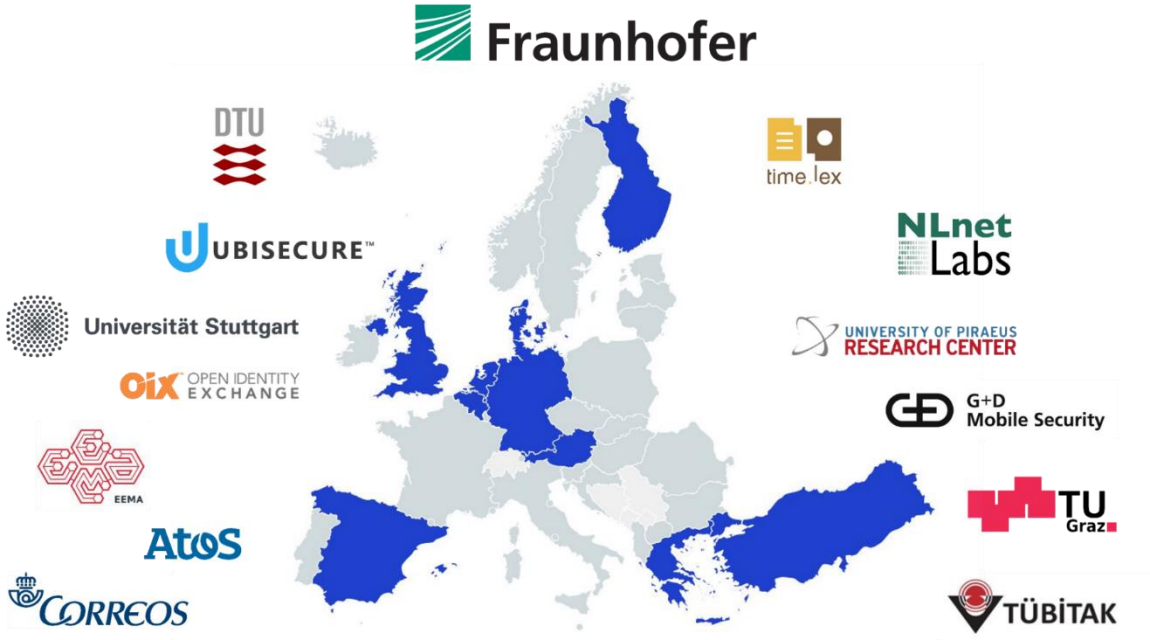
TSPA: Trust Scheme Publication Authority

Concept and Examples of Applications



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

Sven Wagner, University Stuttgart

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

Agenda

- Role of Trust Scheme Publication Authority (TSPA)
- Type of Trust Scheme Publication
- Concept of the TSPA
- DNS-based Publication of Trust Schemes
- Discovery of Trust Scheme Publication Authorities
- Tuple-Based Trust Scheme Publication

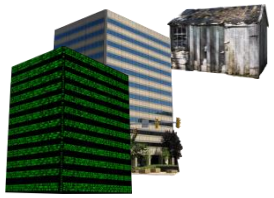
- Predictive Maintenance Use Case: sensor data verification in the IoT
- Use Case: PoC for a Trust Scheme for UNHCR DAFI program

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

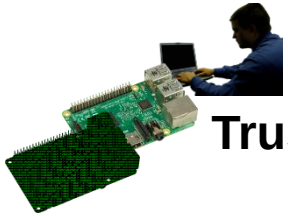
Motivation

- Transactions are increasingly conducted virtually

People



Organizations



Devices/Things

Untrustworthy -- fraud

Trustworthy -- legitimate

- How can we know whether a remote someone/something is trustworthy?
  - determine trustworthiness of involved parties
    - multitude of trust aspects and/or across borders, jurisdictions
- We need help:
  - Trusted Authorities
  - Trusted Third Parties that publish Reputation Ratings

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

Definitions Trust Scheme, Trust List

- Authorities
  - certify trustworthiness of eID of involved parties
  - operate Trust Schemes and publish Trust Lists

- Trust Scheme
  - comprises the organizational, regulatory/legal, and technical measures to assert trust-relevant attributes about enrolled entities in a given domain of trust
  - is operated by a Trust Scheme Provider

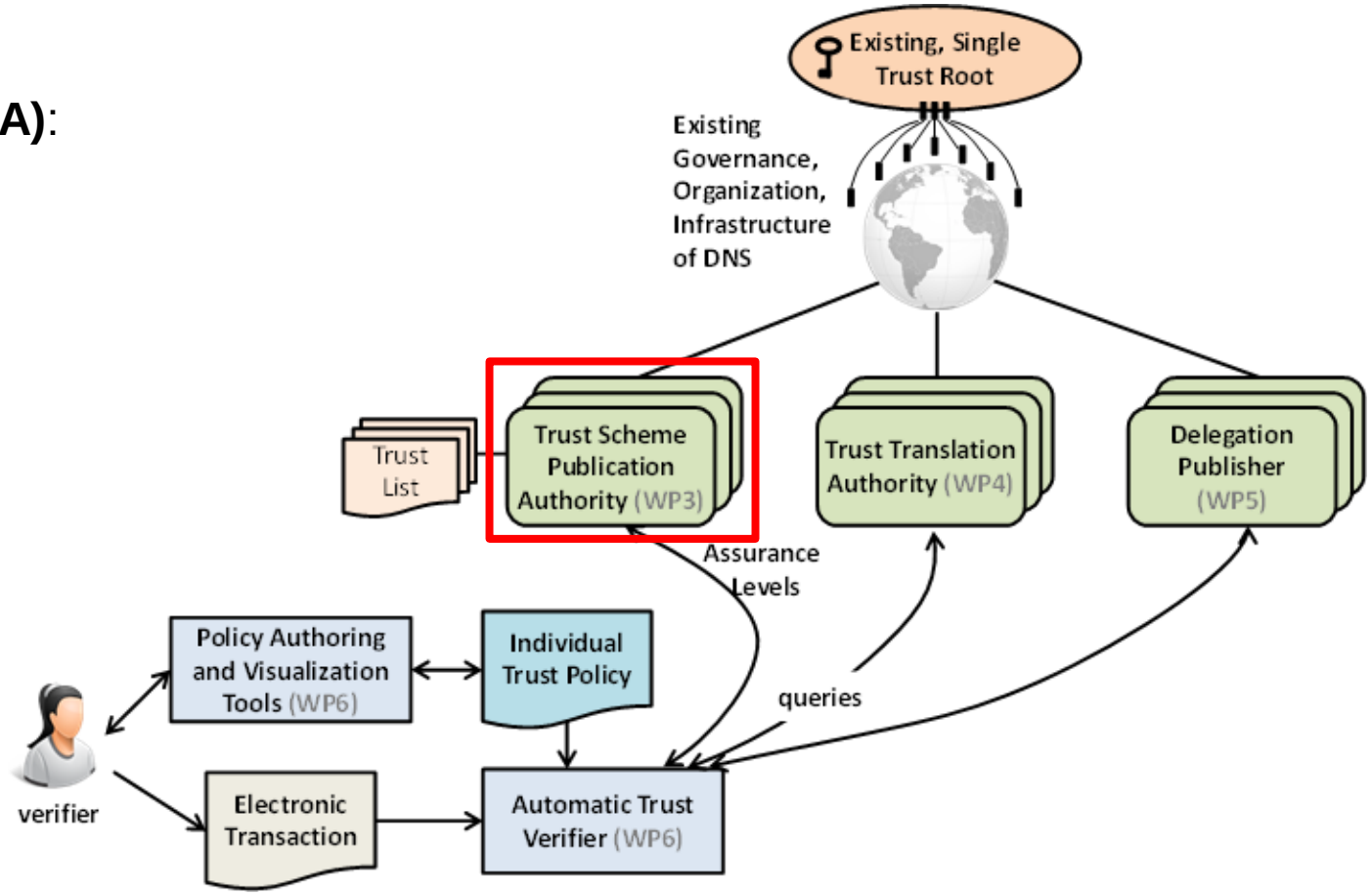
- Trust List
  - list of all the enrolled entities in a specific data file/format certified by the issuing authority
  - existing and widely accepted standard is ETSI TS 119 612

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

The LIGHT*est* Architecture

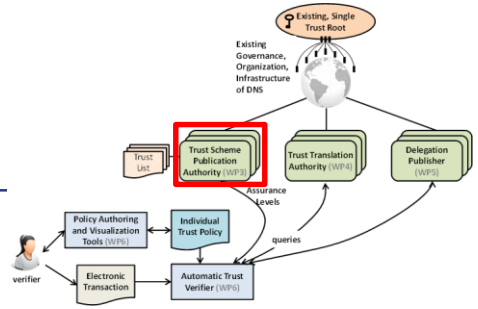
Trust Scheme Publication Authority (TSPA):

- Task: Provide an Infrastructure for
  - Publication of Trust Schemes &
  - Discovery and Verification of Trust Scheme Memberships



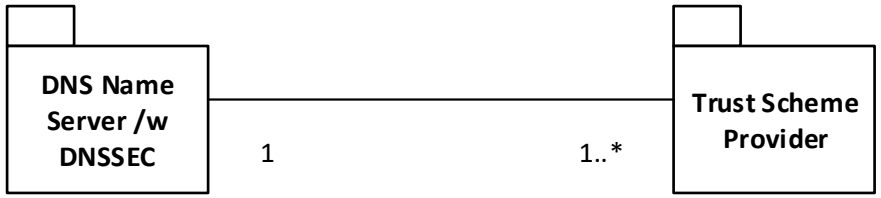
LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Trust Scheme Publication Authority (TSPA)



- **Task:**
  - Infrastructure for - Publication of Trust Schemes &
    - Discovery and Verification of Trust Scheme Memberships

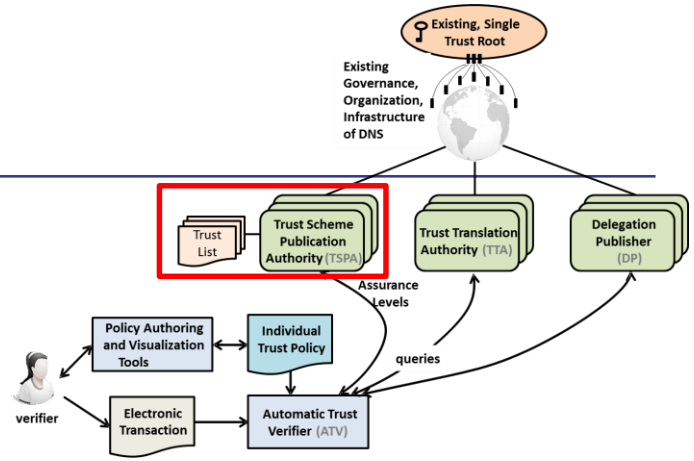
- **TSPA Components:**
  - DNS Name server with DNSSEC extension
  - Trust Scheme Provider(s)



- **Querying of Trust Schemes:**
  - DNS Name Server: discovery of associated Trust Scheme and Trust Scheme Provider
  - Trust Scheme Provider: signed trust list indicating that Issuer operates under the specific Trust Scheme (using existing standards on Trust Service Status Lists, e.g. ETSI TS 119 612)

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

Trust Scheme Publication Authority (TSPA)



Publication of Trust Schemes

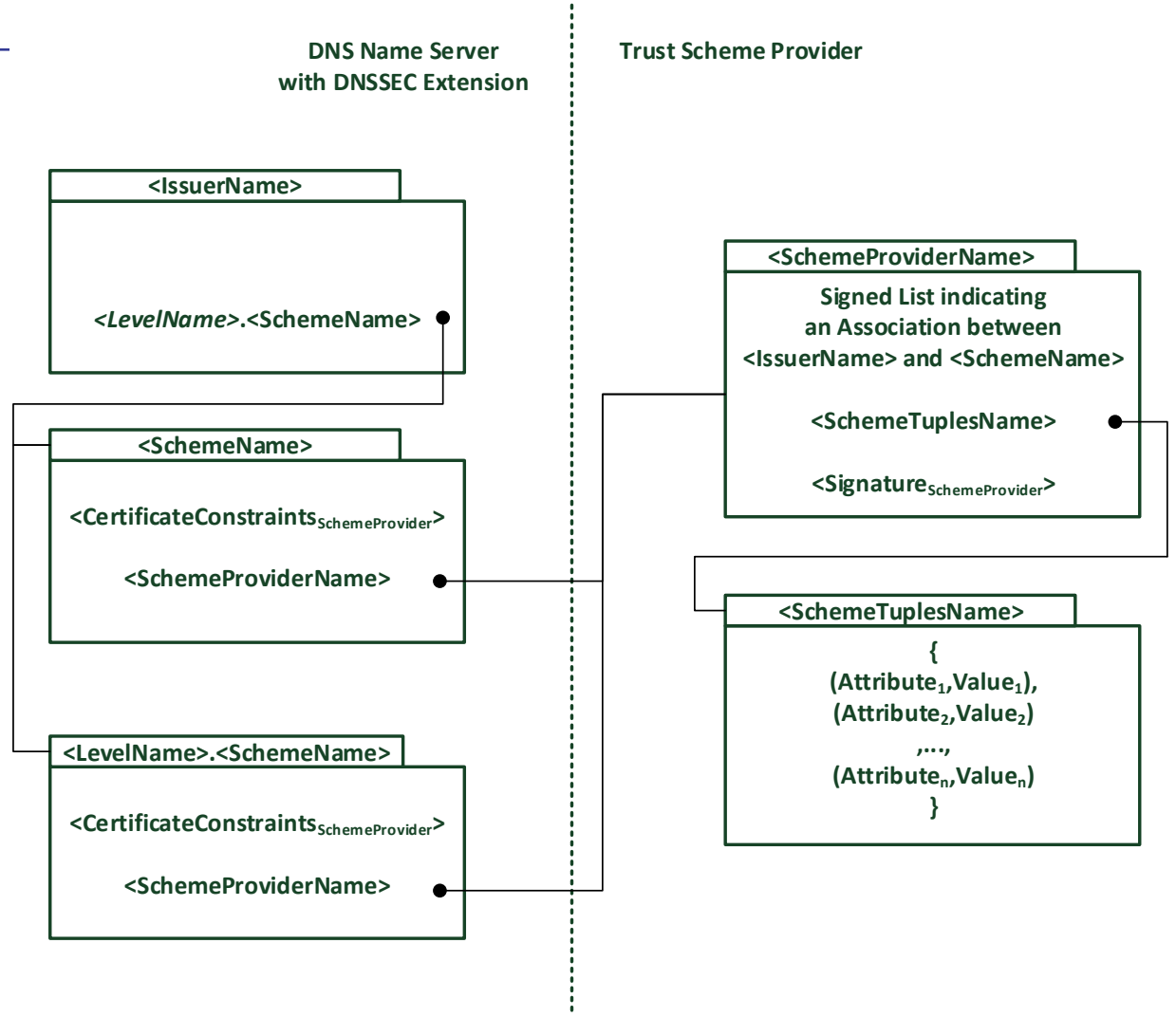
Type of Trust Scheme Publication	Example	Verifiable Information
Boolean	eSig Law of Turkey, FIDO	Compliance of an entity to a trust scheme
Ordinal	LoA4.ISO29115	Compliance of an entity to an ordinal value of a trust scheme
Tuple-Based	{(authentication:2Factor), (identityProofing:inPerson)}	Requirements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

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

Trust Scheme Publication Authority (TSPA)

Concept of the TSPA:

- DNS Name Server
  - discovery of associated Trust Scheme and Trust Scheme Provider
- Trust Scheme Provider
  - signed trust list indicating issuer operates under the specific Trust Scheme (using existing standards on Trust Service Status Lists ETSI TS 119 612)
  - Tuple-based representation of Trust Scheme

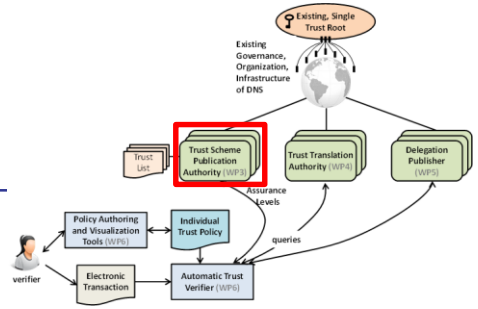


LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

DNS-based Publication of Trust Schemes

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

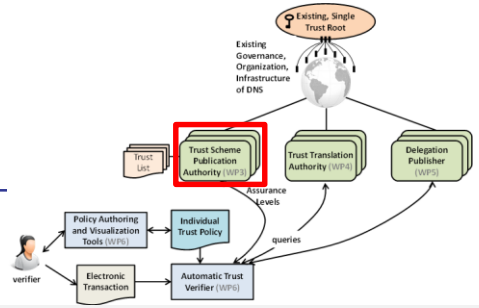
DNS-based Publication of Trust Schemes



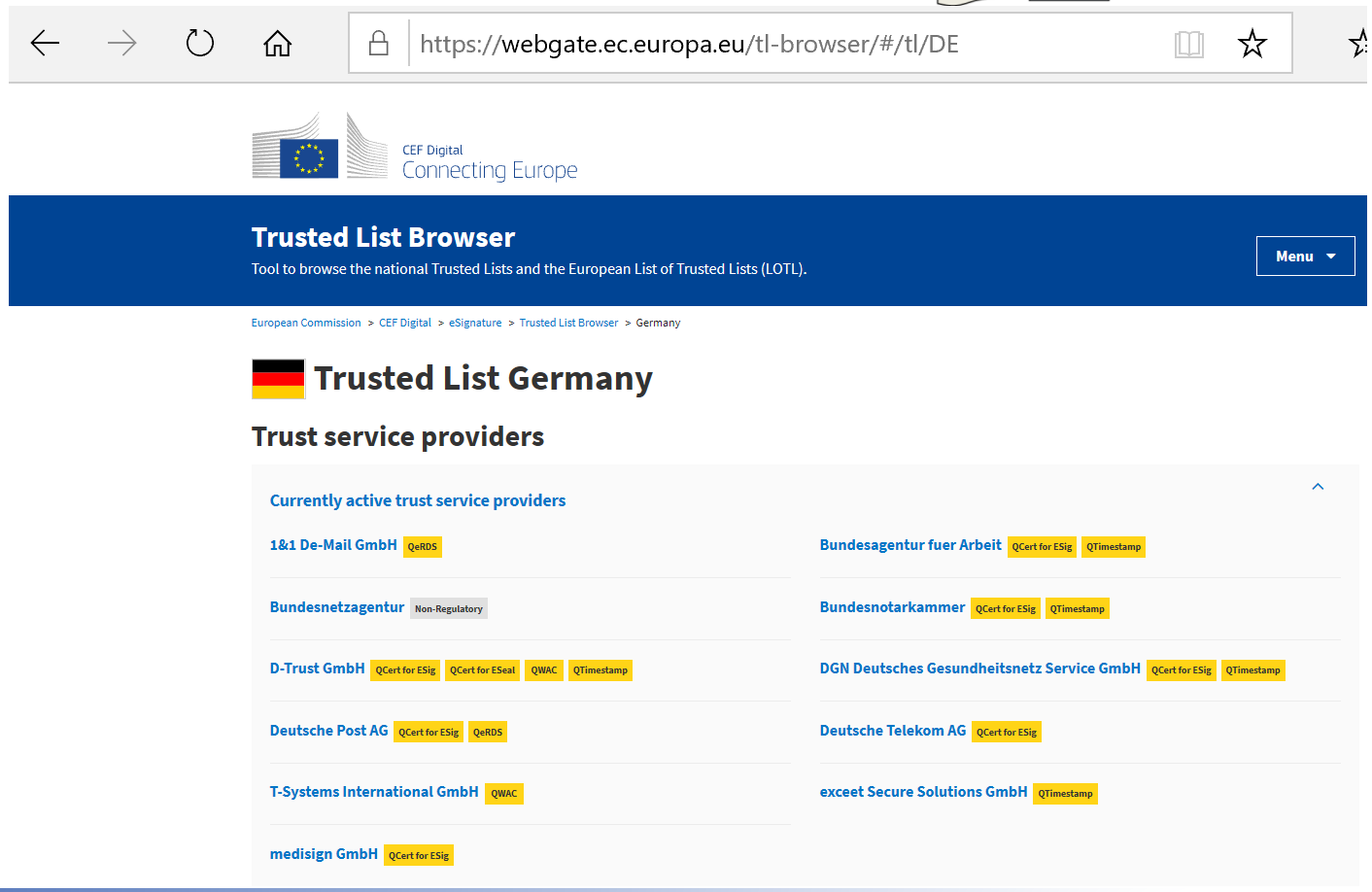
- Consolidated approach to Publishing Trust-related Information in the DNS was developped
  - specified for trust scheme membership publication
    - DNS Name server & Trust Scheme Provider(s)
      - additions in DNS RRs
        - Pointers, URIs
        - Certificate constraints: SMIMEA record data
    - Trust Scheme Provider(s)
      - publication of a signed Trust List (use existing standards: e.g. ETSI TS 119 612)
        - Trust-service Status Lists (TSLs) used in eIDAS

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

DNS-based Publication of Trust Schemes

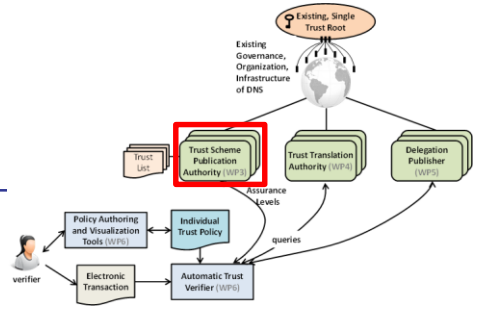


- **Example: eIDAS Germany**
- **qualified trust service provider D-Trust**



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

DNS-based Publication of Trust Schemes



- **Example: eIDAS Germany (with D-Trust as qualified trust service provider)**
- DNS Name server
  - Trust service provider points to trust schemes under the prefix ***_scheme._trust***
    - e.g. D-Trust: ***_scheme._trust. d-trust.net.***
  - Trust Scheme publishes its trust list under the prefix ***_scheme._trust***
    - Trust scheme owned by the German Federal Network Agency: **_scheme._trust.nrca-ds.de.**
    - Published Trust list: *https://www.nrca-ds.de/st/TSL-XML.xml*

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

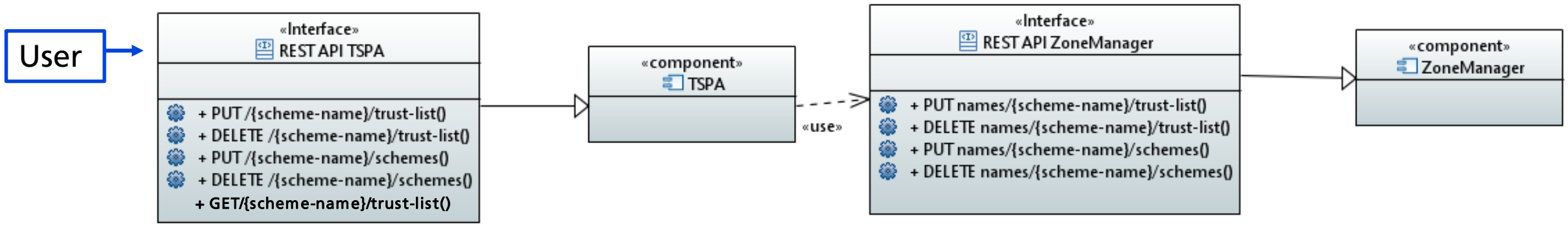
DNS-based Publication of Trust Schemes

- Sections of Published Trust list (ETSI TS 119 612): *https://www.nrca-ds.de/st/TSL-XML.xml*

```
<?xml version="1.0" encoding="UTF-8"?><TrustServiceStatusList
...
<SchemeInformation> ...
        <SchemeOperatorName>
            <Name xml:lang="en">Federal Network Agency</Name> </SchemeOperatorName>
...
 <SchemeName>
            <Name xml:lang="en"> DE:Trusted list including information related to the qualified trust service providers ... together
               with information related to the qualified trust services provided by them, in accordance with ... Regulation (EU) No
               910/2014 ... </Name>  </SchemeName>
 <SchemeTypeCommunityRules>
            <URI xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon</URI> </SchemeTypeCommunityRules>
...
<TrustServiceProviderList> ...
        <TrustServiceProvider> ...
              <TSPName>
                   <Name xml:lang="en"> D-Trust GmbH </Name>
              <TSPInformationURI>
                   <URI xml:lang="en">http://www.d-trust.de/</URI> </TSPInformationURI>...
              <TSPServives> ...
                   <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</ServiceTypeIdentifier> ...
...
<dsig:Signature ...>
        <dsig:X509Certificate>  ... </dsig:X509Certificate>  ... </dsig:Signature>
</TrustServiceStatusList>
```


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

DNS-based Publication of Trust Schemes



- Communication between components for
  - Publishing Data using the TSPA: create, modify and delete Trust Schemes
  - Retrieving Data from the TSPA: querying process
- RESTFUL API for TSPA and ZoneManager
  - Publish trust scheme on TSPA, TSPA will use the ZoneManager to publish the DNS records

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

DNS-based Publication of Trust Schemes

- **2nd Example for Publishing**:
  - Alice operates an TSPA and wants to create a *TrustSchemeAlice*
    - TSPA address: tspa.example.com
  - Alice can publish it by sending the following request:

    PUT https://tspa.example.com/api/v1/TrustSchemeAlice/trust-list TRUST LIST CONTENT

    → DNS-entries for discovery of Trust Scheme and Trust List are created; Trust List information is saved

    …

    ```
    scheme. trust.tspa.example.com. IN URI 1 1 https://tspa.example.com/api/v1/TrustSchemeAlice/trust-list
    ```

    …

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

DNS-based Publication of Trust Schemes

- **2nd Example for Publishing**:
  - Alice operates an TSPA and wants to create a *TrustSchemeAlice*
  - **The-Trust GmbH CA is a qualified trust service provider in TrustSchemeAlice**

  - Trust Scheme Membership claim for The-Trust GmbH CA is as follows:

    PUT https://tspa.the-trust.eu/api/v1/TrustSchemeAlice/schemes {"tspa.example.com", …}

    → This results in the following DNs record

    …

    `scheme. trust.the-trust.eu. PTR scheme. trust.tspa.example.com`

    …

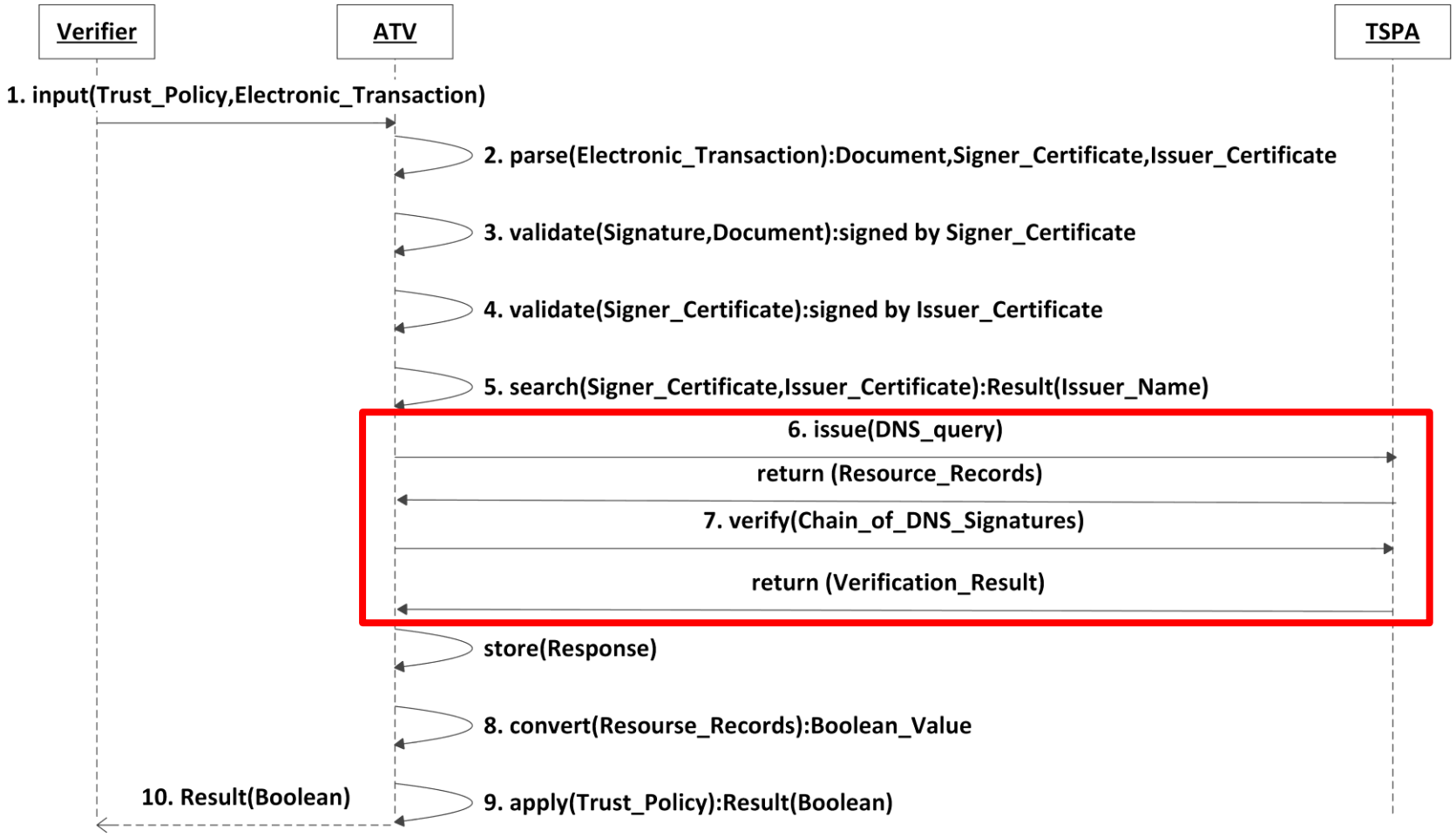
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Discovery of Trust Scheme Publication Authorities

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

Discovery of Trust Scheme Publication Authorities

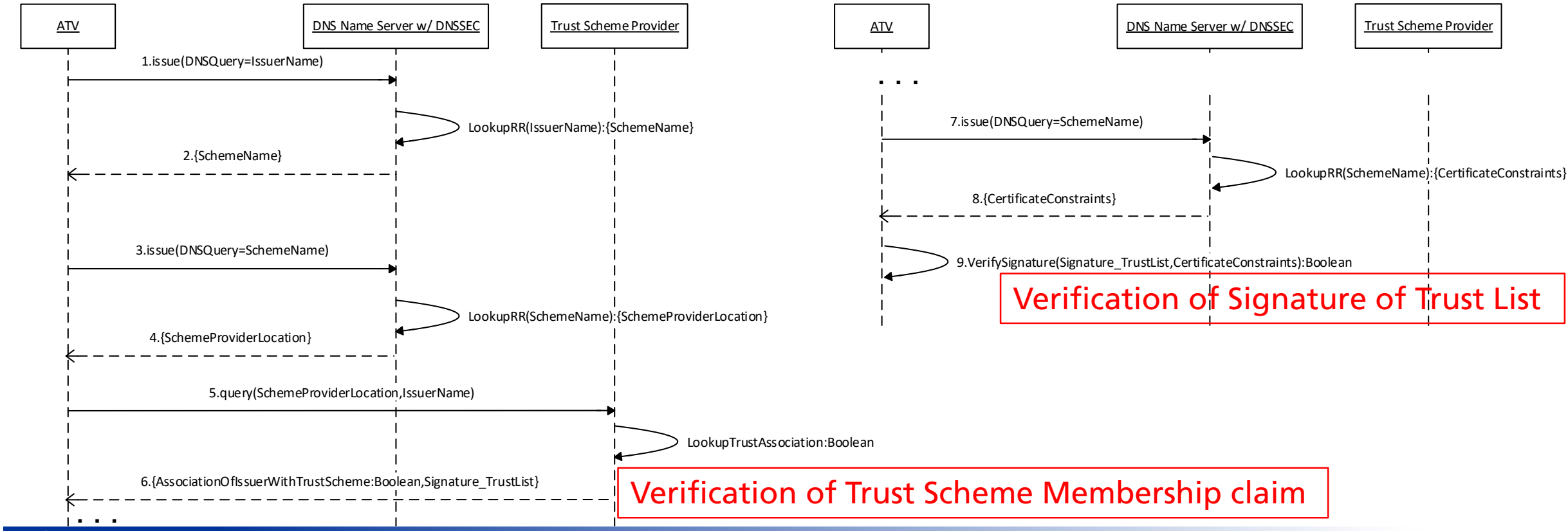
- Information flow (high level)



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

Discovery of Trust Scheme Publication Authorities

- ATV has extracted the Issuer Name from the signer certificate and contacts TSPA



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

Example: Discovery of Trust Scheme Publication Authorities

- **Example: eIDAS Germany (with D-Trust as qualified trust service provider)**
  - DNS query to discover trust scheme

```
;; QUESTION SECTION:
;_scheme._trust.d-trust.net.   IN   PTR

;; ANSWER SECTION:

_scheme._trust.d-trust.net.    IN   PTR   _scheme._trust.nrca-ds.de
```

  - DNS query to discover trust list

```
;; QUESTION SECTION:
;_scheme._trust.nrca-ds.de.    IN   URI
;; ANSWER SECTION:

_scheme._trust.nrca-ds.de.     IN   URI   https://www.nrca-ds.de/st/TSL-XML.xml
```


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

Example: Discovery of Trust Scheme Publication Authorities

- Published Trust list (ETSI TS 119 612): *https://www.nrca-ds.de/st/TSL-XML.xml*

```
<?xml version="1.0" encoding="UTF-8"?><TrustServiceStatusList
...
<SchemeInformation> ...
        <SchemeOperatorName>
            <Name xml:lang="en">Federal Network Agency</Name> </SchemeOperatorName>
...
 <SchemeName>
            <Name xml:lang="en"> DE:Trusted list including information related to the qualified trust service providers ... together
               with information related to the qualified trust services provided by them, in accordance with ... Regulation (EU) No
               910/2014 ... </Name>  </SchemeName>
 <SchemeTypeCommunityRules>
            <URI xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon</URI> </SchemeTypeCommunityRules>
...
<TrustServiceProviderList> ...
        <TrustServiceProvider> ...
              <TSPName>
                   <Name xml:lang="en"> D-Trust GmbH </Name>
              <TSPInformationURI>
                   <URI xml:lang="en">http://www.d-trust.de/</URI> </TSPInformationURI>...
              <TSPServives> ...
                   <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</ServiceTypeIdentifier> ...
...
<dsig:Signature ...>
        <dsig:X509Certificate>  ... </dsig:X509Certificate>  ... </dsig:Signature>
</TrustServiceStatusList>
```


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

Example: Discovery of Trust Scheme Publication Authorities

- Example eIDAS Germany (with D-Trust as qualified trust service provider) ff
  - DNS query to discover certificate constraints

```
;; QUESTION SECTION:
;_scheme._trust.nrca-ds.de.    IN   SMIMEA
;; ANSWER SECTION:

_scheme._trust.nrca-ds.de.    IN   SMIMEA   <SMIMEA record data>
```

  - *<SMIMEA record data>* example

```
3                    ; certificate usage domain issued cert
0                    ; selector: full certificate
1                    ; matching type SHA-256
c70cd54924d4c9cf     ; certificate association data
6ed20dc93c76aabb …
```

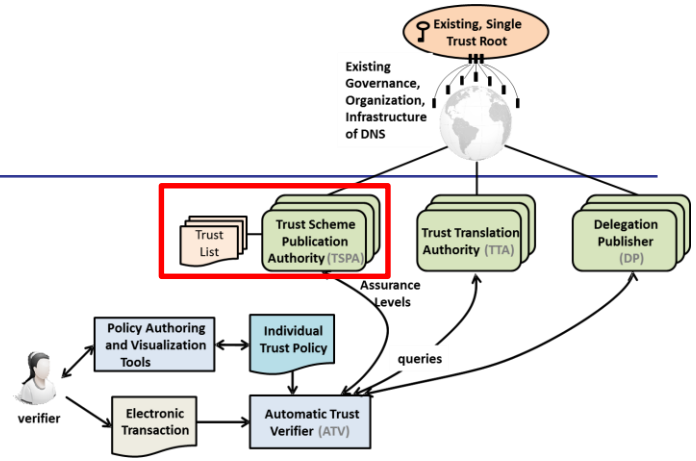
defined in RFC6698 & RFC7218

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

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

Tuple-Based Trust Scheme Publication



Publication of Trust Schemes

Type of Trust Scheme Publication	Example	Verifiable Information
Boolean	eSig Law of Turkey, FIDO	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

- Requirements of a trust scheme
  - vary depending on the Trust Scheme
  - comparison between trust schemes: may be synonymous or homonymous
  - ➢ standardized representation of requirements is needed

- Task: Develop a Unified Data Model for Tuple-Based Trust Scheme Publication
  - each requirement is explicitly represented by only one data pair: (attribute_name, attribute_value)

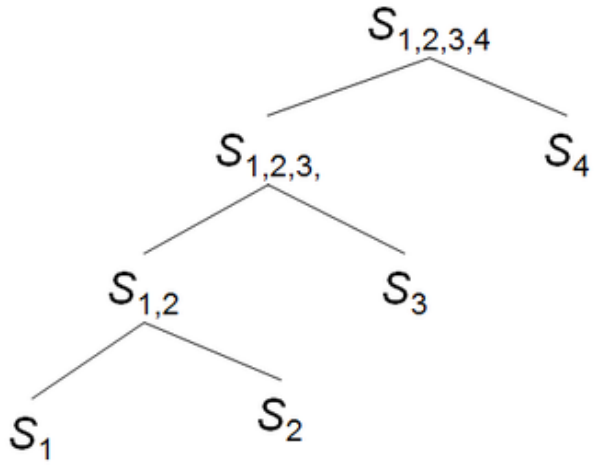
    → requirements of existing trust schemes can be represented with this unified data model

    → enables easier comparison and mapping between trust schemes

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 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

Data Model for Tuple-Based Trust Schemes: Selected Trust Schemes

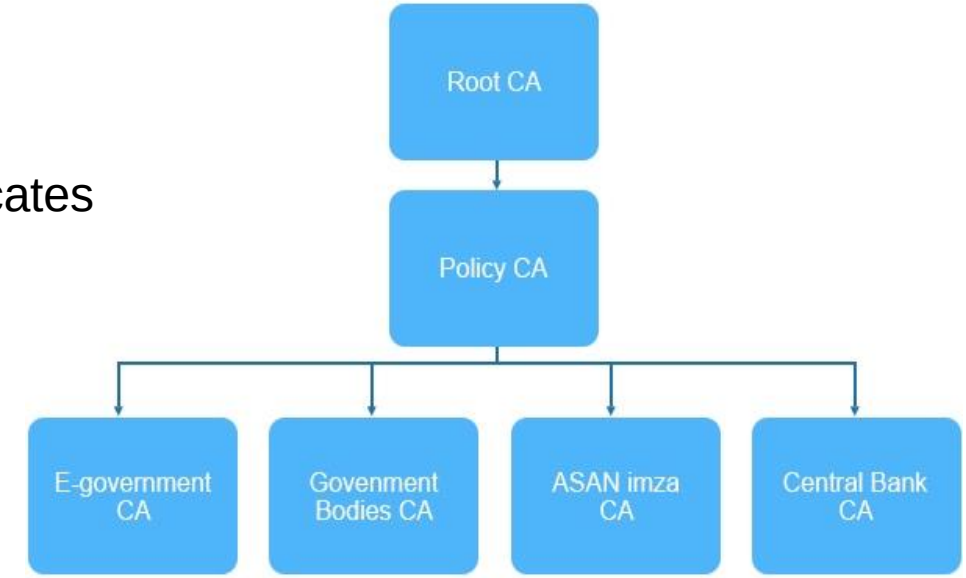
- Goal: get a most complete picture of requirements of existing Trust Schemes

- national Trust Schemes in Europe and beyond
  - Electronic Signature Law of Turkey
  - **Digital Signature Law of Azerbaijan**
  - Chinese Electronic Signature Law
  - Pan-Canadian Trust Framework
- interstate Trust Schemes
  - eIDAS
- Trust Schemes from industry consortia
  - FIDO: Fast Identity Online
  - Minors Trust Framework
  - embedded UICC Remote Provisioning
  - Open-PEPPOL
- exisiting standards
  - ISO/IEC 29115 standard

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: Selected Trust Schemes

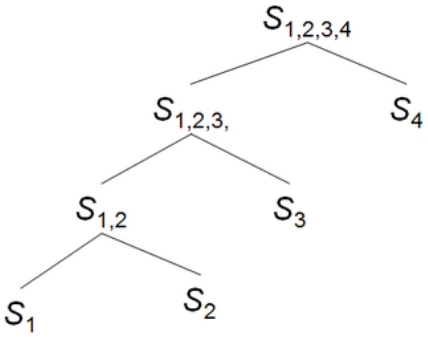
- Digital Signature Law of **Azerbaijan** (since 2004)
  - Regulation enforce usage of qualified digital signatures in public administration
  - Compliance with eIDAS is under consideration
  - PKI structure
    - Own Root CA
    - Trust hierarchy of CAs managing and issuing certificates



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: Consolidation process

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	eIDAS (STORK 2.0)	Data Model v0.6	9
Data Model v0.6	Chinese Electronic Signature Law	Data Model v 0.6	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	0

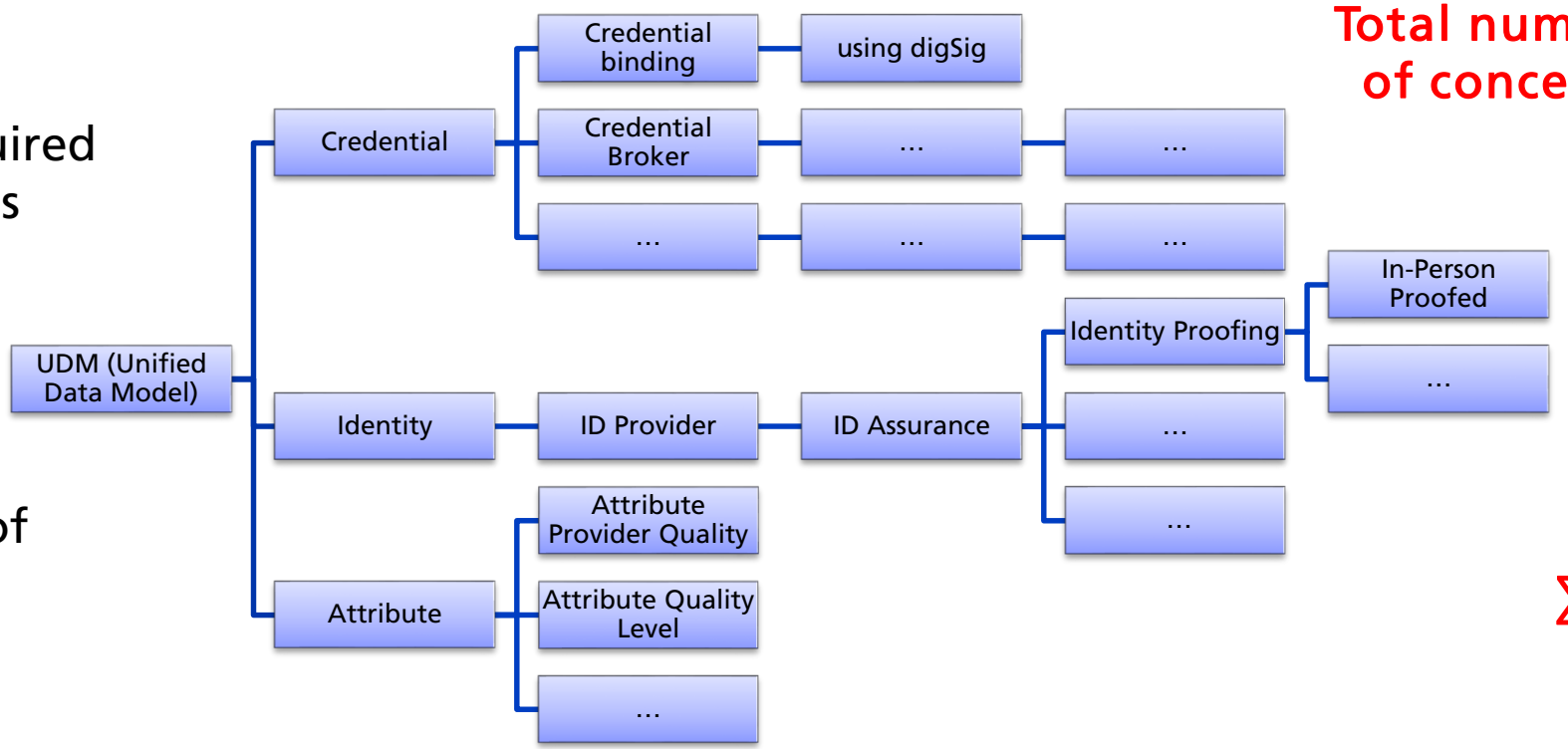


LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

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

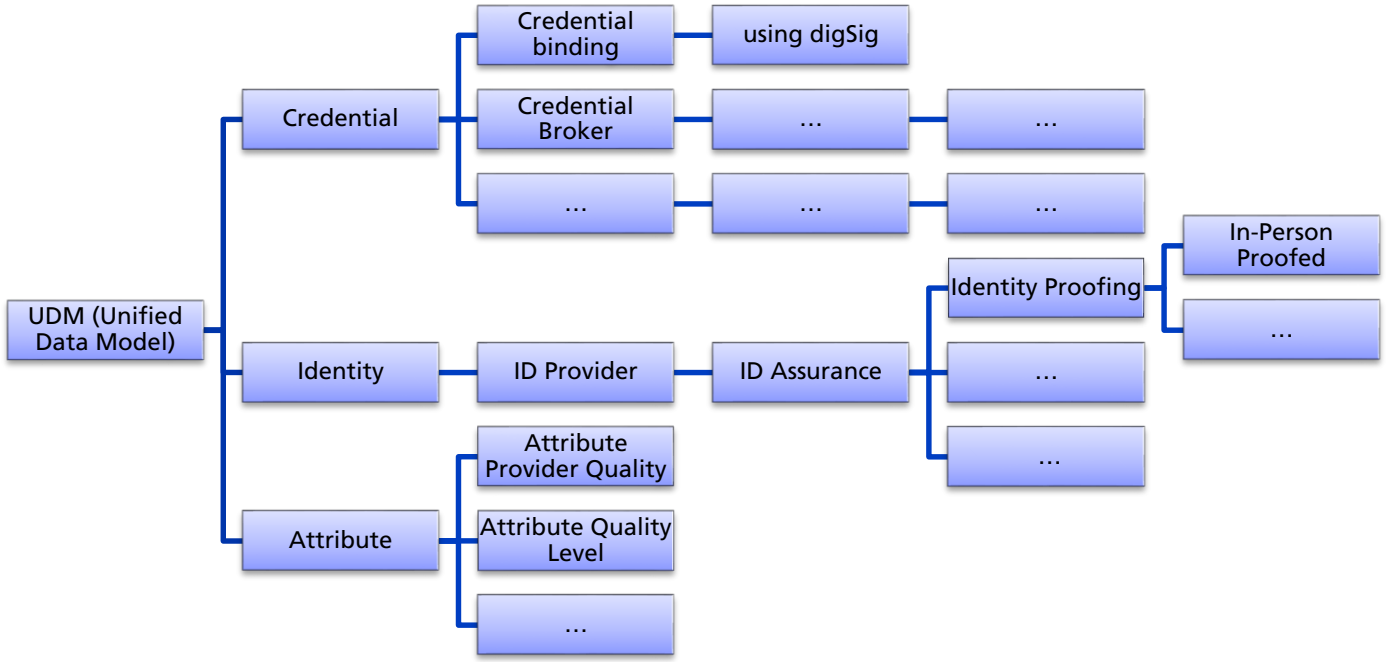
Data Model for Tuple-Based Trust Schemes: Development -2

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

  data pair (attribute_name, attribute_value)

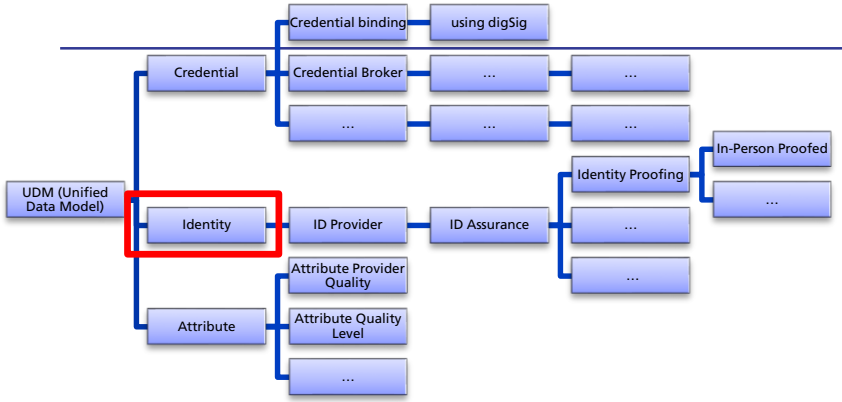
- Attribute values:
  - Boolean: e.g. In-Person Proofed
  - Integer: e.g. Time Limits
  - String: e.g. Credential Broker

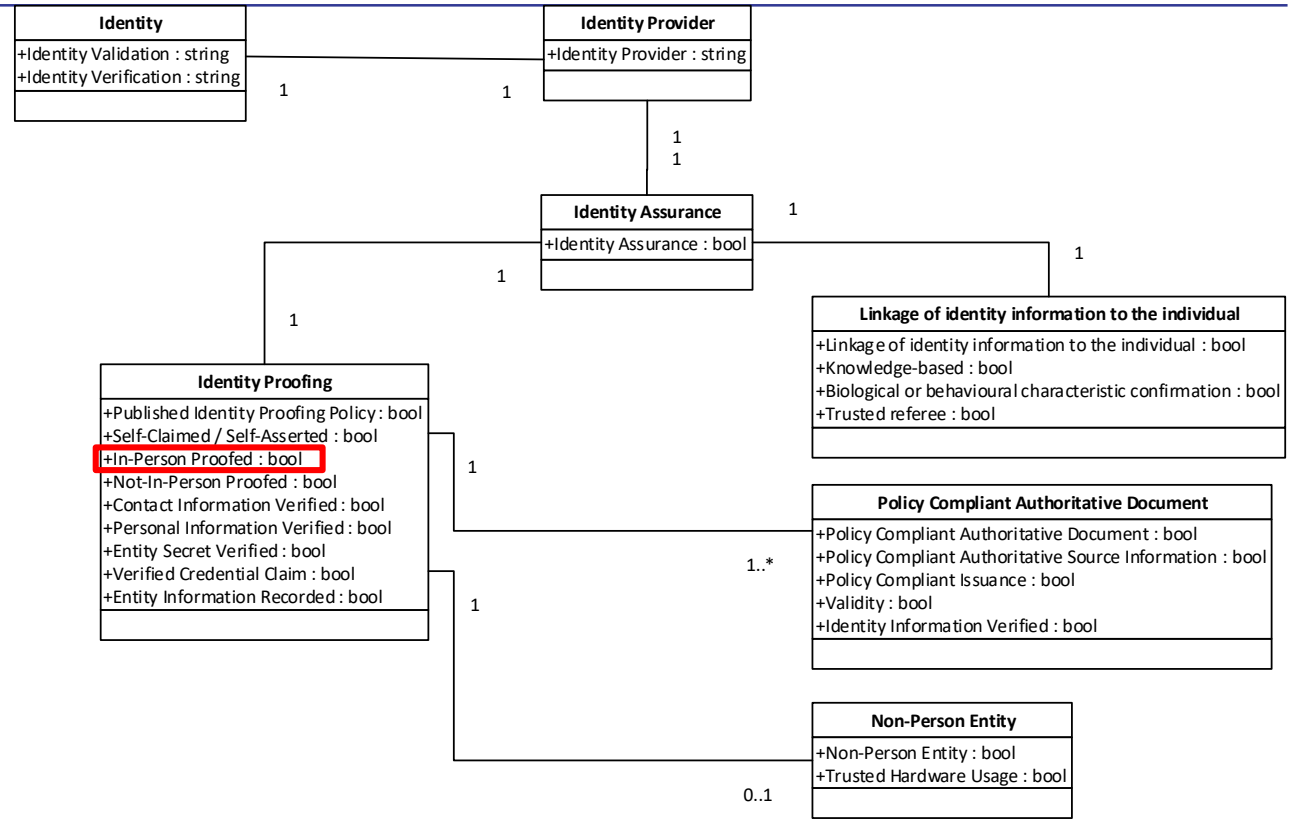
  →Most concepts (85 of 98) are boolean



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

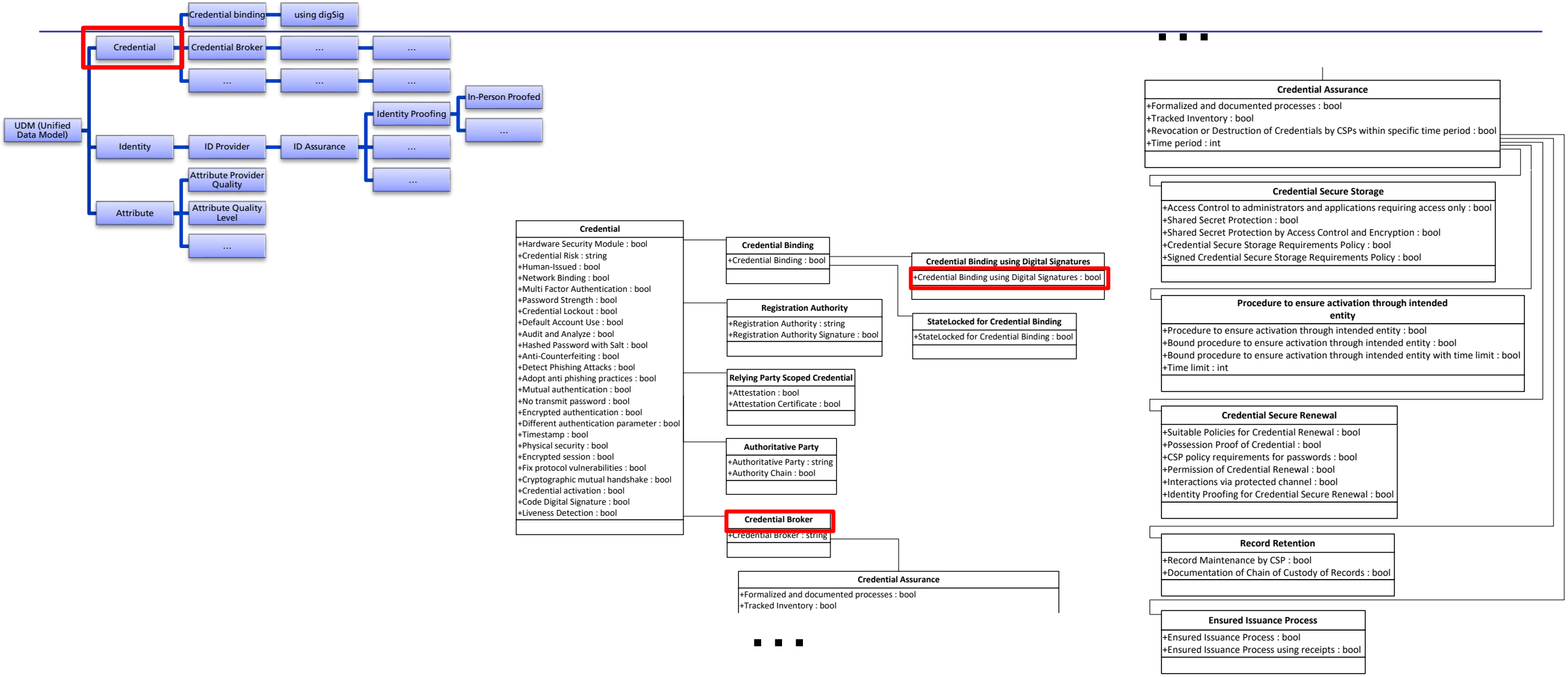
Data Model for Tuple-Based Trust Schemes: Identity





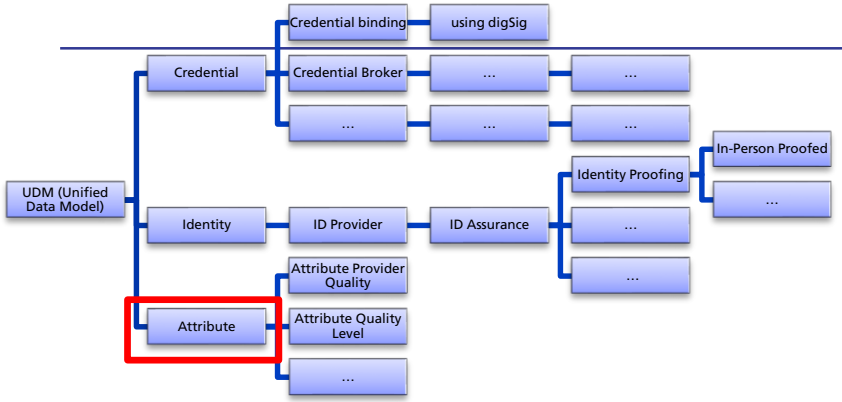
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

Data Model for Tuple-Based Trust Schemes: Credential



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: Attribute



Attribute
+Attribute Assertion Quality Level : string +Attribute Provider Quality : string +Authoritative Identity Source : bool +Link Validaion Quality : string +Maintenance : bool +Unrated Attibute Assertion : bool

1 — 1

Attribute Quality Level
+Attribute Quality Level : string +Linked to unique and verified STORK identifier : bool

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: Publication

- Publication of Trust Schemes: widely accepted standard ETSI TS 119 612 for Trust Lists
- Publication of requirements of Trust Schemes as Tuples
  - 2 options
    1. extend signed trust list (using ETSI TS 119 612) by the tuples
    2. write tuples in an extra document and add pointer from the signed trust list to this document
       - e.g. use tag < *AdditionalServiceInformation* >
  - set of corresponding tuples for the specific trust scheme is written as sequence of attributes in XML
  - schema of a single attribute

`<attributename>` e.g. `<CredentialBindingUsingDigitalSignatures>`

`attributevalue` `true`

`</attributename>` `</CredentialBindingUsingDigitalSignatures>`

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

Modelling of Tuple-Based Trust Scheme Publication

- Open-PEPPOL (Pan-European Public Procurement On-Line)
  - e-Invoicing in OpenPEPPOL environment

- PEPPOL Trust Scheme

```
<?xml version="1.1" encoding="UTF-8"?>
  <AttributesPEPPOL>
   <tuplelist>
    <AuthoritativeParty>
                <CredentialBindingUsingDigitalSignatures>
     …. 11 further tuples of Unified Data Model
    </Identity>
    <trustlevel_ID>
     "trustlevel name"
    </trustlevel_ID>
   </tuplelist>
  </AttributesPEPPOL
```

Attributes
AuthoritativeParty
CredentialBindingUsingDigitalSignatures
EnsuredIssuanceProcessUsingReceipts
ProcedureToEnsureActivationThroughIntendedEntity
CredentialSecureStorage
AccessControlToAdministratorsAndApplicationsRequiringAccessOnly
SuitablePoliciesForCredentialRenewal
RegistrationAuthority
MutualAuthentication
NoTransmitPassword
EncryptedAuthentication
CryptographicMutualHandshake
IdentityValidation

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

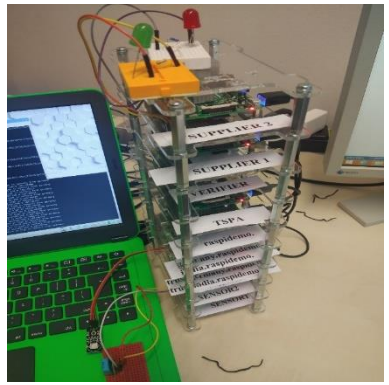
LIGHT^est has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

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

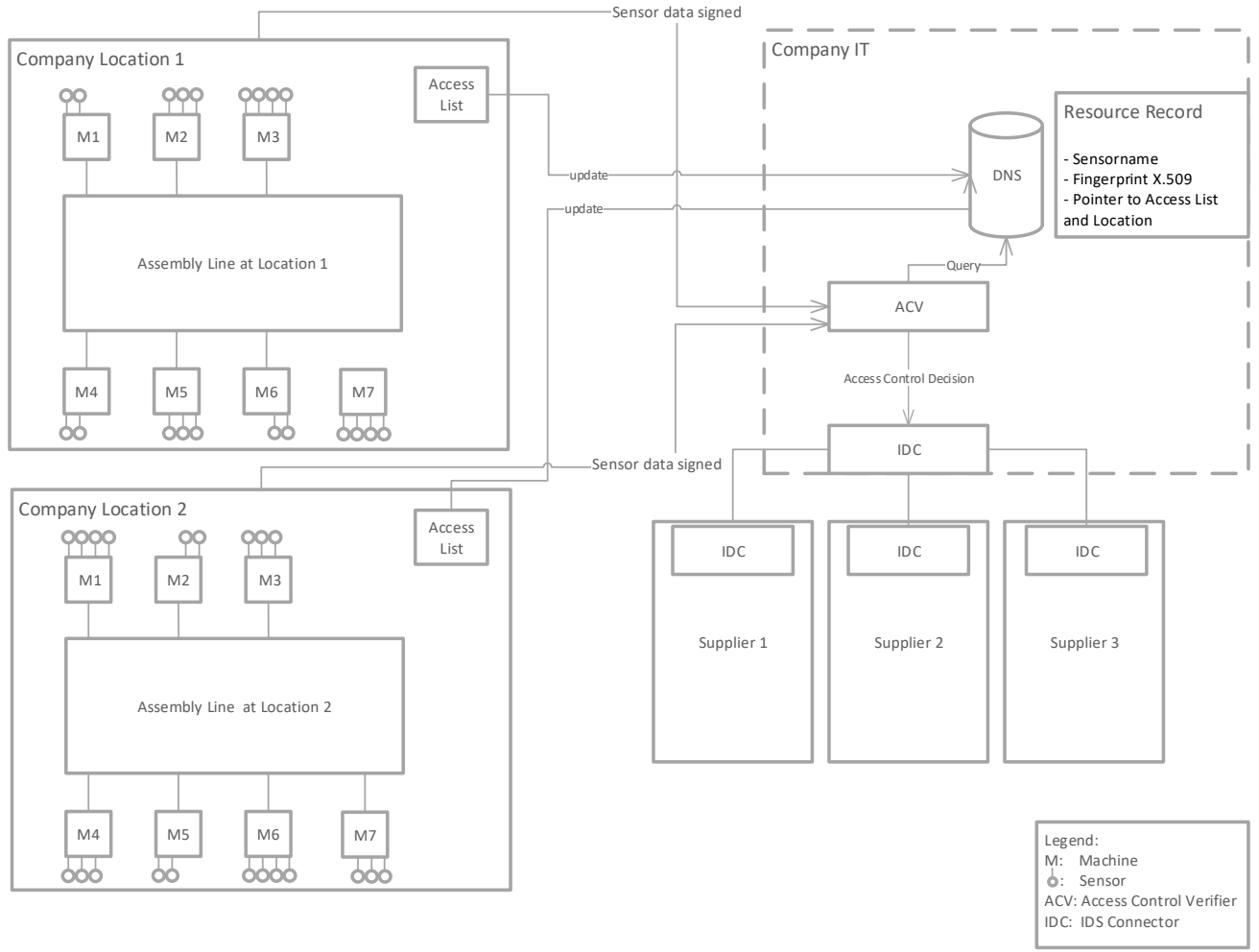


LIGHTest has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

Predictive Maintenance Use Case: sensor data verification in IoT

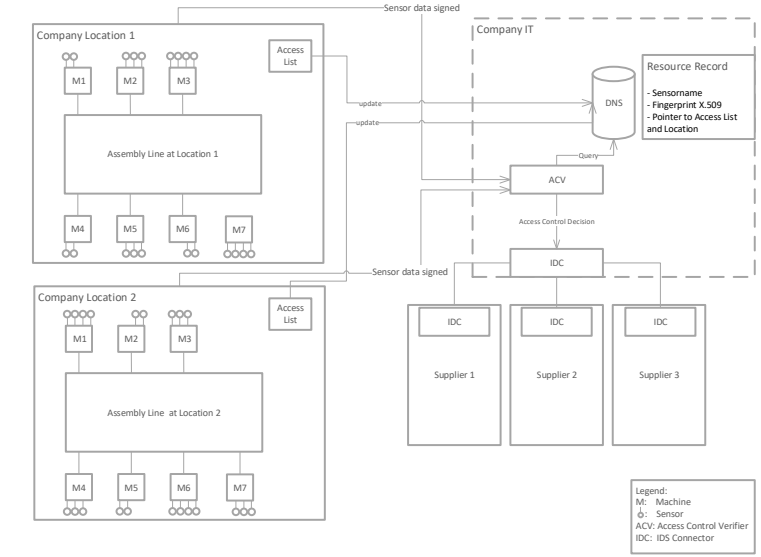
- Scenario setup

- key features of leightweight IAM:
  - decentralized access lists
  - centralized access right location



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

Predictive Maintenance Use Case: sensor data verification in IoT



Components:

- **ACV** (Access Control Verifier)
- Central **DNS server** (with DNSSEC extension)
- **Access Lists**:
  - locally (e.g. foreach location) created and maintained
  - information on installed sensors and their certificates
  - IP-addresses of the corresponding suppliers, a list of possible recipients, etc
- **Access control policy document**:
  - headquarters define specific AC policies for each supplier/ assembly line, etc
  - consider confidentiality of sensor data

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

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 assemply 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

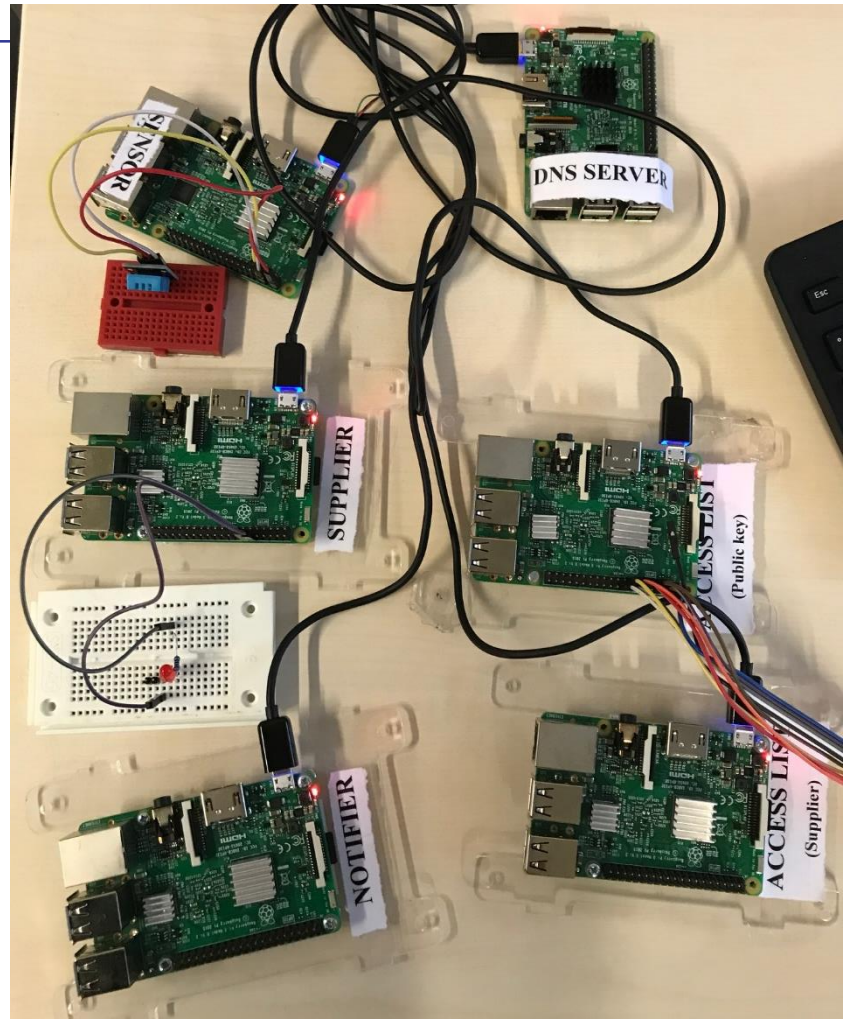
➢ Good scalability for dynamic and large systems

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

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

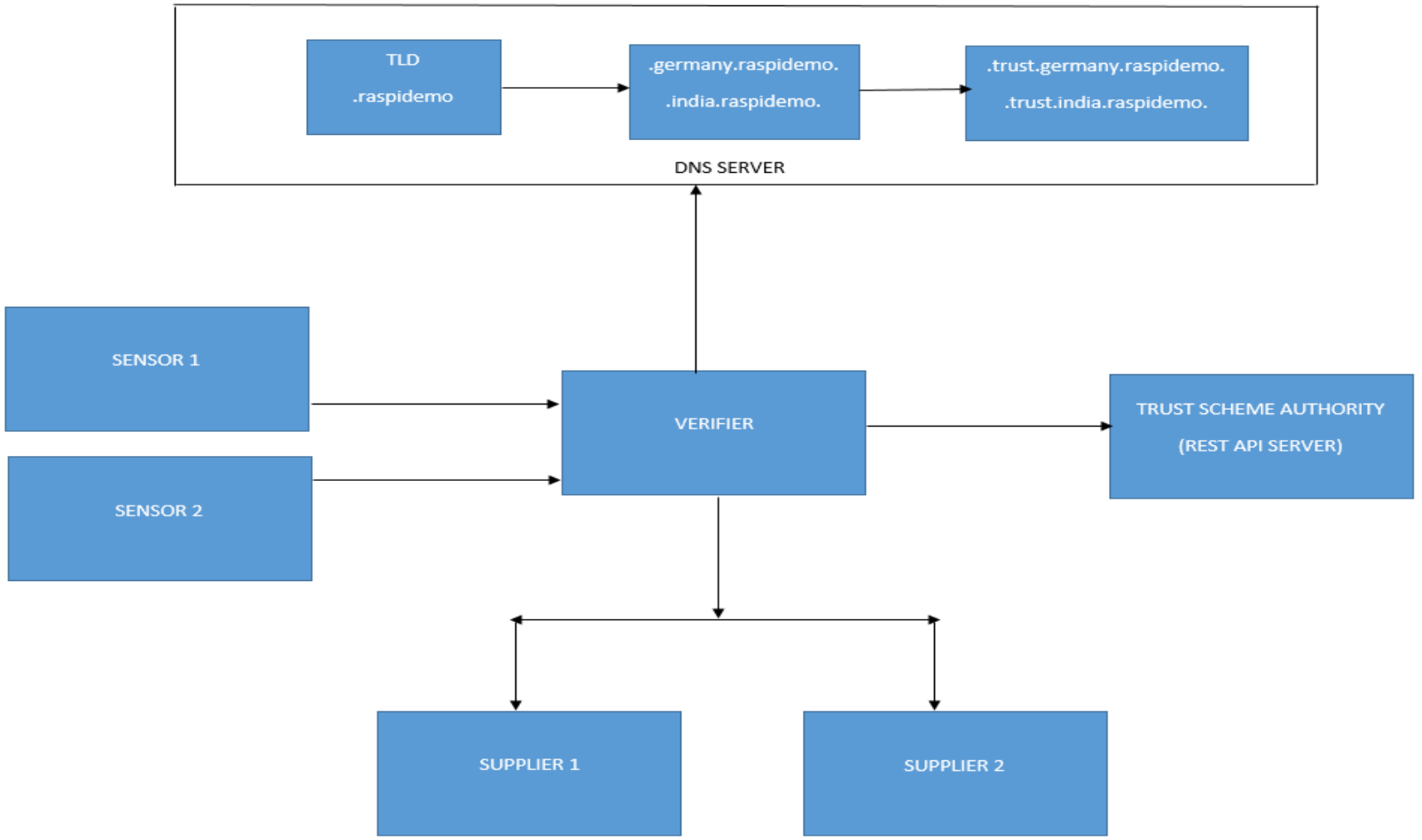
- Example: If T > 25°C then
  - verify sensor
  - provide information to authorized persons only



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

Predictive Maintenance Use Case: sensor data verification in IoT

- Raspberry pi Cluster Block Diagram



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

Distributed Authority of DNS

raspidemo.		
india.raspidemo.	NS	senname.india.raspidemo
senname.india.raspidemo.	A	10.36.28.214
germany.raspidemo.	NS	senname.germany.raspidemo
senname.germany.raspidemo.	A	10.36.28.214
india.raspidemo.	DS	
germany.raspidemo.	DS	
raspidemo.	DNSKEY	

germany.raspidemo.		
germany.raspidemo.	NS	senname.germany.raspidemo
senname.india.raspidemo.	A	10.36.28.214
sensor1.germany.raspidemo.	A	10.36.28.214
sensor1.germany.raspidemo.	PTR	sensor1.trust.germany.raspidemo.
trust.germany.raspidemo.	NS	senname.trust.germany.raspidemo.
senname.trust.germany.raspidemo.	A	10.36.28.213
trust.germany.raspidemo.	DS	
germany.raspidemo.	DNSKEY	

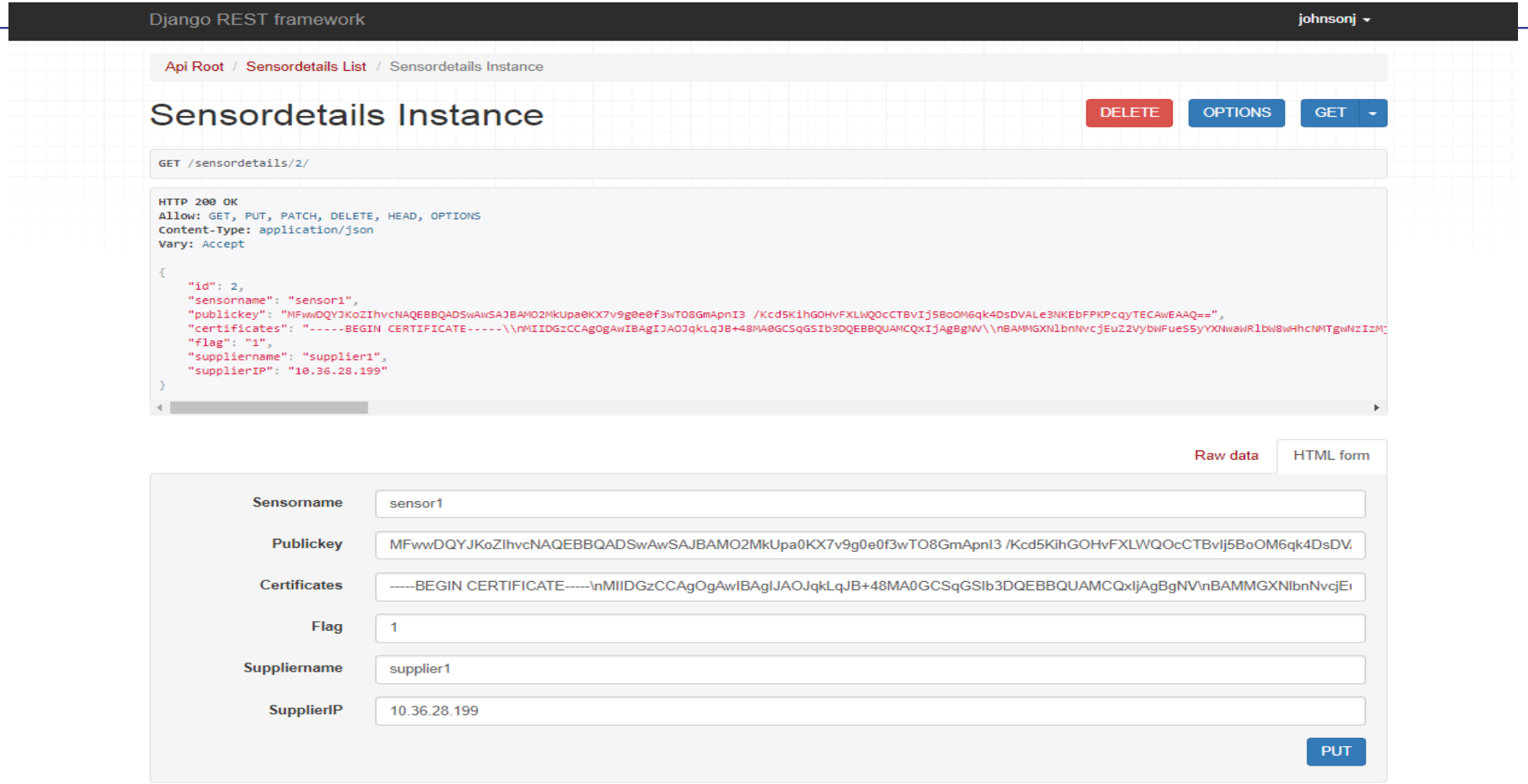
india.raspidemo.		
india.raspidemo.	NS	senname.india.raspidemo.
senname.india.raspidemo.	A	10.36.28.214
sensor1.india.raspidemo.	A	10.36.28.214
sensor1.india.raspidemo.	PTR	sensor1.trust.india.raspidemo.
trust.india.raspidemo.	NS	senname.trust.india.raspidemo.
senname.trust.india.raspidemo.	A	10.36.28.213
trust.india.raspidemo.	DS	
india.raspidemo	DNSKEY	

trust.germany.raspidemo.		
trust.germanyraspidemo.	NS	senname.trust.germany.raspidemo.
senname.trust.germany.raspidemo.	A	10.36.28.213
sensor1.trust.germany.raspidemo.	A	10.36.28.213
_443._tcp.sensor1.trust.germany.raspidemo.	TLSA	3 0 1 xxxyyyzz
_http._tcp.sensor1.trust.germany.raspidemo.	URI	http://ip/sensordetails /2
trust.germany.raspidemo.	DNSKEY	

trust.india.raspidemo.		
trust.india.raspidemo.	NS	senname.trust.india.raspidemo.
senname.trust.india.raspidemo.	A	10.36.28.212
sensor1.trust.india.raspidemo.	A	10.36.28.212
_443._tcp.sensor1.trust.india.raspidemo.	TLSA	3 0 1 xxxzzyyy
_http._tcp.sensor1.trust.india.raspidemo.	URI	http://ip/sensordetails/4
trust.india.raspidemo.	DNSKEY	

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

Predictive Maintenance Use Case: sensor data verification in IoT



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

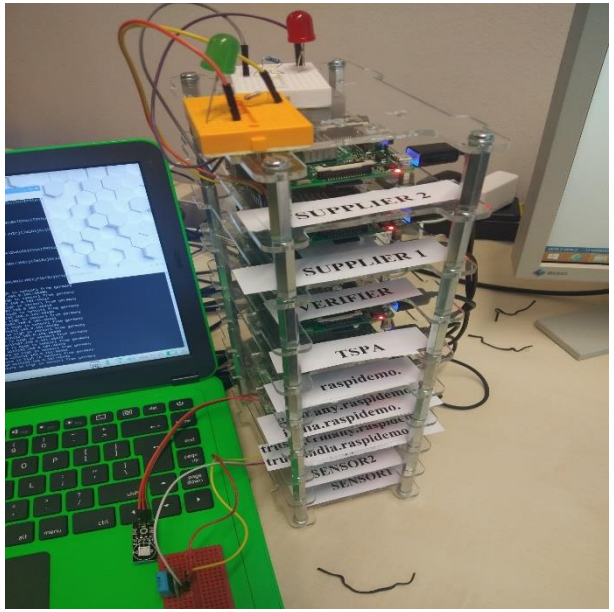
Predictive Maintenance Use Case: sensor data verification in IoT

- Example: One of the sensors indicate a possible problem

- access control policy (easy example):

it simply states that the identity of the sensor is trusted if the sensor is listed in the central DNS server and that the sensor data are send to the corresponding supplier given in the access list

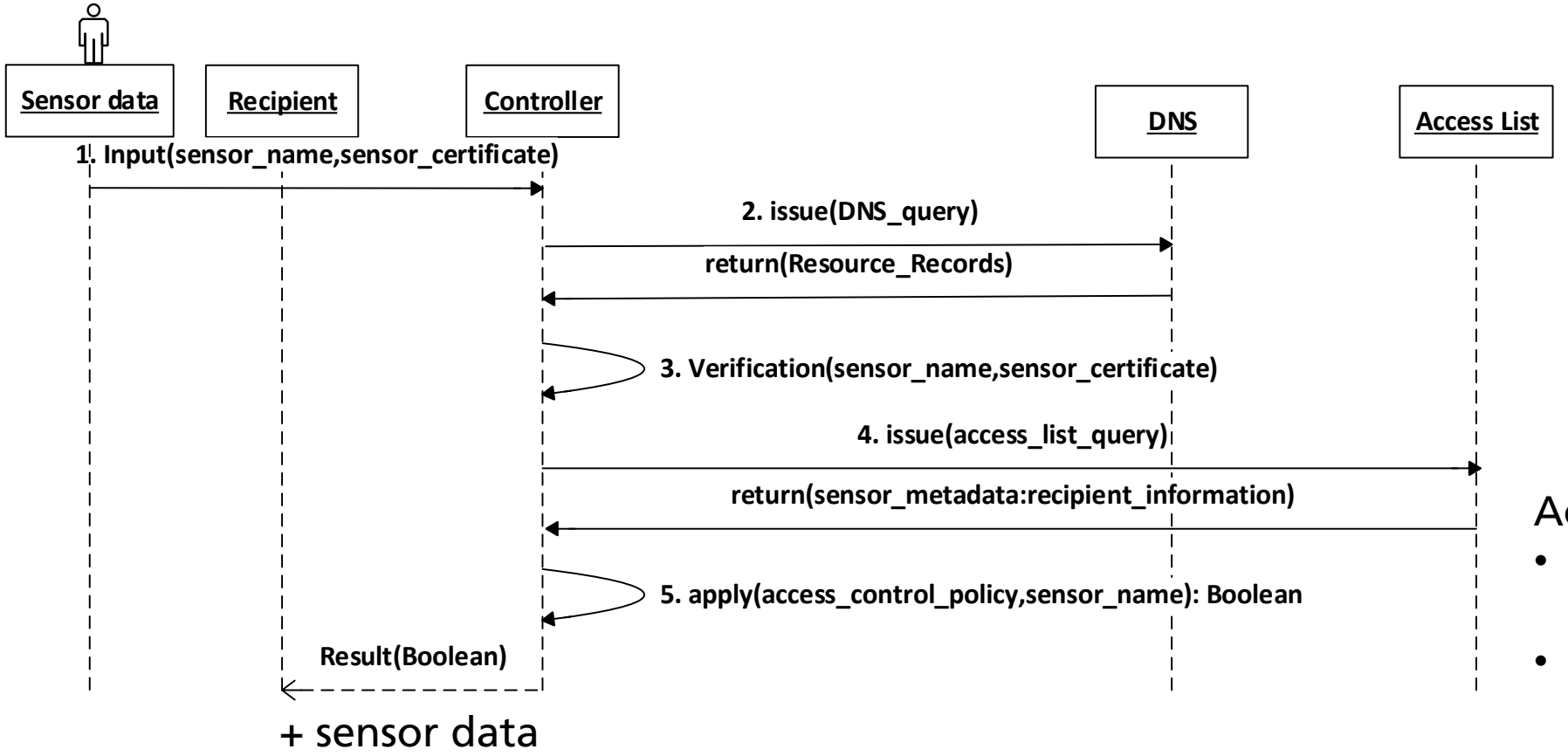
- Demonstrate it with a Raspberry pi cluster



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

Predictive Maintenance Use Case: sensor data verification in IoT

- Information flow for incoming sensor data



Access control policy:

- sensors is trusted if listed in DNS
- Sensor data are transmitted

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

Predictive Maintenance Use Case: sensor data verification in IoT

- Video

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

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

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.

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

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

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

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

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)

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.

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.

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.

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

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

1

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

2

UNHCR
The UN Refugee Agency

DAFI

Notary Bob
- reviews the documents
- verifies authenticity of documents

3

UNHCR
The UN Refugee Agency

Notary Bob
- scans the documents
- signs the documents

4

UNHCR and David
- have a digital document signed & integrated in the **UNHCR trust scheme**
- Documents can be easily accessed & digitally verified

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

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

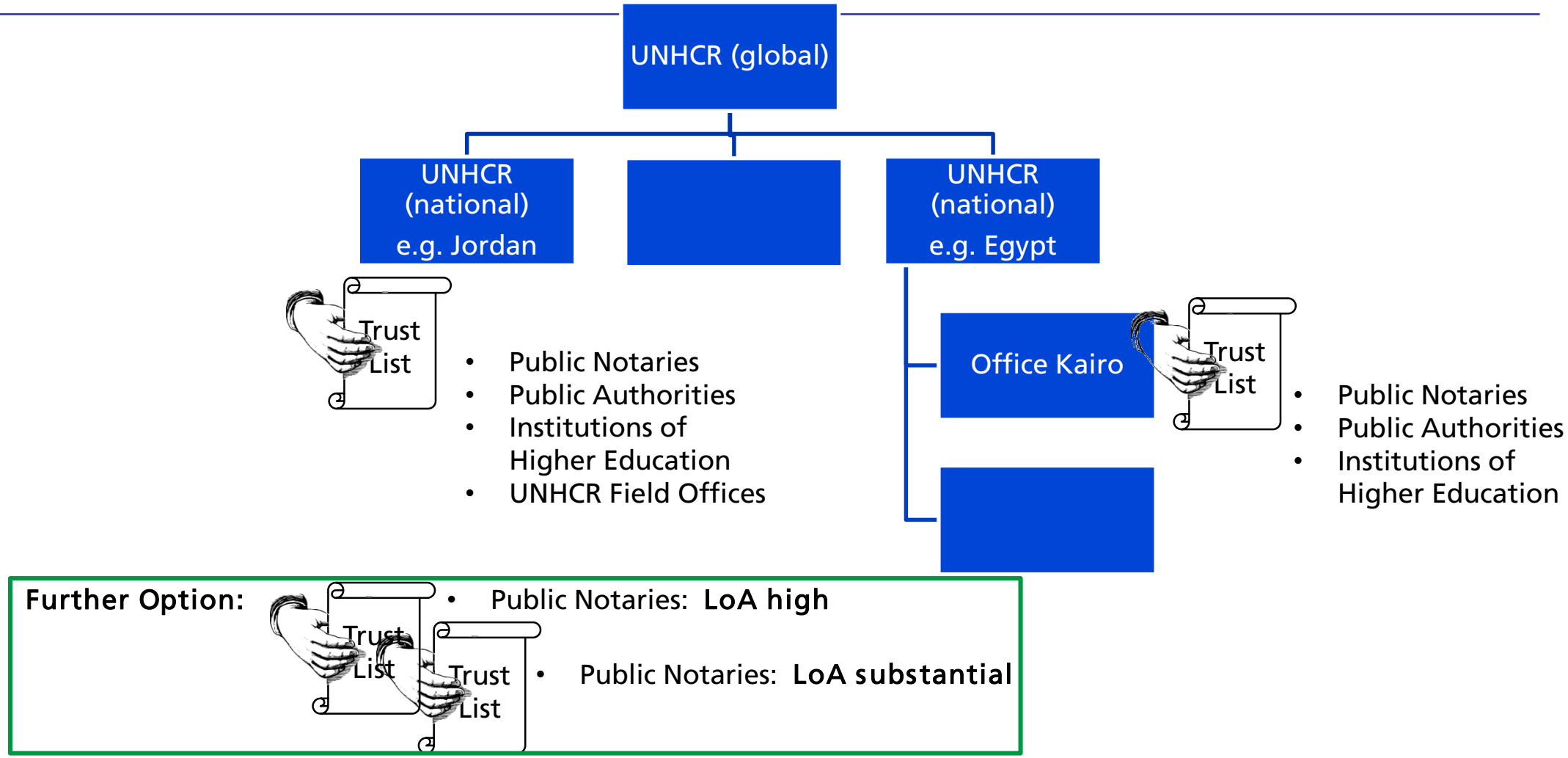
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

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

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

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



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

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

- **Alice from the University wants to verify a signed document from refugee David**
  - verfiy who has digitized and verified the documents
    - verify whether Notary Bob is a member of UNHCR trust scheme

- Alice can use LIGHTest infrastructure here
  - Alice contacts Automatic Trust Verifier (ATV)
  - ATV (internal work flow, no input required from users):

1. Extracts from certificate Trust Scheme Membership Claim: Notary Bob is member of UNHCR TS
2. Query DNS to retrieve correct Trust List of the UNHCR trust scheme
3. Check if Notary Bob is listed as a Trust Service in Trust List
4. Verify: DNS records are authenticated using DNSSEC; certificate used for signing trust list

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

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

- UNHCR Trust Scheme and Notary Bob as Trust Service Provider (fictitious example)
- DNS queries for Trust Scheme Membership (internal work flow, no input required from users)
  - Discovery of trust scheme trust service is a member:

```
;; QUESTION SECTION:
;_scheme._trust.notarybob.example.   IN   PTR

;; ANSWER SECTION:

_scheme._trust.notarybob.example.    IN   PTR
_scheme._trust.unhcr-org.example.
```

  - Discovery of Trust list:

```
;; QUESTION SECTION:
;_scheme._trust.unhcr-org.example.    IN   URI

;; ANSWER SECTION:
_ scheme._trust.unhcr-org.example.    IN   URI   https://www.unhcr-org.example/trustlist/TSL-XML.xml
```


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

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

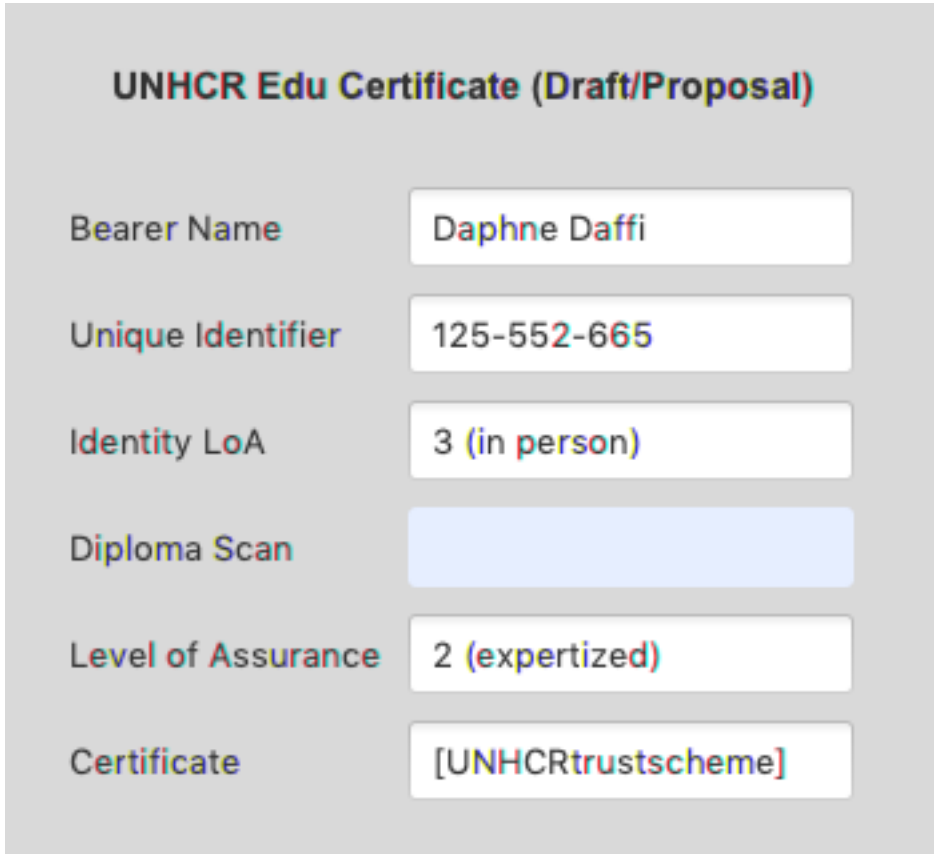
- **UNHCR Trust Scheme** and **Notary Bob** as **Trust Service Provider** (fictitious example)
- Published Trust list (ETSI TS 119 612): *https://www.unhcr-org.example/trustlist/TSL-XML.xml*

```
<?xml version="1.0" encoding="UTF-8"?><TrustServiceStatusList
...
<SchemeInformation>
        <SchemeOperatorName>
            <Name xml:lang="en">UNHCR DAFI</Name> </SchemeOperatorName>
...
 <SchemeName>
            <Name xml:lang="en"> UNHCR Trust Scheme Example: Trusted list including information related to the qualified trust
                                 service providers which are supervised UNHCR DAFI.</Name>  </SchemeName>
 <SchemeTypeCommunityRules>
            <URI xml:lang="en">https://www.unhcr-org.example/trustlist/schemerules.xml</URI> </SchemeTypeCommunityRules>
...
<TrustServiceProviderList>
        <TrustServiceProvider>
                <TSPName>
                    <Name xml:lang="en">Notary Bob</Name>
                <TSPInformationURI>
                    <URI xml:lang="en">https://www.notarybob.example/en/info/TrustServices/</URI> </TSPInformationURI>
..
                       <ServiceTypeIdentifier>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</ServiceTypeIdentifier>
...
<dsig:Signature Id="Signature-111111"> ...    </dsig:Signature>
</TrustServiceStatusList>
```

Similar to eIDAS Trust Service Status Lists

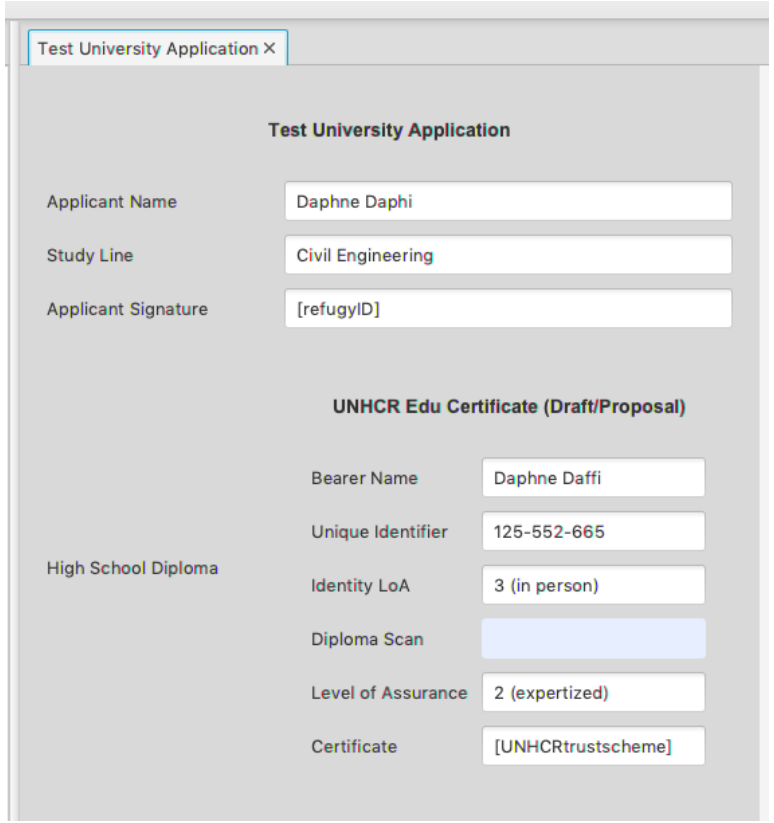
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

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



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

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



- UNHCR Trust Scheme-based Diploma can be attached to this application form

- University is free to define its own policy, e.g.
  - accept everything from UNHCR Trust Scheme with LoA>=2 and
  - everything (LoA>=1), if we know the issuing institute

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

References

- LIGHTest deliverables (public):
  - D3.2: **Conceptual Framework for Trust Schemes**
  - D3.3: **DNS-based Publication of Trust Schemes**
  - D3.4: **Discovery of Trust Scheme Publication Authorities**
  - D3.5**: Open Source Client Library and Server Tools for Trust Schemes**

- **Publications:**
  - G. Wagner et al: **DNS-based Trust Scheme Publication and Discovery**
  - S.Wagner et al: **Unified Data Model for Tuple-Based Trust Scheme Publication**
  - Jeyakumar et al: **Implementation of Distributed Light weight trust infrastructure for automatic validation of faults in an IOT sensor network**
  - **Link:** https://dl.gi.de/handle/20.500.12116/20979/browse?locale-attribute=en

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

Thank you for your Attention!

Dr. Sven Wagner
Fraunhofer IAO / University of Stuttgart IAT

Nobelstr. 12
70569 Stuttgart

sven.wagner@iao.fraunhofer.de

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

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

Appendix

LIGHT^est 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: Selected Trust Schemes

- Goal: get a most complete picture of requirements of existing Trust Schemes

- national Trust Schemes in Europe and beyond
  - Electronic Signature Law of Turkey
  - Digital Signature Law of Azerbaijan
  - Chinese Electronic Signature Law
  - Pan-Canadian Trust Framework
- international Trust Schemes
  - eIDAS
- Trust Schemes from industry consortia
  - FIDO: Fast Identity Online
  - Minors Trust Framework
  - embedded UICC Remote Provisioning
  - Open-PEPPOL
- exisiting standards
  - ISO/IEC 29115 standard

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: Selected Trust Schemes

- national Trust Schemes in Europe and beyond
  - **Electronic Signature Law of Turkey** (since 2004)
    - combination of the EU Directive on Electronic Signatures and ETSI TS 101 733
    - compromises electronic signature, mobile signature and timestamp services
    - PKI structure: Certificates of eSig will be issued by the governmental CA (KAMU-SM)
  - Digital Signature Law of **Azerbaijan** (since 2004)
    - Regulation enforce usage of qualified digital signatures in public administration
    - Compliance with eIDAS is under consideration
    - PKI structure
      - Own Root CA
      - Trust hierarchy of CAs managing and issuing certificates

LIGHT*est* 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: Selected Trust Schemes

- national Trust Schemes in Europe and beyond
  - **Chinese Electronic Signature Law**
    - Regulate electronic signatures and to ensure that e-signatures remain legally binding
    - It is a functional law (started in 2005)
    - Electronic Verification Service: electronic signature needs to be verified by a 3rd party
    - Certificates of the Electronic signatures are valid for 5 years
  - **Pan-Canadian Trust Framework**
    - Enable the Canadian digital identity ecosystem by defining rules for the processes identification, authentication, and authorization
    - Federated Authentication and Brokered Authorization Model
      - Components: individual, relying party, authoritative party, core digital identification and authentication platform service
      - 3 service components: credential services, permission services, identity services

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: Selected Trust Schemes

- international Trust Schemes
  - **eIDAS**
    - regulation on electronic identification and trust services for electronic transactions in the internal market
    - trust services
      - electronic signatures, seals, timestamps, delivery services, website authentication
      - preservation of electronic signatures, seals
    - 3 LOAs for eID: low, substantial, high
    - List of Trust Lists (LoTL)
    - STORK QAA/AQAA: Quality Authentication Assurance; attribute QAA
      - LSP enables interoperability between MSs eID authentication systems
      - LSP feed into the eID trust model in eIDAS

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: Selected Trust Schemes

- Trust Schemes from industry consortia
  - **FIDO: Fast Identity Online** (250 partners from industry)
    - Aim: interoperable specification for mobile authentication
    - Core functionality: secure end-to-end protocol for strong authentication
      - U2F protocol: two-factor authentication
      - UAF protocol: password-less authentication (e.g. biometrics)
    - Principle of FIDO is based on simple challenge-response protocols using asymmetric keys
    - LIGHTest: in signed trust list publish minimum required metadata properties of an acceptable authenticator instead of list of all acceptable authenticators (frequently changes)
  - **Minors Trust Framework**
  - **embedded UICC Remote Provisioning**
  - **Open-PEPPOL**

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: Selected Trust Schemes

- Trust Schemes from industry consortia
  - **Minors Trust Framework**
    - online identity trust model (with NSTIC (National Strategy for Trusted Identities in Cyberspace))
    - Goal: greater child safety, parental empowerment and compliance to regulations
      - allow CSPs to create an online credential for parents and children that can be used by other online service providers. All CSPs agree to defined standards of privacy and security

        → children benefit from being able to interact online in a safe and privacy secure manner
  - **embedded UICC Remote Provisioning**
    - provisioning scheme from GSMA that allows to perform remote management of an embedded an embedded UICC (universal IC card, e.g. SIM card)
    - PKI-based trust scheme allows to identify the various roles and entities within the provisioning flow and is centred around a certificate issuer who acts as a trusted 3rd party
      - Role of the CI is usually taken over by the GSMA, can be also delegated

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: Selected Trust Schemes

- Trust Schemes from industry consortia
  - **Open-PEPPOL**
    - PEPPOL: Pan-European Public Procurement On-Line (initiated in 2008)
    - set of artifacts and specifications enabling cross-border eProcurement
      - which can be implemented in existing eProcurement solutions
    - 4 corner mode for Secure Delivery of electronic document from sender to recipient
      - Access Points connect users to PEPPOL network
      - SMPs: Service Metadata Publisher (info of participants)
      - SML: Service Metadata Locator: knows all APs and list of participants per SMPs
    - Legal framework that defines network governance
    - Open PEPPOL: non-profit association (public sector and private members)
      - responsible for development and maintenance of the PEPPOL specifications, building blocks and its services and implementation across Europe.

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: Selected Trust Schemes

- exisiting standards
  - ISO/IEC 29115 standard
    - Framework for managing entity authentication assurance
    - Framework consists of 3 technical phases
      - Enrolment phase (e.g. application, identity proofing)
      - Credential management phase (e.g. credential creation, storage, revocation)
      - Entity authentication phase
    - Management and organizational aspects
    - Controls used to mitigate authentication threats
      - possible threats for each phase and required controls are provided
    - 4 Levels of Assurance (low, medium, high, very high) for 3 technical aspects
      - Little, some, high, or very high confidence in the claimed or asserted identity

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

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

Trust Scheme Components

- Trust Scheme Policy
  - includes set of requirements
    - specific policy/rules against which services included in the list are approved and assessed
  - description about how to use and interpret the content of the trusted list

- Requirements
  - LIGHTest compiled a universal overview of requirements from in total 11 national, international and industry-based trust schemes
  - Overall, there are three major groups: Credentials, Identity and Attribute
  - Tables in Section 5.4 of PoC document

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

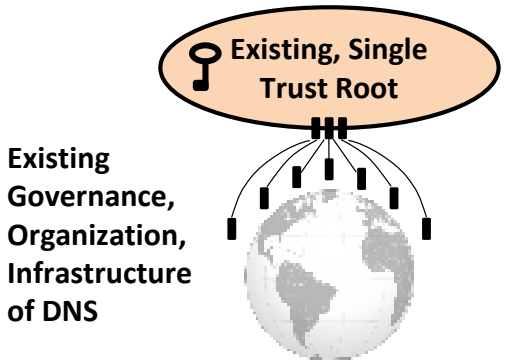
Trust Scheme Components ff

- Trust Scheme Membership
  - statement that an entity is a person/organization that is enrolled in a specific Trust Scheme
  - entity is listed in a trusted list, which corresponds to the trust scheme
  - usually there is not one but several trusted lists within a trust scheme (hierarchical form)

- Trust Anchor
  - each Trust Scheme requires a trust anchor, which is known to be correct without further evidence
  - with this Trust Anchor, any Trust Scheme Membership can be found and verified

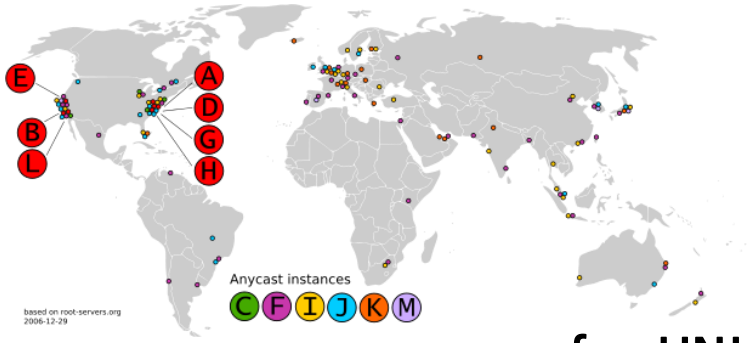
LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

The LIGHT*est* Architecture DNS: The Internet Phone Book



- Root Servers

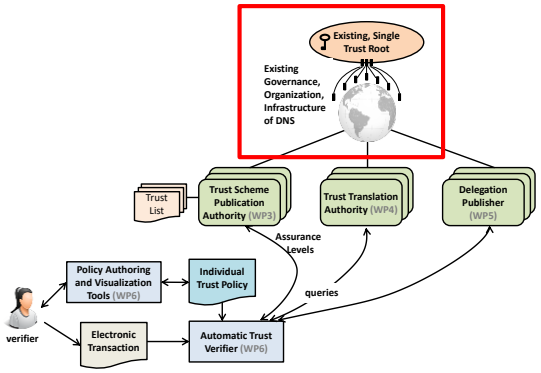
2016: 558 DNS root server instances



- Top-Level-Domain Name Servers

genericTDLs: com, org, edu, info… de, it, at, us, ca, …

for UNHCR: .org



- Most Organizations have existing Name Servers

ec.eu, gov.it, daimler.com, fraunhofer.de

unhcr.org

- Organization can define lower-level names
  - Existing or dedicated name servers
  - trust.ec.eu, eIDAS.trust.ec.eu, signature.eIDAS.trust.ec.eu

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