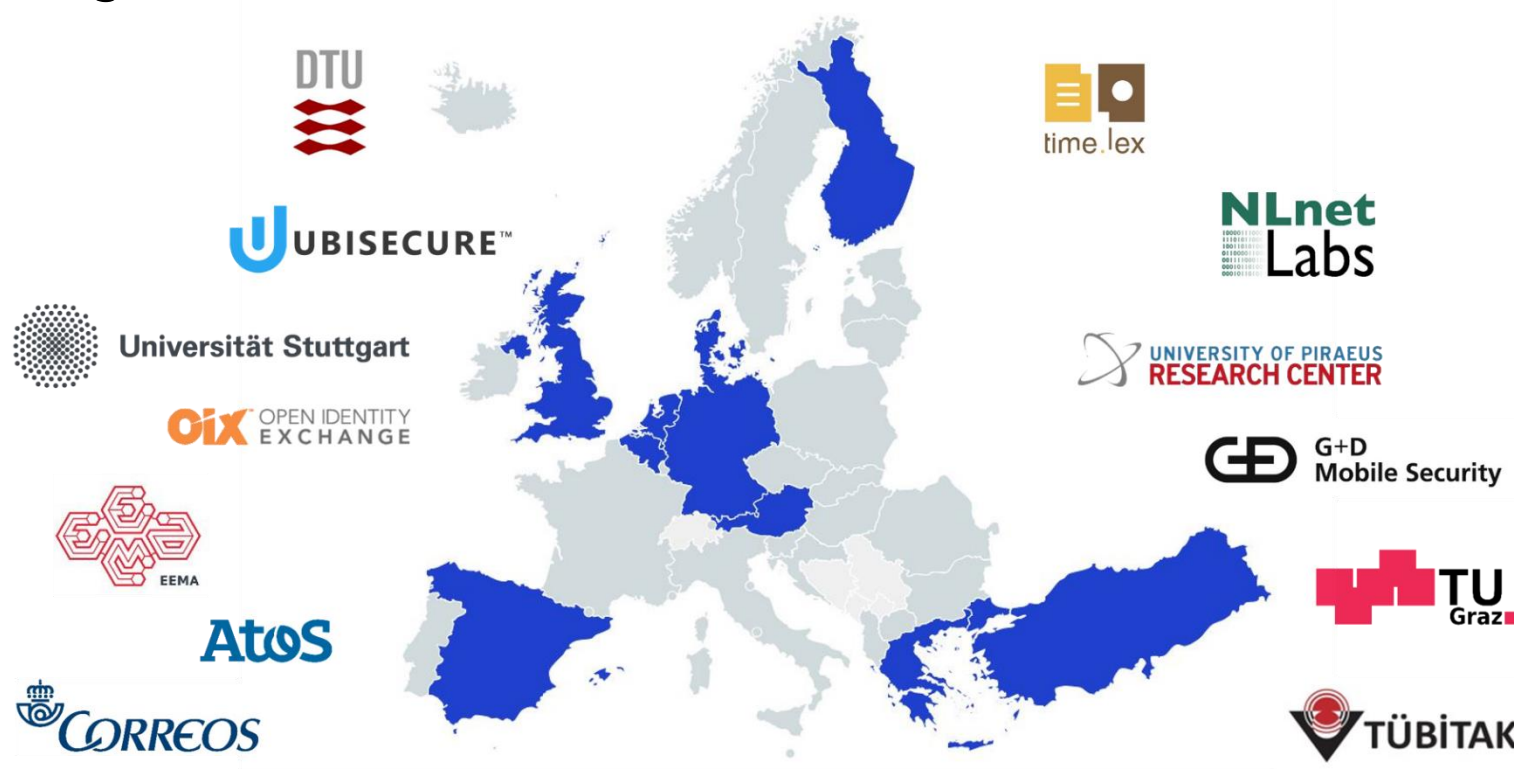# Cross-Border Trust Infrastrucutures:
What the LIGHTest tool has to offer
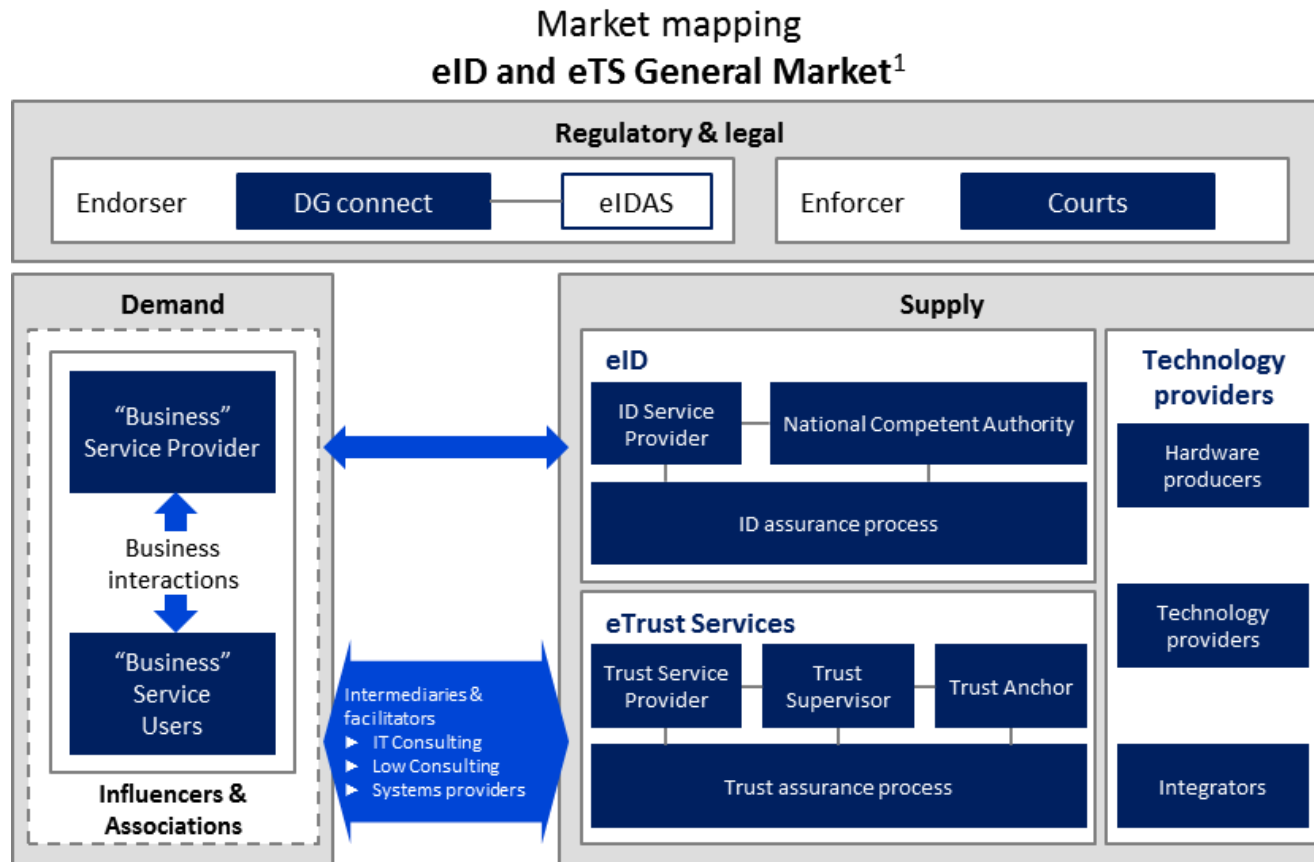
Rachelle Sellung,
University of Stuttgart IAT

Identity Week, June 11th 2019

Seizing Opportunities: eIDAS & Digital Single Market

Market mapping
eID and eTS General Market[1]

Cross-Border Market Size
► **12 M citizens working abroad**[2]
► **70M eCommerce customers**[1]
► **260M e_Registered Deliveries/year**
► **3.5 M patients** in cross-border treatment[1]
► **4bn$ revenues for identity players** in eIDAS services until 2020 (GSMA)
► **4 M Erasmus students 2014-2020**[3]
► **15 M customers in Single Market of financial services**[1]
► **100,000 foreign-owned businesses** by EU citizens[1]

Public Sector: tax applications, social and security services and e-health & e-prescriptions

Private Sector: Banking & insurance, eCommerce, Transport, online platforms

LIGHTest Value Statement

Lightest enables the use of a **global and trusted infrastructure** to determine and verify digital trust assurances to facilitate decision making and assessing risk.
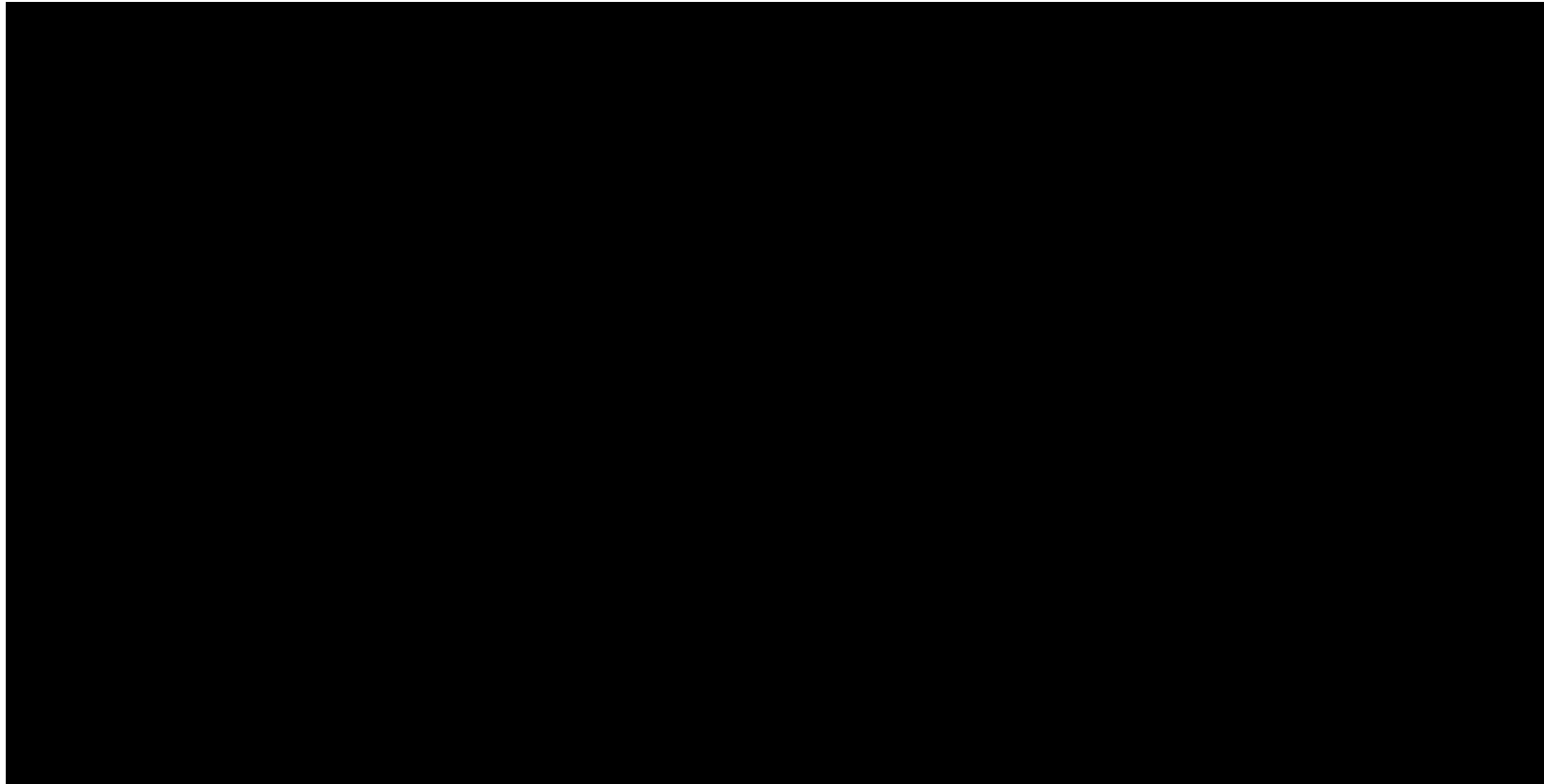
By better understanding operational risk, operational costs can be better controlled. LIGHTest is providing tools for the emerging cross-border trust services market.
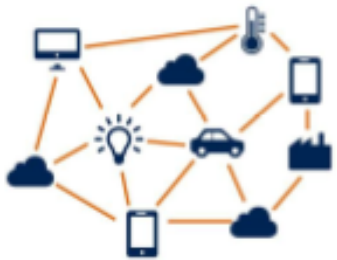

EU Horizon2020 Project: LIGHTest

https://www.youtube.com/watch?v=lEaCMcVer28

Why do we need LIGHTest ?

The emerging market of cross-border trust services

USE CASES

IoT Trust Management

- If a person or company wants to enforce organisational policy, determine which IoT devices are allowed or permissible
- Organise IoT Assistants to communicate based on certifications of a trusted party

Cross-border Certification

- These could be training certificates, government certificates etc, and be specific to a country
- LIGHTest could be used to ensure trust in these certifications and translate these certifications between different countries

Cross-border banking

- Opening a bank account in a different country can be difficult and slow with users needing to assert trustworthy data about themselves to support an application for a new financial service
- LIGHTest could help with this cross-border verification and enable an account to be opened in line with regulatory obligations

Scope of LIGHT*est* Infrastructure

Private Sector

Shipping…
Banking…
Credit Card…
Internet of Things…
Etc.

Both

Notarizations…
Cross-Border Certifications…
Access Control
Management..
Etc.

Public Sector

Health Information
Services..
E-Voting…
Business Registrar…
Etc.

© LIGHT*est* Consortium
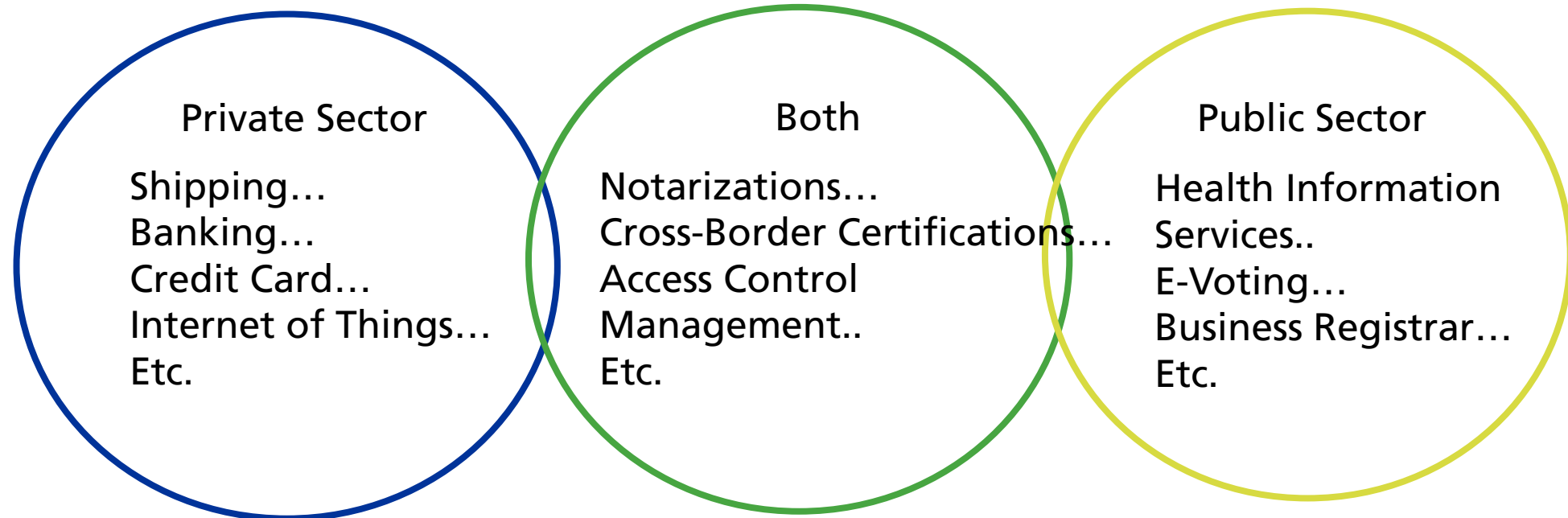
What does LIGHT*est* do? Pilot Demonstrations

Trustworthy communications (by Correos)

- 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
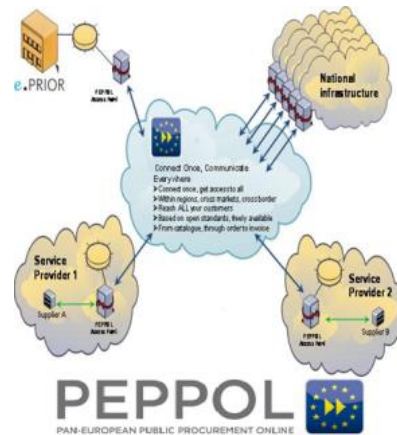
## PEPPOL e-Procurement (by UPRC)

- Approach applicable to other PEPPOL applications
- Demonstrates easy of integration of LIGHT*est* in existing product
  - SHA1 to SHA2 Pilot Scenario: key exchange of root certificates
  - e-Tendering Pilot Scenario

© LIGHT*est* Consortium

Applied Use Cases and Extra Demonstrations

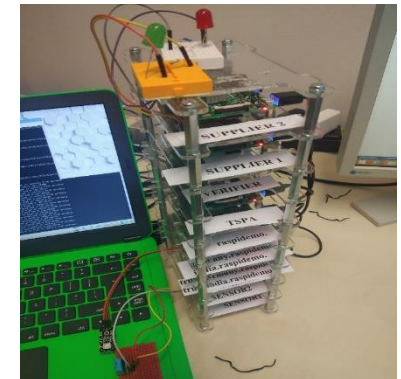**Predictive Maintenance**

Academic Use Case

© LIGHT*est* Consortium
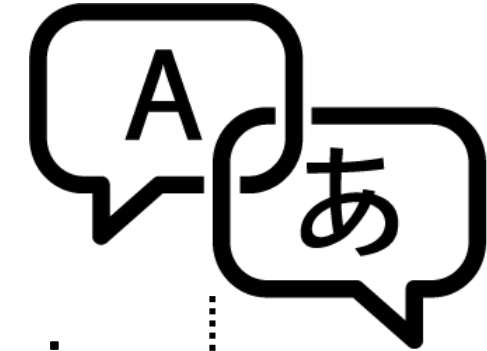
Predictive Maintenance Use Case: sensor data verification in IoT

■ Scenario "predictive maintenance" using sensor data for pre-emptive maintenance decisions

■ Advantages of "predictive maintenance" require some additional and specific security measures:

- guaranteed that no production details are transmitted (data filtering)

- communication flow has to be confidential, integrity protected and authentic

- each supplier can access his own and only his own sensors (in case of several suppliers)

■ **GOAL: Lightweigt Identity and Access Management**

        using LIGHTest infrastructure

■ build a Raspi-Demonstration

© LIGHT*est* Consortium

Predictive Maintenance Use Case: sensor data verification in IoT

Key features:

- decentralized access lists

- centralized access right location

This concept enables

- implementation of additional sensors of a new assembly line/location

- maintenance of existing sensors lists (numer/type of sensors change over time)

- history protocol with timestamp records

by adding (updating) new access lists and corresponding access policy rules

➢ Good scalability for dynamic and large systems

Predictive Maintenance Use Case: sensor data verification in IoT

- Setup with 5 Raspberry Pis

- Raspi 1: Temperature sensor

- Raspi 2: Controller (Notifier)

- Raspi 3: Access List

- Raspi 4: Supplier

- Raspi 5: DNS Server

- Example: If T > 25°C then

  - verify sensor

  - provide information to authorized persons only
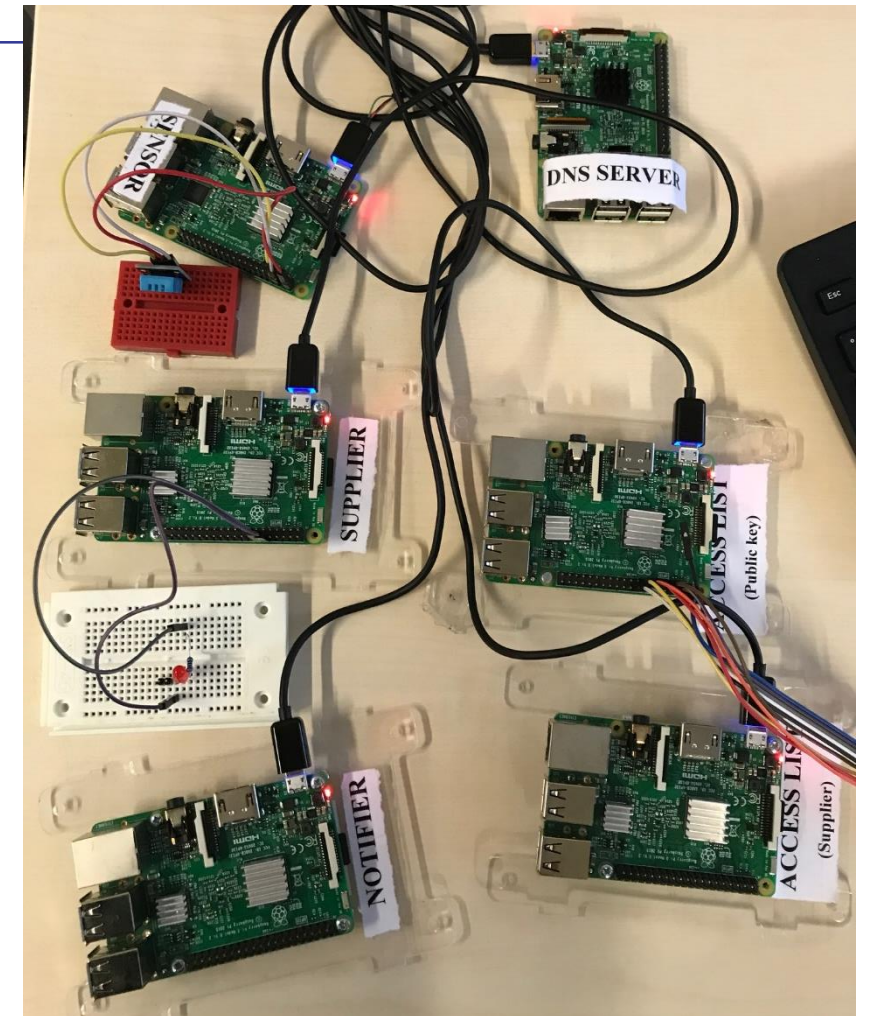
Use Case: PoC for a Trust Scheme for UNHCR DAFI program

- UNHCR contacted the LIGHTest consortium to discuss a digitalization of the German government funded DAFI refugee scholarship programme as a possible use case of the LIGHTest project

- Several pilot projects in order to make better use of data collected when registering refugees
  - create a digital identity for the more than 8 million individuals
  - improve service delivery by UNHCR and other humanitarian actors
    - DAFI refugee scholarship programme which is currently supporting 13,000 refugee students in 50 asylum countries
    - Currently scholarship application, selection, and management are largely analog and paper-based.
    - managing DAFI requires systems of trust management in support of an open ecosystem of different stakeholders and trust schemes, UNHCR contacted the LIGHTest consortium.

© LIGHT*est* Consortium

Use Case: PoC for a Trust Scheme for UNHCR DAFI program

- Benefits for having a UNHCR Trust Scheme:
  - Assists in the Digitalization of the UNHCR
  - Increase mobility of Documents that are processed or officiated by the UNHCR
  - Added security of Documents
  - Formalization of processes
  - …
- Benefits of using LIGHTest Infrastrucutre:
  - Ability to have a Verification and Translation of various Electronic Documents or Certificates from various Countries or Institutions
  - LIGHTest provides privacy tools and guidelines
  - Improved processing of digitalized documents for the DAFI program

Use Case: PoC for a Trust Scheme for UNHCR DAFI program

1 Refugee wants to apply for Scholarship with the DAFI program. In order to do so they bring the appropriately notarized and hardcopy documents. (e.g. passport, UNHCR ID, School Certificates)

2 The DAFI program and UNHCR employees (or other trusted 3rd parties) review the documents for the application and the authenticity of the documents by verifying the notarization of the documents.

3 The UNHCR employee that is apart of the DAFI program stores the digital and physical documents for the applicant. This is done in the form of scanning the document into preferably a readable xml file with an attached photo of document.

The additional step to this process would be to electronically sign this document with the UNHCR unique electronic signature.

4 The Refugee and the UNHCR have a digital document that is signed and integrated in the UNHCR trust scheme that has the ability to be digitally verified and translated according to the University Application process or internal UNHCR use.

Use Case: PoC for a Trust Scheme for UNHCR DAFI program

1

2

3

4

Refugee David

- brings hardcopy documents (e.g. passport, UNHCR ID, School Certificates)

Notary Bob

- reviews the documents
- verifies authenticity of documents

Notary Bob

- scans the documents
- signs the documents

UNHCR and David

- have a digital document signed & integrated in the **UNHCR trust scheme**

- Documents can be easily accessed & digitally verified

Use Case: PoC for a Trust Scheme for UNHCR DAFI program

Required trust infrastructure:
- UNHCR Trust Scheme
- UNHCR Trust List(s)
- UNHCR Trust Scheme Policy

© LIGHT*est* Consortium

Use Case: PoC for a Trust Scheme for UNHCR DAFI program

- UNHCR Trust Scheme

  - Assists in the Digitalization of the UNHCR

  - Added security and increase in mobility of Documents

  - Formalization of processes: Assists in management and control of Documents

- Trust Scheme

  - comprises the organizational, regulatory/legal, and technical measures to assert trust-relevant attributes about enrolled Entities in a given domain of trust. Example: eIDAS

  - 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* Consortium

Breaking new ground in cross-border trust agreements

LIGHTest is a toolbox

- DNS used as a secure discovery and communication tool
- But legal value and compliance doesn't originate from DNS

LIGHTest includes legal tools

- Security built into LIGHTest infrastructure: privacy by design
- Templates for T&Cs, privacy policies and contracts between users

LIGHTest needs to be tailored

- Pilots will show how LIGHTest can be deployed on a contractual basis
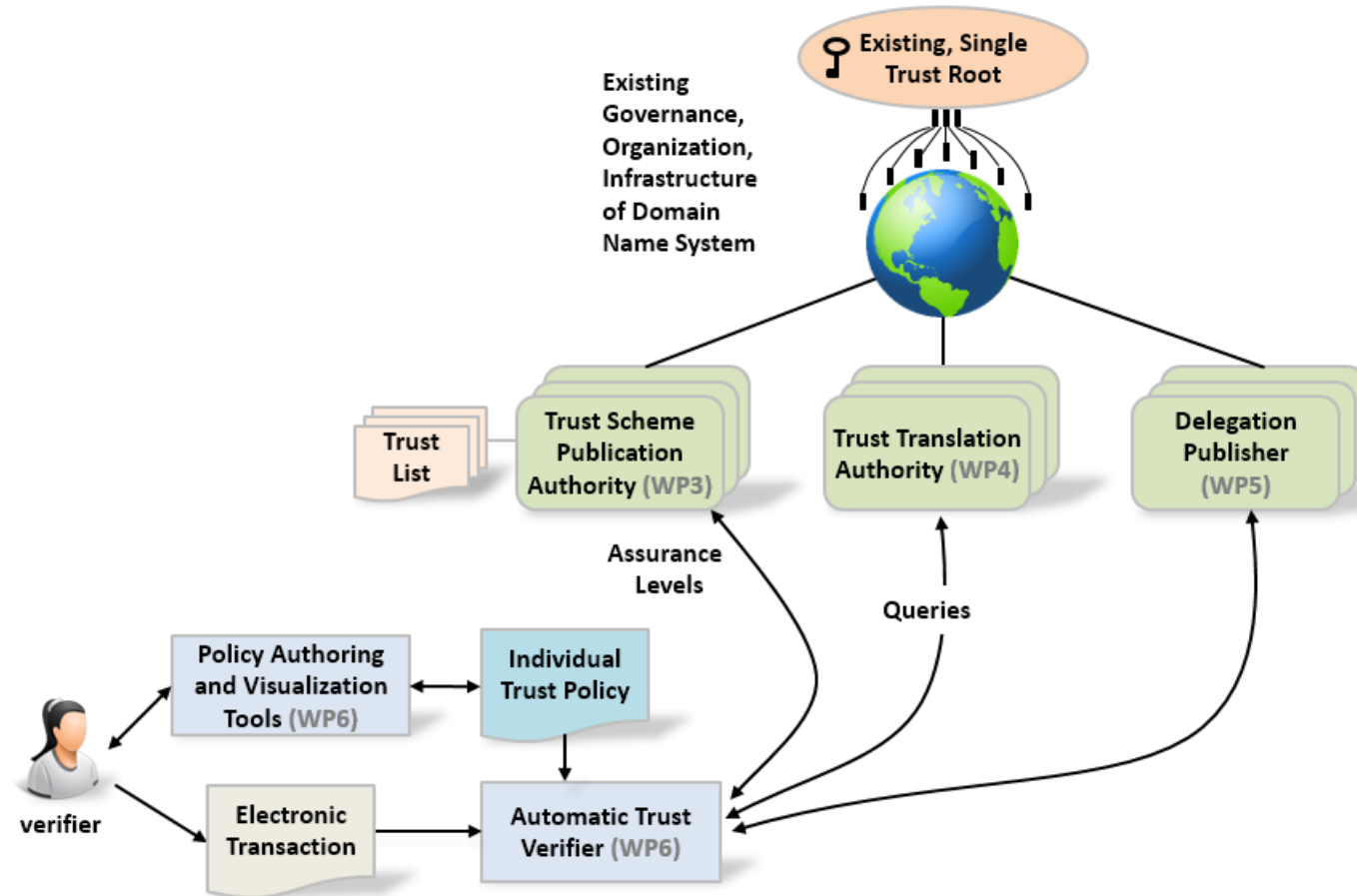- Guidelines to be provided on how LIGHTest can be used in other settings

LIGHTest is not a legislative initiative

- Not aiming to change laws, but show how DNS can be leveraged
- Compliance needs to be assessed in each individual use case

New generation of open standards and technical tools

A Trust Publication

Infrastructure for Publication and Querying of Delegations

Organisation publishes Trust List:
- Who can sign/act in its name for which purposes?

LIGHTest will make it automatic for verifiers to query Trust Lists and combine multiple queries to validate an electronic transaction against an easy to author Trust Policy.

The European LIGHT*est* Project

- Horizon 2020
- Innovation Action
- Call: H2020-DS-2015-1 *Trust eServices*
- Started September 1, 2016
- Ends in November 2019
- Estimated cost of 8.7 Mio Euros
- 14 partners from 9 countries
- Coordinated by Fraunhofer

© LIGHT*est* Consortium