H. Roßnagel et. al. (Eds.): Open Identity Summit 2019,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019 131

Unified Data Model for Tuple-Based Trust Scheme Publication

Sven Wagner[1], Sebastian Kurowski[2], Heiko Roßnagel[2]

Abstract: Trust schemes are widely used by authorities to support verifiers of electronic transactions to determine the trustworthiness of relying parties. With a tuple-based publication, in addition to the trust scheme membership, the requirements of the trust scheme are published. For this, the development and publication of a unified data model derived from existing trust schemes (e.g. eIDAS) is needed, where each requirement is explicitly represented by one tuple. The consolidation and development of this data model, which is based on nine existing trust schemes, is presented along with possible applications and added value (e.g. improved mapping of trust schemes) in the field of trust verification. The data model includes the three abstract concepts Credential, Identity, and Attributes and in total 98 concepts, which can be added to standard trust lists using ETSI TS 119 612.

Keywords: trust infrastructure, trust scheme, trust scheme publication, electronic transaction, trust management, identity management, eIDAS.

1 Introduction and Motivation

In a very wide range of electronic transactions trust services are involved and it is often required to determine the trustworthiness of these trust services. For example, this applies to electronic signatures and timestamps, e-seals, website authentication, e-registered delivery services, or authentication with eIDs. Often, the validation of the trustworthiness of electronic transactions touches a multitude of trust aspects as well as validation across borders and jurisdictions. To determine the trustworthiness of relying parties in electronic transactions, the verifier should know all business partners involved in this process, which in reality is often not the case. Authorities can assist here by certifying the trustworthiness of the electronic identities of the involved parties. For this purpose, authorities operate trust schemes, where the organizational, regulatory, legal, and technical measures to assert trust-relevant attributes about enrolled entities are defined. Furthermore, authorities publish lists of all enrolled entities in this trust scheme in so-called trust lists or trust service status lists.

The process of querying these trust schemes can be however quite cumbersome for

[1] University of Stuttgart, Institute of Human Factors and Technology Management, Allmandring 35, 70569 Stuttgart, {firstname.name}@iat.uni-stuttgart.de
[2] Fraunhofer IAO, Fraunhofer Institute of Industrial Engineering IAO, Nobelstr. 12, 70569 Stuttgart, {firstname.name}@iao.fraunhofer.de

verifiers due to the diversity of applications and systems and due to the lack of a uniform, global standard for trust lists. To ease this challenge for verifiers of electronic transactions, the EU LIGHTest project (https://www.lightest.eu/) develops a lightweight, global trust infrastructure, which enables automatic validation of trust based on the individual, predefined trust policy of the verifier. For this purpose, LIGHTest makes use of the internet Domain Name System DNS with its existing global infrastructure, organization, governance and security standards. This infrastructure enables then both the publishing of trust information and the query of requested trust information, e.g. for the verification of a signed document in the simplest case.

This paper is built on [BL16], which provides an introduction into the LIGHTest project, and [Wa17], where the LIGHTest reference architecture and the Trust Scheme Publication Authority (TSPA), which enables the discovery and verification of trust scheme memberships is introduced. The TSPA hereby consists of a DNS Name Server with DNSSEC extension, and trust scheme providers, which provide the trust lists. The latter can be implemented as regular HTTPS components.

For the publication of trust schemes within LIGHTest, three different types are defined: boolean trust scheme publications indicate the entities that comply with the requirements of the trust scheme. Ordinal trust scheme publications indicate the entities that comply with the requirements of an ordinal aspect; typically, this is a Level of Assurance (LoA), of the trust scheme. Tuple-based trust scheme publications indicate the tuples of a boolean or ordinal trust scheme publication, which contain information on the requirements of the trust scheme as a list of data pairs of (attribute_name, attribute_value). Depending on the considered trust scheme the requirements vary, e.g. for identity proofing. Furthermore, when comparing the requirements between trust schemes, they may be synonymous or homonymous. Therefore, a consolidation process using existing national, international and industry trust schemes is required, which then enables the development of a unified data model for tuple-based trust scheme publications, where each requirement is explicitly represented by only one data pair of (attribute_name, attribute_value). This means that the requirements of existing trust schemes can be represented with this single, unified data model which then enables e.g easier comparison and mapping between trust schemes as well as automated processing of trust verification.

The development of the data model for tuple-based trust scheme publication is the topic of this paper, which is structured as follows. Related work is presented in Chapter 2. The methodology and modelling approach is described in Chapter 3. The selected trust schemes are shortly introduced in Chapter 4. The results of the required steps for the development of the data model are presented in Chapter 5. In Chapter 6, we conclude our findings and provide a summary.

2 Related Work

For the publication that an entity operates under the trust scheme there is an existing and widely accepted standard for trust lists, which is ETSI TS 119 612 [ET15]. This standard 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".

Trust service status lists as defined in ETSI TS 119 612 provide the basis for many trust lists, e.g. the trust lists in the eIDAS regulation, 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" [EI14]. The eIDAS regulation requires LoA mapping of the characteristics of the existing national trust schemes of the EC Member States, e.g. for the German eID scheme to the eIDAS LoAs [FO2017]. There are a few further examples on one-to-one mapping of two trust schemes. On a global level, OIXnet lists worldwide available trust frameworks and registered whitelists and functions as an official, centralized source of documents and information [Se2017].

ETSI TS 119 612 and the eIDAS regulation are both considered in the TSPA of the LIGHTest infrastructure, supporting the application of eIDAS. As the eIDAS regulation is limited to trust services provided to the public, the LIGHTest infrastructure enables also applications beyond the eIDAS framework, e.g. for trust schemes from industry consortia and beyond Europe. Hence, the LIGHTest infrastructure for the verification of trust is conceptually comparable to OCSP for querying the status of individual certificates.

3 Methodology

In order to enable the representation of multiple trust schemes in the data model, a bottom-up modelling approach for the identification of relevant requirements and constructs was followed. This includes two major steps:

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.

Second, each vocabulary was consolidated towards a unified data model of trust scheme publication. The consolidation process is shown in Fig. 1. Each scheme is represented by Sn (n is an arbitrary number). Due to the left-sidedness of this approach, complexity of the consolidation remains feasible. In addition, saturation of the consolidation can be observed. If, for instance no new concepts are added by Scheme S4 to the consolidated Scheme S1,2,3,4 this can be an indicator of saturation of the included constructs.

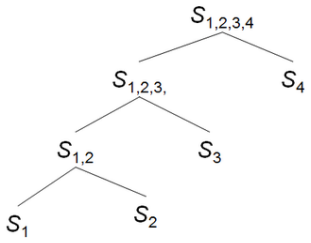

Fig. 1: Consolidation approach of the data model derived from 4 trust schemes

The identified constructs from the consolidation process are then used as input for the development of the data model. This requires three further steps: First, the identified constructs are hierarchically structured to determine high-level abstract concepts. Each of these high-level concepts contains again lists of concepts involved. Second, each concept is transferred into a tuple. Third, the set of tuples that define the tuple-based publication of trust schemes is published as a sequence of attributes in XML and either added to the trust list or published in an extra document with a corresponding pointer.

4 Selected Trust Schemes

To provide the most complete picture of existing trust schemes, national trust schemes from Europe and nations east- and westwards of Europe, international trust schemes, and trust schemes from industry consortiums were selected. These are the following nine schemes: ISO/IEC 29115:2013, the Pan Canadian Trust Framework, FIDO, STORK QAA/AQAA and eIDAS, the Chinese Electronic Signature Law, the Turkey Electronic Signature Law, the Minors Trust Framework, the Trust Scheme of Azerbaijan, and the Embedded UICC Remote Provisioning Scheme. These trust schemes are shortly introduced in the following. For further details we refer to the given references.

The ISO/IEC 29115 standard [IS13] provides an Entity Authentication Assurance Framework (EAAF), which considers three technical phases (enrolment, credential management, entity authentication) plus management and organizational aspects. Actors in the EAAF are entities, credential service providers, registration authorities, relying parties, verifiers, and trusted third parties. The degree of confidence in the entity authentication process is determined by four levels of assurance (LoAs): little, some, high, and very high confidence.

The Pan-Canadian Trust Framework (PCTF) [DI16] aims to enable the Canadian digital identity ecosystem by defining a set of business, technical, and legal rules for the processes identification, authentication, and authorization. It was released by the Digital ID and Authentication Council of Canada (DIACC) in 2016. It contains a Federated

Authentication and Brokered Authorization Model, which has three major service components: credential services, permission services and identity services.

The Fast Identity Online (FIDO) [FI16] alliance is an industry specification group (more than 250 members currently) that aims to define an interoperable specification for mobile authentication to overcome existing fragmentation and silos. 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 STORK QAA/AQAA [ST15] and eIDAS [EI14] are considered together in this context: the large scale pilot STORK, which initiated interoperable cross-border eID which then fed into the eID trust model integrated in eIDAS. The eIDAS regulation was introduced in Chapter 2. It contains several trust services, including electronic signatures, seals, timestamps, registered delivery and website authentication as well as corresponding levels of trust (LoAs).

The Chinese Electronic Signature Law (started in 2005) is a functional law, which regulates electronic signatures and ensures their legally binding. Electronic data are transmitted if the transfer has been authorized by the sender, the receiver verifies receipt, and the electronic signature is verified by a third party.

Turkey's electronic signature law from 2004 is modelled on a combination of the EU Directive on Electronic Signatures and ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats" [ET03]. It compromises electronic signature, mobile signature and timestamp services used in Turkey electronic services.

The Minors Trust Framework [OI18] is an online identity trust model, developed in conjunction with the National Strategy for Trusted Identities in Cyberspace (NSTIC). It consists of a complete set of business (operational), legal and technical policies, which enable Credential Service Providers that issue a child-unique pseudonymous identifier to interoperate and interact with relying parties and other members.

The Trust Scheme of Azerbaijan is based on the law governing digital signatures from 2004 [RA04], which complies with the European Union Directive 1999/93/EC on digital signatures and which is currently updated to be compliant with the eIDAS regulation. In accordance with the Law of the Republic of Azerbaijan, digital signatures created with a qualified certificate have the same legal value as handwritten signatures.

The embedded UICC (Universal Integrated Circuit Card) Remote Provisioning [GS14], which was developed by the GSMA, allows performing remote management of an embedded UICC, which can have a SIM functionality but also other applications (e.g. a payment or eID application). The corresponding PKI-based trust scheme is required to ensure controlled access and mutual authentication of the involved entities.

5 Data Model development

5.1 Consolidation steps

As mentioned in Section 4, nine trust schemes were selected for the retrieval of the tuple-based data model for trust schemes. The different consolidation steps as well as the saturation level of the consolidation are summarized in Tab. 1.

Input Scheme 1	Input Scheme 2	Output Scheme	Saturation ΔS
ISO/IEC29115	PCTF		nA
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 eSig Law	Data Model v 0.6	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	0

Tab. 1: Overview on consolidation steps

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 FIDO. Further consolidation of the STORK QAA/AQAA levels involved 9 concepts due to the introduction of the concept of attributes. The consolidation with the Turkey Electronic Signature Law resulted in an additional concept Authority Chain for verification of Authoritative Party. With the Minors Trust Framework, the Identity Provider, which is comparable to the Credential Broker for credentials is added as additional concept.

Overall, the conducted consolidation approach for the development of the unified data model shows, that saturation could be achieved. The number of new constructs decreased rapidly. With the last five trust schemes only two new constructs were identified, and the Trust Schemes of Azerbaijan and UICC can be completely represented by the constructs of the data model. Hence, the selection of in total nine different national and international, governmental and industrial trust schemes indicates, that the resulting data model should be able to consider all constructs of existing trust schemes and also provides a good basis for future trust schemes.

5.2 Conceptualization of Data Model

For the conceptualization of the data model, the identified constructs from the consolidation process (see Section 5.1) are used and hierarchically structured. The consolidation resulted in three abstract concepts which are required for the description of trust schemes: Credential, Identity, and Attributes. The latter involves attributes which

are not used for authentication, and which are included mainly for compliance with STORK QAA/AQAA. Each of the three abstract concepts contains again lists of concepts involved.

In total, 98 concepts were identified: 62 for Credentials, 27 for Identities, and 9 for Attributes. The complete list of concepts is presented in the UML diagrams in Section 5.3. In general, concepts can be classified as aggregated, generalized, or abstract ones. Aggregating and generalizing concepts are hereby defined as concepts, which can be further specified and which aggregate or generalize these specified concepts. As one example, the hierarchical structure for the concept In-Person Proofed in the concept for Identity is as follows: for the description of an Identity in tuple-based trust schemes the concept Identity Provider is used. The Identity Provider is conceptualized by Identity Assurance, which is an aggregating concept and which consists of Identity Proofing and linkage of identity information to the individual. Both are aggregating concepts and the concept of Identity Proofing includes among other things the concept of In-Person Proofed.

5.3 Data Model for Tuple-Based Trust Schemes

Based on the conceptualization of the data model (see Section 5.2), a data model for representing tuple-based trust schemes is developed. This requires an additional step: each concept that define tuple-based trust schemes is transferred into an attribute and corresponding value, the attribute domain. Thus, each concept can be described as a tuple, the pair of (attribute_name, attribute_value). The attribute value could be as open as the attribute name requires (e.g. boolean or integer values, open text, pre-defined strings). However, a limited attribute domain has some major advantages in the processing and utilization of published tuple-based trust schemes. For example, if the tuples are used in the process of automated trust verification as it is foreseen by the Automatic Trust Verifier (ATV) in the LIGHTest project. Therefore, some concepts were further refined, e.g. by further specialization of the concepts, to achieve as many as possible attributes with a limited attribute domain. A few attributes however do not involve a limited attribute domain and they are referred to as underspecified in the following. One example for underspecified attributes is Authoritative Party, which is defined with an infinitely large domain, due to the fact that the exact numbers are currently unknown and will vary over time. Possible solutions for this issue can make use of regularly updated white lists of accepted entities or string comparison and search for pre-defined and standardized strings. Otherwise, the attributes can be extracted and used as additional information to the trust verification.

As described in Section 5.2, the consolidation resulted in the three abstract concepts Credential, Identity, and Attributes. A UML representation for each of the abstract concepts of the data model is presented in the following.

Fig. 2 shows the corresponding data model for Credentials in tuple-based trust schemes. Most attributes (57 out of 62) of this data model can be described by using

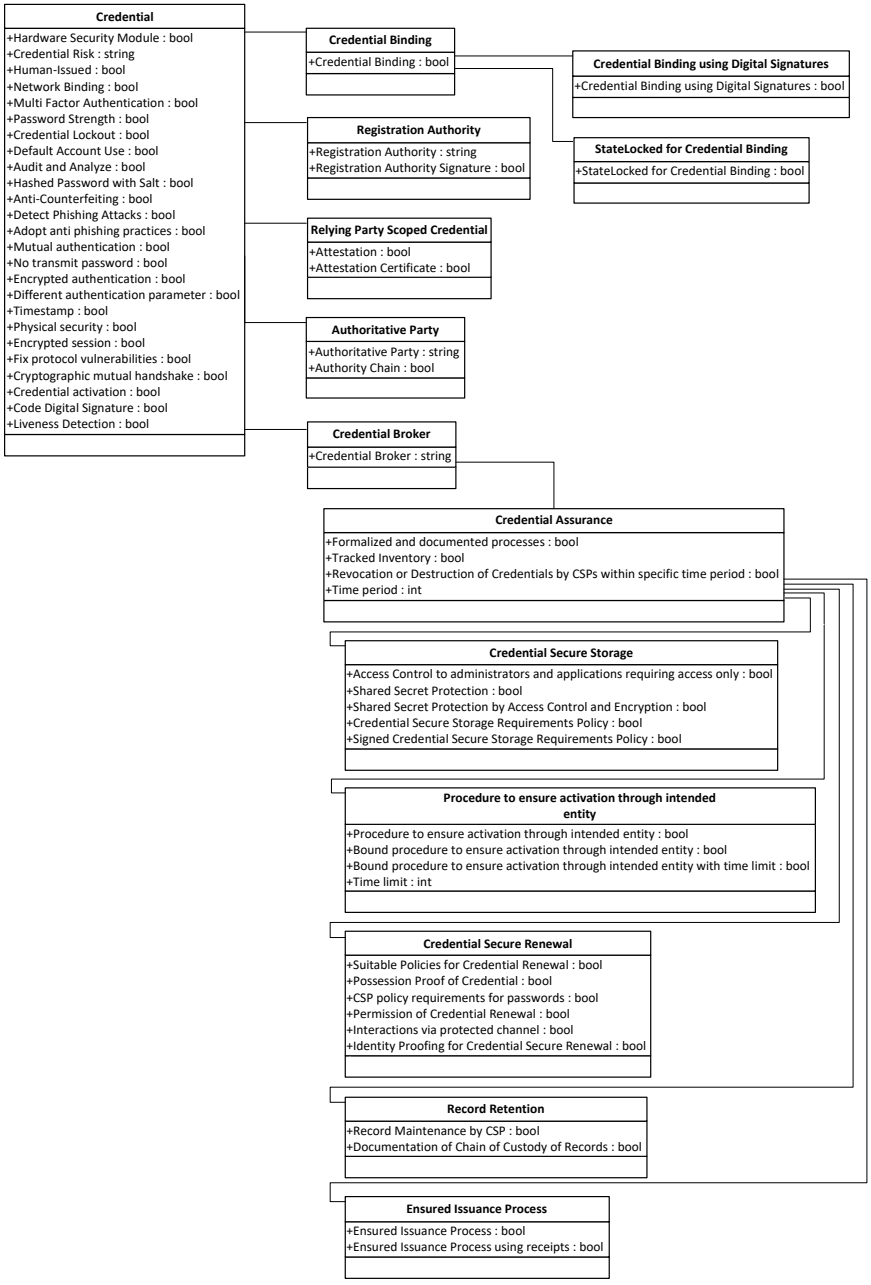

Fig. 2: Tuple-based Trust Schemes: Overview Data Model for Credentials (DIN A3 version available under: https://www.lightest.eu/static/deliverables/D3.2.pdf)

boolean values. These true false statements can be easily used in the process of automated trust verification. Two attributes defining time constraints, Time Limit for the 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 positive integer values. This means for the processing to use conditions on ordered sets, such as $<$, $>$, $\leq$, $\geq$ for these attribute domains. The underspecified attributes Authoritative Party (see above), Credential Broker, and Credential Risk are defined with infinitely large domains as strings for the attribute domain.

The data model for Identities in tuple-based trust schemes is shown in Fig. 3. Similar to the data model for Credentials, the concepts for describing identities can be mostly transformed into attributes with a boolean attribute domain. However, there are also three underspecified attributes, Identity Validation, Identity Verification, and Identity Provider. These attributes are defined as strings for the attribute domain accordingly, and the same solutions for this issue regarding automated processing can be applied as described above. All other 24 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.

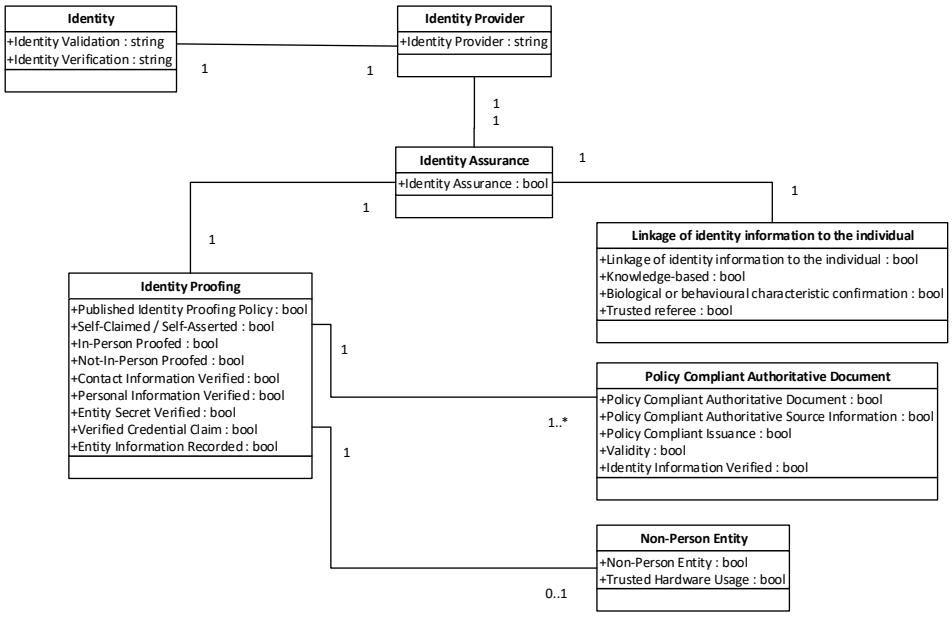

Fig. 3: Tuple-based Trust Schemes: Overview Data Model for Identities

The data model for Attributes in tuple-based trust schemes is shown in Figure 4. Attributes with a boolean domain are Authoritative Identity Source, Maintenance, Unrated Attribute Assertion, and Linked to unique and verified STORK identifier. The

attributes Attribute Assertion Quality Level, Attribute Provider Quality, Link Validation Quality, and Attribute Quality Level involve an underspecified domain which may again be problematic for automated verification.

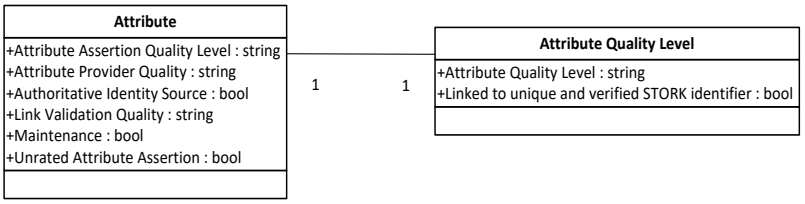

Fig. 4: Tuple-based Trust Schemes: Overview Data Model for Attributes

5.4 Publication of Tuple-Based Trust Schemes

For the publication of trust lists, there is a widely accepted standard, ETSI TS 119 612 [ET15] (see also Chapter 2). The so-called trust service status lists provide among other things "whether a trust service is or was operating under the approval of any recognized scheme" using the tag <TrustServiceProvider>. If in addition the requirements of the trust scheme are requested, the tuples with the attribute name and attribute value needs to be published. The principle for the publication of tuple-based trust schemes is similar to the publication of trust scheme memberships. In general there are two possibilities. First, the signed trust list using ETSI TS 119 612 needs to be extended by the tuples, i.e. the tuples are added in the XML file of the trust list. Second, an extra document, which lists all the tuples is created. In addition, this requires a pointer from the signed trust list to this document, which also should be signed with the same key as the trust list. For the pointer, the field <*AdditionalServiceInformation*> of ETSI TS119 612 can be used in the signed trust list to publish a URI identifying additional information.

The basis for this tuple-based publication is the data model (see Section 5.3). The set of corresponding tuples for a specific trust scheme can be written as a sequence of attributes in XML. The schema of a single attribute is as follows:

```
<!-- attributes of the data model -->
    <attributename>
          attributevalue
    </attributename>
```

For example for the attribute CredentialBindingUsingDigitalSignatures with a boolean attribute value the code is:

```
    <CredentialBindingUsingDigitalSignatures>
          true
    </CredentialBindingUsingDigitalSignatures>
```

Hence, the publication of tuple-based trust schemes contains a list of all tuples of the specific trust scheme using the defined schema from above. This XML code section can be either added to the signed trust list or stored in a signed extra document with the additional pointer from the signed trust list to this document.

6 Summary and Conclusions

With the global trust infrastructure developed in the LIGHTest project, arbitrary authorities can publish their trust information. If in addition to the trust scheme membership, information on the requirements of the trust scheme are relevant, a tuple-based trust scheme publication is required, where each requirement is presented by a tuple, a data pair of (attribute_name, attribute_value).

The publication of tuple-based trust schemes requires the development of a unified data model, where each requirement is explicitly represented by only one data pair. For this purpose, a consolidation process comparing nine existing national, international and industry trust schemes is conducted and saturation could be achieved. The next step, the conceptualization of the data model resulted in the three abstract concepts Credential, Identity, and Attributes and in total 98 concepts for the description of requirements in trust schemes. For each of the concepts the domain of possible values (e.g. Boolean value) was defined. For the publication of the tuple-based trust schemes, the defined tuples are written in XML and either added to the signed trust list using ETSI TS 119612 or stored in an extra document with a corresponding pointer.

To conclude, the presented methodology to publish tuple-based trust schemes based on the developed unified data model extends the data basis for verifiers of electronic transactions. In addition to the query and verification of the trust scheme membership, the defined requirements of the trust scheme can be considered in the verification process. Furthermore, the representation of the requirements of existing trust schemes in this single, unified data model enables easier comparison and mapping between trust schemes and automated processing of trust verification.

Acknowledgments

This research is supported financially by the LIGHTest (Lightweight Infrastructure for Global Heterogeneous Trust Management in support of an open Ecosystem of Stakeholders and Trust schemes) project, which is partially funded by the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321. We acknowledge the work and contributions of the LIGHTest project partners

Bibliography

[BL16] Bruegger, B. P.; Lipp, P.: LIGHT^{est} – A Lightweight Infrastructure for Global Heterogeneous Trust Management. In: Hühnlein D. et al (Hg.): Open Identity Summit 2016, Rome: GI-Edition, Lecture Notes in Informatics. p. 15-26.

[DI16] 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.

[FI16] FIDO Alliance, 2016; https://fidoalliance.org.

[FO17] Federal Office for Information Security: German eID based on Extended Access Control v2, 2017; https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_LoA_Mapping.pdf

[EI14] European Parliament, 'Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC', European Parliament, Brussels, Belgium, Regulation 910/2014, 2014.

[ET03] ETSI: Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats. Sophia Antipolis Cedex, France, Technical Specification ETSI TS 101 733 V1.5.1, 2003.

[ET15] ETSI: Electronic Signatures and Infrastructures (ESI); Trusted Lists. Sophia Antipolis Cedex, France, Technical Specification ETSI TS 119 612 V2.1.1, 2015; https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.01.01_60/ts_119612v020101p.pdf.

[GS14] GSMA: Embedded SIM Remote Provisioning Architecture V 1.1. GSMA, 2014.

[IS13] ISO/IEC 29115:2013: Information technology - Security techniques - Entity authentication assurance framework. ISO/IEC, Geneva, CH, 2013.

[Se17] Sellung, R.; Leszcz, M.; Parks, M.; Dawes, S.: A Global Inventory of Trust Lists, Trust Schemes and Trust Frameworks. In: OIX White Paper The Trust Framework Series, 2017.

[OI18] OIXnet: Minors Trust Framework, 2018; https://www.oixnet.org/registry/minors-trust-framework/.

[ST15] STORK2.0: STORK 2.0: D3.2 Addendum. AQAA Guidelines; 2015; https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=54:d32-addendum-aqaa-guidelines&Itemid=175.

[RA0418] The Law of the Republic of Azerbaijan: Electronic signature and electronic document. Azerbaijan, March 9, 2004.

[Wa17] Wagner, S.; Kurowski S; Laufs, U., Rossnagel, H.: A Mechanism for Discovery and Verification of Trust Scheme Memberships: The Lightest Reference Architecture. In: Fritsch L. et al (Hg.): Open Identity Summit 2017, Karlstad: GI-Edition, Lecture Notes in Informatics. p. 81-92.