



## D11.8

Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)

Document Identification	
<b>Date</b>	30.11.2017
<b>Status</b>	Final
<b>Version</b>	Version 1.00

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

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>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)		<b>Page:</b>	1 of 14
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00	<b>Status:</b> 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.

<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	2 of 14		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00	<b>Status:</b>	Final



## 2. Document Information

### Contributors

Name	Partner
Lorraine Spector	EEMA
Heiko Roßnagel	FHG

### History

Version	Date	Author	Changes
V0.99	29/11/2017	LS	Initial Document
V1.00	30/11/2017	LS	Final Document

<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	3 of 14		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00	<b>Status:</b>	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 (5)	8

<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	4 of 14		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00	<b>Status:</b>	Final



## 4. 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 three-year LIGHT<sup>est</sup> project starts 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

<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	5 of 14		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00	<b>Status:</b>	Final



# Bulletin – A report on dissemination, exploitation and list of technical outcomes (5)



Europe, LIGHT<sup>est</sup> 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 Danmark (DK) and UbiSecure (former Globalsign) (FI). 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>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	6 of 14		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00	<b>Status:</b>	Final



## 5. Project Reference

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

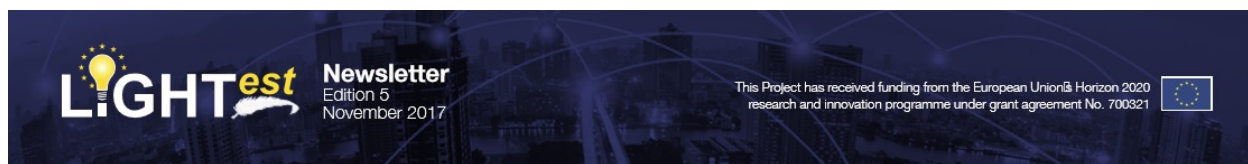
These deliverables are a series of bulletins describing relevant current dissemination outcomes and technical updates thus promoting internal communications.

The reports will be circulated as newsletter.

<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	7 of 14		
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00	<b>Status:</b>	Final



## 6. LIGHTest Bulletin (5)



### View from the Advisory Board - How do you explain LIGHTest?

Since meeting with the project team and some of its members in Graz, I found myself struggling with this. Not only at work, but also at some eIDAS-centric (electronic IDentification, Authentication and trust Services) meetings I attended, where people are talking about EU trusted services.

The main efforts of establishing a single digital market are directed at removing impediments for performing online cross-border transactions by qualifying e-ID, authentication, signatures and seals and find mechanisms such as eIDAS for accepting the qualifications.

Many people involved in this, think that eIDAS (and maybe also a project like FutureTrust) will generate all that is needed to achieve this - it facilitates qualified services and the only stuff needed to use it would be tooling for validation of these qualifiers. They're trying to convince software vendors to incorporate these validation mechanisms into their applications (operating systems, web browsers,

mail clients, document readers). Until full cooperation on this is gained, there's work on plug-ins and stand-alone applications for performing these checks and validations. If stuff turns green or shows a picture of a pretty seal or lock, it would prove qualification and establish trust.

What does it mean when something turns green? It shows you how you can trust a transaction. It typically shows validation that a coherent and consistent set of data has been established. This could be, for example, a document (proven unchanged) signed with a valid signature, based upon an identity (with specific attributes), issued by a qualified or recognised service provider and bound by a specific policy.

Where's the need for LIGHTest? What more would you possibly want? And please bear in mind that all this already is a huge amount of work to establish in itself.

What's still needed is a mechanism to show why a transaction can be trusted. A valid signature by an asserted person or organisation isn't enough. I'd really want to know whether I can trust both this asserted person and the entity or entities certifying the assertion



The Advisory Board members in Graz

and the signature. This sounds like highly personal preferences in trust, but in everyday business this mostly comes down to whether a person or organisation is qualified to make specific assertions. If the signature relates to a document, would the person or organisation signing that document be qualified to state whatever is in its content? And who vouches for this type of qualification?

Although this is almost inconceivable in the EU, not everyone will blindly trust eIDAS. Keep in mind that a person is not their e-ID and an organisation is not their certificate, however many qualifications you attach to them.

The General Meeting in Graz was a great experience to engage in all the perspectives that LIGHTest touches upon - a lot of technical stuff, many legal issues and a good deal of communication. Although the heart of the project is about getting stuff functioning and building it to work, maybe the toughest part will be conveying the value of the results, both during the project and after finishing it. I believe the Advisory Board should keep a special focus on this.

So, my question to you all is: How do you explain LIGHTest?

Author: Esther Makaay, Services Architect, SIDN, Netherlands

<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	8 of 14
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00
		<b>Status:</b>	Final





# Bulletin – A report on dissemination, exploitation and list of technical outcomes (5)



## Communicating the LIGHTest Message

LIGHTest is not like ordinary EU projects. From the outset, it was crafted for globally applicable, cross-sectorial impact - which makes it hard to explain. Nonetheless, the "Elevator Pitch" (a ten-second explanation) is critical to attract interest and ultimately build the longer-term LIGHTest community of users and developers.

General Elevator Pitch

LIGHTest provides transparency of the counterparty's scheme rules for decision-making regarding:

- Terms and conditions
- Security policies
- Authorisation policies
- Delegation policies

and any other published scheme rules.

LIGHTest does NOT issue, repeat or recommend rules, nor does it recommend risk decisions. What it DOES do is provide pointers to where the scheme information is published and tools to understand it.

LIGHTest does this GLOBALLY, piggybacking on existing deployed technologies such as DNS.

LIGHTest must be explained slightly differently to each of the three primary stakeholder groups: Legal; Business; and Technical. For this reason, a tri-channel approach has been created with separate messages and collateral, to provide sufficient relevancy.

Author: John Shamah,  
Chair, EEMA



## Business: LIGHTest facilitating the emerging market of cross-border trust services

LIGHTest allows you to use a global known and trusted infrastructure - the DNS, one of the corner stones of the Internet - to retrieve and verify identity information and determine trust assurances and policies behind it, so facilitating decision making. By better understanding the opportunities and risks, true operational costs can be assessed, and more robust decisions can be made. LIGHTest is providing essential tools for an emerging market.



## Legal: LIGHTest providing the ability to understand cross-border trust agreements

LIGHTest allows you to use a known and trusted global infrastructure - the DNS, one of the corner stones of the Internet - to retrieve and verify identity information and determine trust assurances behind it. LIGHTest can facilitate decision making in numerous contexts: is the person who they claim to be? Can they represent a company? Is a transaction legitimate? Can I trust a document? There are several legislative requirements which need to be taken into account including eIDAS, GDPR (General Data Protection Regulation) and BRIS (Business Registers Interconnection System) as well as a myriad of national laws, depending on use cases. The DNS focusses on enabling technically trustworthy communications, and LIGHTest allows you to build a solution around it that can ensure legal validity as well.



<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	9 of 14
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00
		<b>Status:</b>	Final



# Bulletin – A report on dissemination, exploitation and list of technical outcomes (5)



## Technical: LIGHTest providing the next generation of open-standards and technical trust tools

LIGHTest allows you to use a known and trusted global infrastructure to retrieve and verify identity information and determine trust assurances behind it, to facilitate decision making. LIGHTest creates a global standard method for trust-scheme discovery and trust-scheme verification, utilising DNS as the publication database. LIGHTest enables interoperability between existing frameworks, both cross-border, and cross-application, solving real problems that exist today.



## Project Partner Profile - TÜBİTAK BİLGEM

The Scientific & Technological Research Council of Turkey's (TÜBİTAK) Centre of Research for Informatics and Information Security, Advanced Technologies (BİLGEM) is the leading research institute fulfilling the demands of Turkey in the field of information security technology and electronics.

TÜBİTAK BİLGEM performs security and conformity tests of various communication systems and equipment to define new national standards and to improve the quality and the security of communication. The R&D studies in the field of e-identity and mobile identity proposed in the LIGHTest research project are the main areas of activity of the BİLGEM e-Identity Unit.

The project team has been involved in several EU research projects including FP7 STORK2.0, FP7



e-CODEX, FP7 INGRESS, FP7 BEAT, FP7 ORIGINS, FP7 e-SENS and FutureTrust, in the area of e-Identity, e-Signature, Trust Services, e-government and biometrics. Within LIGHTest, TÜBİTAK BİLGEM is responsible for rendering all software components seamlessly integrated, mature and robust. For this purpose, the methodology and tools of FP7 e-SENS Large Scale Pilot project are used. System integration and interoperability tests will be done with the Minder Testbed, which was developed by BİLGEM as part of the FP7 e-SENS project.

## Introducing the Minder Testbed

Minder is an execution platform that tests software modules in various aspects like conformance testing, interoperability testing, load testing etc. It is possible to test a module with other modules, as a whole system and individually.

It acts as an online programmable flow control engine that provides the capability of interconnecting different systems in one node and enabling architects to perform complex communication operations on those interconnected systems.

The Minder Project started late 2014 and initially focused on the e-SENS requirements. It was developed as an open source project to facilitate sustainable and reusable conformance and interoperability testing .

Later, it converged to a genuine fully generic domain testing platform which may be used to test simulated nodes in a connected network. The current version of Minder is V2.2-Sirius. Minder supports GITB service level compatibility. The minder source code is hosted under the GitHub repository .

Minder interconnects multiple systems through central nodes via adapters. The central nodes (i.e. the minder nodes) allow complex connectivity between the connected systems via test scripts.

Minder allows programmers to write tests scripts in MTDL (Minder Test Definition Language). A programmer can follow, check and manipulate the flow of information to verify that a certain task is being done in the right manner (i.e. against a specification for conformance testing).

In LIGHTest, Minder will act as an intermediate node that will intercept the communication between the ATV and the server components (TSP, TTS, DP). This comprehensive testing process will ensure that the deployed components work in harmony to satisfy the project requirements and use cases.

<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	10 of 14
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00
		<b>Status:</b>	Final



## Why Minder?

- More powerful than any of the known testbeds
- Generic, can be applied to most architectures
- Test scripts can be edited / changed, with no need for re-deployment
- Provides a development framework for creating adapters for any kind of system to communicate with Minder
- Proven quality, being actively used by the CEF eDelivery Service (<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+Conformance+testing>)
- Used for testing many different B2B vendors such as IBM, Flame, EESSI AS4.NET (full list: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSENS+AS4+conformant+solutions>)
- GITB compliant
- Can simulate a node in a network
  - A web service
  - A web service client
  - A node running some binary protocol (use adapters)
- Manage a testing environment by signaling/querying connected nodes
  - e.g. Minder/Kerkovi AS4 Architecture

Author: Dr. Oktay Adalier, eID Department Head, TÜBİTAK BİLGEM



## Trust Domains for Mobile ID Applications with LIGHTest

As the world is going more and more mobile, there is a growing need for mobile ID solutions supporting numerous use cases. Typical examples are e-government services, legally binding signatures, other public services and high-value e-commerce applications. In addition, many financial services are subject to regulation and therefore require trustworthy identity data as well. For these applications it is essential for the relying party to judge the assurance level of a presented identity or an identity attribute.

LIGHTest addresses these needs by designing a derived mobile ID concept that supports the propagation of assurance data throughout the process of identity derivation, storage of derived credentials and authentication to the relying party. The concept is based on the FIDO authentication protocol, enhanced with ID derivation assertions. Since the issuer of the primary identity, the ID derivation service, and the relying party can be part of different trust schemes, the whole environment becomes rather complex. At this point, LIGHTest can support the trust propagation of ID assurance by its core services like trust publication and trust translation. In addition, it allows the creation of trust domains with domain-specific trust information.

As an example, a specific authenticator used in a derived mobile ID scheme could be sufficient for authorisation of payment transactions, but may not be strong enough for e-government applications. With LIGHTest it is possible to create different domains (e.g. one for financial applications and one for e-government) that can publish different trust data to assess the level of assurance of this specific authenticator. Accordingly, a relying party can take the data received within the LIGHTest mobile ID scheme and look up trust information for its specific domain using the LIGHTest infrastructure. Trust domains can be regional domains (e.g. U.S., EU member states) as well as application domains (financial industries, e-government, retail etc.) or a hierarchical combination of regional and application domains.

Consequently, the LIGHTest infrastructure - in conjunction with the LIGHTest mobile ID scheme - offers a flexible framework to tailor sector-specific trust applications and to address the heterogeneous technologies in the mobile ecosystem in a flexible way.

Author: Dr. Frank-Michael Kamm, Technology Director R&D, Giesecke & Devrient Gesellschaft mit beschränkter Haftung, Germany



<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	11 of 14
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00
		<b>Status:</b>	Final



# Bulletin – A report on dissemination, exploitation and list of technical outcomes (5)



Newsletter Edition 5 November 2017

**WP2 Summary**

**Title: Requirements, Concepts and Evaluation**

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

T2.3 Formal Description: the formal basis of the project is to define the trust policy language TPL for specifying trust schemes, trust translation schemes, and delegation schemes.

The first deliverable D2.3 has been submitted in August as planned. This task is now augmented by a work on accountability.

T2.5 DNSSEC summarizes the most important standard the project works on and the corresponding deliverable D2.7 has been submitted.

Tasks T2.9 (Societal requirements) and T2.10 (Legal requirements) complement our set of requirements by the non-technical aspects, and the deliverables D2.9 and D2.10 have also been submitted.

DTU gave a presentation on the WP2 contents as part of the LIGHTest group at the EAB meeting in Darmstadt in September.

The next deliverables in this work package are due in August 2018.

**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 and T3.5. Deliverable 3.3 was kicked-off at the General Meeting in Graz and D3.6 (Cross-Border Legal Compliance and Validity of Trust Scheme Publication) was submitted in month 12.

In August, Heiko Roßnagel presented LIGHTest at the ARES conference in Reggio Calabria, Italy and the BIOSIG conference in Darmstadt, Germany. During November, he also spoke at the ISSE conference in Brussels and at the UNHCR workshop in Munich, which focused on leveraging digital identity opportunities for the benefit of refugees, forcibly displaced and stateless persons. Hans Graux also presented LIGHTest at the OIX Economics of Identity III event in London.

**WP4 Summary**

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

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

Ongoing progress of T4.2: Design of DNS-based Publication of Trust Translation Schemes.

The ToC and work assignment (regarding D4.3), for the rest of the partners are being discussed.

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

Meetings for T4.2 discussion. Open discussion on DNS-based publication for the three technical WPs (3,4 and 5)

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**

We are currently working on the DNS-based publication and the discovery of delegations. Our current view on the publication and the discovery for delegations is that DNS plays a minor role.

DNS is only used to identify the path to the Delegation Publisher component. The Delegation Publisher is then used for the future verification process. Deliverable 5.3 is due in month 18.

**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 for 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 that are due 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**

WP7 is currently focussing on task D7.3 where a demo ID derivation scheme is being implemented. The preparation of the implementation is ongoing with implementation work expected to start soon.

The work on D7.3 is currently on track and a first live demo, showing some core

@LIGHTest\_trust
 LinkedIn [click here](#)

[www.lighttest.eu](http://www.lighttest.eu)
Produced by EEMA - WP11 Lead, LIGHTest

<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	12 of 14
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00
		<b>Status:</b>	Final




Newsletter Edition 5 November 2017

---

parts of the functionality, is planned for the first review meeting in March 2018.

In parallel, the optimisation of software-based credential protection is continuing, by focussing on the resistance against side channel attacks.

**WP8 Summary**

**Title: Integration and Testing**

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

WP8 roadmap and status was presented at the General Meeting. A draft for D8.6 has been created and shared with related partners for the review. It will be released in M16.

**WP10 Summary**

**Title: Transfer to Market**

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

Preparation for the D10.3 (M15): Exploitation Plan and Report (M15) that belongs to the task 10.2.

Managing all the partner work assigned to the task.

**WP11 Summary**

**Title: Dissemination and Communication**

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

Continued promotion of LIGHT<sup>est</sup> throughout the EU and beyond. The LIGHT<sup>est</sup> community website continues to be populated and mature. Events attended included:

- ARES project Conference on Identity Fraud (Italy) <https://www.ares-conference.eu/workshops/cite-2017/>
- European Association for Biometrics (on Trusted biometrics) (Germany) <http://eab.org/events/program/122?ts=1501494814456>
- OID Summit (Sweden) <https://oid2017.hotell.kau.se/>
- World eID (France) <http://www.world-idandcybersecurity.com/>
- ISSE 2017 (Belgium) <http://www.isse.eu.com>

WP11 has been working with WP10 to produce a robust sustainable business plan and WP11 messaging.

### LIGHT<sup>est</sup> at EEMA'S ISSE Conference 2017




LIGHT<sup>est</sup> at EEMA'S ISSE 2017

 @LIGHTest\_trust
  [LinkedIn click here](#)

[www.lighttest.eu](http://www.lighttest.eu)

Produced by EEMA - WP11 Lead, LIGHT<sup>est</sup>

<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	13 of 14
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00
		<b>Status:</b>	Final

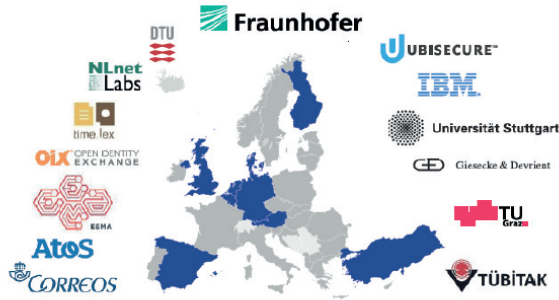




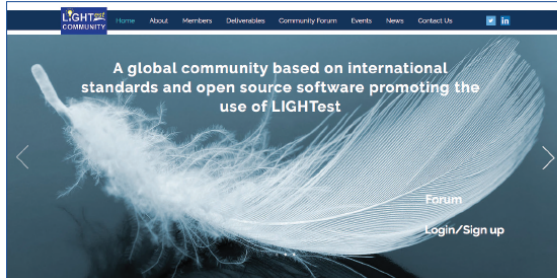
# Bulletin – A report on dissemination, exploitation and list of technical outcomes (5)



## The LIGHTest Project Partners



## The LIGHTest Community Blog

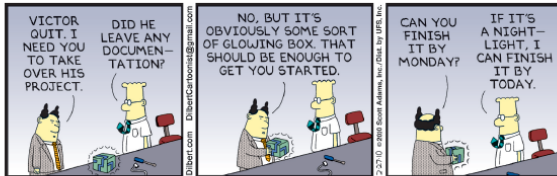


Welcome to the LIGHTest Community Website; a global community based on international standards and open source software promoting the use of LIGHTest. Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Stakeholders and Trust schemes.

This community website encourages associate partners to communicate on our forum as well as disseminate the latest LIGHTest news.

**Formal Description and Analysis of Concepts**  
<http://www.lightest-community.org/formaldescriptionandanalysis>

**Relevant DNSSEC Concepts and Basic Building Blocks**  
<http://www.lightest-community.org/dnssecconceptsandbasicbuildingblocks>



<b>Document name:</b>	Bulletin: A report on dissemination, exploitation and list of technical outcomes (5)	<b>Page:</b>	14 of 14
<b>Dissemination:</b>	PU	<b>Version:</b>	Version 1.00
		<b>Status:</b>	Final

