LIGHTest Newsletter
Edition 5
November 2017

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 - 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 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?

The Advisory Board members in Graz

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

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.

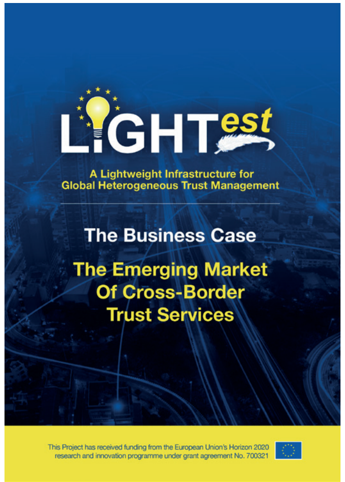
LIGHTest does this GLOBALLY, piggybacking on existing deployed technologies such as DNS.

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.



LIGHTest

A Lightweight Infrastructure for Global Heterogeneous Trust Management

The Business Case

The Emerging Market Of Cross-Border Trust Services

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

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.

LIGHTest

A Lightweight Infrastructure for Global Heterogeneous Trust Management

The Legal Perspective

Breaking New Ground in Cross-Border Trust Agreements

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

Technical: LIGHT^{est} providing the next generation of open-standards and technical trust tools

LIGHT^{est} 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. LIGHT^{est} creates a global standard method for trust-scheme discovery and trust-scheme verification, utilising DNS as the publication database. LIGHT^{est} enables interoperability between existing frameworks, both cross-border, and cross-application, solving real problems that exist today.

LIGHTest

A Lightweight Infrastructure for Global Heterogeneous Trust Management

The Technical Overview

The Next Generation of Open Standards and Technical Trust Tools

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

Project Partner Profile - TÜBİTAK BİLGEM

The Scientific & Technological Research Council of Turkey's (TÜBİTAK) Centre of Research for Informatics and Information Security, Advanced Technologies (BILGEM) 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 LIGHT^{est} research project are the main areas of activity of the BILGEM e-Identity Unit.

TÜBİTAK BİLGEM INFORMATICS AND INFORMATION SECURITY RESEARCH CENTER

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 LIGHT^{est}, 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 BILGEM 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 LIGHT^{est}, 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.

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/e-SENS+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 LIGHT^est^

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.

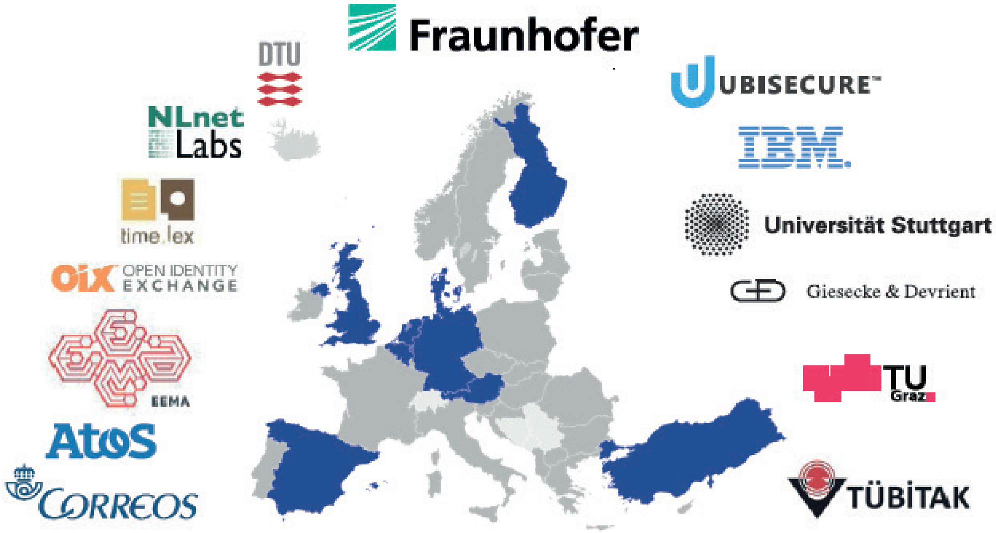
LIGHTest addresses these needs by designing a derived mobile ID concept that supports the propagation of assurance data throughout the process of identity derivation, storage of derived credentials and authentication to the relying party. The concept is based on the FIDO authentication protocol, enhanced 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

The LIGHT^{est} Project Partners



VICTOR QUIT. I NEED YOU TO TAKE OVER HIS PROJECT.
DID HE LEAVE ANY DOCUMENTATION?
NO, BUT IT'S OBVIOUSLY SOME SORT OF GLOWING BOX. THAT SHOULD BE ENOUGH TO GET YOU STARTED.
CAN YOU FINISH IT BY MONDAY?
IF IT'S A NIGHT-LIGHT, I CAN FINISH IT BY TODAY.
Dilbert.com DilbertCartoonist@gmail.com
2-27-10 ©2010 Scott Adams, Inc./Dist. by UFS, Inc.

The LIGHT^{est} Community Blog

LIGHTest COMMUNITY
Home
About
Members
Deliverables
Community Forum
Events
News
Contact Us
A global community based on international standards and open source software promoting the use of LIGHTest
Forum
Login/Sign up

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