State-of-the-Art Analysis

Preliminary

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

Confidential Information – Not to be distributed outside of the LIGHTest Consortium
Agenda

- Foundation of Contributing Partners
- State-of-the-Art Analysis Structure
- Topics of Discussion
- Contact and Future Collaboration
Foundation of Contributing Partners

**Academic Partners**
- Fraunhofer Gesellschaft
- Graz University of Technology
- Technical University of Denmark
- Tübitak
- University of Stuttgart

**Industry Partners**
- ATOS Spain SA
- G&D
- Open Identity Exchange OIX
- IBM
- GMO Global Sign
Agenda

- Foundation of Contributing Partners
- State-of-the-Art Analysis Structure
- Topics of Discussion
- Contact and Future Collaboration
State-of-the-Art Analysis Structure

- Trust Schemes, Lists, and Formats
- Device Attestation Schemes
- Relevant Delegation Schemes
- Relevant Trust Policies and Policy Language
- Trust Translation Schemes
- Best Practice Derivation Schemes for Mobile Identity
- Best Practice of Interaction Design
Agenda

- Foundation of Contributing Partners
- State-of-the-Art Analysis Structure
- Topics of Discussion
- Contact and Future Collaboration
Discussion Topics

- Trust Schemes, Lists, and Formats
- Device Attestation Schemes
- Relevant Delegation Schemes
- Relevant Trust Policies and Policy Language
- Trust Translation Schemes
- Best Practice Derivation Schemes for Mobile Identity
- Best Practice of Interaction Design
Discussion topics

What we have so far

Where we want to further explore

Known Concerns, Questions, and Insights

Any Questions, Concerns or Comments? Let's Talk!
Trust Schemes, Lists, and Formats

Some Trust Lists and Formats we looked at:

- EU Trusted List and Member States Trust Lists
  - ETSI TS 102 231, TS 119 612
- Microsoft Certificate Trust List
- Adobe Approved Trust List
- eduRoam / eduGAIN
- ETSI Signatures and Infrastructures
- NISTIR 8149 Trust Frameworks to Support Identity Federation
- RFC5914 Trust Anchor Format
- RFC5934 Trust Anchor Management Protocol
- RFC6024 Trust Anchor Management Requirements
Initial Abstraction of Trust Schemes

Data Type

- **Boolean**
  - e.g. qualified services, white and black lists

- **Ordinal**
  - Level of Assurance, Reputation Rating

- **Generic Tuple of Attributes**
  - e.g. from business register

Temporal Model

- **Snapshot**
- **Historical**: Sequence of Change Events
Trust Schemes, Lists, and Formats

- Any suggestions or recommendations from previous experiences?

- Any further information on potential trust schemes that don't fit in the abstraction?

- Any additional Trust Schemes that have been missed?

- Thoughts or Concerns?
Device Attestation Schemes

- Divided into Hardware, Software, and Hybrid based Device Attestation Schemes
- Focus is on Verification of Software Running on the Device (Remote or closed)
- Hardware Device Attestation Schemes
  - Trusted Platform Modules
  - Trusted Execution Environments
  - Special CPU instructions
- Software Device Attestation Schemes
  - Software based approaches
- Hybrid based Device Attestation Schemes
  - Minimalized Hardware-use
Device Attestation Schemes

- In order to be successful, Lightest needs to be flexible enough to accept all of these types of Device Attestation Schemes

- Suggestions or Experiences on any of these Device Attestation Schemes?

- Insight on preforming remote attestation to devices?
Trust Translation Schemes

Authoritative Trust Translation Schemes
• A standard or legal norm determines (authoritatively) how a translation (or mapping) of trust or identity assurance should be carried out between two different schemes
• Considered cases of: eIDs, eSignature, eSeals, eTimestamps, eDelivery, website authentication
• International Mapping

Reputation Based Trust Translation Schemes
• Reputation of a given service (or its provider) is determined by different means:
  • By rating mechanisms accessible to stakeholders involved in the use of the services
  • Made public, allowing for comparison and potential mapping across different providers and countries.
Trust Translation Schemes

- Authoritative Trust Translation Schemes
  - Under eIDAS, trust service providers and their services can be broadly classified between “Qualified” and “non-qualified” due to what requirements are met regarding Regulation
  - Cases Considered often did not include Trust Schemes but rather a variety of different Assurance and rating levels
Trust Translation Schemes
Questions, Concerns and Future Direction

- There are a Lack of Trust Translation Schemes in use
  - Sometimes due to Maturity of Services

- Lack of Sources on Applicable Standards and Legal Norms in Non-EU countries

Future Direction:
- Establish and Maintain Dialogue with Policy Decision Makers and Industry at International Level
- Focus on International Aspect of eIDAS regulation between EU countries and 3rd party countries and international organization
Content and Future Contribution

- Please contact me:
  Rachelle Sellung
  University of Stuttgart
  rachelle.sellung@iat.uni-stuttgart.de

- Interest in Participating in Potential Business Use Cases? Let’s Talk!