LIGHTest: Lightweight Infrastrucutre for Global and Heterogeneous Trust Management

Heiko Roßnagel
Institute of Industrial Engineering
Fraunhofer IAO
Stuttgart, Germany
{firstname.name}@iao.fraunhofer.de

Sven Wagner
Institute of Human Factors and
Technology Management
University of Stuttgart
Stuttgart, Germany
{firstname.name}@iat.uni-stuttgart.de

***Abstract*—The EU-funded LIGHTest project is developing a global trust infrastructure that enables an easy and efficient verification process of electronic transactions, even if the involved instances belong to different trust domains. LIGHTest builds on the available internet Domain Name System (DNS) infrastructure. This paper gives an overview on the LIGHTest project, its reference architecture and variety of application fields.**

Keywords—trust infrastructure, trust scheme, electronic transaction, eIDAS, trust policy, LIGHTest, IoT

I. 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. This is also the case for incoming data, e.g. from sensors. 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 task 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.

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 further information on individual aspects of LIGHTest we refer to publications of the project ([1], [2], [3], [4], [5], [6], [7]). More details can be also found on the LIGHTest project web site https://www.lightest.eu/, for example the project deliverables and the LIGHTest Cookbook, which is a practical step-by-step guide to deploying the LIGHTest infrastructure in an everyday ICT environment.

II. Reference Architecture

The LIGHTest reference architecture defines the macroscopic design of the infrastructure as well as the overall system's components, their functionality and their interaction on a high-level view (see Figure 1).

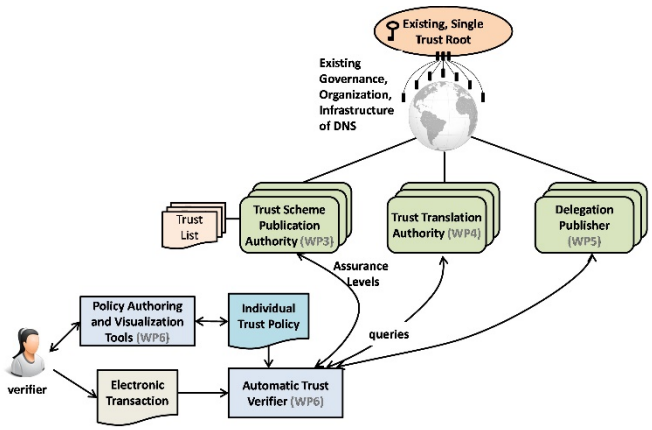

Figure 1: The LIGHTest Reference Architecture (see also [1], [2])

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

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.

The Trust Translation Authority (TTA) 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 (DP) 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.

III. Use Cases and application fields

The LIGHTest reference architecture and its 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-Procurement infrastructure and application scenario, OpenPePPOL. In addition, a mobile ID scheme based on FIDO with extended ID information is implemented using LIGHTest infrastructure. Furthermore, a demo example is presented in the LIGHTest Cookbook.

LIGHTest also supports UNHCR to explore ways to digitalize their documentation processes. 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 optimizes the use of the digital documents and 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 or external (when the documents are being verified by other organizations that trust documents that are given to them by the UNHCR) purposes.

Furthermore, key components of the LIGHTest infrastructure can be used for validation and authentication of data in sensor networks in IoT and IIoT environments, e.g. for predictive maintenance use cases. This is demonstrated in a small sensor network of an organization using a Raspberry Pi Cluster [9]. Further possible applications fields for LIGHTest infrastructure are introduced in [10] for smart farming and in [11] for smart cities.

IV. Summary and conclusions

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. The LIGHTest infrastructure fulfils the main general principles and goals, which are required for a globally scalable trust infrastructure. Furthermore, it is well aligned with existing standards (e.g. ETSI TS 119 612) and fulfils 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 and IIoT as well as for international organizations (e.g. UNHCR)

Acknowledgment

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] B.P. Bruegger, P. Lipp, "LIGHTest – A Lightweight Infrastructure for Global Heterogeneous Trust Management, " in Open Identity Summit 2016, D. Hühnlein D. et al, Eds. Gesellschaft für Informatik, Bonn, 2016.

[2] S. Wagner, S. Kurowski, U. Laufs, H. Roßnagel, "A Mechanism for Discovery and Verification of Trust Scheme Memberships: The Lightest Reference Architecture" in Open Identity Summit 2017, L. Fritsch, H. Roßnagel, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2017.

[3] G. Wagner, O. Omolola, S. More, "Harmonizing Delegation Data Formats" in Open Identity Summit 2017, L. Fritsch, H. Roßnagel, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2017.

[4] G. Wagner, S. Wagner, S. More, M. Hoffmann, "DNS-based Trust Scheme Publication and Discovery," in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019.

[5] S. Wagner, S. Kurowski, H. Roßnagel, "Unified Data Model for Tuple-Based Trust Scheme Publication," in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019.

[6] S. Mödersheim, B. Ni, "GTPL: A Graphical Trust Policy Language," in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019.

[7] S. Weinhardt, D. St. Pierre,"Lessons learned – Conducting a User Experience evaluation of a Trust Policy Authoring Tool, " in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. 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] I.-H. Johnson-Jeyakumar, S. Wagner, H. Roßnagel, "Implementation of Distributed Light weight Trust infrastructure for automatic validation of faults in an IOT sensor network," in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019.

[10] S. Wagner, A. Horch, B. Kilian, H. Roßnagel, „Leichtgewichtige Infrastruktur zur Schaffung von sicherheit und Vertrauen in einem digitalen Ökosystem für Agrardaten." in 38. GIL Jahrestagung, A. Ruckelshausen et al., Eds. Gesellschaft für Informatik, Bonn, 2018.

[11] O. Omolola, S. More, E. Fasllija, G. Wagner, L. Alber, "Policy-based Access Control for the IoT and Smart Cities" in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019.

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