How the DNS Can Support Identification and Trust Services

**Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Stakeholders and Trust schemes**
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
What LIGHT$^{est}$ is and what LIGHT$^{est}$ is NOT

- LIGHTTest **is not** an alternative to eIDs or business registers
- LIGHTTest **does not** allow you to outsource trust decisions
- LIGHTTest **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**
- !
LIGHTest 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
Electronic Transactions & Automated Trust Verification
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).
Automated Trust Verification

- Automatic Trust Verification relies on 2 items: The individual Trust policy, and the Electronic Transaction itself
Prerequisites to Automate Verification of a Trust Policy

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

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

- Discovering where the Trust Policy details are located
  - Where can the counterparty’s policy be found reliably?
Discovering the Location of Trust (Schemes/Lists/Translations)
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
Question: How does the trust verifier find the trust-related documents relevant for verification?
- Which documents might be relevant?
- Where are they?
DNS in LIGHTest: Publishing

- Domain names as identifiers for trust entities
  - trust services
  - trust schemes
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
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.
Translating Trust-
Trustworthy Communication Services Pilot

Bilateral agreements, etc.
Bilateral Agreements in eIDAS regulation

of 23 July 2014
on electronic identification and trust services for electronic transactions in the internal market and
repealing Directive 1999/93/EC

- **Article 14: International Aspects**

  “TS provided by TSPs established in a 3rd country shall be recognised as legally equivalent to
  QTS provided by QTSPs established in the Union where the TS originating from the 3rd
country are recognised under an agreement 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
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
TTA: Trust Translation Authority Supports Automated Trust Verification

TTA allows interop. of trust schemes published by different entities, even across different trust domains, by defining the relation between the trust scheme levels.

- 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
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 between themselves whether their schemes trust each other and in what way (levels): as a result, they provide Trust 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 between a Trusted Scheme and a Recognized Scheme requires to fulfill all conditions in both of them.
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
Example of Trust Translation (Conditional, Ordinal Translation)

- **Conditional translation**

  \[
  \text{translate\_conditional\_level}(\text{EU, US}) \leftarrow \\
  \text{extract(} \text{EU, inperson, true}) , \\
  \text{extract(} \text{EU, loa, 3}) , \\
  \text{extract(} \text{US, level, b}).
  \]

  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**

  \[
  \text{translation}(\text{EU, US}) \leftarrow \\
  \text{extract(} \text{EU, schemename, EUNAME}) , \\
  \text{extract(} \text{US, schemename, USNAME}) , \\
  \text{ordinalTranslation(} \text{EUNAME, USNAME}) .
  \]

  \[
  \text{ordinalTranslation("eu-loa-1","us-c")}. \\
  \text{ordinalTranslation("eu-loa-2","us-c")}. \\
  \text{ordinalTranslation("eu-loa-3","us-b")}. \\
  \text{ordinalTranslation("eu-loa-4","us-a")}. \\
  \]
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:
  - MyMailbox
  - MyNotification
- Published in LIGHTest framework by means of the Trust Scheme Publishing Authority (TSPA)
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*.

- Evaluate & assess communication LoA (e.g., eIDAS low/medium/high) on specific subscribers communications.
**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.
Correos eDelivery Trust 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
Trust Translation in Correos scenario: MyMailbox (Publication)
Trust Translation in Correos scenario: MyMailbox (Verification)
Visualization of LIGHTest Verification
Seizing Opportunities: eIDAS & Digital Single Market

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

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)
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
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