



## Report on Dissemination, Exploitation, and List of Technical Outcomes (12)

Document Identification	
<b>Date</b>	13.08.2019
<b>Status</b>	Final Draft
<b>Version</b>	Version 1.01

<b>Related WP</b>	WP11	<b>Related Deliverable(s)</b>	D11.14
<b>Lead Authors</b>	Lorraine Spector (EEMA)	<b>Dissemination Level</b>	PU
<b>Lead Participants</b>	EEMA	<b>Contributors</b>	FHG
<b>Reviewers</b>	FHG		

This document is issued within the frame and for the purpose of the LIGHT<sup>est</sup> project. LIGHT<sup>est</sup> 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.

<b>Document name:</b>	Report on Dissemination, Exploitation, and List of Technical Outcomes (12)		<b>Page:</b>	1 of 10	
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.01	<b>Status:</b>	Final Draft



## 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.

<b>Document name:</b>	Report on Dissemination, Exploitation, and List of Technical Outcomes (12)	<b>Page:</b>	2 of 10		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.01	<b>Status:</b>	Final Draft



## 2. Document Information

### Contributors

Name	Partner
Lorraine Spector	EEMA

### History

Version	Date	Author	Changes
1.00	13/8/2019	Jon Shamah	Final

<b>Document name:</b>	Report on Dissemination, Exploitation, and List of Technical Outcomes (12)	<b>Page:</b>	3 of 10		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.01	<b>Status:</b>	Final Draft



## 3. Table of Contents

1. Executive Summary	2
2. Document Information	3
Contributors.....	3
History .....	3
3. Table of Contents	4
4. Project Reference	5
5. LIGHTest Bulletin (12)	6
6. Project Description	9

<b>Document name:</b>	Report on Dissemination, Exploitation, and List of Technical Outcomes (12)	<b>Page:</b>	4 of 10		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.01	<b>Status:</b>	Final Draft



## 4. 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.

<b>Document name:</b>	Report on Dissemination, Exploitation, and List of Technical Outcomes (12)	<b>Page:</b>	5 of 10		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.01	<b>Status:</b>	Final Draft



## 5. LIGHTest Bulletin (12)

**Newsletter**  
Edition 12  
August 2019

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

  

### The LIGHTest e-Procurement Pilot and PEPPOL

Pan-European Public Procurement On-Line – or PEPPOL for short – was a project funded in part by the European Commission aiming to provide the technical standards to enable businesses to participate electronically in procurement of all European government institutions in a uniform way. The project ran from 2008 to 2012. Today, PEPPOL is in use in 16 European countries, some of which have made its use mandatory. The project is now overseen by OpenPEPPOL AISBL, a not-for-profit organisation based in Belgium. It has around 250 members from across Europe, both governmental agencies as well as vendors and service providers.

PEPPOL does not constitute an e-procurement platform of its own but rather provides the technical and legal means to allow interoperation between existing platforms. Specifically, it provides three components:

Free to choose ANY Access Point in ANY country

Sign ONE Agreement; Connect to ALL

Open FOUR-Corner Model

NO ROAMING fees between PEPPOL Access Points

*Figure 1. PEPPOL Architecture*

- The PEPPOL e-Delivery Network, a network for securely and reliably exchanging messages between participating entities,
- PEPPOL 'BIS' Specification, a specification of standardized document formats for procurement processes, and
- PEPPOL Transport Infrastructure Agreements (TIA), providing the legal framework for communication between the many connected parties.

The LIGHTest e-Procurement Pilot focuses on the e-delivery network.

This network operates on an open four-corner model, shown in Figure 1. In this model, each organisation participating in PEPPOL chooses an access point that acts on their behalf for sending and receiving messages via the delivery network. Communication between an organisation and their access point

<b>Document name:</b>	Report on Dissemination, Exploitation, and List of Technical Outcomes (12)	<b>Page:</b>	6 of 10
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.01
		<b>Status:</b>	Final Draft



is not regulated by PEPPOL and can happen in whatever form they agree on to accommodate existing systems or procedures. The access point makes sure that documents submitted are either already valid PEPPOL BIS documents or translates them. It then uses the PEPPOL e-delivery network to communicate with the access point chosen by the receiving organisation to deliver the document.

Two directories facilitate this delivery. First, each organisation publishes their receiving capabilities, contact information, and other information through a Service Metadata Publisher (SMP). This publisher is typically operated by the access point directly. To find the SMP responsible for a given organisation, a centralised directory, the Service Metadata Locator (SML) is employed.

#### PEPPOL and LIGHTest

To ensure security and integrity of the network, PEPPOL heavily relies on public key infrastructure (PKI). All access points and SMP providers receive a digital certificate which they use to identify themselves in communication. These certificates are created based on trusted certificate authority (CA) operated by PEPPOL itself. Currently, verification in the network relies on distributing the CA and intermediary certificates between all access points. With LIGHTest, this strict single-root infrastructure can be replaced with a model where

multiple CAs are authorised to create certificates through membership in a trust scheme. In addition, as PEPPOL BIS documents are signed ASIC containers, LIGHTest's Automatic Trust Verifier (ATV) can directly be used by access points and organisations to verify trust into the sender or certain attributes atop the existing PEPPOL network without any changes.

#### The Demonstration Scenario

The pilot will demonstrate the use of LIGHTest technology in a cross-border, healthcare scenario. There will be a fictitious sender named German Medical Device Company in Germany that will send an invoice to French Hospital, a hospital in France for 200 insulin pumps over the PEPPOL network, using the PEPPOL specifications. Preparing and signing message according to the PEPPOL specifications is complex and the German Medical Device Company will delegate the packaging and signing of their invoices.

In the scenario, French Hospital will verify the authenticity of the invoice using LIGHTest technology (Trust Scheme Publication, WP3, and Automatic Trust Verification, WP6) and acknowledge the receipt of the invoice to the sender as specified in the PEPPOL specifications. This is a multi-step process involving multiple message flows. Many of the steps have trust operations and all trust operations

(other than TLS 1.2 authentication) will be done using LIGHTest technology. Furthermore, all trust configuration for the steps will be done with the Policy Authoring and Visualisation Tools (WP6).

Extract from LIGHTest deliverable D9.5.

### LIGHTest Developer's Workshop

The LIGHTest Developer's Workshop was organised by TUBITAK at Shangri-La Bosphorus, Istanbul on 9th and 10th July 2019, with the contribution of project partners involved in the development of LIGHTest components and piloting.



LIGHTest Developers Workshop



Gala Dinner at Lacivert, Bosphorus, Istanbul

### The LIGHTest International Forum Workshop

From 27th – 30th May, a delegation from LIGHTest (Heiko Roßnagel from Fraunhofer; Rachele Sellung, Sven Wagner and Stephanie Weinhardt, from The University of Stuttgart; Stefan More and Lukas Alber from TU Graz) hosted the LIGHTest International Forum Workshop in Baku, Azerbaijan.

The three-day event began with an introduction to the project and a close look at trust infrastructures and how they are developing digitalisation. Highlights from the workshop included sessions focusing on:

#### Usability of Trust Policy Authoring Tools - Concept, Design and Evaluation

Usability of policy authoring tools remains a challenge. However, in a user study, delegates were shown how LIGHTest offers a new approach which has been developed based on a mental concept as opposed to design guidelines.

#### Trust Scheme Publication Authority (TSPA)

The concept of the TSPA and the different possibilities of publishing trust schemes were presented. The TSPA

Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (12)	Page:	7 of 10
Dissemination:	PU	Version:	Version 1.01
		Status:	Final Draft



is one of the key components of the LIGHTest reference architecture and is used in every verification process of an electronic transaction.

Delegates were also introduced to the use of DNS to make trust scheme membership claims discoverable by a verifier in an automated way. Also in this session, proof of concepts (PoC) regarding how the TSPA and further components of the LIGHTest infrastructure can be used were demonstrated for two possible application fields: PoC for a Trust Scheme for UNHCR and PoC for a predictive maintenance use case for sensor data verification in the IoT.



### Automatic Trust Verification

This presentation featured an overview of the technical process of automated trust verification using LIGHTest.

During the session delegates took a user perspective of the process, starting from an electronic transaction received by the central Automated Trust Verifier (ATV) component. It was demonstrated how the ATV processes this electronic transaction and makes a decision about its trust. In addition, delegates were shown how the ATV utilises components such as a trust policy, as well as several other LIGHTest components.



Rashid Azizov, Tahir Mammadov, Elnar Asadov, Heiko Roßnagel

### LIGHTest Tutorial Session on Automatic Trust Verification, Publication, and Policies

A hands-on session using various aspects of the LIGHTest tool, trust schemes, and the Policy Authoring tool.



## EEMA Annual Conference 2019

An Interactive Boardroom Session focusing on LIGHTest and entitled 'Transforming the Way we see Trust' was hosted by EEMA, during its Annual Conference at Microsoft in London on 19th June.

The morning session was Chaired by Rachelle Sellung of University of Stuttgart, who provided the business perspective, alongside Hans Graux an Attorney-at-law and Partner at Timelex who shared the legal considerations, and Martin Hoffmann of NLnet Labs who provided high level technical insight.

### The LIGHTest Project Partners



Document name:	Report on Dissemination, Exploitation, and List of Technical Outcomes (12)	Page:	8 of 10
Dissemination:	PU	Version:	Version 1.01
		Status:	Final Draft





## 6. Project Description

### **LIGHT<sup>est</sup> 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<sup>est</sup> 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<sup>est</sup> 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<sup>est</sup> open source software to easily query this trust information to verify trust in simple signed documents or multi-faceted complex transactions.

The 40 month LIGHT<sup>est</sup> 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<sup>est</sup> consortium consists of 14 partners from 9 European countries and is coordinated by Fraunhofer-Gesellschaft. To reach out beyond Europe, LIGHT<sup>est</sup> attempts to build up a global community based on international standards and open source software.

<b>Document name:</b>	Report on Dissemination, Exploitation, and List of Technical Outcomes (12)	<b>Page:</b>	9 of 10		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.01	<b>Status:</b>	Final Draft



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), and UbiSecure (FI), and University of Piraeus Research Center (GR)

The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.

<b>Document name:</b>	Report on Dissemination, Exploitation, and List of Technical Outcomes (12)	<b>Page:</b>	10 of 10		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.01	<b>Status:</b>	Final Draft

