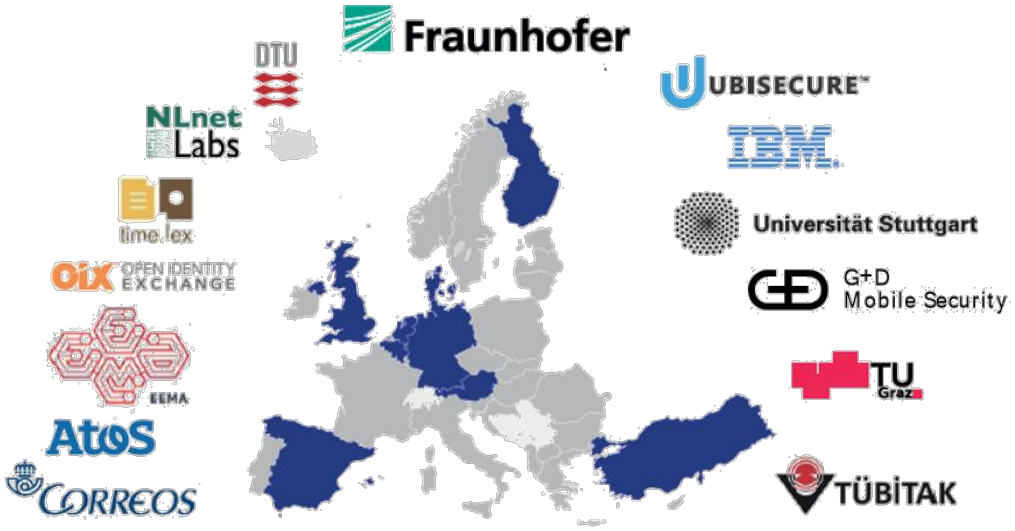
How the DNS Can Support Identification and Trust Services



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

2019

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

Agenda

- What LIGHTest is (and what it is not)
- Electronic Transactions & Automated Trust Verification
- Discovering Location of Trust - Based on DNS
- Translating Trust-Trustworthy Communication Services Pilot
- Trust in Postal Services
- Correos eDelivery trust schemes published in LIGHTest
- Trust Translation in Correos Pilot
- Seizing Market Opportunities with eIDAS & DSM
- Conclusions

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

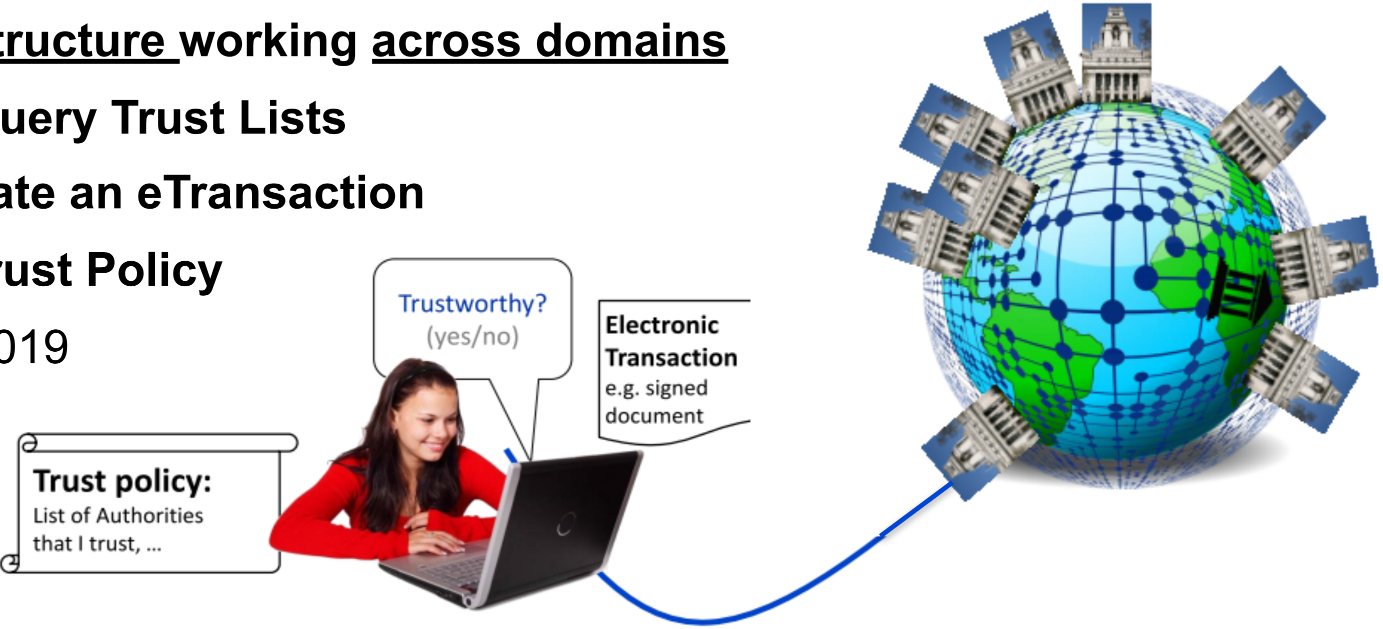
What LIGHT*est* is and what LIGHT*est* is NOT

- LIGHTest is not an alternative to eIDs or business registers
- LIGHTest does not allow you to outsource trust decisions
- LIGHTest does allow you to use **a global, known and trusted infrastructure** to:
  - Retrieve ID+TS information
  - Verify ID+TS information
  - Determine trust assurances behind it
  - Facilitate your own decision making
- While also providing a growth path for European Digital Single Market
  - Through **internationalisation of eID and Trust Services recognition**!
- !

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

LIGHT*est* is a Global, Cross-Domain Trust Infrastructure => Automatic Trust Decisions!

- **A global Standard Way for publishing Trust Lists...**
  - **…on a Global Trust Infrastructure working across domains**
- Make it automatic for Verifiers to **query Trust Lists**
- Combine multiple queries to **validate an eTransaction**
  - against an easy to author **Trust Policy**
- Project completion in December 2019
- Many ways to become involved…
  - Community
  - International Forum
- https://lightest-community.org



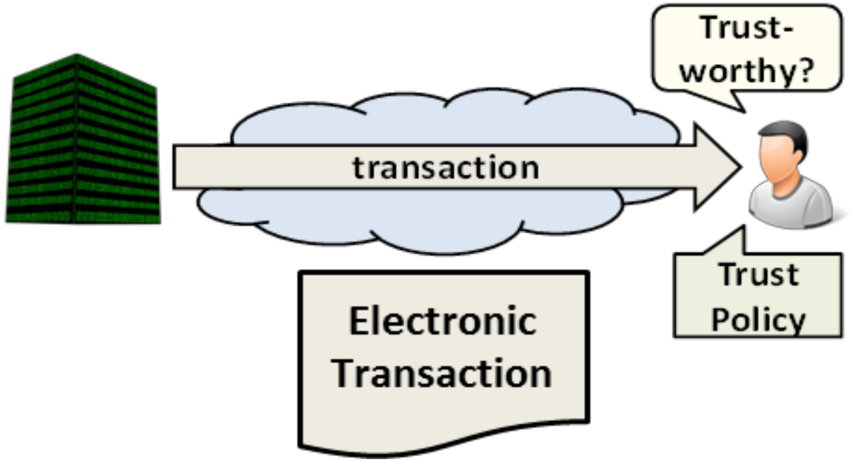
LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Electronic Transactions & Automated Trust Verification

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

The Electronic Transaction

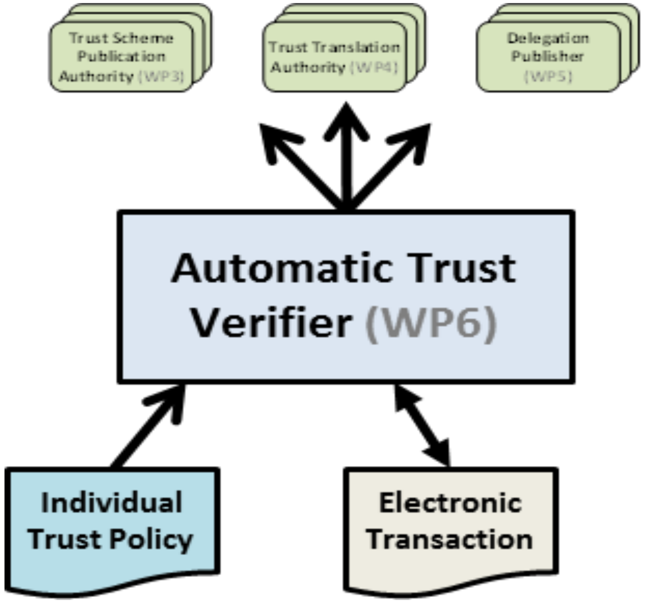
- An electronic transaction is a *container* of a given format (e.g. ASiC) that contains several documents or sub-containers (e.g. electronic transaction data).
- Desirably, documents and containers will be associated (provenance) with an electronic identity, e.g., via electronic signature (also ensuring integrity)

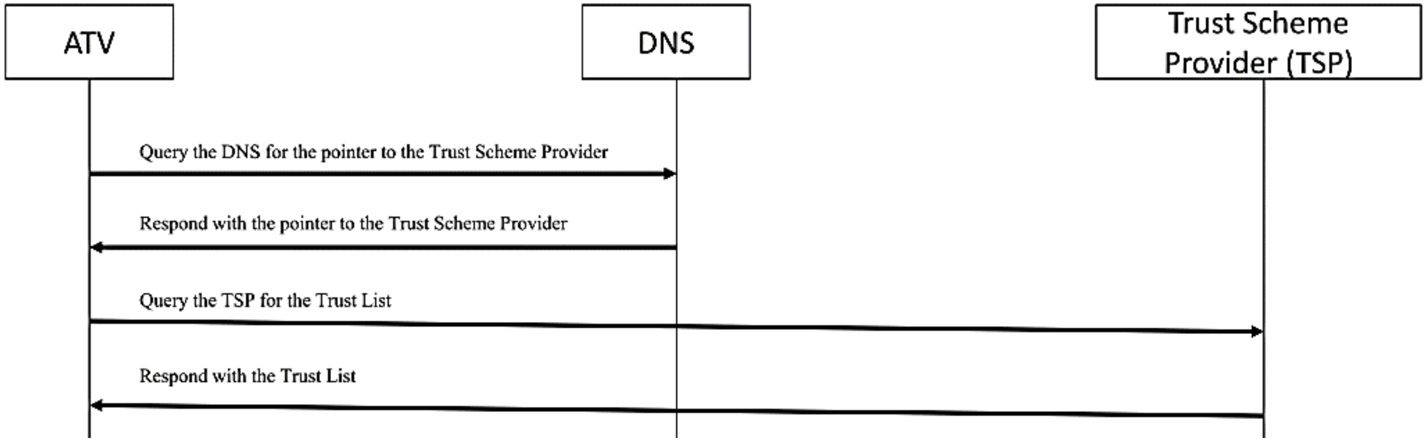


LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Automated Trust Verification

- Automatic Trust Verification relies on 2 items: The individual Trust policy, and the Electronic Transaction itself


Trust Scheme Publication Authority (WP3)
Trust Translation Authority (WP4)
Delegation Publisher (WP5)
Automatic Trust Verifier (WP6)
Individual Trust Policy
Electronic Transaction


ATV
DNS
Trust Scheme Provider (TSP)
Query the DNS for the pointer to the Trust Scheme Provider
Respond with the pointer to the Trust Scheme Provider
Query the TSP for the Trust List
Respond with the Trust List

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

Prerequisites to Automate Verification of a Trust Policy

- Machine Readable and understandable Trust Policy
    - Both parties need to have readable schemes

Policy Authoring

- Comparison / Analysis Tool for Trust Policy
    - Example: NIST Level “3” == EC eIDAS Level “substantial”
    - May require translation capability
    - Needs understanding of any delegation issues

Verificatation and Analysis

- Discovering where the Trust Policy details are located
    - Where can the counterparty’s policy be found reliably?

Publisher

Discovering the Location of Trust (Schemes/Lists/Translations)

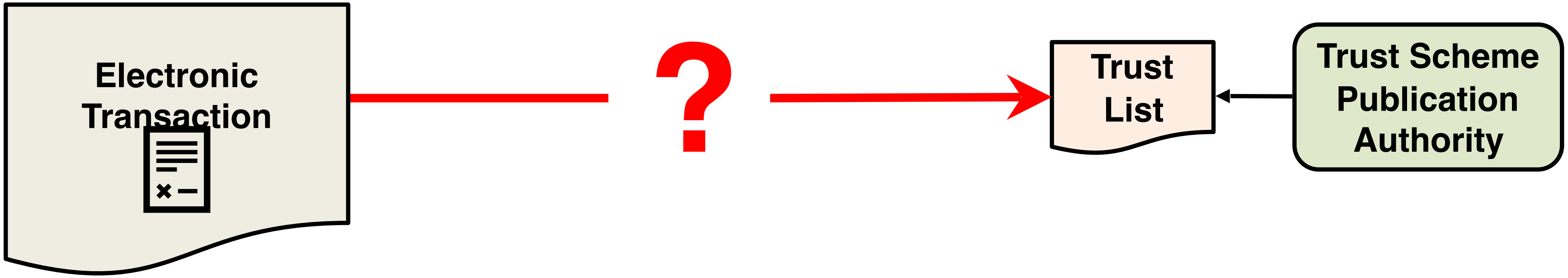
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Why use the DNS in LIGHTest?

- Distributed model of ownership of names and data
  - participants stay in control of what they publish and who they trust
- Proven, widely deployed technology
  - foundation of the Internet for 30 years,
  - scalable, robust and reliable,
  - software, libraries, etc. widely available
- DNSSEC provides a single trust anchor (DNS Single Trust Root)
  - See more details: https://www.lightest.eu/static/deliverables/D2.7.pdf

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

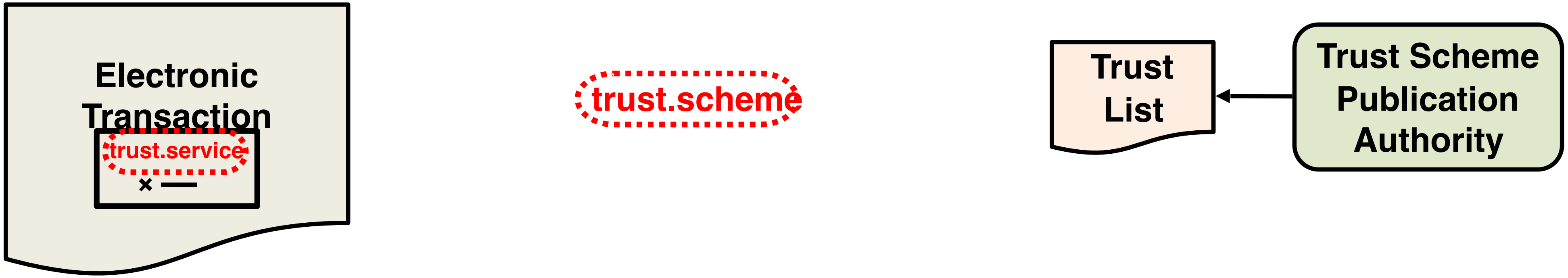
DNS in LIGHTest: Publishing and Finding Trust Information



- Question: How does the trust verifier find the trust-related documents relevant for verification?
  - Which documents might be relevant?
  - Where are they?

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

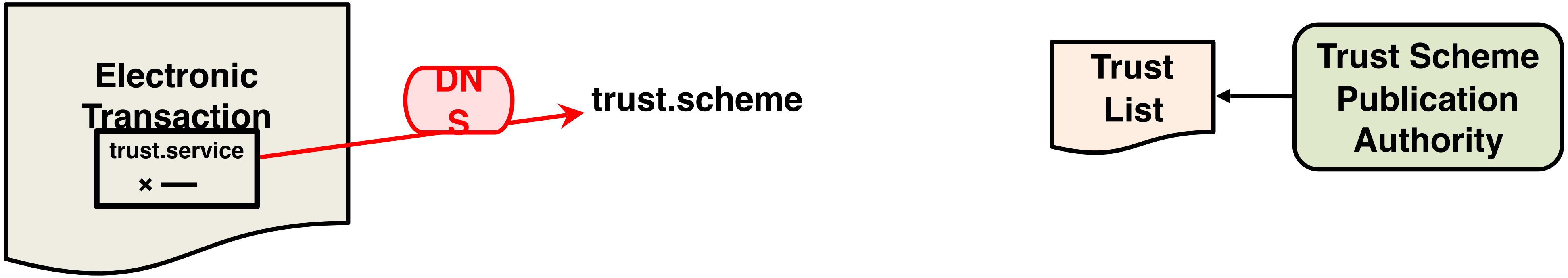
DNS in LIGHTest: Publishing



- Domain names as identifiers for trust entities
  - trust services
  - trust schemes

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

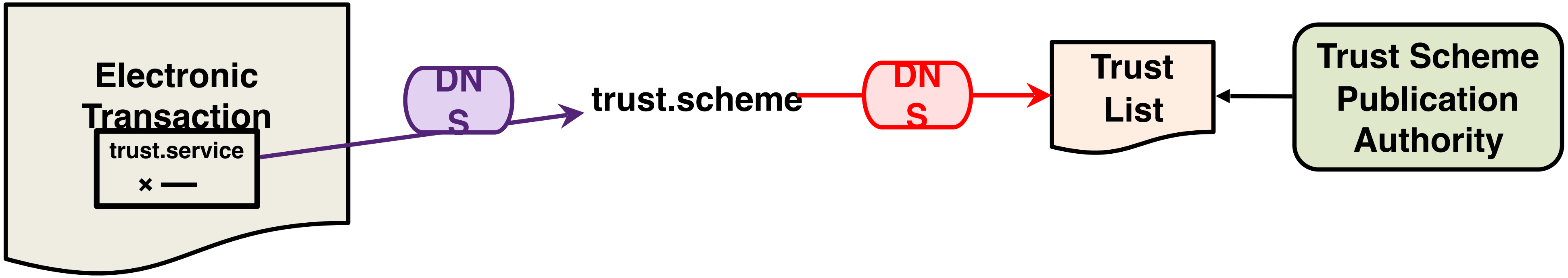
DNS in LIGHTest: Discovery



- Entities publish claims of a relationship with other entities in DNS
  - trust service claims membership with trust scheme
  - trust scheme claims ability to be translated into another scheme

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

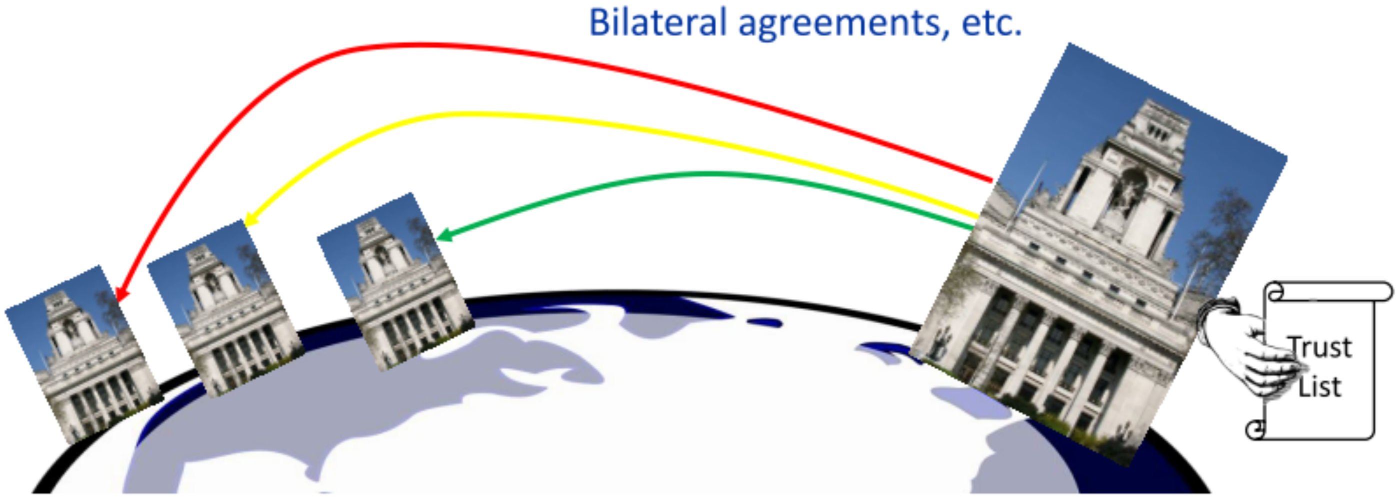
DNS in LIGHTest: Discovery



- Entities publish location of their trust-related documents
  - trust lists
  - trust translation lists
- They can also publish information about the certificates used for signing those documents.

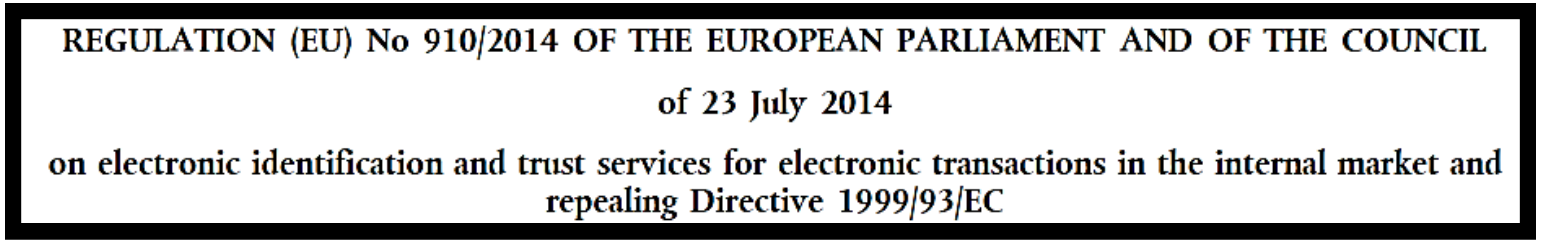
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Translating Trust-
Trustworthy Communication Services Pilot



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

Bilateral Agreements in eIDAS regulation



REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 23 July 2014

on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

- **<u>Article 14: International Aspects</u>**

> ***"TS provided by TSPs established in a 3rd country shall be recognised as <u>legally equivalent</u> to QTS provided by QTSPs established in the Union where the TS originating from the 3rd country are recognised under an <u>agreement</u> concluded between the Union and the 3rd country in question or an international organization"***

⇒*QTSPs from 3rd country/int'l org. must meet reqs. for EU QTSPs, Ex: Recital 67 QWACs*

⇒*QTS provided by QTSPs in EU are recognized as legally equivalent in 3rd country/int'l org.*

- Exception (Art. 2.2): eIDAS will not apply to TS within closed systems resulting from national law / agreements btw. defined set of participants

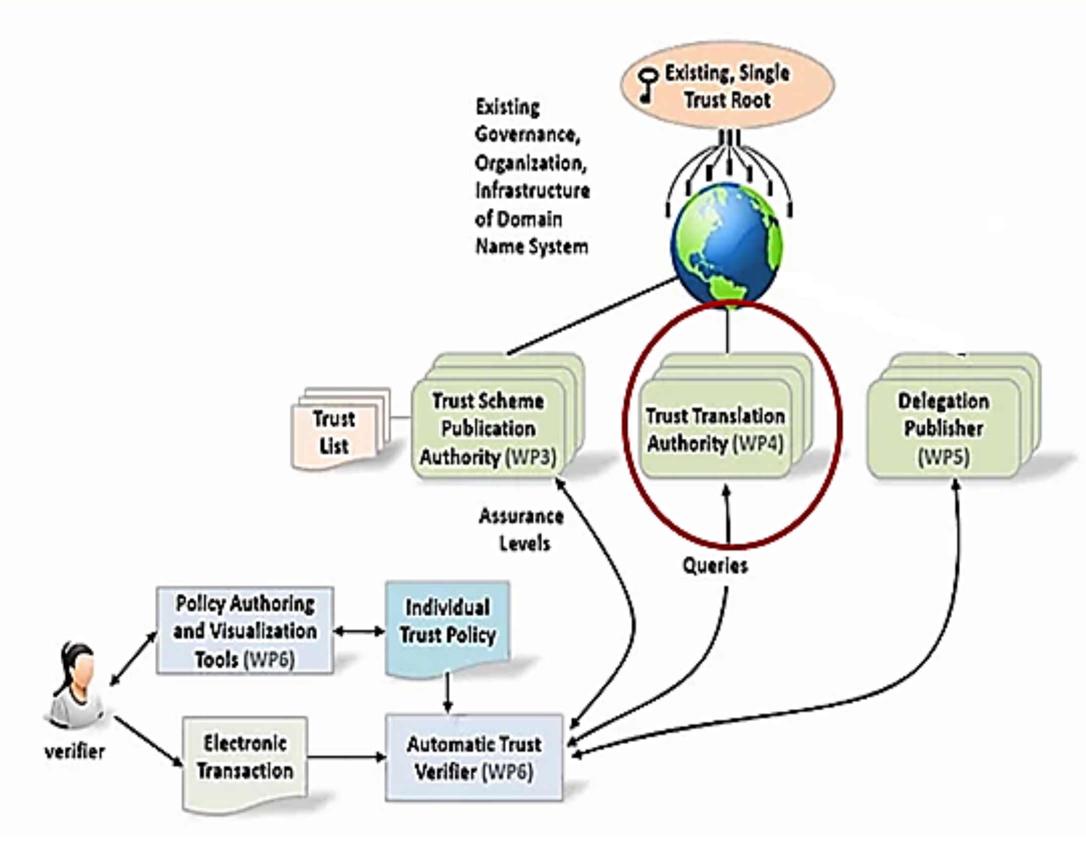
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Trust Translation - Overview

- **Challenges: Why?**
  - Absence of global agreement on LoAs and organizational criteria diversity
  - Necessity of a translation infrastructure between different contexts (cross-sectors, cross-geographical/political/jurisdictional areas)
  - Concrete scheme mappings to be provided by authorities
  - LIGHTest analyzed Trust Schemes: ISO29115, eIDAS (all TS), STORK 2.0 AQAA, US (PIV, NIST DSS), China
- **What**: Development of a **trust translation infrastructure & trust translation model**
  - Transparency to verifiers: DNS-based easy publication of Trust Translation Lists and Discovery of Trust Translation Authorities
  - Verifier expresses trust in translation lists provided by selecting results from the discovery service
  - Seamless integration in trust list-enabled applications at no additional cost

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

TTA: Trust Translation Authority Supports Automated Trust Verification


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)

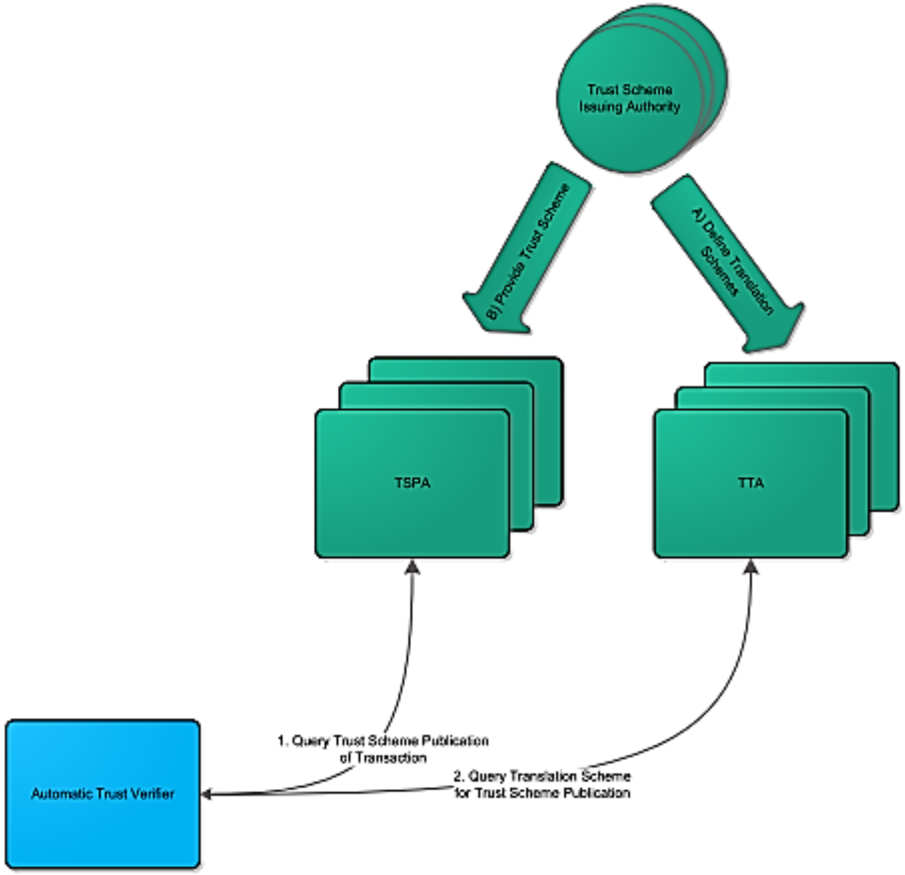
TA allows interop. of trust schemes ublished by different entities, even cross different trust domains, by defining he relation between the trust scheme evels.

- ✓ Flexible support for different TS definitions: Boolean / Ordinal / Tuple-based schemes
- ✓ Discovery mechanisms to assist verifiers to find proper TTA
- ✓ Open source client library that obtains trust translation data through the DNS resolver library
- ✓ Server-side tools able to load translation schemes into DNS name servers
- ✓ Serves securely signed Trust Translation List to ATV

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

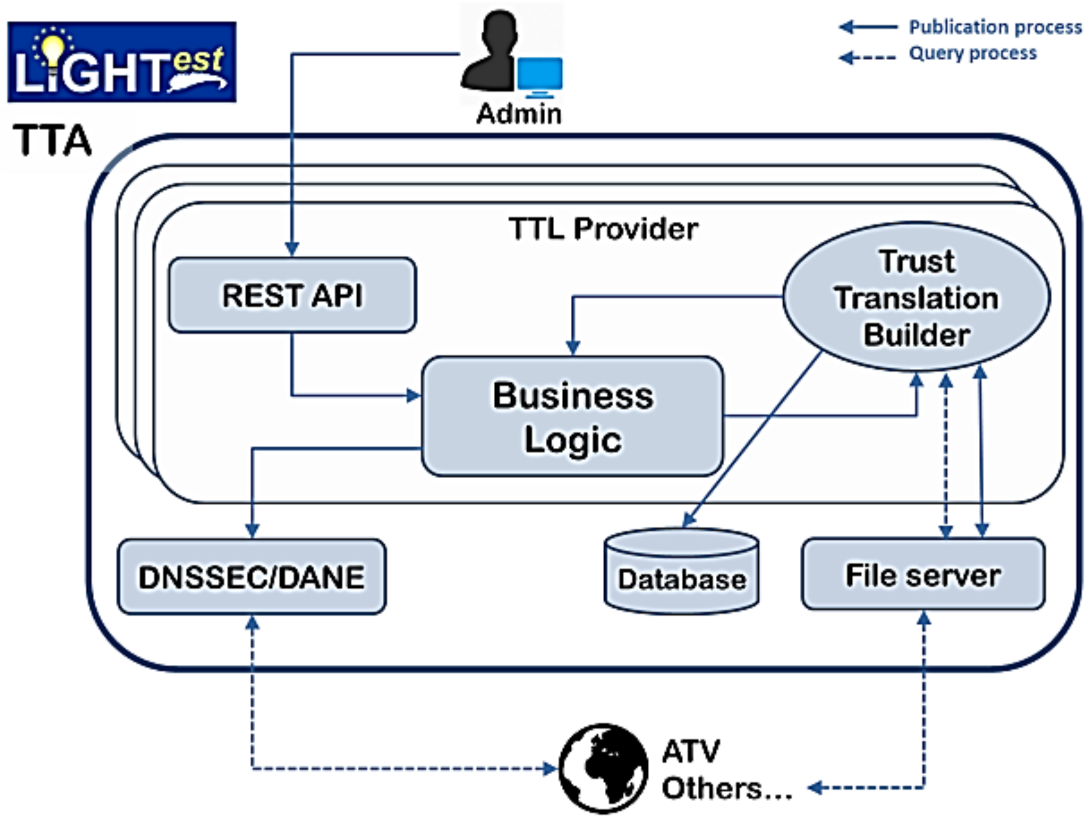
Trust Schemes Publication and Trust Scheme Level Translations

- A Trust Scheme Issuing Authority provides trust scheme representation which is published by TSPA
- Trust Scheme Issuing Authorities negotiate btw. themselves whether their schemes trust each other and in what way (levels): as result they provide Trus Translation Schemes to be published by the TTA in the DNS (URI of TTL). For Discovery of TTS retrieval by name is sufficient.
- A translation btw. Trusted Scheme and Recognized Scheme requires to fulfil all conditions in both of them.


Trust Scheme Issuing Authority
B) Provide Trust Scheme
A) Define Translation Schemes
TSPA
TTA
Automatic Trust Verifier
1. Query Trust Scheme Publication of Transaction
2. Query Translation Scheme for Trust Scheme Publication

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

TTA Internal Architecture: Subcomponents & Data Model

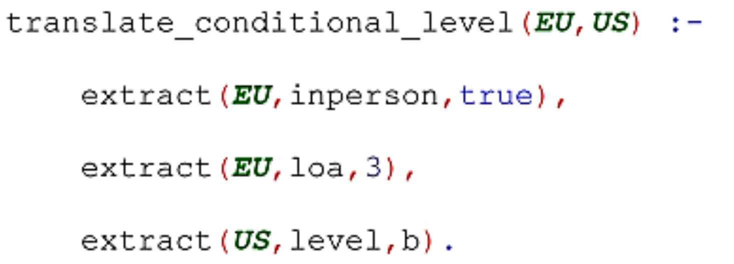


- Core Data Model Entity is the **Agreement**:
  - **Name**
  - **Trust Scheme Publishing Authorities**
  - **Creation date**
  - **Expiration date**
  - **Status**
  - **Pairs of trust levels:**
    - **Source-Target Trust Levels**

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

Example of Trust Translation (Conditional, Ordinal Translation)

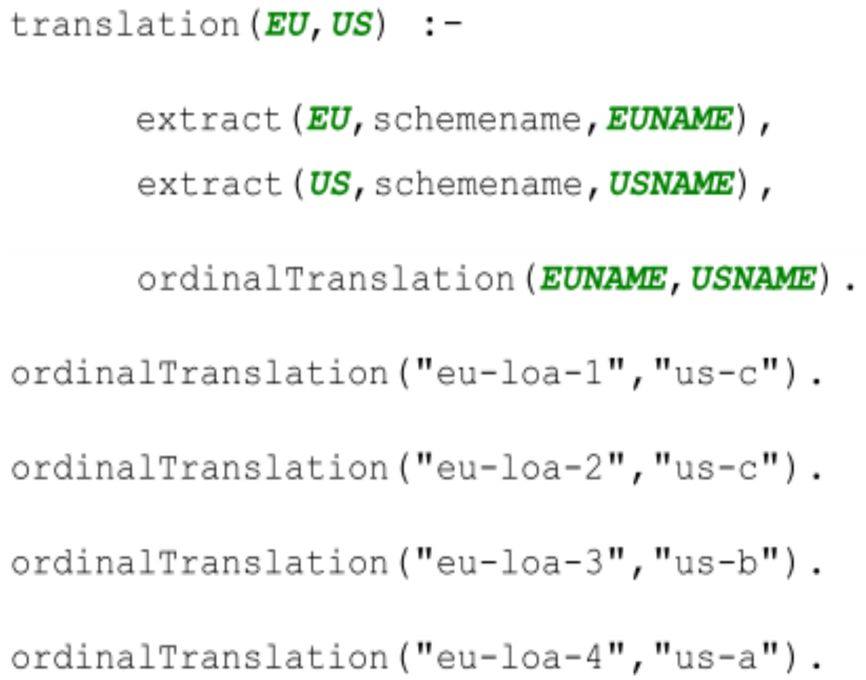
- **Conditional translation**



```
translate_conditional_level(EU,US) :-
    extract(EU,inperson,true),
    extract(EU,loa,3),
    extract(US,level,b).
```

The above clause says that:“EU loa 3 translates to US level b if the EU-scheme has the inperson-attribute, and the value of that attribute is true”.

- **Ordinal Translation**

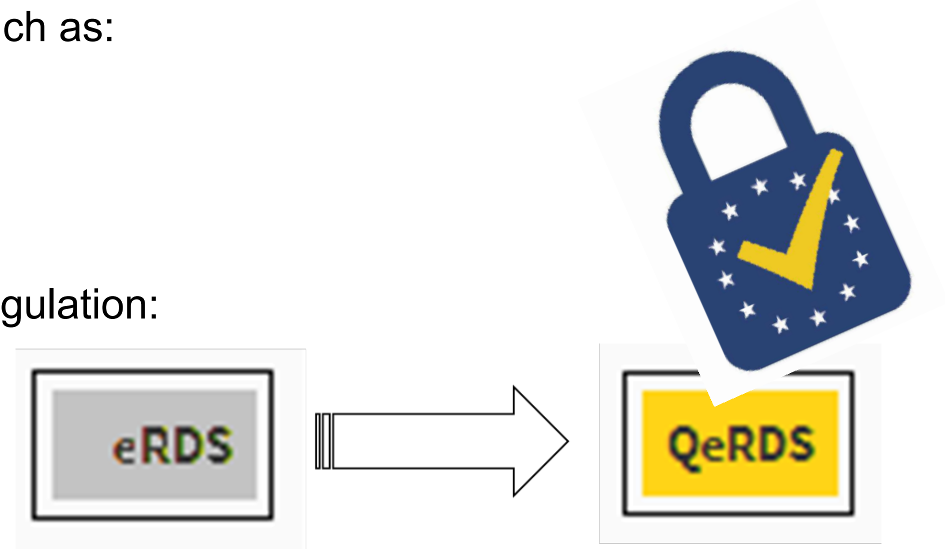


```
translation(EU,US) :-
        extract(EU,schemename,EUNAME),
        extract(US,schemename,USNAME),
        ordinalTranslation(EUNAME,USNAME).
ordinalTranslation("eu-loa-1","us-c").
ordinalTranslation("eu-loa-2","us-c").
ordinalTranslation("eu-loa-3","us-b").
ordinalTranslation("eu-loa-4","us-a").
```

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

Trust in Postal Services

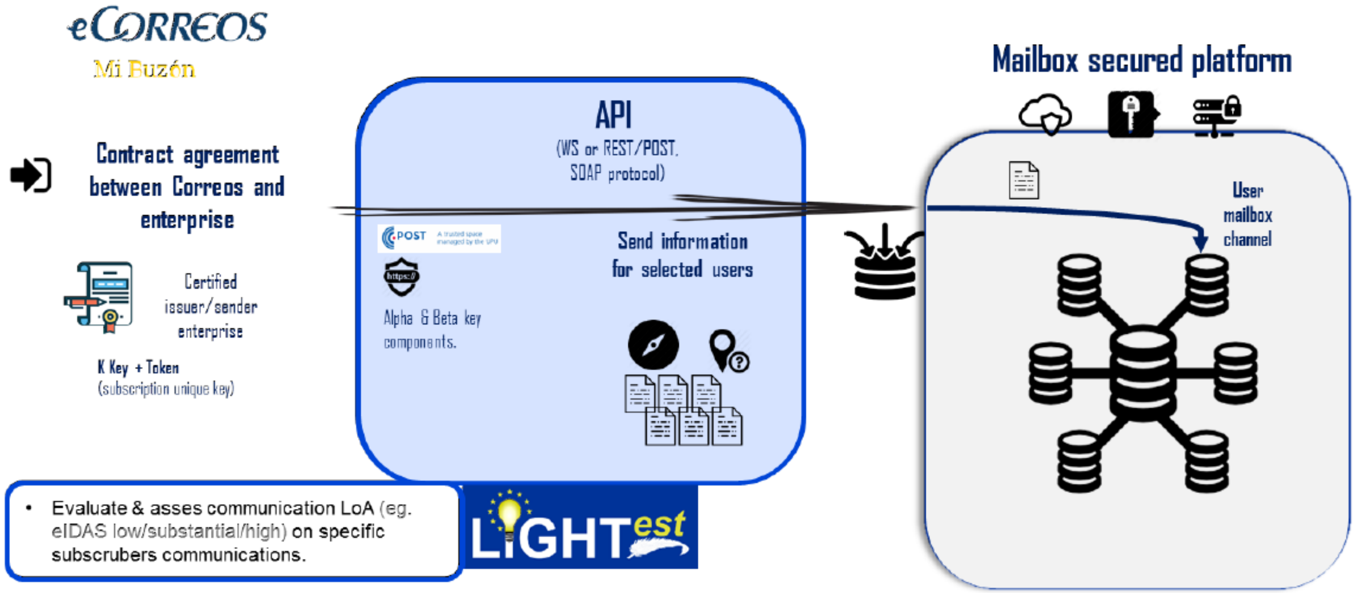
- Correos is the market leader in Spanish Postal sector and a champion in the Digital Transformation
- Interested in providing users with other electronic services such as:
  - MyIdentity
  - MyMailbox
  - MyNotifications
- Aiming at **qualified** level of assurance according to eIDAS regulation:
  - Trust service provider
- Non-qualified electronic registered delivery services:
  - CORREOS MyMailbox
  - CORREOS MyNotification
- Published in LIGHTest framework by means of the Trust Scheme Publishing Authority (TSPA)



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

Correos MyMailbox

- **MyMailbox** is a digital mailbox which enables enterprises/governments/organizations and individuals to create a nexus of safe and secured document based communication. Any document type that has been previously authorized both enterprise and user: contracts, pay sheets, notifications, bank statements, etc. This is *not* an email account; any user may forget about spam or non-desirable information. User will *only receive documents from companies they have subscribed to*.

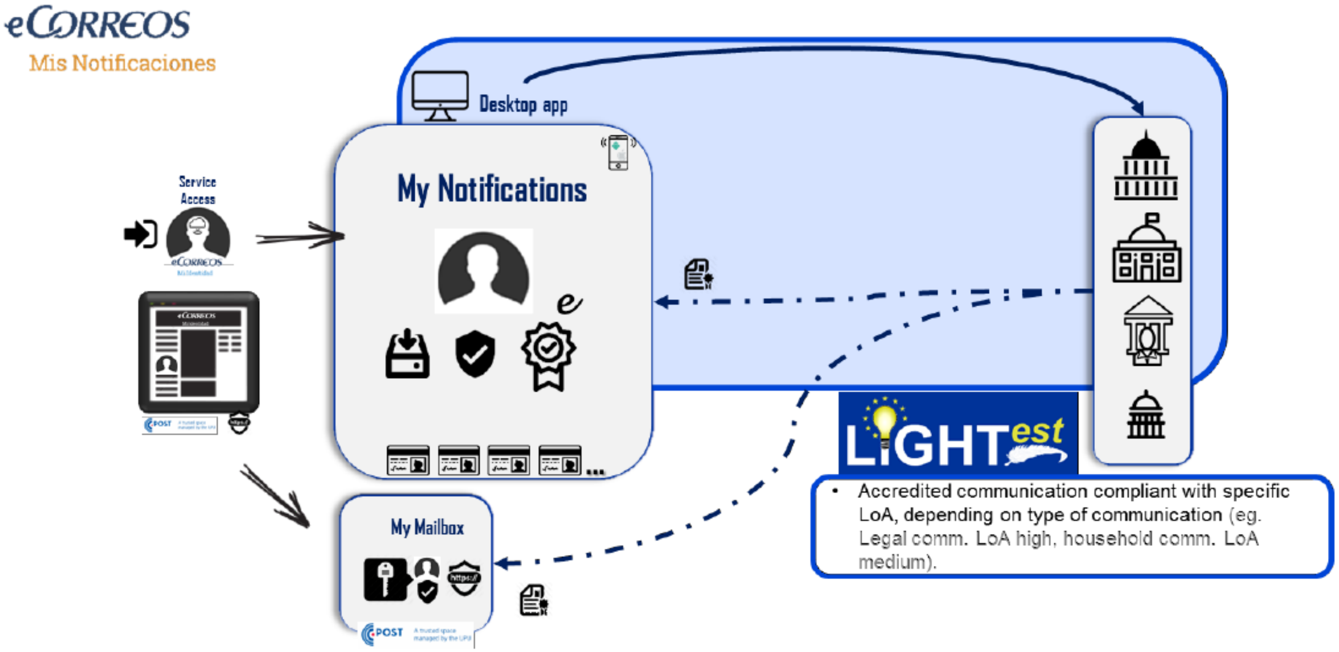

eCORREOS
Mi Buzón
Contract agreement between Correos and enterprise
Certified issuer/sender enterprise
K Key + Token
(subscription unique key)
API
(WS or REST/POST.
SOAP protocol)
POST
https://
Alpha & Beta key components.
Send information for selected users
Mailbox secured platform
User mailbox channel
LIGHTest

- Evaluate & asses communication LoA (eg. eIDAS low/substantial/high) on specific subscrubers communications.

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

Correos MyNotifications

- ***MyNotifications*** is a digital service, aiming to centralize and manage governmental notifications for one or several individuals or legal entities. My Notifications service works by detecting that there are new notifications in some of the governmental agencies electronic service, so user has the opportunity to sign the receipt of the notification and download the associated documents to such notification.

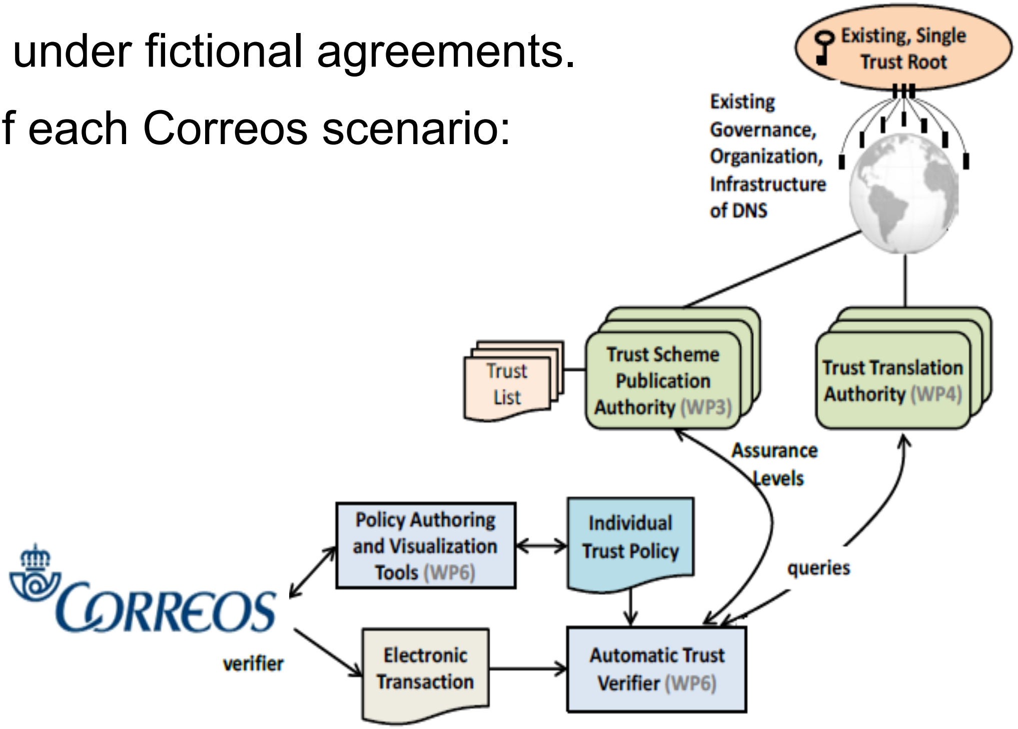


- Accredited communication compliant with specific LoA, depending on type of communication (eg. Legal comm. LoA high, household comm. LoA medium).

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

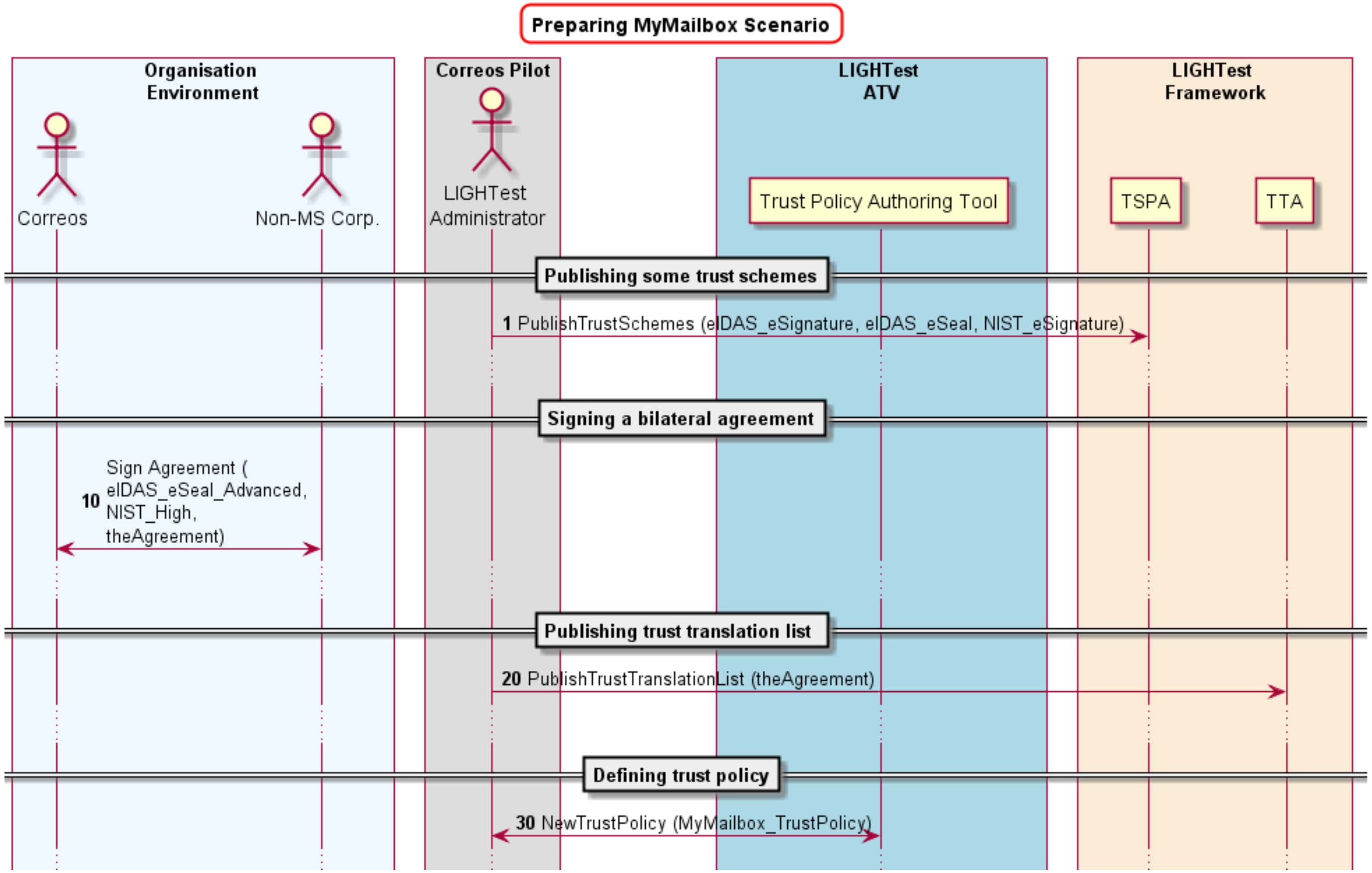
Correoos eDeliveryTrust Schemes in LIGHTest: *Verifying trust*

- Several trust schemes are published by the **TSPA**.
- **Trust policies** are defined by Correos with the **Trust Policy Authoring Tool**.
- **Trust Translation lists** are published by the **TTA**, under fictional agreements.
- The **ATV** is going to verify trust in specific points of each Correos scenario:
  - *Sender* in MyMailbox scenario
  - *Receiver* in MyNotifications scenario


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

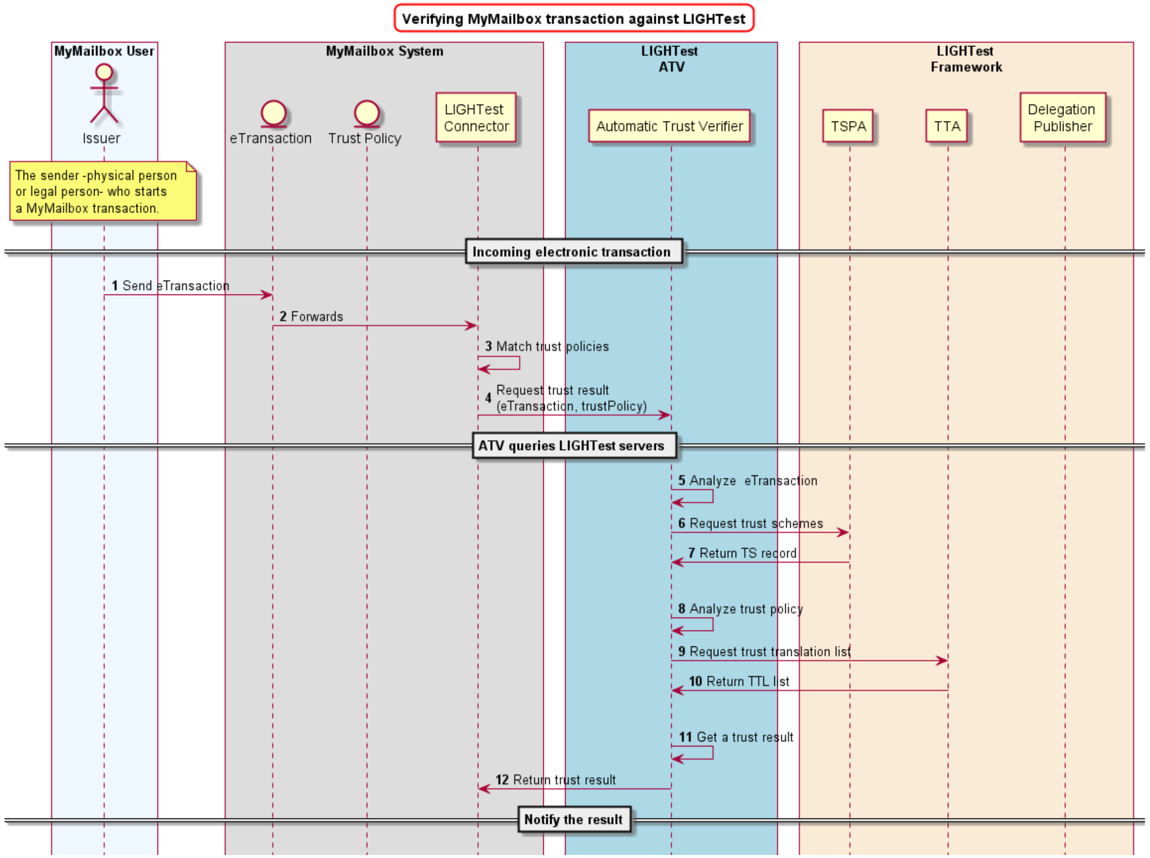
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Trust Translation in Correos scenario: MyMailbox (Publication)


Preparing MyMailbox Scenario
Organisation Environment
Correos
Non-MS Corp.
Correos Pilot
LIGHTest Administrator
LIGHTest ATV
Trust Policy Authoring Tool
LIGHTest Framework
TSPA
TTA
Publishing some trust schemes
1 PublishTrustSchemes (eIDAS_eSignature, eIDAS_eSeal, NIST_eSignature)
Signing a bilateral agreement
10 Sign Agreement (eIDAS_eSeal_Advanced, NIST_High, theAgreement)
Publishing trust translation list
20 PublishTrustTranslationList (theAgreement)
Defining trust policy
30 NewTrustPolicy (MyMailbox_TrustPolicy)

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

Trust Translation in Correos scenario: MyMailbox (Verification)



Verifying MyMailbox transaction against LIGHTest

MyMailbox User

MyMailbox System

LIGHTest ATV

LIGHTest Framework

Issuer

eTransaction

Trust Policy

LIGHTest Connector

Automatic Trust Verifier

TSPA

TTA

Delegation Publisher

The sender -physical person or legal person- who starts a MyMailbox transaction.

Incoming electronic transaction

1 Send eTransaction

2 Forwards

3 Match trust policies

4 Request trust result (eTransaction, trustPolicy)

ATV queries LIGHTest servers

5 Analyze eTransaction

6 Request trust schemes

7 Return TS record

8 Analyze trust policy

9 Request trust translation list

10 Return TTL list

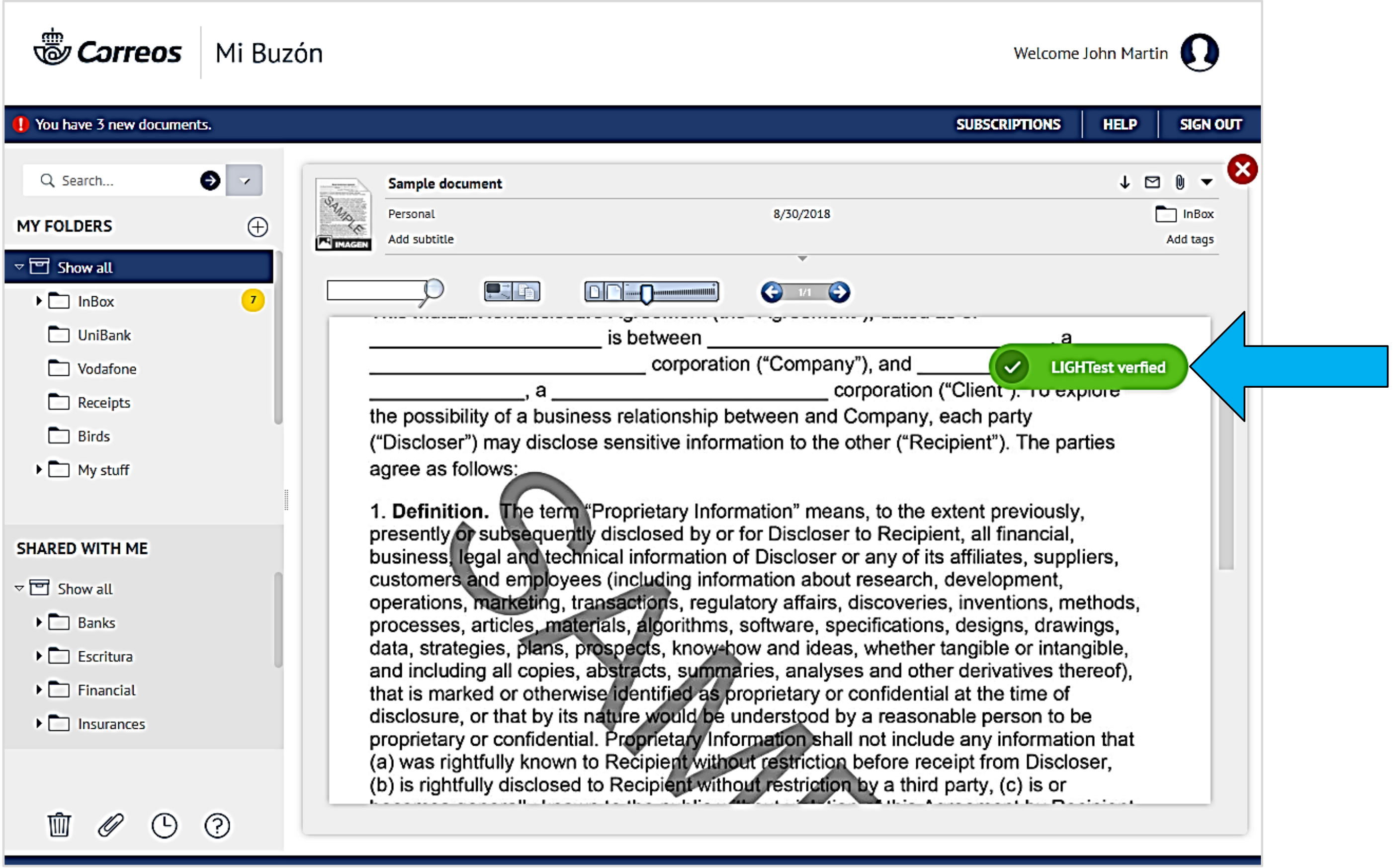
11 Get a trust result

12 Return trust result

Notify the result

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

Visualization of LIGHTest Verification



You have 3 new documents.

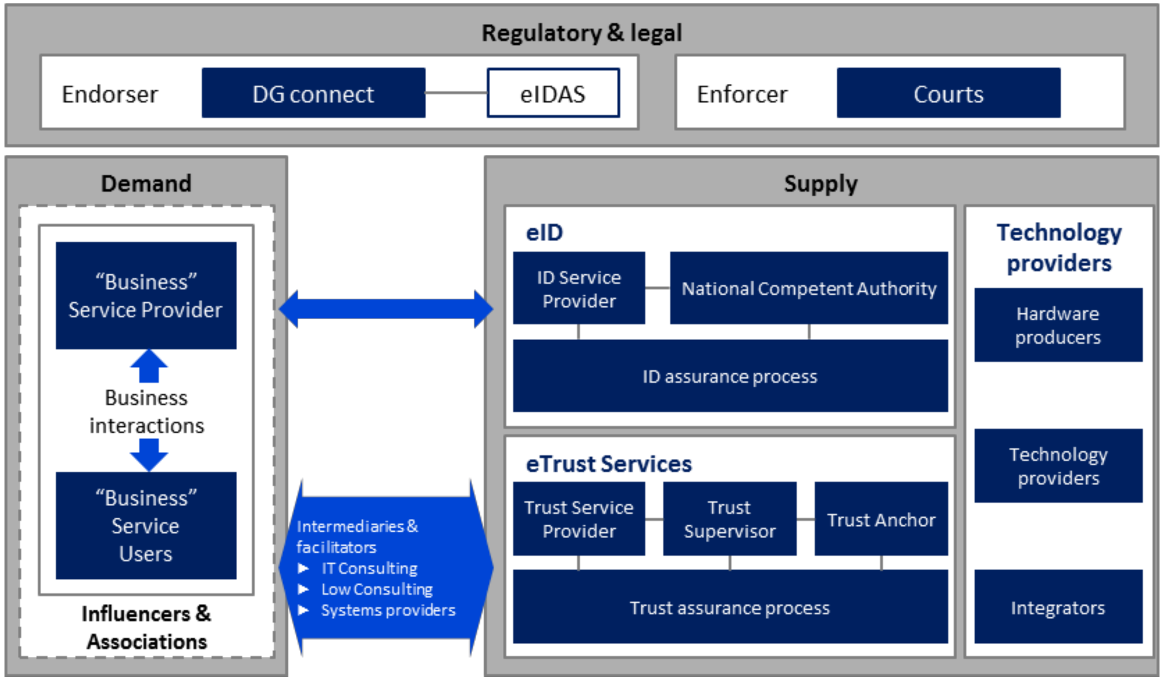
________________________ is between ______________________________, a ___________________________ corporation (“Company”), and ______________________________, a ____________________________ corporation (“Client”). To explore the possibility of a business relationship between and Company, each party (“Discloser”) may disclose sensitive information to the other (“Recipient”). The parties agree as follows:

1. **Definition.** The term “Proprietary Information” means, to the extent previously, presently or subsequently disclosed by or for Discloser to Recipient, all financial, business, legal and technical information of Discloser or any of its affiliates, suppliers, customers and employees (including information about research, development, operations, marketing, transactions, regulatory affairs, discoveries, inventions, methods, processes, articles, materials, algorithms, software, specifications, designs, drawings, data, strategies, plans, prospects, know-how and ideas, whether tangible or intangible, and including all copies, abstracts, summaries, analyses and other derivatives thereof), that is marked or otherwise identified as proprietary or confidential at the time of disclosure, or that by its nature would be understood by a reasonable person to be proprietary or confidential. Proprietary Information shall not include any information that (a) was rightfully known to Recipient without restriction before receipt from Discloser, (b) is rightfully disclosed to Recipient without restriction by a third party, (c) is or

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

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

Source 1: Study on a marketing plan to stimulate the take-up of eID and trust service for the Digital Single Market (SMART 2015/0046)
Source 2: 2017 annual report on intra-EU labour mobility. Source 3; Erasmus+ FAQ, http://europa.eu/rapid/press-release_MEMO-13-1008_en.htm

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

Conclusions

- Trust is complex (depends on technical, organizational, legal aspects) and transient: its validity can be restricted also by time.
- Necessity of a translation infrastructure between different contexts (cross-sectors, cross-geographical/political/jurisdictional areas)
- Concrete scheme mappings to be provided by authorities (e.g. bilateral agreements) => difficulty to reach global agreements on LoAs / technical + organizational criteria
- Trust Translation Schemes are ultimately the result of a political negotiation
- Trust services need to be high quality instrument of legal certainty to reassure customers, protection of emerging trust in digital services
- Building contacts for EU-wide and international relationships to support frontier-less international trust services

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

Thank You

Alberto Crespo

Head of Identity & Privacy Laboratory

Atos Research & Innovation

alberto.crespo@atos.net

https://atos.net/en/insights-and-innovation/innovation-labs#research

http://booklet.atosresearch.eu/content/identity-privacy

Worldwide IT Partner

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