D11.9

Report on Dissemination, Exploitation, and List of Technical Outcomes (6)

Document Identification	
Date	27.02.2018
Status	Final
Version	Version 1.01

Related WP	WP11	**Related Deliverable(s)**	D11.4-15
Lead Authors	Lorraine Spector	**Dissemination Level**	PU
Lead Participants	EEMA	**Contributors**	FHG
Reviewers	USTUTT		

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 is a copy of the report on dissemination, exploitation and list of technical outcomes, in the form of a news bulletin.

2. Document Information

Contributors

Name	Partner
Lorraine Spector	EEMA
Fabina Debicki	USUTT
Heiko Roßnagel	FHG

History

Version	Date	Author	Changes
V1.00	20/02/2018	LS	Initial Document
V1.01	26/02/2018	LS	Insert comments, minor grammar changes

3. Table of Contents

4. Project Description

LIGHT^{est} 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 LIGHT^{est} 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 LIGHT^{est} 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 LIGHT^{est} open source software to easily query this trust information to verify trust in simple signed documents or multi-faceted complex transactions.

The three-year LIGHT^{est} project started on September 1st 2016 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 LIGHT^{est} consortium consists of 14 partners from 9 European countries and is coordinated by Fraunhofer-Gesellschaft. To reach out beyond

Europe, LIGHT^{est} 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 Denmark (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.

5. Project Reference

A report on dissemination, exploitation and list of technical outcomes.

These deliverables are a series of bulletins describing relevant current dissemination outcomes and technical updates thus promoting internal communications.

The reports will be circulated as newsletter.

6. LIGHTest Bulletin (6)

LIGHTest Newsletter
Edition 6
February 2018

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 700321

View from the Advisory Board – A US perspective on the LIGHTest Project: Commercial equivalence as a lubricant for the information economy

From the US commercial perspective, leveraging the DNS infrastructure to publish trust schemes (or contractually bound identity trust frameworks of various kinds) offers, for the first time, the promise of easy global access to authoritative and authentic trust information, and the notion of publishing trust schemes and their policies – representing commercial equivalence in trusted information versus legal equivalence – is built expressly on the EU foundation of two of the most extraordinary legal achievements of our era: the eIDAS Regulation and the GDPR. Now LIGHTest unleashes the ability for both the US and EU commercial sectors to leverage fully these pathbreaking regulations as the basis for a trust infrastructure to grow the global information economy.

At the General Meeting in Graz, Jon Shamah highlighted two important objectives for LIGHTest:

1. Providing scalable transparency to trust services, globally.

2. Extending the EU strategy of eIDAS influence outside of original geographic and sector boundaries.

This is echoed in the D2.9 Report on page 15 – "Observing that the eIDAS Regulation provided a strong and credible trust model for electronic identification and trust services within the European Union, the goal was to find a way to extend this model both geographically (identities and trust services outside the EU) and contextually (other trust information than the trust schemes of the eIDAS Regulation).

The first category of added value LIGHTest brings involves digital identity providers, attribute providers, identity brokers, and Trust Mark issuers. Because the eIDAS cross-border recognition provisions for electronic identification apply only to public sector identity credentials issued by EC member states, EU-US commercial interests still have immediate need for private sources of digital identity credentials, as well as identity attribute brokering services to enable international transactions and data transfers. From the US perspective, the LIGHTest trust model of assurance that is legally defined, based on independent audits, and discoverable through public trust lists, provides a technology and policy tool for achieving identity assurance that can unleash opportunities for international data transfer. As the Social Impact Report notes – "LIGHTest can be used for any trust scheme and any trust decision, whether based on a legislative framework, contractual assurances or even individual preferences, even at a very small ad hoc scale." (D2.9 at page 15.)

The second category of added value occurs when service providers offer validation of non-qualified trust services and the commercial equivalent of such services outside of the EU. Though the usefulness of qualified trust services for achieving legal equivalence is without doubt in a vast number of use cases, US commercial interests merely need the ability to leverage non-qualified electronic signatures, electronic seals, and delivery services. Currently, there is no easy or scalable means by which to find these non-qualified trust

Timothy S. Reiniger, The Timothy Reiniger LLC Advisory Practice

services, validate their authenticity, and translate assurance levels. "Since the number of application areas is practically unlimited – LIGHTest can be used whenever trusted information must be published, validated or translated." (D2.10 page 25.)

The third category of added value results from ability of the LIGHTest infrastructure to enable trust

@LIGHTest_trust LinkedIn www.lightest.eu

Produced by EEMA - WP11 Lead, LIGHTest

translation. "Trust translation essentially relates to an assessment and finding of equivalence between specific trust schemes." (D2.10 page 22.) In particular, EU and US commercial interests will be able to use LIGHTest to assist with publishing and discovering trust information relating to the GDPR compliance. "Compliance with data protection law is particularly crucial to LIGHTest: at its heart, LIGHTest uses a global technology (the DNS) for the publication, validation, and translation of trust information." (D2.10 page 8.) In relation to international data transfers, this could include, for example, use of LIGHTest as a method of discovering all Data Controller and Data Processor registration of certification mechanisms, data protection seals, and data protection marks with the EU Data Protection Board (GDPR Articles 42(8) ,43(6), and 46(2)(f)).

With respect to LIGHTest's value-add for trust translation, of special interest is the current legal challenge to the validity of Standard Contractual Clauses (SCC) as a channel for EU-US data transfers. The Court of Justice of the EU will soon be weighing whether EU citizens have sufficient legal recourse in the US for GDPR violations by US Data Processors when using the SCC data transfer method. One US-based response could be to achieve suitable recourse under the Virginia Electronic Identity Management Law, which specifies that privacy/data protection is a matter to be addressed by identity trust framework providers and operators as minimum criteria. Also the proposed Virginia guidance documents relating to this law contemplate that, for some identity trust framework providers, data protection requirements such as the GDPR will be expressly incorporated. Therefore, the LIGHTest infrastructure could be used to publish the trust policies of such identity trust framework providers (or trust schemes) so as to make it convenient for EU Data Controllers to locate Data Processors in the United States who are members of such a framework and who could be subject to legal recourse in the United States for GDPR violations.

US commercial interests will take great interest in the LIGHTest's implementation of the EU trust management model as a method for achieving commercial equivalence in electronic identification and trust services as well as GDPR compliance. "If two partners (e.g. the EU and the USA) have decided that they wish to acknowledge the equivalence of certain electronic identities and/or trust services, they could use the tools that LIGHTest will provide to discover their trust scheme information, to validate it in individual transactions, and even to facilitate the translation of trust via the DNS based on their agreed equivalence rules." (D2.9 page 10.) Similarly, in the US, the Virginia Electronic Identity Management Law leverages the EU trust model in the form of legally recognized identity trust frameworks that provide a basis for governance and legal recourse relating to electronic identification, identity-related trust services, data protection. Thus, LIGHTest gives US commercial interests a trustset with which to leverage eIDAS, GDPR, and the US-based Virginia law to grow the information economy.

Author: Timothy S. Reiniger, The Timothy Reiniger LLC Advisory Practice

Why are identities a core element of digitalisation?

When looking at successful digitalisation efforts in industry, retail and utilities sectors, or other areas including government, at the core you will typically find a solid identity solution. The reason is simple: the identity solution, trust and information, are often the glue binding things, information elements and content together.

If you look at the digitalisation goals in an organisation, you will find themes such as: reducing risks, improving learning from historical incidents, strengthening security; streamlining of processes and reducing manual input; improving data accessibility and enabling better decision-making; enabling real-time analytics and increasing automation; using data to maximise asset value through optimisation and process improvements.

Realising these goals typically requires an identity and access management (IAM) solution. Examples of IAM use cases in digitalisation projects include:

- User authentication and identity verification, including verification of the organisation information of the identity in question; roles and attributes based access to information and content.
- Verification of accessed target services and the endpoint "things" to ensure that they and the output they deliver can be trusted.
- Delegated management of identity, access and authorisation to enable sufficient management and ensure that the identity information is up to date and can be trusted.

The identity information is from one perspective a representation of the user. The identity solution then, based on that identity information, ensures that the user gets a consistent and integrated view and access to all the content he/she is supposed to reach.

Think of all the various services, internal as well as external, that a person in an organisation requires during a typical day at work. Now, picture the access to all those services as a kind of dashboard user-experience. Whether there actually is

one single view dashboard, or just a smooth and consistent easy access to all that is relevant is not really the point. The essential point is that the access from the user perspective should be smooth, in order to reach the services and tools they need, as if there was one integrated dashboard with all those services readily available.

With a solid IAM solution in place this is the vision that can be delivered, ensuring that only authorised users get access to their services and content smoothly and securely.

Author: Charles Sederholm - Director, Business Development, Ubisecure

Why did Ubisecure join LIGHTest?

UBISECURE™

As a platform and service provider for externally facing customer IAM, Ubisecure is positioned at the interfaces and interaction points of transactions involving identity information. Many Ubisecure customer organisations and the typical use cases our products solve deal with cross-organisational and cross-border interaction. Hence it is only natural that we want to participate in developments that bring essential elements of technologies and principles forward.

We also have almost as a corporate culture a tradition throughout our 15+ year history to participate in joint efforts, for instance standardisation of core identity-related standards and interop enabling activities such as SAML, OpenID Connect/OAuth2, GSMA Mobile Connect, and national efforts such as eID and eIDAS.

So, when we were asked to join LIGHTest, we responded positively and since the LIGHTest kick-off we have very much enjoyed the interaction and discussions with some of the key players in the security and identity scene; and their very experienced experts, who are part of the LIGHTest project team.

URL: https://www.ubisecure.com

Author: Charles Sederholm - Director, Business Development, Ubisecure

NLNETLABS

Project partner profile - NLnet Labs

NLnet Labs is a non-profit foundation that develops open source software and open standards for the benefit of the Internet. It focuses its activities on technology and architecture that are fundamental for turning the world-wide collection of interconnected networks into the Internet. Prominent among these technologies is the Domain Name Service (DNS). NLnet Labs developed and now maintains several widely used software packages covering the entire range of deployment such as NSD, Unbound, OpenDNSSEC and getdns. The team contributes to the development of the open standards underpinning the DNS through participation with organisations such as the Internet Engineering Task Force (IETF), ICANN, the DNS Operation and Research Center (DNS-OARC), regional Internet registry meetings like RIPE and LACNIC, as well as meetings of the operational user community such as NANOG.

NLnet Labs contributes the experience gained from both architectural work as well as practical implementation and operation of the DNS to the LIGHTest project. As part of the WPs 3, 4, and 5, NLnet Labs participates in designing the global, distributed infrastructure for publishing and verifying trust-related information on top of the DNS, with an aim to ultimately introduce this infrastructure into the relevant standards bodies, in particular, the DNS community within the IETF, and, together with these bodies, foster LIGHTest's success beyond the initial project.

As NLnet Labs' software will be used for the implementations and pilots, NLnet Labs will provide support for configuration and extensions to the software.

URL: https://www.nlnetlabs.nl

Author: Martin Hoffmann, Systems Architect, NLnet Labs

LIGHTest Newsletter Edition 6 February 2018

WP2 Summary

Title: **Requirements, Concepts and Evaluation**

Lead Partner: **DTU, Denmark**
Contact: **Sebastian Moedersheim**

T2.3: Formal Description. The work on accountability has continued, however is now on hold as the main researcher at DTU has left. We hope to find a new employee soon.

The next deliverables are in M24, namely D2.5 on the formal description in the second version, and D2.12, namely the first evaluation. Also, in M26 will be D2.8 on the critical infrastructure analysis.

WP3 Summary

Title: **Infrastructure for the Publication and Querying of Trust Schemes**

Lead Partner: **FHG, Germany**
Contact: **Dr. Heiko Roßnagel**

Current work is focusing on T3.2: Design of DNS-based Publication of Trust Schemes for D3.3 (which will be submitted in M18). A consolidated approach to publishing trust-related information in DNS was developed in collaboration with WP4 and WP5.

Roßnagel, Sellung, Mödersheim, and Wagner participated at a joint workshopwith UNCHR, Copenhagen, Denmark on 13th February 2018.

WP4 Summary

Title: **Infrastructure for Translations across Trust Domains**

Lead Partner: **ATOS, Spain**
Contact: **Javier Presa**

T4.2: Design of DNS-based Publication of Trust Translation Schemes was finished producing the deliverable D4.3.

Meetings with WP3, WP5 and WP6 to discuss the design of the DNS-based publication in the three WPs.

Preparation of activities T4.3 and T4.4 in order for them to be started in this period. Activities T4.3 & T4.4 to be started in this period.

WP5 Summary

Title: **Infrastructure for the Publication and Querying of Delegations**

Lead Partner: **TU Graz, Austria**
Contact: **Dr. Peter Lipp**

Recently, we have been investigating different protocols to answer the question of how to publish delegations on a Delegation Provider. D5.3 will be submitted at the end of February.

WP6 Summary

Title: **Trust Policy and Automatic Trust Decisions**

Lead Partner: **TU Graz, Austria**
Contact: **Dr. Peter Lipp**

The two tasks - T6.1 (Requirements and Design of a Conceptual Framework for Trust Policies) and T6.2 (Usability and Interaction Design) are in progress. T6.1 defines the requirements for the trust policies and the tool that is needed to create and edit such trust policies. T6.2 focuses on how to provide a design that is user-friendly and easy to use for non-technical users.

Two intermediate deliverables have been submitted for internal review.

WP7 Summary

Title: **Trust Propagation of Derived mobile IDs**

Lead Partner: **Giesecke & Devrient Gesellschaft mit beschränkter Haftung, Germany**
Contact: **Dr. Frank-Michael Kamm**

The focus is currently on T7.3, where a demo ID derivation scheme is being implemented. The implementation work for the proof-of-concept has started and is showing good progress. In parallel, the optimisation of software-based credential protection is continuing by focussing on the resistance against side channel attacks.

The next deliverable is D7.3, focused on the demo implementation of the defined mobile ID scheme. A first live demo, showing some core parts of the functionality is planned for the first review meeting in April 2018.

WP8 Summary

Title: **Integration and Testing**

Lead Partner: **TÜBITAK, Turkey**
Contact: **Dr. Muhammet Yildiz**

D8.6 was finished and submitted on M16. The WP started the implementation of the testing components for the testing architecture and is planning to demonstrate a sample at the general meeting in Seville.

WP10 Summary

Title: **Transfer to Market**

Lead Partner: **ATOS, Spain**
Contact: **Alberto Miranda**

The first milestone T10.4 (LIGHTest Sustainability and Adoption Roadmap) has been achieved with the submission of the deliverable D10.6. Preparation for the D10.9: Standardisation (M24) that belongs to the T10.5.

@LIGHTest_trust LinkedIn www.lightest.eu Produced by EEMA - WP11 Lead, LIGHTest

LIGHTest Newsletter Edition 6 February 2018

WP11 Summary

Title: **Dissemination and Communication**

Lead Partner: **EEMA, Belgium**
Contact: **Jon Shamah**

The WP continues to promote the project and the LIGHTest Community Website continues to be populated.

WP11 continues to work with WP10 to produce a robust sustainable business plan and WP11 messaging.

EEMA presented at the RECRED H2020 Clustering Workshop in Athens, Greece, which aimed to establish tight connections with relative H2020 projects in the field of privacy and security.

WP delivered D11.9.

Activities & Events

18 March 2018
IETF Meeting, London, UK
www.ietf.org/meeting/upcoming.html

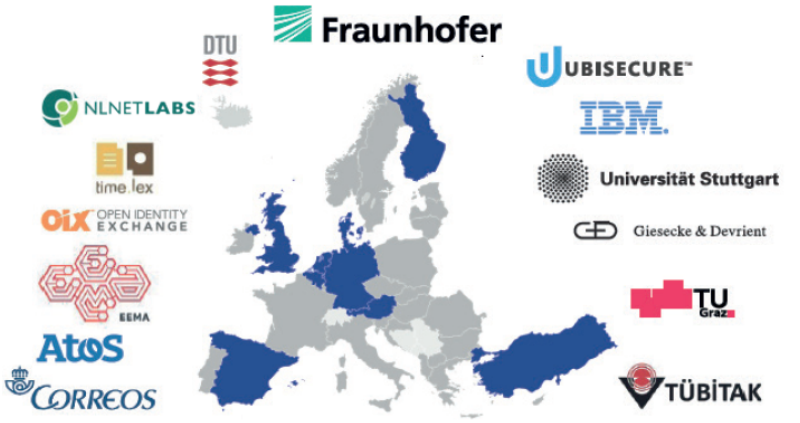
26 – 28 March 2018
KNOW Identity 2018, Washington D.C., USA
www.knowidentityconference.com

13 – 14 June 2018
EEMA Annual Conference on Identity, London, UK
www.eema.org

14 – 15 June 2018
MGOV, Brighton, UK
www.m4life.org

24 - 27 June 2018
Identiverse, Boston, USA
www.identiverse.com

The LIGHTest Project Partners



@LIGHTest_trust LinkedIn www.lightest.eu Produced by EEMA - WP11 Lead, LIGHTest