12

The LIGHTest Project: Overview, Reference Architecture and Trust Scheme Publication Authority

Heiko Roßnagel[1] and Sven Wagner[2]

[1]Fraunhofer IAO, Fraunhofer Institute of Industrial Engineering IAO, Nobelstr. 12, 70569 Stuttgart, Germany
[2]University Stuttgart, Institute of Human Factors and Technology Management, Allmandring 35, 70569 Stuttgart, Germany
E-mail: heiko.roßnagel@iao.fraunhofer.de; sven.wagner@iat.uni-stuttgart.de

There is an increasing amount of electronic transactions in business and peoples everyday lives. To know who is on the other end of the transaction, it is often necessary to have assistance from authorities to certify trustworthy electronic identities. The EU-funded LIGHTest project assists here, by building a global trust infrastructure using DNS, where arbitrary authorities can publish their trust information. This enables then an automatic verification process of electronic transactions. This paper gives an overview on the project, its reference architecture with its main components and its application fields.

12.1 Introduction

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 has started on September 1st, 2016 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), Giesecke + Devrient (DE), Danmarks Tekniske Universitet (DK), TUBITAK (TR), Universität Stuttgart (DE), Open Identity Exchange (GB), NLNet Labs (NL), CORREOS (ES), University of Piraeus (GR), and Ubisecure (FI).

This paper provides on overview on the LIGHTest project, its reference architecture with its main components and its application fields. This overview is based on already published and accepted papers within this project. Due to the complexity and the wide-range of the project not all topics and work packages can be integrated in this paper. For more details, we refer to the LIGHTest project web site https://www.lightest.eu/.

This paper is structured as follows. Section 12.1 introduces related work. In Section 12.1 an overview of the LIGHTest reference architecture and usage scenarios examples are presented. The concept and role of the Trust Scheme Publication Authority (TSPA) is described in more detail in Section 12.1, by way of example for the components of the LIGHTest reference architecture. The TSPA is one of the key components of the LIGHTest reference architecture, which is used in every verification process. In Section 12.1, the Trust Police Language (TPL) and the Policy Authoring and Visualization Tools used in LIGHTest are introduced. A short discussion and outlook is given in Section 12.1 and a summary is provided in Section 12.1.

For further details, we refer to the following publications: [1] provided a first introduction into the LIGHTest project. In [2] the LIGHTest reference architecture and the Trust Scheme Publication Authority (TSPA) are presented. [3] proposes a delegation scheme that provides a general representation of delegations that can be extended to different domains. In [4] the external API of the involved components, and how they can be used to publish trust scheme information in the TSPA are described as well as how to use DNS to make trust scheme membership claims discoverable by a verifier in an automated way. If in addition to the Trust Scheme Membership, the requirements of the Trust Scheme are published, a Unified Data Model is required. In [5], the development and publication of such a Unified Data Model derived from existing trust schemes (e.g. eIDAS) is described. [6] present the Graphical Trust Policy Language (GTPL), as an easy-to-use interface for the trust policy language TPL proposed by LIGHTest. In [7], a low- and a high-fidelity prototype of the trust policy authoring tool were developed to evaluate the design, in particular considering novice users.

12.2 Related Work

Most of the existing trust infrastructures follow the subsidiarity principle. One prominent example is the eIDAS Regulation (EU) N° 910/2014 ([8]) on electronic identification and trust services for electronic transactions in the internal market. This includes that each Member State establishes and publishes national trusted lists of qualified trust service providers. For the access of these trusted lists, the EC publishes a central list (“List of Trusted Lists”) which contains links to these lists. Due to the fact that for verifiers the direct use of trust lists can be very onerous, in particular for international electronic transactions, LIGHTest provides a framework that is conceptually

comparable to OCSP for querying the status of individual certificates and which facilities the verification of trust.

DANE (DNS-based Authentication of Names Entities) is a standard using DNS and the DNS security extension DNSSEC to derive trust in TLS server certificates (RCF6698 [9] and RCF7218 [10]). For this purpose, the DNS resource record TLSA was introduced which associates a TLS server certificate (or public key) with the domain name where the record is found. Within LIGHTest, the DANE standard is used to secure network communication and where certificates are used for verifying data.

Much like TLSA, the SMIMEA mechanism [11] provides a number of ways to limit the certificates that are acceptable for a certain e-mail address. It associates an SMIME user's certificate with the intended domain name by certificate constraints. In LIGHTest, the SMIMEA resource record is used to verify if the certificate used for signing the trust list is valid.

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 [12]. 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". Within LIGHTest, the ETSI TS 119 612 standard is used for the representation of Trust Lists.

12.3 Reference Architecture

This section gives an overview of the LIGHTest reference architecture. It defines the macroscopic design of the LIGHTest infrastructure as well as the overall system's components, their functionality and their interaction on a high-level view. Second, examples of usage scenarios are presented. For more details, we refer to [2].

12.3.1 Components of the Reference Architecture

Figure 12.1 shows the LIGHTest reference architecture with all the major software components and their interactions (see also [1] and [2]). It illustrates how a verifier can validate a received electronic transaction based on her individual trust policy and queries to the LIGHTest reference trust infrastructure.

The verifier interacts with the Policy Authoring and Visualization Tools (e.g. desktop or web applications). These tools also facilitate non-technical users the visualization and editing of trust policies, which can be individual

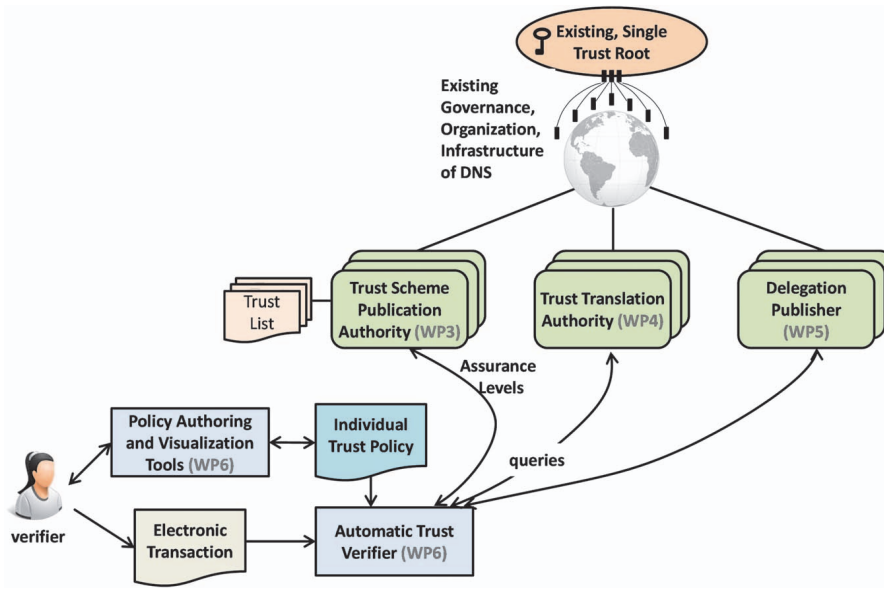

Figure 12.1 The LIGHTest reference architecture (see also [1, 2]).

and specific for each transaction. The role of the trust policy is the provision of formal instructions for the validation of trustworthiness for a given type of electronic transaction. For example, it states which trust lists from which authorities should be used. Further details are given in Section 12.1.

The Automatic Trust Verifier (ATV) takes the electronic transaction and trust policy as input and provides as output if the electronic transaction is trustworthy or not. In addition, the ATV may provide an explanation of its decision, in particular if the transaction was considered as not trustworthy.

The Trust Scheme Publication Authority (TSPA) uses a standard DNS Name Server with DNSSEC extension. A server publishes multiple trust lists under different sub-domains of the authority's domain name. The TSPA enables discovery and verification of trust scheme memberships. In Section 12.1, the TSPA is described in more detail.

The Trust Translation Authority also uses a standard DNS Name Server with DNSSEC extension. Here, a server publishes trust data under different sub-domains of the authority's domain name. In addition, trust translation lists express which authorities from other trust domains are trusted.

The Delegation Publisher uses a DNS Name Server with DNSSEC extension to discover the location (IP address) of the delegation provider, given

that the user knows the correct domain name. The delegations themselves are not published in DNS mainly due to privacy reasons.

12.3.2 Usage Scenarios

In this section, examples of usage scenarios are presented. There are basic scenarios for trust publication, trust translation, and trust delegation, which can be used for qualified signatures, qualified seals, qualified identities, or qualified timestamps. The functionality (publish, translate, delegate) of the basic scenarios can be used to realise a wide range of more sophisticated scenarios. These scenarios can be either variants of the basic scenarios or a combination of different basic scenarios. A combination can be composing two trust services in a chaining process where the output level of the inner trust service becomes the input level of the outer trust service. For example, qualified delivery services, where E-registered delivery can be realised using a combination of the scenarios signature and timestamps. Another example is qualified website authentication, where trust publication with qualified identities is the basic scenario and additionally, trust translation could be used to e.g. authenticate third party users/things.

As an example for a basic scenario, a successful trust scheme membership verification for qualified signatures is presented. For this example, the following preconditions and assumptions for the electronic transaction and trust policy are made:

1. As preconditions, it is assumed that the verifier and signer are both located in the EC/eIDAS trust domain and that the eIDAS trust domain contains the actual eIDAS trust scheme. This means that trust translation is not required in this scenario. This could for example be managed in the following domain name structure: trust.ec.europa.eu - signature - TrustScheme - actual eIDAS trust scheme for qualified signature.
2. For the electronic transaction, it is assumed that the transaction is simply a signed document. Furthermore, the certificate used to sign the document contains a link to the trust list (Trust Membership Claim) for easier discovery such as “Issuer Alt Name: XYZ.qualified.trust.admin.ec” that points to the DNS resource records of the native trust scheme for qualified signatures. In addition, this trust scheme lists the certificate as qualified.
3. For the trust policy, it is assumed that trust policy simply states that the signature of the document is trusted if the issuer of the certificate is listed in TrustScheme.signature.trust.ec.europa.eu. Hence it is published as a

Boolean trust scheme publication (see Section 12.1 for the definition of Boolean trust scheme publication).

For the basic scenario of a successful trust scheme membership verification for qualified signatures with the preconditions and assumptions mentioned above, the corresponding information flow in the architecture is described in the following and depicted in Figure 12.2.

In step 1, the verifier feeds both, the Trust Policy and the Electronic Transaction into the ATV. The ATV parses the electronic transaction and yields the document, the signer certificate and the issuer certificate (step 2). In step 3, the ATV validates the signature on the document to make sure it is signed by the signer certificate. Next, the ATV validates that the signer certificate is signed by the issuer certificate (step 4). In step 5, the ATV searches the signer certificate and the issuer certificate for discovery information. The ATV finds a Trust Membership Claim in the signer certificate: "Issuer Alt Name: XYZ.qualified.trust.admin.ec". Hence, the issuer name is extracted from the certificate. In step 6, the ATV contacts the TSPA for retrieving the associated trust scheme. Therefore, the ATV issues a DNS query for all relevant resource records for boolean trust schemes for XYZ.qualified.trust.admin.ec. In step 7, the ATV verifies the chain of signatures from the DNS trust root of the

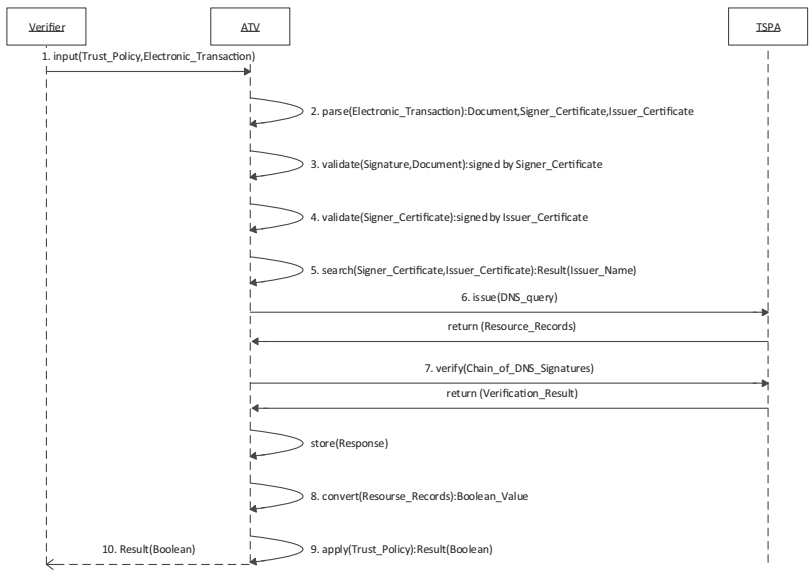

Figure 12.2 Sequence diagram for trust publication of a qualified signature (Boolean), [2].

DNS response using a validating resolver and stores the response as a "receipt" for future justification of its decision. Next, the ATV converts the resource records of the response into a boolean value (step 8). In the final step, the ATV looks at the trust policy and detects that the trust scheme, TrustScheme.signature.trust.ec.europa.eu is trusted (step 9). Hence, the overall result of applying the trust policy to the electronic transaction is trusted and sent back to the verifier (step 10).

The basic structure of the information flow for the other basic scenarios is similar. For qualified seals, qualified identities, or qualified timestamps it is mainly the domain name structure which differs. For trust translation, and trust delegation there are in addition some additional steps required using the Trust Translation Authority and the Delegation Publisher, respectively.

12.4 Trust Scheme Publication Authority

Knowing which trust scheme the issuer of the signers' certificate complies to is critical, in order to be able to verify whether an electronic transaction complies with the users' trust policy. It shows which security controls, and security requirements are fulfilled by the certificate issuer and thus indicate the security quality of the certificate that is used, e.g. for signing a document. The Trust Scheme Publication Authority (TSPA) is therefore an important component of the LIGHTest reference architecture. It enables discovery and verification of trust scheme memberships. Trust scheme publications are always associated with lists that indicate the membership of an entity with the referred to trust scheme. The described setup, which involve a trust list and a trust list provider aligns well with existing trust list standards (e.g. ETSI TS 119 612 [12]).

12.4.1 Trust Schemes and Trust Scheme Publications

A trust scheme itself can for example be constituted by requirements to information security processes, processes for issuance or revocation, requirements towards used technologies, or simply one single one-dimensional requirement, e.g. the geographical location of an entity. While some trust schemes, such as ETSI_EN_319_401 [13], just flatly lay out managerial requirements, trust schemes such as ISO/IEC 29115:2013 [14] further use different level of assurances to define which requirements must be met to comply with the trust scheme. In summary this all means, that a trust scheme can be published as a boolean trust scheme publication (e.g. [13]), and a

Table 12.1 Types of trust scheme publications in LIGHTest, [2]

Type of Trust Scheme Publication	Example	Verifiable Information
Boolean	ETSI_EN_319_401	Compliance of an entity to a trust scheme
Ordinal	LoA4.ISO29115	Compliance of an entity to an ordinal value of a trust scheme
Tuple-Based	{(authentication:2Factor), (identityProofing: inPerson)}	Requirements of a trust scheme

ordinal trust scheme publication (e.g. [14]) (see Table 12.1). Boolean trust scheme publications indicate the entities that comply with the requirements of the trust scheme, and thus are a member of the trust scheme. Ordinal trust scheme publications indicate the entities that comply with the requirements of an ordinal aspect (e.g. a level of assurance) of the trust scheme.

Both, Boolean and ordinal trust scheme publications do not provide any information on the requirements of the trust scheme, or the ordinal value (e.g. Level of Assurance) of the trust scheme that is represented by the trust scheme publication. In order to fill this gap, tuple-based trust scheme publications provide the requirements of a trust scheme in the form of attributes and values.

For this purpose, 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. With this a unified view on the requirements of trust schemes is provided, which can be used within the TSPA. The consolidation and development of this Data Model, which is based on nine existing trust schemes, is presented along with possible applications in the field of trust verification in [5]. The unified 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 119612.

12.4.2 Concept for Trust Scheme Publication Authority (TSPA)

The concept of the TSPA in LIGHTest 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. 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. The use of pointers ensures the limited size of DNS messages, which is required for fast response times in the discovery process.

The use of the DNS Name Server system by LIGHTest enables easy and widespread adoption of the approach. We assume that the trust scheme of a certificate issuer is unknown, upon receiving an electronic transaction. The TSPA therefore provides the capability to discover a trust scheme membership claim for a certificate issuer, and verify this claim. The discovery of a trust scheme membership claim is done by using the domain name resolution capabilities of the DNS Name Server. Figure 12.3 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).

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 (indicated by <*IssuerName*>), and include the Name of the associated Trust Scheme. Data Containers for a Trust Scheme are identified by a SchemeName (indicated by <*SchemeName*>), in the boolean case, and an additional LevelName in the ordinal case (indicated by <*LevelName*>.<*SchemeName*>). A Trust Scheme data container includes the Trust Scheme Provider Domain Name (indicated by <*SchemeProviderName*>). The data containers for the Issuer, trust scheme name and ordinal level of a trust scheme include in addition certificate constraints, which enable to limit the certificates accepted for signing the trust list, using the SMIMEA DNS resource record. Hence, in the LIGHTest ecosystem, the SMIMEA resource record is used to verify if the certificate used for signing the trust list is valid. These records on the DNS Name Server have been developed in a consolidated approach to publishing trust-related information in general in the DNS within in LIGHTest project.

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

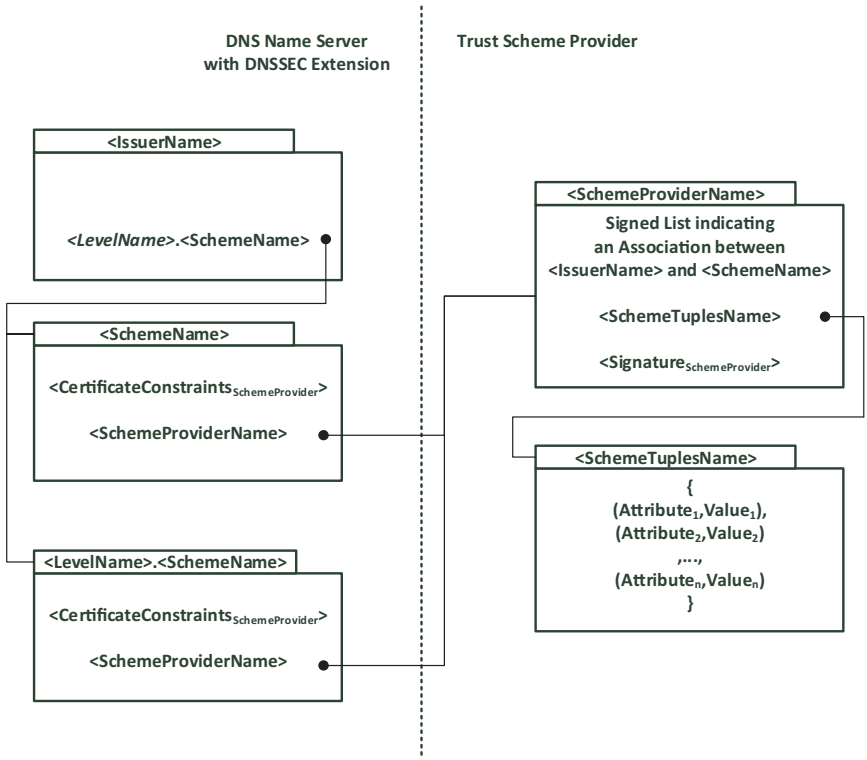

Figure 12.3 Representation of trust scheme publications in the TSPA, [5].

no additional DNS entry for the tuple-based trust schemes required. It uses the same as for the Trust Scheme Provider.

12.4.3 DNS-based Trust Scheme Publication and Discovery

The processes of Trust Scheme publication and discovery of trust lists using DNS is described in detail in [4]. To enable the automatic verification process of an electronic transaction using the ATV, it is required that the verifier knows where the trust scheme is saved at, and it would be more desirable if a CA can publish its membership claim. In order to be found in the DNS, each trust service and trust scheme taking part in LIGHTest picks a domain name as its identifier and announces this name in its associated certificates.

To update nameservers, the following two components were introduced: TSPA (concept of TSPA is introduced in Section 12.1) and ZoneManager.

The TSPA component itself acts as the endpoint for operators, which can be clients publishing trust schemes. It receives all relevant data via an HTTPS API to create the trust scheme. It can process links to existing trust schemes (e.g. eIDAS) as well as full trust scheme data. In the first case, the TSPA component creates the DNS entries together with the ZoneManager. In the second case, the TSPA component stores the trust scheme data locally and creates the DNS entries together with the ZoneManager. The second component, the ZoneManager, acts as the endpoint on the nameserver and modifies the zone data directly. It also ensures any zone data is properly signed using an existing DNSSEC setup. The ZoneManager's interface is only called from the TSPA component, and must never be called from the operator directly. Both components implement a RESTful API that is used by clients to publish the trust scheme information.

12.5 Trust Policy

As introduced in the Reference Architecture in Section 12.1, a verifier can validate a received electronic transaction based on her individual trust policy and queries to the LIGHTest reference trust infrastructure. To do so, the verifier has to provide the electronic transaction as well as an individual trust policy, which contains the formal instructions for the validation of trustworthiness for a given type of electronic transaction as input. The newly, in LIGHTest developed Policy Authoring and Visualization Tools facilitate and support also non-technical users to define their trust policies.

A Trust Policy is a recipe, expressed in a Trust Policy Language, that takes an Electronic Transaction and potentially multiple Trust Schemes, Trust Translation Schemes and Delegation Schemes as input and creates a single Boolean value (trusted [y/n]) and optionally an explanation (e.g., why not trusted) as output. For this purpose, a trust policy language is required, which is a formal language with well-defined semantics that is based on a mathematical formalism and is used to express the recipe of a trust policy. For the trust policy language in LIGHTest (LIGHTest TPL) the logic programming language Prolog that is based on Horn clauses only is used.

To facilitate the usage of LIGHTest TPL, [6] developed the Graphical Trust Policy Language (GTPL), which is an easy-to-use interface for the trust policy language TPL proposed by the LIGHTest project. GTPL uses a simple graphical representation where the central graphical metaphor is to consider the input like certificates or documents as forms and the policy author describes "what to look for" in these forms by putting constrains on the

form's fields. GTPL closes the gap between languages on a logical-technical level such as TPL that require some expertise to use, and very basic interfaces like the LIGHTest Graphical-Layer that allow only a selection from a set of very basic patterns.

Furthermore, it is main goal of the project to develop and evaluate a trust policy authoring tool, considering especially novice users. As most contributions on usable policy authoring and IT-security only focus on the design phase of a tool and on stating guidelines how to make these tools and systems more user friendly. But there is a need for also evaluating tools, not only regarding usability but also user experience. For this purpose, a low- and a high-fidelity prototype were developed to evaluate the design (for further details see [7]). With the low-fidelity prototype a usability evaluation during the beginning of the design phase was conducted. After a design iteration a user experience evaluation with the high-fidelity prototype was conducted and the lessons learned derived from the results are considered.

12.6 Discussion and Outlook

The LIGHTest reference architecture and trust scheme publication authority (TSPA) support the implementation of the eIDAS Regulation ([8]). It enables the integration of existing trust lists using the global DNS infrastructure. Furthermore, it even expands eIDAS towards a global market and multi-users from the public and private sector. For the demonstration of the functionality of the LIGHTest infrastructure, two real world pilots are conducted within LIGHTest: In the first one, LIGHTest is integrated in the existing cloud based platform for trusted communication, the e-Correos platform. In the second one, LIGHTest is integrated in an existing e-Invoicing infrastructure and application scenario, OpenPePPOL.

Furthermore, key components of the LIGHTest infrastructure can be used for validation and authentication of data in sensor networks in IoT, e.g. for predictive maintenance use cases. This is demonstrated in a small sensor network of an organization using a Raspberry pi Cluster (see [15]).

LIGHTest supports UNHCR to explore ways to digitalize their documentation processes e.g. for the DAFI program. As the UNHCR deals with many sensitive documents and information, it is vital to be able to trust and verify the source of the documents after it is digitalized. This is especially important as it adds a higher level of security for such sensitive data and information. By digitalizing the documents using a Trust Scheme, it adds a level of security that not only optimizes the use of the digital documents, but also helps keep

them secure. With that, after a trust scheme is made the digital documents created in the Trust Scheme can be verified and translated for both internal (with other UNHCR locations and Partners) or external (when the documents are being verified by other organizations that trust documents that are given to them by the UNHCR) purposes.

12.7 Summary

There is a high need for assistance from authorities to certify trustworthy electronic identities due to the worldwide increasing amount of electronic transactions. Within the EU-funded LIGHTest project, a global trust infrastructure based on DNS is built, where arbitrary authorities can publish their trust information. In this paper, a high level description of the LIGHTest reference architecture, its components and its application fields are presented. In addition, the Trust Scheme Publication Authority and the Trust Policy are described in more detail.

The reference architecture and the concept for Trust Scheme Publication Authority fulfil the main general principles and goals, which are required to develop a globally scalable trust infrastructure. Furthermore, it is well aligned with existing standards (e.g. ETSI TS 119 612) and fulfil the requirements using DNS name servers to build a global trust infrastructure.

In addition to the LIGHTest pilots for e-Correos and Open-PePPOL, there are a multitude of use cases, e.g. for sensor validation in the field of IoT or for international organizations (e.g. UNHCR).

Acknowledgements

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.

References

[1] Bruegger, B. P.; Lipp, P.: LIGHTest – A Lightweight Infrastructure for Global Heterogeneous Trust Management. In: Hühnlein D. et al.

(Hgeds.): Open Identity Summit 2016, Rome: GI-Edition, Lecture Notes in Informatics. S. 15—26.

[2] 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.; Roßnagel, H.; Hühnlein, D., eds.): Open Identity Summit 2017. Gesellschaft für Informatik, Bonn, 2017.

[3] Wagner, G.; Omolola, O.; More, S.: Harmonizing Delegation Data Formats. In (Fritsch, L.; Roßnagel, H.; Hühnlein, D., eds.): Open Identity Summit 2017. Gesellschaft für Informatik, Bonn, 2017.

[4] Wagner, G.; Wagner, S.; More, S.; Hoffmann, H.: DNS-based Trust Scheme Publication and Discovery. In (Roßnagel, H.; Wagner, S.; Hühnlein, D., eds.): Accepted for Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.

[5] Wagner, S.; Kurowski, S.; Roßnagel, H.: Unified Data Model for Tuple-Based Trust Scheme Publication. In (Roßnagel, H.; Wagner, S.; Hühnlein, D., eds.): Accepted for Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.

[6] Mödersheim, S.; Ni, B.: GTPL: A Graphical Trust Policy Language. In (Roßnagel, H.; Wagner, S.; Hühnlein, D., eds.): Accepted for Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.

[7] Weinhardt, S.; St. Pierre, D.: Lessons learned – Conducting a User Experience evaluation of a Trust Policy Authoring Tool. In (Roßnagel, H.; Wagner, S.; Hühnlein, D., eds.): Accepted for Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.

[8] 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.

[9] Hoffman, P.; Schlyter J.: The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, RFC 6698, DOI 0.17487/RFC6698, 2012, http://www.rfc-editor.org/info/rfc6698

[10] Gudmundsson, O.: Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE), RFC 7218, DOI 10.17487/RFC7218, 2014, http://www.rfc-editor.org/info/rfc7218

[11] Hoffman, P.; Schlyter, J.: Using Secure DNS to Associate Certificates with Domain Names for S/MIME, RFC 8162, RFC Editor, May 2017.

[12] ETSI: Electronic Signatures and Infrastructures (ESI); Trusted Lists. Sophia Antipolis Cedex, France, Technical Specification ETSI TS 119 612 V1.1.1, 2013; http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/01.01.01_60/ts_119612v010101p.pdf

[13] ETSI: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. ETSI, Sophia Antipois Cedex, France, European Standard ETSI EN 319 401, 2016; http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf

[14] ISO/IEC 29115: Information technology – Security techniques – Entity authentication assurance framework. ISO/IEC, Geneva, CH (2013).

[15] Johnson-Jeyakumar, I.-H.; Wagner, S.; Roßnagel, H.: Implementation of Distributed Light weight trust infrastructure for automatic validation of faults in an IOT sensor network. In (Rossnagel, H.; Wagner, S.; Hühnlein, D., eds.):Accepted for Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, 2019.