D3.2

Conceptual Framework for Trust Schemes (2)

Document Identification	
Date	28.08.2018
Status	Final
Version	Version 1.0

Related WP	WP2	**Related Deliverable(s)**	D3.1, D2.1
Lead Authors	FHG	**Dissemination Level**	PU
Lead Participants	FHG	**Contributors**	USTUTT, TUG, G+D, ATOS,TUBITAK,DTU,GS, OIX
Reviewers	Martin Hoffmann (NLNET), Jon Shamah (EEMA)		

This document is issued within the frame and for the purpose of the LIGHT*est* project. LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No 700321.

1. Executive Summary

This document provides a Conceptual Framework for Trust Schemes in LIGHTest. This is the second deliverable, which presents a refined and aligned description of the Conceptual Framework for Trust Schemes, which uses D3.1 submitted in project month M08 as bedrock and also incorporates the results of the WP3 tasks T3.2 “Design of DNS-based Publication of Trust Schemes”, and T3.3 “Discovery of Trust Scheme Publication Authorities”.

The Conceptual Framework for Trust Schemes in LIGHTest includes a data model for a unified representation of Tuple-Based Trust Schemes, along with a Concept of the Trust Scheme Publication Authority (TSPA) which outlines how Boolean, Ordinal, and Tuple-Based Trust Schemes can be published. The TSPA hereby consists of the DNS Name Server with DNSSEC Extension, and Trust Scheme Providers. The latter can be implemented as regular HTTPS components. The DNS Name Server is only used for discovering a claim of Boolean or Ordinal Trust Scheme Association with an Issuer, and for Discovery of the Trust List which is provided by the Trust Scheme Provider. The usage of the DNS Name Server with DNSSEC for discovery of the associated Trust Scheme, and of the Trust List aligns well with existing usages of DNS, which is expected to support adoption of the LIGHTest infrastructure.

The Trust Scheme Provider publishes a signed Trust List, which indicates that an Issuer operates under the Trust Scheme of the Trust Scheme Provider. For the representation of these Trust Lists in LIGHTest, the existing and widely accepted standard for trust lists ETSI TS 119 612 [1] is used. This also enables integration of LIGHTest within eIDAS. Furthermore, the Trust Scheme Provider may publish Tuple-Based Trust Scheme Publications. This kind of Trust Scheme Publication includes information on the requirements that an Issuer must adhere to, in order to operate under the Trust Scheme.

These requirements are laid out in Trust Schemes such as STORK QAA/AQAA, eIDAS, PCTF, the Electronic Signature Law of the People’s Republic of China, FIDO, the international standard ISO/IEC 29115:2013, the Turkey Electronic Signature Law, the Minors Trust Framework, the Trust Scheme of Azerbaijan, and the Embedded UICC Remote Provisioning Scheme. However, when comparing the requirements between trust schemes, they may be synonymous. Additionally, when transferring the requirements into attributes and values, the attribute domain which includes all possible values, may be unlimited. Both synonymous attributes, and unspecified attribute domains may hinder automated processing by the Automatic Trust Verifier (ATV), as foreseen in D2.14.

Therefore, a unified data model for Tuple-Based Trust Scheme Publications is described. This unified data model was obtained by consolidating selected Trust Schemes, and refining the obtained requirements, towards attributes with specified domains. This resulted in a Data Model which contains attributes with domains which are either a finite set of values, or even boolean. For a few attributes however, the attribute domain remains underspecified, e.g. for the attribute authoritative party, where the exact number is currently unknown and will vary over time. This needs to be considered in the processing by the ATV. For the publication of Tuple-Based Trust

Schemes, a standardized data representation for the tuples was developed which can be either added to the signed trust list or stored in an extra document with a pointer from the signed trust list to this extra document.

2. Document Information

2.1 Contributors

Name	Partner
Sebastian Kurowski	FHG
Sven Wagner	USTUTT
Uwe Laufs	FHG
Heiko Roßnagel	FHG
Peter Lipp	TUG
Olamide Omolola	TUG
Frank-Michael Kamm	G+D
Rachelle Sellung	USTUTT
Lorenzo Rosa	ATOS
Miryam Villegas	ATOS
Javier Presa	ATOS
Miguel A. Mateo	ATOS
Muhammet Yildiz	TUBITAK
Melis Cetinkaya	TUBITAK
Edona Fasllija	TUBITAK
Elif Ustundag	TUBITAK
Burcin Bozkurt	TUBITAK
Sebastian Mödersheim	DTU
Rasmus Birkedal	DTU
Bihan Ni	DTU
Jesse Kurtto	GS
Sue Dawes	OIX
Michelle Parks	OIX
Arif Mailov	Ministry of Communications and High Technologies of the Republic of Azerbaijan

2.2 History

Version	Date	Author	Changes
V0.1	20.06.2018	FHG	Initial draft, Table of Content
V0.15	26.06.2018	FHG, USTUTT, TUBITAK, OIX	Update section 6, Draft for Section 7.10, Draft for Section 7.11,
V0.2	12.07.2018	TUBITAK, OIX, USTUTT G+D DTU	Update Section 7.2.8 Update Section 7.2.9 Section 7.2.7 Section 7.2.11 Section 7.2.12
V0.3		TUBITAK, OIX, G+D, DTU, USTUTT, FHG	Section 7.3
V0.5		FHG, USTUTT	Section 7.4,7.5,7.6

V0.7		ATOS, FHG	Section 7.5
V0.8	03.08.2018	FHG, USTUTT	Compilation of final draft
V1.0	27.08.2018	FHG	Integrating review suggestions, formatting changes

3. Table of Contents

3.1 Table of Figures

3.2 Table of Tables

3.3 Table of Acronyms

ATV	Automatic Trust Verifier
CA	Certification Authority
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
TLS	Transport Layer Security
TSP	Trust Service Provider
TSPA	Trust Scheme Publication Authority

4. Scope of the Deliverable

This Deliverable D3.2 is the second Deliverable, which describes the Conceptual Framework for Trust Schemes in LIGHTest. The overall goal of this deliverable is to introduce a representation of generic trust schemes in suitable data formats, and to provide the concept for publication of trust schemes. The bedrock for this deliverable is D3.1, which has outlined the first version of the Conceptual Framework for Trust Schemes in a timely fashion in M08 of the project. Furthermore, D3.2 builds upon the results of D3.3 “DNS-based Publication of Trust Schemes”, and D3.4 “Discovery of Trust Scheme Publication Authorities”, as well as the identified Trust Schemes in Deliverable D2.1, D2.7 “Relevant DNSSEC Concepts and Basic Building Blocks” and the Reference Architecture which is outlined in D2.14.

In the following, the Conceptual Framework for Trust Schemes is introduced by providing a Concept for the Trust Scheme Publication Authority (TSPA), and the Publication of Boolean, and Ordinal Trust Schemes (Section 6). Additionally, a Data Model for the Publication of Tuple-Based Trust Schemes is introduced based upon the Consolidation of selected existing trust schemes (Section 7).

The Deliverable therefore first outlines the TSPA and its components (Section 6.1), along with the usage of the TSPA in the Reference Architecture of LIGHTest (Section 6.2). Publication of Boolean and Ordinal Trust Schemes, along with the respective Trust Lists is discussed in Section 6.3, including the underlying Trust Model (Section 6.3.1), the Publication of Trust Lists in Compliance with eIDAS (Section 6.3.2), Querying of the Trust Scheme Association of an Issuer (Section 6.3.3), and Querying of Tuple-Based Trust Schemes (Section 6.3.4).

In order to provide a unified representation of Tuple-Based Trust Schemes, which can be processed by the ATV for automated trust verification, Section 7 introduces the Data Model for Tuple-Based Trust Scheme Publications. This includes a description of the modelling methodology in Section 7.1, and an introduction of the Trust Schemes that have been considered for modelling the unified representation (Section 7.2). The retrieved concepts of Tuple-Based Trust Schemes are described in Section 7.3. These concepts have been further refined towards attributes with strictly defined attribute domains. These attributes provide the unified representation. The unified data model is presented in Section 7.4. The approach and an example for the publication of Tuple-Based Trust Schemes is presented in Section 7.5. The modelling of the publication of Tuple-Based Trust Schemes is demonstrated for another trust scheme, which is not considered in the consolidation process in Section 7.6.

5. Terminology

The following provides a description of terms that are used within the Conceptual Framework for Trust Schemes. It builds upon the Terminology in D2.14.

Entity

An Entity is a person, organization, or thing that is enrolled in a Trust Scheme and certain attributes of which are certified by a Trust Scheme Authority.

Trust Scheme

A Trust Scheme is operated by a Trust Scheme Authority and comprises the organizational, regulatory/legal, and technical measures to assert trust-relevant attributes about enrolled Entities in a given domain of trust. A Trust Scheme operates in a given Trust Domain and typically has a declared or implied purpose.

Trust Scheme Publication

The main purpose of the Trust Scheme Publication Authority (TSPA) is to provide the associated Trust Scheme Publication for an Entity, e.g. the Issuer of a Certificate. A Trust Scheme Publication is always operated by a Trust Scheme Provider, and associated with a Trust List which indicates that an Entity operates under the Trust Scheme, which the Trust Scheme Publication corresponds to. A Trust Scheme Publication in LIGHTest can be a Boolean, Ordinal and Tuple-Based Trust Scheme Publication.

Boolean Trust Scheme Publication

A Boolean Trust Scheme Publication indicates that an Entity operates under the Trust Scheme. A Boolean Trust Scheme Publication can be provided by publishing a Trust List under the Trust Scheme Name. Any Trust Scheme in LIGHTest can be published as one Boolean trust scheme. For example, a Boolean Trust Scheme Publication can contain a list of all companies that meet the requirements of a Trust Scheme.

Ordinal Trust Scheme Publication

An Ordinal Trust Scheme Publication indicates that an Entity operates under an ordinal value of the Trust Scheme that the Publication corresponds to. Typically, this ordinal value is a Level of Assurance (LoA). An Ordinal Trust Scheme Publication can be provided by publishing a Trust List under the Ordinal Value of the Trust Scheme and the Trust Scheme Name. Therefore, any Trust Scheme in LIGHTest, which provides ordinal values (e.g. LoAs), can be published as Ordinal Trust Scheme Publications. Any Ordinal Trust Scheme Publication corresponds to exactly one ordinal value of the Trust Scheme. For example, an Ordinal Trust Scheme Publication can contain a list of all companies that meet the LoA3 level requirements of a Trust Scheme.

Tuple-Based Trust Scheme Publications

A Tuple-Based Trust Scheme indicates the tuples of a Boolean or Ordinal Trust Scheme Publication, that an Entity operates under. Tuples are data pairs in the form of attributes and values. They contain the requirements of the Trust Scheme and it is provided for further reasoning by the ATV, after the discovery of the Trust List. Any Boolean or Ordinal Trust Scheme Publication can be accompanied by a Tuple-Based Trust Scheme Publication. For example, a Tuple-Based Trust Scheme Publication can contain a list of all Trust Schemes that a company participates in (e.g. indicating that company A is supervised, that company A is rated as LoA3, and that company A is ISO certified).

Trust List

A Trust List is a specific data file of a specific format that is certified by the issuing authority (e.g., via electronic signature). It provides a list of all the enrolled entities. Trust Lists in LIGHTest can be associated with a Boolean or Ordinal Trust Scheme Publication.

Trust Scheme Provider

A Trust Scheme Provider operates a Trust Scheme. It decides, whether an Entity is associated with its Trust Scheme. The Trust Scheme Provider in LIGHTest provides the Trust Lists for a Trust Scheme, and may further provide a Tuple-Based Trust Scheme Publication of its Trust Scheme.

Automatic Trust Verifier

The Automatic Trust Verifier (ATV) in LIGHTest takes an Electronic Transaction and Trust Policy as input (see D2.14). The ATV provides as outputs if the Electronic Transaction is trustworthy and optionally with explanation of its reasoning. It uses a pluggable parser for Electronic Transactions as sub-component. More information are provided in the deliverables of the Work Package 6.

6. Concept for Trust Scheme Publications

6.1 Outline of the Trust Scheme Publication Authority

A Trust Scheme Publication Authority (TSPA) enables the ATV to acquire a signed trust list, using a DNS Name Server with DNSSEC extension. A server publishes one or multiple Trust Lists under different sub-domains of the Authority's domain name. A TSPA therefore provides the capability for the ATV to look-up the association of an identifier with a trust scheme, or the properties of the trust scheme which constitute trust.

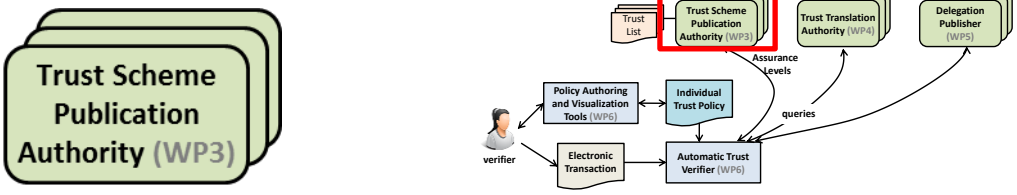

Figure 1 Trust Scheme Publication Authority

The TSPA consists of two components. It uses an off-the-shelf DNS Name Server with DNSSEC extension, in order to enable discovery of the Trust Scheme Provider that operates a Trust Scheme. The Trust Scheme Provider constitutes the second component of the TSPA. It provides a signed Trust List, which indicates that a certificate Issuer is trusted under the scheme operated by the Trust Scheme Provider. It further provides the Tuple-Based representation of a Trust Scheme (see Figure 2).

Figure 2 Components of the TSPA

As the DNS Name Server is only used to provide pointers to location of resources rather than storing the respective resources as DNS resource records directly, the TSPA is well-aligned with existing DNS practices.

Possibilities of Trust Scheme Representations

Table 1 provides an overview on the possible representations of a trust scheme in LIGHTest. All types of Trust Schemes can be published in an Ordinal, Tuple-Based or Boolean representation. While Ordinal Trust schemes can be published in a Tuple-Based or Boolean representation, Boolean and Tuple-Based Trust Schemes cannot be represented in an Ordinal representation.

From \ To	Boolean	Ordinal	Tuple-Based
Boolean	Yes	No	Yes
Ordinal	Yes	Yes	Yes
Tuple-Based	Yes	No	Yes

Table 1 Possibilities of Trust Scheme Representations

This means, that a Trust Scheme can be published as Ordinal Trust Scheme Publication (e.g. LoA3.ISO29115), Boolean Trust Scheme Publication (e.g. ISO29115), and Tuple-Based Trust Scheme Publication (e.g. tuples.ISO29115 or tuples.LoA3.ISO29115) at the same time in LIGHTest.

6.2 Querying of Trust Schemes with the TSPA

The LIGHTest Reference Architecture [2] introduces various scenarios, in which the TSPA is contributing to the automated trust verification. In these scenarios the TSPA provides the capability of responding to a DNS query issue for a certificate issuer name, and the verification of the DNS signature chain (see Figure 3).

In the scenarios provided by [2], the ATV extracts the signer certificate that was used for an electronic transaction along with Issuer certificate (Step 2). This is followed by a validation of the document signature with the signer certificate, and of the signer certificate signature with the issuer certificate (Steps 3 and 4). Finally, the issuer name is extracted from the certificate (Step 5).

The TSPA is now used for retrieving the associated trust scheme (Step 6).

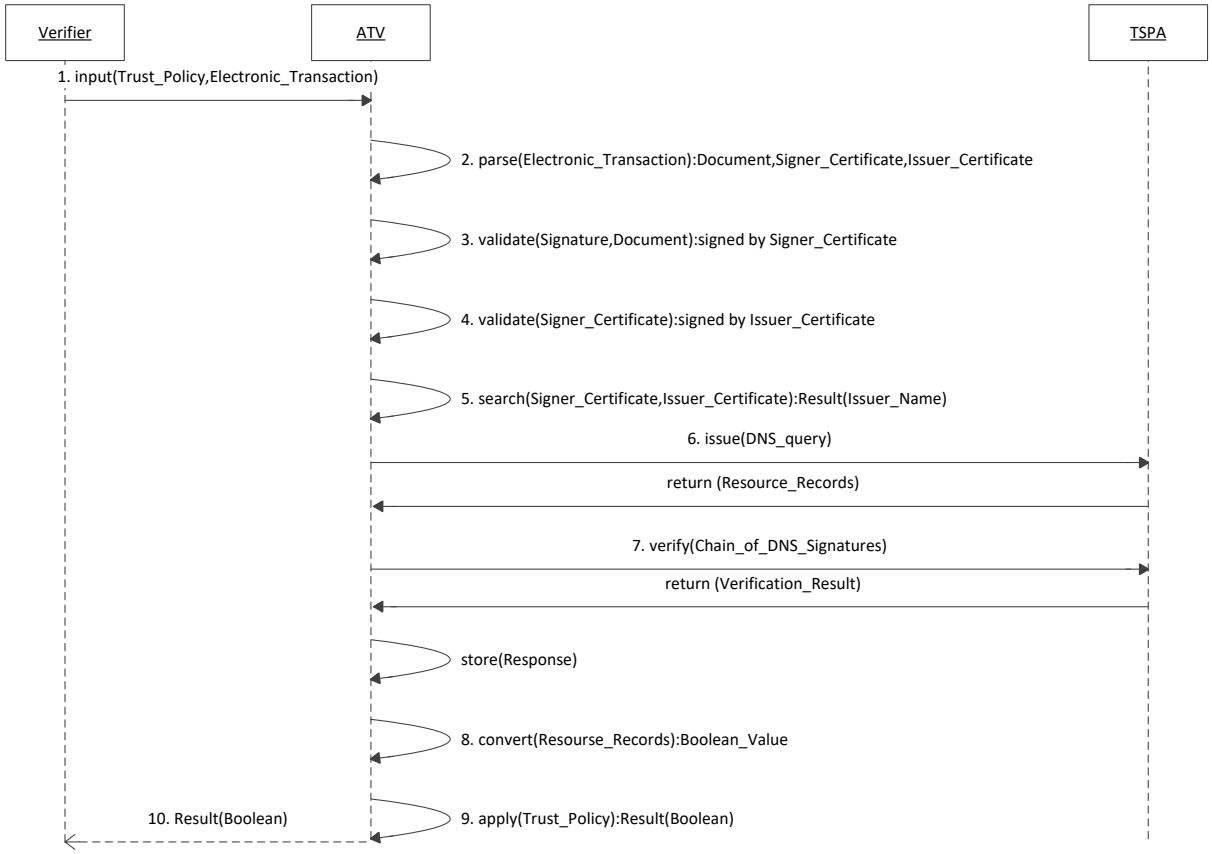

Figure 3 Scenario for qualified electronic signatures and boolean trust schemes [2]

At Step 6, the ATV only knows the Issuer Name but not the associated Trust Scheme. Therefore, discovery of the Trust Scheme, and the operating Trust Scheme Provider is required. The following notation aims at indicating the exchanges that take place between the ATV and the TSPA.

The ATV queries the DNS records for the Issuer Name which contains a claim that the issuer operates under a certain trust scheme (Steps 1 – 4).

1. ATV: The ATV extracts the Issuer Name
2. ATV: The ATV extracts the Scheme Name from the claim of the Issuer in the DNS records of the Issuer Name
3. ATV → TSPA/DNS: The ATV contacts the TSPA and provides the Scheme Name
4. TSPA/DNS → ATV: The TSPA provides the Trust Scheme Provider

5. ATV → TSPA/Trust Scheme Provider: The ATV contacts the Trust Scheme Provider and provides the Scheme Name and the Issuer Name
6. TSPA/Trust Scheme Provider → ATV: The Trust Scheme Provider provides a statement indicating that the Issuer operates under the provided Scheme Name, signed with the Trust Scheme Provider Certificate
7. ATV → TSPA/DNS: The ATV contacts the TSPA and provides the Scheme Name
8. TSPA/DNS → ATV: The TSPA provides the SMIMEA record for the Scheme Name
9. ATV: The ATV verifies if the certificate used for signing the trusted list was valid

Therefore, the ATV requests a signed statement by the Trust Scheme Provider which indicates that the Issuer operates under the Trust Scheme (Step 5 – 6). For the verification that the statement was retrieved from the correct Trust Scheme, the validity of the certificate used for signing the trust list is checked making use of the SMIMEA resource record data.

Technically, the obtained DNS records after Step 4 contain the set of all the trust schemes the issuer claims to operate under. In case the issuer claims to operate under more than one trust scheme, the following Steps 4 – 9 need to be repeated for all schemes that were recognised by the ATV.

Discovery of the Trust Scheme, under which an Issuer operates therefore, always requires querying the DNS Name Server with DNSSEC extension and the Trust Scheme Provider. The latter provides a signed statement of association of an Issuer with the Trust Scheme. Such statements can be provided by using existing standards on Trust Service Status Lists (TSLs), as e.g. ETSI TS 119 612 [1].

6.3 Publication of Trust Schemes in the TSPA

Figure 4 provides an overview on the concept for trust scheme publishing in the TSPA. Since the TSPA is using the DNS Name Server mainly for pointing towards the Trust Scheme Provider and the tuple-based representation of a trust scheme, the concept is divided into the DNS records on the DNS Name Server (left side), and the data containers on the Trust Scheme Provider (right side). Figure 4 is an updated version compared to D3.1 [3].

The DNS Name Server may communicate via UDP or TCP (if possible), whereas the Trust Scheme Provider is provided as a HTTPS component and communicates via TCP. The used transport protocol does not affect the functionality of the TSPA and is therefore exchangeable. The Trust Scheme Provider uses TLS for securing the communication channel, in order to comply with the Security and Accountability Requirements (SAR) of LIGHTest.

The records on the DNS Name Server include a Data Container for the Issuer, and for boolean and ordinal trust schemes. Data Containers for an Issuer are identified by an Issuer Name, and include the Name of the associated Trust Scheme (SchemeName). Data Containers for a Trust Scheme are identified by a SchemeName, in the boolean case, and an additional LevelName in the ordinal case. A Trust Scheme data container includes the Trust Scheme Provider Domain Name (SchemeProviderName).

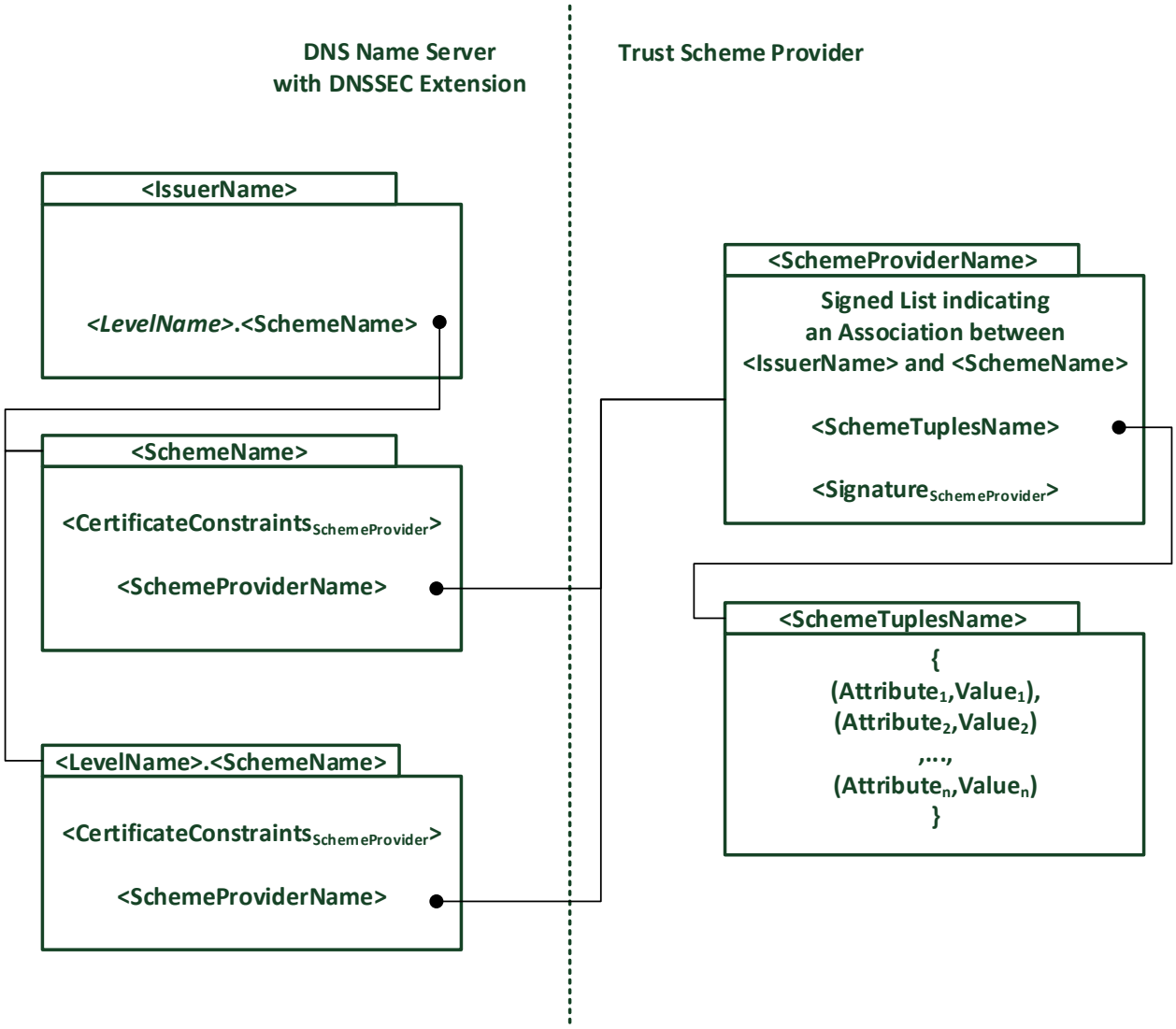

Figure 4 Overview on the concept for trust scheme publishing in the TSPA

In the updated version, the data containers for the Issuer, trust scheme name and ordinal level of a trust scheme do not include the fingerprints of the corresponding certificates of the issuer and trust scheme provider anymore as resource records. Instead, the certificates, which are accepted for signing the trust list, are limited. This can be realized by publishing certificate constraints in the DNS using the SMIMEA DNS resource record. These modifications in the resource records are a result from the consolidated approach to publishing trust-related information in the DNS (for further details see e.g. Section 5 in D3.3 [4] or D3.4 [5]).

The SMIMEA resource record was introduced in the deliverable D2.7 “Relevant DNSSEC Concepts and Basic Building Blocks” [6] and it is defined in [7]. The SMIMEA mechanism associate an SMIME user’s certificate with the intended domain name by a number of ways to limit the accepted certificates (CertificateConstraints). In LIGHTest, the SMIMEA resource record

is used to verify if the certificate used for signing the trust list is valid. This is explained in more detail and demonstrated by way of example in D3.4 [5].

For the publication of tuple-based trust schemes, the tuples are published either in the signed trust list itself or listed in an extra document with a pointer from the signed trust list to this document. For both cases, there is no additional DNS entry for the tuple-based trust schemes required. It uses the same as for the Trust Scheme Provider

6.3.1 Trust Model of Trust Scheme Publication and Querying

The Trust Scheme Publication Authority involves both a DNS Name Server component, and at least one Trust Scheme Provider. This means that the TSPA operates in light of multiple possible stakeholders and hence is a joint operation by many different parties. The purpose of this section is therefore to indicate the trust relationships between the different stakeholders, which are required for operating, and using the TSPA.

The key purpose of the automated trust validation provided by the ATV in LIGHTest is to assure the ATV user that the Issuer of a certificate operates under a trusted scheme. Any scenario indicated in D2.14 involves the ATV, and the Issuer of a certificate (see Figure 5).

DNSSEC introduces a trust chain from the DNS root towards the respective DNS Name Servers, whereas each key pair used by a DNS Name Server operator for signing resource records is verifiable with the DNS Name Server that is higher in the hierarchy. If one assumes that the ATV trusts the DNS root, trust in the Operator of the DNS Name Server that contains the Issuer Records (DNS Ops Issuer), and the Trust Scheme Records (DNS Ops Scheme) can be inferred via verification against the certificate chain.

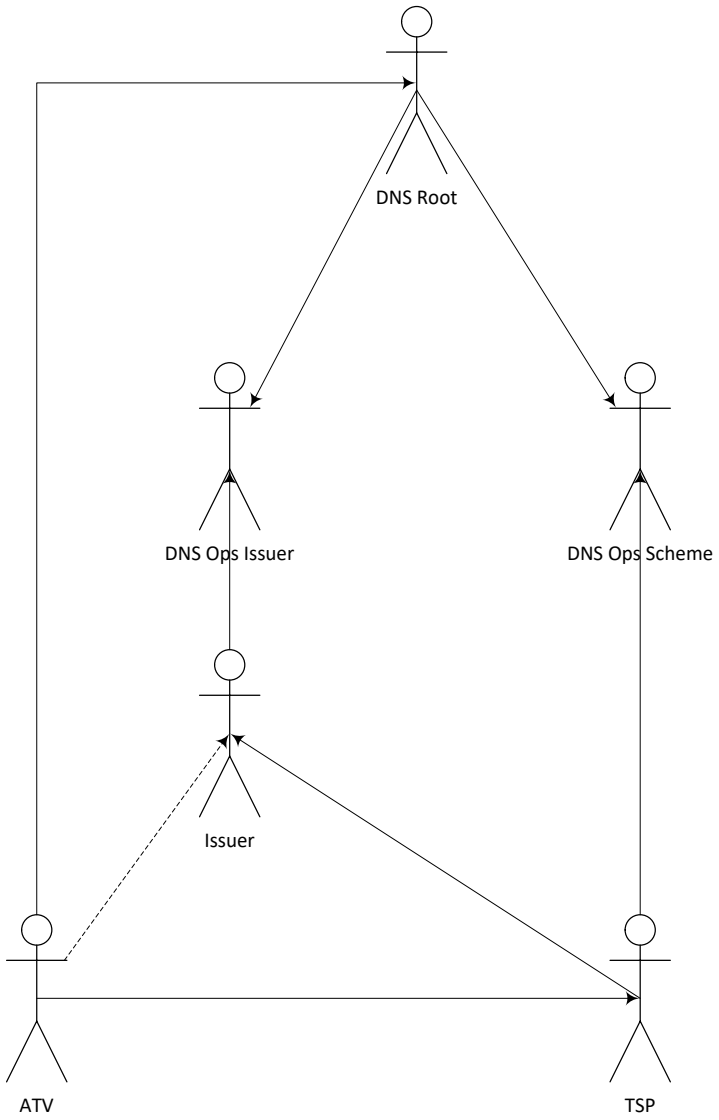

Figure 5 Trust Relationships around the TSPA. Solid lines indicate trust, dashed lines indicate an inferred trust relationship

The Issuer of a Certificate must ensure, that the DNS Ops Issuer is maintaining correct DNS Records for the Issuers' Certificate. This can too be verified from Trust in the DNS Root. Furthermore, it is provided, if the Issuer also acts as the Operator of the DNS Name Server that contains the DNS Records for the Certificate Issuer (DNS Ops Issuer).

The same holds for the Trust Scheme Provider. Trust of the Trust Scheme Provider in the DNS Ops Scheme can also be implied from Trust in the DNS Root. Furthermore, it is provided if the Trust Scheme Provider also acts as the Operator of the DNS Name Server that contains the DNS Records for the Trust Scheme Provider (DNS Ops Scheme).

If the Issuer also acts as the Operator of the DNS Name Server, the DNS Ops Issuer may be able to publish false Scheme Associations for an Issuer. In fact, this will lead to a "denial of

service" (i.e., not finding a scheme association at all) rather than a false association, because the published scheme association is only a claim. Accordingly, if the Trust Scheme Provider also acts as the DNS Name Server, the DNS Ops Scheme may be able to publish false Trust Scheme Provider Locations. However, this issue can be mitigated by using contractual obligations between Issuer and the DNS Ops Issuer, and the Trust Scheme Provider and DNS Ops Scheme.

Under these circumstances, the ATV can infer trust in an Issuer, by using it's Trust Policy: Discovery of the Trust Scheme Provider is assumed to be trusted, due to the Trust in the DNS Root. Therefore, the ATV can use the trust membership claim provided by DNS Ops Issuer to discover the Trust Scheme Provider, and finally verify the trust membership claim with the signed statement of the Trust Scheme Provider.

It should be noted that 'trust' in the sense of this Deliverable only refers to the conviction that the technical validation of assertions in relation to a trust scheme is done correctly. The legal trust that such assertions are factually true and can be relied upon (if this is required for a use case) must be created externally, e.g. through legislation, contracts or policies. This topic is further explored in other deliverables, notably D6.7 Cross-Border Legal Compliance and Validity of Trust Policy and Trust Decisions.

6.3.2 Representation of Trust Scheme Associations in the Trust Scheme Provider

ETSI TS 119 612 [1] provides "a format and mechanisms for establishing, locating, accessing and authenticating a trusted list which makes available trust service status information so that interested parties may determine the status of a listed trust service at a given time." [1, p. 9] As such it includes a format for Trusted Lists which include" information about the status and the status history of the trust services (including certification services) from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation" [1, p. 12]. Publication of Trusted Lists is hereby achieved via Trust-service Status Lists (TSLs), which make "available trust service status information such that interested parties may determine whether a trust service is or was operating under the approval of any recognized scheme at either the time the service was provided, or the time at which a transaction reliant on that service took place." [1, p. 11]. Trust Service Status Lists provide information on the compliance of a trust service, provided by a trust service provider, with a defined trust scheme, along with historic information. As such, TSLs provide the basis for Trusted Lists as foreseen in the European Regulation No 910/2014 on "electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC" [8], which is in the following referred to as eIDAS regulation. In there "Trusted Lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision" [8, p. Para. 46].

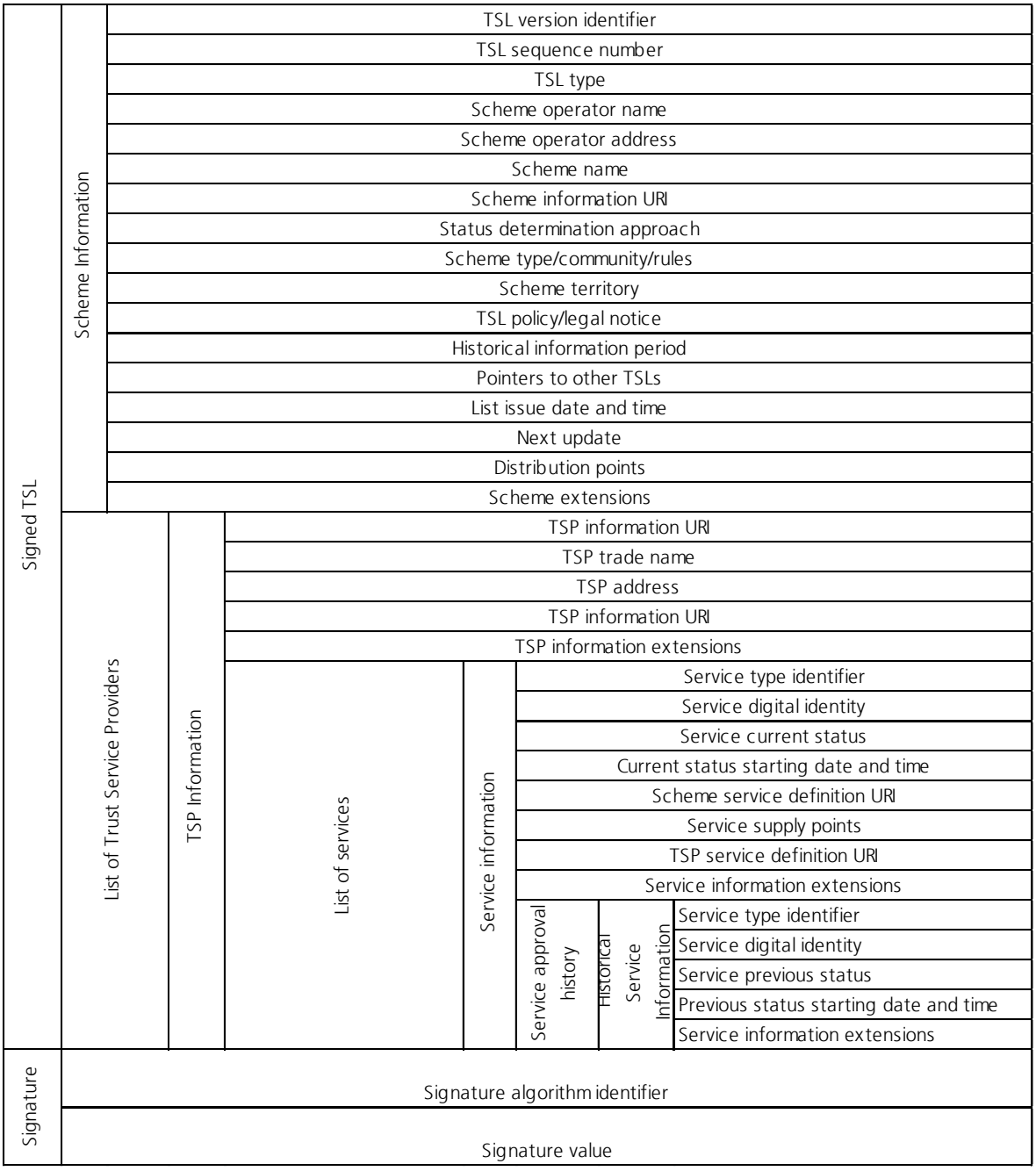

Figure 6 Overview on TSL contents as defined in ETSI TS 119 621. Adapted from [2]

While Trusted Lists and eIDAS are important concepts and regulations to consider in LIGHTest, they do not apply exclusively, as eIDAS only applies to "...trust services provided to the public [which have] effects on third parties..." [8, p. Para. 21]. Furthermore, the LIGHTest infrastructure has many applications outside the context of trust services as defined in eIDAS.

Yet, in order to provide support for eIDAS in LIGHTest, support of Trusted Lists or TSLs, as in ETSI TS 119 612 [1], which is a specification based on ETSI TS 102 231, is crucial, since it is

explicitly mentioned in the Commission Implementing Decision (EU) 2015/1505 [9]. Article 1 of this Implementing Decision requires Member States to "*establish, publish and maintain trusted lists including information on the qualified trust providers which they supervise, as well as information on the qualified trust services provided by them. Those lists shall comply with the technical specifications set out in Annex I.*" [9]. Annex I explicitly references TS 119 612.

A Trusted List as in ETSI TS 119 612 provides the association of an Issuer with a Trust Scheme, while enabling authenticity of the claim by enabling verification via the Trust Scheme Provider certificate. A Trusted List provides information on the trust scheme, along with approval and historical approval information of a trust service. Any information on the Trusted List is signed with the trust scheme operator, or in the sense of LIGHTest, the Trust Scheme Provider certificate. Figure 6 indicates the contents of a Trusted List as described in ETSI TS 119 612.

As ETSI TS 119 612 is a widely accepted and used standard for trust lists (e.g. for the eIDAS trusted list) it was decided to use this standard for the representation of the Trust List in LIGHTest at the Trust Scheme Provider. Since the mechanism used for Trust Scheme Publication in LIGHTest (i.e., HTTPS) allows both for requesting and providing different document types, this is only a choice for now and other formats can be used later on should they prove valuable.

6.3.3 Querying of Trust Scheme Association

Querying of the Trust Scheme Publication Authority can be divided into two subprocesses. Any query hereby first aims at discovering the trust scheme. As the ATV initially only knows the Issuer Name, but neither the Trust Scheme Name, nor the Trust Scheme Provider, discovery of the Trust Scheme Name (or Scheme Name) is provided by a claim of the Issuer, that it operates under the Trust Scheme. Of course, this claim must be validated against the actual association of the Issuer provided by the Trust Scheme Provider. Therefore, validation of this claim is achieved by discovery of the Trust Scheme Provider that is associated with a Scheme Name, and retrieval of a signed statement of association of an Issuer with the Trust Scheme operated by the Trust Scheme Provider.

In addition to the signed statement of association of an Issuer with a certain Trust Scheme, trust of the Trust Scheme Provider in the DNS Name Server needs to be verified as well. This is described in detail in the developed "Consolidated approach for publishing trust-related information in the DNS" in subsection "Authenticity of trust declarations" (e.g. section 5.4 in D3.3 [4] and D3.4 [5]). In summary, each DNS resource record set that is used in the querying process requires DNSSEC validation. For the communication with the Trust Scheme Provider, it must be ensured that the ATV communicates with the correct server. This can be achieved using the DANE (DNS-based Authentication of Named Entities) protocol, which allows to publish information about the certificates used in DNS. In case that the server is not operated under authority of the originator of the declaration (i.e. the signed trust list in the TSPA), the originator

can define conditions the certificate has to fulfill to be accepted via SMIMEA resource records and which then can be verified by the ATV.

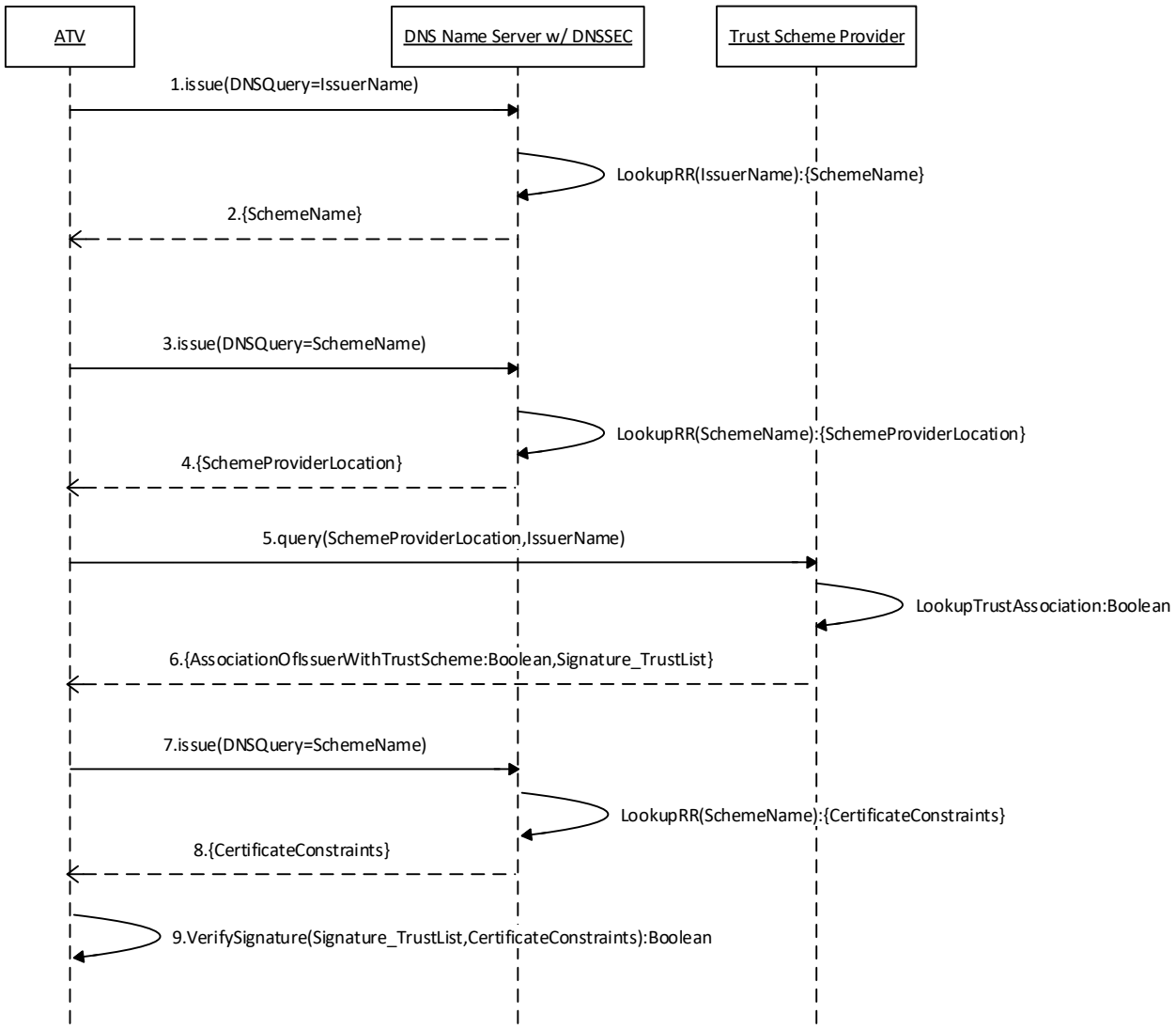

Figure 7 Querying of Trust Schemes in the TSPA

Using the claim by the Issuer for discovery of the associated trust scheme the process for querying and verifying Trust Schemes is shown in Figure 7. This process consists of the following steps:

1. The ATV issues a query to the DNS Name Server with the Issuer Name.
2. The DNS Name Server delivers the record for the Issuer Name that contains the name of the associated trust scheme. The name of the associated trust scheme indicates the Scheme Name (SchemeName), in the case of a Boolean Trust Scheme Publication, and the ordinal value of the Scheme Name (LevelName.SchemeName) in the case of an

Ordinal Trust Scheme Publication. This step has previously been described as the Issuers' claim of trust scheme association (see Section 6.2).

3. The ATV now queries the DNS Name Server for the associated trust scheme.
4. The DNS Name Server provides the record for the Trust Scheme Provider, which contains the Location of the Trust Scheme Provider (SchemeProviderLocation).
5. The ATV now queries the Trust Scheme Provider by using SchemeProviderLocation, and provides the Issuer Name to the Trust Scheme Provider.
6. The Trust Scheme Provider queries its Trust List and verifies whether the Issuer Certificate is listed indicating that the Issuer is operating under its Trust Scheme. The Trust Scheme Provider finally provides a signed statement of association of an Issuer Name with a Trust Scheme. The ATV can now verify that the statement of association of an Issuer with a Trust Scheme was made by the Trust Scheme Provider.
7. The ATV queries again the DNS Name Server for the associated trust scheme.
8. The DNS Name Server provides the SMIMEA record for the Scheme Name that contains constraints, which limit the accepted certificates for the signature of the trusted list (CertificateConstraints).
9. The ATV can now verify if the certificate used for signing the trusted list was valid.

There are different message formats which are exchanged between TSPA and ATV: First, DNS queries for PTR, URI, and SMIMEA resource record data for the discovery and verification process (see e.g. Section 7.1 in D3.3 [4]). In DNS, the proposed pair of prefixes for LIGHTest of the form *_aspect._application* is ***_scheme._trust*** for trust scheme publication (see e.g. D3.3 [4]). Second, the signed statement of association of an Issuer Name with a Trust Scheme is provided as a signed XML-file.

6.3.4 Querying of Tuple-Based Trust Schemes

Tuple-Based Trust Schemes provide further details on the trust scheme and enable the ATV to reason, not only based on the ATV users' trust in a trust scheme, but also on the ATV users' trust in properties of trust schemes. Retrieval of the Tuple-Based representation of a trust scheme (Tuple-Based Trust Scheme) can be done via the previously discovered Trust Scheme Provider. A Tuple-Based trust scheme at the Trust Scheme Provider can be provided in two possible ways: (1) the tuples are added to the trust list or (2) an extra document which lists the tuples and a pointer from the trust list to this document (see also Figure 4). In both cases, this requires an additional query of the Trust Scheme Provider. This is demonstrated in Figure 8: Steps 1 – 9 are the same as for querying Boolean or ordinal Trust Schemes. In addition, the ATV can now access the Tuple-Based Trust Scheme by:

10. Querying again the Trust Scheme Provider.
11. The Trust Scheme Provider now provides a list of tuples (attributes and values) to the ATV.

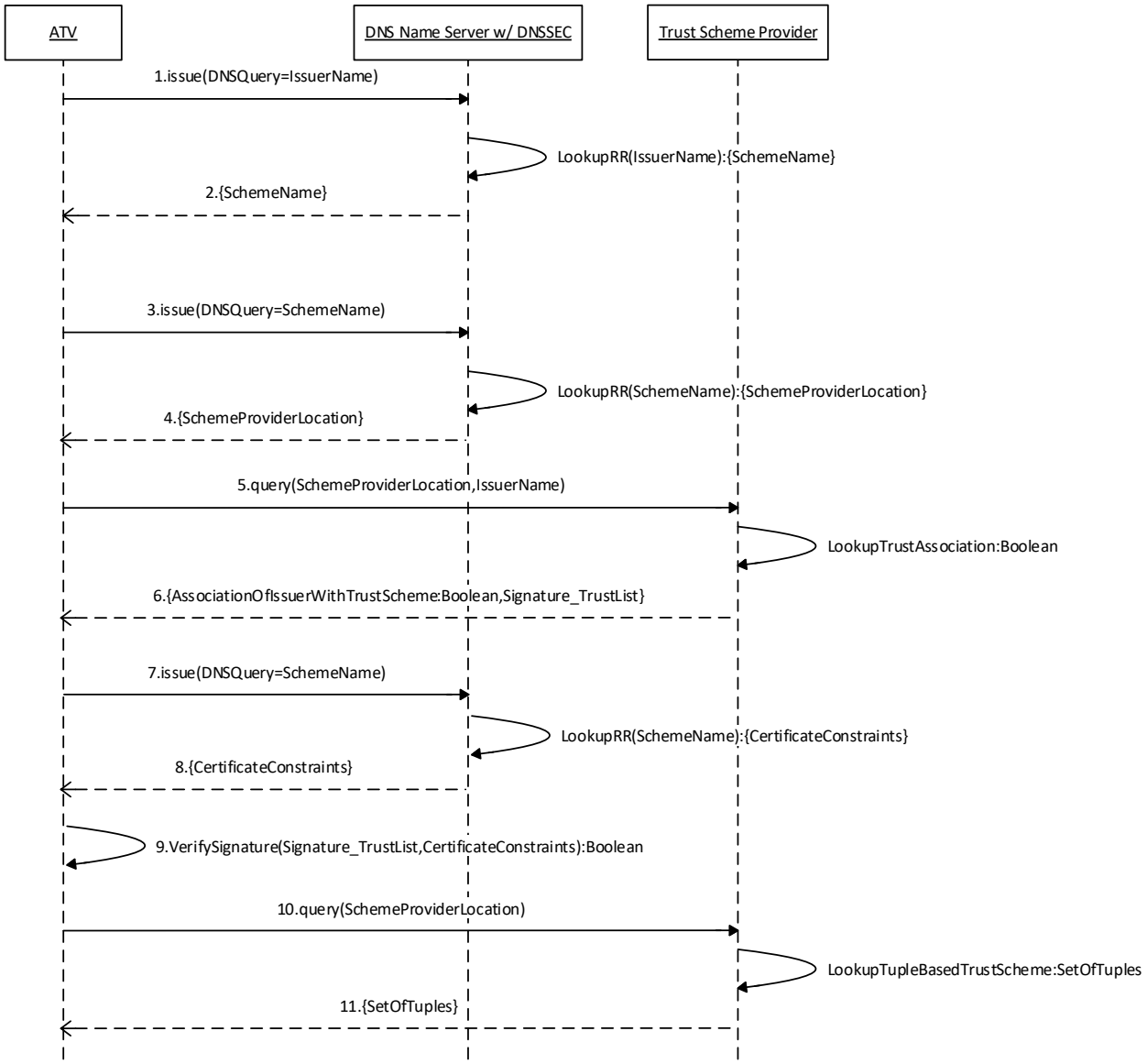

Figure 8 Querying of Tuple-Based Trust Schemes in the TSPA

As ETSI TS 119 612 is used for the representation of trust list in LIGHTest at the Trust Scheme Provider, the message format for the response in Step 11 is also XML. This allows to use XML namespaces to embed this information interoperably in the ETSI TS 119 612 trust list document.

7. Data Model of Tuple-Based Trust Scheme Publication Authorities

7.1 Modelling Approach and Methodology

In order to enable the representation of multiple trust schemes in the TSPA, a bottom-up modelling approach was followed. First, constructs were identified in the selected trust schemes, and were compiled to a vocabulary of the trust scheme along with a definition of each construct. These vocabularies were used to identify aggregations of the constructs within each scheme.

In the next step, each vocabulary was consolidated towards a unified data model of trust scheme publication authorities. The consolidation process is shown in Figure 9. Each scheme is represented by S_n where n represents an arbitrary number. Due to the left-sidedness of the consolidation approach, complexity of the consolidation remains feasible. Additionally, saturation of the consolidation can be observed. Saturation in this context can be defined by the number of new concepts that are included in the framework. If, for instance no new concepts are added by Scheme S_4 to the consolidated Scheme $S_{1,2,3,4}$, saturation of the included constructs can be assumed.

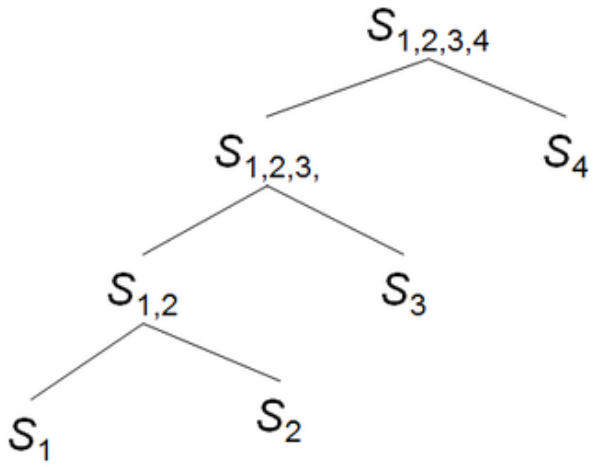

Figure 9 Consolidation approach of the data model having 4 trust schemes

Naturally, such a definition of saturation is always affected by the completeness of the observed trust schemes. Therefore, further validation of the universal trust framework, especially the data model of trust scheme publication authorities was conducted for D3.2, by representation of different cases of trust of additional trust schemes.

The conducted consolidation which led to the data model presented in this section was retrieved with the instance of the process described above, that is shown in Table 2. For retrieval of the Tuple-Based data model for trust schemes, the following trust schemes were considered in D3.1: The Pan Canadian Trust Framework (PCTF), STORK QAA/AQAA, eIDAS, FIDO, ISO/IEC 29115:2013 and the Chinese Electronic Signature Law. In D3.2, the following trust schemes

were considered to further validate the universal trust framework: The Turkey Electronic Signature Law, The Minors Trust Framework (MTF), The Trust Scheme of Azerbaijan, and the Embedded UICC Remote Provisioning Scheme (UICC).

These Trust Schemes are assumed to provide the most complete picture, as they include national trust schemes from nations both east- and westwards of Europe, along with European, and International Trust Schemes as well as Trust Schemes from industry consortiums.

Input Scheme 1	Input Scheme 2	Consolidation Result	Saturation ΔS (min ΔS)
ISO/IEC 29115	PCTF	Data Model v0.2	n.a.
Data Model v0.2	FIDO	Data Model v0.4	3
Data Model v0.4	QAA/AQAA, eIDAS	Data Model v0.6	9
Data Model v0.6	Chinese Electronic Signature Law	Data Model v 0.6 (Data model of D3.1)	0
Data Model v0.6	Turkey eSig Law	Data Model v0.8	1
Data Model v0.8	MTF	Data Model	1
Data Model	Trust Scheme of Azerbaijan	Data Model	0
Data Model	UICC	Data Model (see Sections 7.2.7 and 7.4)	0

Table 2 Overview on consolidation steps in D3.1 (above thick line) and D3.2 (below thick line)

An overview on the consolidation steps is presented in Table 2. Throughout consolidation, the saturation of the consolidation was observed. Saturation in the sense of the conducted consolidation is defined as the number of new concepts, that are introduced by consolidating the respective trust scheme. Therefore, the initial consolidation of ISO/IEC 29115 and PCTF is not associated with a saturation value. Consolidation of the first data model version with FIDO resulted in three additional concepts due to the relying party scoped credential of the FIDO scheme. Further consolidation of the STORK QAA/AQAA levels involved 9 concepts due to the introduction of the concept of attributes, which may be different from the attributes used for authentication. Finally, the consolidation of the Data Model with the Chinese Electronic Signature Law resulted in no new concepts being added to the data model.

The further validation of the universal data model for D3.2 with the additional trust schemes Turkey Electronic Signature Law, MTF, the Trust Scheme of Azerbaijan, and UICC resulted in only two additional concepts. The first new concept is Authority Chain for verification of Authoritative Party from the Turkey Electronic Signature Law. The second new concept is the Identity Provider from the Minors Trust Framework, which is comparable to the Credential Broker for credentials.

Overall, the conducted consolidation approach for the development of the unified data model shows, that saturation could be achieved. The number of new concepts in the second iteration decreased to two considering four further trust schemes with different backgrounds. The selection of in total nine different national and international, governmental and industrial trust schemes indicates, that the resulting data model is able to consider all existing trust schemes and also provides a good basis for future trust schemes.

7.2 Selected Trust Schemes

7.2.1 Pan Canadian Trust Framework

Introduction: The Pan-Canadian Trust Framework (PCTF) aims to enable the Canadian digital identity ecosystem by defining a set of business, technical, and legal rules for the processes such as identification, authentication, and authorization of accessing resources across organizations.

The PCTF was released by the Digital ID and Authentication Council of Canada (DIACC) in 2016, as the result of a collaborative work between DIACC and the Pan-Canadian Identity Management Sub-Committee (IMSC) of the Joint Councils of Canada, the Public Sector Chief Information Officer Council (PSCIOC) and the Public Sector Service Delivery Council (PSSDC) [10].

The purpose of this section is to describe the background, context, collaborative approach to develop a Pan-Canadian Trust Framework (PCTF) and the principles it relies on.

Background and Context: The historical background of PCTF is summarized in [11] as follows: The first steps toward the PCTF were taken in 2007, when the Pan-Canadian Strategy for Identity Management and Authentication was published by the Inter-Jurisdictional Identity Management and Authentication Task Force (IATF). Later on, in 2010, IMSC published the Pan-Canadian Assurance Model followed by Trusting Identities: Pan-Canadian Approach to Enabling better Services for Canadians in 2011. In 2014, the Federal-Provincial-Territorial (FPT) Deputy Ministers' Table on Service Delivery Collaboration approved the Pan-Canadian Identity Validation Standard. This standard regulates identity validation requests and responses between federal, provincial, territorial and municipal government organizations.

From the practical point of view, guidelines on Authentication and Identification were published by The Office of the Privacy Commissioner. Industry Canada has published Canada's Principles for Electronic Authentication [12] and later on the Treasury Board Secretariat published the Directive on Identity Management, the Standard on Identity and Credential Assurance, and related guidelines [13].

However, there was still a need to develop a model for a pan-Canadian digital identity ecosystem that will enable all players (public and private) to safely and securely use their digital identity online.

Canadian documents currently used to identify individuals are The Canadian e-passport and the Government of British Columbia's Services Card, the latter being a provincially issued smart services card. These documents represent physical credentials with electronic capabilities for individuals to digitally identify themselves, anonymously if they so choose, in alignment with Canadian regulations.

PCTF Purposes and Main Definitions: "The PCTF describes the roles, services, and requirements to be agreed on between participating service delivery and commercial industry sector organizations, to meet current and future Canadian innovation needs." [10].

The PCTF develops common terminology, concepts and technical specifications in order to enable digital identity ecosystem participants to securely interact with each other. The PCTF is designed to offer mechanisms for digital identification, electronic authentication, online credential, and authorization systems used to provide services to government entities, citizens, business partners, and customers [10]. The main functionalities are shown in Figure 10.

Figure 10 PCTF Functionalities — https://diacc.ca/pan-canadian-trust-framework/

The PCTF aims to fulfill the following purposes described in [8] for the Canadian Digital Ecosystem:

1. Access Federation
2. Digital Identity Federation
3. Technical interoperability
4. Policy interoperability
5. Legal administration

Principles: The PCTF leverages the concepts identified in the Principles for Electronic Authentication developed by Industry Canada [12] and extends those to 10 requirements for the Canadian digital ecosystem in [10]. These purposes are listed below:

1. Robust, secure, scalable;
2. Implement, protect, and enhance Privacy by Design;
3. Transparent in governance and operation;
4. Inclusive, open, and meets broad stakeholder needs;
5. Provides Canadians choice, control, and convenience;
6. Built on open standards-based protocol;
7. Interoperable with international standards;
8. Cost effective and open to competitive market forces;
9. Able to be independently assessed, audited, and subject to enforcement;
10. Minimizes data transfer between authoritative sources and will not create new identity databases

The Federated Authentication and Brokered Authorization Model: DIACC has developed a simple model for the Canadian Digital Identity Ecosystem called the Federated Authentication and Brokered Authorization Model. This model mainly consists of the following components described in [11]:

> *The individual*—The person seeking to provide proof of their identification to conduct a digital transaction or interaction
>
> *The relying party*—An organization, individual or system that needs to access an authoritative party as authorized by the user (individual)
>
> *The authoritative pa*rty—An approved, recognized or trusted body that provides assurances (of credential or identity) to relying parties
>
> *The core digital identification and authentication platform service*—A digital identity infrastructure service consisting of separate, bounded, discrete components for:
>
> • Personal agents (whether mobile device based or Web-based)
>
> • Authentication services
>
> • Core registrar/identifier exchanger service

This model has three major service components: *credential services*, *permission services* and *identity services*.

In this proposal, DIACC defines the digital method used to ascertain identity provided that the electronic method is sufficient in strength to meet key identification requirements as the Electronic Confirmation of Identity process. This method consists of two parts:

• Electronically confirming the accuracy of a person's identity information using an accredited, authoritative source, referred to as *identity validation*

• Ensuring that the identity information being confirmed relates to the person making the claim, referred to as *identity verification*

Together, when these objectives are met, they can provide a level of assurance that an individual is actually who they say they are and be relied on as a digital alternative to an in-person and/or document-based identity-proofing process. The Credential and Identity Levels of Assurance taken as reference for determining these LoAs are the ones described in the Standard on Identity and Credential Assurance of the Government of Canada. Appendix B summarizes the Standardized Assurance Level Framework, while the controls that should be taken in order to mitigate Identity and Credential Risks and the resulting Levels of Assurances are described in the Appendix C of this Standard.

Figure 11 provides an overview of the PCTF identity credential levels of assurance, and Figure 12 on the PCTF in general. Both are represented as UML diagrams.

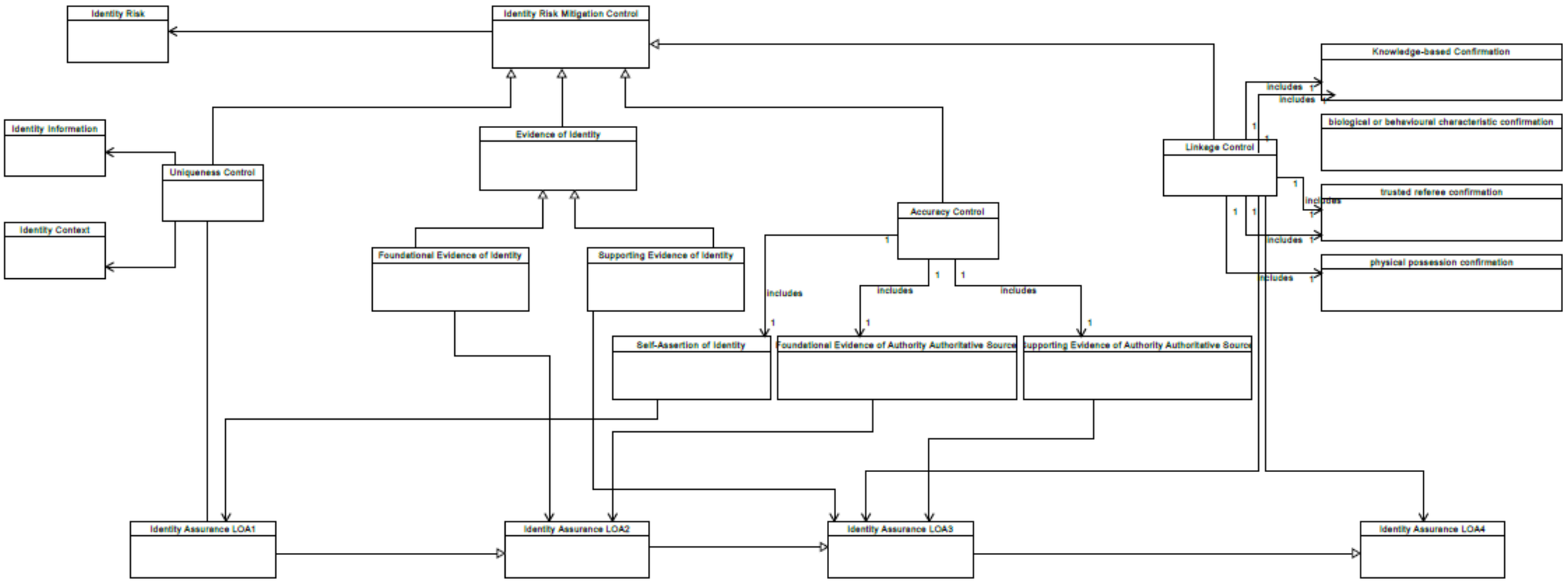

Figure 11 UML Diagram of the PCTF identity credential levels of assurance

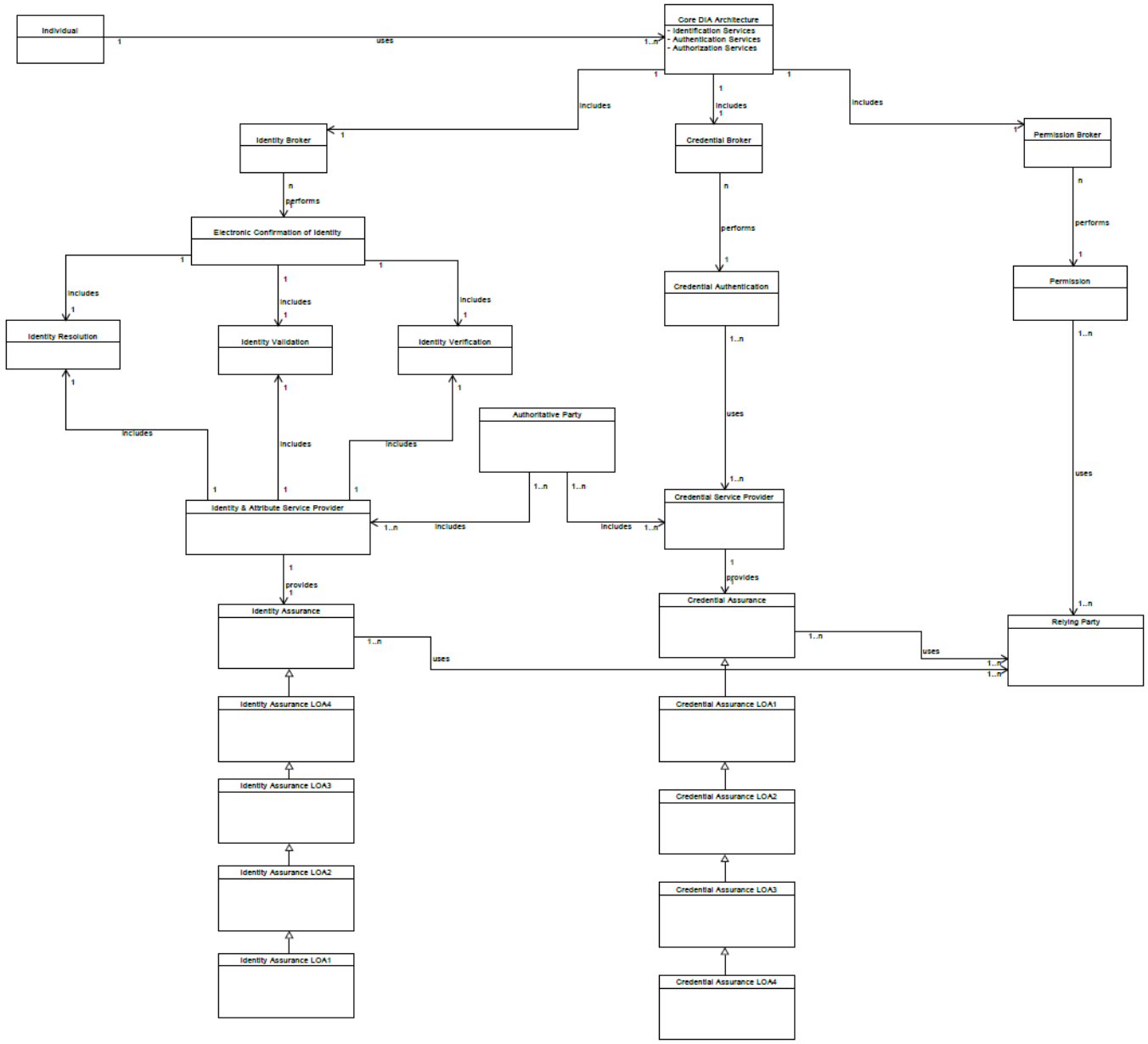

Figure 12 UML diagram of the PCTF

7.2.2 ISO/IEC 29115

The purpose of the international standard ISO/IEC 29115 is to provide a framework for managing entity authentication assurance. Here, assurance refers to the confidence in authentication transactions and all therein-required processes and activities.

An overview of the framework is depicted in Figure 13. The actors and components of the Entity Authentication Assurance Framework (EAAF) are introduced in the following. For a detailed description, we refer to the original document of the international standard ISO/IEC 29115:2013 [14].

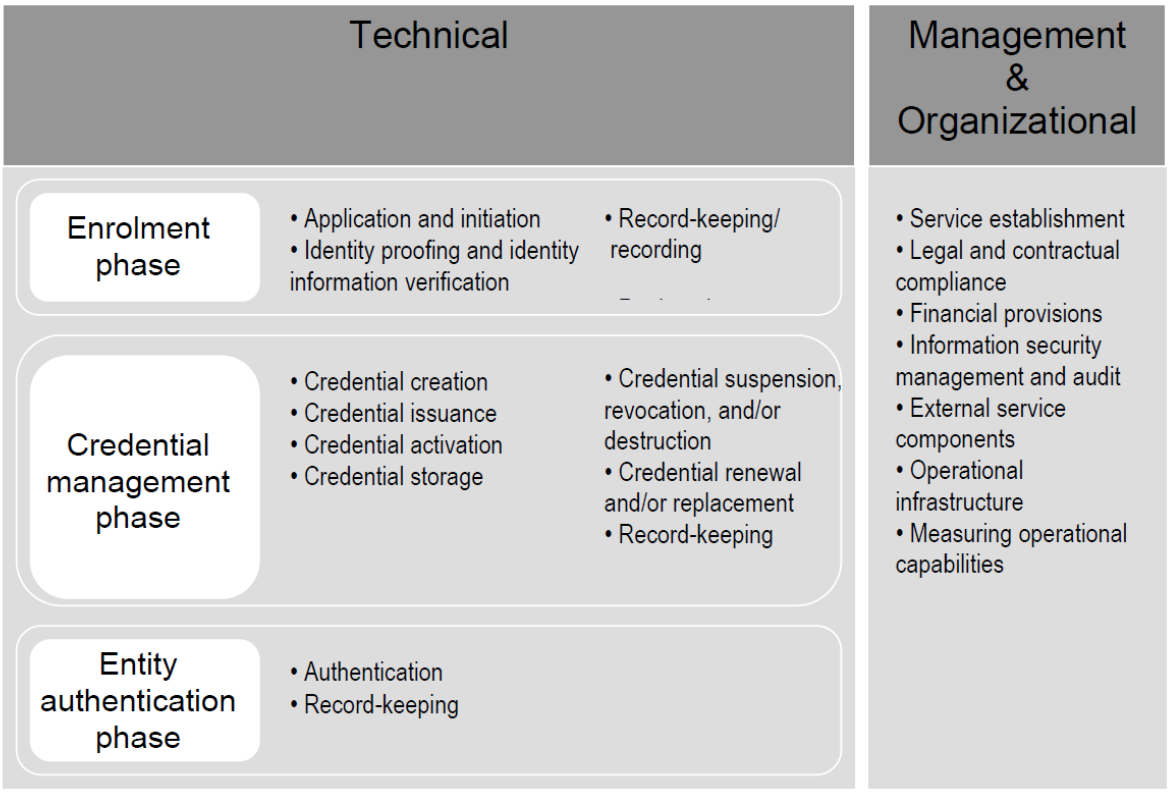

Figure 13: Overview of the Entity Authentication Assurance Framework [14]

In the EAAF the following **actors** are involved: entities, credential service providers, registration authorities, relying parties, verifiers, and trusted third parties. The actors may all come from the same or from different organizations. Relationships between organizations may exist, e.g. shared or interacting components, systems, and services.

In the EAAF four **levels of assurance (LoAs)** for entity authentication are defined which determines the degree of confidence in the processes. The degree of assurance that the entity uses the specific identity which was assigned to it, increases from LoA1 (lowest level of assurance) to LoA4 (highest level of assurance). This is depicted in Figure 14.

Level	Description
1 – Low	Little or no confidence in the claimed or asserted identity
2 – Medium	Some confidence in the claimed or asserted identity
3 – High	High confidence in the claimed or asserted identity
4 – Very high	Very high confidence in the claimed or asserted identity

Figure 14 Levels of Assurance [14]

The selection of an appropriate LoA depends on the given situation in the decision process. It is essentially a question of risk. This means that the likelihood of occurrence and possible harm of an authentication error determines the LoA. In general, for higher risks higher LoA are recommended.

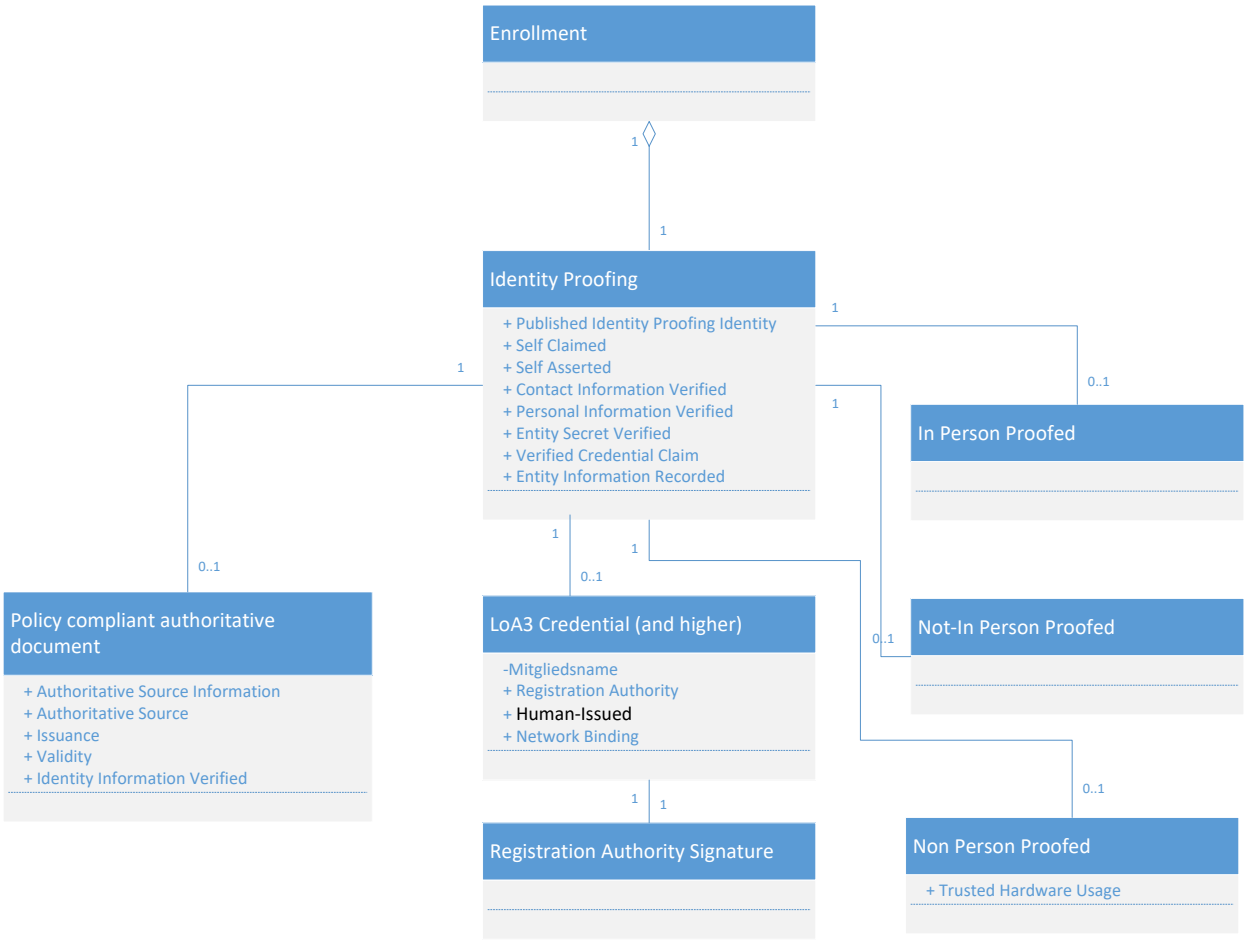

Figure 15 UML Diagram of the Enrolment Phase

Therefore, for each of the four LoAs and for all three phases of the framework, the requirements and implementation guidance are provided in the EAAF. In order to achieve interoperability between different LoA models, it also provides guidance for mapping other authentication

assurance schemes to the four given LoAs of the EAAF. Furthermore, the EAAF provides guidance for exchanging the results of authentication that are based on the four LoAs to complete the transaction or activity.

The **EAAF** (see Figure 13) consists of three phases: enrolment, credential management, and entity authentication. The **enrolment phase** (see Figure 15) involves the processes application and initiation, identity proofing, identity information verification, and record-keeping/recording. These processes of the enrolment phase may be either conducted entirely by a single or by a number of organizations with defined relationships and shared or interacting components, systems, and services. For the four LoAs the required processes differ with in general increasing complexity for higher LoAs. For example for entity enrolling the processes for LoA1 are minimal (e.g., create an new user with password), whereas for LoA4 an In-person meeting of the entity and the registration authority and extensive identity proofing is required. All processes which are required for the lifecycle management of a credential are included in the **credential management phase** (see Figure 16). It may involve some or all of the processes listed in Figure 13.

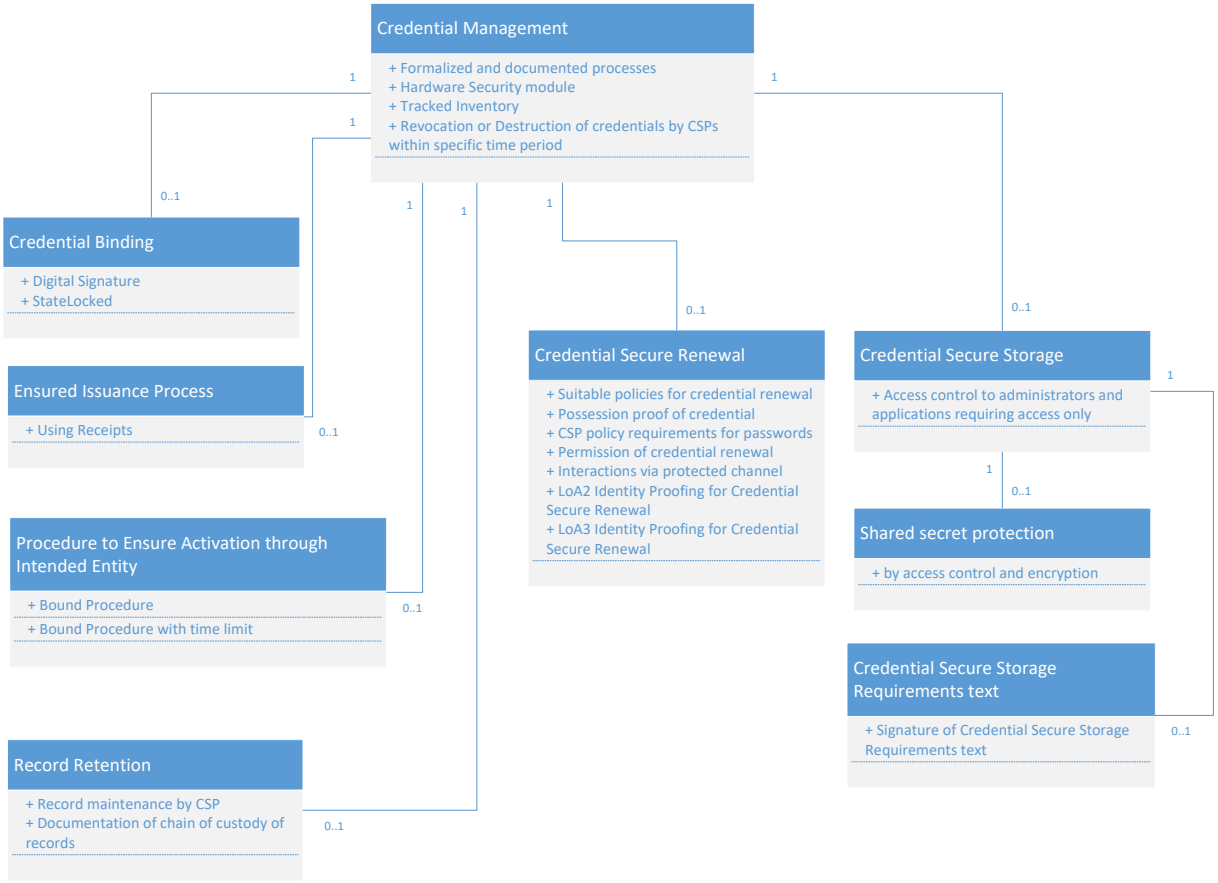

Figure 16 UML Diagram of the Credential Management Phase

In the **entity authentication phase**, the entity attests its identity to a relying party using its credential from the enrolment phase. In addition, purposes like service provision, compliance, accountability, and/or legal requirements claim to monitor and record-keep events in the authentication phase. Besides the technical aspects (enrolment, credential management, and entity authentication) also regulations and contractual agreements on the management and organization of the required service provision belong to the entity authentication assurance. This means that the security in providing entity authentication assurance using a technically in-depth set-up may lag behind because of insufficient management. Therefore, the EAAF also includes **management and organizational** aspects**.** The corresponding processes are listed in Figure 13. Note, that for the management and organizational aspects no specific criteria for each LoA are provided. These criteria and conformance assessment for management and organizational considerations are outside of the scope of this EAAF. However, they should be provided within a trust framework. In general the EAAF is technology neutral.

This international standard provides in addition guidance concerning **controls** that should be used to **mitigate authentication threats**. For this purpose, possible threats to each phase (enrolment, credential management, authentication) and for each LoA of the EAAF are identified, and required controls against these threats are provided. For example, impersonation is a threat to the enrolment phase. Required controls to protect against impersonation can be identity proofing using policy adherence, In-Person proofing, or authoritative information.

7.2.3 eIDAS

The eIDAS Regulation (Regulation (EU) N°910/2014 [8]) on electronic identification and trust services for electronic transactions in the internal market provides a regulatory environment for **electronic identification and trust services**, including electronic signatures, seals, timestamps, registered delivery and website authentication.

Since July 2016, the provisions applicable to trust services apply directly in the 28 Member States. *This means that trust services under eIDAS are no longer regulated by national laws. As a result, the qualified trust services are recognized independently of the Member State where the **Qualified Trust Service Provider** is established or where the specific qualified trust service is offered* (according to [15]).

The qualified status is granted in this way, as summarized in [15]:

1. The trust service provider and the qualified trust service(s) it intends to provide are assessed by an “eIDAS” accredited **conformity assessment body** for compliance with the Regulation.
2. The trust service provider sends the conformity assessment report (which must prove they comply with the Regulation requirements) to their national **supervisory body** as part of a notification that they intend to become qualified.
3. The supervisory body verifies that the trust service provider and the trust services proposed for qualifications actually meet the requirements set out by the Regulation, and

if so, grants the qualified status and adds to the national **Trusted List** the information on the qualified trust service provider and on the qualified trust services that they provide.

As is said in eIDAS regulation [8], from a legal point of view, both qualified and non-qualified trust services benefit from a non-discrimination clause as evidence in Courts. In other words, trust services cannot be discarded by the judge only on the ground that they are electronic. However, because of the more stringent requirements applicable to qualified trust service providers, qualified trust services generally provide a stronger specific legal effect than non-qualified ones as well as a higher technical security. *Qualified trust services therefore provide higher legal certainty and higher security of electronic transactions.*

The following electronic services fall under the eIDAS regulation and its related Secondary Legislation on electronic identification [16] and the electronic trust services [9]. According to such legislation, several levels of trust are identified:

- Electronic identity: means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.
  According to Article 8 of [8], the assurance levels low, substantial and high shall meet respectively the following criteria:
  a) **assurance level low** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;
  b) **assurance level substantial** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;
  c) **assurance level high** shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.
- Electronic signature: data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
  eIDAS distinguishes among **non-qualified**, **advanced (**non-qualified also**), and qualified electronic signature**.

- Electronic seal: data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.
  eIDAS distinguishes among **non-qualified**, **advanced (**non-qualified also**) and qualified electronic seal**.
- Electronic timestamps: issued to ensure the correctness of the time linked to data / documents.
  eIDAS differentiates between **non-qualified and qualified electronic timestamps**.
- Electronic registered delivery services: This is a secure channel for the transmission of documents bringing evidence of (the time of) sending and receiving the message. As said in [15], *the Regulation does not make the equivalence between (qualified) electronic registered delivery services and registered postal mail (registered items) defined under the Postal Directive*. Member States remain *free* to establish such equivalence at national level. *In other words, when the law requires fulfilling a specific procedure by sending a registered postal mail, using (qualified) electronic registered delivery services would meet this requirement only if the national law has established the equivalence*.
  eIDAS discriminates between **non-qualified and qualified electronic registered delivery services**.
- Electronic website authentication: Certificates for website authentication are issued to ensure the users (in particular citizens and SMEs) that behind the website there is a legal person identifiable by trustworthy information. It is important to notice that that qualified certificates for website authentication may be issued to natural persons while existing certificates like the Extended Validation (EV) ones, can only be issued to legal ones [17].
  Non-qualified and qualified electronic certificates for website authentication can be distinguished in the eIDAS regulation.

In the following UML diagram (Figure 17), the eIDAS trust scheme is summarised:

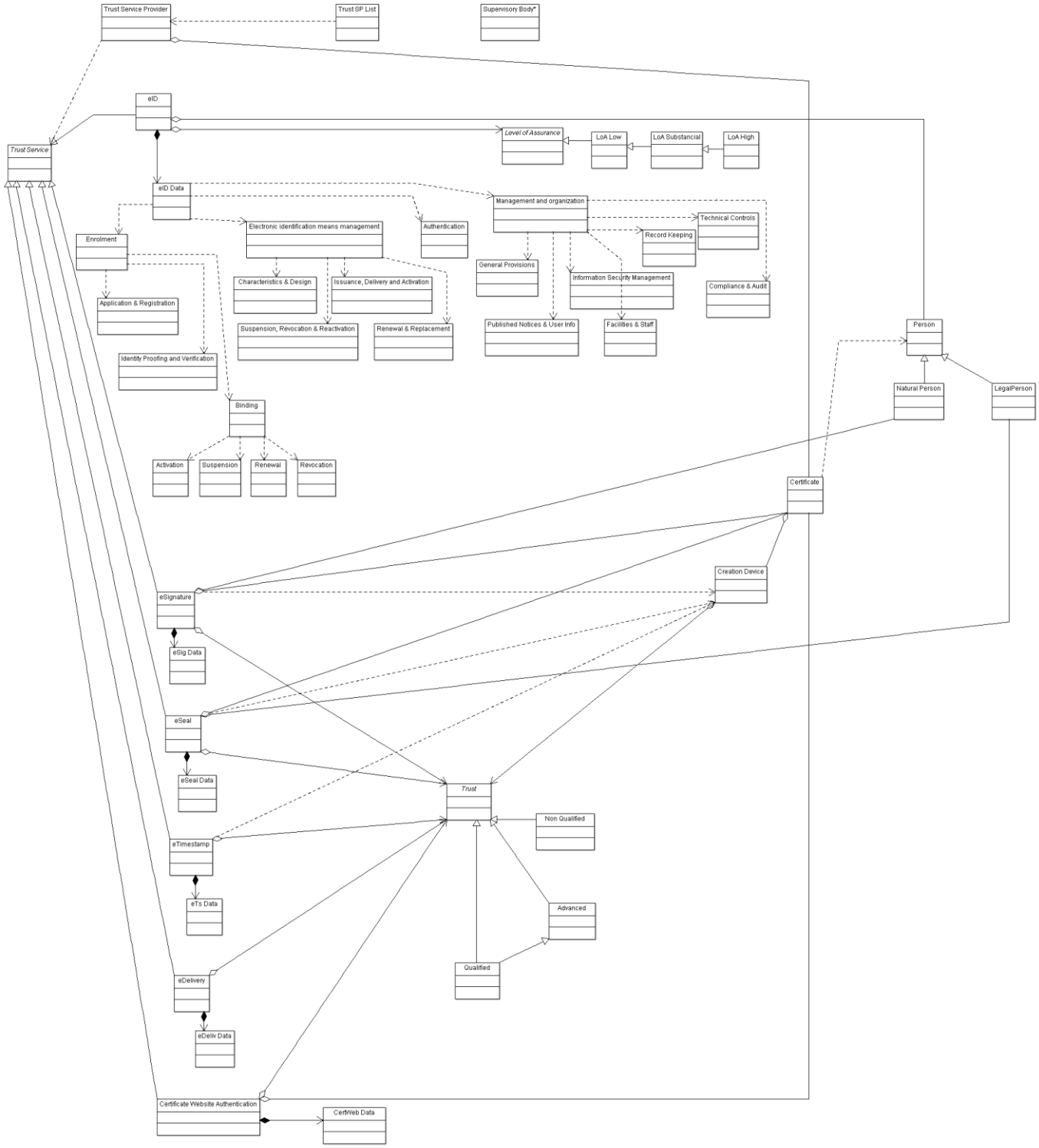

Figure 17: eIDAS trust scheme

7.2.4 STORK QAA/AQAA

The AQAA was created as an expansion to one of the primary outputs of STORK, namely the QAA (Quality Authentication Assurance) model, which permits quality levels to be assigned to various eID solutions, based on some of their main characteristics. The original STORK QAA framework included four levels of authentication assurance, as is said in [18].

Within STORK 2.0, the QAA model was reviewed, resulting in an attribute QAA (AQAA). The AQAA allows **quality levels** to be assigned **to attribute assertions**, comparable in intent and set-up to the original QAA.

Thus, two types of quality statements can be made on the basis of STORK and STORK 2.0 outputs:

- An **assertion of quality of the eID** under the QAA, ranging from level 1 to 4;
- An **assertion of quality of specific attributes or attribute sets** under the AQAA, ranging from level 1 to 4.

This also implies that certain choices must be made when identity information combines eID information and attribute information, as explained in [19]:

a. When eID statements are combined with an attribute statement, it is possible to make a separate statement of quality for both sets (e.g. name and address are QAA level 4, and academic qualification is AQAA level 3);
b. Similarly, when eID statements are combined with an attribute statement that consists of multiple attributes, it is possible to make a separate statement of quality for all sets of information (e.g. name and address are QAA level 4, academic qualification is AQAA level 3, and university where a diploma is issued is AQAA level 4);
c. Or alternatively, all information is combined into a single statement, in which case the lowest rating should be selected (e.g. name, address, academic qualification and university are all level 3, since this is the lowest rating of the set).

The AQAA is agnostic on which approach is chosen; this is a design choice. However, the principle above must always be respected: ***whenever quality rated identity information is provided and combined into a single assertion with a single quality statement, the lowest quality level should be assigned to this assertion*** [19].

Furthermore, it is strongly advisable to at least keep eID quality statements and attribute quality statements distinct (options *a* and *b* above, but not option *c*), since *the QAA and AQAA criteria are not directly comparable*, and the AQAA is still largely untested in practice. Mixing the criteria into a single quality rating therefore not only removes potentially important information from the service provider (who may have different quality requirements for each attribute), but also risks sending a misleading message with respect to the data quality.

The AQAA is based on a few principles, which are summarised in [19] and extracted here:

- *When an attribute assertion is carried out based on identification by a STORK eID at the attribute provider's, its quality is the minimum between **the eID quality** (given under the STORK QAA levels) **and the attribute quality** (given under the AQAA criteria presented below):*

Attribute assertion quality		eID quality under old QAA policy			
		Level 1	**Level 2**	**Level 3**	**Level 4**
Attribute quality under new criteria	**Level 1**	Level 1	Level 1	Level 1	Level 1
	Level 2	Level 1	Level 2	Level 2	Level 2
	Level 3	Level 1	Level 2	Level 3	Level 3
	Level 4	Level 1	Level 2	Level 3	Level 4

Figure 18 AQAA criteria (source [19])

- *The attribute assertion quality is defined only upon authentication with a STORK eID: in case a non-STORK eID is used, no AQAA rating can be provided for the attribute assertion, as STORK can evaluate the strength of the attribute request authentication and of the related policies only if a STORK eID is used. Lacking this, only an unrated attribute assertion can be performed.*

- *Moreover, it follows that only if a STORK eID is used first for authentication, can an AQAA rating be provided, since the principle of STORK is that the end user has to personally request the transfer of specific attributes to the service provider, and thus AQAA is not to be applied if the end user is not directly involved in provisioning the attributes. While it would be feasible from the technical point of view, and likely very useful, to locally store specific attribute requests, and to have a C-PEPS provision them directly to the service provider, this would give the service provider an effective mandate enabling them to validate attributes without the end user involvement, and this would pose significant privacy and policy issues.*

As a special case, it is possible to apply AQAA in the situation where attribute assertions are retrieved through chaining, that is where a STORK eID is not applied directly, but rather through intermediation of other attribute providers (i.e. where the attribute assertion is retrieved on the basis on another attribute assertion, provided by an attribute provider to which the user has authenticated using a STORK eID). In this case, the criteria are applied in the sense that the eID quality of the final attribute assertion is determined as the joint quality of the original eID and of the intermediate attribute assertion.

Note: when STORK eID is referenced above, eIDAS electronic identification could be written for the same effects. See section 7.2.3 eIDAS.

The following UML diagram (Figure 19) shows STORK QAA/AQAA trust scheme:

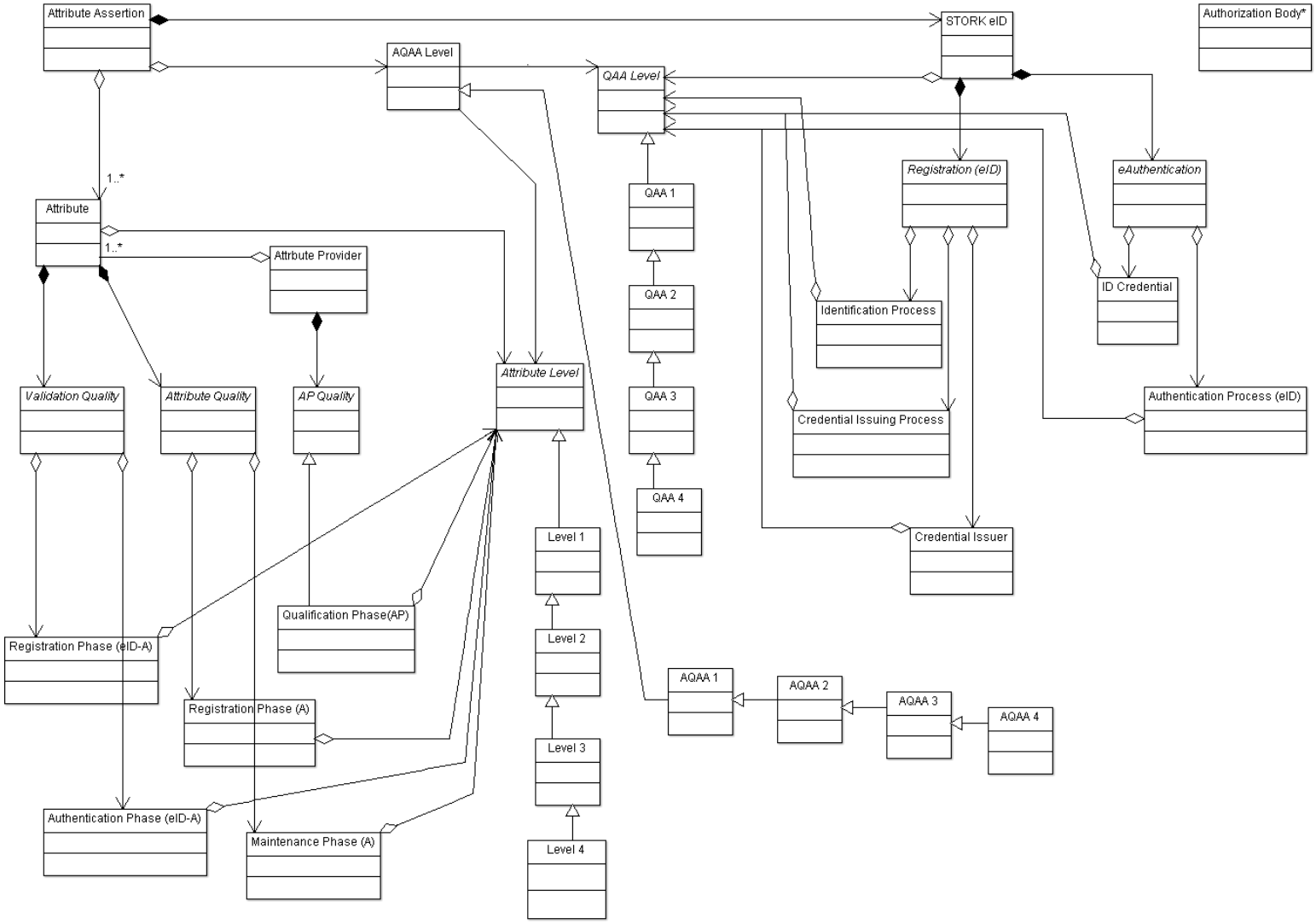

Figure 19: STORK QAA/AQAA trust scheme

7.2.5 Electronic Signature Law of the People's Republic of China

Introduction: Electronic signature has been recognised in China since 2004 with the People's Republic of China Electronic Signature Law coming into force on 1st April 2005.

The debate on regulating electronic commerce in China has been both lengthy and intense with the first regulation in China on electronic commerce being traced back to March 1999 where it is mentioned in the Contract Law. These first mentions only go as far as recognising a 'data message' as a form of writing, but did not address legal requirements such proving originality or how it might be admissible as evidence. There was a slow progression over the following years to 2004 with regulations such as the Internet Information Service Administration Measure 2000 and scattered local and departmental government regulations that covered areas such as information security and intellectual property. Although this law was the first national e-commerce legislation in China, in some cities certification authorities (CAs) were set up — in places such as Shenzhen, Shanghai and Beijing and then in the year 2000 the China Financial Certification Authority was set up by twelve banks. At that time there is evidence of some local governments releasing rules on digital signatures, as the need to regulate and administer the certification services came apparent. As the importance of electronic commerce in China's economic development was recognised the State Councils Informationalisations office enacted the 'Electronic Signatures Ordinance of People's Republic of China in 2002. This was an attempt to standardise CAs and clarify legal validity of e-records or e-documents but as a regulation was more administrative. The response to this action was that it was a decided a law was needed rather than an ordinance.

China's law is modelled on a combination of the EU Directive on Electronic Signatures, UNCRITRAL Model Laws and United Nations Conventions on Electronic Communications International Contracts. It is considered a two-tier jurisdiction as it gives digital signatures the same status as those written by hand. Companies can choose to select different forms of signatures and customise their business processes based on the form that is more appropriate for each use case.

For a valid contract under Chinese Law, a written signature is not required. Contracts can be considered valid if agreed verbally, electronically or in a physical paper document. For this to be valid, sufficient evidence needs to be provided that the contract was created electronically. For the contract to be admissible and authentic, digital transaction management solutions are often used.

The law was created to regulate electronic signatures and in effect provides all the framework necessary to ensure that e-signatures remain legally binding in China. This is slightly different to other schemes as rather than being a specific trust scheme, this is a functioning law.

The difference between digital and electronic signatures: Before we consider the law itself, it is worth looking into more detail about the difference between digital and electronic signatures as they have an impact on both the law mentioned below and also the level of trust required for

each. CoSign [20] have put together a guide to digital signatures which lays out the differences in detail.

Digital signatures are a sub-group of electronic signatures providing the highest level of security and universal acceptance so they cannot be copied or tampered with. Digital signatures are based on Public Key Infrastructure technology and the only signature standard which is accepted by governments around the world. The use of cryptographic operations mean that a digital signature creates a 'fingerprint' unique to both the signer and the content.

Electronic signatures are based on proprietary formats that may use a digitized image of a handwritten signature, symbol or voiceprint to identify the author of an electronic document. They are legally enforceable but they are vulnerable to copying and tampering and require proprietary software for validation. Hence the law below requiring electronic validation services.

Contents of the law: The electronic signatures law consists of five chapters, general articles, **data message**, electronic signatures and recognition, legal liability and supplementary articles. The law does not just deal with electronic signatures but also data messages.

What is included in the provisions: The data included will be that which is included or attached in **electronic data** for identification of the signer and the electronic proof that the signer agrees with the contents.

There are some cases which are exempt from the law:

- Documents concerning personal relationships e.g. adoption
- Documents concerning trade of immovable estates such as land
- Documents concerning termination of public services such as water or electricity
- Documents concerning other inapplicable situations regulated by law or administrative regulations

Data Requirements: It is vital that all the data must be accessible at any time. Data must also be in the same format when it was first **created**, sent or received even if it has been changed to different formats. The data must also include a **time** stamp and the **place of business** for the originator is considered as where the data message was despatched and similarly for where the data message is received.

The electronic data must be **reliable** in the following ways:

- How it was created, preserved or circulated
- Completeness of the electronic data must be maintained
- The way the **senders** are identified

The time stamp which is automatically generated when the data message enters a certain information system may be of interest to LIGHTest, if the information system is beyond control of the addresser or the system for the receipt of the data message. As is the principal place of business if there is an address of either the addresser or the receiver.

Transformation of data: Electronic data can only be considered transmitted when one of the following occurs:

- Electronic data transfer has been authorised by the sender
- Electronic data is automatically transferred by the sender's information system
- The receiver of the electronic data verifies **receipt**

When the sender acquires the receiver's confirmation, the electronic data is considered received and this is the confirmation that a data message has been transmitted. This may be of interest to LIGHTest if required by laws and administrative regulations or by agreement between the parties concerned.

Electronic Verification Services: If an electronic signature needs to be verified by a third party, the service needs to meet the following criteria:

- Suitable **staff** are available for the provision of electronic verification services
- **Funds and business places** are suited for the provision of the electronic verification services
- **Technology and equipment** must comply with the safety standards of the State
- Certificates for the use of the codes approved by the code control institution of the State

All electronic verification services must **apply** to the department in charge of the information industry and be granted **approval**. All rules for electronic verification should be in conformity with the **regulations** of the State and be published. These rules will include scope of liability, norms for operation and the protective measures for information safety.

Once an electronic signatory applies for an electronic verification, the electronic verification service will check the identity of the applicant and examine the relevant **materials** before creating a certificate.

The Certificate of the Electronic Signature: This will be issued by the electronic verification service and include:

- Name of electronic verification service
- Name of certificate holder
- Serial number of the certificate
- Term of validity for the certificate
- Validation data of the electronic signature of the certificate holder
- Electronic signature of the electronic verification service

The electronic verification service will guarantee that the items listed above in the certificate are **complete and accurate**.

Certificates will be preserved for at least **five years** after the certificate is no longer valid. Electronic signatures issuers for electronic verification services based overseas are on an equal legal standing to the ones issues by electronic verification services established in accordance with this law.

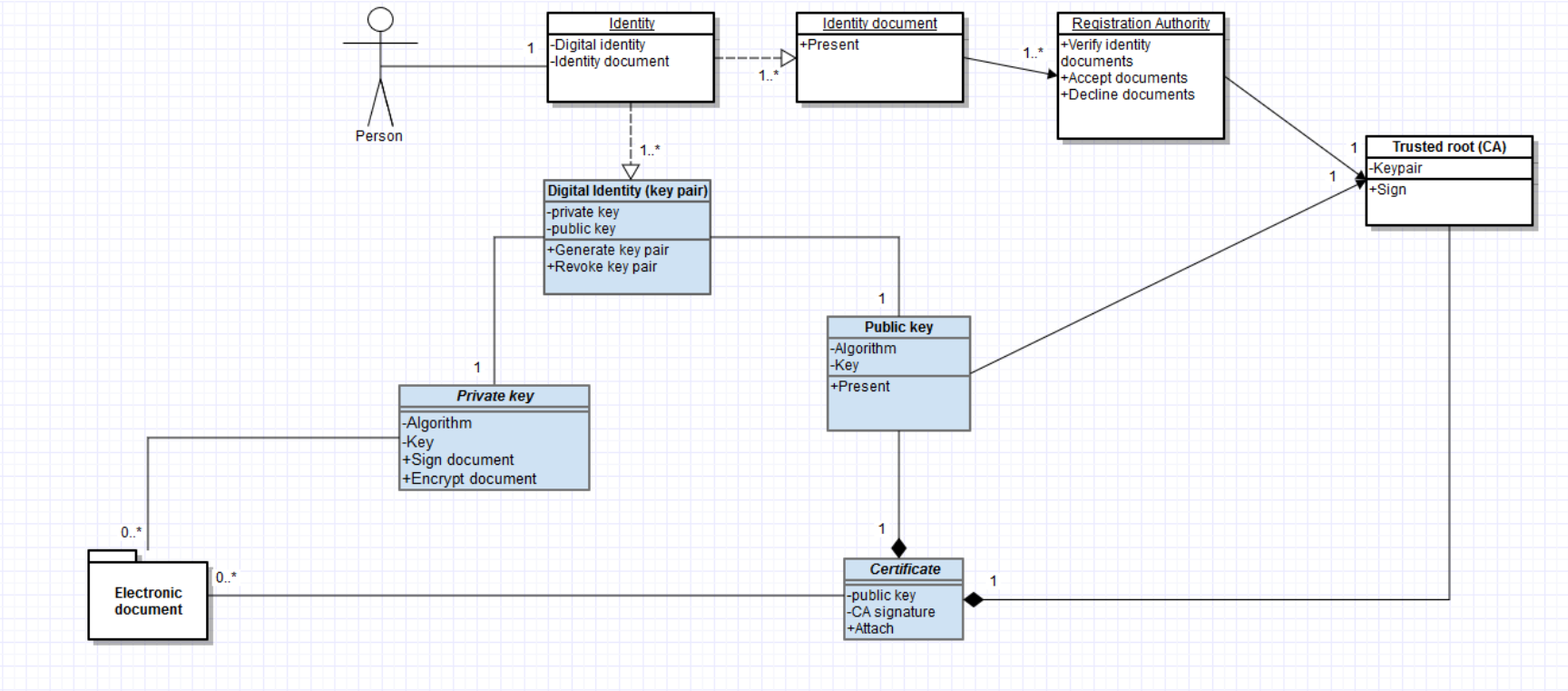

Figure 20 UML Diagram of the Electronic Signature Law of the People's Republic of China

7.2.6 FIDO

The Fast Identity Online (FIDO) alliance is an industry specification group with now more than 250 members that aims to define an interoperable specification for mobile authentication to overcome existing fragmentation and silos. Technically, FIDO concentrates on authentication only and explicitly excludes identity and ID federation. It can however be embedded into identity schemes and combined with ID federation, although not directly supported by the FIDO protocol. The core functionality of the FIDO framework is a secure end-to-end protocol for strong authentication that allows a relying party to recognise a returning and previously registered user in a reliable and secure way. The main goal of the protocol is to provide a stronger authentication than the typical username/password authentication (one-factor authentication) and preferably a password-less user experience.

FIDO has originally two flavours of the protocol, the U2F-protocol for two-factor authentication and the UAF-protocol for password-less authentication (e.g. using biometrics) and transaction signing. Both protocol versions exist under the FIDO 1.x specifications [21] and are currently unified in the upcoming FIDO 2.0 (formerly UFS-protocol) specification.

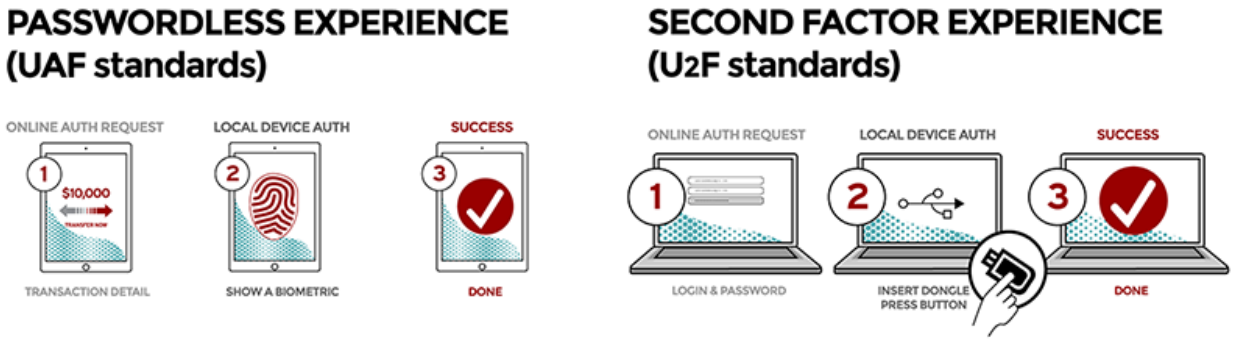

Figure 21 User experience of the two FIDO protocol versions UAF (left) for password-less authentication and transaction signing and U2F (right) for two-factor authentication [21].

One of the main challenges for strong authentication is to establish trust into the authenticity of the user credentials with respect to the registered credentials and also into the authenticity of the authenticator used. The latter is of special importance in an open ecosystem like FIDO where the user can bring his own authenticator to register and authenticate towards a relying party. FIDO is addressing this challenge by providing an integrated attestation scheme for the authenticator that is based on a lightweight PKI.

The principle of FIDO is based on simple challenge-response protocols using asymmetric keys. In contrast to previous PKI-based systems FIDO wants to explicitly reduce complexity by restricting PKI to the absolute minimum. As a consequence, the user-centric registration triggers the generation of the FIDO key pair and exports the public key to the service provider while the private key is kept on the user side. No further PKI is used in the registration and authentication step.

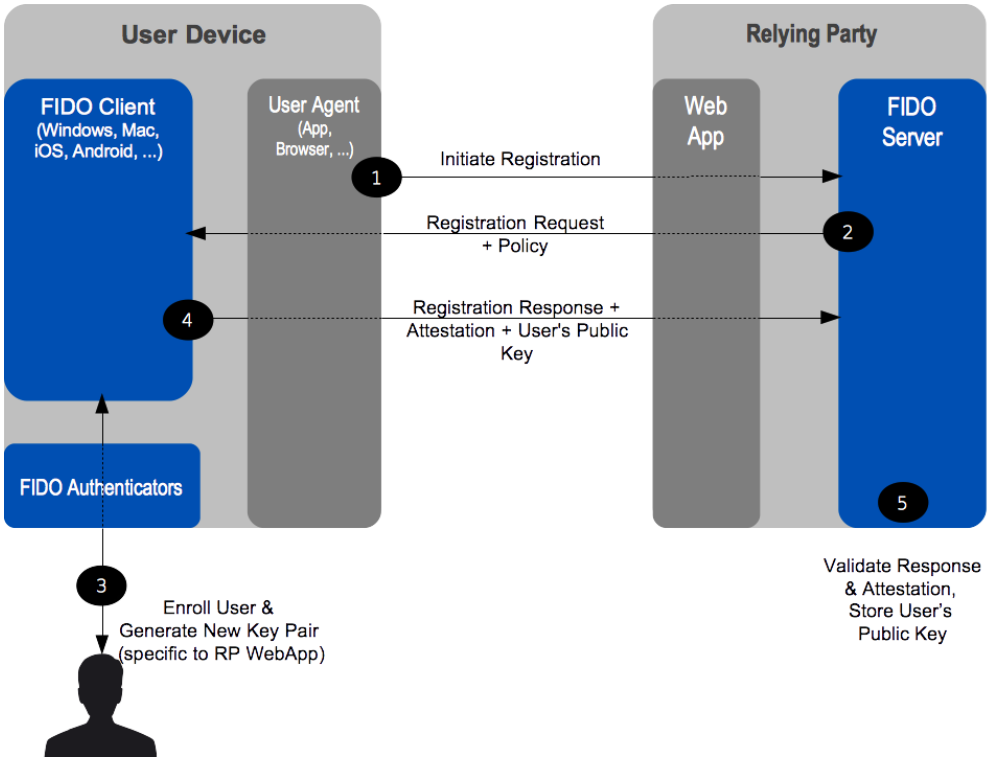

Figure 22 Principle of user registration in the FIDO UAF protocol [21]

When the user triggers a registration event the FIDO server answers with a registration request and a policy that allows the relying party to request a certain type of authenticators (see Figure 22). The client will only register those authenticators that comply with the policy. After generating a new key pair — potentially accompanied by a biometric enrolment of the user — the FIDO client answers with the registration response containing the user's public key as well as the attestation of the authenticator. The relying party is then able to verify the attestation based on a metadata database containing the attestation certificates of known authenticators.

After a successful registration the user can authenticate to the relying party using the previously generated key pair (see Figure 23). The client triggers the authentication which is answered by the FIDO server with an authentication request (including a challenge) and the policy for accepted authenticators. The client then asks for local user verification which unlocks the private key. This allows the authenticator to sign the challenge and to provide attestation with the authenticator attestation key. The FIDO server can validate the authentication response based on the user public key that was stored during registration and the attestation certificate of the authenticator, provided by a metadata database or an external metadata service.

FIDO UAF also offers the option of transaction signing which is achieved by adding transaction data to the authentication request and including the signed hash of the transaction data into the authentication response.

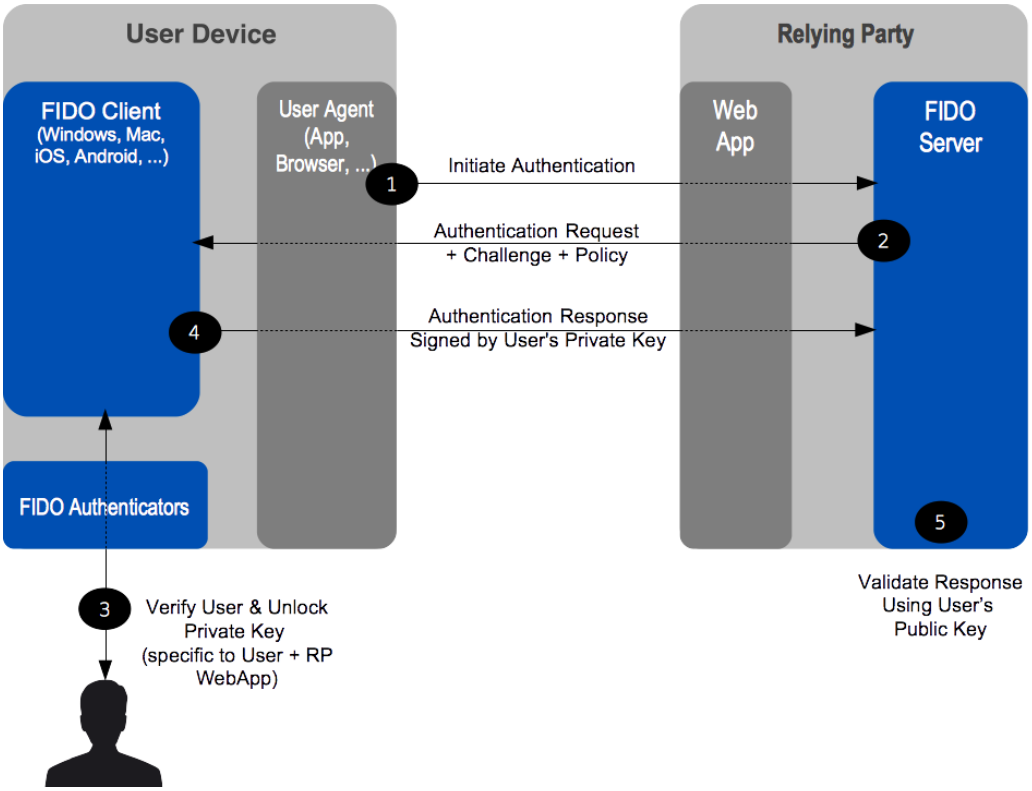

Figure 23 FIDO UAF authentication flow [21]

Since FIDO is following a lean design approach the protocol tries to minimize the trust infrastructure as much as possible. A kind of trust scheme can only be found for the authenticator attestation. It is based on a lightweight PKI used for device attestation where the authenticator proves its integrity with a self-signed certificate of the authenticator manufacturer that is published in a metadata database. The PKI is restricted to the absolute minimum and is only integrated due to the need to identify the type of authenticator that is used. Attestation is required due to the open nature of the FIDO authenticator landscape. In principle, every authenticator that complies with the FIDO protocol specifications can be used on the client side. As a consequence, there will be a large variety of authenticators with significantly different security levels. The range can include pure software implementations as well as TEE-based authenticators or hardware-supported devices (smart cards, µSD cards, USB tokens…). In order to enforce certain security policies, the relying party needs to know which type of authenticator is available and how trustworthy this can be. With the attestation certificates the relying party could restrict the range to only known authenticators.

Based on previous experience of PKI, the FIDO alliance has deliberately refrained from requiring a complete PKI chain based on a CA hierarchy in order to keep the system simple and to lower the technical and commercial hurdles for implementation. This is the reason why the attestation key is not signed by a CA but rather by the authenticator manufacturer as a self-signed certificate. Nevertheless, in the LIGHTest context it would be possible to define the policy of accepted authenticators within a trust scheme or trust domain. The policy can be published in a

trust list or repository and can be obtained by the FIDO server from this repository. This extension of the FIDO concept will not require a change of the FIDO protocol itself but only impacts the method by which the FIDO server obtains the policy for accepted authenticators.

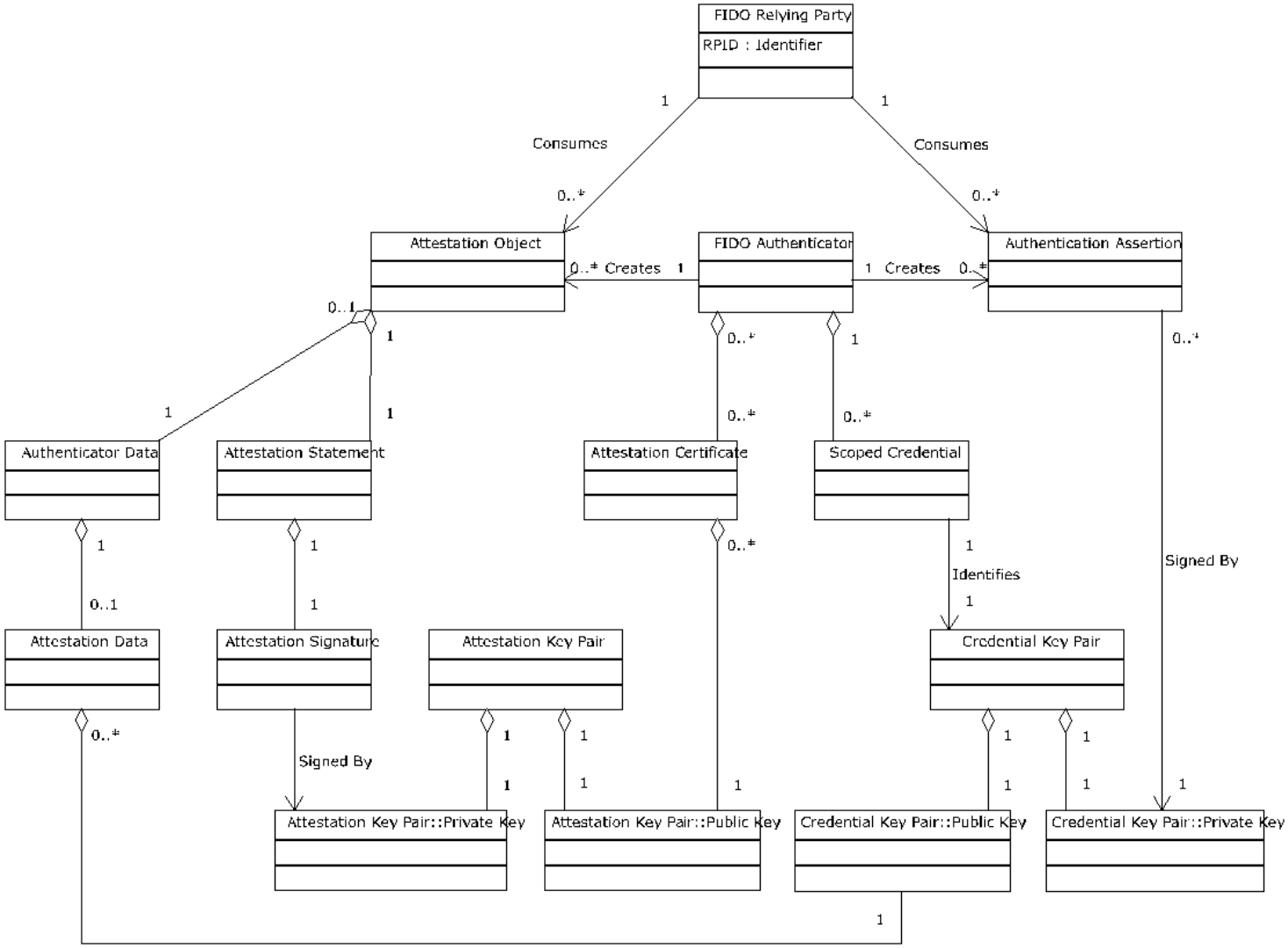

Figure 24 UML Diagram of FIDO

7.2.7 Trust Scheme of Turkey

Electronic signature has been recognised in Turkey since 2004 with T.C 5070 Electronic Signature Law, coming into force on 15 January of 2004 and 1999 European Union directive.

Turkey's law is modelled on a combination of the EU Directive on Electronic Signatures and ETSI TS 101 733 V1.5.1 (2003-7 12): "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats".

Electronic signature law compromises electronic signature, mobile signature and timestamp services used in Turkey electronic services. The aim of the act is to provide legal and technical aspects of the implementation and usage of the services in accurate manner.

The following concepts, based on ETSI TS 101 733 V1.5.1 (2003-7 12): "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats", are used to provide and manage electronic/mobile signature and timestamp services:

1. Electronic data: Data to be signed
2. Electronic signature: Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication
3. Signature Owner: A real person that uses a signing tool to create an electronic signature
4. Signature Generation Data: Data that may be used by the signature owner of electronic signatures to generate the signature from
5. Signature Generation Device: A software or hardware tool that uses the signing data to create an electronic signature
6. Signature Verification Data: Data that may be used by a verifier of electronic signatures to determine the signature is valid
7. Timestamp: A record confirmed by electronic signature by the electronic certificate service provider in order to determine when an electronic data is generated, modified, sent, received, and / or saved
8. Electronic Certificate: The electronic record that links the signature owner's signature verification data with the identification information

In practical means, electronic signature indicates that the signature is generated in a secure environment and the person has already verified his identity and approved the content. Turkey's electronic signature law, prepared according to the European Union Directive, includes the "qualified electronic signature" properties as follows:

a. Signature should belong to only the signature owner

b. Signature should provide to identify the identity of the signature owner

c. Signature should be prepared only within the consent and knowledge of the signature owner

d. Signature should provide to be able to determine whether an alteration on the signature data has been made

Electronic signature, **timestamp and certification validation services** use the signature formats, defined above, for the verification of electronic signature data. The verification procedures are based on, CEN Workshop Agreement CWA 14171, July 2001. To verify any electronic signature, the following procedures should be supplied:

- The electronic data to be signed
- The electronic signature of the electronic data
- The verification data to be used to verify the electronic signature. The data could contain electronic certificates, CRLs, OCSP responses, trusted timestamp obtained from trusted timestamp servers.

In order to state that trusted electronic signature is verified and valid according to regulations, the signature should be generated by the qualified electronic certificate and a trusted signature creation device. The qualified certificate details are obtained from RFC 3739 and ETSI TS 101 862 specifications. A trusted defined attachment should be available in the qualified certificates and the existence of the attachment should be controlled during signature verification process.

The certificate of the electronic signature will be issued by the governmental certificate authority (KAMU-SM) and should include the followings:

- The extension stating that the certificate is “qualified”
- Identity information of the certificate service provider with the country name
- The identity information of the certificate owner
- Validation data of the electronic signature of the certificate holder
- Beginning and End-date for the validity of the certificate,
- Etc.

The PKI infrastructure of KAMU-SM is given in the following figure:

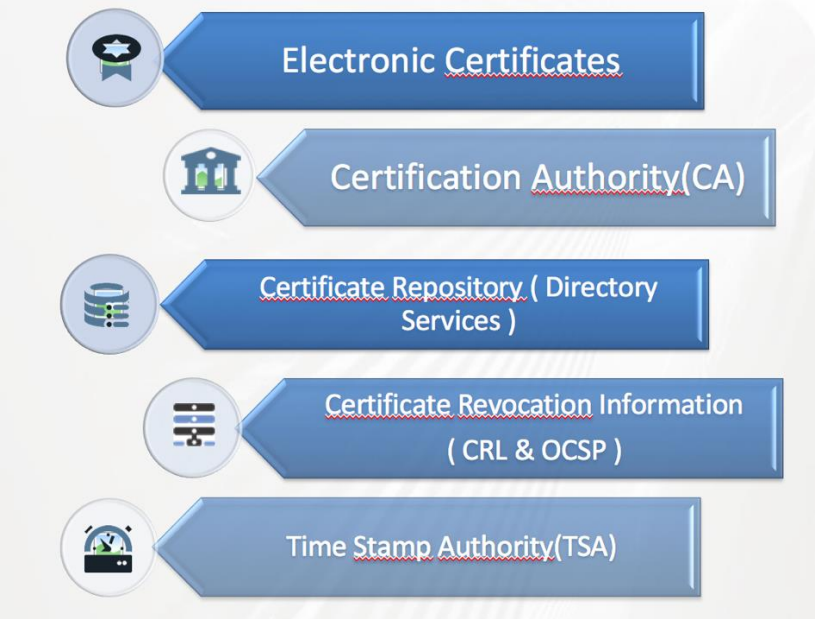

Figure 25 PKI Structure of KAMU-SM in Turkey

Certification Authority is the authority that checks the public key owners identity and generates and signs the corresponding electronic certificate. If someone wants to send an encrypted message to some other person, the public key of the receipient is required. In this case, Certificate Repository (Directory Services), LDAP is used to publish the electronic certificates used for encrytion. If someone lose/forget his private key or some information changed in the certificate, then these certificates must be revoked. Certification Authority (CA) issues the validity information of the electronic certificates with Certificate Revocation List or OCSP services.

In electronic signature, the accuracy of time is very critical and secure time is provided by Timestamping Authority (TSA).

KAMU-SM electronic signature infrastructure services support electronic signature standarts that are based on ETSI TS 101 733 V1.5.1 (2003-7 12). There are currently three different e-signature standarts:

- XML Advanced Signature (XADES): Digital signatures are represented in XML Format.
- CMS Advanced Signature (CADES): Signature is represented in binary format called ASN-1
- PDF Advanced Signature (PADES): PDF is an ISO standard. The signature is located in to pdf document directly in PADES.

Electronic signature types are defined in two categories to serve for different needs. The first category is electronic signature formats. The second category is electronic signature formats

with validation data. Electronic signature formats include Basic Electronic Signature (BES) and Explicity Policy Electronic Signature (EPES). Electronic signature formats with validation data include Extended Long Electronic Signature (ES-X Long), Extended Electronic Signature with Time Type 1 (ES-X Type 1), Extended Electronic Signature with Time Type 2 (ES-X Type 2), Extended Long Electronic Signature with Time (ES-X Long Type 1 or 2) and Archival Electronic Signature (ES-A). The following figüre illustrates the electronic signature types.

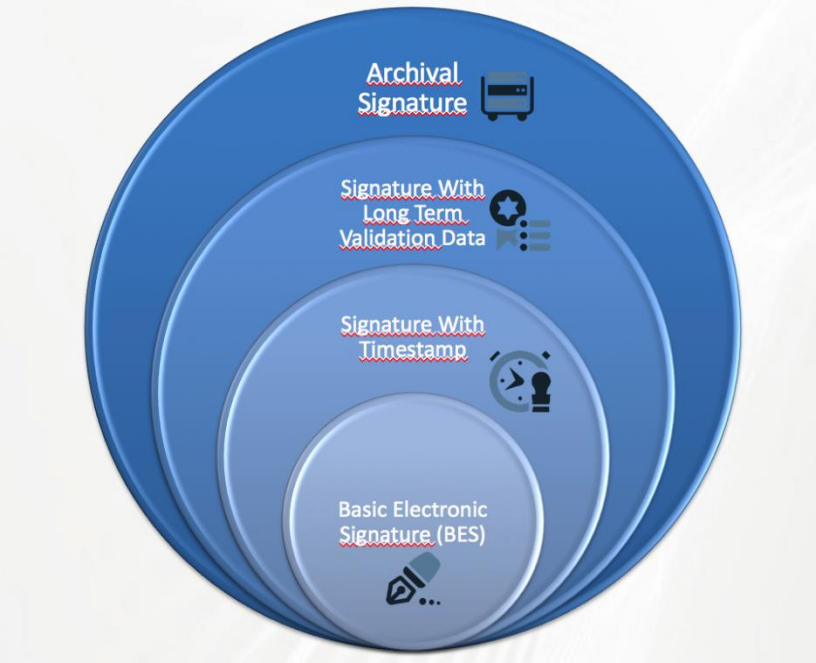

Figure 26 Signature Types

The UML diagram fort he electronic signature service is given below:

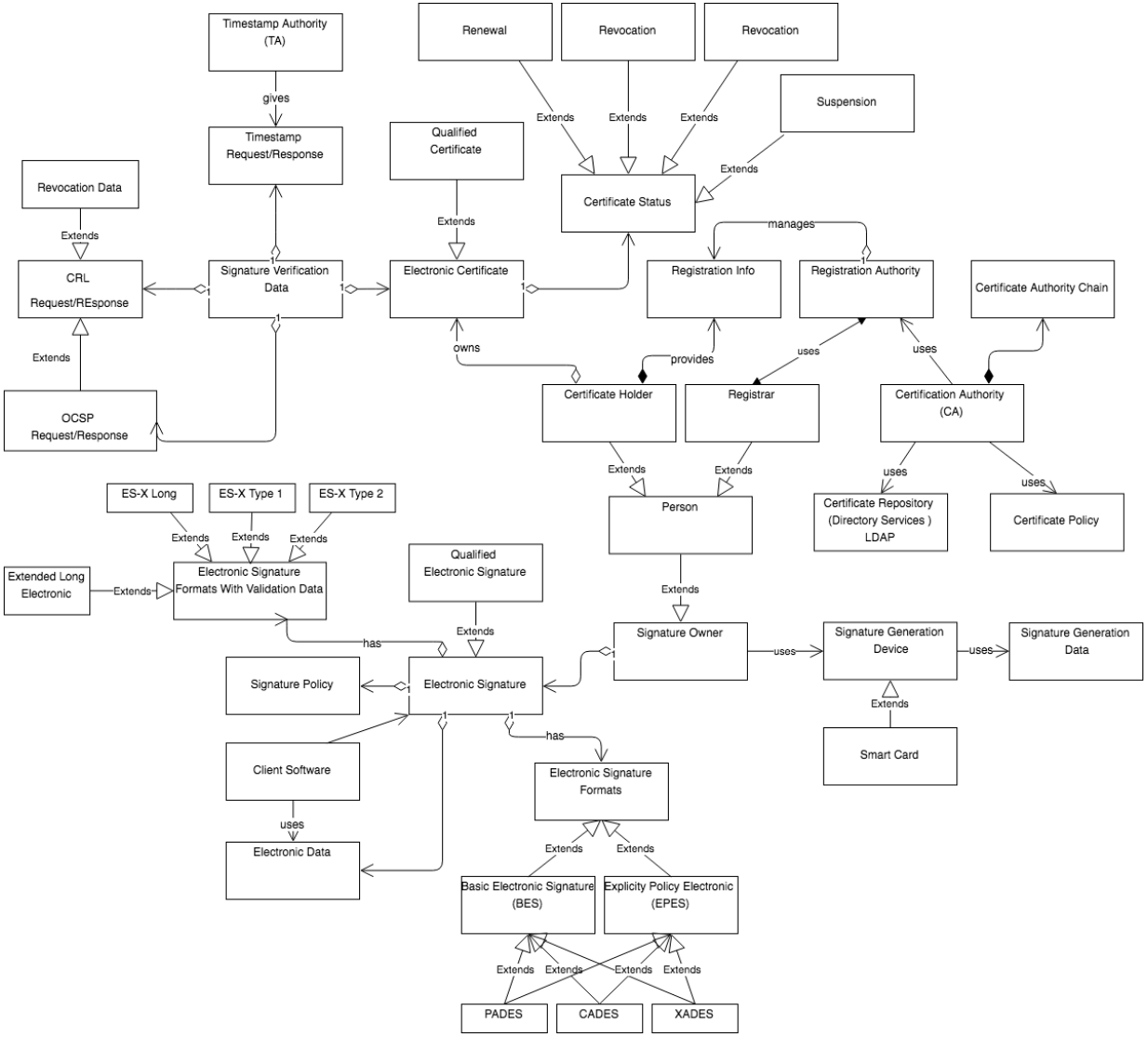

Figure 27 UML Diagram for Turkey Electronic Signature Service Constructs

7.2.8 Minors Trust Framework

Background

The Minors Trust Framework [22] is an online identity trust model, developed in conjunction with NSTIC (National Strategy for Trusted Identities in Cyberspace). Four guiding principles set out in NSTIC inform the MTF:

- Privacy-enhancing and voluntary;
- Secure and resilient;
- Interoperable; and
- Cost effective and easy to use

The goal of developing this Trust Framework is to bring participating organisations together with consumers in order to work together towards greater child safety, parental empowerment and compliance to regulations whilst maintaining consumer access and privacy. The Operating Rules for the Minors Trust Federation (Federation) are embodied in the MTF, and a deeper level of trust with parents is built for service providers that participate in the Federation.

This complete set of business (operational), legal and technical policies enable MTF members to identify and sign up children (minors) and their parents quickly, safely and in a privacy enhancing way.

How it works

The aim of the MTF is to allow credential service providers (CSPs) to create an online credential for parents and children that can be used by other online service providers. All CSPs agree to standards of privacy and security under the Federation. It is free and simple to use and the parents only need to have their identity verified once by an Identity Provider. Once accepted, parents can then pre-consent to their child's access to other Federation approved online services. The children benefit from being able to interact online in a safe and privacy secure manner and rather than acting as they have been doing, lying about their age, being excluded and/or marginalized, online services that sign on to the Federation will empower children to be full internet citizens, in good standing, that can experience the benefits of the world-wide web in a privacy-preserving, safe environment operating within the law.

MTF Governance

The MTF is enforced, modified and promoted through the Generational Trust Alliance ("Foundation"), [23] a Delaware LLP funded through Member fees, grants and sponsorships.

The Foundation's responsibility is to promote MTF and increase adoption, mainly the assessment guidelines for all Federation participants, ensuring all assessments are verified and finally enforcing adherence to the MTF.

The MTF also has a governance layer which comprises of Dispute Resolution Service Providers (DRSPs). This gives a forum to any participants who feel that their personal information or the child's information has been misused or disclosed to unauthorized parties.

MTF Policies

- Federation Operating Policy and Procedures Documentation
- Service provider certification at multiple levels of assurance
- Interoperable policies, protocols and reference implementation allowing identity verification services, attribute providers and credentialing authorities to engage with Federation members
- Identity ecosystem participants fostering adoption that represents millions of children and parents
- Oversight by the Generational Trust Alliance

Technical Description

The MTF is the collection of legal, technical, and operational policies that underpin trust across service providers and consumers that conduct transactions online. Federation Participants issue federated credentials to Adults and Children so that the Adult may grant verifiable parental consent to Federation and COPPA certified online services. The MTF enables Credential Service Providers that issue a Child-unique pseudonymous identifier to interoperate and interact with Relying Parties and other Members.

Figure 28 shows the flow for a child that is, or presumed to be, under thirteen years of age and is a case study for PRIVO [24]. When that child accesses a COPPA-regulated website or online service for the first time, they may be asked their age and for their parent-linked online identifier to initiate the COPPA consent process. The parent can give their sign-up information and proof of identity via an IdP if they want to sign up for an MTF Credential. Once the parent's ID is verified the CSP/CMA in this example case, can create and issue the Federation compliant identity credential to the parent, who can associate it with each of their children which begins the consent process for each Federation-compliant online service. Once this has happened the child can interact directly with the website or access the online service.

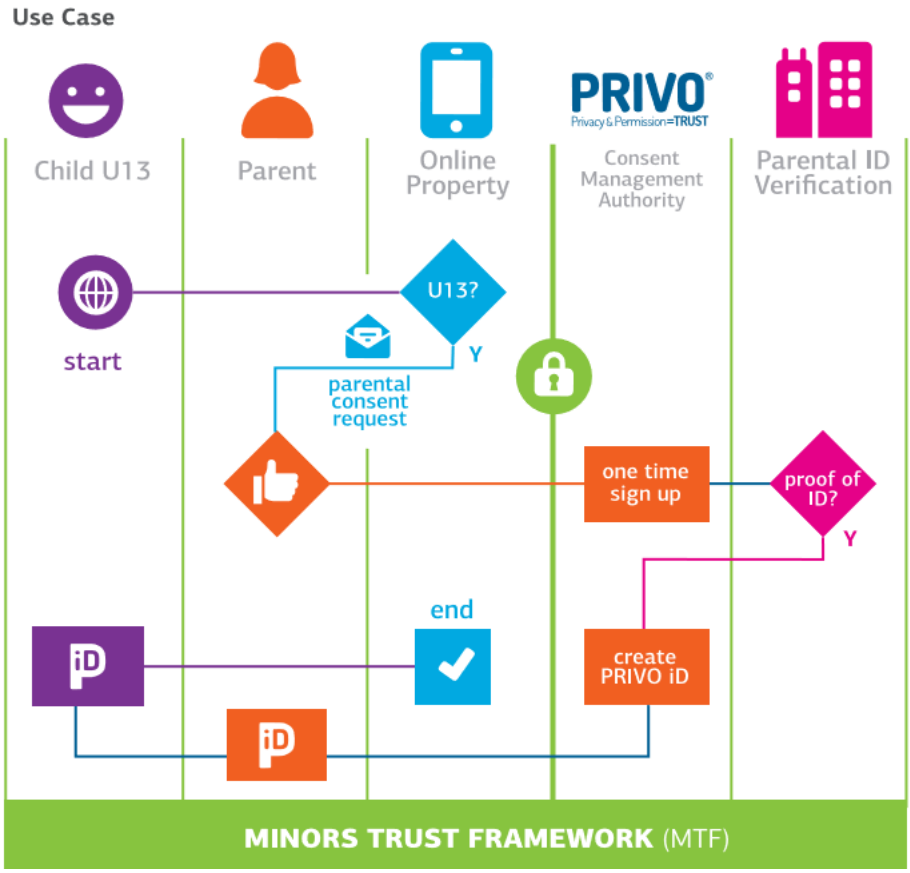

Figure 28: overview of the Primary MTF Use Case – PRIVO Example [23]

COPPA and User Segments

The consent requirements of COPPA depend on which segment an organisation falls under, and these are core to both the MTF's consent management function and to COPPA's enforcement, and many of these are defined clearly in the MTF Credentials section of the Trust Framework. The User Segments that are defined include individual users; child directed websites, apps and online services; child directed: children as primary audience, children as non-primary audience and general audience, websites and online services; aggregators; restricting access to adult content.

Credentials: Parent, Delegated Adult, Young Adult, Minor and Institutional

There are a number of different credentials that are certified under the MTF:

- Parent Credential
- Delegated Adult
- Young Adult Credential – for those aged 18-20 and associated with minor activities
- Minor Credential

- Institutional Credential – authorised persons of accredited educational institutions, non-educational institutions and commercial organisations

MTF Credential Verification Levels and Identity Assurance Programme

An MTF Credential Identity Assertion Profile (IAP) specifies a set of criteria that, if met or exceeded by a service provider, provide a useful tool by which a CSP and/or RP might determine whether Assertions of Identity conforming to those criteria can be used to help manage access to its service(s). The MTF defines IAPs to meet the requirements of a community of interested CSPs, RPs, and IdPs specifically those achieving compliance with COPPA, FERPA, and in the future, the Federal Identity, Credential, and Access Management (FICAM) requirements. The MTF intends to minimize the number of profiles by making them applicable to the broadest audience of CSPs, IdPs, and RPs. MTF Assessors have the role of reviewing MTF service provider's adherence to the IAPs. A list of the various credentials is below:

- Parent self-asserted
- Parent verified
- Parent verified plus
- Delegated adult
- Young adult
- Minor
- Institutional – including educational self-asserted, educational verified, non-commercial

MTF Participant's Federation Registration and Credential Issuance Process

Registration: At registration information is captured depending on which type of MTF Credential is being acquired — both adults and minors can register through MTF-supporting relying parties or directly with a CSP. In the case of Verified Institutional Adults they must register through their educational or non-educational institution.

Attribute Proofing: Attributes can be proofed through the inspection of identity documents issued by government agencies or others.

Adult verification: Attributes can be verified by trusted third parties. CSPs will not generally keep any PII that are considered sensitive, for example social security numbers.

Relationship verification: Attributes that have been used to prove an adult's identity, may also be used to verify the relationship to their minor.

Credential issuance: CSPs act as the custodian of attribute information and therefore maintain a registration services of parents and minors that serve as the identity stores to issue a token or

MTF parent and minor's credential. This credential is then used to access the services or applications required.

Attributes and Exchange Process

To use Federation-compliant authentication credentials, RPs may exchange a subset of their registration information with the CSP to provide independent adult and subsequent relationship verification. Any additional information collected must be handled in a transparent way.

The basic set of attributes to be exchanged is listed below:

Data Elements	Child (U13)	Minor (13-17)	Adult	Educator/Non-Parent Adult
Birth Date/Range	Required	Required	Required	Required
Unique Identifier (Site Based)	Required	Required	Required	Required
Password/Pin	Required	Required	Required	Required
Email	Permitted*	Required	Required	Required
First Name	Permitted	Permitted	Required	Required
Last Name	Permitted*	Permitted	Required	Required
Gender	Permitted	Permitted	Permitted	Permitted
Physical Address	Permitted*	Permitted	Permitted	Permitted
GPS Location	Permitted*	Permitted	Permitted	Permitted
Telephone Number	Permitted*	Permitted	Permitted	Permitted
Secret Q&A	Permitted*	Permitted	Permitted	Permitted
Device ID	Permitted*	Permitted	Permitted	Permitted
Authentication Source	Required	Required	Required	Required
MTF Permissions	N/A	Permitted	Required	Required
EULA/ToS Acceptance	N/A	Permitted	Required	Required
Trusted Institutional Parties	N/A	Permitted	Permitted	Required

*Permitted with Parental Consent

Table 3: MTF participant's credential attributes and exchange process [23]

MTF Certification Requirements: All Participants

The Foundation maintains the certification process as part of it's operating and governance structure. The criteria focusing on business and technical conformity to the MTF requirements to establish trust throughout the process. The assessment criteria focuses on organizational, business and technical requirements.

Figure 29: Certification process flow [23]

Compatibility with Other Digital Trust Networks

The MTF intends to be compatible with other digital trust networks as long as their rules and principles are in alignment with the MTF. Any trust networks who wish to work with the MTF must meet the following rules:

1. They must provide an explicit reference to the current version of the MTF; and
2. They must not define principles or rules that are in conflict with, or requiring an alternate interpretation of, the principles or rules defined in the MTF.

Functional Elements:

The below chart shows all the functional elements, grouped into core operations. Although not all will come up in each identity interaction, some may be invoked multiple times.

The following table gives descriptions of the roles in the functional elements layer. All Federation participants may serve in more than one role and they do not need to execute all functions in that role.

	Registration				Credentialing				Authentication Request				Authorization				Transaction Intermediation			
Role	Application	Attribute Control	Attribute Verification	Eligibility Decision	Credential Provisioning	Token Binding	Attribute Binding	Revocation	Authentication Request	Credential Presentation	Credential Validation	Authentication Decision	Authorization Request	Attribute Control	Attribute Verification	Authorization Decision	Blinding	Pseudonymization/ Anonymization	Exchange	Periodic & Event-Based Updates
User Person attempting to establish a digital identity and/or use a credential to access a protected resource.	●	●								●			●							
Credential Service Provider (CSP) Manages the credentialing and authentication core operations.					●	●	●	●		●	●	●								
Consent Management Authority (CMA) Manages consents by Parents/Guardians, Educators, or other Authorized Adults for Child/Minor use of RP services, features, and functions		●	●	●							●	●			●	●	●	●		
Authentication Service Provider Manages authentication core operations.											●	●								
Registration Authority (RA) Manages the registration core operation.		●	●	●																●
Identity Provider (IDP) Manages the registration, credentialing, and authentication core operation.		●	●	●	●	●	●	●		●	●	●								●
Attribute Authority (AA) Executes the attribute verification and attribute control functions in support of the core operations. May include Federal, State, or local governments, schools, service and commercial organizations, or technology organizations who may verify unique device characteristics.			●					●						●						●
Relying Party (RP) Relies upon other entities to execute the core operations and functions in order to authorize access to protected resources.				●			●									●				
Intermediary Executes the transaction intermediary core operation.																	●	●	●	

Table 4: Functional role description matrix [23]

7.2.9 Trust Scheme of Azerbaijan

Azerbaijan has a law governing digital signatures since 2004 [25]. This law is in compliance with the European Union Directive 1999/93/EC on digital signatures. At the moment the draft of a new law in compliance with the EU regulation 2014 (e-IDAS) is under the consideration of the

administration. For implementation of provisions of the law normative acts of the Cabinet of Ministers were approved in 2006 [26]. These regulations were enforcing the usage of digital signature in public administration. Only qualified signatures and certified signing tools can be used for electronic document flows in information systems of the public administration and local self-governance bodies. In accordance with the Law of the Republic of Azerbaijan, digital signatures created by certified signature means with a qualified certificate have the same legal value as a handwritten signature.

The Public Key Infrastructure has been built and delivered to production in 2011 for issuance of qualified certificates. The Certificate Services Center (CSC) was created in the same year within the Data Processing Center of the Ministry of Transport, Communications and High Technologies and is an operator responsible for issuing qualified certificates for digital signing and digital authentication for government bodies, businesses and citizens in the Republic of Azerbaijan. The validity period of digital certificates is three years. The Certificate Services Center is carrying out the management of digital certificate lifecycle and provides services on issuing, suspension, revocation and activation of digital certificates. It provides timestamp services to all digital signature owners the since 2011. Integrity is one of the most important requirements that allows for a signing process to be secure and provides full legal guarantees. Timestamp is a tool, which guarantees the integrity of digital signatures. Certificates for digital seal issued to governing bodies and legal entities are securing invoices, statements, medical reports and custom declarations.

The implementation of digital signature tools in legally binding document circulation is based on specifications that define the use of public key cryptography (digital signature) and approval of the quality of digital signature tools is required. The development and deployment of electronic signature tools providing qualified signature is carried out by licensed organizations only. The organization certifying the compliance of digital signature tools with the existing requirements and standards is the certification laboratory of the Ministry of Transport, Communications and High Technologies.

In accordance with Presidential Decree No.65 the Ministry of Transport, Communications and High Technologies is the executive authority responsible for accreditation and registration of certificate centers in the Republic of Azerbaijan [27]. Accreditation is conducted by the Certificate Services Center of the Ministry of Transport, Communications and High Technologies and is accompanied by issuing qualified certificates of the CSC Root Authority to organizations that passed accreditation. The trust hierarchy of Certificate Authorities (CA) managing and issuing certificates is shown in Figure 30.

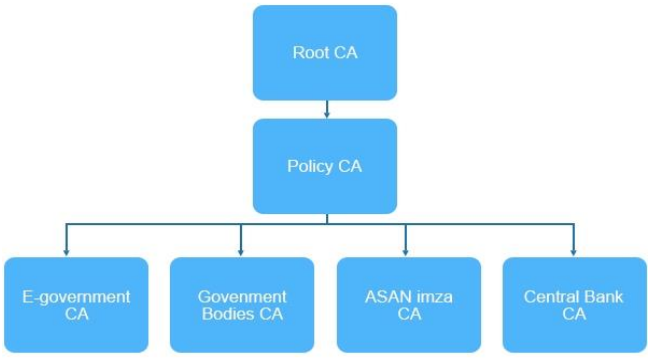

Figure 30: Trust hierarchy of Certificate Authorities (CA) in the Republic of Azerbaijan

From an organizational point of view the Root Center is a structural unit of the Certificate Services Center of the Ministry of Transport, Communications and High Technologies. The Root Center is involved in the issuance of certificates for subordinate Certification Authorities in order to provide extensive usage of digital signatures. It provides the certificate for the registration of next level Certificate Authorities. The Root Center is operating offline and employs a high level of security to protect its important components. The Root Center is self-signed because it stands on the highest hierarchy level.

On the second level of 3-tier trust model is the Policy CA of CSC. It's purpose is to describe the policies and procedures implemented in the organization.

There are four Certificate Authorities on the third level of the hierarchy. The first two CA's belong to the CSC, while the accredited "ASAN imza" Certificate Authority was established by the Ministry of Taxes of the Republic of Azerbaijan. This CA is issuing qualified certificates to state authorities, local self-government bodies, business entities and individuals. Finally, the "Central Bank" CA is managing and issuing qualified certificates to bank clients and employees.

The Certificate Authorities are carrying out the following procedures: issuing of qualified certificates; suspension, resuming and revocation of certificates; provision of information on certificates upon request; provision of time indicators and digital seals.

Each certificate contains: title and address of the center granting certificate (country), serial number of the certificate, name and surname of the signature holder or pseudonym, validity of the certificate (time and date of beginning and ending), signature verification information of the signature holder, and title of signature means in which signature verification information will be used. Certificates for citizens include their unique personal identification numbers (PIN) while for employees of organizations (legal entities or governing bodies) the organization's unique VAT number is added.

Registration Authorities (RA) are verifying the identity of applicants prior to issuing digital certificates. The Certificate Services Center has 66 registration points situated in the regional post offices of the country. Citizen can apply for digital signature certificates submitting their

applications online or physically deliver filled applications together with the original document and its copy confirming their identity. The registration point authority compares the applications of the owners of a signature with the information of the state register of identity cards (IAMAS) of the Ministry of Internal Affairs and other sources of information, reviews and approves or rejects them.

Legal entities can apply for digital signature certificates submitting their applications online or physically deliver filled applications and documents in accordance with the list of required documents provided by CSC. They also must provide copies of identity cards of each applicant and a sample of a seal approved by the head of the organization. The application procedure for governing bodies works in the similar manner.

Figure 31 demonstrates the business workflow for registration and issuing of digital certificates in CSC.

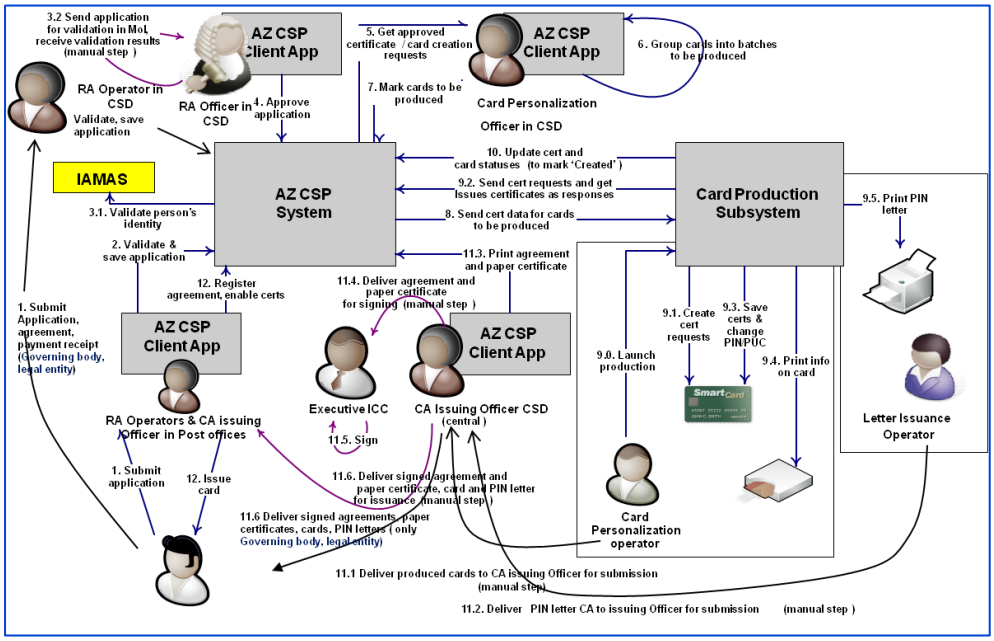

Figure 31: Business workflow for registration and issuing of digital certificates in CSC

The Certificate Service Center is also the provider of digital signature certificates for the national identity card. The new generation national identity card (e-ID) of the citizens of the Republic of Azerbaijan will be issued by the Ministry of Internal Affairs on 1 September 2018. A new Public Key Infrastructure has been built by the Certificate Services Center of the Ministry of Transport, Communications and High Technologies and is ready for exploitation.

The e-ID chip will contain two digital certificates issued by the Certificate Services Center of the Ministry of Transport, Communications and High Technologies. The e-ID card is a document for personal identification of citizens and can be used for identification of a certificate holder on the internet and for digitally signing electronic documents with legal value. The new generation identity card also is ready for use in electronic services of the e-government portal. It is suitable

for services ranging from banking solutions and electronic commerce to national health services. This identity card will be valid for 10 years and include electronic X.509 certificates valid for 5 years. Upon expiration, certificates can be renewed for the next 5 years. Citizens aged 15 and above receive their identity cards containing two certificates – one certificate for identification and another one for digital signing. Citizens aged 10 to 14 years have only one certificate for personal identification. Finally, citizens below age 10 will not have any certificates in the chip of e-ID card.

The chip of e-ID card is CC EAL6+ certified and provides outstanding security, including superior protection against hardware attack scenarios. Two certificates and keys (for identification and digital signing) contained in the chip of e-ID card use the ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm with hash function SHA256. The identity card has all security features specific for a similar type of identity card on polycarbonate material.

Citizens can apply at all regional police departments of the Ministry of Internal Affairs of the Republic of Azerbaijan (81 departments) and ASAN (State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan) service centers (11 centers) to receive the new generation ID cards. Personalization of ID cards will be carried out by the 9 personalization officies of the Minisrty of Internal Affairs and 4 ASAN service centers. The validity of information presented in application form will be verified via a service of state register of identity cards (IAMAS) of the Ministry of Internal Affairs.

7.2.10 Embedded UICC Remote Provisioning

For several decades, the SIM card for mobile phones has been the predominant access token for end user devices connecting to the mobile network. But since the LIGHTest partner G+D shipped the first commercial SIM card worldwide in the early 1990s, market requirements have changed and the upcoming Internet of Things (IoT) is currently triggering some fundamental transistions. For most IoT devices there is a need to manage mobile network subscriptions remotely since the device may not be physically accessible all the time. As an example, it would be quite unhandy to call a connected car to the dealer's garage in order to switch the subscription to another mobile network provider.

Therefore, the GSMA has developed a provisioning scheme that allows to perform remote management of an embedded SIM card, or more generally speaking an embedded UICC (universal IC card) which can have a SIM functionality but also other applications as well (e.g. a payment or eID application) [28], [29]. Since managing applications — including mobile network connectivity — is a security critical task, a corresponding trust scheme is required to ensure controlled access and mutual authentication of the involved entities. This PKI-based trust scheme allows to identify the various roles and entities within the provisioning flow and is centred around a certificate issuer who acts as a trusted 3rd party.

Within the GSMA remote provisioning architecture, the following roles and entities are the most relevant for understanding the trust scheme [28]:

eUICC Manufacturer (EUM): this is the provider of the eUICC hardware and OS software stack. The initial cryptographic configuration and security architecture of the eUICC is provided by the manufacturer. The EUM also issues the eUICC certificate to allow authentication to other entities and key establishment for secure communication.

Mobile Network Operator (MNO): the MNO provides connectivity to the mobile network and defines the policy rules that control the profile management of the subscription profile.

Subscription Manager-Data Preparation (SM-DP): This entity acts on behalf of the MNO and personalizes the initially un-personalized profile with the concrete user credentials of a specific UICC. The SM-DP can also enable or delete profiles on the UICC on request by the MNO.

Subscription Manager-Secure Routing (SM-SR): The SM-SR provides the transport layer for communication with the eUICC and is the only entity that is allowed to establish a secured and authenticated communication channel with the eUICC. This role can be within the same organisational entity as the SM-DP.

Certificate Issuer (CI): This entity acts as a trusted 3rd party and issues certificates for the EUM, SM-SR, SM-DP and MNO. It acts as a trust anchor of the remote provisioning system.

An overview of the relevant entities and their relations is shown in Figure 32.

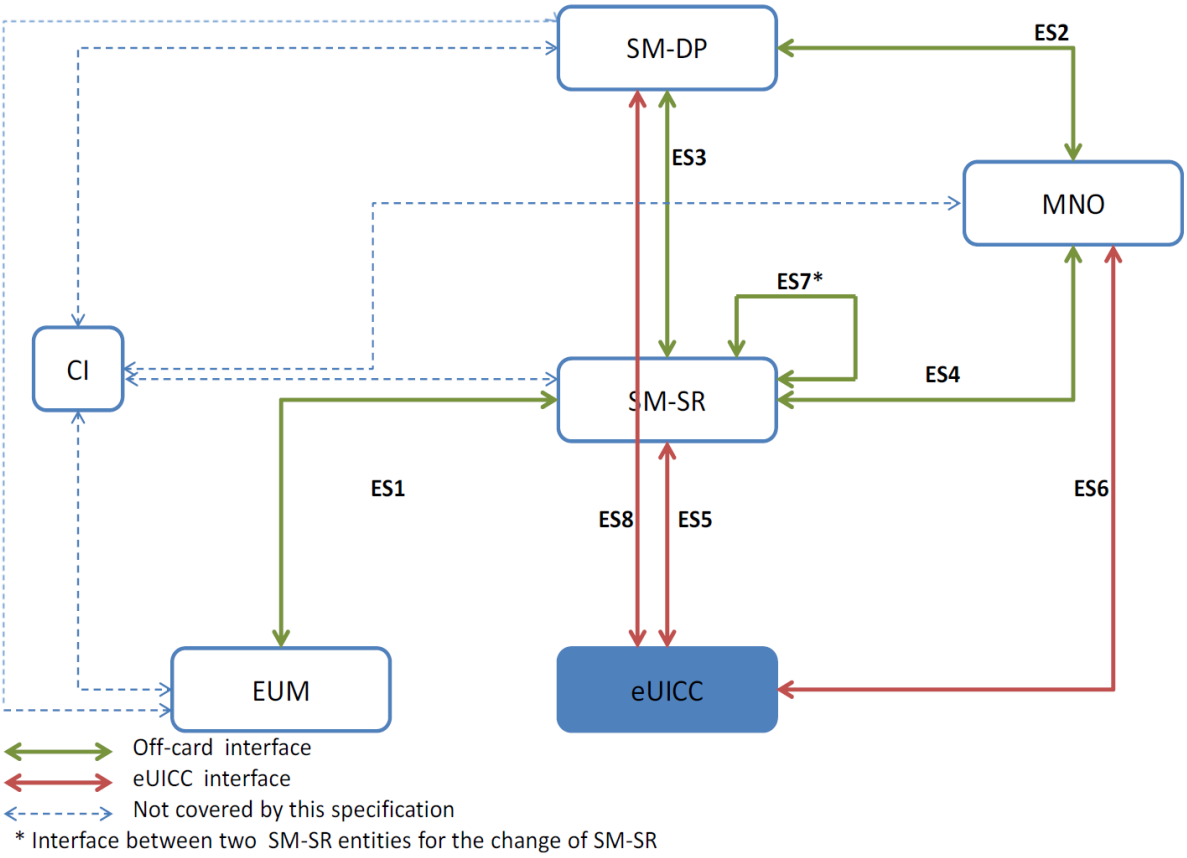

Figure 32: Entities and relations of the remote UICC provisioning system. From [29].

The different roles and responsibilities of the trust scheme participants are also reflected on the eUICC itself. This is accomplished by card security domains, according to Global Platform Card Specifications [30]. The following security domains are available on an eUICC:

eUICC Certificate Authority Security Domain (ECASD): this domain contains the unique and non-modifiable private key of the eUICC, the associated certificate and the root public key(s) of the Certificate Issuer (CI). It is therefore also the on-card representation of the CI. The eUICC manufacturer (EUM) configures the card during manufacturing.

Issuer Security Domain-Root (ISD-R): this is the on-card representation of the SM-SR and is used to provide secure transport channels to the SM-SR. This domain can create new ISD-profile domains (see below) for new subscription profiles.

Issuer Security Domain-Profile (ISD-P): this is the on-card representation of the SM-DP (or MNO) and contains the actual profile and keys for profile management of the SM-DP. The key set for personalisation is also used to decrypt the profile sent by the SM-DP. The ISD-P domain

can optionally also contain a profile-specific CASD (Certificate Authority Security Domain) that provides security services to the profile domain when the profile is in an enabled state.

Within the trust scheme of remote eUICC provisioning, the CI has a central role in the certificate chain and acts as a trust anchor of the scheme. The following certificates are provided by the CI [29]:

- A self-signed Root Certificate used to verify certificates issued and signed by the CI.
- A public key as part of the Root Certificate, used on the eUICC to verify certificates issued by the CI.
- A certificate signed by the CI to authenticate the SM-DP. This certificate is used for loading and installing the profile.
- A certificate signed by the CI to authenticate the SM-SR. This certificate is used to manage SM-SR access.
- A certificate, signed by the CI, to authenticate the EUM. It is used in both, the download and installation of the profile and the SM-R access.

The self-signed root certificate and the EUM certificate are based on X.509, including the extensions `SubjectAltName` and `SubjectKeyIdentifier`. The other certificates are based on Global Platform card specifications ([30], Amendment E).

An overview of the certificate chain is shown in Figure 33. Although the GSMA trust scheme is an industry-driven scheme with a very special functionality, the general structures are nevertheless comparable to other schemes like eIDAS.

The role of the CI is usually taken over by the GSMA itself, which also issues and maintains the specifications of eSIM management in general. Therefore, the eSIM management can be regarded as a global trust scheme. As a consequence, trust translation is therefore usually not required. It is possible however that other organisations act as a CI on behalf of the GSMA. This is the case for some regional sub-organisations as well as for certain larger mobile device manufacturers that maintain their own CI root under the roof of the GSMA.

For this reason, the LIGHTest infrastructure seems to be very beneficial to publish the trust information of allowed Cis on a global level. The GSMA could therefore act as a root of trust and trust scheme authority for all organisations that act as a CI within the eSIM management

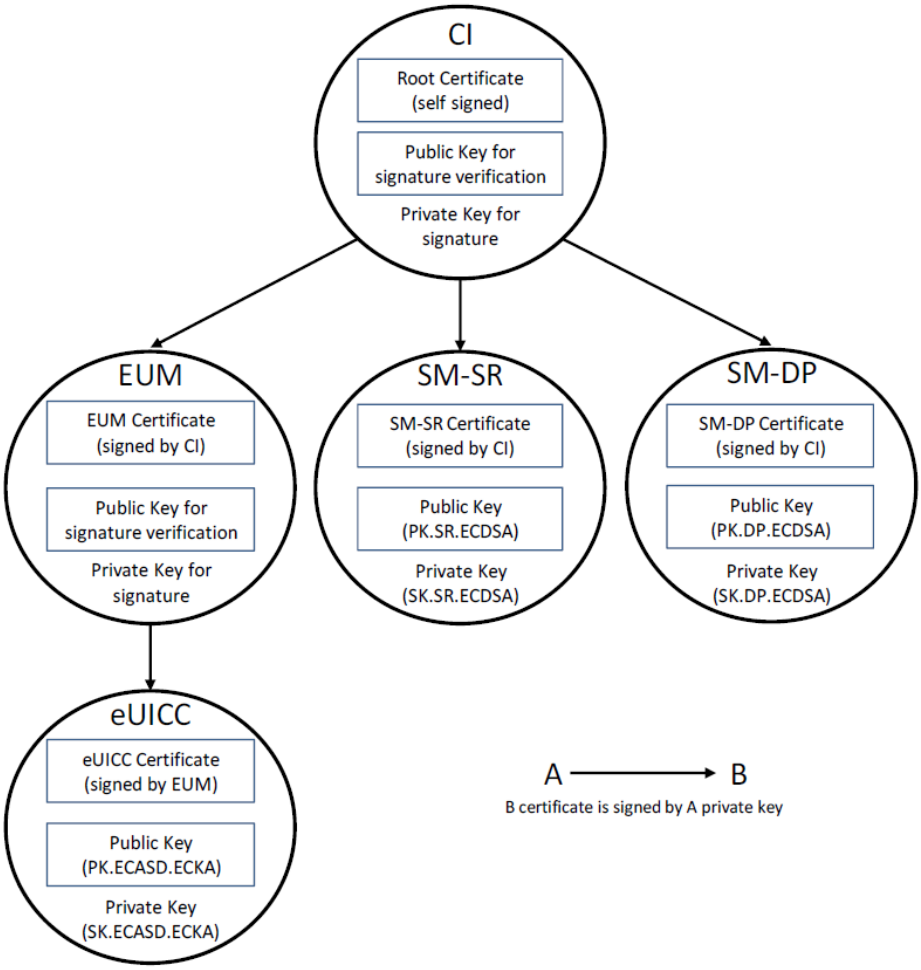

Figure 33: Certificate chain of the eUICC remote provisioning scheme. From [29].

scheme. The global infrastructure that LIGHTest offers could be used to establish many Cis within the scheme and therefore also trigger competition.

7.2.11 Trust Scheme for PEPPOL

The Pan-European Public Procurement On-Line (PEPPOL) project was initiated in 2008 with the aim of simplifying electronic procurement across borders by developing technology standards that could be implemented across all governments within Europe. The overall objective was to enable business to communicate electronically with any European government institution in the procurement process, increasing efficiencies and reducing costs. Through agreement on specification for cross-border procurement, the PEPPOL has contributed to the development of a pan-European, standardized IT infrastructure. PEPPOL has not replaced, but build upon, the existing national eProcurement systems buy using information and communication technologies to enable them to connect with each other. PEPPOL's transport infrastructure interconnects

eProcurement systems using common and nationally compatible standards. Access to the PEPPOL infrastructure takes place through Access Points which are provided by both government agencies and private companies, and provides services for eProcurement with standardized electronic document formats. PEPPOL developed the Business Interoperability Specification (BIS) for common eProcurement processes such as eCatalogue, eOrders, and eInvoices to standardize electronic documents exchanged and validated through an open and secure network, between sending and receiving Access Points for public sector buyers and their suppliers across Europe. Once connected to the PEPPOL Transport Infrastructure, organizations can reach any other community already using the PEPPOL network. [31] [32]

PEPPOL provides three components [33]:

(1) PEPPOL e-Delivery Network, a network for securely and reliably exchanging messages between participating entities.
(2) PEPPOL 'BIS' Specification, a specification of standardized document formats for procurement processes.
(3) PEPPOL Transport Infrastructure Agreement (TIA), providing the legal framework for communication between the many connected parties.

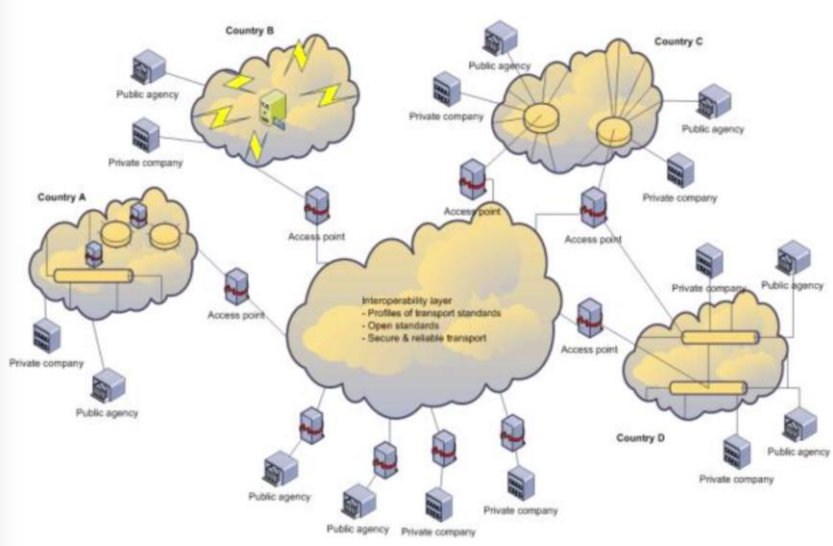

Figure 34: Overview the PEPPOL eDelivery Network [34]

The eDelivery Network uses a four-corner architecture where participants use an Assess Point of their choice to connect to the network which then takes care of the message exchange with the participant's business partner (through the Access Point chosen by the partner).

Access Point (AP):

PEPPOL Access Points (Aps) form a secure network by connecting to each other using the same transport protocol and document format, applying digital signature algorithm to secure message content. Operators of Aps connect to their customers through existing network and use the

PEPPOL network to exchange electronic documents (for example an eInvoice, an eOrder or an eCatalogue) with each other. The sender can be a large corporation, an SME or a public administration, and uses an Access Point to connect to the PEPPOL network, specifying the type of the document being sent and the recipient which is uniquely identified in the network by a business ID. Access Points can either be built by an organization or provided as a service from an IT provider offering PEPPOL capabilities. [31]

SMPs (publishing the capabilities of PEPPOL participants)

The PEPPOL infrastructure maintains centralized addressing and metadata information on servers called Service Metadata Publishers (SMPs) which contain the delivery addresses and their receiving capacity (business processes and document types supported, etc.) of the parties' Access Points. All PEPPOL participating organizations (such as contracting authorities or suppliers) publish their delivery address and receiving capabilities to a Service Metadata Publisher. SMPs store information about the users connected to the PEPPOL network, providing details about the business document types supported and the business collaboration profiles that can be processed through the national infrastructure. SMPs can be provided as an independent service by a third party organization. [31]

SML (central registration system for addressing)

In order to deliver electronic documents from a sender to the correct recipient, all PEPPOL Access Points need to know about each other and the participants they support. To do this PEPPOL maintains one centralized service, called the Service Metadata Locator (SML). The PEPPOL SML defines which Service Metadata Publisher (SMP) to use for finding out the delivery details of any PEPPOL participant. The SML service specification is based in the use of DNS (Domain Name System) lookups to find the address of the Service Metadata for a given participant identifier. The SML contains the related SMP for every participant identifier. The SML service itself plays the role of providing controlled access to the creation and update of entries in the DNS. [31] [32]

For a sender to send a document to the recipient, the first step in the discovery process is to establish of the location of the Service Metadata relating to the particular participant identifier to which the sender want to send. Each participant identifier is registered with only one Service Metadata Publisher (SMP). The sender uses the business ID (recipient) to look up the SMP using the DNS-based SML service, then it returns the corresponding SMP IP Address. The sender can then retrieve Service Metadata using SMP services to obtain the metadata about the participant identifier, which includes the information (Document Identifier and recipient Access Point Web Service Address) necessary to transmit the message to the recipient Access Point represented by that participant identifier. [31]

PEPPOL PKI (security and trust)

Security and integrity of the business transactions through the PEPPOL eDelivery Network relies on using a Public Key Infrastructure (PKI) to establish a trusted network. When Access Points or

SMP providers sign the PEPPOL Transport Infrastructure Agreements they are provided with a PEPPOL Digital Certificate which they use to identify themselves in communications on the PEPPOL network. Upon successfully completing the certification process, an access point submit a certificate signing request to the OpenPEPPOL authority which creates a certificate signed within the PEPPOL trust chain. The certificate is valid as long as the Transport Infrastructure Agreement is valid and can be revoked if service providers are in breach of the Agreement. This ensures only known and trusted providers provide services on the eDelivery Network. Communication between an organization and their access point is not regulated by PEPPOL and can happen in whatever form they agree on to accommodate existing systems or procedures. Therefore, it is the responsibility of the Access point provider and its connected participants to ensure that the information is also sufficiently secured during the communication between Access Point and participant. A sender Access Point is required to authenticate the sender of document and vouch for its identity to the recipient and send the result of the authentication to the recipient. To this end, the sender Access Point issues a SAML 2.0 token stating the sender identity, level of identity assurance (1-4) where level 1 is low confidence in claimed identify and level 4 is very high confidence in claimed identity. To our knowledge, however, this assurance level is so far not considered any further in the PEPPOL network. The PEPPOL ROOT PKI is used to create the core “circle of trust” in PEPPOL between Access Points, SMPs, and SMLs. A Certificate Authority (CA) issuing digital certificates under a central PEPPOL root certificate. Anyone with a PEPPOL certificate is considered as a valid member of the infrastructure. Service providers can validate peers just by installing the PEPPOL root certificate. [32] [31].

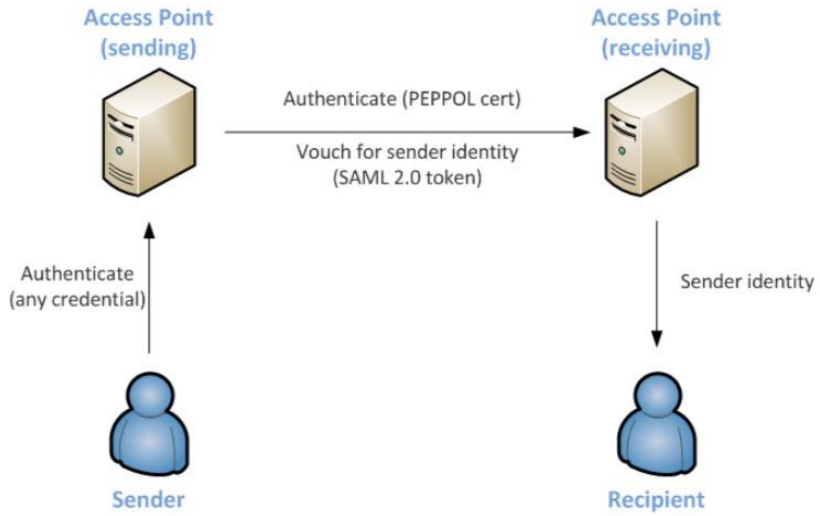

Figure 35: PEPPOL authentication [32]

For the secure message exchange between the access points both transport and message level security are used. For transport level security, TLS can be used, for message level security, PEPPOL employs AS4 protocol (in older versions, AS2) from the ebMS OASIS standard, to protect the confidentiality and integrity of the exchanged information and to ensure non-repudiation of receipt.

AS4 User Messages include both signing and encrypting to protect the integrity and confidentiality of the business documents. The Access Point must acknowledge received User messages using a signed non-repudiation Receipt which contains the digest of the payload of the original message. Every PEPPOL message sent through the Access Point must be signed by the certificate issued by the PEPPOL PKI to the Access Point provider. The receiving Access Point is able to validate the certificate using the PEPPOL PKI CA certificates without the need to know the certificate of the sending Access Point beforehand. Every PEPPOL message received by an OpenPEPPOL Access Point must be authenticated by verifying that it is properly signed using the embedded certificate and that the signing certificate is itself signed by within the OpenPEPPOL trust chain. [34] [33]

Existing Trust Schemes Used in the PEPPOL

There is currently no explicit trust scheme specified, but implicitly the network relies on a straightforward public-key infrastructure based on a single root certificate. All access points and SMP providers receive a digital certificate which they use to identify themselves in communication. These certificates are created based on trusted certificate authority (CA) operated by PEPPOL itself. Verification in the network relies in distributing the CA and intermediary certificates between all access points. [33]

Integration of LIGHTest

The idea to integrate LIGHTest into PEPPOL is that we can basically generalize this to use certificates of any trust scheme like for instance eIDAS (as the most relevant in the European Union). With LIGHTest, the single root certificate can be replaced by the trust list in a trust scheme. For instance, LIGHTest's Automatic Trust Verifier (ATV) can use trust lists to verify Access Points and SMPs.

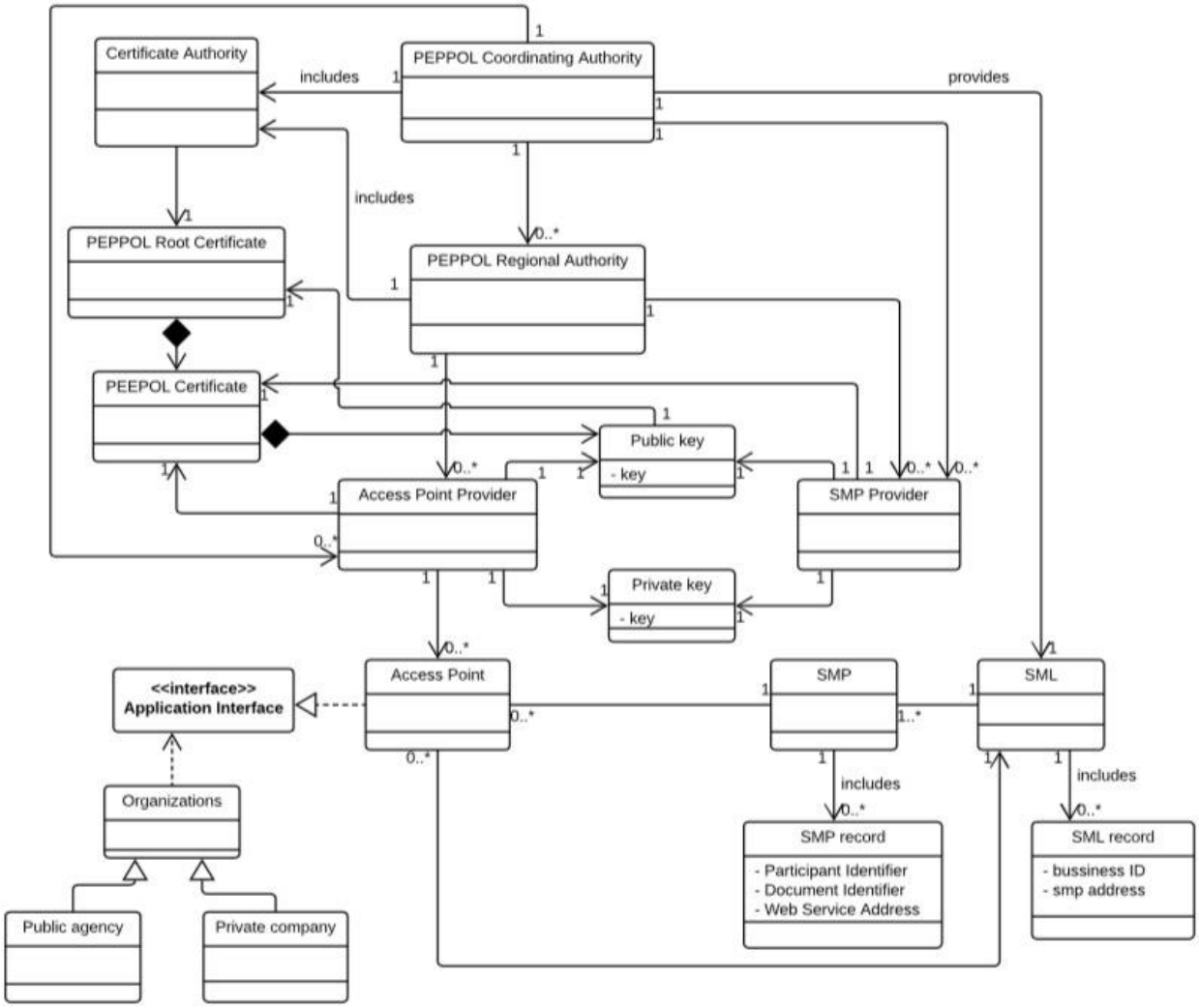

Figure 36: UML Diagram of the PEPPOL structure

7.3 Conceptualization of a Data Model for Tuple-Based Trust Schemes

The consolidation resulted in three abstract concepts which are required for description of trust schemes: Credential, Identity, and Attributes, whereas the latter involves attributes which are not used for authentication, and are included mainly for compliance with STORK QAA/AQAA. The following provides a list of the concepts of Credential, Identity, and Attributes. Hereby the concepts involved with Credentials, Identities, and Attributes are both visualized and described. Any written text hereby indicates the concepts in bold in the text (e.g. **Credential Secure**

Storage) in order to ease the understanding of the description. Furthermore, the concepts are described in Tables.

7.3.1 Credentials in Tuple-Based Trust Schemes

Figure 37 shows an overview on the concepts involved in the establishment of trust in credentials of Tuple-Based trust schemes. Hereby abstract concepts, such as the **Authoritative party** are included along with concepts that are either aggregated, such as **Credential Assurance**, or generalized, such as **Procedure to ensure activation through intended entity**. Table 5 provides the description of the concepts used for defining a credential.

Concept	Description
Authoritative Party	An approved, recognized or trusted body that provides assurances (of credential or identity) to relying parties
Credential Binding	Assurance that credential is/remains bound to correct entity
Hardware Security Module	Containment in the credentials against tampering
Credential Broker	Broker for credential service between an individual and an Authoritative Party (Credential Service Party)
Registration Authority	A Registration Authority that provides the credential.
Relying Party Scoped Credential	A credential that allows a user to authenticate itself to the relying party for which the credential was made
Credential Risk	The risk that an individual, organization or device has lost control over the credential that has been issued
Human-Issued	Indicating that a credential has been issued by a human
Network Binding	Indicating that a credential binds a subject to a network
Multi Factor Authentication	Two or more credentials implementing different authentication factors shall be used
Password Strength	Use of strong passwords shall be enforced
Credential Lockout	Lockout mechanism shall be used after a certain number of failed password attempts
Default Account Use	Default account names/passwords shall not be used
Audit and Analyze	Audit trail of failed logins to analyze for patterns of online password guessing attempts
Hashed Password with Salt	Use of hashed passwords with salt
Anti-Counterfeiting	Use of anti-counterfeiting measures on devices holding credentials
Detect Phishing Attacks	Use of practices to detect phishing
Adopt Anti Phishing Practices	Use practices such as disabling images, disabling hyperlinks etc.
Mutual Authentication	Use of mutual authentication mechanisms, e.g. to protect against Man in the Middle (MitM) attacks
No transmit password	Do not transmit passwords over the network (e.g. Kerberos protocol)
Encrypted Authentication	Encrypt data prior to transit if authentication exchange over a network is necessary
Different Authentication Parameter	Use different authentication parameter for each authentication transaction
Timestamp	Timestamp each message with a non-forgeable timestamp
Physical Security	Use physical security mechanisms (i.e., tamper evidence, detection, and response)
Encrypted Session	Protects against session hijacking and man in the middle
Fix Protocol Vulnerabilities	Use platform patches to fix protocol vulnerabilities (e.g., TCP/IP)

Concept	Description
Cryptographic Mutual Handshake	Use mutual handshake exchange based on cryptography (e.g., SSL/TLS)
Credential Activation	An activation feature shall be required to use the credential (e.g. entering a PIN into the hardware device containing the credential).
Code Digital Signature	Verify digital signatures against a trusted source to counter the downloading of software that has been modified by unauthorized parties
Liveness Detection	Use liveness detection techniques to identify the use of artificial biometric characteristics (e.g., forged fingerprints).

Table 5 Description of the concepts that define a credential in Tuple-Based trust schemes

Generalizing concepts in Table 5 include **Credential Binding**, which can be specialized into **Credential Binding using Digital Signatures**, and **StateLocked for Credential Binding**. Both are mechanisms, which provide tamper resistance of the Credential Binding.

Aggregating concepts in Table 5 involve the **Authoritative Party,** the **Registration Authority**, the **Relying Party Scoped Credential**, and the **Credential Broker**.

The **Authoritative Party** which provides assurances of credentials or identities to relying parties may additionally require the verification of the **Authority Chain**, e.g. of Certification Authorities.

The **Registration Authority** may also sign a Credential, in which case the **Registration Authority Signature** additionally defines the Credential.

The **Relying Party Scoped Credential** is a credential that allows a user to authenticate itself to the relying party for which the credential was made. It includes **Attestation**, which ensures that the scoped Credential has been registered by an authenticator with a relying party. This **Attestation** can further be supported by an **Attestation Certificate**, which is a X.509 certificate for an attestation key pair used by an authenticator to register a scoped credential with a relying party. The **Attestation Certificate** itself is not a scoped credential.

The **Credential Broker** is conceptualized by **Credential Assurance**, which is the assurance that an individual, organization or device has maintained control over what has been entrusted (for example, key, token, document, identifier) and that the credential has not been compromised (for example, tampered with, modified). **Credential Assurance** aggregates the concepts that are described in Table 6.

Concept	Description
Formalized and documented processes	Minimum Requirement for Credential Creation
Tracked Inventory	Keep the hardware device physically secure and the inventory tracked to prevent unauthorized creation of credentials
Ensured Issuance Process	Ensure that credential is provided to correct entity (authorized representative)
Procedure to ensure activation through intended entity	Procedure to ensure that a credential is activated only if it is under the control of the intended entity.
Credential Secure Storage	Requirements for Secure Storage of Credentials

Revocation or Destruction of Credentials by CSPs within specific time period	Revocation or Destruction of credentials by CSPs within a specific time period defined by organizational policy
Credential Secure Renewal	Requirements for Credential Secure Renewal
Record Retention	Requirements for Record Retention at the Credential Provider

Table 6 Description of the Concepts that define Credential Assurance in Tuple-Based Trust Schemes

The concepts that define **Credential Assurance** in Tuple-Based trust schemes further involve aggregating and generalizing concepts. Generalizing concepts include the **Ensured Issuance Process**, and the **Procedure to ensure activation through intended entity**. The **Ensured Issuance Process** can be specialized to the **Ensured Issuance Process using Receipts**, which involves in-person or secure channel delivery of a credential with receipt signature.

The **Procedure to ensure activation through intended entity** specializes to the **bound procedure to ensure activation through intended entity**, and the **bound procedure to ensure activation through intended entity with time limit**. The **bound procedure to ensure activation through intended entity** ensures that the Entity is bound to activation of credential (e.g. challenge-response protocol). The **bound procedure to ensure activation through intended entity with time limit** ensures that the entity is bound to activation of credential (e.g. challenge-response protocol) within a period of time.

Finally, **Credential Assurance** involves aggregating concepts, which are the **Credential Secure Storage**, **Credential Secure Renewal**, and **Record Retention**.

Record Retention consists of the **Record Maintenance by the CSP**, and the **Documentation of Chain of Custody of Records**. **Record Maintenance by the CSP** involves that the record of registration, etc. shall be maintained by the CSP. Duration of retention is specified in the CSP policy. The **Documentation of Chain of Custody of Records** requires that formalized, documented procedures shall be developed for the chain of custody for each record.

7.3.1.1 Credential Secure Storage

Credential Secure Storage involves **Access Control to administrators and applications requiring access only**, **Shared Secret Protection**, and the **Credential Secure Storage Requirements Policy**. **Access Control to administrators and applications requiring access only**, demands an exclusive access control. **Shared Secret protection** requires the shared secret to be stored adequately, e.g. not as plaintext. This can be further specialized towards **Shared secret protection by access control and encryption**, which demands that protection of shared secrets by access controls to administrators and applications that require access. Shared secrets shall be encrypted and the encryption key for the shared secret shall itself be encrypted and stored in a cryptographic module (hardware or software).

Finally, **Credential Secure Storage Requirements Policy** demands that entities acknowledge that they understand these requirements and agree to protect credentials in accordance with these requirements. This can be further specialized into the **Signed Credential Secure Storage**

Requirements Policy, where the entities sign a document acknowledging that they understand these requirements and agree to protect credentials in accordance with these requirements.

7.3.1.2 Credential Secure Renewal

Credential Secure Renewal includes **Suitable Policies for Credential Renewal**, **Possession Proof of Credential**, **CSP policy requirements for passwords**, **Permission of credential renewal**, **Interactions via protected channel**, and **Identity Proofing for Credential Secure Renewal**. **Suitable Policies for Credential Renewal** means the existence of policies for renewal and replacement of credentials. **Possession Proof of Credential** involves a Proof-of-possession of the unexpired current credential to the CSP before renewal. **CSP policy requirements for passwords** requires that Passwords shall meet minimum CSP policy requirements for password strength and re-use. **Permission of credential renewal** requires that after expiry of the current credential, renewal shall not be permitted. **Interactions via protected channel** mean that all interactions shall occur over a protected channel such as SSL/TLS. Finally, **Identity Proofing for Credential Secure Renewal** requires that identity proofing with adequate assurance is used prior to renewal of a credential (see Section 7.3.2).

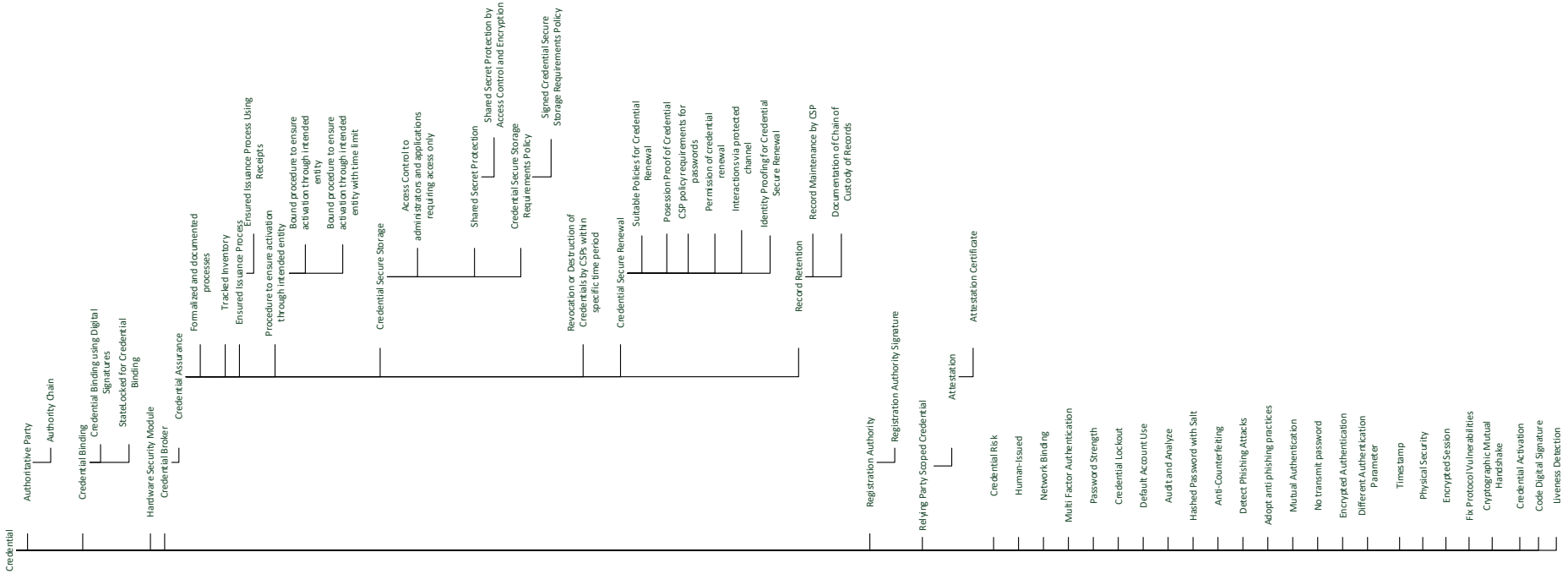

Figure 37 Overview on the Concepts of Credentials in Tuple-Based Trust Schemes

7.3.2 Identities in Tuple-Based Trust Schemes

An **Identity** in Tuple-Based Trust Schemes is described by the **Identity Validation**, the **Identity Verification**, and the **Identity Provider**. **Identity Validation** involves the confirmation of the accuracy of identity information. Although both **Identity Validation**, and **Identity Verification** are closely related to concepts included in the **Identity Provider**, they are both used in a more abstract sense (e.g. in PCTF, the Electronic Signature Law of the People's Republic of China, Minors Trust Framework, etc). In order to prevent the data model for Tuple-Based trust schemes to capture all the possible aspects of the abstract usage of these concepts, they are additionally included.

Identity Validation involves the confirmation of the accuracy of identity information, whereas **Identity Verification** ensures the linkage of identity information.

The **Identity Provider** is conceptualized by **Identity Assurance,** which is the assurance that an individual, organization, or device is who they claim to be. **Identity Assurance** is an aggregating concept, which consist of **Identity Proofing** and **Linkage of identity information to the individual**. **Identity proofing** validates the identifiers of an identity, whereas **Linkage of identity information to the individual** ensures that identity information, once confirmed as accurate, relates to the individual making the claim. Both are aggregating concepts. Their included concepts are further described in Table 7 and Table 8.

Concept	Description
Published Identity Proofing Policy	A published identity proofing policy, which must be adhered to, is always required. This is always part of the identity proofing process
Self-Claimed / Self-Asserted	An identifier may be self-claimed or self-asserted.
Policy Compliant Authoritative Document	The policy compliant authoritative document should be identity proofing policy compliant.
In-Person Proofed	In Person Proofing is foreseen for Person Entities
Not-In-Person Proofed	Not-In-Person Proofing is foreseen for Person Entities
Non-Person Entity	Non-Person Entities can be enrolled
Contact Information Verified	Contact Information has to be verified by a third party.
Personal Information Verified	Personal Information has to be verified by a third party.
Entity Secret Verified	Additional secrets of the entity have to be verified.
Verified Credential Claim	The claim of possession of a LoA3 Credential has to be verified.
Entity Information Recorded	Information on Non-Person Entities have to be recorded (e.g. MAC Adress, IP Adress, etc.).

Table 7 Description of the Concepts that define Identity Proofing in Tuple-Based Trust Schemes

Identity Proofing includes two aggregating concepts, which are the **Policy Compliant Authoritative Document**, and the **Non-Person Entity.** A **Non-Person Entity** involves **Trusted Hardware Usage**. A **Policy Compliant Authoritative Document** is further defined by the concepts of **Policy Compliant authoritative source information**, **Policy compliant**

authoritative source, **Policy compliant issuance**, **Validity**, and **Identity Information Verified.** The **Policy compliant authoritative source information** is any information from a policy compliant authoritative document of the entity that should be provided for identity proofing. The **Policy compliant authoritative source** provides the policy compliant authoritative document. **Policy compliant Issuance** ensures that the authoritative document is issued in compliance with the identity proofing policy. The **Validity** of the authoritative document should be provided. Finally, **Identity Information Verified** requires the identity information to be verified by a third party.

Concept	Description
Knowledge-based	A process that compares personal or private information (i.e., shared secrets) to establish an individual's identity. Examples of information that can be used for knowledge-based confirmation include passwords, personal identification numbers, hint questions, program-specific information and credit or financial information.
Biological or behavioural characteristic confirmation	A process that compares biological (anatomical and physiological) characteristics in order to establish a link to an individual (for example, facial photo comparison).
Trusted referee	A process that relies on a trusted referee to establish a link to an individual. The trusted referee is determined by program-specific criteria. Examples of trusted referee include guarantor, notary and certified agent.
Physical possession confirmation	A process that requires physical possession or presentation of evidence to establish an individual's identity.

Table 8 Description of the Concepts that define Linkage of identity information to the individual in Tuple-Based Trust Schemes

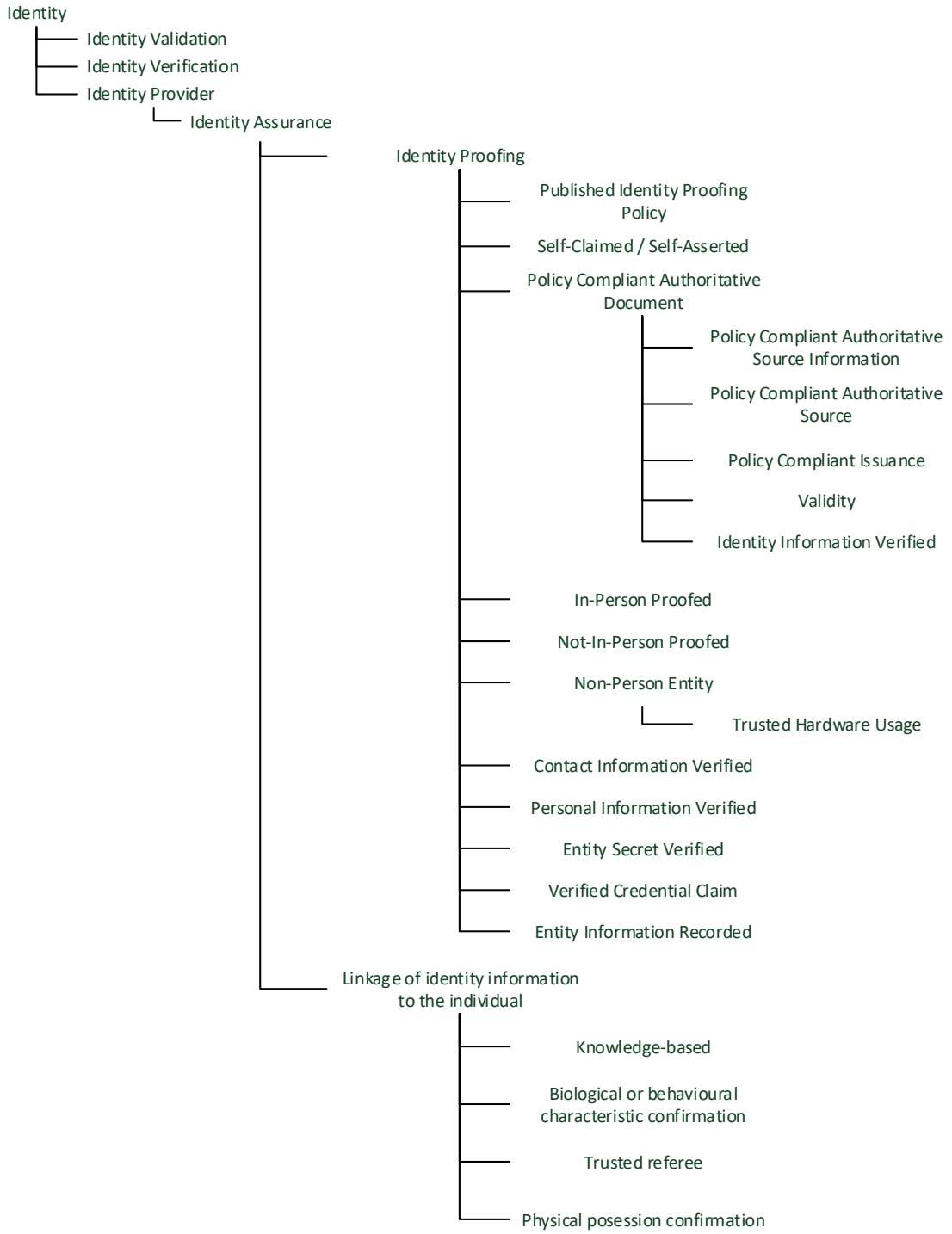

Figure 38 Overview on the Concepts that define Identities in Tuple-Based Trust Schemes

7.3.3 Attributes in Tuple-Based Trust Schemes

Figure 39 provides an overview on the concepts that define Attributes in Tuple-Based Trust Schemes. These concepts originate mainly from the STORK QAA/AQAA. The concept **Attribute Quality Level** further includes the concept **Linked to unique and verified STORK identifier**. This indicates, that attributes are linked to a unique and verified STORK identifier.

Descriptions of the remaining attributes are provided in Table 9.

Concept	Description
Attribute Assertion Quality Level	Quality rating for attribute assertion, being the result of using a STORK QAA (eIDAS) rated eID to access an attribute.
Attribute Quality Level	Level of quality rating for attributes, depending on two sub-criteria: (1) To what extent does the attribute provider ensure the accuracy of the attribute as such at the time of initial registration and (2) To what extent does the attribute provider ensure that the accuracy of the attribute as such is maintained/updated/verified after the initial registration.
Attribute Provider Quality	Quality rating expressing to what extent a service provider can rely on the attribute provider statements.
Authoritative Identity Source	In order to achieve a level 4 validation of the quality of an attribute, it is necessary (but not sufficient) that the attribute provider is the official (legally recognised as authentic/authoritative) identity source or identity database for the representation of companies within its country of establishment.
Link Validation Quality	Quality rating depending on two subcriteria: (1) To what extent does the AP ensure that the attribute information can be attributed to a uniquely identified person when the attributes are initially registered and (2) To what extent does the AP check that the attribute information can be attributed to a uniquely identified person during STORK 2.0 authentications.
Maintenance	Process to ensure that the attribute correctness is maintained over time after the initial registration.
Unrated Attribute Assertion	When a non-STORK eID is used for re-authentication, the attribute assertions must be provided without an AQAA rating for the attribute assertion.

Table 9 Description of the Concepts that define Attributes in Tuple-Based Trust Schemes

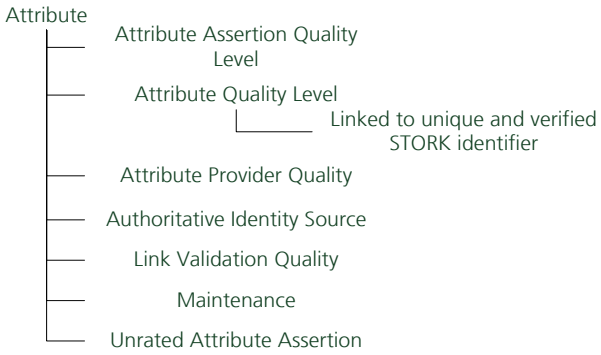

Figure 39 Overview on the Concepts that define Attributes in Tuple-Based Trust Schemes

7.4 Data Model for Tuple-Based Trust Schemes

Based on the concepts from Section 7.2.7 a data model for representing Tuple-Based trust schemes in the TSP can be provided. In order to retrieve the data model, the concepts that define Tuple-Based trust schemes were reviewed regarding their attribute domains. An attribute domain involves all possible values for an attribute. Hereby all concepts were initially considered as attributes.

The concepts were further refined, e.g. by further specialization of the concepts, until a limited attribute domain could be achieved. This however, left some attributes which do not involve a limited attribute domain[1]. Those attributes are in the following referred to as underspecified.

The following section presents the data models for Tuple-Based Trust Schemes, and discusses the steps taken to retrieve specified domains for attributes, where necessary.

7.4.1 Data Model for Credentials in Tuple-Based Trust Schemes

Figure 40 provides a UML representation of the Data Model for Credentials in Tuple-Based Trust Schemes. Most attributes of this data model can be described by using boolean values. However, the attribute **Time limit** of **Procedure to ensure activation through intended entity**, and the **Time Period** associated with **Revocation or Destruction of Credentials by CSPs within specific time period** are both positive integer values. These attributes provide refinements of the concepts **Bound procedure to ensure activation through intended time limit**, and **Revocation or Destruction of Credentials within time period**. While this refinement provides a fully specified boolean domain for **Revocation or Destruction of Credentials by CSPs within specific time period**, and **Bound procedure to ensure activation through intended entity with time limit**, it yields a large, yet ordered domain for **Time limit** and **Time**

[1] One such attribute refers to the use of a policy compliant authoritative document, to corroborate identity claims; the type of documents can have an arbitrarily high number values (e.g. eID, nPA, identity card, etc.).

period. This means for the processing in the ATV to use conditions on ordered sets, such as $<, >, \leq, \geq$ for the domain for **Time limit** and **Time period**.

An underspecification issue arises with **Authoritative Party** and **Credential Broker**, which is currently defined with an infinitely large domain. The reason for this is that for both, **Authoritative Party** and **Credential Broker**, the exact numbers are currently unknown and will vary over time. This may hinder automated processing by the ATV. Possible solutions for this issue can make use of white lists of accepted entities, which need a regular update, which might however cause a scalability issue. Another possibility could be string comparison and search for pre-defined and standardized strings for the specific trust scheme. Otherwise, the attributes can be extracted and provided as additional information to the automated decision of the ATV.

The remaining attributes use a boolean domain, and thus suffer no underspecification issues.

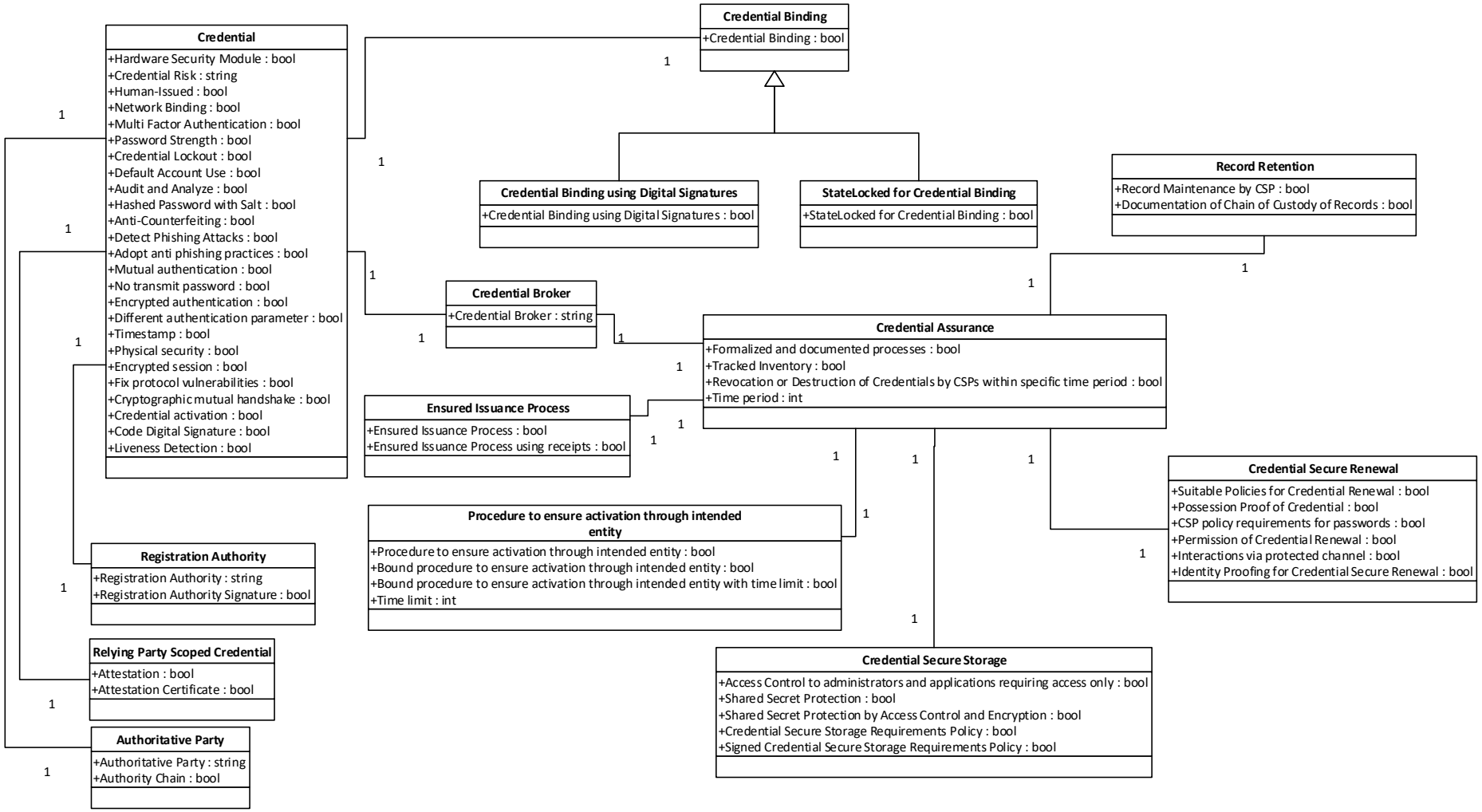

Figure 40 Overview on the Data Model for Credentials in Tuple-Based Trust Schemes

7.4.2 Data Model for Identities in Tuple-Based Trust Schemes

The Data Model for Identities in Tuple-Based Trust Schemes is shown in Figure 41. As in the Data Model for Credentials in Tuple-Based Trust Schemes, the concepts for describing identities can be mostly transformed into attributes with a boolean domain. This is however not possible for the attributes **Identity Validation**, and **Identity Verification** which are both underspecified concepts. Also for the attribute **Identity Provider** an underspecification issue arises due to the fact that the exact numbers is unknown and also varies over time. This may hinder automated processing by the ATV. Possible solutions for this issue are described in the previous Section 7.4.1. All Attributes involved in **Identity Proofing**, **Non-Person Entity**, and **Linkage of identity information to the individual** can be described by using attributes with a boolean domain. The same holds for the attributes involved in **Policy Compliant Authoritative Document**. These attributes mostly stem out of concepts from the PCTF, the Electronic Signature Law of the People's Republic of China, ISO/IEC 29115:2013, and Embedded UICC Remote Provisioning. In there, they are introduced as boolean concepts[2].

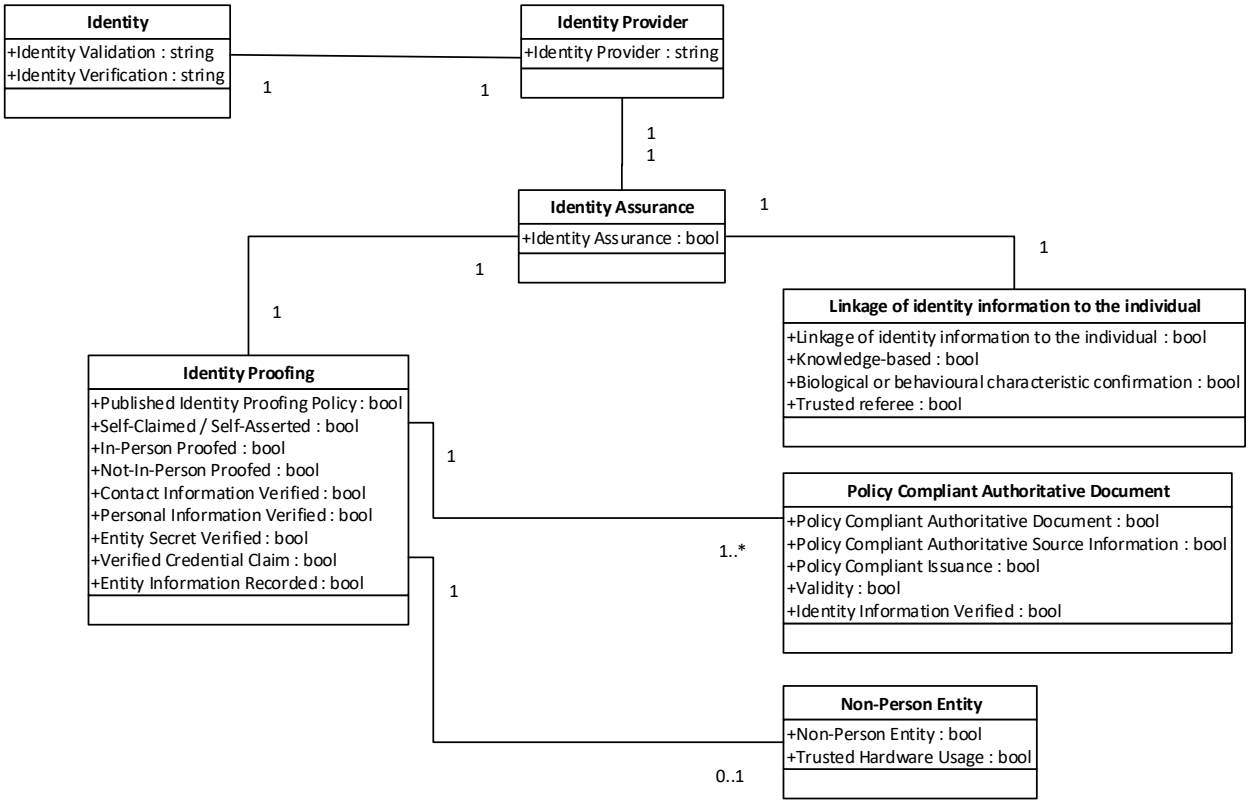

Figure 41 Overview on the Data Model for Identities in Tuple-Based Trust Schemes

[2] For instance, ISO/IEC 29115:2013 simply states that in higher level of assurances, the provision of one, or more policy compliant authoritative documents is required. This can be transformed into a boolean domain.

An identity can be described by multiple instances of **Policy Compliant Authoritative Document**. This is extracted from ISO/IEC 29115:2013, where the highest level of assurance requires the provision of an additional **Policy Compliant Authoritative Document**.

Finally, **Identity Proofing** for a **Non-Person Entity** may not be foreseen in some schemes and is therefore considered optional.

7.4.3 Data Model for Attributes in Tuple-Based Trust Schemes

The Data Model for Attributes in Tuple-Based Trust Schemes is shown in Figure 42. The attributes **Authoritative Identity Source**, **Maintenance**, and **Linked to unique and verified STROK identifier** all include a boolean domain, when transformed from their respective Concepts. Further specialization was not required. However, the attributes **Attribute Assertion Quality Level**, **Attribute Provider Quality**, **Link Validation Quality**, and **Attribute Quality Level** are underspecified as concepts, and thus each involve an underspecified domain which may be problematic for automated verification in the ATV (see also Section7.4.1 for more details).

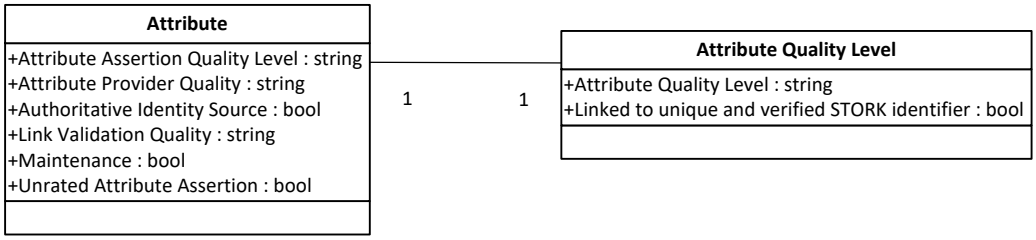

Figure 42 Overview on the Data Model for Attributes in Tuple-Based Trust Schemes

7.5 Publication of Tuple-Based Trust Schemes

Since any boolean/ordinal trust scheme can be expressed as a tuple-based trust scheme (see Table 1), the following paragraphs are applicable to *every* trust scheme in LIGHTest framework.

The publication of trust schemes is based on the ETSI standard TS 119 612 [1], used by eIDAS to represent trust lists [8].

For the publication of Tuple-Based Trust Schemes the two options suggested in D3.3 [4] should be possible: tuples as part of the signed trust list and tuples in an extra document to be reached with a pointer from the main document accessed by the TSPA.

Taking into account LIGHTest has to work with/within eIDAS regulation, there are good reasons not to extend that standard, but to use certain fields to cope with the list of tuples that characterizes a given trust scheme (boolean, ordinal or purely tuple-based).

A tuple is a pair of (attribute_name, attribute_value), where the name is fixed by the trust scheme itself, and the value could be as open as the trust scheme requires (boolean or integer values, open text, pre-defined strings, etc.).

There are in principle two different ways for the Publication of Tuple-Based Trust Schemes. First, the publication of the relevant attributes of the generic Unified Data Model for Credentials, Identities, and Attributes of the tuple-based trust scheme. The schema of an attribute with a *boolean* attribute value is as follows:

```
<!-- attributes of the Unified Data Model -->
<attributename>
   attributevalue
</attributename>
<!—example of an attribute of the Unified Data Model -->
<CredentialBindingUsingDigitalSignatures>
   true
</CredentialBindingUsingDigitalSignatures>
```

In section 7.5.2 the publication of tuple-based trust schemes using the Unified Data Model is demonstrated for the example of FIDO UAF Authenticators.

Second, the publication of a tuple-based trust scheme which trust levels are defined through a list of tuples (attribute_name, attribute_value). A given trust level in a trust scheme consists of a list of tuples (with at least one tuple, in case of the boolean/ordinal case, as it is shown below).

With that view of trust levels specified by tuples, LIGHTest implements an extra document containing all the trust levels: each trust level is specified by all the tuples with its attributes names and values related. This extra document, not included in the TS 119 612, follows the following schema:

```
<!-- definition of simple elements -->
<xs:element name="trustlevelname" type="xs:string"/> <!-- trustlevelname
TSPA -->
<xs:element  name="attributename"  type="xs:string"/>  <!--  attributename
TSPA -->
<xs:element name="attributevalue" type="xs:string"/> <!-- attributevalue
TSPA -->
<!-- definition of complex elements -->
<xs:element name="tuple">
 <xs:complexType>
  <xs:sequence>
    <xs:element ref="attributename" />
    <xs:element ref="attributevalue" />
   </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:element name="tuplelist">
```

```
 <xs:complexType>
  <xs:sequence>
    <xs:element ref="tuple" maxOccurs="unbounded"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>
<xs:element name="trustlevel">
 <xs:complexType>
  <xs:sequence>
    <xs:element ref="trustlevelname" />
    <xs:element ref="tuplelist" />
  </xs:sequence>
 </xs:complexType>
</xs:element>
```

Now a pointer from the signed trust list to this document is required, and it should be signed with the same key as the trust list. The field *<AdditionalServiceInformation>* which belongs to the service information extensions of ETSI TS119612 and it is used in the signed trust list to publish a URI identifying additional information, will contain the pointer to the tuple-based trust levels defined in the published trust scheme.

Any LIGHTest component will be able to process the tuple-based trust level list contained in that extra document, called the **tuple-based trust level doc** from now.

7.5.1 1.1.2 Example with trust levels

Following, some trust levels of the three kinds of trust schemes are to be expressed with the above XML schema for publishing trust levels in LIGHTest.

As a **boolean** trust scheme, we take the eTimestamp in the eIDAS regulation [8]. As it is defined there, such eTimestamp can be qualified or not.

```
<trustlevel trustlevelname="eIDASeTimestamp" >
<tuplelist>
      <tuple
            attributename="isQualified" attributevalue="true">
      </tuple>
</tuplelist>
</trustlevel>
```

In case of an **ordinal** trust scheme, we can select now the eIdentity in the ISO 29115 Standard [14]. As it is defined there, such trust levels for the eIdentity can be 1-Low,2-Medium,3-High, and 4-Very High (or LoA1, LoA2, LoA3, LoA4, respectively).

```
<trustlevel trustlevelname="ISO29115eIdentity" >
<tuplelist>
      <tuple
```

```
        attributename="LoA1234" attributevalue=”LoA1” | “LoA2” | “LoA3” |
"LoA4">
        </tuple>
</tuplelist>
</trustlevel>
```

The **tuple-based** trust scheme we chose is related to FIDO standards. FIDO UAF authenticators are described by a tuple-based trust scheme by means of these attributes, among others [35]:

- Authenticator Version
- Authenticator ID (AAID)
- Attestation Certificate
- User verification method such as fingerprint biometrics
- Whether keys are protected by Trusted Execution Environment (TEE) or Secure Element (SE)
- Whether biometrics are protected by TEE

For simplicity, the example (extracted from [35]) to be expressed as a tuple-based trust level doc consists of the following tuples:

- Fingerprint based user verification allowing up to 5 registered fingers, with false acceptance rate of 0.002% and rate limiting attempts for 30 seconds after 5 false trials.
- Authenticator is embedded with the FIDO User device.
- The authentication keys are protected by TEE and are restricted to sign valid FIDO sign assertions only.
- The (fingerprint) matcher is implemented in TEE.
- The Transaction Confirmation Display is implemented in a TEE.
- The Transaction Confirmation Display supports display of "image/png" objects only.
- Display has a width of 320 and a height of 480 pixels. A bit depth of 16 bits per pixel offering True Color (=Color Type 2).
- The zlib compression method (0). It doesn't support filtering (i.e. filter type of=0) and no interlacing support (interlace method=0).
- The Authenticator can act as first factor or as second factor, i.e. isSecondFactorOnly = false.
- It supports the "UAFV1TLV" assertion scheme.
- It uses the ALG_SIGN_SECP256R1_ECDSA_SHA256_RAW authentication algorithm.
- It uses the ALG_KEY_ECC_X962_RAW public key format (0x100=256 decimal).
- It only implements the TAG_ATTESTATION_BASIC_FULL method (0x3E07=15879 decimal).
- It implements UAF protocol version (upv) 1.0 and 1.1.

A sample of a trust level for a FIDO UAF authenticator is expressed following. Note, not all possible values of the tuples are expected from the TSPA, but only the ones for demonstrating

the option of a second document for the publication of tuple-based trust schemes are expressed here.

```
<trustlevel trustlevelname="FIDOUAFauthenticator_example">
   <tuplelist>
         <tuple
               attributename="UserVerification"
               attributevalue="Fingerprint based, up to 5 registered
fingers, false acceptance rate of 0.002%, rate limiting attempts for 30
seconds after 5 false trials">
         </tuple>
         <tuple
               attributename="AuthenticatorEmbeddedWithFIDOUserDevice"
               attributevalue="true">
         </tuple>
         <tuple
               attributename="AuthenticationKeysProtection"
               attributevalue="TEE">
         </tuple>
         <tuple
               attributename="FingerprintMatcher"
               attributevalue="TEE">
         </tuple>
         <tuple
               attributename="TransactionConfirmationDisplay"
               attributevalue="TEE">
         </tuple>
         <tuple
               attributename="TransactionConfirmationDisplayObject"
               attributevalue="image/png">
         </tuple>
         <tuple
               attributename="Width-HeightDisplay"
               attributevalue="320-480pixels">
         </tuple>
         <tuple
               attributename="CompressionMethod"
               attributevalue="zlib">
         </tuple>
         <tuple
               attributename="isSecondFactorOnly"
               attributevalue="false">
         </tuple>
         <tuple
               attributename="AssertionScheme"
               attributevalue="UAFV1TLV">
         </tuple>
         <tuple
```

```
                attributename="AuthenticationAlgorithm"
                attributevalue="ALG_SIGN_SECP256R1_ECDSA_SHA256_RAW">
            </tuple>
            <tuple
                attributename="PublicKeyFormat"
                attributevalue="ALG_KEY_ECC_X962_RAW">
            </tuple>
            <tuple
                attributename="MethodImplemented"
                attributevalue="TAG_ATTESTATION_BASIC_FULL">
            </tuple>
            <tuple
                attributename="UAFversion"
                attributevalue="1.0-1.1">
            </tuple>
    </tuplelist>
</trustlevel>
```

7.5.2 1.1.3 Example with Unified Data model

The same FIDO example with attributes is now included in the Unified Data model of Credentials-Identities-Attributes. This is shown in Table 10.

Table 10: FIDO UAF Authenticator in the Unified Data Model

Attribute	FIDO UAF Authenticator example
Credential	AuthenticatorEmbeddedWithFIDOUserDevice, UAFversion
Credential binding using digital signatures	AuthenticationKeysProtection, FingerprintMatcher
StateLocked for Credential binding	TransactionConfirmationDisplay, TransactionConfirmationDisplayObject, Width-HeightDisplay
Hardware Security Module	AuthenticationKeysProtection, FingerprintMatcher
Bound procedure to ensure activation through intended entity	AssertionScheme
Credential Secure Storage	CompressionMethod
Attestation	AssertionScheme
Attestation Certificate	AuthenticationAlgorithm, PublicKeyFormat
Multi Factor Authentication	isSecondFactorOnly
Mutual authentication	MethodImplemented
Cryptographic Mutual Handshake	MethodImplemented
Biological or behavioral characteristic confirmation	UserVerification

The FIDO UAF Authenticator comprises the attributes indicated in Table 10 of the Unified Data model. This set of tuples can be written in XML as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
…
<Attributes_FIDO_UAF_Authenticator>
<tuplelist>
  <Credential>
   true
   <CredentialBinding>
    <CredentialBindingUsingDigitalSignatures>
    true
    </CredentialBindingUsingDigitalSignatures>
    <StateLockedforCredentialBinding>
    true
    </StateLockedforCredentialBinding>
   </CredentialBinding>
   <HardwareSecurityModule>
   true
   </HardwareSecurityModule>
   <CredentialBroker>
    <CredentialAssurance>
     <BoundProcedureToEnsureActivationThroughIntendedEntity>
      true
      </BoundProcedureToEnsureActivationThroughIntendedEntity>
      <CredentialSecureStorage>
      true
      </CredentialSecureStorage>
    </CredentialAssurance>
   </CredentialBroker>
   <RelyingPartyScopedCredential>
     <Attestation>
     true
     </Attestation>
     <AttestationCertificate>
     true
     </AttestationCertificate>
   </RelyingPartyScopedCredential>
   <MultiFactorAuthentication>
   true
   </MultiFactorAuthentication>
   <MutualAuthentication>
   true
   </MutualAuthentication>
   <CryptographicMutualHandshake>
   true
   </CryptographicMutualHandshake>
```

```
  </Credential>
  <Identity>
   <LinkageOfIdentityInformationToTheIndividual>
      <BiologicalOrBehaviouralCharacteristicConfirmation>
      true
      </BiologicalOrBehaviouralCharacteristicConfirmation>
   </LinkageOfIdentityInformationToTheIndividual>
  </Identity>
<trustlevel_ID> "trustlevel name" </trustlevel_ID>
 </tuplelist>
</Attributes_FIDO_UAF_Authenticator>
```

In addition to the attributes of the FIDO UAF Authenticator as listed in Table 10, the attribute trust_level_ID is included. This is in particular required as link to the Trust Translation Authority (TTA), which publishes its Trust Translation Lists based on this name for this specific trust scheme. Hence, the attribute trust_level_ID should be added in every tuple based trust scheme publication of the Unified Data Model.

This XML code section can be either added to the signed trust list or stored in a signed extra document with in addition a pointer from the signed trust list to this document using the field <AdditionalServiceInformation> of ETSI TS119612. The corresponding entry in the trust list could look like this:

```
< AdditionalServiceInformation >
      <OtherInformation>
            <URI xml:lang="en"> http://example.com/lightest/TSPA/tuple-
            based-trust-schemes/UDM/fido-uaf.xml </URI>
      </OtherInformation>
</ AdditionalServiceInformation>
```

7.6 Modelling of Tuple-Based Trust Schemes

For a further validation and application of the unified data model, an additional trust scheme, which is not considered in the consolidation process for the publication of tuple-base trust schemes, is selected. It is the Trust Scheme for PEPPOL, which is described in Section 7.2.11 and which is used in the LIGHTest pilot demonstration “E-Procurement-Pilot”.

In accordance to the other selected trust schemes, the constructs were identified for the PEPPOL trust scheme, compiled to a vocabulary and consolidated towards the unified data model of trust scheme publication authorities (see Section 7.4).All identified constructs of the PEPPOL trust scheme can be represented by the unified data model. The corresponding constructs are shown in the following as the tuple based publication of the PEPPOL trust scheme in XML format.

```
<?xml version="1.1" encoding="UTF-8"?>
```

```
<AttributesPEPPOL>
<tuplelist>
<AuthoritativeParty>
string_with_name
</AuthoritativeParty>
<Credential>
 <CredentialBinding>
  <CredentialBindingUsingDigitalSignatures>
  true
  </CredentialBindingUsingDigitalSignatures>
 </CredentialBinding>
 <CredentialBroker>
   <CredentialAssurance>
    <EnsuredIssuanceProcess>
     <EnsuredIssuanceProcessUsingReceipts>
       true
       </EnsuredIssuanceProcessUsingReceipts>
      </EnsuredIssuanceProcess>
    <ProcedureToEnsureActivationThroughIntendedEntity>
      true
      </ProcedureToEnsureActivationThroughIntendedEntity>
      <CredentialSecureStorage>
      true
       <AccessControlToAdministratorsAndApplicationsRequiringAccessOnly>
      true

</AccessControlToAdministratorsAndApplicationsRequiringAccessOnly>
      </CredentialSecureStorage>
      <CredentialSecureRenewal>
       <SuitablePoliciesForCredentialRenewal>
       true
       </SuitablePoliciesForCredentialRenewal>
      </CredentialSecureRenewal>
   </CredentialAssurance>
  </CredentialBroker>
  <RegistrationAuthority>
  string_with_name
  </RegistrationAuthority>
  <MutualAuthentication>
  true
  </MutualAuthentication>
  <NoTransmitPassword>
  true
  </NoTransmitPassword>
  <EncryptedAuthentication>
  true
  </EncryptedAuthentication>
  <CryptographicMutualHandshake>
```

```
  true
  </CryptographicMutualHandshake>
 </Credential>
 <Identity>
  <IdentityValidation>
  string_confirming_accuracy_Id
  </IdentityValidation>
 </Identity>
<trustlevel_ID>
 "trustlevel name"
</trustlevel_ID>
</tuplelist>
</AttributesPEPPOL>
```

As described in Section 7.5, this XML code section can be either added to the signed trust list of PEPPOL or stored in a signed extra document with in addition a pointer from the signed trust list to this document using the field <AdditionalServiceInformation> of ETSI TS119612. The corresponding entry in the trust list could look like this:

```
< AdditionalServiceInformation >
      <OtherInformation>
            < URI xml:lang="en">
            http://example.com/lightest/TSPA/tuple-based-trust-
            schemes/UDM/peppol.xml
            </URI>
      </OtherInformation>
</ AdditionalServiceInformation>
```

8. Summary and Conclusion

This Deliverable outlines the Conceptual Framework for Trust Schemes in LIGHTest, which includes a Conceptualization of the Trust Scheme Publication Authority (TSPA), the representation of Boolean and Ordinal Trust Schemes, and the Representation of Tuple-Based Trust Schemes. While Boolean and Ordinal Trust Schemes can be represented in the form of signed Trust Lists, Tuple-Based Trust Schemes require a standardized data representation, which introduces standardized attributes with specified value domains. Therefore the Conceptual Framework for Trust Schemes further introduces a standardized data model based on the consolidation of four of the most important trust schemes in D3.1: ISO/IEC 29115:2013, STORK QAA/AQAA, the Electronic Signature Law of the People's Republic of China, and FIDO. Furthermore, STORK QAA/AQAA have been considered together with their usage within eIDAS. In D3.2, the following trust schemes were considered for further validation: The Turkey Electronic Signature Law, The Minors Trust Framework, The Trust Scheme of Azerbaijan, and the Embedded UICC Remote Provisioning Scheme.

These trust schemes were iteratively consolidated towards the data model for Tuple-Based Trust Schemes. Hereby, saturation of consolidation, in terms of newly introduced attributes was measured throughout the consolidation. In D3.1, indication of full saturation was not yet entirely achieved. However, in D3.2 with the five additional trust schemes it was achieved. This indicates, that the resulting data model is able to consider all existing trust schemes and also provides a good basis for future trust schemes.

The Concept for Trust Scheme Publications outlines the components of the TSPA, namely the DNS Name Server with DNSSEC extension and the Trust Scheme Provider. The results of D3.3 "DNS-based Publication of Trust Schemes", D3.4 "Discovery of Trust Scheme Publication Authorities", are incorporated in the concept, as well as considering the results of D2.7 "Relevant DNSSEC Concepts and Basic Building Blocks" which ensure good alignment with existing DNS practices.

The Concept along with the Data Model enables the discovery of the Trust Scheme Provider, provides verifiability of claimed associations with trust schemes, and provides the possibility to publish Boolean, Ordinal, and Tuple-Based Trust Scheme Publications. For the publication of Tuple-Based Trust Schemes, a standardized data representation for the tuples was developed which can be either added to the signed trust list or stored in an extra document with a pointer from the signed trust list to this extra document. Furthermore, the concept is well-aligned with the requirements of eIDAS, as representation of Trusted Lists is possible at the Trust Scheme Provider. This representation further enables the introduction of further information on Trust Scheme Association, such as the Trust Scheme Association History (historical information).

As for eIDAS, the existing and widely accepted standard for trust lists ETSI TS 119 612 [1] is used for the representation of Trust Lists in LIGHTest at the Trust Scheme Provider. Furthermore, it provides flexibility and scalability by its use of DNS Name Servers for Discovery

of the Trust List, which enables large-scale, global rollout of the Trust Scheme Publication Authorities.

In addition, the developed methodology in this Deliverable is used in a similar form for trust translations across trust domains (Work package 4). This enables translations of equivalent trust assessments across schemes for worldwide applications.

9. References

[1] ETSI TS 119 612, „Electronic Signatures and Infrastructures (ESI);Trusted Lists," European Telecommunications Standards Institute; Technical Specification, Sophia Antipolis Cedex, V2.1.1 (2015-07), 2015.

[2] The LIGHTest Project, D2.14 - Reference Architecture, Project Delivarable, 2017.

[3] The LIGHTest Project, D3.1 - Conceptual Framework for Trust Schemes (1), Project Deliverable, 2017.

[4] The LIGHTest Project, D3.3 - DNS-based Publication of Trust Schemes, Project Deliverable, 2018.

[5] The LIGHTest Project, D3.4: Discovery of Trust Scheme Publication Authorities, Project Deliverable, 2018.

[6] The LIGHTest Project, D2.7 -Relevant DNSSEC Concepts and Basic Building Blocks, Project Deliverable, 2017.

[7] P. Hoffmann, J. Schlyter, Using Secure DNS to Associate Certificates with Domain Names for S/MIME, RFC8162, Internet Engineering Task Force, May 2017.

[8] European Commission, „Eur-Lex: Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG. [Zugriff am 2017].

[9] European Commission, „Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electr," 2015. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0005. [Zugriff am 2018].

[10] DIACC Trust Framework Expert Committee, Pan-Canadian Trust Framework Overview - A collaborative approach to developing a Pan-Canadian Trust Framework, Digital ID and Authentication Council of Canada, 2016.

[11] DIACC, „Building Canada's digital identity future," Digital Identification and Authentication Council of Canada, , May 2015.

[12] Industry Canada, „Principles for Electronic Authentication - A Canadian Framework," Industry Canada, Ottawa, Ottawa, 2004.

[13] Government of Canada, „Standard on Identity and Credential Assurance," Government of Canada, Quebec, 2013.

[14] ISO/IEC, Information technology -- Security techniques -- Entity authentication assurance framework, Geneva, CH, 2013.

[15] European Commission, „eIDAS Observatory: Questions and Answers on rules applicable to Trust Services as of 1 July 2016," 2016. [Online]. Available: https://ec.europa.eu/futurium/en/content/questions-and-answers-rules-applicable-trust-services-1-july-2016. [Zugriff am 2017].

[16] European Commission, „Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for

assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the Eu," 2015. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002. [Zugriff am 2017].

[17] CAB Forum, „CA/Browser Forum," 2017. [Online]. Available: https://cabforum.org/. [Zugriff am 2017].

[18] STORK, „EU: STORK project Deliverable - D2.3 Quality authenticator scheme," 2009. [Online]. Available: https://joinup.ec.europa.eu/community/epractice/document/eu-stork-project-deliverable-quality-authenticator-scheme. [Zugriff am 2017].

[19] STORK2.0, „STORK 2.0: D3.2 Addendum. AQAA Guidelines," 2015. [Online]. Available: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=54:d32-addendum-aqaa-guidelines&Itemid=175. [Zugriff am 2017].

[20] CoSign, „The Ultimate Guide to Digital Signatures - Comprehensive Answers to the 20 most important questions," CoSign, Whitepaper, San Francisco.

[21] FIDO Alliance, „FIDO Alliance," 2016. [Online]. Available: https://fidoalliance.org/. [Zugriff am 05 10 2016].

[22] OIXnet, „OIXnet," 2018. [Online]. Available: http://www.oixnet.org/. [Zugriff am 17 July 2018].

[23] G. T. Alliance, 2017. [Online]. Available: http://oixnet.org/wp-content/uploads/2017/01/Minors-Trust-Framework-Document_01_20_17.pdf. [Zugriff am 16 July 2018].

[24] PRIVO, „PRIVO," 2018. [Online]. Available: https://www.privo.com/about-us. [Zugriff am 17 July 2018].

[25] The Law of the Republic of Azerbaijan, „Electronic signature and electronic document," Azerbaijan, March 9, 2004.

[26] „Normative acts for implementation of the law on electronic signature and electronic document," Cabinet of Ministers of the Republic of Azerbaijan, No. 27, January 28, 2006.

[27] „Application of the Law Electronic signature and electronic document," Presidential Decree, No.65, 26 May, 2004.

[28] GSMA, „Embedded SIM Remote Provisioning Architecture V 1.1," GSMA, 2014.

[29] GSMA, „Remote Provisioning Architecture for Embedded UICC - Technical Specification V 3.2," GSMA, 2017.

[30] Global Platform, „Card SPecifications V 2.2.1," 2011.

[31] PEPPOL eDelivery Network-An overview.

[32] PEPPOL Transport Infrastructure Technical Overview, 2011.

[33] 'E-Procurement: Requirements, Scenarios and Demo Data, 2018.

[34] PEPPOL Transport Infrastructure AS4 Profile, 2017.

[35] FIDO Alliance, „FIDO Metadata Statements," 02 02 2017. [Online]. Available: https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-metadata-statement-v1.1-id-20170202.html. [Zugriff am 2018].

10. Project Description

LIGHTest project to build a global trust infrastructure that enables electronic transactions in a wide variety of applications

An ever increasing number of transactions are conducted virtually over the Internet. How can you be sure that the person making the transaction is who they say they are? The EU-funded project LIGHTest addresses this issue by creating a global trust infrastructure. It will provide a solution that allows one to distinguish legitimate identities from frauds. This is key in being able to bring an efficiency of electronic transactions to a wide application field ranging from simple verification of electronic signatures, over eProcurement, eJustice, eHealth, and law enforcement, up to the verification of trust in sensors and devices in the Internet of Things.

Traditionally, we often knew our business partners personally, which meant that impersonation and fraud were uncommon. Whether regarding the single European market place or on a Global scale, there is an increasing amount of electronic transactions that are becoming a part of peoples everyday lives, where decisions on establishing who is on the other end of the transaction is important. Clearly, it is necessary to have assistance from authorities to certify trustworthy electronic identities. This has already been done. For example, the EC and Member States have legally binding electronic signatures. But how can we query such authorities in a secure manner? With the current lack of a worldwide standard for publishing and querying trust information, this would be a prohibitively complex leading to verifiers having to deal with a high number of formats and protocols.

The EU-funded LIGHTest project attempts to solve this problem by building a global trust infrastructure where arbitrary authorities can publish their trust information. Setting up a global infrastructure is an ambitious objective; however, given the already existing infrastructure, organization, governance and security standards of the Internet Domain Name System, it is with confidence that this is possible. The EC and Member States can use this to publish lists of qualified trust services, as business registrars and authorities can in health, law enforcement and justice. In the private sector, this can be used to establish trust in inter-banking, international trade, shipping, business reputation and credit rating. Companies, administrations, and citizens can then use LIGHTest open source software to easily query this trust information to verify trust in simple signed documents or multi-faceted complex transactions.

The three-year LIGHTest project starts on September 1st and has an estimated cost of almost 9 Million Euros. It is partially funded by the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321. The LIGHTest consortium consists of 14 partners from 9 European countries and is coordinated by Fraunhofer-Gesellschaft. To reach out beyond Europe, LIGHTest attempts to build up a global community based on international standards and open source software.

The partners are ATOS (ES), Time Lex (BE), Technische Universität Graz (AU), EEMA (BE), G+D (DE), Danmarks tekniske Universitet (DK), TUBITAK (TR), Universität Stuttgart (DE), Open Identity Exchange (GB), NLNet Labs (NL), CORREOS (ES), IBM Danmark (DK) and Ubisecure (FI). The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.