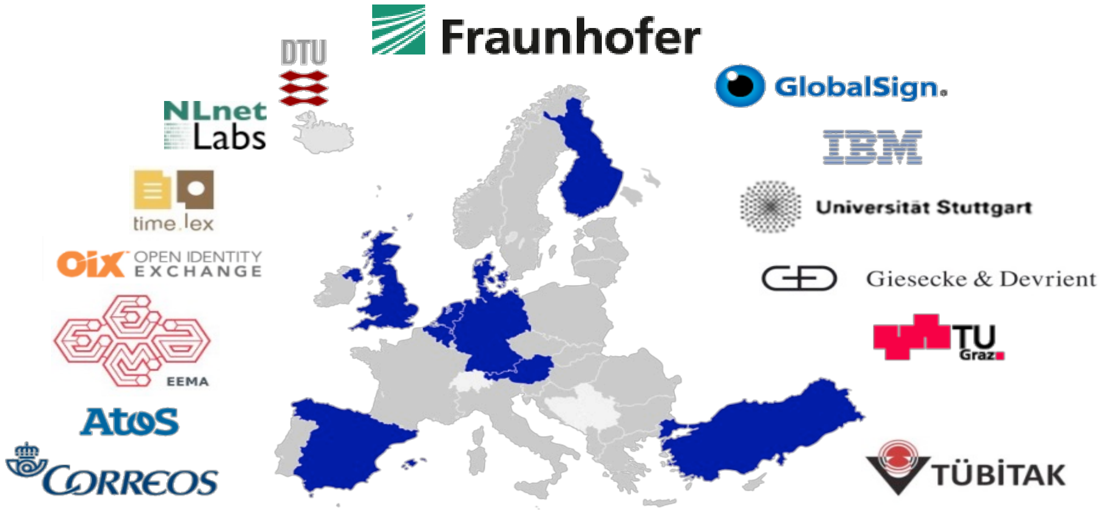
LIGHTest

Benno Overeinder, NLnet Labs

A Lightweight Infrastructure for Global Heterogeneous Trust Management



Lightweight **I**nfrastructure for **G**lobal **H**eterogeneous **T**rust management in support of an open **E**cosystem of **S**takeholders and **T**rust schemes

IRTF side meeting, Prague, CZ, July 17th, 2017

LIGHTest has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

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

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

Trust is a Diverse Creature

Authorities

- Governments for qualified signature and trust services
- Business registers
- Professional registers (health, justice, law-enforcement, ..)
- Corporate internal registers

Other user identification schemes

- Self-governed
- Reputation based

IoT device identification

LIGHTest has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

Automatically Verifying Trust

- Which trust schemes is the issuer a part of?
  - I can only check for schemes I know of.
  - For each scheme, I need to know where to find the trust lists.
- Does the trust scheme provide sufficient guarantees for my use case?
  - This is a difficult question for a machine!

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

What does LIGHT^{est} do?

Infrastructure for Publication and Querying of Trust Schemes

Create a global standard way for:

- Trust Scheme Discovery
  - how trust providers publish a claim to membership in a trust scheme,
- Trust Scheme Verification
  - how trust schemes publish their trust lists.

Utilize DNS as the basis for these publications

- verifiable via DNSSEC.

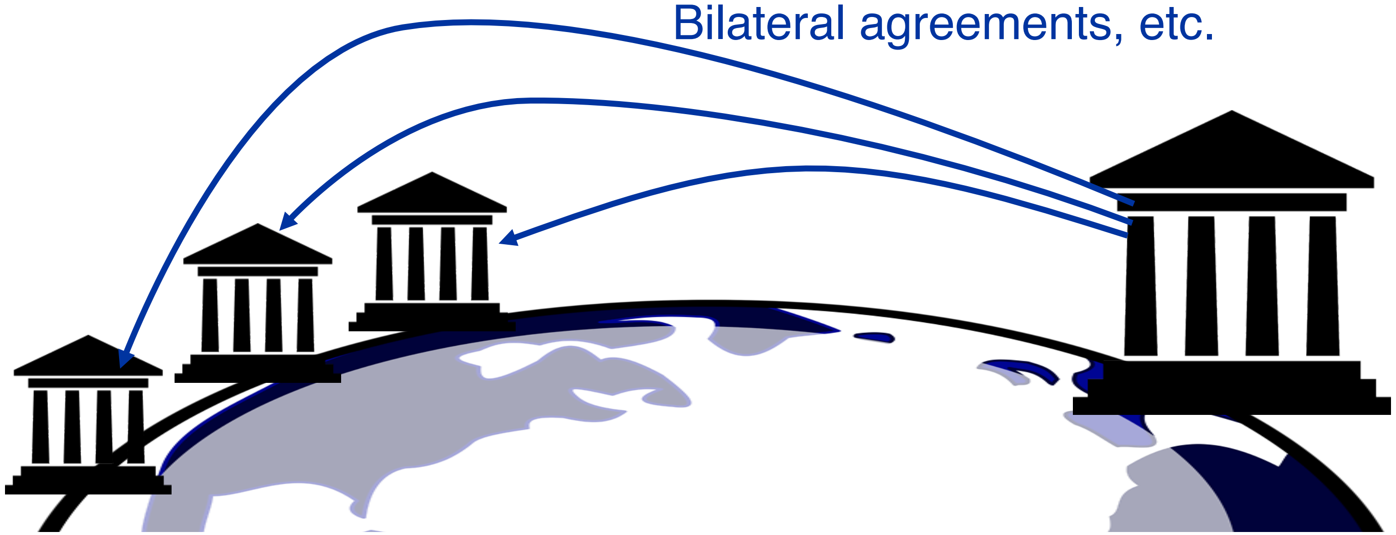
LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

What does LIGHT*est* do?

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”



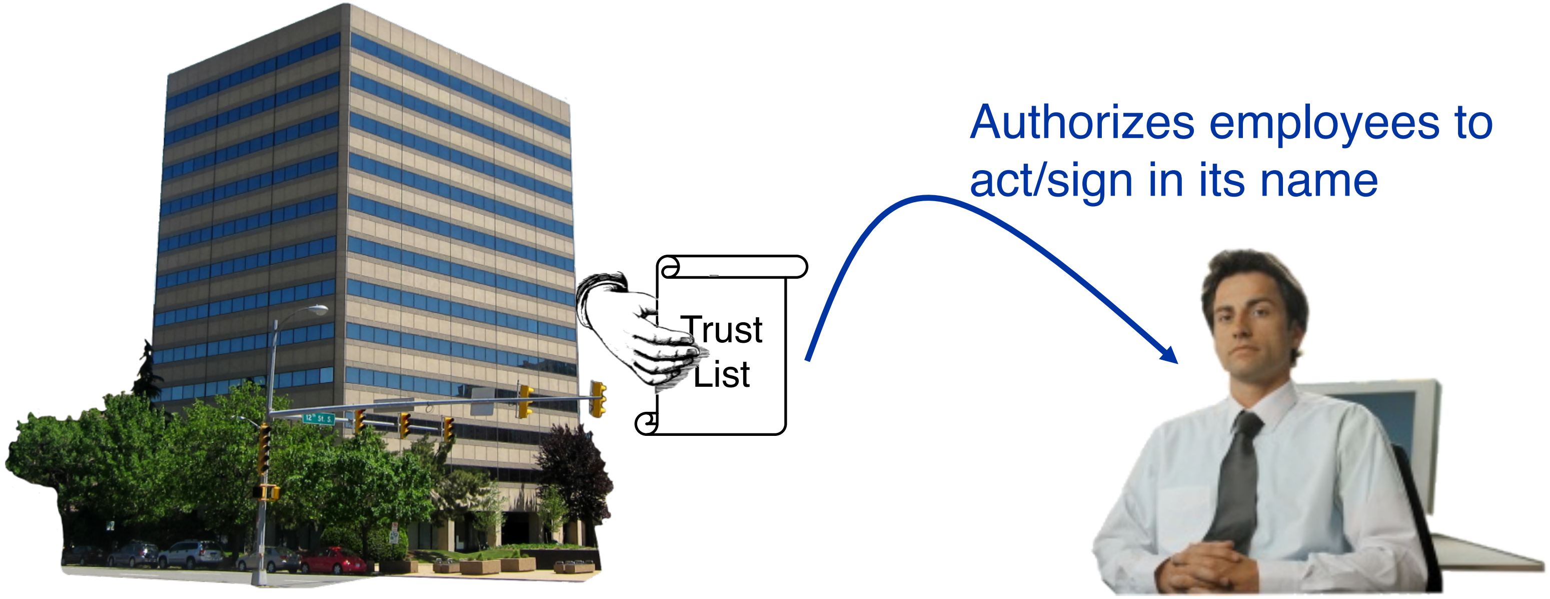
LIGHT*est* has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

What does LIGHT^{est} do?

Infrastructure for the Publication and Querying of Delegations

Delegation:

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



Trust List

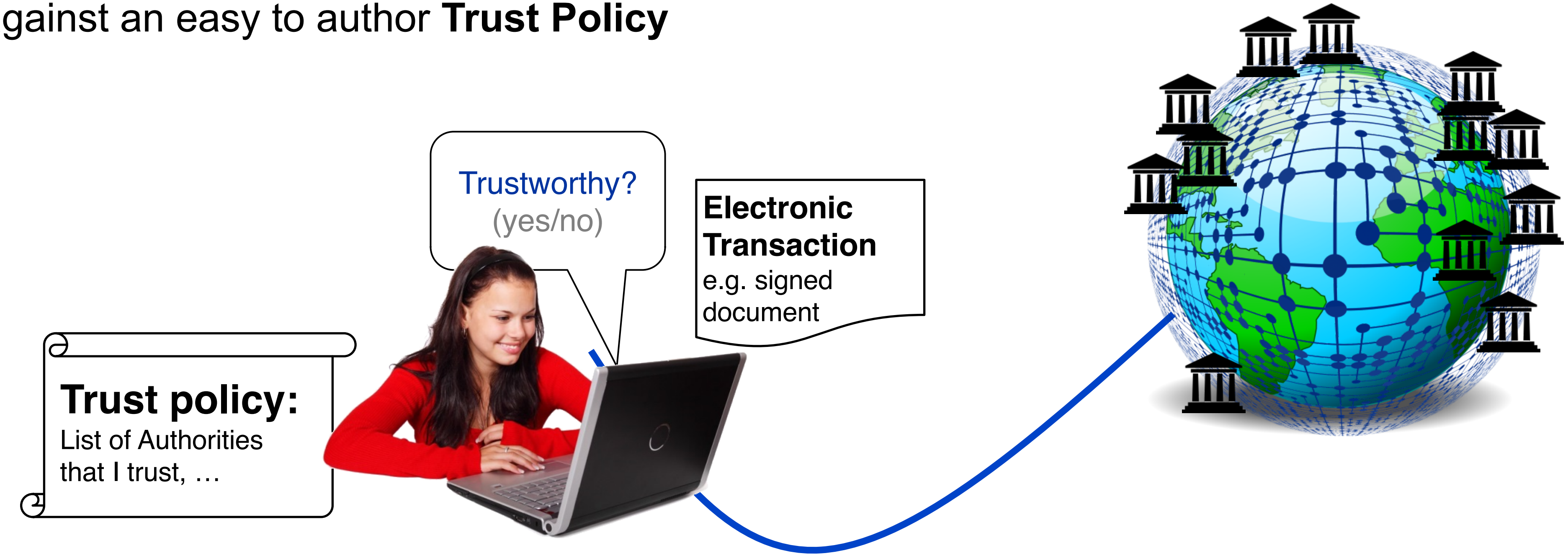
Authorizes employees to act/sign in its name

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

What does LIGHT*est* do?

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**



Trustworthy?
(yes/no)

Electronic Transaction
e.g. signed document

Trust policy:
List of Authorities that I trust, …

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

What does LIGHT^{est} do?

Trust Propagation of Derived Mobile IDs

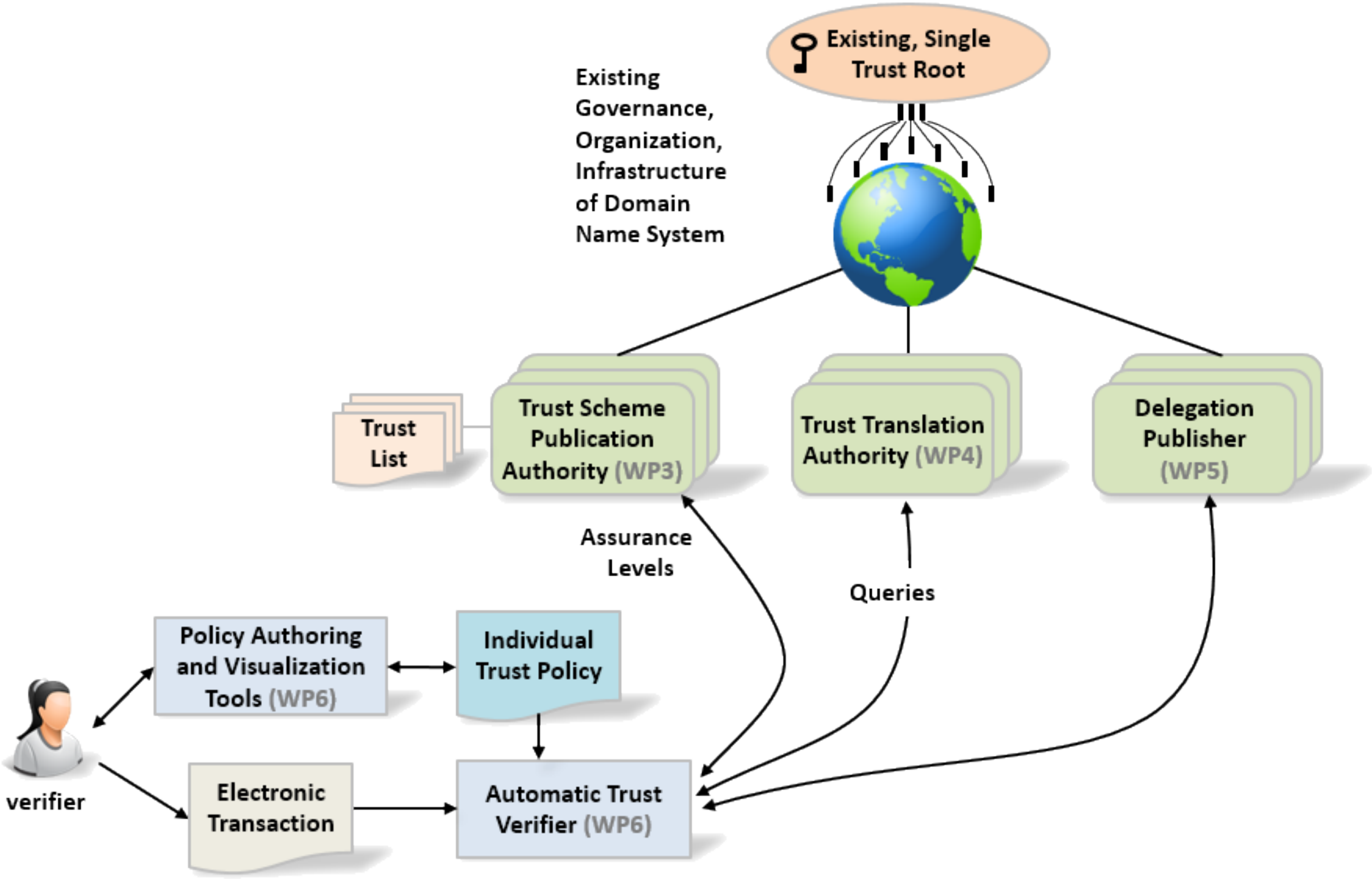
- Trustworthy through secure enrollment
  - Birth and population registers
  - in person issuance
- Often unfit for mobile use

- Derive mobile identities from eIDs
- How does trust propagate???

- Currently lacks highly trusted electronic identities

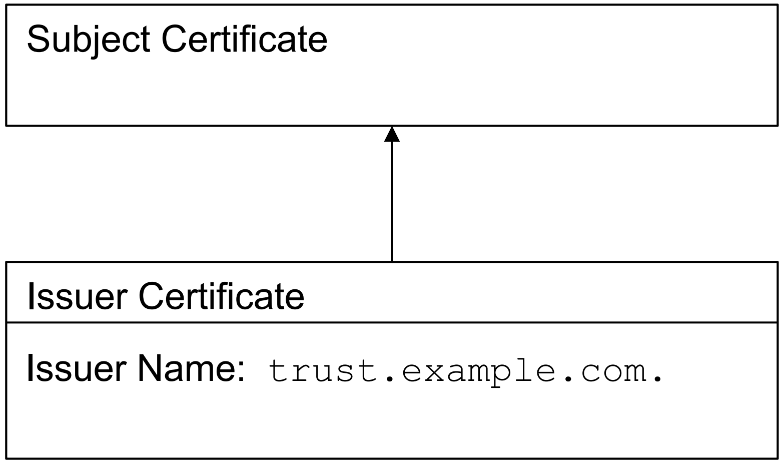
LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

The LIGHT^{est} Architecture


Existing, Single Trust Root
Existing Governance, Organization, Infrastructure of Domain Name System
Trust List
Trust Scheme Publication Authority (WP3)
Trust Translation Authority (WP4)
Delegation Publisher (WP5)
Assurance Levels
Queries
Policy Authoring and Visualization Tools (WP6)
Individual Trust Policy
verifier
Electronic Transaction
Automatic Trust Verifier (WP6)

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

Trust Scheme Discovery



DNS

`trust.example.com.`

- DANE-style publication of issuer certificate
- references to one or more trust scheme names
  - `scheme.example.com.`

LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Trust Scheme Verification

DNS

`scheme.example.com.`

- pointer to resource location of trust list

  `https://example.com/trust-scheme/list.xml`

- DANE/TLSA for authenticated transport encryption
- DANE-style publication of certificates used for signing the trust list

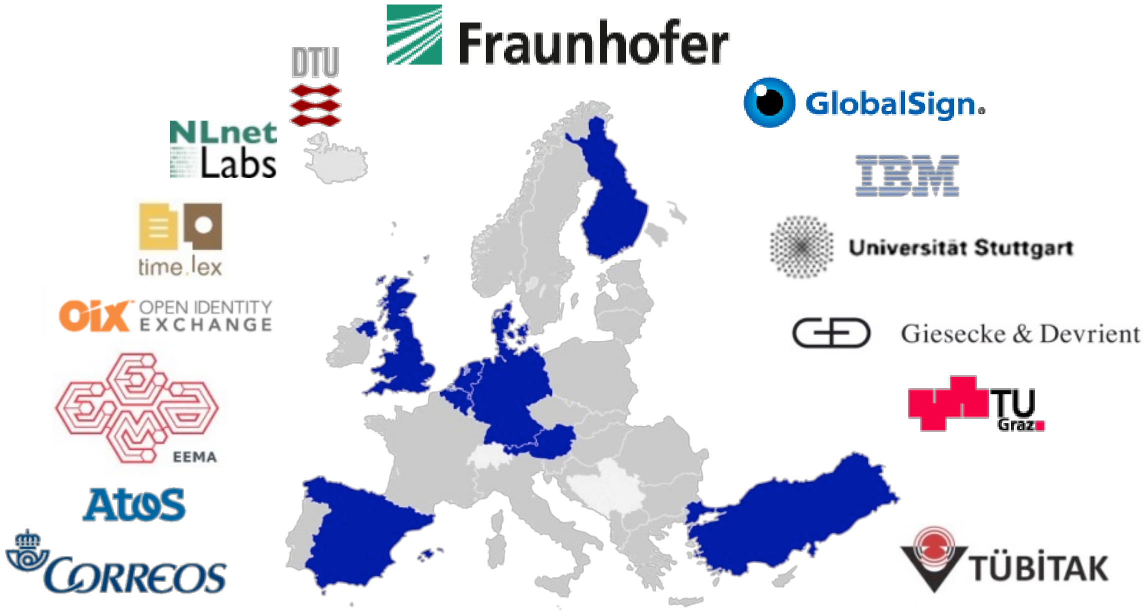
HTTPS

- Trust list in a standard format
  - reference to issuer certificate used by `trust.example.com.`

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

The European LIGHT^{est} Project

- Horizon 2020
- Innovation Action
- Call: H2020-DS-2015-1 *Trust eServices*
- Started September 1, 2016
- 36 months
- 14 partners from 9 countries
- Coordinated by Fraunhofer



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

Contact

Martin Hoffmann

NLnet Labs, Amsterdam

martin@NLnetLabs.nl

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