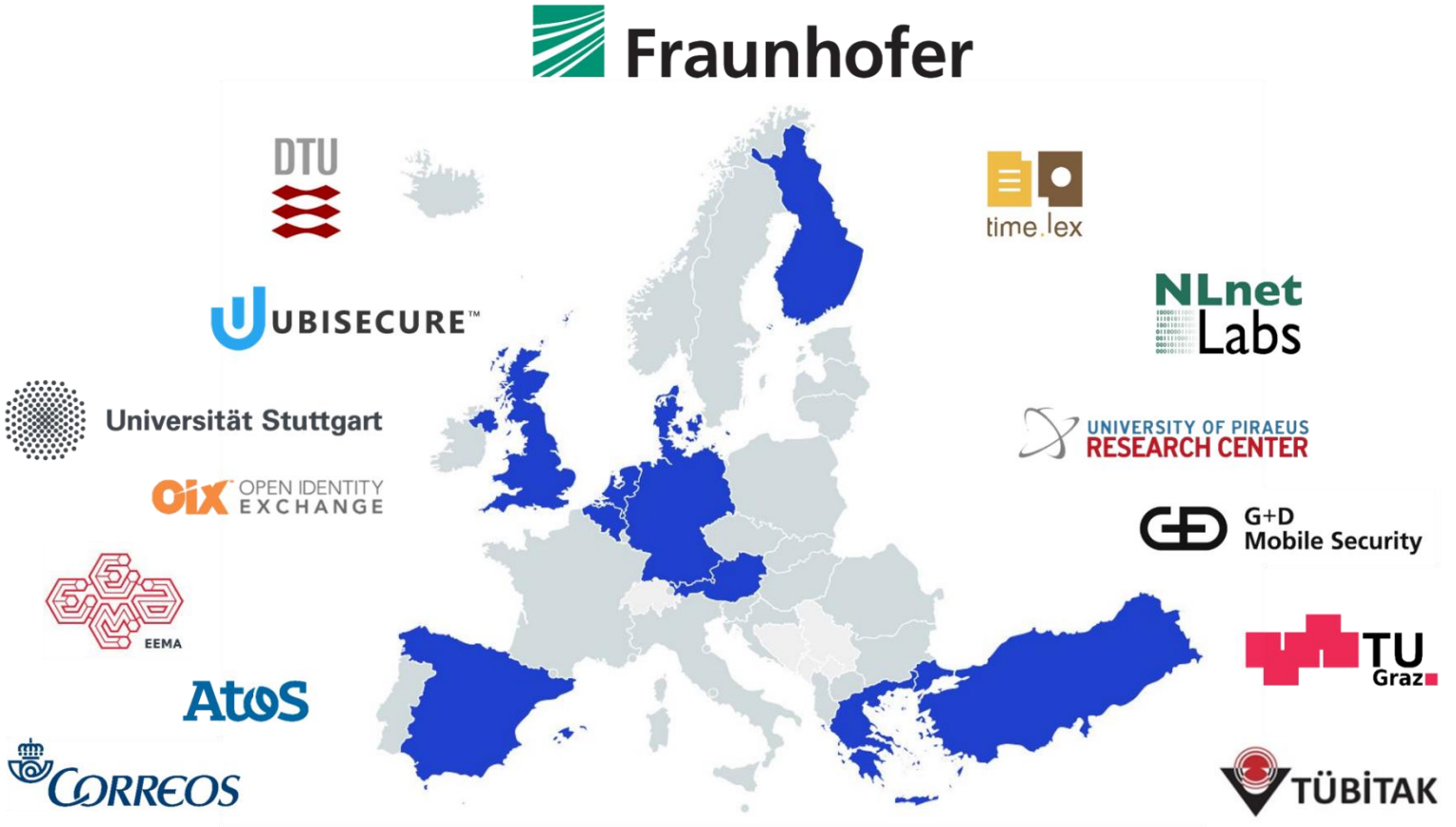
LIGHTest State of Play

April 30th 2019



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

Trust in a changing world

In the old days

- our world was smaller
- we knew our business partners
- Deals were sealed in personal contact

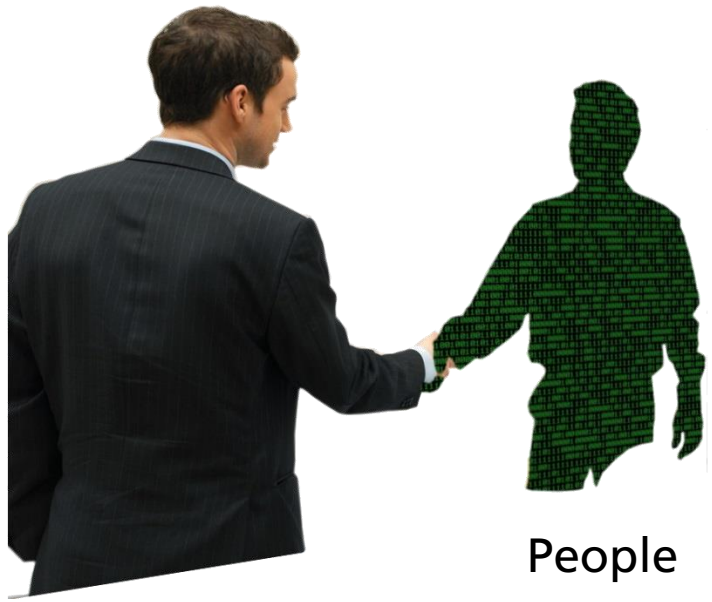
Increasingly

- we operate Europe- or World-wide
- we don’t know our business partners
- Deals are sealed remotely through Cyberspace

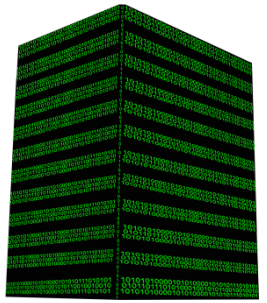
LIGHT*est* has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

Transactions are increasingly conducted virtually

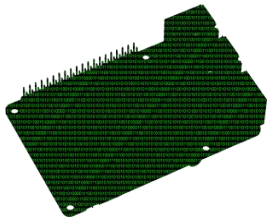
We have virtual transactions with..



People



Organizations



Devices/Things

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

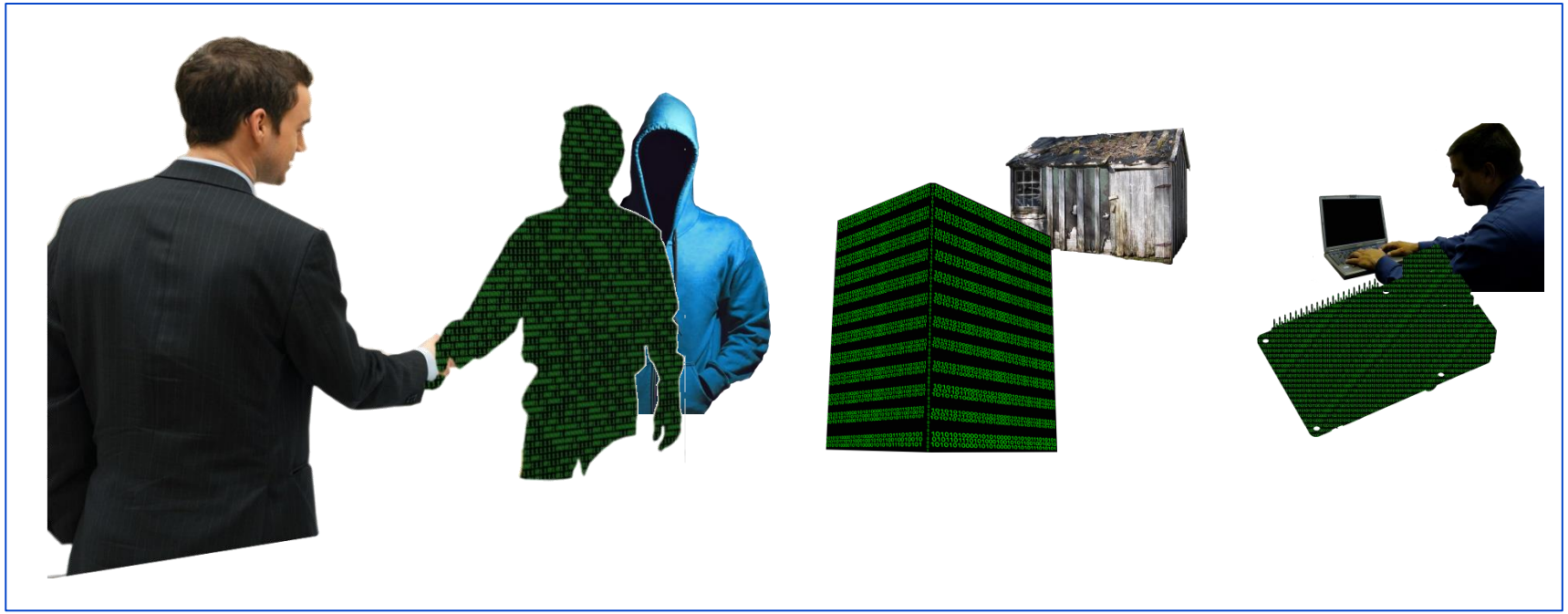
But who is really behind the electronic identity?

As expected from the appearance:
Trustworthy -- legitimate

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

But who is really behind the electronic identity?

Not what we expect!!!
Untrustworthy -- fraud

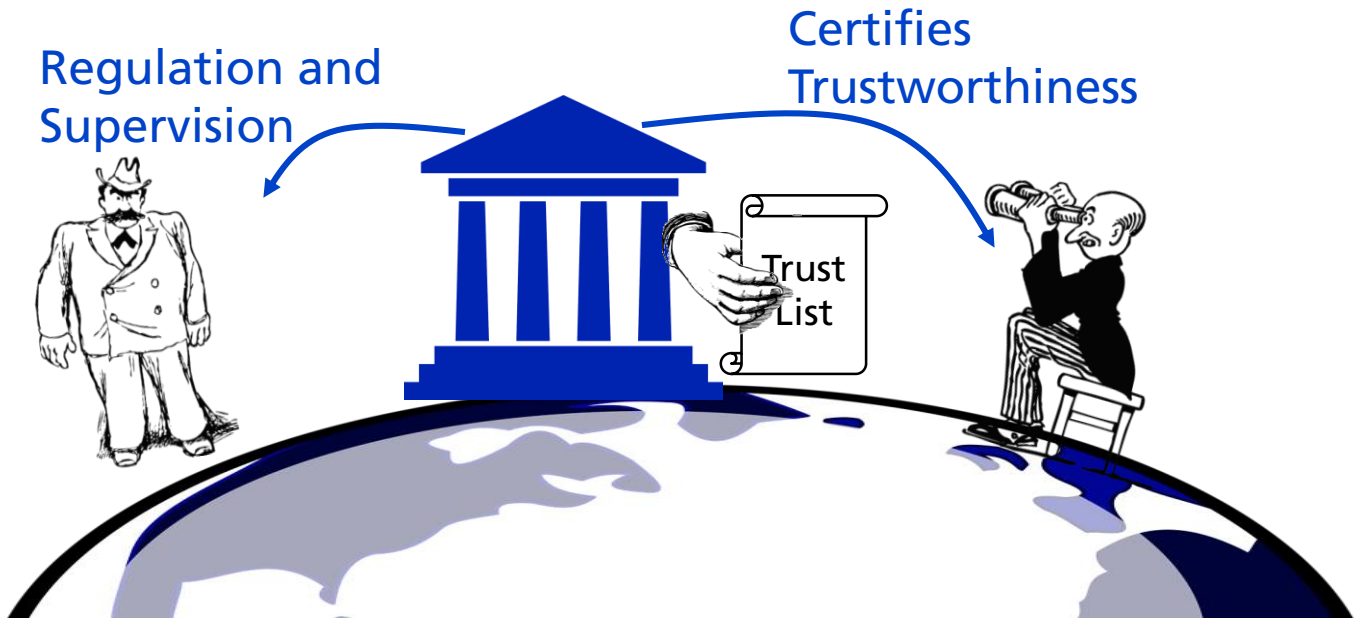


LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

How can we know whether a remote someone/something is trustworthy?

We need Help:

- Trusted **Authorities**
- Trusted Third Parties that publish **Reputation** Ratings



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

Trust Domains

- Verification is done by following the chain of trust (certificate chain) until you reach the trust anchor (root certificate)
  - Works well within a single trust domain

- But what about transactions between entities from different trust domains?
  - Different root certificates
  - Trust has to be established
  - Could be done with a trust list containing the root certificates or a list of lists

➢ **A global trust list would solve this problem**

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

How realistic is a global trust list?

- Who would operate and control that trust list?
  - US?, EU?, Russia?, China?
  - UN?, FIFA?
  - Facebook?, Google?
- What about the entries?
  - How is it ensured that they are genuine?
  - Do I have to trust them?
  - Are they being trusted automatically?
  - What about Levels of Assurance?

➢ **We need a better approach**

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

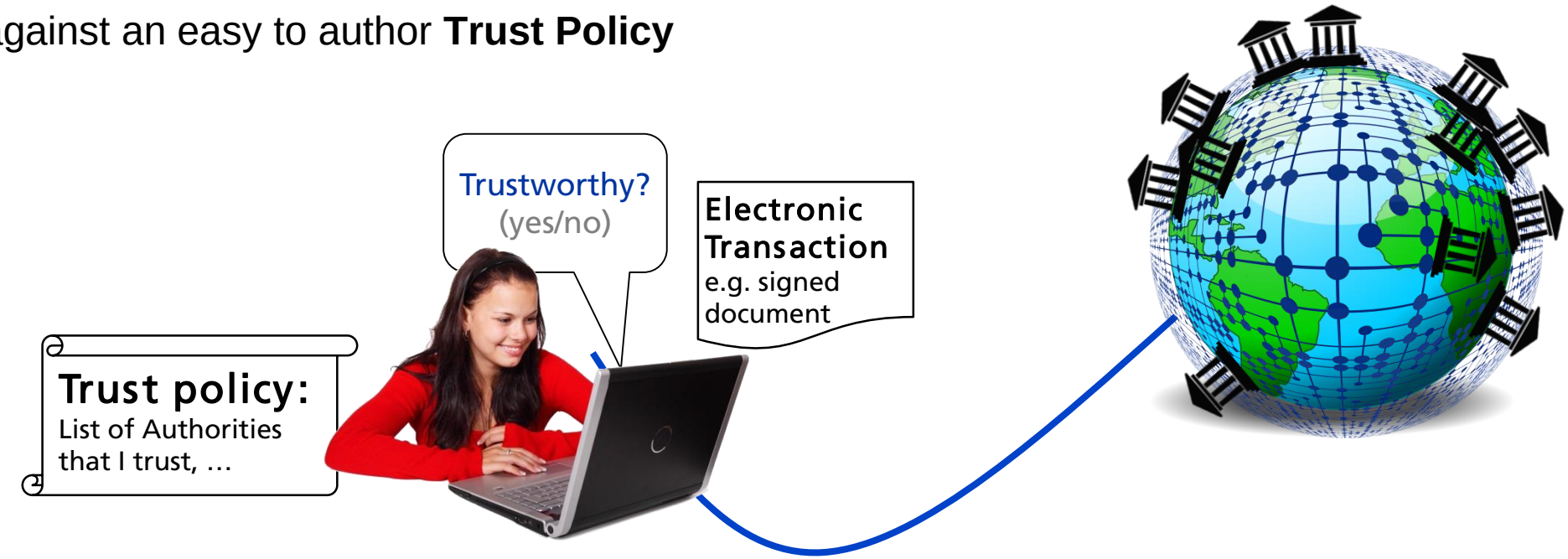
Authorities:

- 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? Trust Policy and Automatic Trust Decisions

- Make it automatic for Verifiers to **query Trust Lists**
- Combine multiple queries to **validate**
  - an **Electronic Transaction**
  - against an easy to author **Trust Policy**



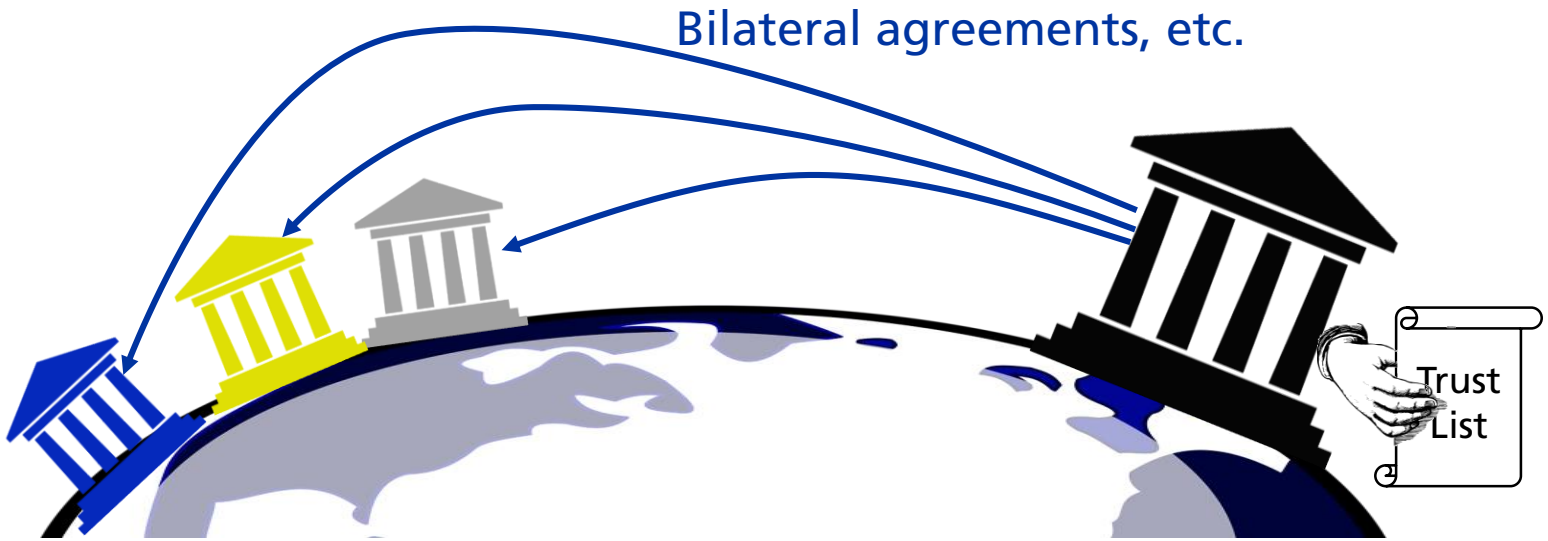
LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

What does LIGHT*est* do?

Infrastructure for the Translation across Trust Domains

Authority publishes Trust List on..

- ..which authorities from other trust domains are trustworthy
- ..how to translate foreign into native trust schemes
  - NIST: Level “3” == EC eIDAS: Level “substantial”



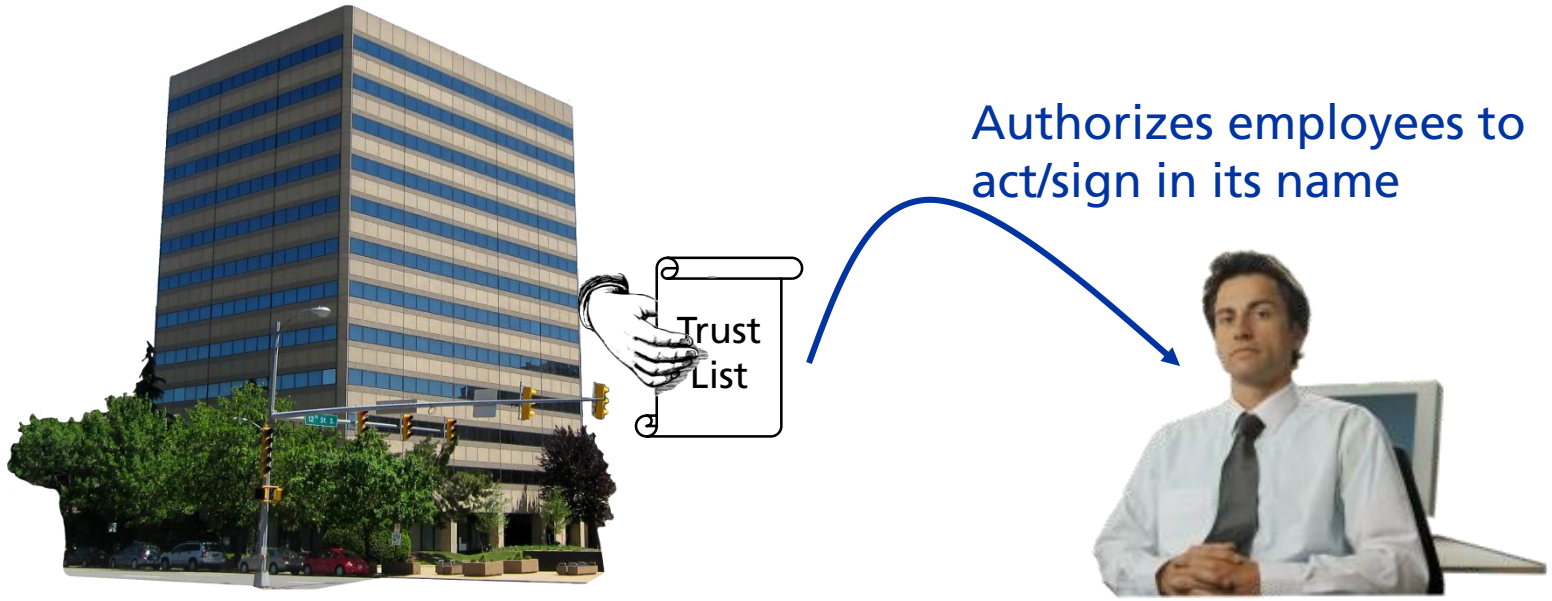
LIGHT*est* has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

What does LIGHT*est* do?

Infrastructure for the Publication and Querying of Delegations

Delegation:

- Organization publishes Trust List on..
- ..who can sign/act in its name for which purposes



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? Trust Propagation of Derived Mobile IDs

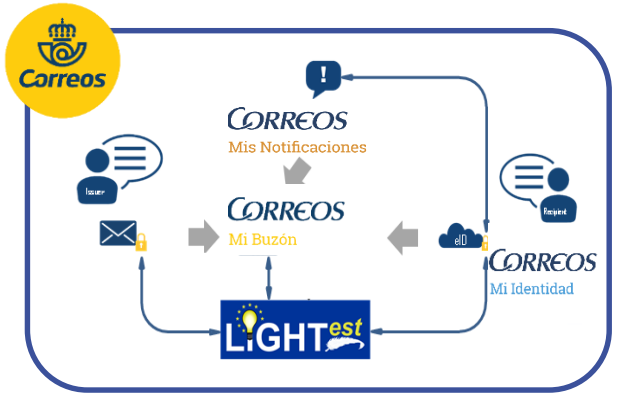
- Trustworthy through secure enrollment
  - Birth and population registers
  - in person issuance
- Often unfit for mobile use

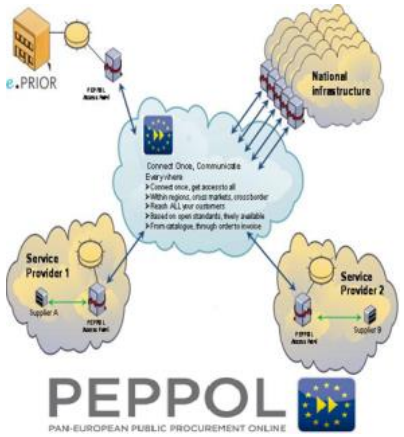
- Derive mobile identities from eIDs
- How does trust propagate???

- Currently lacks highly trusted electronic identities

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? 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

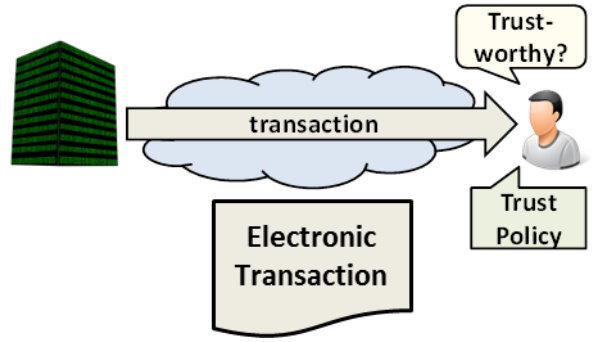
PEPPOL e-Procurement (by UPRC)

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

LIGHT^{est} *in a nutshell: Goal*

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

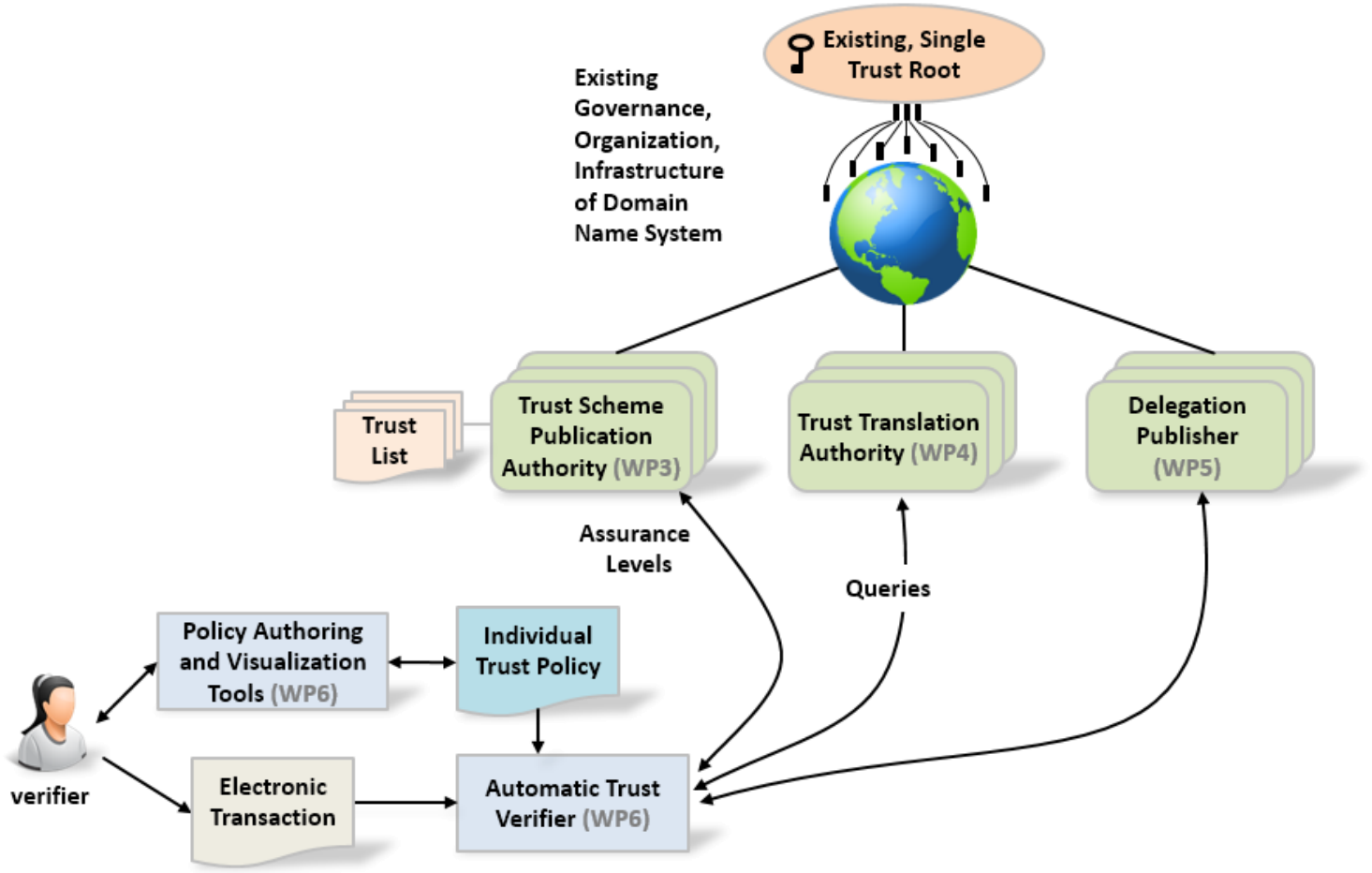
LIGHT^{est} has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

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 information
  - Verify ID information
  - Determine trust assurances behind it
  - Facilitate your own decision making
- While also providing a growth path for future European ID policy!

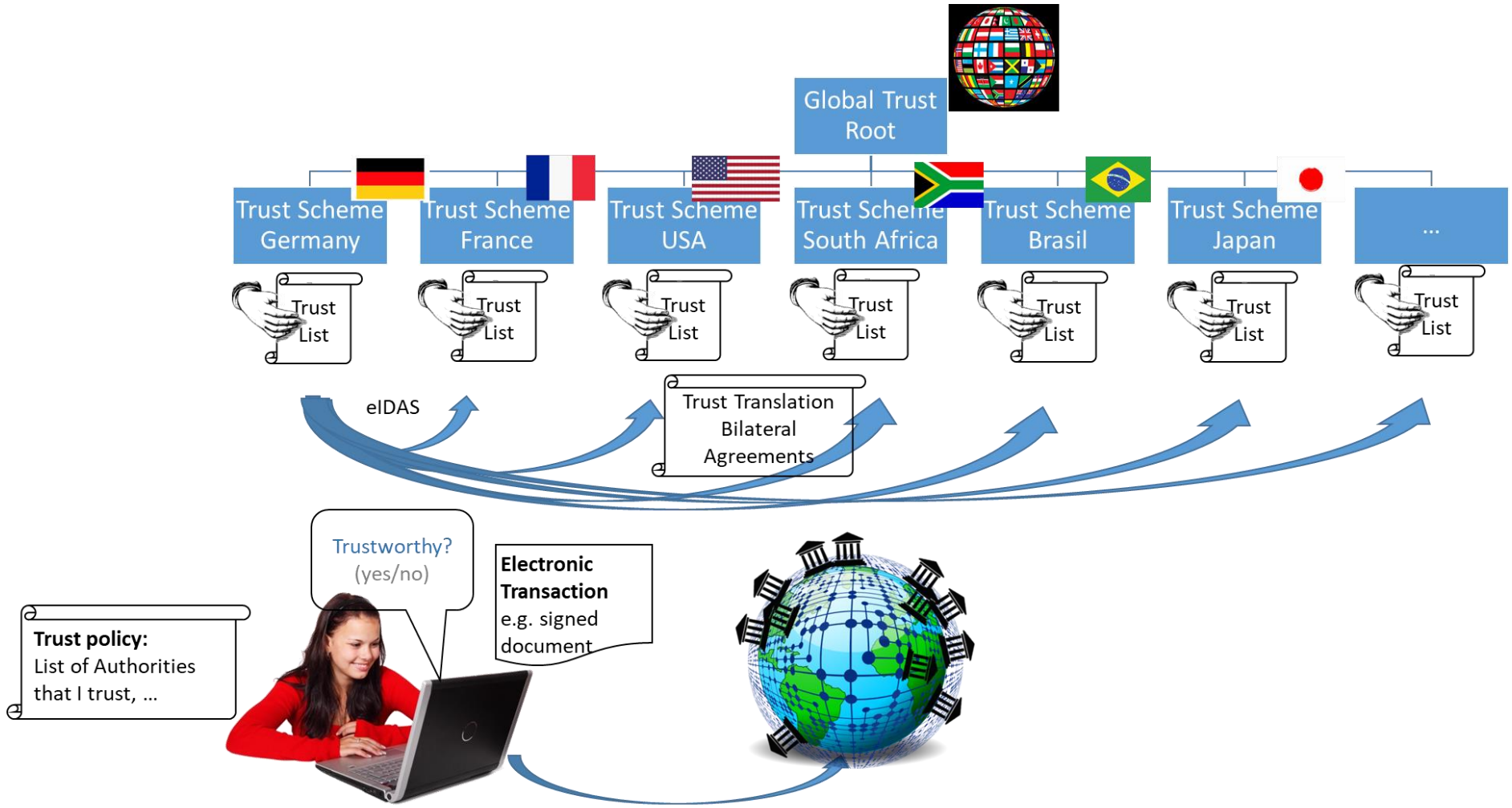
LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

The LIGHT*est* Architecture



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

Control remains locally – Source can be verified

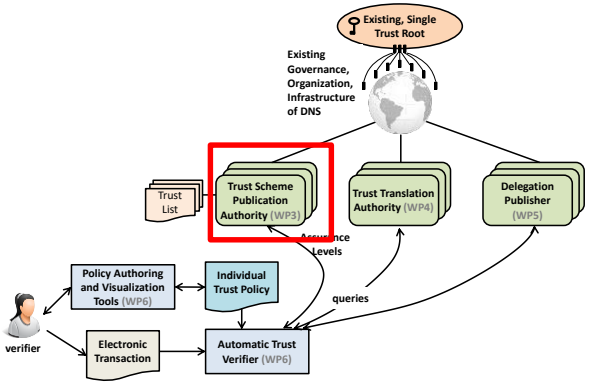


LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

TSPA: Infrastructure for Publication and Querying of Trust Schemes

Publication of Trust Schemes

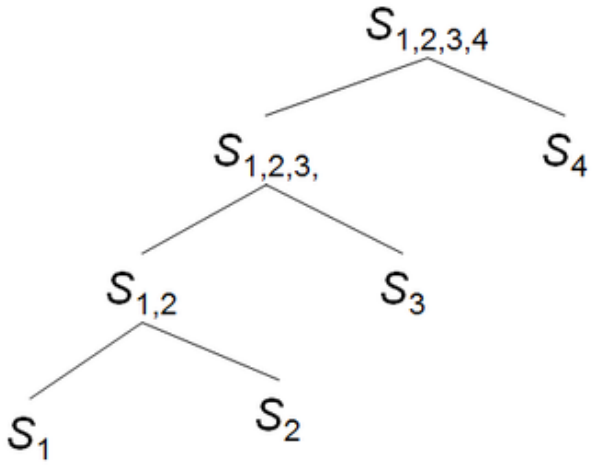
Type of Trust Scheme Publication	Example	Verifiable Information
Boolean	ETSI_EN_319_401	Compliance of an entity to a trust scheme
Ordinal	LoA4.ISO29115	Compliance of an entity to an ordinal value of a trust scheme
Tuple-Based	{(authentication:2Factor), (identityProofing:inPerson)}	Requirements of a trust scheme



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

Tuple-Based Trust Scheme Publication: Methodology

- Development of Unified Data Model for Tuple-Based Trust Scheme Publication
  - Bottom-up modelling approach for identification of requirements
- Consolidation using existing trust schemes
  - identify requirements of selected trust schemes
  - consolidate towards a unified data model
- Development of the Data model
  - structure requirements in hierarchical form of abstract concepts
  - transfer concepts into tuples (attribute_name, attribute_value)
  - publish tuples as a sequence of attributes



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

Examined Trust Schemes

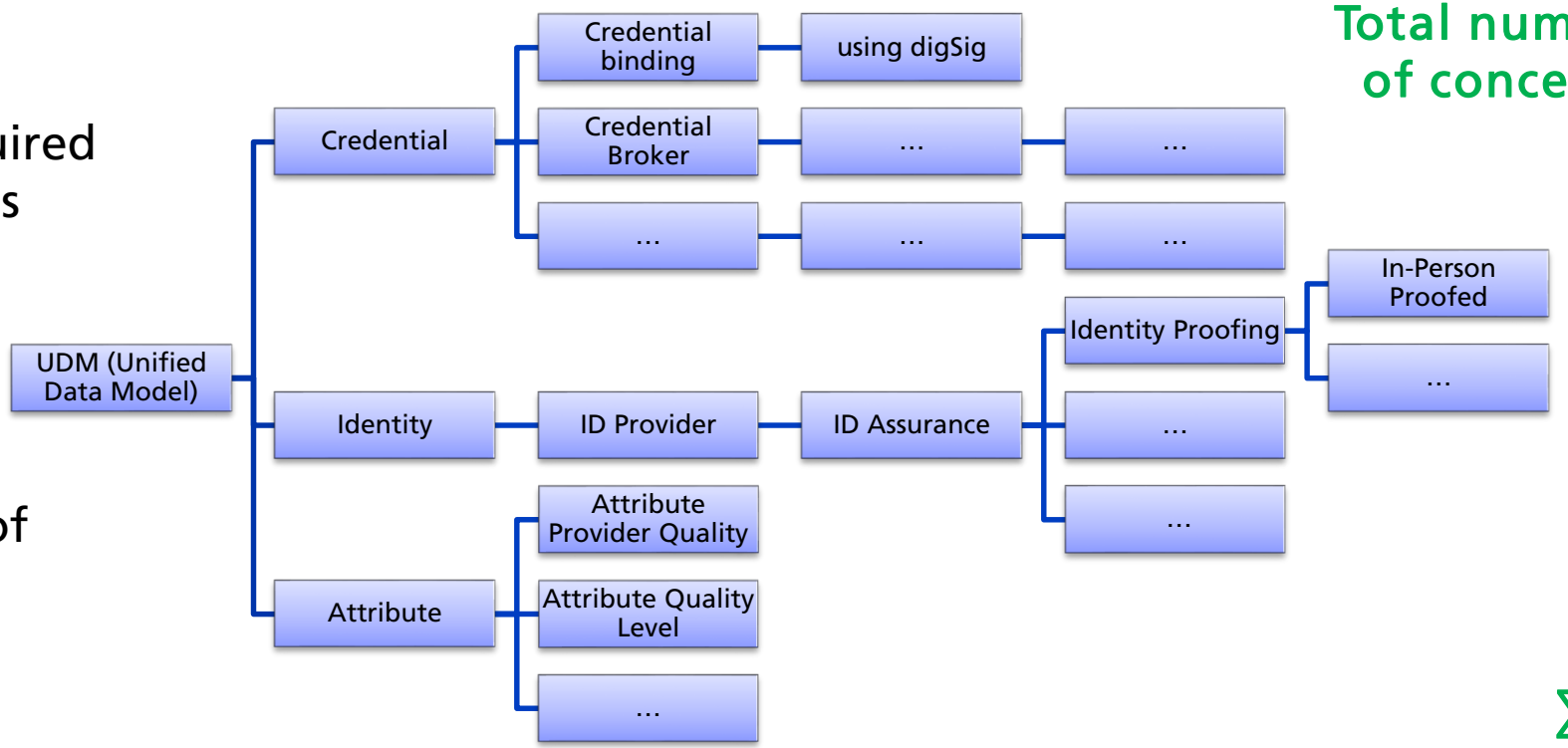
Input Scheme 1	Input Scheme 2	Consolidation Result	Saturation ΔS (min ΔS)
ISO/IEC 29115	PCTF	Data Model v0.2	n.a.
Data Model v0.2	FIDO	Data Model v0.4	3
Data Model v0.4	QAA/AQAA, eIDAS	Data Model v0.6	9
Data Model v0.6	Chinese Electronic Signature Law	Data Model v 0.6 (Data model of D3.1)	0
Data Model v0.6	Turkey eSig Law	Data Model v0.8	1
Data Model v0.8	MTF	Data Model	1
Data Model	Trust Scheme of Azerbaijan	Data Model	0
Data Model	UICC	Data Model (see Sections 7.2.7 and 7.4)	0

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

Data Model for Tuple-Based Trust Schemes: Development -1

- Conceptualization of data model
  - structure identified requirements of consolidation in hierarchical form of concepts

➢ Result: 3 abstract concepts required for description of Trust Schemes
  - Credential
  - Identity
  - Attributes
- each of them contains list of concepts involved



Total number of concepts:
62
27
9
∑ 98

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

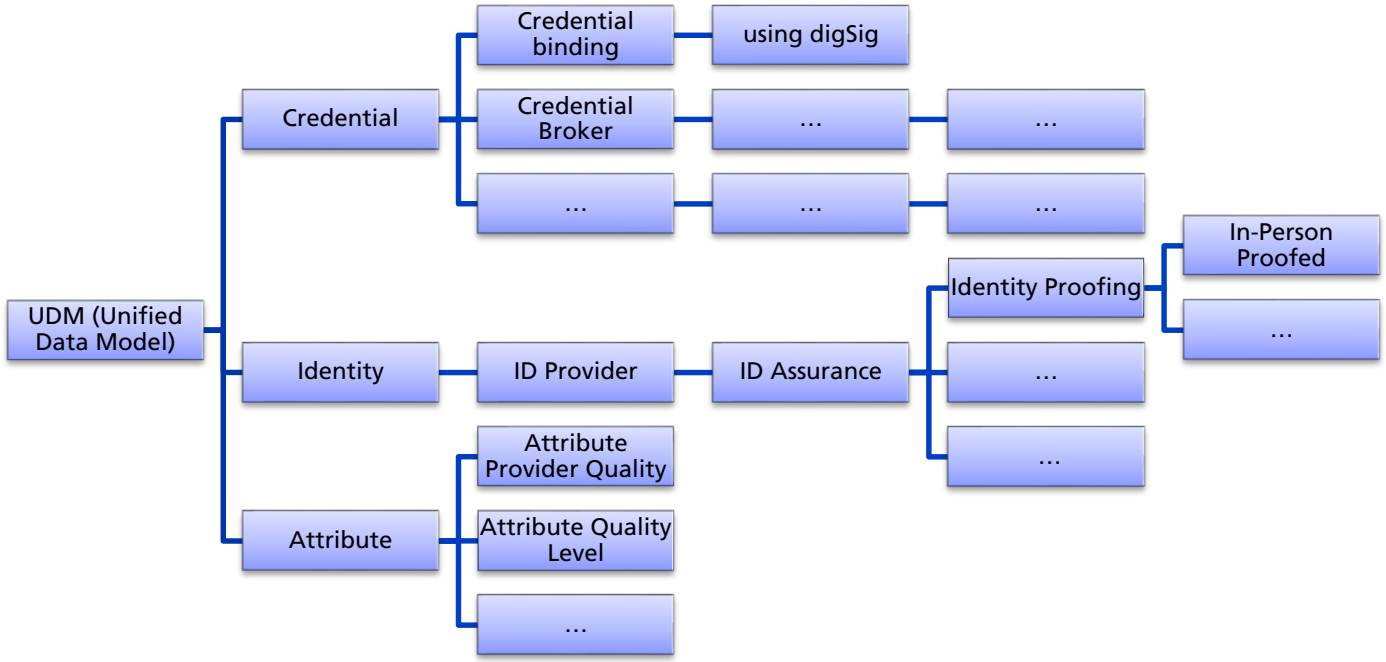
Data Model for Tuple-Based Trust Schemes: Development -2

- Development of the data model
  - Concepts are reviewed regarding their attribute domains
  - Each concept is transferred into tuples:

  data pair (attribute_name, attribute_value)

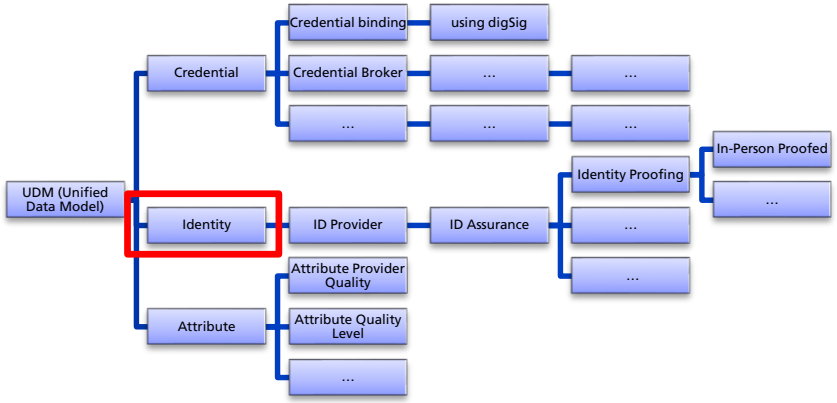
- Attribute values:
  - Boolean: e.g. In-Person Proofed
  - Integer: e.g. Time Limits
  - String: e.g. Credential Broker

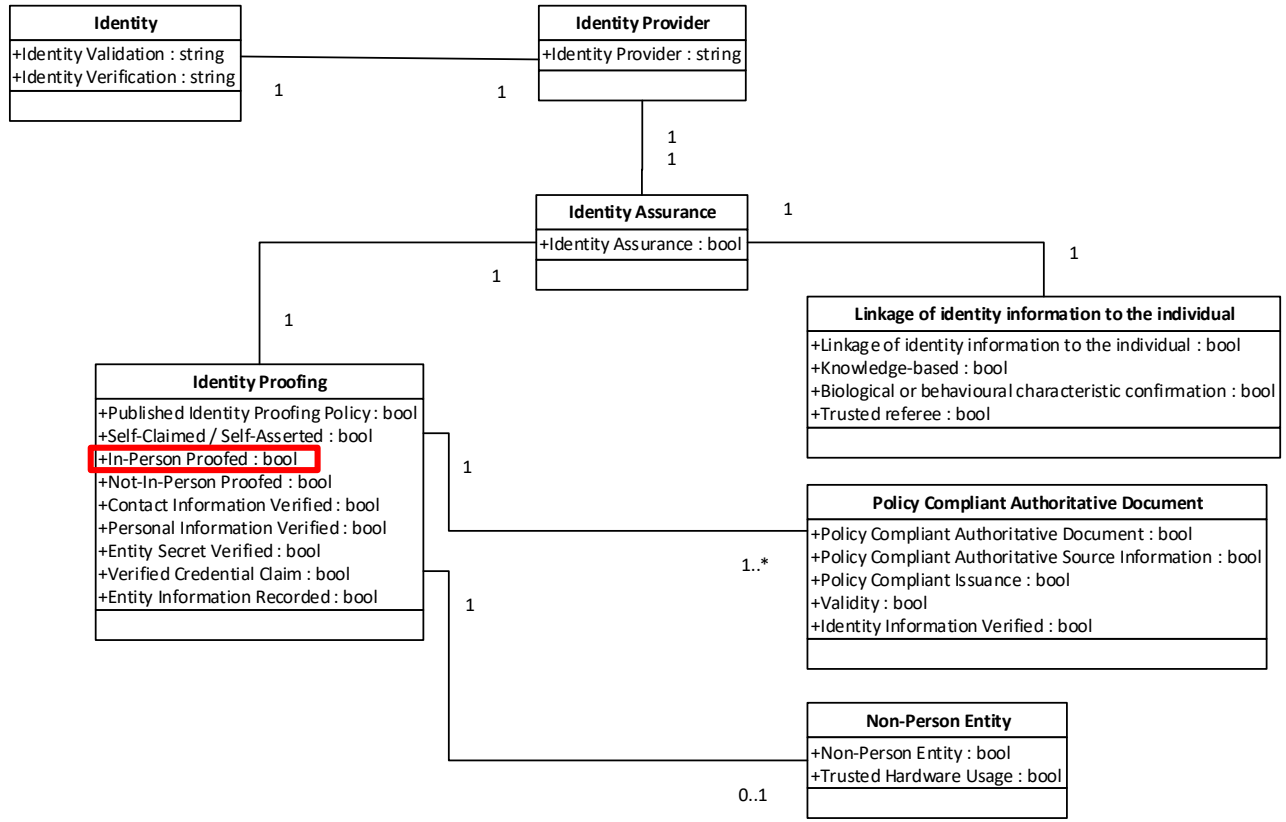
  →Most concepts (85 of 98) are boolean



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

Data Model for Tuple-Based Trust Schemes: Identity





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

UNHCR Workshops

- **Joint Workshop on Digital Identity related to ID2020**, Munich, Germany, 16 November 2017
- **UNHCR Workshop- LIGHTest collaboration**, Copenhagen, Denmark, 13 February 2018
- **UNHCR/LIGHTest Workshop**, Amman, Jordan, 9-10 July, 2018
- **Workshop Meeting** regarding UNHCR Trust Scheme Development, Copenhagen, Denmark, 05 Feburary 2019

DAFI

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

Some recent publications

Open Identity Summit – Garmisch-Partenkirchen

- Georg Wagner, Stefan More, Sven Wagner and Martin Hoffmann
  - DNS-based Trust Scheme Publication and Discovery
- Sven Wagner, Sebastian Kurowski and Heiko Roßnagel
  - Unified Data Model for Tuple-Based Trust Scheme Publication
- Sebastian A. Mödersheim and Bihang Ni
  - GTPL: A Graphical Trust Policy Language
- Stephanie Weinhardt and Doreen St.Pierre
  - Lessons learned – Conducting a User Experience evaluation of a Trust Policy Authoring Tool
- Isaac Henderson Johnson Jeyakumar, Sven Wagner and Heiko Roßnagel
  - Implementation of Distributed Light weight trust infrastructure for automatic validation of faults in an IOT sensor network

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

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