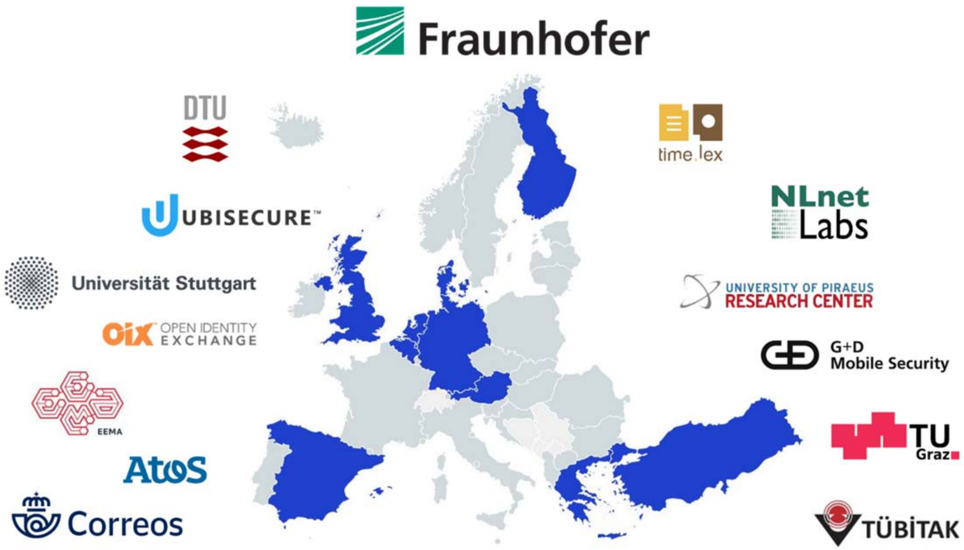
LIGHT*est*

A Lightweight Infrastructure for Global Heterogeneous Trust Management

Heiko Roßnagel, Fraunhofer IAO,
Sven Wagner, University Stuttgart, IAT

ITG Workshop on IT Security (ITSec),
Tübingen, April 2nd 2020



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

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

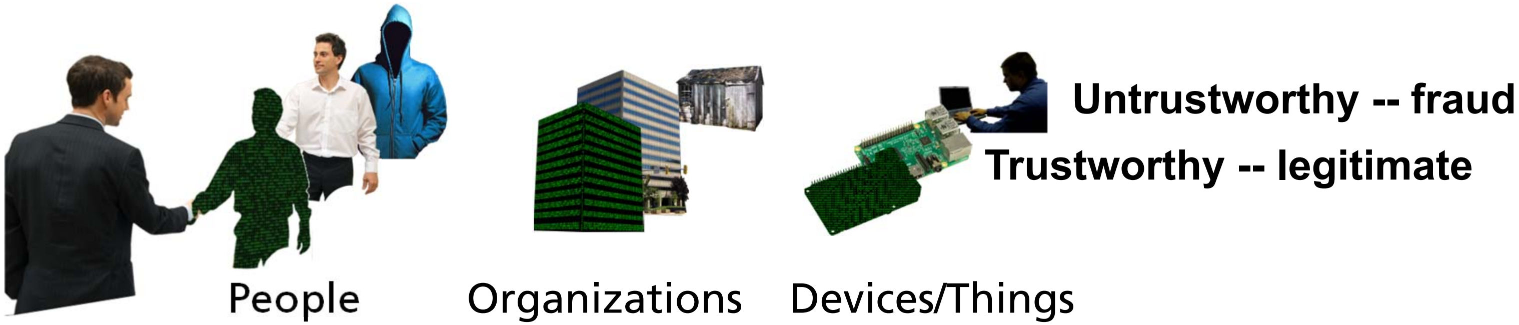
Agenda

- Motivation
- What does LIGHT*est* do?
- Reference Architecture
- Use Cases
- Summary

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

Trust in a changing world

- Transactions are increasingly conducted virtually



Untrustworthy -- fraud

Trustworthy -- legitimate

People Organizations Devices/Things

- How can we know whether a remote someone/something is trustworthy?
  - determine trustworthiness of involved parties
    - multitude of trust aspects and/or across borders, jurisdictions
- We need help:
  - Trusted Authorities
  - Trusted Third Parties that publish Reputation Ratings

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

Definitions

- Authorities
  - certify trustworthiness of eID of involved parties
  - operate Trust Schemes and publish Trust Lists

- Trust Scheme
  - comprises the organizational, regulatory/legal, and technical measures to assert trust-relevant attributes about enrolled entities in a given domain of trust
  - is operated by a Trust Scheme Provider

- Trust List
  - list of all the enrolled entities in a specific data file/format certified by the issuing authority
  - existing and widely accepted standard is ETSI TS 119 612

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 publishing Trust Lists..**
- **..on a global Trust Infrastructure**

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

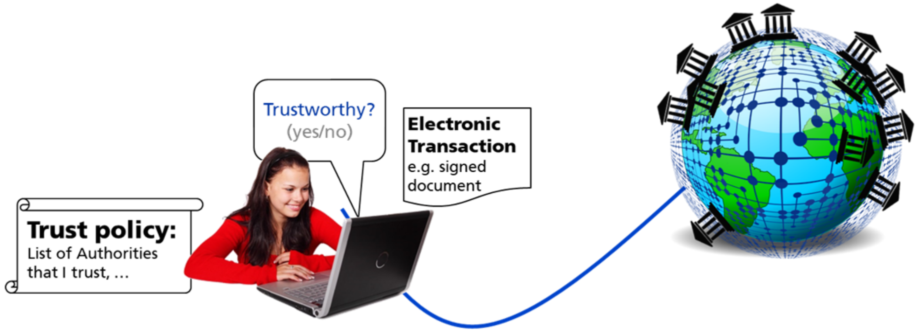
Authorities:

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

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

provide parties of electronic transactions with **automatic validation of trust** based on their **individual trust policies**



- Development of a lightweight, global trust infrastructure for
  - publication,
  - querying, and
  - cross-jurisdiction translation

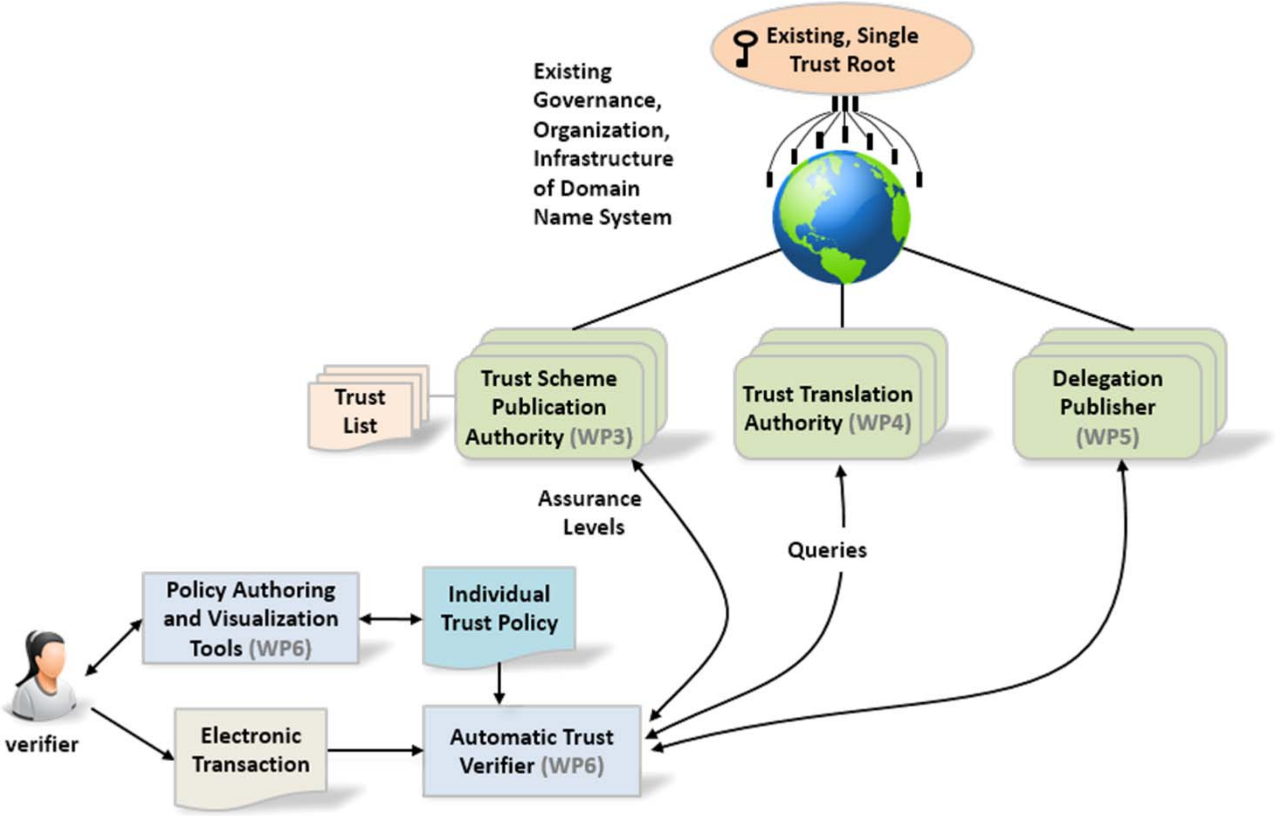
  of relevant information (e.g. trust scheme, level of assurance)
- using the existing **global Domain Name System (DNS)**

➢ Enables retrieval & discovery of ID information

➢ Facilitates your own decision making

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

LIGHT^{est} Reference Architecture



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

LIGHT^{est} Reference Architecture

Trust Scheme Publication Authority (TSPA)

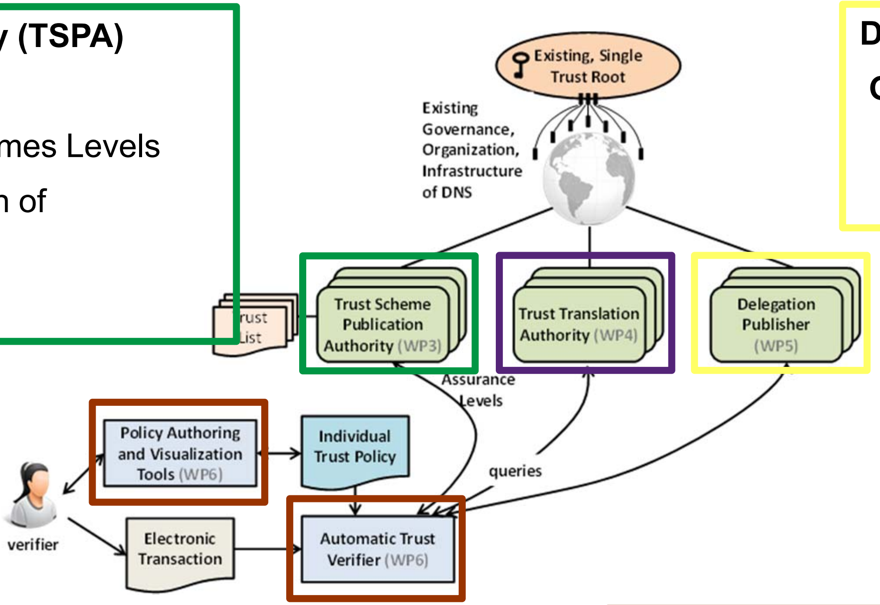
Goal: Provide an Infrastructure for

- Publication of Trust Schemes Levels
- Discovery and Verification of Trust Scheme Memberships

Delegation Provider (DP)

Goal: Provide an Infrastructure for

- Publication of Delegations
- Discovery of Delegations


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

Trust Policy Authoring Tool (TPAT)

Goal: Provide a GUI for

- Trust Policy Editing
- Support for expert- and non-expert users

Trust Translation Authority (TTA)

Goal: Provide an Infrastructure for

- Publication of Trust Schemes Levels Translations
- Discovery of those Translations

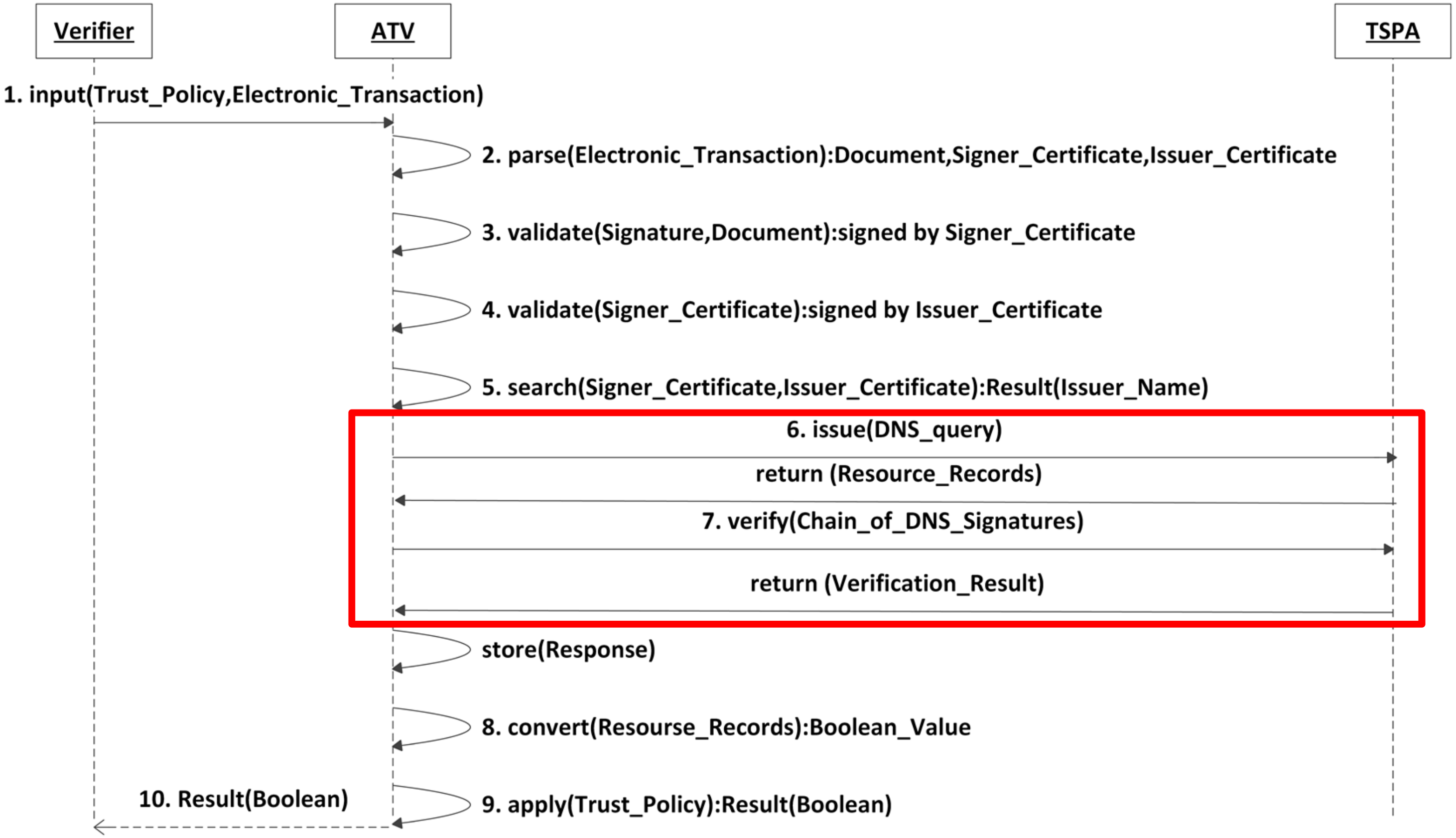
Automatic Trust Verifier (ATV)

Goal: Provide a Tool or Library for

- Gathering of Information from other Components
- Automated Verification of Electronic Transactions based on Trust Policies

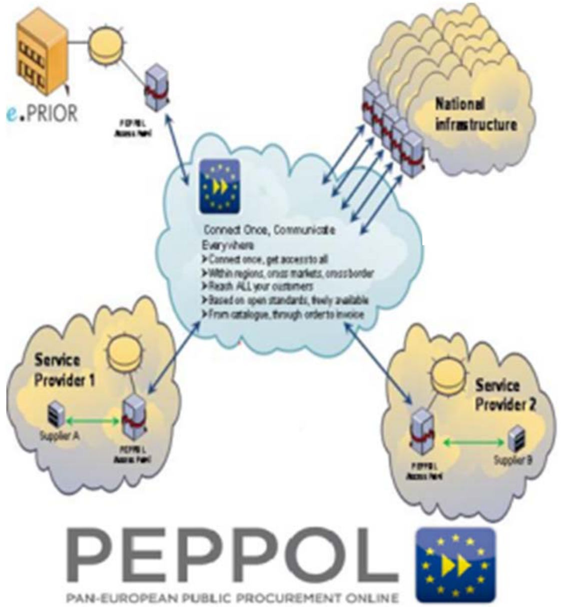
LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

LIGHT*est* : Information flow (high level)


Verifier
ATV
TSPA
1. input(Trust_Policy,Electronic_Transaction)
2. parse(Electronic_Transaction):Document,Signer_Certificate,Issuer_Certificate
3. validate(Signature,Document):signed by Signer_Certificate
4. validate(Signer_Certificate):signed by Issuer_Certificate
5. search(Signer_Certificate,Issuer_Certificate):Result(Issuer_Name)
6. issue(DNS_query)
return (Resource_Records)
7. verify(Chain_of_DNS_Signatures)
return (Verification_Result)
store(Response)
8. convert(Resourse_Records):Boolean_Value
10. Result(Boolean)
9. apply(Trust_Policy):Result(Boolean)

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

Use Cases: Pilots


e.PRIOR
PEPPOL Access Point
National infrastructure
Connect Once, Communicate Everywhere
➤Connect once, get access to all
➤Within regions, cross markets, cross border
➤Reach ALL your customers
➤Based on open standards, freely available
➤From catalogue, through order to invoice
Service Provider 1
Supplier A
PEPPOL Access Point
Service Provider 2
PEPPOL Access Point
Supplier B
PEPPOL
PAN-EUROPEAN PUBLIC PROCUREMENT ONLINE

PEPPOL e-Procurement

- Demonstrates integration of LIGHT*est* in an existing product
- Two pilot use cases

1. Trust establishment on eDelivery Access Points (APs)
    - update the PKI seamlessly using LIGHTest on a closed trust environment (key exchange of root certificates)
2. Trust establishment between pre-award Service Providers (SPs)
    - Using the LIGHTest infrastructure in a healthcare procurement scenario
    - Delegation verification between end users

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

Use Cases: Pilots

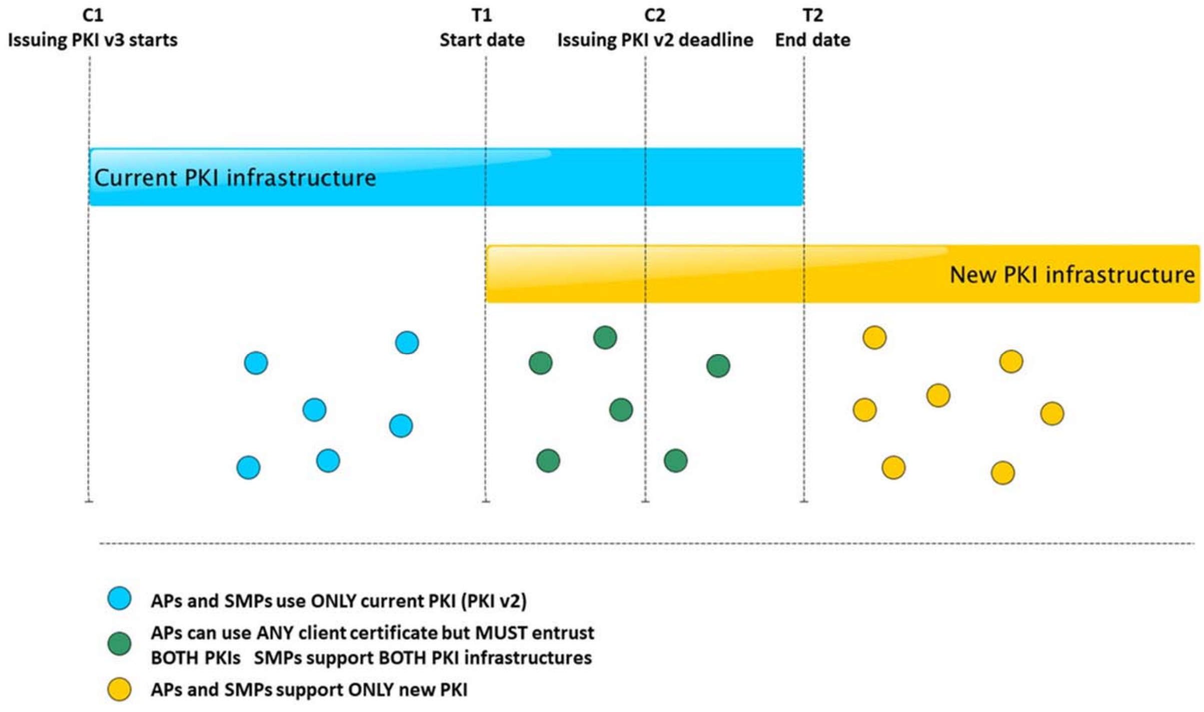
PEPPOL e-Procurement

Use Case 1:

- update the PKI seamlessly
- flexible and no downtime

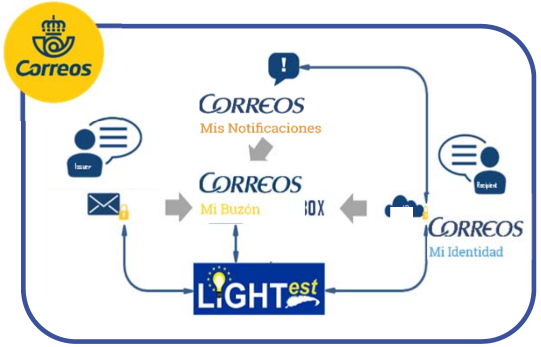
→ LIGHTest is used as a “Trust Scheme Migration Tool”

- migration time is reduced (6 months without to 1 month with LIGHTest)


C1
Issuing PKI v3 starts
T1
Start date
C2
Issuing PKI v2 deadline
T2
End date
Current PKI infrastructure
New PKI infrastructure
APs and SMPs use ONLY current PKI (PKI v2)
APs can use ANY client certificate but MUST entrust BOTH PKIs SMPs support BOTH PKI infrastructures
APs and SMPs support ONLY new PKI

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

Use Cases: Pilots



Correos: Trustworthy communications

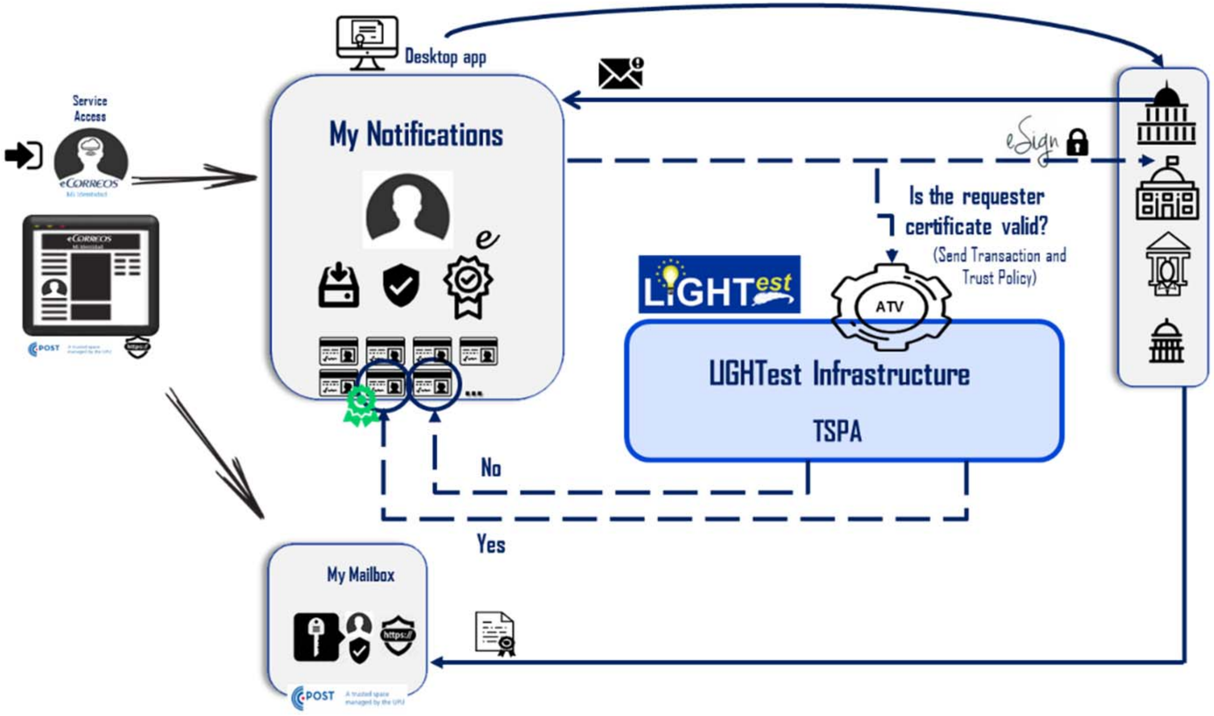
- Spanish Postal Service, one of largest world-wide
- Verified identities of users
- Trustworthy communications between different users (companies, individuals etc)
- Citizens and businesses receive official notifications from several administrations
- Two pilot use cases:
  - My Mailbox
  - My Notification

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

Use Cases: Pilots

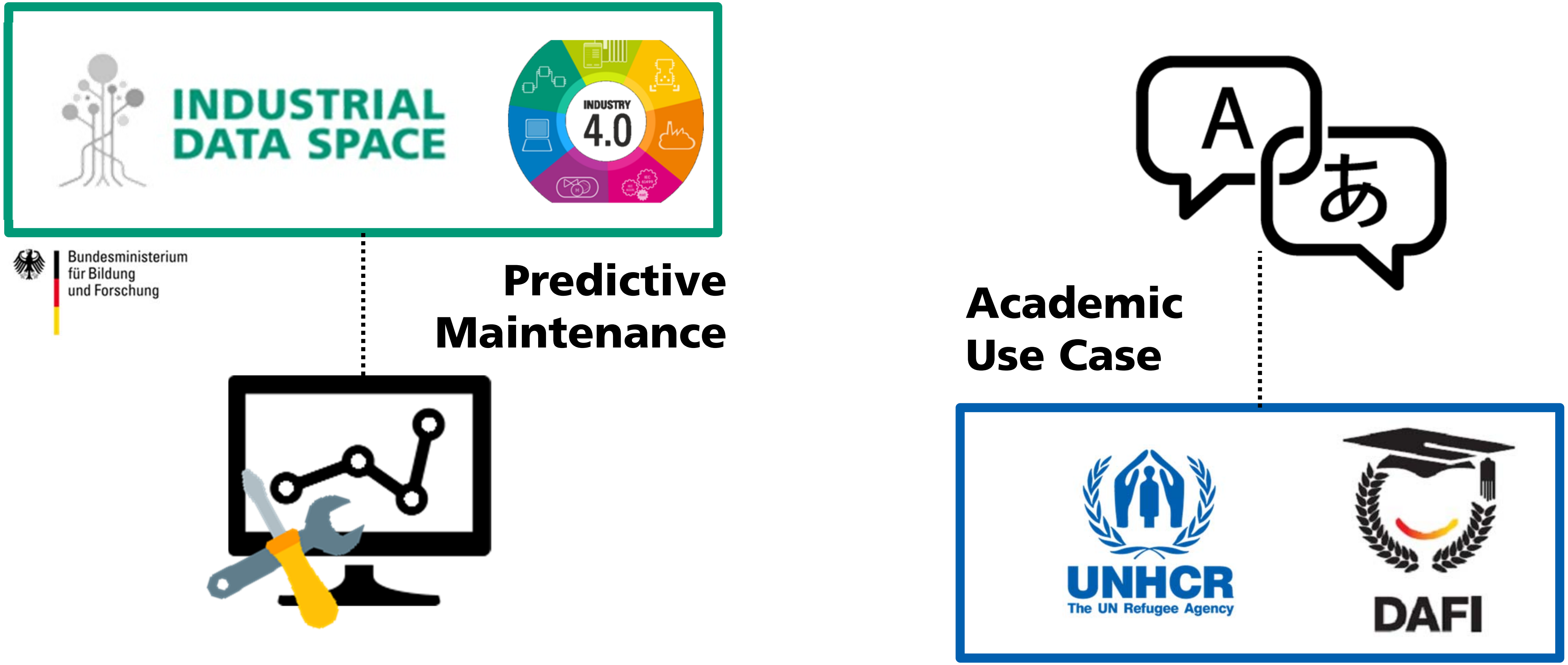
Correos: Trustworthy communications

- check eIDAS compliance of the signature from the request



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

Use Cases: further demonstrations



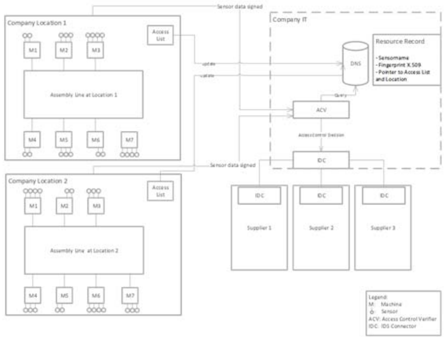
Predictive Maintenance

Academic Use Case

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

Use Cases: further demonstrations

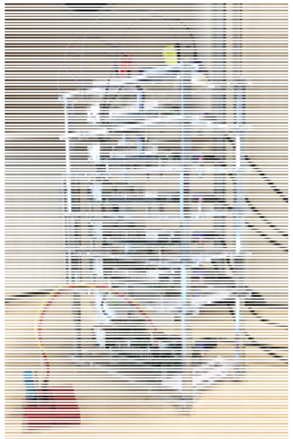
- Use case „end to end sensors”, scenario “predictive maintenance”
- **GOAL: Lightweigt Identity and Access Management using LIGHTest infrastructure**



- Key features:
  - decentralized access lists (sensor lists)
  - centralized access right location (policy for sensor data)

  → Good scalability for dynamic and large systems

- build a Raspi-Demonstration



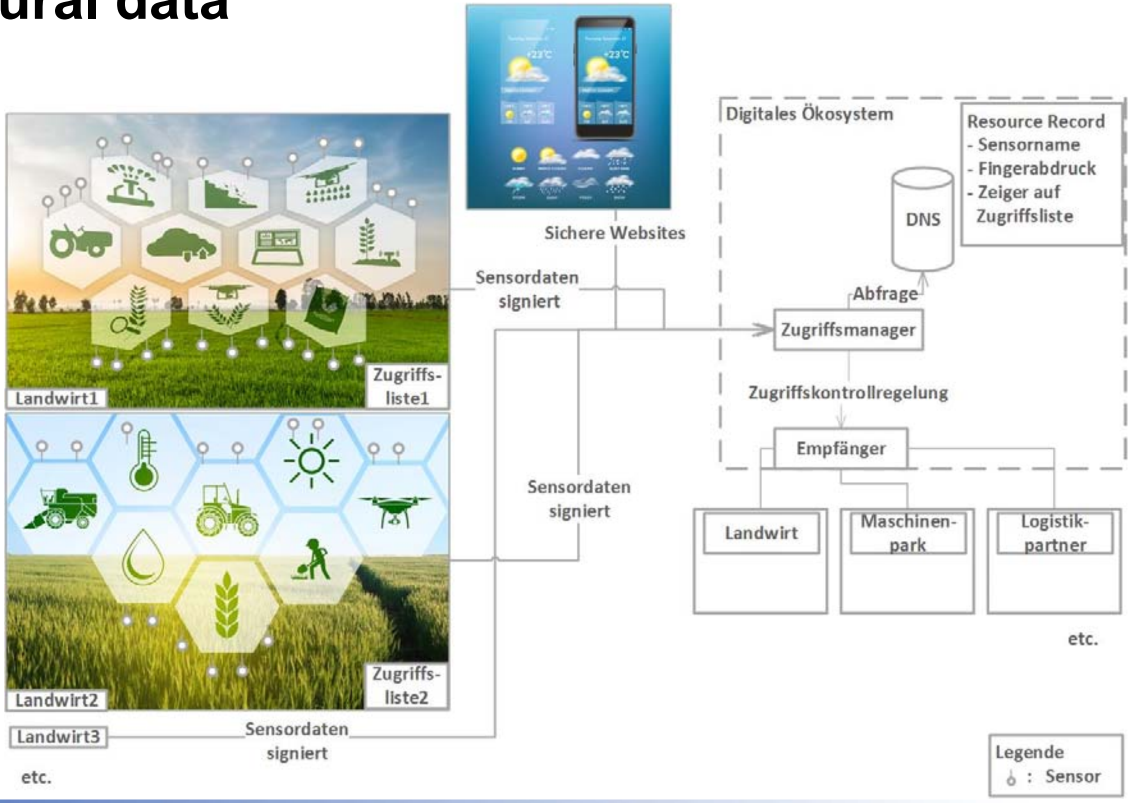
LIGHTest has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

Use Cases: further demonstrations

Lightweigth Identity and Access Management for a Digital Ecosystem for Agricultural data

- Smart Agriculture:
  - variety of different IoT sensors in use
  - plus WWW and satellite data

- Example: farmer network



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

The LIGHTest Cookbook

A step-by-step guide to deploying LIGHTest

(with accompanying demo)

THE LIGHT*est* COOKBOOK

LIGHT*est*, initially funded by the European Commission is 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. User organisations 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*est* open source software to easily query this trust information to verify trust in simple signed documents or multi-faceted complex transactions.

This is a simple step-by-step guide to establishing a framework demonstrating the basic rules of LIGHT*est* in an everyday ICT environment.

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

LIGHT*est*

THE LIGHT*est* COOKBOOK

A Practical Guide to deploying a Lightweight Infrastructure for Global Heterogeneous Trust Management

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

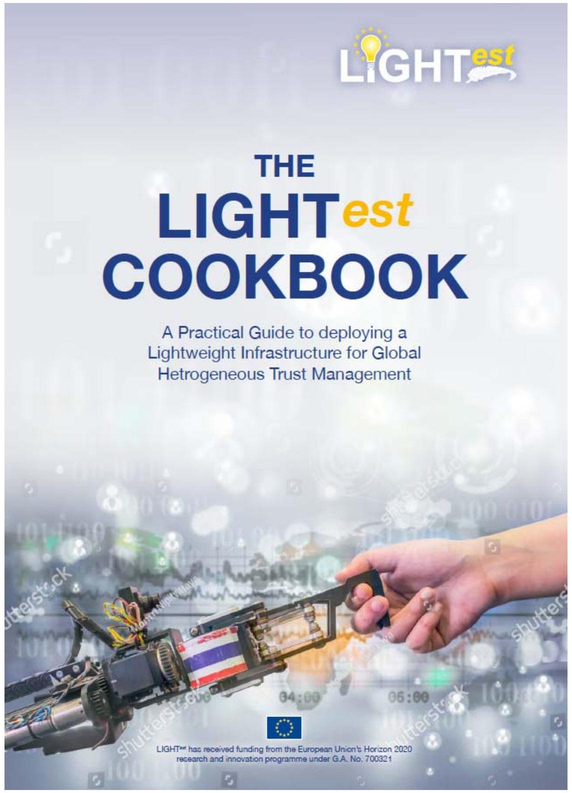
https://www.lightest.eu/static/lightest_cookbook/LIGHTest_Cookbook_v1.0.pdf

The LIGHTest Cookbook

Table of Content

- Benefits using LIGHTest
- An Introduction to LIGHTest in Action: **demo example**
- Overview of infrastructure
- **Installation instruction and examples for end-users and TSPs**
  - ATV, TSPA, TTA
- Policy Tool and ATV
  - **TPAT**: supports writing trust policies
- Use Cases and Examples
  - Open Peppol, Correos, mobile ID scheme using FIDO
- Beyond LIGHTest

→ **LIGHT^est^ helps you manage trust and risk in your business**



LIGHTest

THE LIGHTest COOKBOOK

A Practical Guide to deploying a Lightweight Infrastructure for Global Hetrogeneous Trust Management

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

45 pages

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

Summary

- There is a high need for assistance from authorities to certify trustworthy electronic identities

- LIGHTest project
  - global trust infrastructure based on DNS is built,
  - arbitrary authorities can publish their trust information using existing standards (trust lists)
  - supports automatic trust verification (ATV) on electronic transactions / incoming sensor sensor data

- Multitude of use cases where LIGHTest can support
  - verification of electronic documents (orders, receipts, etc)
  - sensor data validation in IoT and IIoT applications
  - international organizations (digitalization processes)

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

Contact

Dr. Heiko Roßnagel
Fraunhofer IAO

Nobelstr. 12
70569 Stuttgart

heiko.rossnagel@iao.fraunhofer.de

Dr. Sven Wagner
University Stuttgart IAT

Nobelstr. 12
70569 Stuttgart

sven.wagner@iat.uni-stuttgart.de

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

References

- Project webpage: http://lightest.eu/
- Community webpage: http://www.lightest-community.org/

- Papers:

- I.-H. Johnson-Jeyakumar, S. Wagner, H. Roßnagel, “Implementation of Distributed Light weight Trust infrastructure for automatic validation of faults in an IOT sensor network,” in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019.
- S. Mödersheim, B. Ni, “GTPL: A Graphical Trust Policy Language,” in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019.
- O. Omolola, S. More, E. Fasllija, G. Wagner, L. Alber, “Policy-based Access Control for the IoT and Smart Cities” in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019.
- G. Wagner, S. Wagner, S. More, M. Hoffmann, “DNS-based Trust Scheme Publication and Discovery,” in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019.
- S. Wagner, S. Kurowski, H. Roßnagel, “Unified Data Model for Tuple-Based Trust Scheme Publication,” in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019.
- S. Weinhardt, D. St. Pierre,”Lessons learned – Conducting a User Experience evaluation of a Trust Policy Authoring Tool, “ in Open Identity Summit 2019, H. Roßnagel, S. Wagner, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2019
- S. Wagner, A. Horch, B. Kilian, H. Roßnagel, „Leichtgewichtige Infrastruktur zur Schaffung von sicherheit und Vertrauen in einem digitalen Ökosystem für Agrardaten.“ in 38. GIL Jahrestagung, A. Ruckelshausen et al., Eds. Gesellschaft für Informatik, Bonn, 2018.
- G. Wagner, O. Omolola, S. More, “Harmonizing Delegation Data Formats” in Open Identity Summit 2017, L. Fritsch, H. Roßnagel, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2017.
- S. Wagner, S. Kurowski, U. Laufs, H. Roßnagel, “A Mechanism for Discovery and Verification of Trust Scheme Memberships: The Lightest Reference Architecture” in Open Identity Summit 2017, L. Fritsch, H. Roßnagel, D. Hühnlein, Eds. Gesellschaft für Informatik, Bonn, 2017.
- B.P. Bruegger, P. Lipp, “LIGHTest – A Lightweight Infrastructure for Global Heterogeneous Trust Management, ” in Open Identity Summit 2016, D. Hühnlein D. et al, Eds. Gesellschaft für Informatik, Bonn, 2016.

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