



Report on Dissemination, Exploitation, and List of Technical Outcomes (7)

Document Identification	
Date	09.05.2018
Status	Final
Version	Version 1.00

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

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.

This document and its content are the property of the *Lightest* Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the *Lightest* Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the *Lightest* Partners.

Each *Lightest* Partner may use this document in conformity with the *Lightest* Consortium Grant Agreement provisions.

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	1 of 12
Dissemination:	PU	Version:	Version 1.00
		Status:	Final



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.

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	2 of 12		
Dissemination:	PU	Version:	Version 1.00	Status:	Final



2. Document Information

Contributors

Name	Partner
Lorraine Spector	EEMA
Heiko Roßnagel	FHG

History

Version	Date	Author	Changes
V1.00	09/05/2018	Lorraine Spector	Initial Document

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	3 of 12		
Dissemination:	PU	Version:	Version 1.00	Status:	Final



3. Table of Contents

1. Executive Summary	2
2. Document Information	3
Contributors.....	3
History	3
3. Table of Contents	4
4. Project Description	5
5. Project Reference	7
6. LIGHTest Bulletin (7)	8

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	4 of 12		
Dissemination:	PU	Version:	Version 1.00	Status:	Final



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

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	5 of 12		
Dissemination:	PU	Version:	Version 1.00	Status:	Final



Report on Dissemination, Exploitation, and List of Technical Outcomes (7)



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.

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	6 of 12		
Dissemination:	PU	Version:	Version 1.00	Status:	Final



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 newsletters.


Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	7 of 12		
Dissemination:	PU	Version:	Version 1.00	Status:	Final




6. LIGHTest Bulletin (7)



Newsletter
Edition 7 - Internal
May 2018

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

Trusted mobile IDs using LIGHTest



Dr. Frank-Michael Kamm,
G+D Mobile Security

When a service provider such as a bank wants to on-board a new customer by a fully digital flow, it faces the challenges to determine the Level of Assurance (LoA) of the customer identity, to technically link the

identity to authentication credentials, and to provide a smooth and user-friendly online flow. In addition, the process must comply with existing regulations like eIDAS, GDPR and the Payment Service Directive (PSD2). If the customer has a non-European ID, this requires trust translation from the foreign scheme to eIDAS. In addition, compliance to national regulations may restrict the choice of allowed authenticators.

To address these challenges, LIGHTest WP7 develops technologies to use mobile IDs with known trust levels based on FIDO technology. The goal is to provide a mobile ID and strong authentication concept that allows a service provider to determine which overall LoA can be achieved with a specific mobile ID and authentication method.

The FIDO protocol is particularly well suited for this approach since it already provides an internal attestation scheme, allowing a relying party to verify which type of authenticator is used. By querying the LIGHTest infrastructure, it can be verified whether this specific authenticator complies with a regional or industry-specific trust schemes. As an example, a national

banking regulator could establish a national trust scheme for financial applications and could publish the types of accepted authenticators. The complex landscape of involved roles and trust schemes is shown in Figure 1. Since the issuers of the primary and secondary (mobile) ID, the authenticator manufacturer and the relying party can be located in different trust schemes, a propagation of trust information (like the LoA) requires heavy use of the LIGHTest infrastructure.

With the technologies developed in WP7, service providers can obtain the overall LoA of a mobile ID and can ensure compliance with their specific trust scheme. All of this occurs in a user-friendly way and is compatible to modern authentication technologies like biometrics.

As the identity and authentication challenges are of extreme importance for the digitalisation strategy of many major service providers, this topic will gain further business relevance over the next years.

Author: Dr. Frank-Michael Kamm, G+D Mobile Security

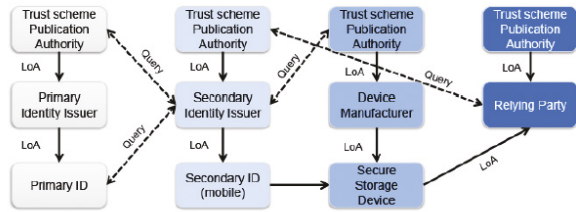




Figure 1: Roles and relationships in the complex landscape of derived mobile IDs across different trust schemes.

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

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	8 of 12
Dissemination:	PU	Version:	Version 1.00
		Status:	Final



DNS - A perfect foundation for the LIGHTest global trust infrastructure

The Internet, made up of millions of computers connected in a complex fashion, employs a system of numbers to find these computers. Not entirely unlike the system of telephone numbers used by its predecessor, these numbers aren't particularly friendly. Humans prefer to give meaning to the world through names. The Domain Name System, DNS for short, builds a bridge between the world of numbers and the world of names. Through its service, a computer system being provided by its human user with the name of another system can find that system's numeric address, as well as additional related information.

Following the nature of the Internet itself, the DNS isn't provided through a single, centrally controlled naming office. Rather, everyone is responsible for providing the service for their own systems. The DNS is the combined effort of everyone naming their own corner of the Internet. It is held together by the names themselves as they name a system within a larger system. In their distinct form dots separate the systems from small to large. The LIGHTest website, www.lightest.eu, thus is provided by a computer named www

within the domain lightest.eu which itself is part of the domain eu.

Each domain is responsible for providing its own name service. It also knows where its subordinate domains provide their name service. This is all information they need so that if someone asks them for a name, they can either provide the information for the name or point to where that information may possibly be found elsewhere.

In the original DNS specification, designed more than thirty years ago in the early days of the Internet, data received from any of these name services was blindly trusted as authentic. A clever malfasant can manipulate this data, however, and trick computers into connecting to the wrong system—with varyingly terrifying consequences. The DNS Security Extensions, DNS-SEC, were added to deal with this issue and provide a means to verify that DNS data is authentic and can be trusted.

With this confidence in the correctness of its data, publishing trust-related information by associating it with domain names becomes a perfect foundation for the LIGHTest global trust infrastructure.

Author: Martin Hoffmann, Systems Architect, NLnet Labs

Project partner profile - Correos



Correos is a global operator of physical, digital and parcel

solutions. In addition, it is Spain's designated company for the provision of universal postal service, with efficiency, quality and sustainability.

The company is leading an effort on secure digital communications, by offering its cloud-based eCorreos suite & platform, and so becoming a trusted digital third party. Today, Correos is offering a set of very ambitious services in order to take a leading role in public digitalisation: facilitating online communications between citizens, businesses and governments.

For more than 10 years, Correos has been the provider of secure electronic notifications to the Ministry of Finance and other agencies in Spain. Moreover, it has been managing more than 11 million electronic notifications annually, securely and reliably handling them to over 1 million customers.

In order to provide this secure online platform, eCorreos is hosted under a .post domain. Post project was developed with high standards of security (including DNS-SEC) and sponsored by the Universal Postal Union (UPU) agency of the United Nations.

Putting LIGHTest to the test with eCorreos



Javier Salazar, Digital Strategy Project Manager, Correos

Aiming to innovate and develop online trusted services, Correos decided to enroll in the LIGHTest project, making its mature cloud-based platform, eCorreos, available to market-check LIGHTest. Therefore, the possible benefits of using an additional trust management DNS infrastructure will be tested and so its market acceptance.

In order to proceed with a real market test, Correos has offered to test LIGHTest with three of its digital services (eCorreos):

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	9 of 12
Dissemination:	PU	Version:	Version 1.00
		Status:	Final



Report on Dissemination, Exploitation, and List of Technical Outcomes (7)



LIGHTest
Newsletter Edition 7 - Internal May 2018

eCORREOS
Mi Identidad

- My identity ("Mi Identidad"): provides secured digital identities to citizens, businesses and governments. Therefore, acting as a trusted third party to validate identity attributes, raising third parties trust on individuals. It acts as a gateway to eCorreos services and even non-Correos applications.

eCORREOS
Mis Notificaciones

- My Notifications ("Mis Notificaciones"): is a digital service, within the eCorreos suite, aiming to centralize and manage governmental notifications for one or several individuals or legal entities.

eCORREOS
Mi Buzón

- My Mailbox ("Mi Buzón"): is meant to be a space where citizens, companies and governments will be able to send and receive relevant documentation (like a digital version of the physical mailbox). Information will be stored with all legal guarantees and high security standards. Moreover, sender and receiver are validated and uniquely identified by Correos. Individuals can subscribe to any verified business/government agency to start receiving trusted information.

Even though this is only part of a whole suite, these services represent the best fit sample to be used within the LIGHTest pilot. Put simply, My Identity is the gateway to My Notifications and My Mailbox. The last two represent different perspectives on the matter of using digitally trusted communications between two parties.

Every use case or scenario that will be validated with LIGHTest will increase eCorreos service robustness and maximise guarantees in terms of trust and confidence to its customers.

Author: Javier Salazar, Digital Strategy Project Manager, Correos

LIGHTest Business Brochure, facilitating the emerging market of cross-border trust services

WP2 Summary

Title: Requirements, Concepts and Evaluation

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

T2.3 (a new graphical notation for TPL) is in progress, which will make the specification of TPL even easier! Note that this is still at the expert level, while normal users may use the graphical and natural language interfaces developed by USTUTT.

T2.7 The evaluation is now commencing.

In M24, several deliverables are due, namely the first version of the evaluation and the second version of the formal description.

WP3 Summary

Title: Infrastructure for the Publication and Querying of Trust Schemes

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

T3.1 Design of a Conceptual Framework for Trust Schemes

T3.3 Discovery of Trust Scheme Publication Authorities

T3.4 Open Source Client Library and Server Tools for Trust Schemes

T3.5 Ensuring Cross-Border Legal Compliance and Validity of Trust Scheme Publication

The current work focuses on all tasks from above. D3.3 (DNS-based Publication of Trust Schemes) was submitted on time in M18 and D3.4 (Discovery of Trust Scheme Publication Authorities) will be submitted in M21.

WP4 Summary

Title: Infrastructure for Translations across Trust Domains

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

T4.3 (Discovery of Trust Translation Authorities) is about to finish, producing the deliverable D4.4 and T4.4 has started as part of the development. There are regular meetings taking place with the other technical WP's (3,5 & 6) to discuss the aspects of the tasks.

WP5 Summary

Title: Infrastructure for the Publication and Querying of Delegations

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

Currently, we are working on the discovery of delegations on the Delegation Provider, investigating different protocols to answer the

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

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	10 of 12
Dissemination:	PU	Version:	Version 1.00
		Status:	Final



Report on Dissemination, Exploitation, and List of Technical Outcomes (7)



question of how to publish delegations on a Delegation Provider.

We have successfully implemented a Graphical User Interface (GUI) for the publication of delegations.

D5.4 will be submitted in M21.

WP6 Summary

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

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

T6.1 (Requirements and Design of a Conceptual Framework for Trust Policies) and T6.2 (Usability and Interaction Design) are currently in progress.

T6.1 defines the requirements for the trust policies and for the tool that is needed to create and edit such trust policies.

T6.2 is looking at how to provide a design that is user-friendly and easy to use for non-technical users.

Two intermediate deliverables that are due have been submitted for internal review and work is in progress on the final deliverable for T6.1.

WP7 Summary

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

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

WP7 is currently working in parallel on T7.3, T7.4 and T7.5. These tasks deal with the implementation of the demo derivation scheme, the integration of trust environments into the demo and the implementation of a demonstrator application. The work on all tasks is showing good progress.

A first version of the demo application shows the actual user flow and the binding between FIDO credentials and the ID derivation. The enhancement of software-based credential protection is progressing as well, allowing better side-channel resistance for the credential protection in future.

The next deliverable is D7.3 on the demo implementation of the defined mobile ID scheme.

WP8 Summary

Title: **Integration and Testing**

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

A demonstration of the LIGHTest Minder Applied testing architecture was performed at the Seville General Assembly. We are currently preparing for the M24 deliverables - D8.1, D8.3, D8.7 and D8.8.

WP10 Summary

Title: **Transfer to Market**

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

Work is ongoing preparing for D10.9 (Standardisation) which belongs to T10.5. This includes regular contact with all the partners assigned to the task. There were no expected deliverables within this period.

WP11 Summary

Title: **Dissemination and Communication**

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

WP 11 continued disseminating LIGHTest values into the market and continued work on D11.10.

A new Advisory Board member from Azerbaijan was approved by majority vote and is expected to be inducted by the summer.

LIGHTest had a meeting with UNHCR with regards to applicability.

Data governance and transparency using LIGHTest was discussed at the ID-Next Conference round table in Eindhoven, Netherlands.

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 RECED H2020 Clustering Workshop in Athens, Greece, which aimed to establish tight connections with related H2020 projects in the field of privacy and security.

WP delivered D11.9.

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	11 of 12
Dissemination:	PU	Version:	Version 1.00
		Status:	Final





The LIGHTest team met in Seville, Spain from 6th – 8th March for the fourth General Meeting

Activities & Events

13 – 14 June 2018

EEMA Annual Conference – Maximising Digital Transformation Using Trusted Identities, London, UK

www.eema.org

14 – 15 June 2018

MGOV, Brighton, UK

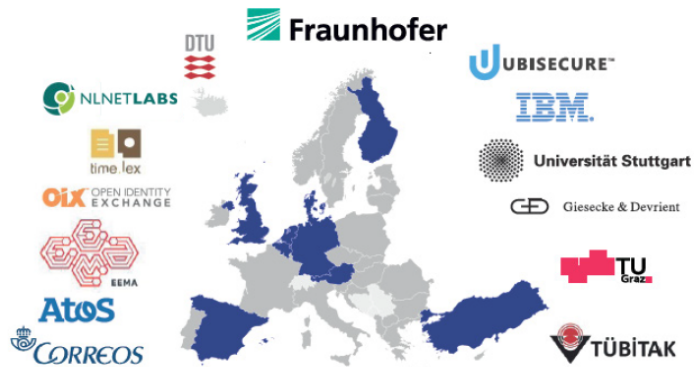
www.m4life.org

24 - 27 June 2018

Identiverse, Boston, USA

www.identiverse.com

The LIGHTest Project Partners



Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (7)	Page:	12 of 12
Dissemination:	PU	Version:	Version 1.00
		Status:	Final

