A Lightweight Infrastructure for Global Heterogeneous Trust Management

Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Stakeholders and Trust schemes

Open Identity Summit, Rome, October 13, 2016
Bud P. Bruegger (Fraunhofer IAO)
Peter Lipp (TU Graz)
Agenda

- European Project and Global Initiative (organizational)
- The Problem
- What LIGHT\textsuperscript{est} does
- Vision and Major Selling Point
- Going Global
- Invitation to Collaborate
LIGHT\textsuperscript{est} is a Global Initiative set up by an EU-Funded Project

Objective: Creation of a Global Trust Infrastructure

Global Initiative
- LIGHT\textsuperscript{est}-trust.{org, net, com}
- LIGHT\textsuperscript{est}.info

Global community open to all stakeholders
- builds a global community
- creates open standards
- provides open source software

EU Project
- LIGHT\textsuperscript{est}-trust.eu
- LIGHT\textsuperscript{est}.eu

LIGHT\textsuperscript{est} Consortium

Open invitation for collaboration to all interested stakeholders
- Any geographic region
- Any application field

LIGHT\textsuperscript{est} has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321.

Open Identity Summit, Rome, October 13, 2016
Bud P. Bruegger (Fraunhofer IAO)
Peter Lipp (TU Graz)
The European LIGHT\textsuperscript{est} Project

- Horizon 2020
- Innovation Action
- Call: H2020-DS-2015-1 \textit{Trust eServices}
- Starts September 1, 2016
- 36 months
- Estimated cost of 8.7 Mio Euros
- 14 partners from 9 countries
- Coordinated by Fraunhofer
Agenda

- European Project and Global Initiative (organizational)
- The Problem
- What LIGHT\textsuperscript{est} does
- Vision and Major Selling Point
- Going Global
- Invitation to Collaborate
Trust in a changing world

In the old days
- our world was smaller
- we knew our business partners
- Deals were sealed in personal contact

Increasingly
- we operate Europe- or World-wide
- we don’t know our business partners
- Deals are sealed remotely through Cyberspace
Transactions are increasingly conducted Virtually

We have virtual transactions with...

People  Organizations  Devices/Things
But who is really behind the electronic identity?

As expected from the appearance: **Trustworthy -- legitimate**
But who is really behind the electronic identity?

Not what we expect!!!

Untrustworthy -- fraud
How can we know whether a remote someone/something is trustworthy?

We need Help:

- Trusted Authorities
- Trusted Third Parties that publish Reputation Ratings
Agenda

- European Project and Global Initiative (organizational)
- The Problem
- **What LIGHTest does**
- Vision and Major Selling Point
- Going Global
- Invitation to Collaborate
The LIGHTest Architecture

Existing, Single Trust Root

Existing Governance, Organization, Infrastructure of DNS

Trust Scheme Publication Authority (WP3)
Trust Translation Authority (WP4)
Delegation Publisher (WP5)

Trust List

Policy Authoring and Visualization Tools (WP6)
Individual Trust Policy
Automatic Trust Verifier (WP6)

 verifier

Electronic Transaction

Assurance Levels

queries
The LIGHTest Architecture
DNS: The Internet Phone Book

- **Root Servers**
  2016: 558 DNS root server instances

- **Top-Level-Domain Name Servers**
  genericTDLs: com, org, edu, info... de, it, at, us, ca, ...

- **Most Organizations have existing Name Servers**
  ec.eu, gov.it, daimler.com, fraunhofer.de

- **Organization can define lower-level names**
  - Existing or dedicated name servers
  - trust.ec.eu, eIDAS.trust.ec.eu, signature.eIDAS.trust.ec.eu

---

Open Identity Summit, Rome, October 13, 2016

Bud P. Bruegger (Fraunhofer IAO)
Peter Lipp (TU Graz)

LIGHTest has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321
What does LIGHT$^{est}$ do? (WP3)

Infrastructure for Publication and Querying of Trust Schemes

- Create a global Standard Way for publishing Trust Lists.
- ..on a global Trust Infrastructure

- Across domains
- Accommodate diverse perceptions of trust
  - No global agreement needed

Authorities:
- EC and MS for qualified signature and trust services
- Business registers
- Professional registers (health, justice, law-enforcement, ..)
- Corporate internal registers
- …
What does LIGHT$^{est}$ do? (WP6)

Trust Policy and Automatic Trust Decisions

- Make it automatic for Verifiers to **query Trust Lists**
- Combine multiple queries to **validate**
  - an **Electronic Transaction**
  - against an easy to author **Trust Policy**

**Trust policy:**
List of Authorities that I trust, ...

**Trustworthy?**
(yes/no)

**Electronic Transaction**
e.g. signed document
What does LIGHT\textsuperscript{est} do? (WP5)

Infrastructure for the Publication and Querying of Delegations

Delegation:

- Organization publishes Trust List on..
- ..who can sign/act in its name for which purposes

Authorizes employees to act/sign in its name
What does LIGHTest do? (WP4)

Infrastructure for the Translation across Trust Domains

Authority publishes Trust List on:

- which authorities from other trust domains are trustworthy
- how to translate foreign into native trust schemes

- NIST: Level “3” == EC eIDAS: Level “substantial”

Bilateral agreements, etc.
What does LIGHT\textsuperscript{est} do? (WP7)

Trust Propagation of Derived Mobile IDs

- Trustworthy through secure enrollment
  - Birth and population registers
  - In person issuance
- Often unfit for mobile use
- Derive mobile identities from eIDs
- How does trust propagate???
- Currently lacks highly trusted electronic identities

Trust Propagation of Derived Mobile IDs
What does LIGHT\textsuperscript{est} do? (WP9)

Pilot Demonstrations

\textbf{e-Correos} (by Correos)

- Spanish Postal Service, one of largest world-wide
- electronic registered delivery service
- Identities of users
- Citizens and businesses receive official notifications from various administrations

\textbf{PEPPOL e-Invoicing} (by IBM)

- e-Invoicing in OpenPEPPOL environment
- Approach applicable to other PEPPOL applications
- Demonstrates easy of integration of LIGHT\textsuperscript{est} in existing product
- Demonstrates “delegation-enabling” an application with LIGHT\textsuperscript{est}.
Agenda

- European Project and Global Initiative (organizational)
- The Problem
- What LIGHT\textsuperscript{est} does
- Vision and Major Selling Point
- Going Global
- Invitation to Collaborate
The Vision of LIGHT\textsuperscript{est}

- Out of Reach:
  - Setting up and funding a global server infrastructure
  - Setting up a global organization (Registries)
  - Consensus on the Governance of a global Single Trust Root

- By using the existing Domain Name System:

\textbf{LIGHT\textsuperscript{est} is the ONLY possible way to create a global, cross-domain trust infrastructure}
THE Unique Selling Point

- A multitude of Trust Anchors is very difficult to provision
- LIGHT$^\text{est}$ uses the Single Trust Root of the DNS

The single trust root of LIGHT$^\text{est}$ brings multi-faceted trust decisions in the realm of the feasible
Agenda

- European Project and Global Initiative (organizational)
- The Problem
- What LIGHT\textsuperscript{est} does
- Vision and Major Selling Point
- Going Global
- Invitation to Collaborate
Going Global
Community Building

- We need to go beyond the limits of the Consortium
- Build up a global community around the vision of LIGHT\textsuperscript{est}
- Go “Viral”
Going Global Approach

- Global Players in the Consortium
  - OIX, GlobalSign, IBM
- Members of Existing Communities in Consortium
  - IETF Dane
- Advisory Board
- Associate Partners
- Loosely linked Web-based Community
Going Global
Community Based Dissemination

Empower the Community to Disseminate the LIGHTest Vision/Technology

- Open Source and (International) Open Standards
- Open Document Licenses for Dissemination Material
  - Empower Others to Disseminate the Vision
    - Adapt to new application fields
    - Translate
    - ...

Agenda

- European Project and Global Initiative (organizational)
- The Problem
- What LIGHTest does
- Vision and Major Selling Point
- Going Global
- Invitation to Collaborate
Invitation to Collaborate

First Focus: **Inventories**
- trust schemes and trust (status) lists
- trust list formats
- device attestation schemes
- delegation (mandate) schemes
- trust policies and policy languages
- trust translation schemes
- derivation schemes for mobile identities

Contact: Rachelle Sellung  <rachelle.sellung@iat.uni-stuttgart.de>

Later: An open, global LIGHTest Community..  (stay tuned)
Contact

- Bud P. Bruegger  
  <bud.bruegger@iao.fraunhofer.de>

- Peter Lipp 
  <peter.lipp@iaik.tugraz.at>

- Rachelle Sellung  (Inventories) 
  <rachelle.sellung@iat.uni-stuttgart.de>