LIGHTest
Newsletter
Edition 7 - External
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

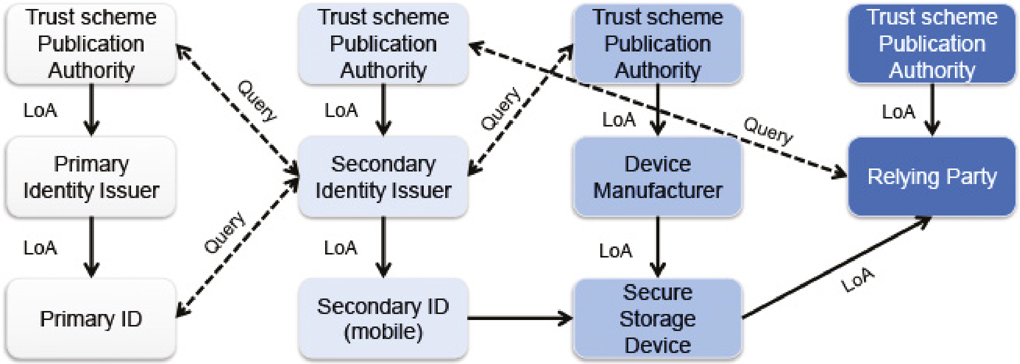

Trust scheme Publication Authority
Trust scheme Publication Authority
Trust scheme Publication Authority
Trust scheme Publication Authority
LoA
Query
LoA
Query
LoA
Query
LoA
Primary Identity Issuer
Secondary Identity Issuer
Device Manufacturer
Relying Party
LoA
Query
LoA
LoA
LoA
Primary ID
Secondary ID (mobile)
Secure Storage Device

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

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 malfeasant 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):

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 LIGHT^{est} 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 LIGHT^{est} 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
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

LIGHT^{est} Business Brochure, facilitating the emerging market of cross-border trust services

The LIGHT^{est} 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

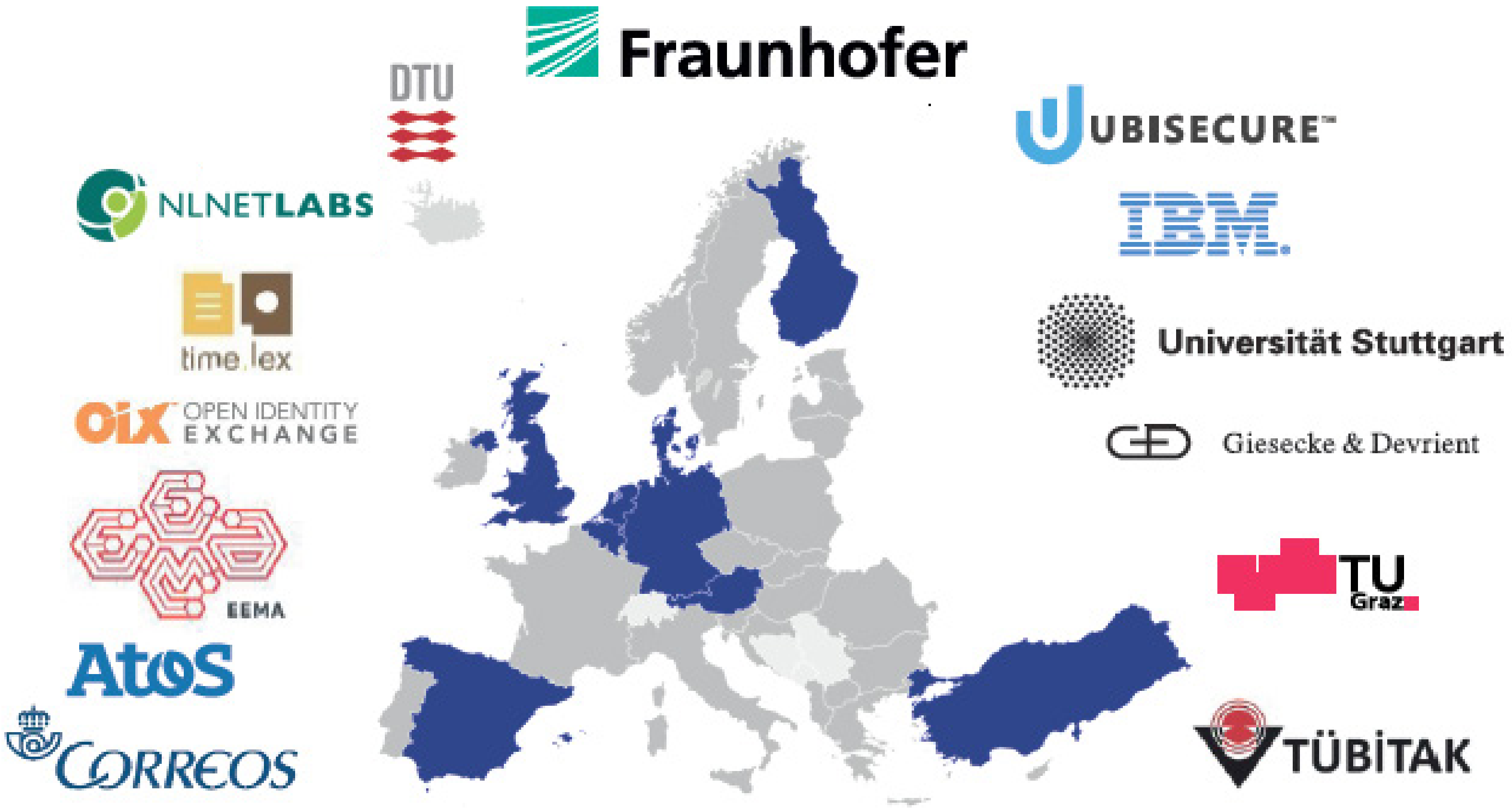
www.m4life.org

24 - 27 June 2018

Identiverse, Boston, USA

www.identiverse.com

The LIGHTest Project Partners



I ESTIMATED THE PROJECT TIMELINE BY ASSUMING THAT EVERY-ONE INVOLVED WILL WASTE ONE WEEK.
THAT'S A STUPID WAY TO DO A TIMELINE. SET UP A MEETING AND I'LL SHOW YOU HOW IT'S SUPPOSED TO BE DONE.
HE'S AVAILABLE IN A WEEK.

Dilbert.com DilbertCartoonist@gmail.com

5-13-11 ©2011 Scott Adams, Inc. Dist. by Universal Uclick