidence and records;

(j) lifecycle.

2.3. Trust Service Provider Status shall remain separate from the Status and Service Permission of each Trust Service provided by that Provider.

2.4. Recognition or Qualified Status of a Trust Service Provider shall not, by itself, recognise, activate or qualify a Trust Service.

2.5. Provision of more than one Trust Service by the same Trust Service Provider shall not merge those Trust Services or their outputs, evidence, responsibility, Status or lifecycle.

2.6. Shared personnel, systems, mechanisms, devices, Sources, endpoints or Technical Exchange Routes shall not merge separate Trust Services.

2.7. A technical operator, subcontractor, Intermediary or component provider shall not acquire Trust Service Provider Status solely by supporting a Trust Service.

2.8. The Trust Service Provider shall remain responsible for each Trust Service within the assigned Provider Scope, including where another Actor performs a supporting or outsourced function.

Article 3: Independent recognition, Service Permission and qualification

3.1. A Framework Body shall recognise each Trust Service separately within an identified Service Scope.

3.2. A Trust Service-recognition decision shall identify:

(a) the Trust Service Provider;

(b) the Trust Service Category;

(c) the service identifier;

(d) the Service Scope;

(e) the native Trust Service Outputs;

(f) the applicable Schemes and Profiles;

(g) the material dependencies;

(h) the applicable Assurance Conditions;

(i) the Effective Date and Validity Period;

(j) the lifecycle conditions;

(k) the restrictions and caveats.

3.3. A Trust Service shall operate only where the applicable Framework Decision assigns Service Permission within the recognised Service Scope.

3.4. Recognition, registration, listing, technical availability or successful testing shall not, by itself, assign Service Permission or operational activation.

3.5. Each Trust Service shall be assessed and qualified independently under the applicable service-specific Qualified Profile.

3.6. Qualified Trust Service Status shall require Qualified Trust Service Provider Status, Conformity Assessment and qualified dependencies required by Part IX and Part X.

3.7. Qualified Trust Service Provider Status shall not transfer to a Trust Service, and Qualified Trust Service Status shall not transfer to another Trust Service, Trust Service Output, Trust Object, Source, mechanism, device or component.

3.8. The responsible Framework Body shall publish authorised Trust Service Provider Status and Trust Service Status through the Humanitarian Trust List or another governance-controlled publication mechanism.

3.9. Publication or discovery of a Trust Service shall not, by itself, create Service Permission, access, disclosure, Authorisation, Technical Exchange Permission or Controlled Reliance.

SECTION 3: IDENTIFICATION SERVICE

Article 4: Identification Service classification

4.1. An Identification Service shall establish, verify, maintain or resolve an identification basis concerning an identified Subject within an assigned Service Scope.

4.2. Identification Service Functions shall include, where assigned:

(a) Identity Proofing;

(b) Identity Registration;

(c) person or organisation binding;

(d) Identifier assignment and management;

(e) Identity Resolution;

(f) duplicate detection;

(g) identity-record linking and separation;

(h) identity lifecycle management;

(i) reproofing, recovery and closure.

4.3. The native Trust Service Outputs of an Identification Service shall be:

(a) Identification Results;

(b) Identity Resolution Results.

4.4. Identity Proofing, Identity Registration, Identity Resolution, duplicate detection and identity lifecycle management shall remain functions of the Identification Service and shall not constitute separate Trust Service Categories.

4.5. An Identification Service shall not issue an Electronic Attestation unless the same or another Trust Service Provider separately provides an Electronic Attestation Service for that issuance.

4.6. An Identification Result or Identity Resolution Result shall not, by itself, create Authorisation, access, disclosure permission, eligibility, entitlement, a finding of fraud or a local decision outside the assigned Service Scope.

4.7. The applicable Profile shall define the permitted functions, evidence, Sources, Assurance Conditions, output classes, human-review conditions, accessibility safeguards and lifecycle requirements.

SECTION 4: AUTHENTICATION SERVICE

Article 5: Authentication Service classification

5.1. An Authentication Service shall confirm an asserted identity, Role, origin, device, session, transaction, service, Trust Object or Controlled Interaction within an assigned Service Scope.

5.2. An Authentication Service shall use Authentication Mechanisms governed by the applicable Profile.

5.3. The native Trust Service Output of an Authentication Service shall be an Authentication Outcome.

5.4. The Authentication Outcome shall identify the asserted matter, Authentication Mechanism, context, result, Assurance information, evaluation time, Validity Period, restrictions and caveats.

5.5. A successful Authentication Outcome shall not, by itself, create Authorisation, access, disclosure permission, Controlled Reliance, eligibility, entitlement or Trust Service recognition.

5.6. An Authentication Mechanism or Authenticator shall remain separate from the Authentication Service and Authentication Outcome.

5.7. The applicable Profile shall define the permitted Authentication Mechanisms, Assurance Conditions, risk controls, outcome classes, accessibility safeguards and lifecycle requirements.

SECTION 5: AUTHORISATION SERVICE

Article 6: Authorisation Service classification

6.1. An Authorisation Service shall determine whether an identified action, access, disclosure, exchange, service use or Controlled Interaction is permitted within an assigned Service Scope.

6.2. An Authorisation Service shall evaluate, where applicable:

(a) Authorisation Policies;

(b) Roles and Mandates;

(c) Attributes and Status information;

(d) purpose and context;

(e) Access Conditions;

(f) Disclosure Conditions;

(g) security and safeguard conditions;

(h) Reliance Conditions.

6.3. The native Trust Service Output of an Authorisation Service shall be an Authorisation Outcome.

6.4. Responsibility for defining an Authorisation Policy shall remain with the Actor or Framework Body assigned that responsibility.

6.5. The Policy Decision Function shall evaluate the applicable policy and shall not alter that policy.

6.6. The Policy Enforcement Function shall apply the Authorisation Outcome to the requested action only where an applicable Framework Instrument assigns that function.

6.7. Policy evaluation and policy enforcement shall remain functions associated with Authorisation and shall not constitute separate Trust Service Categories.

6.8. An Authorisation Outcome shall not, by itself, execute or enforce the authorised action or create Controlled Reliance.

SECTION 6: DIGITAL SIGNING SERVICE

Article 7: Digital Signing Service classification

7.1. A Digital Signing Service shall create Digital Signatures through controlled use of Digital Signature Creation Data and an identified Digital Signature Creation Mechanism or Device.

7.2. A Digital Signing Service shall support local or remote creation only within the assigned Service Scope and control model.

7.3. The native Trust Service Outputs of a Digital Signing Service shall be:

(a) a Digital Signature;

(b) the creation evidence required for Validation.

7.4. Creation evidence shall constitute an Evidence Artefact unless Part VI assigns it another Trust Object Category.

7.5. A Digital Signature produced by a Digital Signing Service shall not, by itself, constitute an Electronic Signature or Electronic Seal.

7.6. Digital Signature Creation Data, the creation mechanism or device, the Digital Signature and the Digital Signing Service shall remain separate Controlled Matters with separate responsibility, Status and lifecycle.

7.7. Use of a Qualified Digital Signature Creation Device shall constitute a dependency condition and shall not, by itself, qualify the Digital Signing Service or Digital Signature.

7.8. The applicable Profile shall define the creation-control model, permitted mechanisms and devices, local or remote operation, evidence, key lifecycle, compromise handling and Validation requirements.

SECTION 7: ELECTRONIC SIGNATURE SERVICE

Article 8: Electronic Signature Service classification

8.1. An Electronic Signature Service shall create or manage Electronic Signatures attributable to natural persons within an assigned Service Scope.

8.2. An Electronic Signature Service shall establish the association between:

(a) the Signatory;

(b) the signing act;

(c) the signed data;

(d) the applicable Digital Signature;

(e) the applicable creation mechanism or device;

(f) the evidence of signing intent or approval required by the applicable Profile.

8.3. The native Trust Service Outputs of an Electronic Signature Service shall be:

(a) an Electronic Signature;

(b) Signature Evidence.

8.4. Signature Evidence shall remain an Evidence Artefact and shall not, by itself, constitute an Electronic Signature or separate Trust Service Category.

8.5. Where an Electronic Signature Service depends on a Digital Signing Service, each Trust Service shall retain its independent identity, Status, responsibility, evidence and lifecycle.

8.6. The applicable Profile shall define the Signatory control model, signing intent, permitted creation arrangements, evidence, Validation, accessibility and lifecycle requirements.

8.7. Framework recognition or qualification shall not, by itself, assign External Legal Status or External Legal Effect to an Electronic Signature.

SECTION 8: ELECTRONIC SEAL SERVICE

Article 9: Electronic Seal Service classification

9.1. An Electronic Seal Service shall create or manage Electronic Seals attributable to legal entities within an assigned Service Scope.

9.2. An Electronic Seal Service shall establish the association between:

(a) the Seal Creator;

(b) the authorised sealing process;

(c) the sealed data;

(d) the applicable Digital Signature;

(e) the applicable creation mechanism or device;

(f) the organisational-control evidence required by the applicable Profile.

9.3. The native Trust Service Outputs of an Electronic Seal Service shall be:

(a) an Electronic Seal;

(b) Seal Evidence.

9.4. Seal Evidence shall remain an Evidence Artefact and shall not, by itself, constitute an Electronic Seal or separate Trust Service Category.

9.5. Where an Electronic Seal Service depends on a Digital Signing Service, each Trust Service shall retain its independent identity, Status, responsibility, evidence and lifecycle.

9.6. The applicable Profile shall define the organisational control model, authorised sealing process, permitted creation arrangements, evidence, Validation and lifecycle requirements.

9.7. Framework recognition or qualification shall not, by itself, assign External Legal Status or External Legal Effect to an Electronic Seal.

SECTION 9: ELECTRONIC TIMESTAMP SERVICE

Article 10: Electronic Timestamp Service classification

10.1. An Electronic Timestamp Service shall bind identified electronic data to an identified time within an assigned Service Scope.

10.2. The native Trust Service Output of an Electronic Timestamp Service shall be an Electronic Timestamp.

10.3. The time source, time-control process, protection object and Electronic Timestamp shall remain separately identifiable Controlled Matters.

10.4. An Electronic Timestamp Service shall ensure that the time value, data reference, accuracy, uncertainty, protection and Validation evidence satisfy the applicable Profile.

10.5. The applicable Profile shall define the time-source, accuracy, traceability, protection, evidence, Validity Period, continuity and qualified-dependency requirements.

10.6. Qualified Status assigned to a time source, protection object or dependency shall not transfer to the Electronic Timestamp Service or Electronic Timestamp.

SECTION 10: ELECTRONIC ATTESTATION SERVICE

Article 11: Electronic Attestation Service classification

11.1. An Electronic Attestation Service shall create, issue and manage Electronic Attestations within an assigned Service Scope.

11.2. The native Trust Service Output of an Electronic Attestation Service shall be an Electronic Attestation.

11.3. An Electronic Attestation Service shall remain case-neutral and shall not change category according to the sector, programme, decision or use case to which an Attestation Statement relates.

11.4. A Certificate shall be issued as the specialised Electronic Attestation Category established by Part VI and the applicable Profile for Certificates.

11.5. The applicable Attestation Profile shall determine whether an Electronic Attestation requires:

(a) a Source;

(b) an Authoritative Source;

(c) a Qualified Authoritative Source;

(d) another evidence basis;

(e) no Source dependency.

11.6. An Electronic Attestation Service shall maintain the issuance, Status, Correction, Replacement, Suspension, Withdrawal, Revocation and preservation information required by the applicable Profile.

11.7. An Electronic Attestation Service shall not acquire responsibility for the underlying business, eligibility, entitlement, assessment, programme or local decision solely by issuing an Electronic Attestation representing that matter.

11.8. Issuance of another Trust Service Output as an Electronic Attestation shall create a separate Electronic Attestation in accordance with Annex C.

SECTION 11: VALIDATION AND VERIFICATION SERVICE

Article 12: Validation and Verification Service classification

12.1. A Validation and Verification Service shall verify identified properties, validate identified Controlled Matters or provide authorised Status information within an assigned Service Scope.

12.2. The native Trust Service Outputs of a Validation and Verification Service shall be:

(a) Verification Results;

(b) Validation Results;

(c) Status Responses.

12.3. Verification, Validation and Status evaluation shall remain functions of the Validation and Verification Service and shall not constitute separate Trust Service Categories.

12.4. Where evaluation depends on governance Status, the Validation and Verification Service shall use Status information authorised or published by the responsible Framework Body, including the Humanitarian Trust List where applicable.

12.5. Operation of a Validation and Verification Service shall not transfer governance, Decision Competence or Status Publication responsibility for the Humanitarian Trust List to the Trust Service Provider.

12.6. A Verification Result, Validation Result or Status Response shall not create or alter the underlying Status, Source, Trust Object, Authorisation, policy, Framework Decision or Controlled Reliance.

12.7. The applicable Profile shall define the evaluated matters, evaluation basis, evidence, Status information, result classes, Validity Periods, restrictions, caveats and historical-validation requirements.

SECTION 12: FEDERATED DATA EXCHANGE SERVICE

Article 13: Federated Data Exchange Service classification

13.1. A Federated Data Exchange Service shall provide controlled exchange of requests, responses, Trust Objects, Trust Service Outputs and Exchange Evidence between recognised Actors or Federation Domains within an assigned Service Scope.

13.2. The native Trust Service Outputs of a Federated Data Exchange Service shall be:

(a) Exchange Evidence;

(b) Controlled Exchange Results.

13.3. A Federated Data Exchange Service shall provide, according to the applicable Profile:

(a) identification and Authentication of participating endpoints;

(b) route and destination resolution;

(c) Transport Confidentiality;

(d) Payload Confidentiality where required;

(e) Integrity and Authenticity protection;

(f) request and response correlation;

(g) replay and duplicate-message controls;

(h) exchange-status and error handling;

(i) continuity and Recovery controls.

13.4. Delivery evidence shall remain a subordinate exchange-evidence function and shall not constitute a separate Trust Service Category.

13.5. A Federated Data Exchange Service shall use Humanitarian Trust List and federation-discovery information only as authorised by the responsible Framework Body.

13.6. A Federated Data Exchange Service shall not operate, control or assign Status through the Humanitarian Trust List.

13.7. A Federated Data Exchange Service shall not, by itself, create access, disclosure permission, acceptance of content, a business decision, Source Status, Trust Service Status or Controlled Reliance.

13.8. An Authorisation Service or local Policy Enforcement Function shall determine and enforce the applicable exchange permission where required.

SECTION 13: COMPOSITION AND SHARED IMPLEMENTATION

Article 14: Trust Service composition and separate responsibility

14.1. One Controlled Interaction shall invoke more than one Trust Service where the applicable Scheme and Profiles assign that composition.

14.2. A composite implementation shall identify each constituent Trust Service, Trust Service Provider, Service Scope, Service Permission, native output, dependency and responsibility.

14.3. A shared user interface, workflow, endpoint, infrastructure component, transaction identifier or operational team shall not merge the constituent Trust Services.

14.4. Each constituent Trust Service shall remain separately recognisable, assessable, qualifiable, supervisable and subject to its own lifecycle.

14.5. A composite service label, product name or procurement package shall not create a new Trust Service Category.

14.6. Failure or non-conformity of one constituent Trust Service shall affect another constituent Trust Service only where an identified dependency or Framework Decision establishes that effect.

14.7. A Trust Service Provider shall maintain evidence sufficient to distinguish:

(a) the function performed by each Trust Service;

(b) the input and native output of each Trust Service;

(c) the systems, mechanisms and devices used;

(d) the applicable Status and qualified dependencies;

(e) the Actor responsible for each function and output.

14.8. Integrated operation shall not transfer responsibility for a local Authorisation, acceptance under a Local Trust Acceptance Policy or Controlled Reliance decision to another Trust Service.

SECTION 14: DEPENDENCIES

Article 15: Trust Service dependencies and propagation

15.1. A Trust Service dependency shall identify the relationship between a dependent Trust Service and each supporting Controlled Matter required for its operation, outputs, Assurance or Status.

15.2. A Trust Service dependency shall include, where applicable:

(a) another Trust Service;

(b) a Trust Service Provider or supporting Provider;

(c) a Source or Source Basis;

(d) a Trust Object or Trust Service Output;

(e) a creation mechanism or device;

(f) an Authentication Mechanism or Authorisation Policy;

(g) a Technical Exchange Route or endpoint;

(h) governance Status or Humanitarian Trust List information;

(i) an applicable Framework Instrument or Recognised Standard.

15.3. A dependency record shall identify:

(a) the dependent Trust Service;

(b) the supporting Controlled Matter;

(c) the dependency type and scope;

(d) the required Status, Assurance or qualification condition;

(e) the applicable Version;

(f) the lifecycle and failure effect;

(g) the Responsible Actor.

15.4. A dependency shall not transfer identity, Trust Service Provider Status, Trust Service Status, Service Permission, Assurance, Qualified Status, responsibility or Controlled Effect.

15.5. Loss, restriction, Suspension, Withdrawal, Revocation, expiry or unavailability of a dependency shall affect the dependent Trust Service only where the applicable Profile, Service Permission or Framework Decision establishes that effect.

15.6. Loss, restriction, Suspension or Withdrawal of the Trust Service Provider Status required for a Trust Service shall trigger restriction, Suspension or Review of the dependent Service Permission within the affected Provider Scope.

15.7. Use of a qualified dependency shall not, by itself, establish Qualified Trust Service Status.

15.8. A Trust Service Provider shall monitor each material dependency and retain the evidence required to evaluate its current and Historical State.

SECTION 15: LIFECYCLE AND CASE NEUTRALITY

Article 16: Trust Service lifecycle and historical treatment

16.1. The lifecycle of a Trust Service shall identify, where applicable:

(a) proposal and assessment;

(b) recognition;

(c) assignment of Service Permission;

(d) operational activation;

(e) operation and surveillance;

(f) restriction;

(g) Suspension;

(h) Withdrawal;

(i) cessation;

(j) Transition, Replacement or supersession;

(k) archival and historical treatment.

16.2. A lifecycle action shall identify the affected Trust Service and Service Scope and shall not automatically apply to another Trust Service provided by the same Provider.

16.3. Restriction, Suspension, Withdrawal or cessation of a Trust Service shall be published by the responsible Framework Body where publication is authorised.

16.4. A Trust Service Provider shall preserve the records, Status information, Validation dependencies and evidence required after restriction, Suspension, Withdrawal or cessation.

16.5. Restriction, Suspension, Withdrawal or cessation shall not automatically invalidate Trust Objects or Trust Service Outputs created before the Effective Date of that action.

16.6. The applicable Profile shall define the effect of a lifecycle action on:

(a) new requests;

(b) existing Controlled Interactions;

(c) existing Trust Objects and Trust Service Outputs;

(d) continuing Status Responses and Validation;

(e) transition, replacement and preservation;

(f) Review and Remedy.

16.7. Historical Trust Service Status, Service Scope, Service Permission, Versions and dependencies shall remain reconstructable where required for Validation, Review, Remedy or Controlled Reliance.

Article 17: Case neutrality, subordinate functions and controlled extension

17.1. A Trust Service Category shall be defined by its stable function and native outputs and shall not change according to a sector, programme, business process or use case.

17.2. A Scheme shall select the Trust Services required for an identified purpose without redefining or merging their Categories.

17.3. A Profile shall select the requirements, options, Assurance Conditions, dependencies and lifecycle conditions applicable to an existing Trust Service Category.

17.4. A subordinate Trust Service Function shall remain mapped to its parent Trust Service Category in the Instrument Code Catalogue.

17.5. The following functions shall remain within their assigned parent categories:

(a) Identity Proofing, Identity Registration, Identity Resolution and identity lifecycle management within the Identification Service;

(b) policy evaluation within the Authorisation Service;

(c) Status evaluation within the Validation and Verification Service;

(d) delivery evidence within the Federated Data Exchange Service.

17.6. Humanitarian Trust List publication, federation discovery, Register operation and Catalogue operation shall remain Framework Governance Functions and shall not constitute Trust Services.

17.7. Preservation, archival and evidence retention shall remain horizontal lifecycle functions unless the Main Parts establish a separate Trust Service Category through amendment.

17.8. A specialised implementation, product, workflow or contractual service shall not create a new Trust Service Category by name or configuration.

17.9. A new subordinate function within an existing Trust Service Category shall be governed through the applicable Framework Instrument and Instrument Code Catalogue where it does not alter the parent Category or Controlled Effect.

17.10. A new Trust Service Category shall require amendment of Parts II and IX and corresponding amendment of this Annex.

ANNEX E: SOURCE AND AUTHORITATIVE SOURCE MODEL

IDEHA-ANN-SRC-GEN-001 Version: 0.1

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter, Source boundaries and Status model

1.1. This Annex establishes the common model applicable to Sources, Authoritative Sources and Qualified Authoritative Sources under Parts II, VII and X.

1.2. The Source model shall distinguish:

(a) a recognised Source and its Source Status;

(b) an Authoritative Source and its Authoritative Source Status;

(c) a Qualified Authoritative Source and its Qualified Authoritative Source Status.

1.3. A Source shall remain separate from:

(a) a Trust Service Provider;

(b) a Trust Service;

(c) a Trust Service Output;

(d) a Trust Object;

(e) a Technical Exchange Route;

(f) a Humanitarian Trust List Entry;

(g) a local Authorisation or Controlled Reliance decision.

1.4. Recognition, use, copying, technical availability, registration, publication or exchange of a Source shall not, by itself, assign Authoritative Source Status, Qualified Authoritative Source Status, access, disclosure permission, Service Permission, Technical Exchange Permission or Controlled Reliance.

1.5. A Source shall support one or more Trust Services or other authorised functions only within its recognised Source Scope and applicable conditions.

1.6. A Trust Service Output or Trust Object shall require a Source dependency only where the applicable Profile assigns that dependency.

1.7. This Annex shall not:

(a) define particular data elements, sector datasets, code lists or programme indicators;

(b) prescribe technical schemas, formats, protocols, interfaces or algorithms;

(c) designate a Source or assign Source Status;

(d) authorise access, disclosure, exchange or Controlled Reliance;

(e) convert a Source into a Trust Service, Trust Service Output or Trust Object.

Article 2: Source Profiles

2.1. Each recognised Source shall be governed by an applicable Source Profile.

2.2. A Source Profile shall identify:

(a) the Source and its Identifier;

(b) the Source Holder and Source Steward;

(c) the mandate and recognised purpose;

(d) the Source Scope;

(e) the information, Attribute, Subject or record categories maintained by the Source;

(f) the applicable semantic model, definitions, classifications, taxonomies, controlled vocabularies and code lists;

(g) the Data Quality and Freshness Conditions;

(h) the Provenance and evidence requirements;

(i) the permitted collection, creation, import, transformation, aggregation and derivation methods;

(j) the Access Conditions and Disclosure Conditions;

(k) the permitted Trust Service uses and outputs;

(l) the Correction, Review and Remedy Routes;

(m) the security, retention, archival and lifecycle conditions;

(n) the applicable Assurance Conditions and dependencies.

2.3. A Source Profile shall identify each condition applicable only to part of the Source Scope.

2.4. A Qualified Profile for an Authoritative Source shall identify the additional qualified conditions, Conformity Assessment requirements, surveillance requirements and Qualified Scope.

2.5. A Source Profile or Qualified Profile shall not, by itself, assign Source Status, Authoritative Source Status or Qualified Authoritative Source Status.

2.6. A Technical Specification shall establish the technical schemas, formats, validation rules, interfaces and implementation parameters selected by the Source Profile where such requirements are necessary.

2.7. A change to a Source Profile shall be managed under Part XIII and shall not silently change the meaning or Status of information created under an earlier Version.

Article 3: Source Holder, Source Steward and responsibility separation

3.1. A Source Holder shall maintain and operate the Source within the recognised Source Scope and in accordance with the applicable Source Profile.

3.2. A Source Holder shall remain responsible for:

(a) operational custody and availability of the Source;

(b) implementation of access, disclosure and security controls;

(c) recording of material creation, update, Correction and lifecycle events;

(d) preservation of operational Provenance and evidence;

(e) notification of material changes, incidents and non-conformities.

3.3. A Source Steward shall remain responsible, within its assigned scope, for:

(a) the mandate and recognised purpose of the Source;

(b) semantic definitions and relationships;

(c) classifications, taxonomies, controlled vocabularies and code lists;

(d) Data Quality requirements and evaluation rules;

(e) Provenance and derivation requirements;

(f) Correction and conflict-resolution conditions;

(g) lifecycle and change proposals affecting the Source Profile.

3.4. Where the same Actor performs the Source Holder and Source Steward functions, the responsibilities, evidence and controls applicable to each function shall remain separately identifiable.

3.5. A Source Holder or Source Steward shall not acquire Trust Service Provider Status, Authoritative Source Status, Qualified Authoritative Source Status or Decision Competence by reason only of performing that function.

3.6. Outsourcing of a Source function shall not remove the responsibility assigned to the Source Holder or Source Steward.

3.7. A Source Profile shall identify the Responsible Actor for each material Source function where responsibility is distributed between more than one Actor.

SECTION 2: SOURCE DESIGNATION, QUALIFICATION AND SCOPE

Article 4: Source Designation and Authoritative Source Status

4.1. A Source shall have Authoritative Source Status only through Source Designation by a Framework Body acting within its Decision Competence.

4.2. A Source Designation decision shall identify:

(a) the Source and Source Holder;

(b) the authoritative Source Scope;

(c) the information for which the Source is authoritative;

(d) the recognised purpose;

(e) the evidence supporting the designation;

(f) the applicable Data Quality, semantic, Provenance, Freshness, security and Assurance Conditions;

(g) the Effective Date and review date;

(h) the restrictions, caveats and Reliance Limits;

(i) the Correction, restriction, Suspension and Withdrawal conditions;

(j) the applicable Status Publication arrangement.

4.3. The designation evidence shall identify the basis on which the Source maintains the information within the authoritative Source Scope, including where applicable:

(a) direct creation or registration by the Source under its mandate;

(b) direct receipt from the originating Actor or system;

(c) controlled incorporation from another recognised Source or Authoritative Source;

(d) derivation from identified Source information under a governed rule.

4.4. The bases referred to in paragraph 4.3 shall describe Provenance and shall not create additional Source Status categories.

4.5. Authoritative Source Status shall apply only to the identified Source and authoritative Source Scope.

4.6. Information outside the authoritative Source Scope shall not be treated as authoritative by reason only of its inclusion in the same Source.

4.7. A copy, extract, replica, transformation, aggregation or derivative shall not inherit Authoritative Source Status.

4.8. Authoritative Source Status shall not, by itself, create access, disclosure permission, Authorisation, Service Permission, Technical Exchange Permission or Controlled Reliance.

Article 5: Qualified Authoritative Source Status

5.1. An Authoritative Source shall have Qualified Authoritative Source Status only through Decision-Based Qualification in accordance with Part X.

5.2. Qualified Authoritative Source Status shall require:

(a) an applicable Qualified Profile for the Authoritative Source;

(b) satisfaction of the applicable Data Quality, semantic, Provenance, security, continuity and lifecycle conditions;

(c) completion of the required Conformity Assessment;

(d) resolution of each material non-conformity;

(e) a recorded evidence basis;

(f) a Framework Decision assigning Qualified Authoritative Source Status and Qualified Scope.

5.3. The Qualified Scope shall identify each data, Subject, population, geographic, organisational, temporal, purpose and operational boundary to which Qualified Authoritative Source Status applies.

5.4. Qualified Authoritative Source Status shall not transfer to:

(a) the Source Holder;

(b) the Source Steward;

(c) a Trust Service using the Source;

(d) a Trust Service Output based on the Source;

(e) a Trust Object referring to the Source;

(f) a copy, extract, transformation, aggregation or derivative;

(g) another Source within the same system or organisation.

5.5. A material change affecting the Qualified Scope, Provenance, Data Quality, semantics, security, continuity or lifecycle shall trigger reassessment before Qualified Authoritative Source Status continues to apply to the changed matter.

5.6. The competent Framework Body shall publish authorised Qualified Authoritative Source Status through the Humanitarian Trust List or another governance-controlled publication mechanism where publication is authorised.

5.7. Publication shall communicate Qualified Authoritative Source Status and shall not create that Status.

Article 6: Source Scope

6.1. A Source Scope shall define the precise boundary within which Source Status applies.

6.2. The Source Scope shall identify, where applicable:

(a) the data elements, Attributes, information or record categories;

(b) the Subject or object categories;

(c) the population scope;

(d) the geographic scope;

(e) the organisational scope;

(f) the temporal scope;

(g) the recognised purpose;

(h) the permitted functions and Trust Service uses;

(i) the restrictions and exclusions.

6.3. Source Status applying to one element, category, population, territory, organisation, period or purpose shall not imply Source Status outside that boundary.

6.4. A Source Scope shall distinguish information for which the Source is authoritative from information that is informative, imported, derived, provisional, disputed or outside the authoritative scope.

6.5. Overlapping Source Scopes shall be recognised only where the applicable Source Profiles and Framework Decisions define:

(a) the relationship between the Sources;

(b) the purpose for which each Source is used;

(c) the treatment of consistency and conflict;

(d) the applicable precedence, escalation and Review conditions;

(e) the effect on Trust Service Outputs and Controlled Reliance.

6.6. Resolution of conflicting Source information shall not alter Source Status unless a Framework Decision assigns that Controlled Effect.

6.7. A Relying Actor shall determine acceptance of Source information within its applicable Trust Acceptance Policy and shall not alter the Source Status assigned by a Framework Body.

SECTION 3: QUALITY, SEMANTICS, PROVENANCE AND TIME

Article 7: Data Quality and semantic governance

7.1. A Source Holder shall maintain Data Quality in accordance with the applicable Source Profile.

7.2. The applicable Source Profile shall define the required conditions concerning:

(a) accuracy;

(b) completeness;

(c) consistency;

(d) validity;

(e) uniqueness;

(f) currentness and timeliness;

(g) traceability;

(h) semantic consistency;

(i) Correction.

7.3. Data Quality shall be evaluated within the Source Scope and for the recognised purpose and shall not be inferred from a general quality statement applying to another scope or purpose.

7.4. A Source Steward shall govern the semantic artefacts required to interpret Source information, including where applicable:

(a) canonical definitions;

(b) concept and relationship models;

(c) ontologies;

(d) taxonomies and classifications;

(e) controlled vocabularies and code lists;

(f) multilingual labels and script representations;

(g) rules for cardinality, validity and permitted value states.

7.5. Estimated, approximate, incomplete, disputed, unverified, derived, unknown, unavailable, withheld and not-applicable values shall remain distinguishable where those states are relevant to interpretation or reliance.

7.6. A semantic change shall identify the affected concept, earlier and later meaning, Version, Effective Date, compatibility condition and migration treatment.

7.7. A semantic change shall not retrospectively alter the meaning of information created under an earlier Version.

7.8. A quality or semantic limitation capable of affecting Trust Service use or Controlled Reliance shall be recorded and made available through the applicable Profile, Source evidence or output caveat.

Article 8: Provenance, copying, transformation, aggregation and derivation

8.1. Provenance shall enable reconstruction of the origin, custody, generation, import, transformation, Correction, supersession and lifecycle of Source information.

8.2. Provenance shall identify, where applicable:

(a) the originating Source, Actor or system;

(b) the method and time of creation or collection;

(c) the responsible Actor or automated function;

(d) each import, copy, extraction or replication event;

(e) each material transformation, normalisation or aggregation;

(f) each derivation rule and Version;

(g) each Correction, supersession or replacement;

(h) the applicable Source Status, Source Scope and Version at the relevant time.

8.3. A copy, extract or replica shall identify the originating Source and the conditions under which synchronisation, Correction and Status changes are propagated.

8.4. A transformation or aggregation shall identify:

(a) each input Source or record;

(b) the transformation or aggregation rule;

(c) the rule Version;

(d) the responsible Actor or system;

(e) the processing time;

(f) each material quality or semantic effect;

(g) the conditions for Correction and reprocessing.

8.5. A derived value shall identify:

(a) each Source value on which it depends;

(b) the derivation rule and Version;

(c) the derivation time;

(d) the responsible Actor or system;

(e) the quality, Freshness and uncertainty conditions;

(f) the conditions for re-derivation.

8.6. A copy, extract, replica, transformation, aggregation or derivative shall constitute a separate Controlled Matter where independently maintained or relied upon.

8.7. A separate Controlled Matter referred to in paragraph 8.6 shall require separate Source recognition where it is to be treated as a Source.

8.8. Provenance information shall be protected against unauthorised alteration and retained for the period required for Validation, Review, Remedy and Historical State reconstruction.

Article 9: Freshness, Version and Historical State

9.1. Source information used for an identified purpose shall satisfy the applicable Freshness Condition.

9.2. A Freshness Condition shall identify:

(a) the relevant event or observation time;

(b) the record creation or update time;

(c) the maximum permitted age or review interval;

(d) the conditions requiring re-verification or re-collection;

(e) the treatment of unavailable or stale information.

9.3. Event time, record time, update time, retrieval time, Verification time and Trust Object issuance time shall remain distinguishable where relevant to the purpose.

9.4. A Version of a Source shall identify an immutable state of the Source structure, semantics, rules or controlled content to which that Version applies.

9.5. A later Version of a Source shall not overwrite the Historical State required to evaluate an earlier Trust Service Output, Trust Object, decision or Controlled Reliance.

9.6. Historical State shall identify, where applicable:

(a) the Version of the Source;

(b) the Source Status and Source Scope;

(c) the semantic and quality rules;

(d) the relevant records and Provenance;

(e) the applicable restrictions, caveats and dependencies;

(f) the Effective Date and period of application.

9.7. A later Correction or Status change shall not retrospectively alter an earlier Historical State unless an authorised decision assigns that effect on a recorded evidence basis.

SECTION 4: ACCESS, VERIFICATION, LIFECYCLE AND CROSS-DOMAIN USE

Article 10: Access, disclosure and purpose boundaries

10.1. Access to a Source shall remain separate from disclosure, Trust Service use, Technical Exchange Permission, Authorisation and Controlled Reliance.

10.2. A Source Holder shall provide access or disclosure only where:

(a) the Requesting Actor is identified and authenticated as required;

(b) the purpose is authorised;

(c) the applicable Access Conditions are satisfied;

(d) the applicable Disclosure Conditions are satisfied;

(e) the information is limited to what is necessary for the authorised purpose;

(f) the applicable security and Protected-Person Safeguards are satisfied;

(g) the required evidence is recorded.

10.3. A Technical Exchange Route, Endpoint, discovery record or successful Authentication Outcome shall not, by itself, create access or disclosure permission.

10.4. Source recognition, Authoritative Source Status or Qualified Authoritative Source Status shall not, by itself, create access or disclosure permission.

10.5. A Source Holder shall enforce purpose, access, disclosure, onward-use, retention and deletion conditions within its responsibility.

10.6. A Trust Service Provider using a Source shall remain responsible for compliance with the Service Scope, applicable Profile and Authorisation Outcome.

10.7. A Relying Actor shall remain responsible for acceptance and Controlled Reliance under its applicable Trust Acceptance Policy.

10.8. Cross-domain access shall not circumvent the controls of the originating or receiving Federation Domain.

10.9. Access, disclosure, refusal and restriction decisions having a material effect shall remain attributable, traceable and reviewable.

Article 11: Source Verification and separate representation

11.1. Source Verification shall evaluate specified properties of a Source or Source Basis within the Service Scope of a Validation and Verification Service.

11.2. Source Verification shall identify, where applicable:

(a) the Source and Source Scope;

(b) the Source Status and relevant Effective Date;

(c) the property or condition evaluated;

(d) the evidence and Status information used;

(e) the applicable Profile and Version;

(f) the evaluation time and Freshness Condition;

(g) the Verification Result;

(h) each limitation, caveat and indeterminate condition.

11.3. Source Verification shall produce a Verification Result and shall not alter the Source, Source Status, Source Scope or underlying Source record.

11.4. A Verification Result shall not, by itself, assign Authoritative Source Status, Qualified Authoritative Source Status, access, disclosure permission, Authorisation or Controlled Reliance.

11.5. Where Source information or a Verification Result is represented in an Electronic Attestation, the Electronic Attestation shall constitute a separate Trust Object issued through an Electronic Attestation Service.

11.6. The Electronic Attestation referred to in paragraph 11.5 shall have its own Issuer, Identifier, Serial Number, Profile, Status, protection, dependencies and lifecycle.

11.7. Issuance of an Electronic Attestation shall not convert the Source, Source record or Verification Result into an Electronic Attestation.

11.8. Unavailability of a Source or required evidence shall produce the indeterminate or unavailable outcome defined by the applicable Profile and shall not be represented as a negative factual determination without an evidence basis.

11.9. Historical Source Verification shall use the Source Status, Source Scope, Version, semantics, Provenance and evidence applicable at the relevant time.

Article 12: Correction, lifecycle and cross-domain recognition

12.1. A recognised Source shall have accessible Correction, Review and Remedy Routes proportionate to its purpose, Source Scope and potential Controlled Effects.

12.2. A Correction record relating to a Source shall identify:

(a) the affected Source information;

(b) the error, omission or inconsistency;

(c) the evidence basis;

(d) the corrected information;

(e) the Effective Date;

(f) the responsible Actor;

(g) the effect on dependent Controlled Matters;

(h) the required notification or re-evaluation.

12.3. Correction of Source information shall not alter an existing signed, sealed, timestamped or otherwise integrity-protected Trust Object or Trust Service Output.

12.4. Where corrected Source information affects an existing Trust Service Output or Trust Object, the responsible Actor shall apply the applicable re-evaluation, replacement, supersession, restriction, Suspension, Withdrawal, Revocation, notification or corrective-issuance procedure.

12.5. A Framework Body shall restrict, suspend, withdraw or reinstate Source Status only within its Decision Competence and on a recorded evidence basis.

12.6. A Source lifecycle action shall affect a dependent Trust Service, Trust Service Output or Trust Object only through an identified dependency and within the affected scope and time.

12.7. Restriction, Suspension or Withdrawal of Source Status shall not automatically invalidate a Trust Service Output or Trust Object created before the Effective Date of that action.

12.8. Cross-domain recognition and use of a Source shall identify:

(a) the originating and receiving Federation Domains;

(b) the Source Status and Source Scope;

(c) the Federation Trust Relationship;

(d) the recognised purpose;

(e) the Access Conditions, Disclosure Conditions and Reliance Conditions;

(f) the Correction, Review, Remedy and incident-coordination routes.

12.9. Source Status in one Federation Domain shall not automatically create equivalent Source Status in another Federation Domain.

12.10. The competent Framework Body in the receiving Federation Domain shall determine recognition within its Decision Competence, and each Relying Actor shall determine acceptance under its applicable Trust Acceptance Policy.

12.11. Cross-domain coordination shall not transfer Decision Competence between Federation Domains unless a Federation Agreement expressly assigns that Decision Competence.

12.12. Historical Source Status, Version, Provenance, Correction and cross-domain recognition information shall remain reconstructable for Validation, Review, Remedy and Controlled Reliance.

ANNEX F: ASSURANCE, CONFORMITY ASSESSMENT AND QUALIFICATION MODEL

IDEHA-ANN-ASR-GEN-001 Version: 0.1

SECTION 1: GENERAL PROVISIONS AND ASSURANCE

Article 1: Subject matter and separation of functions

1.1. This Annex establishes the common model applicable to Assurance, Conformity Assessment and Qualification under Parts III, IV, VI, VII, VIII, IX and X.

1.2. Assurance, Conformity Assessment, Qualification, recognition, supervision, Status Publication and Controlled Reliance shall remain separate functions and Controlled Effects.

1.3. An Assurance outcome shall not, by itself, constitute:

(a) a Conformity Assessment Result;

(b) recognition;

(c) Service Permission or operational activation;

(d) a qualification decision;

(e) Qualified Status;

(f) permission for Controlled Reliance.

1.4. A Conformity Assessment Result shall not, by itself, assign recognition, Qualified Status, Service Permission, Technical Exchange Permission or Controlled Reliance.

1.5. Qualified Status shall arise only through:

(a) Decision-Based Qualification for an eligible governance Status; or

(b) Object-Instance Qualification for an eligible individual Trust Object or Trust Service Output.

1.6. Qualification shall apply only to the identified Status-Bearing Matter and Qualified Scope.

1.7. This Annex shall not:

(a) create a Trust Service Category, Trust Object Category or qualification route;

(b) designate a Conformity Assessment Body or assign Qualified Status;

(c) prescribe a named assessment standard, test method, algorithm, product or certification scheme;

(d) establish equivalence with an External Legal Status or External Legal Effect;

(e) authorise access, disclosure, operational activation or Controlled Reliance.

Article 2: Assurance Objects and Assurance Domains

2.1. Assurance shall be assigned to an identified Assurance Object within an identified Assurance Domain.

2.2. An Assurance Object shall be a Controlled Matter identified by the applicable Profile.

2.3. An Assurance Domain shall identify the subject area within which confidence is evaluated.

2.4. The applicable Profile shall identify, where relevant, Assurance Domains concerning:

(a) governance and responsibility;

(b) functional performance;

(c) identity, attribution or control;

(d) Source and Data Quality;

(e) security and Confidentiality;

(f) operational resilience and Continuity;

(g) evidence, Provenance and traceability;

(h) lifecycle and Status control;

(i) another domain required for the recognised purpose.

2.5. Assurance assigned in one Assurance Domain shall not automatically apply in another Assurance Domain.

2.6. Assurance assigned to one Assurance Object shall not transfer to another Assurance Object.

2.7. The applicable Profile shall identify:

(a) the Assurance Object;

(b) each applicable Assurance Domain;

(c) the Assurance Conditions;

(d) the evidence basis;

(e) the evaluation method;

(f) the outcome classes;

(g) the Validity Period or review condition;

(h) each limitation, caveat and dependency.

2.8. The same Controlled Matter shall have different Assurance outcomes in different Assurance Domains where the applicable evidence and conditions support those outcomes.

Article 3: Assurance Levels

3.1. The Framework shall recognise Low, Substantial and High Assurance Levels.

3.2. A Low Assurance Level shall indicate limited confidence that the Assurance Object satisfies the applicable Assurance Conditions.

3.3. A Substantial Assurance Level shall indicate substantial confidence that the Assurance Object satisfies the applicable Assurance Conditions.

3.4. A High Assurance Level shall indicate high confidence that the Assurance Object satisfies the applicable Assurance Conditions.

3.5. The applicable Profile shall define the requirements, evidence and evaluation method for each Assurance Level within the relevant Assurance Domain.

3.6. Assignment of the same Assurance Level in different Assurance Domains, Profiles, Schemes or Federation Domains shall not establish equivalence unless an applicable Framework Instrument expressly establishes the mapping and evidence basis.

3.7. An Assurance Level shall not be inferred from:

(a) recognition of an Actor, Source, Provider or Trust Service;

(b) inclusion in a Register, Catalogue or Humanitarian Trust List;

(c) technical availability or successful testing;

(d) the Assurance Level of a dependency;

(e) the Qualified Status of another Controlled Matter.

3.8. A High Assurance Level shall not, by itself, create Qualified Status.

3.9. A Qualified Profile shall identify the Assurance Levels required for the qualified category and Qualified Scope.

Article 4: Assurance evidence, limitations and composite evaluations

4.1. An Assurance outcome shall be supported by evidence appropriate to the Assurance Object, Assurance Domain, recognised purpose and evaluation time.

4.2. Assurance evidence shall be:

(a) relevant to the Assurance Condition evaluated;

(b) attributable to an identified Actor, Source, process, system, mechanism or device;

(c) sufficiently current for the evaluation purpose;

(d) protected against unauthorised alteration;

(e) traceable to the evaluation and applicable Profile Version;

(f) retained according to the applicable lifecycle conditions.

4.3. The evaluation shall identify incomplete, conflicting, unavailable, stale, disputed or indeterminate evidence.

4.4. An Assurance outcome shall identify each material:

(a) limitation;

(b) caveat;

(c) unverified condition;

(d) dependency;

(e) review or re-evaluation trigger.

4.5. Where an Assurance outcome depends on more than one Assurance Object or Assurance Domain, the applicable Profile shall define a composite evaluation.

4.6. A composite evaluation shall identify:

(a) each constituent Assurance Object;

(b) each applicable Assurance Domain and Assurance Level;

(c) each mandatory and conditional dependency;

(d) the combination rule;

(e) the effect of unavailable, suspended, withdrawn, non-conforming or indeterminate dependencies;

(f) the resulting Assurance outcome and limitations.

4.7. A composite Assurance Level shall not be inferred solely from the highest, lowest or numerical sum of the constituent Assurance Levels.

4.8. Evidence or Assurance relating to one constituent matter shall not transfer to another constituent matter.

4.9. A material change affecting evidence, an Assurance Condition or a dependency shall trigger re-evaluation where required by the applicable Profile.

SECTION 2: CONFORMITY ASSESSMENT

Article 5: Assessment subjects, scope and evidence

5.1. Conformity Assessment shall determine whether an identified assessment subject satisfies the requirements assigned by the Framework and applicable Framework Instruments.

5.2. An assessment subject shall be:

(a) a Trust Service Provider;

(b) a Trust Service;

(c) an Authoritative Source;

(d) a creation mechanism or device;

(e) a Trust Object type, Trust Service Output type, process, system or component where the applicable Profile requires assessment;

(f) another Controlled Matter for which the Framework expressly requires Conformity Assessment.

5.3. The assessment scope shall identify, where applicable:

(a) the Provider Scope;

(b) the Service Scope;

(c) the Source Scope;

(d) the Trust Object Category or output type;

(e) the mechanism, device, system or component;

(f) the operational locations and organisational functions;

(g) the applicable Schemes, Profiles and Technical Specifications;

(h) the applicable requirements and Versions;

(i) the material dependencies;

(j) the period to which the assessment applies.

5.4. A Conformity Assessment shall examine the organisational, governance, functional, technical, security, continuity, evidence, lifecycle and safeguard requirements applicable to the assessment subject.

5.5. Technical testing alone shall not constitute a complete Conformity Assessment where requirements outside the tested technical scope apply.

5.6. The assessment evidence shall identify:

(a) the evidence source and owner;

(b) the requirement supported;

(c) the collection or observation method;

(d) the relevant Version and time;

(e) the integrity and retention controls;

(f) each limitation affecting the evidence.

5.7. A Conformity Assessment shall not extend beyond the evidence and scope assessed.

Article 6: Competence, independence and Conformity Assessment Results

6.1. An Actor shall perform Conformity Assessment only where recognised as a Conformity Assessment Body for the relevant scope.

6.2. A Conformity Assessment Body shall possess the competence, resources, methods and independence required by the applicable Framework Instrument.

6.3. A Conformity Assessment Body shall identify and manage conflicts of interest affecting the assessment.

6.4. An Actor shall not assess a matter for which its operational responsibility impairs the independence or credibility of the assessment.

6.5. Use of a subcontractor shall not remove the responsibility of the recognised Conformity Assessment Body.

6.6. A Conformity Assessment shall produce a Conformity Assessment Result identifying:

(a) the assessment subject and assessed scope;

(b) the applicable requirements, Profiles, Technical Specifications and Versions;

(c) the methods and evidence used;

(d) each finding and non-conformity;

(e) each limitation and caveat;

(f) the assessment conclusion;

(g) the issue date and period of applicability;

(h) the responsible Conformity Assessment Body.

6.7. A limitation preventing a complete assessment shall be reflected in the assessment conclusion.

6.8. A positive Conformity Assessment Result shall not, by itself, assign recognition, Service Permission, operational activation or Qualified Status.

6.9. A Conformity Assessment Result shall be protected against unauthorised alteration and retained for the period required for qualification, supervision, Review, Remedy and Historical State reconstruction.

SECTION 3: DECISION-BASED QUALIFICATION

Article 7: Qualified Trust Service Provider Status

7.1. Qualified Trust Service Provider Status shall apply only through Decision-Based Qualification.

7.2. A Framework Body shall assign Qualified Trust Service Provider Status only where:

(a) an applicable Qualified Profile for the Trust Service Provider is in force;

(b) the Provider satisfies the applicable organisational, governance, personnel, security, continuity, evidence and lifecycle conditions;

(c) the required Conformity Assessment has been completed;

(d) each material non-conformity has been resolved;

(e) the evidence basis and Qualified Scope have been recorded.

7.3. The Qualified Scope assigned to a Trust Service Provider shall identify:

(a) the Trust Service Provider;

(b) the organisational functions and locations covered;

(c) the common controls and systems covered;

(d) the Trust Services to which the Provider assessment relates;

(e) the material dependencies covered;

(f) the Effective Date, Validity Period and review date;

(g) the restrictions and caveats.

7.4. Qualified Trust Service Provider Status shall not transfer to:

(a) a Trust Service;

(b) a Trust Service Output;

(c) a Trust Object;

(d) a Source;

(e) a mechanism, device, system or component;

(f) a subcontractor or dependency.

7.5. Each Trust Service provided by a Qualified Trust Service Provider shall require separate recognition, Service Permission and qualification where Qualified Trust Service Status is sought.

7.6. The competent Framework Body shall publish authorised Qualified Trust Service Provider Status through the Humanitarian Trust List.

7.7. A material change affecting the Qualified Scope shall be assessed before Qualified Trust Service Provider Status continues to apply to the changed matter.

Article 8: Qualified Trust Service Status

8.1. Qualified Trust Service Status shall apply only through Decision-Based Qualification of an identified Trust Service.

8.2. A Framework Body shall assign Qualified Trust Service Status only where:

(a) the Trust Service Provider has Qualified Trust Service Provider Status for the relevant Provider Scope;

(b) an applicable service-specific Qualified Profile is in force;

(c) the Trust Service satisfies the applicable functional, operational, security, continuity, evidence and lifecycle conditions;

(d) the required Conformity Assessment has been completed;

(e) each material non-conformity has been resolved;

(f) the evidence basis and Qualified Scope have been recorded.

8.3. The Qualified Scope assigned to a Trust Service shall identify:

(a) the Trust Service and Trust Service Category;

(b) the Trust Service Provider;

(c) the Service Scope and native outputs;

(d) the applicable Schemes and Profiles;

(e) the systems, mechanisms, devices, Sources and dependencies covered;

(f) the operational locations and interfaces covered;

(g) the Effective Date, Validity Period and review date;

(h) the restrictions and caveats.

8.4. Each Trust Service shall be assessed and qualified independently, including where more than one Trust Service shares the same Provider, personnel, system, mechanism, device, Source or Technical Exchange Route.

8.5. Qualified Trust Service Status shall not transfer to:

(a) the Trust Service Provider outside its Qualified Scope;

(b) another Trust Service;

(c) a Trust Service Output;

(d) a Trust Object;

(e) a Source;

(f) a mechanism or device.

8.6. The competent Framework Body shall publish authorised Qualified Trust Service Status through the Humanitarian Trust List.

8.7. A material change affecting the Service Scope, native outputs, dependencies, security, continuity or assessed implementation shall trigger reassessment before Qualified Trust Service Status continues to apply to the changed matter.

Article 9: Qualified Authoritative Source Status

9.1. Qualified Authoritative Source Status shall apply only through Decision-Based Qualification of an identified Authoritative Source.

9.2. A Framework Body shall assign Qualified Authoritative Source Status only where:

(a) the Source has Authoritative Source Status for the relevant Source Scope;

(b) an applicable Qualified Profile for the Authoritative Source is in force;

(c) the Source satisfies the applicable Data Quality, semantic, Provenance, security, continuity and lifecycle conditions;

(d) the required Conformity Assessment has been completed;

(e) each material non-conformity has been resolved;

(f) the evidence basis and Qualified Scope have been recorded.

9.3. The Qualified Scope assigned to an Authoritative Source shall identify the Source, Source Holder, authoritative information, Subjects or objects, population, geographic, organisational, temporal and purpose boundaries, Effective Date, Validity Period, restrictions and caveats.

9.4. Qualified Authoritative Source Status shall not transfer to:

(a) the Source Holder or Source Steward;

(b) another Source;

(c) a copy, extract, transformation, aggregation or derivative;

(d) a Trust Service using the Source;

(e) a Trust Service Output or Trust Object based on the Source.

9.5. The competent Framework Body shall publish authorised Qualified Authoritative Source Status through the Humanitarian Trust List or another governance-controlled publication mechanism where publication is authorised.

9.6. A material change affecting the Qualified Scope, Data Quality, semantics, Provenance, security, continuity or lifecycle shall trigger reassessment before Qualified Authoritative Source Status continues to apply to the changed matter.

Article 10: Qualified creation mechanisms and devices

10.1. Qualified Status assigned to a creation mechanism or device shall apply only through Decision-Based Qualification.

10.2. A Framework Body shall assign Qualified Status to a creation mechanism or device only where:

(a) the category is eligible for qualification under the Main Parts;

(b) an applicable Qualified Profile is in force;

(c) the required Conformity Assessment has been completed;

(d) each material non-conformity has been resolved;

(e) the mechanism or device and qualified configuration are uniquely identified;

(f) the Qualified Scope and evidence basis have been recorded.

10.3. The Qualified Scope shall identify:

(a) the responsible Provider or operator;

(b) the model and unique identifier;

(c) the hardware, software and firmware Versions;

(d) the approved configuration;

(e) the assigned function;

(f) the operational environment and control model;

(g) the material dependencies;

(h) the Effective Date, Validity Period and review date;

(i) the restrictions and caveats.

10.4. Qualified Status assigned to a mechanism or device shall not transfer to:

(a) another instance or configuration;

(b) the Trust Service using it;

(c) the Trust Service Provider;

(d) a Trust Object or Trust Service Output produced through it;

(e) another mechanism, device, system or component.

10.5. The competent Framework Body shall publish authorised Qualified Status information through the Humanitarian Trust List or an applicable governance Register where publication is authorised.

10.6. A material change to the hardware, software, firmware, configuration, operational environment, control model or dependency shall trigger reassessment before Qualified Status continues to apply to the changed matter.

SECTION 4: OBJECT-INSTANCE QUALIFICATION AND NON-TRANSFER

Article 11: Qualified Trust Objects and eligible Trust Service Outputs

11.1. Object-Instance Qualification shall apply to each individual Trust Object and Trust Service Output eligible for Qualified Status under Part VI.

11.2. An individual Trust Object or eligible Trust Service Output shall have Qualified Status only where:

(a) it satisfies the applicable Qualified Object Profile;

(b) it is created or issued through the Trust Service Status required by that Profile;

(c) each required qualified dependency is valid within its assigned scope and at the relevant time;

(d) it contains or references the required creation, issuance, protection, Status and lifecycle evidence;

(e) Validation confirms satisfaction of the applicable qualified conditions.

11.3. Object-Instance Qualification shall not require an individual Framework Decision unless the Main Parts expressly assign that requirement.

11.4. The applicable Qualified Object Profile shall identify:

(a) the eligible Trust Object Category or output type;

(b) the time at which the qualified conditions shall be satisfied;

(c) the required issuing or producing Trust Service Status;

(d) the required qualified dependencies;

(e) the required evidence, protection and Status information;

(f) the Validation method and result classes;

(g) the lifecycle, restriction, Suspension, Withdrawal and Revocation conditions;

(h) the conditions for historical Validation.

11.5. Qualified Status of an individual object or output shall be evidenced through the object or output, applicable Qualified Object Profile, producing-service Status, dependency Status, Validation Result and authorised Status information.

11.6. Qualified Status of an individual object or output shall not transfer to its Issuer, Subject, Trust Service Provider, Trust Service, Source Basis, protection object or dependency.

11.7. Individual Trust Objects shall not ordinarily receive Humanitarian Trust List Entries and shall use the applicable Status Response and Validation mechanisms.

11.8. A Trust Service Output represented through an Electronic Attestation shall remain the original output, and the Electronic Attestation shall require separate evaluation under its applicable Qualified Object Profile where Qualified Status is sought for the Electronic Attestation.

Article 12: Qualified Status non-transfer matrix

12.1. Qualified Status shall remain specific to the Status-Bearing Matter, qualification route and Qualified Scope through which that Status is assigned or established.

12.2. The qualification route, principal evidence and non-transfer boundary shall be determined in accordance with Table 1.

Status-Bearing Matter	Qualification route	Principal qualification basis	Principal Status evidence or publication	Qualified Status shall not transfer to
Trust Service Provider	Decision-Based Qualification	Qualified Profile for the Trust Service Provider, Conformity Assessment Result and Framework Decision	Humanitarian Trust List	Trust Services, outputs, Trust Objects, Sources, mechanisms, devices or dependencies

Status-Bearing Matter	Qualification route	Principal qualification basis	Principal Status evidence or publication	Qualified Status shall not transfer to
Trust Service	Decision-Based Qualification	Service-specific Qualified Profile, Conformity Assessment Result and Framework Decision	Humanitarian Trust List	Provider outside its Qualified Scope, other services, outputs, Trust Objects, Sources, mechanisms or devices
Authoritative Source	Decision-Based Qualification	Qualified Profile for the Authoritative Source, Conformity Assessment Result and Framework Decision	Humanitarian Trust List or governance-controlled publication where authorised	Source Holder, Source Steward, other Sources, derivatives, services, outputs or Trust Objects
Creation mechanism or device	Decision-Based Qualification	Qualified Profile for the mechanism or device, Conformity Assessment Result and Framework Decision	Humanitarian Trust List or governance Register where authorised	Other instances or configurations, Provider, service, output or Trust Object
Individual Trust Object or eligible Trust Service Output	Object-Instance Qualification	Qualified Object Profile, required service and dependency Status, object evidence and Validation	Trust Object or output, Status Response and Validation Result	Issuer, Subject, Provider, service, Source Basis, protection object or dependency

12.3. Table 1 shall form an integral part of this Annex and shall not create a new eligible category or qualification route.

12.4. Qualified Status assigned or established under one row of Table 1 shall not satisfy a condition assigned to another row unless the applicable Qualified Profile expressly requires that Status as a dependency.

12.5. A shared Provider, system, mechanism, device, Source, Certificate, protection object or Technical Exchange Route shall not merge the qualified identity or Qualified Scope of separate Status-Bearing Matters.

12.6. A Scheme, Profile, Implementation Guideline, Technical Specification, Humanitarian Trust List Entry, Register Entry or Catalogue Entry shall not extend Qualified Status beyond the applicable qualified conditions and route.

Article 13: Qualified dependencies and composite arrangements

13.1. A Qualified Profile shall identify each mandatory or conditional qualified dependency applicable to the qualified matter.

13.2. A qualified dependency shall be evaluated according to:

(a) its identity and category;

(b) its Qualified Status and Qualified Scope;

(c) the relevant time;

(d) the applicable Status and evidence source;

(e) the relationship to the dependent matter;

(f) the effect of restriction, Suspension, Withdrawal, Revocation, Expiry or unavailability.

13.3. Qualified Status of a dependency shall constitute a condition and shall not transfer to the dependent matter.

13.4. A composite arrangement comprising more than one Trust Service, Source, Trust Object, mechanism, device or other dependency shall retain the independent identity, Status, Assurance, evidence and lifecycle of each constituent matter.

13.5. The applicable Qualified Profile shall define the combination rule and the outcome where:

(a) a mandatory dependency is unavailable or indeterminate;

(b) a dependency no longer has the required Status;

(c) dependencies have different Validity Periods;

(d) a dependency is replaced or superseded;

(e) Historical State must be reconstructed.

13.6. Failure of one qualified dependency shall affect another qualified matter only within the dependency, scope and time established by the applicable Qualified Profile and evidence.

13.7. A composite qualified outcome shall not be represented as valid where a mandatory qualified dependency is unresolved.

SECTION 5: SURVEILLANCE AND QUALIFICATION LIFECYCLE

Article 14: Surveillance, reassessment and non-conformity

14.1. A Decision-Based Qualification subject shall be subject to surveillance and reassessment according to the applicable Qualified Profile and qualification decision.

14.2. Surveillance shall examine, where applicable:

(a) continued satisfaction of the qualified conditions;

(b) material organisational or operational changes;

(c) security, continuity and incident conditions;

(d) changes to systems, mechanisms, devices, Sources and dependencies;

(e) complaints, Review outcomes and field-performance evidence;

(f) corrective actions and earlier non-conformities.

14.3. Reassessment shall occur where a material change affects the Qualified Scope, applicable requirements, evidence, dependency or operational conditions.

14.4. Individual Trust Objects and eligible Trust Service Outputs shall be subject to re-Validation and Status evaluation rather than organisational surveillance, except where the applicable Qualified Object Profile requires an object-specific review.

14.5. A non-conformity record shall identify:

(a) the affected Status-Bearing Matter and Qualified Scope;

(b) the failed requirement;

(c) the evidence basis;

(d) the actual or potential effect;

(e) the affected dependencies, outputs and historical period;

(f) the required corrective action;

(g) the correction period;

(h) the Verification and closure conditions.

14.6. A material non-conformity shall prevent a positive qualification or continued Qualified Status where the failed requirement is necessary for the applicable qualified conditions.

14.7. Failure to correct a material non-conformity shall trigger the applicable restriction, Suspension, Withdrawal, Revocation or reassessment procedure.

14.8. A non-conformity affecting one qualified matter shall not automatically affect every related Provider, service, Source, mechanism, device, output or Trust Object.

Article 15: Restriction, Suspension, Withdrawal and historical Validation

15.1. A Framework Body shall restrict, suspend, withdraw or reinstate Decision-Based Qualified Status only within its Decision Competence and on a recorded evidence basis.

15.2. A qualification lifecycle decision shall identify:

(a) the affected Status-Bearing Matter and Qualified Scope;

(b) the applicable Qualified Profile and Version;

(c) the evidence and non-conformity basis;

(d) the Controlled Effect and Effective Date;

(e) the effect on dependencies, services, outputs and Trust Objects;

(f) the required Status Publication and notifications;

(g) the Review and Remedy Routes.

15.3. Restriction, Suspension or Withdrawal shall apply only to the affected Qualified Scope unless an identified dependency and evidence require a broader effect.

15.4. Restriction, Suspension or Withdrawal of a Trust Service Provider, Trust Service, Authoritative Source, mechanism or device shall not automatically remove the Qualified Status of an individual Trust Object created before the Effective Date of that action.

15.5. Historical Validation of an individual Trust Object or eligible Trust Service Output shall use:

(a) the Qualified Object Profile and Version applicable at the relevant time;

(b) the producing Trust Service Status and Provider Status applicable at that time;

(c) the Status of each required Source, Certificate, protection object, mechanism, device and other dependency at that time;

(d) the creation, issuance, protection and lifecycle evidence;

(e) each applicable restriction, caveat, Revocation and effective period;

(f) the authorised Historical State and Status information.

15.6. A later change, restriction, Suspension, Withdrawal or Revocation shall not retrospectively alter an earlier qualified outcome unless the applicable Framework Decision, Qualified Profile or evidence establishes that the relevant qualified conditions were not satisfied at the earlier time.

15.7. Current validity and historical qualification shall remain distinguishable.

15.8. The competent Framework Body shall publish authorised changes to Qualified Status assigned through Decision-Based Qualification through the Humanitarian Trust List or another governance-controlled publication mechanism.

15.9. Individual-object Status changes shall be communicated through the applicable Status Response, Revocation, Validation and lifecycle mechanisms.

15.10. Qualified Status information, qualification decisions, Conformity Assessment Results, surveillance records, Status histories and Validation evidence shall remain available for the period required for Review, Remedy, Controlled Reliance and Historical State reconstruction.

ANNEX G: SECURITY ARCHITECTURE AND CONTROLLED EXCHANGE MODEL

IDEHA-ANN-PUB-GEN-001 Version:0.1

SECTION 1: GENERAL PROVISIONS AND GOVERNANCE OWNERSHIP

Article 1: Subject matter and governance ownership

1.1. This Annex establishes the common model applicable to the Humanitarian Trust List, Status Publication, governance-controlled Registers and Catalogues, and federation discovery under Parts II, IV, IX, X and XIII.

1.2. The competent Framework Body shall own and control the Humanitarian Trust List and each governance-controlled Register and Catalogue within its Decision Competence.

1.3. The competent Framework Body shall determine:

(a) eligibility for listing or recording;

(b) the Status, scope and Discovery Metadata to be published;

(c) the applicable publication and access class;

(d) the Effective Date and lifecycle of each Entry;

(e) the Correction, restriction, Suspension, Withdrawal and archival treatment;

(f) the authenticity, Integrity, Availability and historical preservation of the publication or record set.

1.4. A technical operator shall support publication, distribution, storage, search, replication or recovery only under the instructions and controls of the competent Framework Body.

1.5. A technical operator shall not acquire Decision Competence, Trust Service Provider Status, ownership of the Humanitarian Trust List or authority to assign or alter Status by reason only of performing a supporting function.

1.6. The Humanitarian Trust List shall not constitute a Trust Service.

1.7. This Annex shall not:

(a) create a Status or qualification route;

(b) recognise a Trust Service Provider, Trust Service, Source, Framework Instrument, mechanism, device, Actor or Federation Domain;

(c) assign Service Permission, Technical Exchange Permission, access, disclosure, Authorisation or Controlled Reliance;

(d) prescribe a technical protocol, schema, format, algorithm, product or deployment model;

(e) require centralised storage of all Entries or Discovery Metadata.

Article 2: Listable Status-Bearing Matters

2.1. A Status-Bearing Matter shall receive a Humanitarian Trust List Entry only where the Main Parts or an authorised Framework Decision establish that publication is required or permitted.

2.2. Subject to paragraph 2.1, listable Status-Bearing Matters shall include, where applicable:

(a) a Federation Domain or Federation Trust Relationship;

(b) a Recognised Actor, Assigned Role or Participation Status whose publication is necessary for the recognised purpose;

(c) a Trust Service Provider;

(d) a Trust Service;

(e) a Source, Authoritative Source or Qualified Authoritative Source;

(f) an eligible creation mechanism or device;

(g) a Technical Exchange Route or route operator whose Status Publication is authorised;

(h) a Framework Instrument;

(i) another Status-Bearing Matter expressly designated as listable by the Main Parts.

2.3. Individual high-volume Trust Objects and Trust Service Outputs shall not ordinarily receive Humanitarian Trust List Entries.

2.4. Status concerning an individual Trust Object or Trust Service Output shall ordinarily be provided through Validation and an authorised Status Response where the applicable Profile requires current Status information.

2.5. A natural person shall not be listed unless the applicable Framework Instrument expressly requires publication, the publication is necessary and proportionate for the recognised purpose, and the applicable Protected-Person Safeguards are satisfied.

2.6. Eligibility for listing shall not, by itself, create or alter Status.

2.7. The same Status-Bearing Matter shall have separate Entries or separately identifiable Status components where different Statuses, scopes, Federation Domains or publication classes require independent lifecycle treatment.

SECTION 2: HUMANITARIAN TRUST LIST ENTRIES AND STATUS PUBLICATION

Article 3: Humanitarian Trust List Entry structure

3.1. A Humanitarian Trust List Entry shall identify or reference:

(a) the Entry identifier;

(b) the identified Status-Bearing Matter and its identifier;

(c) the category of the Status-Bearing Matter;

(d) the competent Framework Body;

(e) the applicable Federation Domain;

(f) the published Status and scope;

(g) the Framework Decision and Decision File reference;

(h) the Effective Date;

(i) the Validity Period or review date, where applicable;

(j) each restriction, caveat, Suspension, Withdrawal or other lifecycle condition;

(k) the authorised Discovery Metadata, where applicable;

(l) the publication and access class;

(m) the Entry Version and predecessor or successor relationship;

(n) the applicable Correction and Review Routes.

3.2. An Entry shall contain only the information necessary for Status Publication, federation discovery, Validation, accountability and historical reconstruction within its authorised publication class.

3.3. An Entry shall reference the supporting Framework Decision and shall not reproduce a Decision File or underlying evidence unless the applicable publication policy expressly authorises that disclosure.

3.4. An Entry identifier shall remain separate from the identifier of the Status-Bearing Matter described by the Entry.

3.5. A change to an Entry shall preserve the predecessor relationship and Historical State required to determine the Status and Discovery Metadata applicable at an identified time.

3.6. An Entry shall not be treated as the underlying Status-Bearing Matter, Framework Decision, Source, Trust Service, Trust Object or Trust Service Output.

Article 4: Status information and decision references

4.1. Status Publication shall communicate an authorised Framework Decision and shall not create the Status being published.

4.2. Published Status information shall identify, where applicable:

(a) recognition or designation Status;

(b) Trust Service Provider Status or Trust Service Status;

(c) Authoritative Source Status or Qualified Authoritative Source Status;

(d) Qualified Status and Qualified Scope;

(e) Active, Restricted, Suspended, Withdrawn, Revoked, Superseded, Archived or Transitional Status;

(f) the Effective Date and Validity Period;

(g) the scope, restrictions and caveats;

(h) the applicable decision reference.

4.3. Provider Status and the Status of each Trust Service provided by that Provider shall remain separately identifiable.

4.4. Qualified Status assigned through Decision-Based Qualification shall remain separately identifiable for each qualified Trust Service Provider, Trust Service, Authoritative Source, creation mechanism or device.

4.5. Publication of Qualified Status shall not qualify the listed matter and shall not extend Qualified Status beyond the Qualified Scope assigned by the applicable qualification decision.

4.6. A Status change shall take effect according to the Effective Date assigned by the competent Framework Body and shall not be inferred solely from the time at which the Entry is technically published or retrieved.

4.7. A later Status shall not overwrite the Historical State of an earlier Status.

4.8. Where a Decision File or supporting evidence is subject to restricted access, the Entry shall publish only the decision reference and authorised summary information.

SECTION 3: DISCOVERY AND FEDERATION RESOLUTION

Article 5: Discovery Metadata and the address-book function

5.1. The Humanitarian Trust List shall constitute the governance-controlled address-book and federation-discovery publication for listable Status-Bearing Matters.

5.2. The Framework shall not establish a separate address-book publication for the same governance and discovery function.

5.3. Discovery Metadata shall identify or reference, where applicable:

(a) the Federation Domain;

(b) the recognised Actor or Trust Service Provider;

(c) the Trust Service or Source;

(d) the service, Source or route identifier;

(e) the Endpoint;

(f) the Interface Modality;

(g) the applicable Technical Exchange Route;

(h) the information required to authenticate or validate the Endpoint, Trust Service or publication;

(i) the applicable Status Response location or Validation reference;

(j) the authoritative Humanitarian Trust List reference for a Federation Domain or Nested Federation;

(k) the operational contact or escalation reference where publication is authorised.

5.4. Discovery Metadata shall remain limited to the information necessary to locate, identify, authenticate or resolve the relevant matter.

5.5. Public Discovery Metadata shall not expose security-sensitive network, configuration, credential, personal or operational information.

5.6. An Endpoint reference shall identify where an Actor, Trust Service, Source or Technical Exchange Route is reached and shall not establish Service Permission, Technical Exchange Permission, access, disclosure, Authorisation or Controlled Reliance.

5.7. A local directory, search index, cache or operational view derived from the Humanitarian Trust List shall remain a derivative representation and shall identify the authoritative Entry and Version from which it was derived.

Article 6: Separate authority for Status and Discovery Metadata changes

6.1. Status information and Discovery Metadata shall have separate change authority, evidence and lifecycle treatment.

6.2. Only a Framework Body acting within its Decision Competence shall assign, extend, restrict, suspend, withdraw, revoke, reinstate or otherwise change published Status.

6.3. The Actor responsible for a listed Endpoint, Trust Service, Source, route or operational contact shall submit a material Discovery Metadata change through the applicable update route.

6.4. The competent Framework Body shall verify or cause the verification of a Discovery Metadata change before authoritative publication.

6.5. A technical operator shall implement an authorised publication change only where the applicable instruction, evidence reference and Effective Date are recorded.

6.6. A Discovery Metadata change shall not, by itself:

(a) assign or alter Status;

(b) extend a Service Scope, Provider Scope, Source Scope or Qualified Scope;

(c) activate a Trust Service or Technical Exchange Route;

(d) create access, disclosure, Authorisation or Controlled Reliance.

6.7. A Status change shall trigger review of the related Discovery Metadata where continued publication or routing would conflict with the changed Status.

6.8. Each material Status or Discovery Metadata change shall remain attributable, versioned and historically reconstructable.

Article 7: Integrity, Authenticity, Availability and historical entries

7.1. The competent Framework Body shall ensure the Integrity, Authenticity, Availability and historical preservation of the authoritative Humanitarian Trust List.

7.2. Each authoritative publication Version shall identify:

(a) the responsible Framework Body;

(b) the publication identifier and Version;

(c) the issue time;

(d) the Effective Date or covered period;

(e) the predecessor publication Version;

(f) the applicable publication and access classes.

7.3. Each authoritative publication Version shall be protected by an Electronic Seal attributable to the competent Framework Body or its responsible legal entity, or by an Electronic Signature attributable to an authorised natural person acting for that Body.

7.4. The applicable Profile shall define whether an Electronic Timestamp or another independent time-evidence requirement applies to the authoritative publication Version.

7.5. A distributed, replicated or cached copy shall preserve the authoritative object-level protection, publication identifier, Version and provenance.

7.6. Failure of a publication channel shall not authorise use of an unverifiable or unauthenticated list copy.

7.7. Continuity arrangements shall support restoration of the authoritative publication, current Entries, Historical State and evidence of publication changes.

7.8. An earlier Entry or publication Version shall remain available where required for Validation, Review, Remedy, audit and evaluation of earlier Controlled Reliance.

Article 8: Federation Domains, Nested Federation and authoritative list references

8.1. Each Federation Domain shall identify the competent Framework Body and authoritative Humanitarian Trust List or authorised Humanitarian Trust List view applicable within that domain.

8.2. The Framework shall support centralised, distributed, nested and hybrid publication arrangements without changing the Decision Competence retained by each Federation Domain.

8.3. A parent Federation Domain shall reference the authoritative Humanitarian Trust List of a Nested Federation where the applicable Federation Agreement assigns that relationship.

8.4. A parent-domain reference shall identify:

(a) the Nested Federation Domain;

(b) the competent Framework Body of that domain;

(c) the authoritative list identifier and discovery reference;

(d) the Federation Trust Relationship and scope;

(e) the Effective Date and lifecycle Status;

(f) the applicable mapping, restriction and reliance conditions.

8.5. A parent Federation Domain shall not be required to reproduce each Entry maintained by a Nested Federation.

8.6. Aggregation of Entries from another Federation Domain shall occur only where the Federation Agreement defines the aggregation authority, provenance, update, conflict, historical and Correction conditions.

8.7. A reference to or aggregation of another Federation Domain's Entries shall not transfer Decision Competence or convert the receiving Framework Body into the assigning body for the published Status.

8.8. Withdrawal or Suspension of a Federation Trust Relationship shall trigger review of the affected list references, Discovery Metadata, caching conditions and cross-domain resolution paths.

Article 9: Cross-domain resolution, caching and historical reconstruction

9.1. Cross-domain discovery shall resolve the authoritative publication chain from the receiving Federation Domain to the originating Federation Domain or listed matter.

9.2. A cross-domain resolution shall verify, where applicable:

(a) the identity and Status of each Federation Domain in the resolution path;

(b) the authenticity and Integrity of each authoritative publication Version;

(c) the Federation Trust Relationship and scope;

(d) the current or historically applicable Entry;

(e) the applicable mapping and restriction conditions;

(f) the freshness and validity of cached information.

9.3. A cache shall identify:

(a) the authoritative list and Entry references;

(b) the retrieved Version;

(c) the retrieval time;

(d) the freshness or expiry condition;

(e) the applicable fallback and refresh rule.

9.4. Cached Status or Discovery Metadata shall not be used beyond its authorised freshness or expiry condition.

9.5. Use of a cache shall not create or alter Status and shall not make the cache the authoritative Humanitarian Trust List.

9.6. A historical resolution shall use the Status, Discovery Metadata, Federation Trust Relationship, publication Version and mapping conditions applicable at the relevant time.

9.7. Where an authoritative publication cannot be resolved or validated, the result shall be indeterminate unless an applicable Framework Instrument establishes a controlled fallback route.

9.8. A successful cross-domain resolution shall not, by itself, require acceptance or Controlled Reliance by the receiving Relying Actor.

SECTION 4: REGISTERS, CATALOGUES AND PUBLICATION CLASSES

Article 10: Distinct functions of the Humanitarian Trust List, Registers and Catalogues

10.1. The Humanitarian Trust List shall publish authorised Status and Discovery Metadata for listable Status-Bearing Matters.

10.2. A Register shall record identified Controlled Matters, decisions, evidence references and lifecycle information for an assigned governance purpose.

10.3. A Catalogue shall organise or list recognised categories, types, functions, codes, Schemes, Profiles or other Controlled Matters for an assigned governance purpose.

10.4. A Decision File shall evidence a Framework Decision and shall remain separate from the Humanitarian Trust List, Register or Catalogue Entry that references that decision.

10.5. A Status Response shall provide authorised Status information concerning an identified Status-Bearing Matter and shall remain a Trust Service Output of a Validation and Verification Service.

10.6. The Humanitarian Trust List, a Register, a Catalogue, a Decision File and a Status Response shall not be treated as interchangeable records or functions.

10.7. The competent Framework Body shall identify the authoritative record for each governance data element where the same information is referenced across more than one record set.

10.8. The Trust Service Catalogue and Trust Object Catalogue shall record only the categories established by Parts IX and VI respectively and shall not create or remove a category.

10.9. The Instrument Code Catalogue shall record the codes governed by Annex B and shall not create a new Framework Instrument category, Trust Service Category, Trust Object Category or Controlled Effect.

10.10. A Standards Register, qualification record, mechanism or device Register, Scheme Catalogue or Profile Catalogue shall operate only within the enabling Framework Instrument and assigned Decision Competence.

Article 11: Publication and access classes

11.1. Each Humanitarian Trust List, Register and Catalogue field shall be assigned an access or publication class appropriate to its purpose, sensitivity and risk.

11.2. Publication and access classes shall distinguish, where applicable:

(a) public information;

(b) federation-restricted information;

(c) operational information;

(d) supervisory or assessment information;

(e) Protection-Sensitive or Security-Sensitive Information.

11.3. Public information shall contain only information suitable for unrestricted disclosure.

11.4. Federation-restricted, operational, supervisory, Protection-Sensitive or Security-Sensitive Information shall be disclosed only to an authorised Actor for an identified purpose and scope.

11.5. A public view shall not include personal data, protected-person information, confidential decision evidence, security configurations, private cryptographic material or sensitive Endpoint details unless the applicable Framework Instrument expressly authorises that disclosure.

11.6. Different authorised views of the same Entry shall reference the same authoritative Entry identifier and Version.

11.7. Restriction of one field or view shall not obscure the published Status where public Status Publication is required, but the reason or evidence supporting that Status shall remain restricted where necessary.

11.8. Access to restricted records or fields shall be attributable and recorded where required by the applicable Framework Instrument.

11.9. A publication or access class shall not alter the underlying Status, scope, Decision Competence or Controlled Effect.

SECTION 5: NO-EFFECT BOUNDARIES

Article 12: No-effect rules

12.1. Inclusion in the Humanitarian Trust List shall not, by itself, constitute the Framework Decision assigning the published Status.

12.2. Discovery of an Actor, Trust Service Provider, Trust Service, Source, Endpoint, Federation Domain or Technical Exchange Route shall not, by itself, create:

(a) recognition;

(b) Service Permission;

(c) Technical Exchange Permission;

(d) access or disclosure permission;

(e) Authorisation;

(f) Controlled Reliance.

12.3. Publication of Trust Service Provider Status shall not qualify or activate a Trust Service provided by that Provider.

12.4. Publication of Trust Service Status shall not qualify a Trust Service Output or Trust Object and shall not require a Relying Actor to accept that output or object.

12.5. Publication of Authoritative Source Status or Qualified Authoritative Source Status shall not authorise access to, disclosure from or reliance on the Source.

12.6. Publication of Qualified Status shall communicate the applicable qualification decision and Qualified Scope and shall not create or extend Qualified Status.

12.7. Inclusion in a Register or Catalogue shall not, by itself, create recognition, Status, qualification, permission, operational activation or Controlled Reliance.

12.8. Successful validation of a Humanitarian Trust List Entry or publication Version shall confirm the authenticity and Integrity of that publication and shall not determine the correctness of the underlying Framework Decision.

12.9. A Status Response shall not create or alter the Status that it reports.

12.10. A Humanitarian Trust List, Register, Catalogue, local directory, cache, discovery index or technical publication component shall not become a Trust Service by reason only of supporting Status Publication or discovery.

ANNEX H: SECURITY, CONFIDENTIALITY, INCIDENT AND CONTINUITY MODEL

IDEHA-ANN-SEC-GEN-001 Version: 0.1

SECTION 1: GENERAL SECURITY MODEL

Article 1: Subject matter and scope

1.1. This Annex establishes the common security, Confidentiality, incident, Continuity and Recovery model required by Parts III, IX, XI and XIII.

1.2. This Annex shall apply to each Controlled Matter and Controlled Interaction within the scope assigned by the Framework, the applicable Scheme and the applicable Profile.

1.3. This Annex shall govern the relationships between security responsibilities, trust boundaries, protection layers, dependencies, Security Incidents, Status effects and Recovery.

1.4. The applicable Implementation Guideline, Profile and Technical Specification shall define the detailed controls, parameters, algorithms, configurations, evidence and testing requirements necessary to implement this Annex.

1.5. This Annex shall not:

(a) prescribe a particular technology, product, protocol, algorithm, key length, device or deployment model;

(b) assign recognition, Status, Service Permission, Technical Exchange Permission, Authorisation, Controlled Reliance or Qualified Status;

(c) transfer security responsibility between Actors;

(d) treat a technical security capability as sufficient evidence of compliance with the Framework.

Article 2: Security responsibility, domains and trust boundaries

2.1. Each Responsible Actor shall retain security responsibility for the Controlled Matters and Controlled Interactions within its assigned scope.

2.2. A security domain shall identify:

(a) the Controlled Matters protected;

(b) the organisational, physical, technical and Federation Boundaries;

(c) the responsible Roles and decision routes;

(d) the authorised Actors and protected functions;

(e) the applicable Security Conditions and Protected-Person Safeguards;

(f) the dependencies and external interfaces;

(g) the monitoring, evidence, incident and Continuity arrangements.

2.3. A Controlled Environment shall constitute a security domain or a defined part of a security domain assigned enhanced controls for an identified function, Trust Service, Trust Object, Source, mechanism or device.

2.4. A transition across a security domain, organisational boundary or Federation Boundary shall be treated as a controlled boundary crossing and shall satisfy the applicable Authentication, Authorisation, Confidentiality, Integrity, evidence and policy conditions.

2.5. Where the same Actor operates more than one security domain, the identity, responsibility, access conditions and evidence of each domain shall remain separately identifiable.

2.6. Shared infrastructure, outsourcing, federation, technical intermediation or common ownership shall not transfer security responsibility or merge the Status of separate Actors, Trust Services, Sources, Trust Objects, mechanisms, devices or routes.

2.7. A Technical Exchange Route Operator or other supporting Actor shall acquire only the access and responsibility expressly assigned to that Actor.

SECTION 2: CONFIDENTIALITY, INTEGRITY AND AUTHENTICITY

Article 3: Confidentiality layers

3.1. Confidentiality shall be applied through separately identifiable protection layers according to the applicable purpose, risk and Profile.

3.2. Transport Confidentiality shall protect information while it is transmitted through a Technical Exchange Route or between technical components.

3.3. Payload Confidentiality shall protect the content of a Controlled Interaction so that plaintext access is limited to authorised processing Actors.

3.4. Storage confidentiality shall protect information while retained in a system, device, record store, backup, archive or other storage environment.

3.5. Processing confidentiality shall protect information while it is used, transformed, evaluated or otherwise processed within an authorised environment.

3.6. Disclosure control shall determine whether, how, to whom and for which purpose information is made available.

3.7. Satisfaction of one Confidentiality layer shall not, by itself, satisfy another Confidentiality layer.

3.8. Confidentiality shall remain separate from Integrity, Authenticity, Authorisation, Status, Validation and Controlled Reliance.

3.9. The applicable Profile shall identify the required Confidentiality layers, authorised processing Actors, permitted Metadata and lifecycle conditions.

Article 4: Plaintext access and intermediary exclusion

4.1. Where Payload Confidentiality applies, the payload shall be protected before it enters a Technical Exchange Route or intermediary processing path.

4.2. 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.

4.3. A Technical Exchange Route Operator, Intermediary, Federated Data Exchange Service Provider or unrelated component shall not have plaintext access by reason only of transporting, routing, storing, monitoring or recording the Controlled Interaction.

4.4. Decryption material shall remain unavailable to an Actor that has not been assigned a plaintext-processing function.

4.5. Routing Metadata, Discovery Metadata, operational logs, error information and Exchange Evidence shall contain only the information necessary and authorised for their assigned purpose.

4.6. Each material plaintext access shall be attributable and evidenced where required by the applicable Profile.

4.7. Technical ability to access, decrypt or process information shall not, by itself, create Authorisation, disclosure permission, ownership or Controlled Reliance.

4.8. Where an authorised processing Actor is added or removed, the applicable access, key, evidence and lifecycle conditions shall be updated before the change has operational effect.

Article 5: Integrity, Authenticity, Accountability and independent protection

5.1. A Controlled Matter shall be protected against unauthorised alteration, substitution, deletion, corruption, replay and incorrect lifecycle transition according to the applicable Profile.

5.2. A statement-bearing Trust Object or Trust Service Output crossing an organisational boundary or Federation Boundary shall have the independent object-level protection required by Part VI and the applicable Profile.

5.3. Transport protection shall not replace an Electronic Signature, Electronic Seal, Electronic Timestamp, Certificate, Digital Signature or other object-level protection required for independent Verification or Validation.

5.4. Object-level protection shall not replace Transport Confidentiality, Payload Confidentiality or Authorisation where those controls apply.

5.5. A Controlled Interaction shall include correlation, replay, duplication and sequencing controls where those risks are material.

5.6. A material action, access, disclosure, decision, change or lifecycle transition shall be attributable to the responsible Actor, Trust Service, mechanism, device or system where Accountability requires that attribution.

5.7. Evidence supporting Integrity, Authenticity or Accountability shall identify the protected matter, protection method, applicable Version, time, responsible Actor and Validation basis.

5.8. A signed, sealed, timestamped or otherwise integrity-protected Trust Object shall not be corrected through alteration after issuance.

5.9. Successful Verification of Integrity or Authenticity shall not, by itself, create Authorisation, acceptance or Controlled Reliance.

SECTION 3: PROTECTED FUNCTIONS, INFORMATION AND MONITORING

Article 6: Protected functions and cryptographic material

6.1. A protected function shall include a function whose compromise is capable of materially affecting a Trust Service, Trust Object, Source, Status, Qualified Status, Controlled Interaction or Protected Person.

6.2. Protected functions shall include, where applicable:

(a) Digital Signature creation;

(b) Electronic Signature and Electronic Seal creation or management;

(c) Electronic Timestamp creation;

(d) Certificate or Electronic Attestation issuance;

(e) Authentication and Authorisation;

(f) Validation and Status evaluation;

(g) key, secret, creation-data and device administration;

(h) privileged administration and security monitoring.

6.3. Digital Signature Creation Data, Digital Signature Validation Data, encryption keys, Authentication secrets and other cryptographic material shall remain subject to separately assigned lifecycle controls.

6.4. The lifecycle referred to in paragraph 6.3 shall address:

(a) generation and initialisation;

(b) activation and Authorisation;

(c) storage and use;

(d) backup and Recovery;

(e) rotation and replacement;

(f) restriction, Suspension and Revocation;

(g) secure destruction.

6.5. A local, remote, shared or distributed creation arrangement shall preserve the control, activation, separation and evidence conditions assigned to the Signatory, Seal Creator or other authorised Actor.

6.6. Each material mechanism and device shall remain identifiable by its category, instance, configuration, software or firmware Version, operational environment and lifecycle Status.

6.7. Qualified Status of a mechanism or device shall not transfer to the Trust Service Provider, Trust Service, Trust Object or Trust Service Output using that mechanism or device.

6.8. Compromise or suspected compromise of protected creation data, cryptographic material, an Authenticator, mechanism or device shall trigger the applicable incident, restriction, Suspension, Revocation, replacement and notification conditions.

6.9. Detailed cryptographic and device requirements shall remain in the applicable Implementation Guideline, Profile, Technical Specification and Standards Register.

Article 7: Restricted, Protection-Sensitive and Security-Sensitive Information

7.1. A Responsible Actor shall classify information according to the risks arising from its access, use, combination, alteration, loss, disclosure and retention.

7.2. Restricted Information, Protection-Sensitive Information and Security-Sensitive Information shall be subject to assigned controls concerning:

(a) collection and creation;

(b) access and processing;

(c) disclosure and onward transfer;

(d) aggregation and linkage;

(e) logging and monitoring;

(f) retention, archival and Deletion;

(g) incident response and Recovery.

7.3. Public or federation-wide publication shall not disclose Protection-Sensitive Information or Security-Sensitive Information unless the applicable Framework Instrument expressly authorises that disclosure and the necessary safeguards are satisfied.

7.4. Logs, evidence records and monitoring information shall not reproduce Restricted Information beyond what is necessary for their assigned purpose.

7.5. A Responsible Actor shall assess whether aggregation, linkage or repeated access creates a protection or re-identification risk greater than the risk associated with each individual item of information.

7.6. Retention shall remain limited to the assigned purpose and period and shall preserve the evidence required for security, Validation, Review and Remedy.

7.7. Deletion or destruction shall not remove evidence required to demonstrate a material security action, incident, Status effect or Remedy.

7.8. A security control shall not create unjustified exclusion or remove an Accessible Alternative required for a Protected Person.

Article 8: Security monitoring, vulnerability management and evidence

8.1. A Responsible Actor shall monitor the security conditions of each material system, Trust Service, Source, mechanism, device, dependency and Technical Exchange Route within its assigned scope.

8.2. Monitoring shall distinguish:

(a) an ordinary operational event;

(b) a control weakness;

(c) a vulnerability;

(d) an attempted compromise;

(e) a confirmed Security Incident.

8.3. A vulnerability-management process shall address identification, assessment, prioritisation, remediation, mitigation, verification, disclosure and closure.

8.4. A material vulnerability shall be evaluated for its effect on Provider Status, Trust Service Status, Source Status, Trust Object validity, Assurance, Qualified Status, Technical Exchange Permission and dependent Federation Domains.

8.5. A change to security-relevant software, firmware, configuration, algorithm, parameter, mechanism or device shall follow the applicable Change Control route before continued operation under the existing Status or Qualified Scope.

8.6. Monitoring and testing evidence shall identify the scope, time, method, Version, findings, limitations and responsible Actor.

8.7. A monitoring finding or vulnerability record shall not, by itself, change Status or invalidate a Controlled Matter.

8.8. Vulnerability information shall be restricted where disclosure before remediation is capable of increasing risk.

SECTION 4: INCIDENT, CONTINUITY AND RECOVERY MODEL

Article 9: Security Incident classification, recording and notification

9.1. A security event shall be classified as a Security Incident where it affects or is capable of materially affecting a Controlled Matter or Controlled Interaction.

9.2. A Security Incident classification shall identify:

(a) the affected Controlled Matters and Controlled Interactions;

(b) the originating cause and affected period, where known;

(c) the severity and geographic or Federation scope;

(d) the affected Actors and persons;

(e) the affected security conditions, Statuses and dependencies;

(f) the actual and potential Controlled Effects;

(g) the required containment, notification and Recovery actions.

9.3. A Security Incident record shall preserve the evidence necessary for investigation, Status evaluation, Correction, Review, Remedy and historical reconstruction.

9.4. The Responsible Actor shall notify the competent Framework Body, supervision function, affected Actors and affected persons where the applicable Framework Instrument requires notification.

9.5. A notification shall contain only the information necessary and authorised for the recipient and shall not disclose protected investigation or security information without an authorised basis.

9.6. Detection, recording or notification of a Security Incident shall not, by itself, assign liability, change Status, invalidate a Trust Object or determine a final Remedy.

9.7. An incident affecting a Protected Person shall be handled through an accessible communication and Remedy route appropriate to the protection risk.

Article 10: Scoped dependency propagation and Status effects

10.1. The effect of a Security Incident shall be determined for each affected Controlled Matter according to the evidence, affected period, recognised dependency and applicable Profile.

10.2. The incident evaluation shall distinguish effects on:

(a) a Trust Service Provider and its Provider Scope;

(b) each affected Trust Service and Service Scope;

(c) each affected Trust Object or Trust Service Output category and issuance period;

(d) each affected Source and Source Scope;

(e) each affected mechanism, device, component or Technical Exchange Route;

(f) each affected Federation Domain and Cross-Domain Reliance relationship.

10.3. A shared-component incident shall not automatically restrict, suspend, withdraw or invalidate every dependent Controlled Matter.

10.4. A Security Incident affecting a qualified matter shall trigger evaluation of the precise Status-Bearing Matter and Qualified Scope.

10.5. A Trust Object or Trust Service Output created before an incident shall not automatically become invalid unless the evidence and applicable lifecycle rules establish that effect.

10.6. The competent Framework Body shall assign and publish each governance Status change through the applicable decision and Status Publication route.

10.7. A Trust Service Provider or technical operator shall not assign or alter governance Status by reason only of detecting, containing or recovering from an incident.

10.8. Recovery of a technical condition shall not, by itself, reinstate Status, Service Permission, Technical Exchange Permission or Qualified Status.

Article 11: Continuity and Degraded Operation

11.1. A Responsible Actor shall maintain Continuity arrangements proportionate to the criticality, risk, humanitarian consequence and Assurance Conditions of the assigned function.

11.2. Continuity arrangements shall address, where applicable:

(a) loss of personnel or facilities;

(b) loss of systems, devices, Sources, routes or connectivity;

(c) failure of a Trust Service or mandatory dependency;

(d) compromise of security controls or cryptographic material;

(e) protection and Recovery of records, Trust Objects and evidence;

(f) alternative operational and communication arrangements;

(g) priorities, restoration objectives and decision routes.

11.3. Degraded Operation shall occur only where an applicable Framework Instrument and authorised decision permit continued operation under restricted conditions.

11.4. A Degraded Operation decision shall identify:

(a) the affected function, Trust Service or Controlled Matter;

(b) the reason and evidence basis;

(c) the restricted scope and temporary controls;

(d) the permitted interactions and outputs;

(e) the applicable caveats and Reliance Limits;

(f) the start time, review interval and exit condition.

11.5. Degraded Operation shall not continue where a mandatory Security Condition, Protected-Person Safeguard, evidence condition or qualified condition cannot be satisfied.

11.6. An output produced during Degraded Operation shall identify the applicable limitation where the Profile requires that limitation to be communicated.

11.7. Continuity arrangements shall not activate an unrecognised Actor, Trust Service, Source, mechanism, device or Technical Exchange Route.

11.8. Continuity arrangements shall preserve Accessible Alternatives and avoid unjustified exclusion of Protected Persons.

Article 12: Recovery, cross-domain coordination and closure

12.1. Recovery shall restore the required security, operation, evidence and lifecycle conditions for the affected Controlled Matter.

12.2. Before normal operation resumes, the Responsible Actor shall verify:

(a) containment and correction of the originating cause;

(b) Integrity of systems, records, Trust Objects and evidence;

(c) protection of creation data, Validation Data, secrets and cryptographic material;

(d) readiness of mandatory dependencies;

(e) completion of required testing, reassessment and Status evaluation;

(f) completion of required notification and publication actions.

12.3. Where a Security Incident affects more than one Federation Domain, the participating Framework Bodies and Responsible Actors shall coordinate evidence, containment, Status evaluation, communication, Recovery and Remedy under the applicable Federation Agreement.

12.4. Cross-domain coordination shall preserve the Decision Competence, security responsibility, authoritative records and Historical State of each Federation Domain.

12.5. An incident shall be closed only where:

(a) the Recovery evidence is complete;

(b) required corrective actions have been verified;

(c) residual risks have been accepted within assigned Decision Competence;

(d) required Status Publication and Humanitarian Trust List updates are complete;

(e) affected Actors and persons have received required information;

(f) continuing Review, Remedy, monitoring and surveillance obligations are recorded.

12.6. Closure shall preserve the incident record, affected period, Status history, dependency evaluation and evidence required for later Validation, Review and Remedy.

12.7. Closure in one Federation Domain shall not determine closure in another Federation Domain unless the applicable Federation Agreement assigns that effect.

ANNEX E: SOURCE AND AUTHORITATIVE SOURCE MODEL

IDEHA-ANN-SRC-GEN-001 Version: 0.1

SECTION 1: GENERAL PROVISIONS

Article 1: Subject matter, Source boundaries and Status model

1.1. This Annex establishes the common model applicable to Sources, Authoritative Sources and Qualified Authoritative Sources under Parts II, VII and X.

1.2. The Source model shall distinguish:

(a) a recognised Source and its Source Status;

(b) an Authoritative Source and its Authoritative Source Status;

(c) a Qualified Authoritative Source and its Qualified Authoritative Source Status.

1.3. A Source shall remain separate from:

(a) a Trust Service Provider;

(b) a Trust Service;

(c) a Trust Service Output;

(d) a Trust Object;

(e) a Technical Exchange Route;

(f) a Humanitarian Trust List Entry;

(g) a local Authorisation or Controlled Reliance decision.

1.4. Recognition, use, copying, technical availability, registration, publication or exchange of a Source shall not, by itself, assign Authoritative Source Status, Qualified Authoritative Source Status, access, disclosure permission, Service Permission, Technical Exchange Permission or Controlled Reliance.

1.5. A Source shall support one or more Trust Services or other authorised functions only within its recognised Source Scope and applicable conditions.

1.6. A Trust Service Output or Trust Object shall require a Source dependency only where the applicable Profile assigns that dependency.

1.7. This Annex shall not:

(a) define particular data elements, sector datasets, code lists or programme indicators;

(b) prescribe technical schemas, formats, protocols, interfaces or algorithms;

(c) designate a Source or assign Source Status;

(d) authorise access, disclosure, exchange or Controlled Reliance;

(e) convert a Source into a Trust Service, Trust Service Output or Trust Object.

Article 2: Source Profiles

2.1. Each recognised Source shall be governed by an applicable Source Profile.

2.2. A Source Profile shall identify:

(a) the Source and its Identifier;

(b) the Source Holder and Source Steward;

(c) the mandate and recognised purpose;

(d) the Source Scope;

(e) the information, Attribute, Subject or record categories maintained by the Source;

(f) the applicable semantic model, definitions, classifications, taxonomies, controlled vocabularies and code lists;

(g) the Data Quality and Freshness Conditions;

(h) the Provenance and evidence requirements;

(i) the permitted collection, creation, import, transformation, aggregation and derivation methods;

(j) the Access Conditions and Disclosure Conditions;

(k) the permitted Trust Service uses and outputs;

(l) the Correction, Review and Remedy Routes;

(m) the security, retention, archival and lifecycle conditions;

(n) the applicable Assurance Conditions and dependencies.

2.3. A Source Profile shall identify each condition applicable only to part of the Source Scope.

2.4. A Qualified Profile for an Authoritative Source shall identify the additional qualified conditions, Conformity Assessment requirements, surveillance requirements and Qualified Scope.

2.5. A Source Profile or Qualified Profile shall not, by itself, assign Source Status, Authoritative Source Status or Qualified Authoritative Source Status.

2.6. A Technical Specification shall establish the technical schemas, formats, validation rules, interfaces and implementation parameters selected by the Source Profile where such requirements are necessary.

2.7. A change to a Source Profile shall be managed under Part XIII and shall not silently change the meaning or Status of information created under an earlier Version.

Article 3: Source Holder, Source Steward and responsibility separation

3.1. A Source Holder shall maintain and operate the Source within the recognised Source Scope and in accordance with the applicable Source Profile.

3.2. A Source Holder shall remain responsible for:

(a) operational custody and availability of the Source;

(b) implementation of access, disclosure and security controls;

(c) recording of material creation, update, Correction and lifecycle events;

(d) preservation of operational Provenance and evidence;

(e) notification of material changes, incidents and non-conformities.

3.3. A Source Steward shall remain responsible, within its assigned scope, for:

(a) the mandate and recognised purpose of the Source;

(b) semantic definitions and relationships;

(c) classifications, taxonomies, controlled vocabularies and code lists;

(d) Data Quality requirements and evaluation rules;

(e) Provenance and derivation requirements;

(f) Correction and conflict-resolution conditions;

(g) lifecycle and change proposals affecting the Source Profile.

3.4. Where the same Actor performs the Source Holder and Source Steward functions, the responsibilities, evidence and controls applicable to each function shall remain separately identifiable.

3.5. A Source Holder or Source Steward shall not acquire Trust Service Provider Status, Authoritative Source Status, Qualified Authoritative Source Status or Decision Competence by reason only of performing that function.

3.6. Outsourcing of a Source function shall not remove the responsibility assigned to the Source Holder or Source Steward.

3.7. A Source Profile shall identify the Responsible Actor for each material Source function where responsibility is distributed between more than one Actor.

SECTION 2: SOURCE DESIGNATION, QUALIFICATION AND SCOPE

Article 4: Source Designation and Authoritative Source Status

4.1. A Source shall have Authoritative Source Status only through Source Designation by a Framework Body acting within its Decision Competence.

4.2. A Source Designation decision shall identify:

(a) the Source and Source Holder;

(b) the authoritative Source Scope;

(c) the information for which the Source is authoritative;

(d) the recognised purpose;

(e) the evidence supporting the designation;

(f) the applicable Data Quality, semantic, Provenance, Freshness, security and Assurance Conditions;

(g) the Effective Date and review date;

(h) the restrictions, caveats and Reliance Limits;

(i) the Correction, restriction, Suspension and Withdrawal conditions;

(j) the applicable Status Publication arrangement.

4.3. The designation evidence shall identify the basis on which the Source maintains the information within the authoritative Source Scope, including where applicable:

(a) direct creation or registration by the Source under its mandate;

(b) direct receipt from the originating Actor or system;

(c) controlled incorporation from another recognised Source or Authoritative Source;

(d) derivation from identified Source information under a governed rule.

4.4. The bases referred to in paragraph 4.3 shall describe Provenance and shall not create additional Source Status categories.

4.5. Authoritative Source Status shall apply only to the identified Source and authoritative Source Scope.

4.6. Information outside the authoritative Source Scope shall not be treated as authoritative by reason only of its inclusion in the same Source.

4.7. A copy, extract, replica, transformation, aggregation or derivative shall not inherit Authoritative Source Status.

4.8. Authoritative Source Status shall not, by itself, create access, disclosure permission, Authorisation, Service Permission, Technical Exchange Permission or Controlled Reliance.

Article 5: Qualified Authoritative Source Status

5.1. An Authoritative Source shall have Qualified Authoritative Source Status only through Decision-Based Qualification in accordance with Part X.

5.2. Qualified Authoritative Source Status shall require:

(a) an applicable Qualified Profile for the Authoritative Source;

(b) satisfaction of the applicable Data Quality, semantic, Provenance, security, continuity and lifecycle conditions;

(c) completion of the required Conformity Assessment;

(d) resolution of each material non-conformity;

(e) a recorded evidence basis;

(f) a Framework Decision assigning Qualified Authoritative Source Status and Qualified Scope.

5.3. The Qualified Scope shall identify each data, Subject, population, geographic, organisational, temporal, purpose and operational boundary to which Qualified Authoritative Source Status applies.

5.4. Qualified Authoritative Source Status shall not transfer to:

(a) the Source Holder;

(b) the Source Steward;

(c) a Trust Service using the Source;

(d) a Trust Service Output based on the Source;

(e) a Trust Object referring to the Source;

(f) a copy, extract, transformation, aggregation or derivative;

(g) another Source within the same system or organisation.

5.5. A material change affecting the Qualified Scope, Provenance, Data Quality, semantics, security, continuity or lifecycle shall trigger reassessment before Qualified Authoritative Source Status continues to apply to the changed matter.

5.6. The competent Framework Body shall publish authorised Qualified Authoritative Source Status through the Humanitarian Trust List or another governance-controlled publication mechanism where publication is authorised.

5.7. Publication shall communicate Qualified Authoritative Source Status and shall not create that Status.

Article 6: Source Scope

6.1. A Source Scope shall define the precise boundary within which Source Status applies.

6.2. The Source Scope shall identify, where applicable:

(a) the data elements, Attributes, information or record categories;

(b) the Subject or object categories;

(c) the population scope;

(d) the geographic scope;

(e) the organisational scope;

(f) the temporal scope;

(g) the recognised purpose;

(h) the permitted functions and Trust Service uses;

(i) the restrictions and exclusions.

6.3. Source Status applying to one element, category, population, territory, organisation, period or purpose shall not imply Source Status outside that boundary.

6.4. A Source Scope shall distinguish information for which the Source is authoritative from information that is informative, imported, derived, provisional, disputed or outside the authoritative scope.

6.5. Overlapping Source Scopes shall be recognised only where the applicable Source Profiles and Framework Decisions define:

(a) the relationship between the Sources;

(b) the purpose for which each Source is used;

(c) the treatment of consistency and conflict;

(d) the applicable precedence, escalation and Review conditions;

(e) the effect on Trust Service Outputs and Controlled Reliance.

6.6. Resolution of conflicting Source information shall not alter Source Status unless a Framework Decision assigns that Controlled Effect.

6.7. A Relying Actor shall determine acceptance of Source information within its applicable Trust Acceptance Policy and shall not alter the Source Status assigned by a Framework Body.

SECTION 3: QUALITY, SEMANTICS, PROVENANCE AND TIME

Article 7: Data Quality and semantic governance

7.1. A Source Holder shall maintain Data Quality in accordance with the applicable Source Profile.

7.2. The applicable Source Profile shall define the required conditions concerning:

(a) accuracy;

(b) completeness;

(c) consistency;

(d) validity;

(e) uniqueness;

(f) currentness and timeliness;

(g) traceability;

(h) semantic consistency;

(i) Correction.

7.3. Data Quality shall be evaluated within the Source Scope and for the recognised purpose and shall not be inferred from a general quality statement applying to another scope or purpose.

7.4. A Source Steward shall govern the semantic artefacts required to interpret Source information, including where applicable:

(a) canonical definitions;

(b) concept and relationship models;

(c) ontologies;

(d) taxonomies and classifications;

(e) controlled vocabularies and code lists;

(f) multilingual labels and script representations;

(g) rules for cardinality, validity and permitted value states.

7.5. Estimated, approximate, incomplete, disputed, unverified, derived, unknown, unavailable, withheld and not-applicable values shall remain distinguishable where those states are relevant to interpretation or reliance.

7.6. A semantic change shall identify the affected concept, earlier and later meaning, Version, Effective Date, compatibility condition and migration treatment.

7.7. A semantic change shall not retrospectively alter the meaning of information created under an earlier Version.

7.8. A quality or semantic limitation capable of affecting Trust Service use or Controlled Reliance shall be recorded and made available through the applicable Profile, Source evidence or output caveat.

Article 8: Provenance, copying, transformation, aggregation and derivation

8.1. Provenance shall enable reconstruction of the origin, custody, generation, import, transformation, Correction, supersession and lifecycle of Source information.

8.2. Provenance shall identify, where applicable:

(a) the originating Source, Actor or system;

(b) the method and time of creation or collection;

(c) the responsible Actor or automated function;

(d) each import, copy, extraction or replication event;

(e) each material transformation, normalisation or aggregation;

(f) each derivation rule and Version;

(g) each Correction, supersession or replacement;

(h) the applicable Source Status, Source Scope and Version at the relevant time.

8.3. A copy, extract or replica shall identify the originating Source and the conditions under which synchronisation, Correction and Status changes are propagated.

8.4. A transformation or aggregation shall identify:

(a) each input Source or record;

(b) the transformation or aggregation rule;

(c) the rule Version;

(d) the responsible Actor or system;

(e) the processing time;

(f) each material quality or semantic effect;

(g) the conditions for Correction and reprocessing.

8.5. A derived value shall identify:

(a) each Source value on which it depends;

(b) the derivation rule and Version;

(c) the derivation time;

(d) the responsible Actor or system;

(e) the quality, Freshness and uncertainty conditions;

(f) the conditions for re-derivation.

8.6. A copy, extract, replica, transformation, aggregation or derivative shall constitute a separate Controlled Matter where independently maintained or relied upon.

8.7. A separate Controlled Matter referred to in paragraph 8.6 shall require separate Source recognition where it is to be treated as a Source.

8.8. Provenance information shall be protected against unauthorised alteration and retained for the period required for Validation, Review, Remedy and Historical State reconstruction.

Article 9: Freshness, Version and Historical State

9.1. Source information used for an identified purpose shall satisfy the applicable Freshness Condition.

9.2. A Freshness Condition shall identify:

(a) the relevant event or observation time;

(b) the record creation or update time;

(c) the maximum permitted age or review interval;

(d) the conditions requiring re-verification or re-collection;

(e) the treatment of unavailable or stale information.

9.3. Event time, record time, update time, retrieval time, Verification time and Trust Object issuance time shall remain distinguishable where relevant to the purpose.

9.4. A Version of a Source shall identify an immutable state of the Source structure, semantics, rules or controlled content to which that Version applies.

9.5. A later Version of a Source shall not overwrite the Historical State required to evaluate an earlier Trust Service Output, Trust Object, decision or Controlled Reliance.

9.6. Historical State shall identify, where applicable:

(a) the Version of the Source;

(b) the Source Status and Source Scope;

(c) the semantic and quality rules;

(d) the relevant records and Provenance;

(e) the applicable restrictions, caveats and dependencies;

(f) the Effective Date and period of application.

9.7. A later Correction or Status change shall not retrospectively alter an earlier Historical State unless an authorised decision assigns that effect on a recorded evidence basis.

SECTION 4: ACCESS, VERIFICATION, LIFECYCLE AND CROSS-DOMAIN USE

Article 10: Access, disclosure and purpose boundaries

10.1. Access to a Source shall remain separate from disclosure, Trust Service use, Technical Exchange Permission, Authorisation and Controlled Reliance.

10.2. A Source Holder shall provide access or disclosure only where:

(a) the Requesting Actor is identified and authenticated as required;

(b) the purpose is authorised;

(c) the applicable Access Conditions are satisfied;

(d) the applicable Disclosure Conditions are satisfied;

(e) the information is limited to what is necessary for the authorised purpose;

(f) the applicable security and Protected-Person Safeguards are satisfied;

(g) the required evidence is recorded.

10.3. A Technical Exchange Route, Endpoint, discovery record or successful Authentication Outcome shall not, by itself, create access or disclosure permission.

10.4. Source recognition, Authoritative Source Status or Qualified Authoritative Source Status shall not, by itself, create access or disclosure permission.

10.5. A Source Holder shall enforce purpose, access, disclosure, onward-use, retention and deletion conditions within its responsibility.

10.6. A Trust Service Provider using a Source shall remain responsible for compliance with the Service Scope, applicable Profile and Authorisation Outcome.

10.7. A Relying Actor shall remain responsible for acceptance and Controlled Reliance under its applicable Trust Acceptance Policy.

10.8. Cross-domain access shall not circumvent the controls of the originating or receiving Federation Domain.

10.9. Access, disclosure, refusal and restriction decisions having a material effect shall remain attributable, traceable and reviewable.

Article 11: Source Verification and separate representation

11.1. Source Verification shall evaluate specified properties of a Source or Source Basis within the Service Scope of a Validation and Verification Service.

11.2. Source Verification shall identify, where applicable:

(a) the Source and Source Scope;

(b) the Source Status and relevant Effective Date;

(c) the property or condition evaluated;

(d) the evidence and Status information used;

(e) the applicable Profile and Version;

(f) the evaluation time and Freshness Condition;

(g) the Verification Result;

(h) each limitation, caveat and indeterminate condition.

11.3. Source Verification shall produce a Verification Result and shall not alter the Source, Source Status, Source Scope or underlying Source record.

11.4. A Verification Result shall not, by itself, assign Authoritative Source Status, Qualified Authoritative Source Status, access, disclosure permission, Authorisation or Controlled Reliance.

11.5. Where Source information or a Verification Result is represented in an Electronic Attestation, the Electronic Attestation shall constitute a separate Trust Object issued through an Electronic Attestation Service.

11.6. The Electronic Attestation referred to in paragraph 11.5 shall have its own Issuer, Identifier, Serial Number, Profile, Status, protection, dependencies and lifecycle.

11.7. Issuance of an Electronic Attestation shall not convert the Source, Source record or Verification Result into an Electronic Attestation.

11.8. Unavailability of a Source or required evidence shall produce the indeterminate or unavailable outcome defined by the applicable Profile and shall not be represented as a negative factual determination without an evidence basis.

11.9. Historical Source Verification shall use the Source Status, Source Scope, Version, semantics, Provenance and evidence applicable at the relevant time.

Article 12: Correction, lifecycle and cross-domain recognition

12.1. A recognised Source shall have accessible Correction, Review and Remedy Routes proportionate to its purpose, Source Scope and potential Controlled Effects.

12.2. A Correction record relating to a Source shall identify:

(a) the affected Source information;

(b) the error, omission or inconsistency;

(c) the evidence basis;

(d) the corrected information;

(e) the Effective Date;

(f) the responsible Actor;

(g) the effect on dependent Controlled Matters;

(h) the required notification or re-evaluation.

12.3. Correction of Source information shall not alter an existing signed, sealed, timestamped or otherwise integrity-protected Trust Object or Trust Service Output.

12.4. Where corrected Source information affects an existing Trust Service Output or Trust Object, the responsible Actor shall apply the applicable re-evaluation, replacement, supersession, restriction, Suspension, Withdrawal, Revocation, notification or corrective-issuance procedure.

12.5. A Framework Body shall restrict, suspend, withdraw or reinstate Source Status only within its Decision Competence and on a recorded evidence basis.

12.6. A Source lifecycle action shall affect a dependent Trust Service, Trust Service Output or Trust Object only through an identified dependency and within the affected scope and time.

12.7. Restriction, Suspension or Withdrawal of Source Status shall not automatically invalidate a Trust Service Output or Trust Object created before the Effective Date of that action.

12.8. Cross-domain recognition and use of a Source shall identify:

(a) the originating and receiving Federation Domains;

(b) the Source Status and Source Scope;

(c) the Federation Trust Relationship;

(d) the recognised purpose;

(e) the Access Conditions, Disclosure Conditions and Reliance Conditions;

(f) the Correction, Review, Remedy and incident-coordination routes.

12.9. Source Status in one Federation Domain shall not automatically create equivalent Source Status in another Federation Domain.

12.10. The competent Framework Body in the receiving Federation Domain shall determine recognition within its Decision Competence, and each Relying Actor shall determine acceptance under its applicable Trust Acceptance Policy.

12.11. Cross-domain coordination shall not transfer Decision Competence between Federation Domains unless a Federation Agreement expressly assigns that Decision Competence.

12.12. Historical Source Status, Version, Provenance, Correction and cross-domain recognition information shall remain reconstructable for Validation, Review, Remedy and Controlled Reliance.

IMPLEMENTATION GUIDELINES

i Companion document

The Implementation Guidelines are published as a separate companion document: IDEHA Trust Framework — Implementation Guidelines.