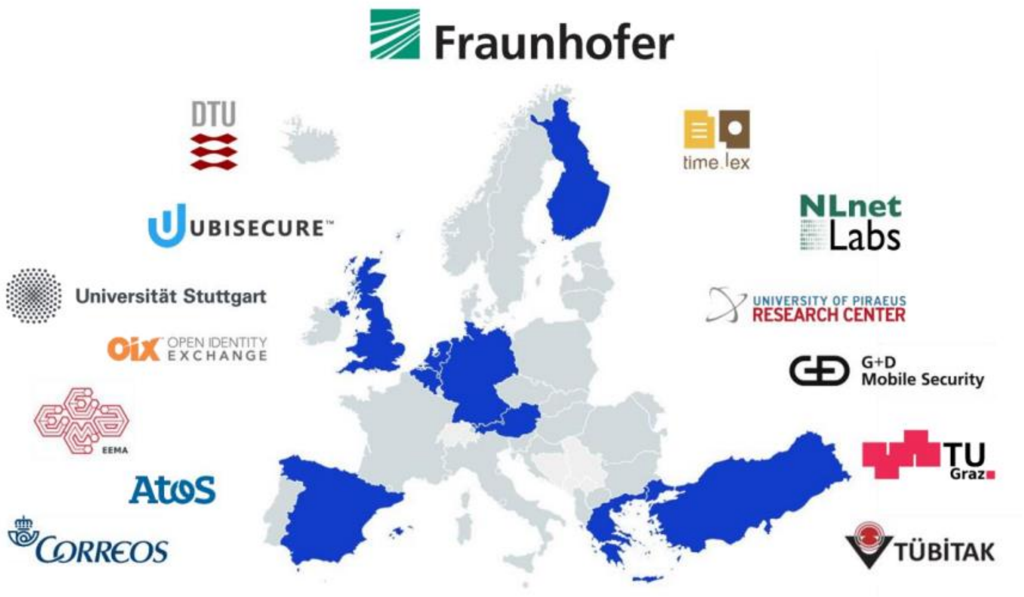
LIGHT*est*

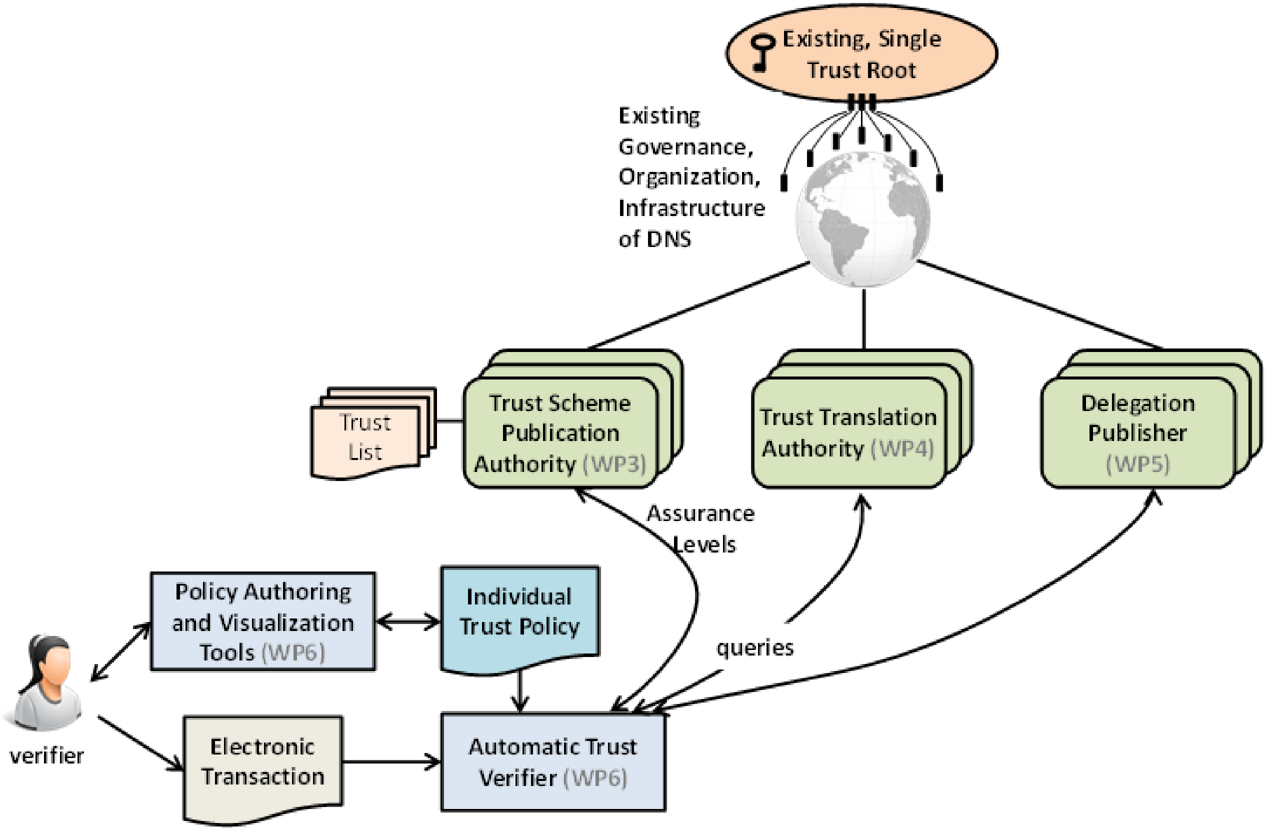
A Lightweight Infrastructure for Global Heterogeneous Trust Management



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

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

Reference Architecture of LIGHT^{est}


Existing, Single Trust Root
Existing Governance, Organization, Infrastructure of DNS
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)

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

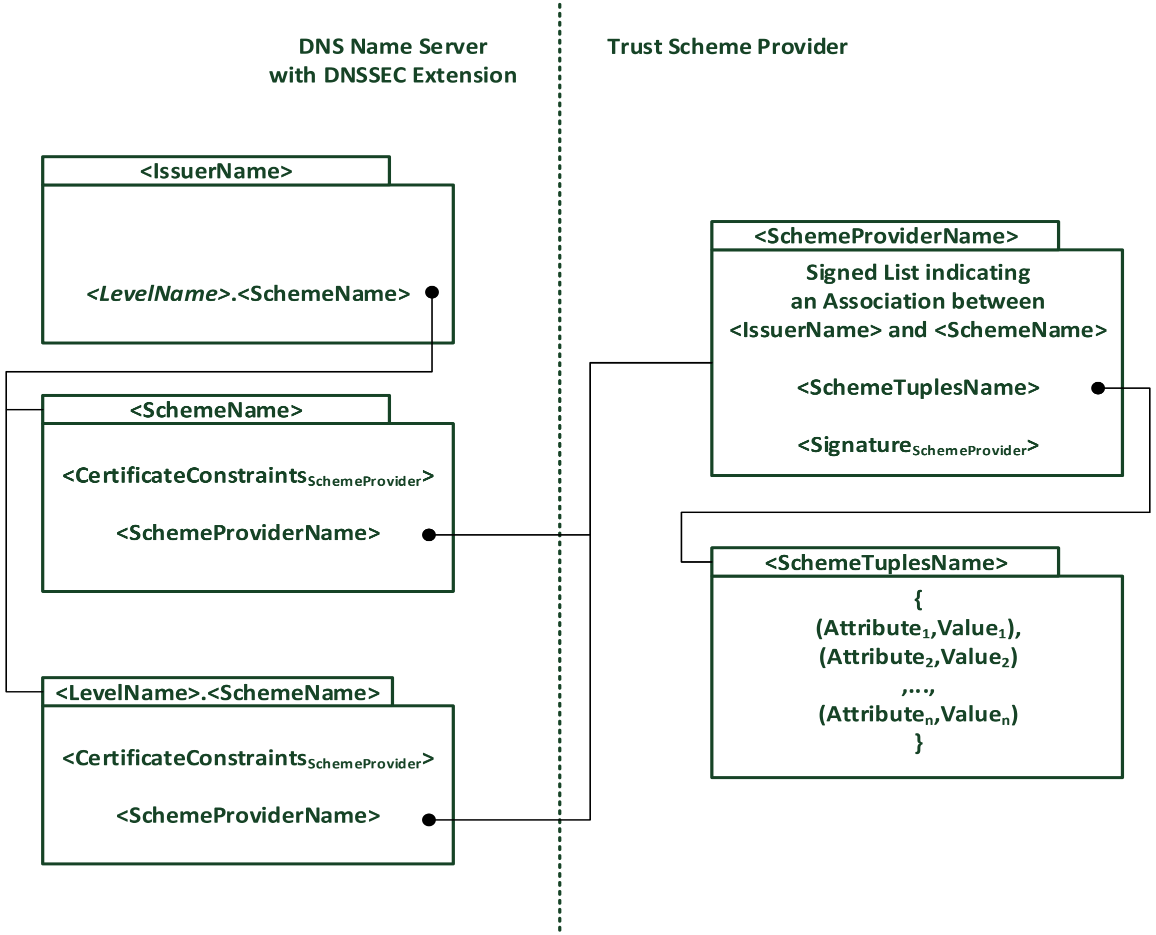
Trust Scheme Publication Authority (TSPA)

- **Open Source Client Library and Server Tools (available on IAK Git) that aim to design**
  - **A conceptual framework** to represent arbitrary trust schemes.
  - Trust schemes to be **published/queried over DNS**
  - **The discovery** of Trust Scheme Publication Authorities.
- **Legal Toolbox**, publicly available soon (M36 of the project),
  - Cross-Border **Legal Compliance and Validity** of this trust scheme publishing

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

Conceptual Framework for Trust Scheme of 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

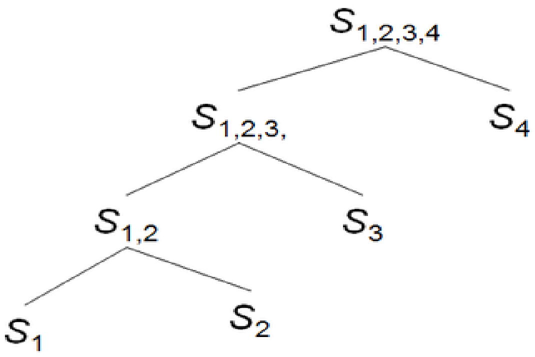
Publication of Trust Schemes

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

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 Representation

- Bottom-up modelling approach
    - Consolidation of existing trust schemes
    - Conceptualization of data model
    - Development of data model
        - Tuples (attribute_name, attribute_value)
- Modelling of Tuple-Based Trust Schemes



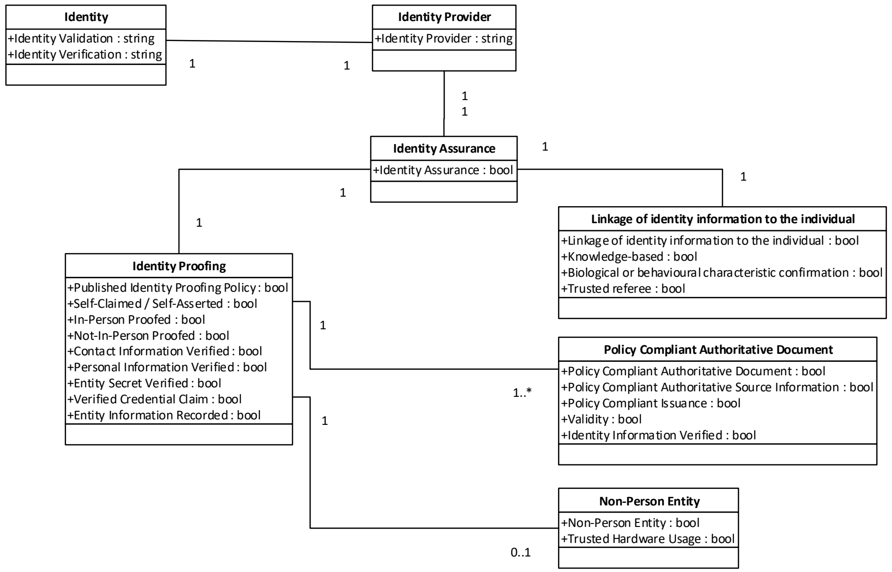
Input Scheme 1	Input Scheme 2	Consolidation Result	Saturation ΔS (min ΔS)
ISO/IEC 29115	PCTF	Data Model v0.2	n.a.
Data Model v0.2	FIDO	Data Model v0.4	3
Data Model v0.4	QAA/AQAA, eIDAS	Data Model v0.6	9
Data Model v0.6	Chinese eSig Law	Data Model v 0.6 (Data model of D3.1)	0
Data Model v0.6	Turkey eSig 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	0

Wagner S. et al., 2019

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 Representation&Publication

- Data model
  - 27 concepts for Identity
  - 62 concepts for Credential
  - 9 concepts for Attributes
- 2 new constructs:
  - Authority Chain
  - Identity Provider



Identity
+Identity Validation : string
+Identity Verification : string

Identity Provider
+Identity Provider : string

Identity Assurance
+Identity Assurance : bool

Linkage of identity information to the individual
+Linkage of identity information to the individual : bool
+Knowledge-based : bool
+Biological or behavioural characteristic confirmation : bool
+Trusted referee : bool

Identity Proofing
+Published Identity Proofing Policy : bool
+Self-Claimed / Self-Asserted : bool
+In-Person Proofed : bool
+Not-In-Person Proofed : bool
+Contact Information Verified : bool
+Personal Information Verified : bool
+Entity Secret Verified : bool
+Verified Credential Claim : bool
+Entity Information Recorded : bool

Policy Compliant Authoritative Document
+Policy Compliant Authoritative Document : bool
+Policy Compliant Authoritative Source Information : bool
+Policy Compliant Issuance : bool
+Validity : bool
+Identity Information Verified : bool

Non-Person Entity
+Non-Person Entity : bool
+Trusted Hardware Usage : bool

Wagner S. et al., 2019

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

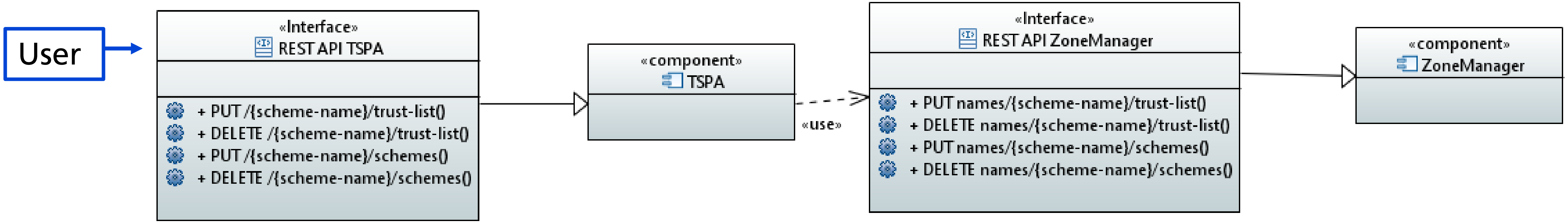
Tuple-Based Trust Scheme Representation&Publication

- Modelling of Tuple-Based Trust Schemes
  - Publication of Tuples of the generic Unified Data Model, e.g.

    <CredentialBindingUsingDigitalSignatures> true </CredentialBindingUsingDigitalSignatures>
  - Publication of Tuples-Based Trust Schemes
    - as part of the signed trust list
    - extra document with pointer from the trust list, e.g. <AdditionalServiceInformation>

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

DNS-based Trust Scheme Publication and Discovery


User
«Interface»
REST API TSPA
+ PUT /{scheme-name}/trust-list()
+ DELETE /{scheme-name}/trust-list()
+ PUT /{scheme-name}/schemes()
+ DELETE /{scheme-name}/schemes()
«component»
TSPA
«use»
«Interface»
REST API ZoneManager
+ PUT names/{scheme-name}/trust-list()
+ DELETE names/{scheme-name}/trust-list()
+ PUT names/{scheme-name}/schemes()
+ DELETE names/{scheme-name}/schemes()
«component»
ZoneManager

- Communication between components (DNS Name Server AND Trust Scheme Provider) for
  - Publishing Data using the TSPA: create, modify and delete Trust Schemes
  - Retrieving Data from the TSPA: querying process

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

- Example eIDAS Austria (with A-Trust as qualified trust service provider)
    - DNS query to discover trust scheme

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

;; ANSWER SECTION:

_scheme._trust.a-trust.net.   IN  PTR  _scheme._trust.nrca-ds.at
```

-
    - DNS query to discover trust list

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

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

Discovery of Trust Scheme Publication Authorities

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

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

_scheme._trust.nrca-ds.at.   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

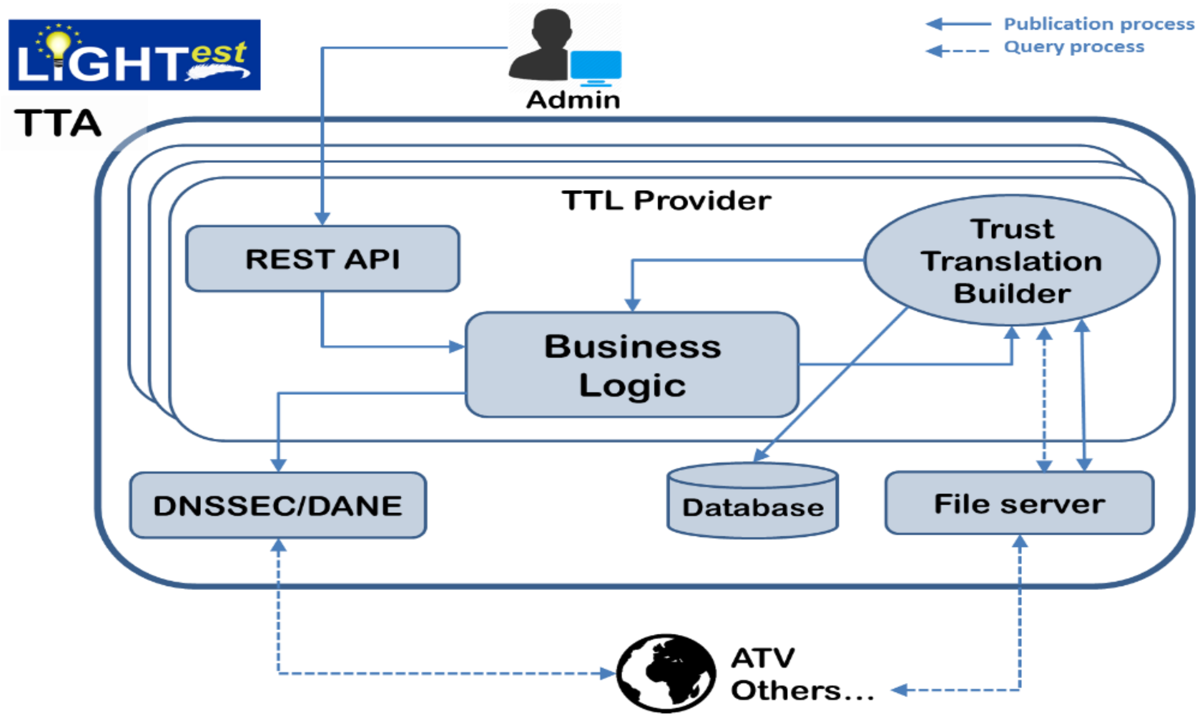
LIGHTest has received funding from the European Union’s Horizon 2020 research and innovation programme under G.A. No. 700321

Trust Translation Authority (TTA)

- **Open Source Client Library and Server Tools (available on IAK Git) that aim to design**
  - **A conceptual framework** to represent arbitrary trust translation schemes.
  - Trust translation schemes to be **published/queried over DNS**
  - **The discovery** of Trust Translation Authorities.
- **Legal Toolbox**, publicly available soon (M36 of the project),
  - Cross-Border **Legal Compliance and Validity** of these trust translations publishing

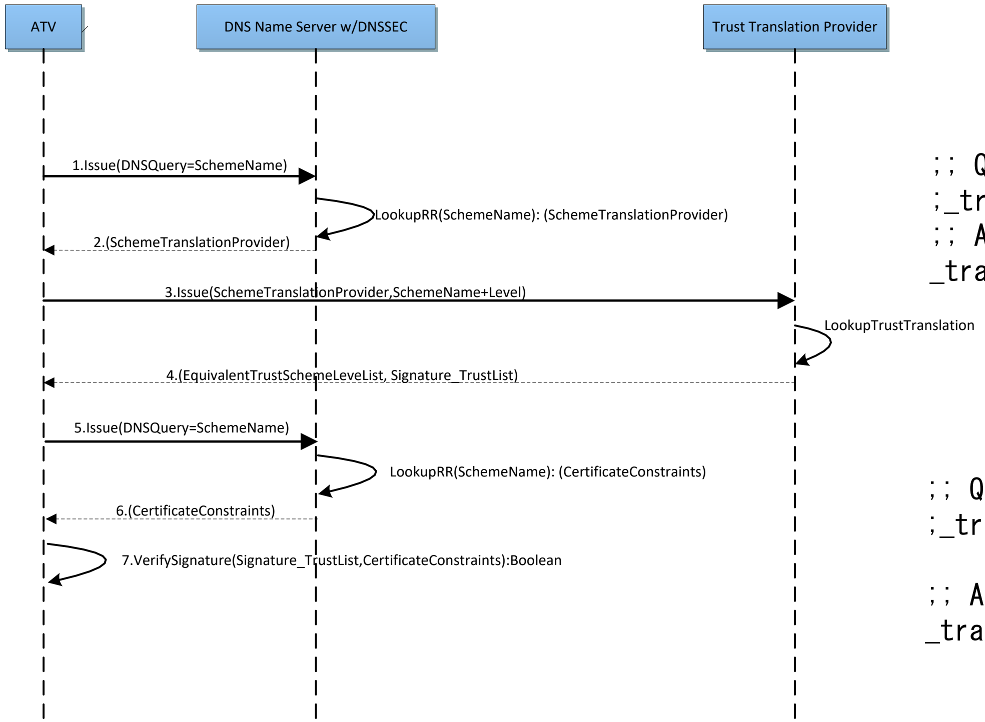
LIGHTest has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321

TTA subcomponents



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

Discovery of Trust Translation Authorities


ATV
DNS Name Server w/DNSSEC
Trust Translation Provider
1.Issue(DNSQuery=SchemeName)
LookupRR(SchemeName): (SchemeTranslationProvider)
2.(SchemeTranslationProvider)
3.Issue(SchemeTranslationProvider,SchemeName+Level)
LookupTrustTranslation
4.(EquivalentTrustSchemeLeveList, Signature_TrustList)
5.Issue(DNSQuery=SchemeName)
LookupRR(SchemeName): (CertificateConstraints)
6.(CertificateConstraints)
7.VerifySignature(Signature_TrustList,CertificateConstraints):Boolean

how users (ATV) query TTA

find Trust Translations Lists

```
;; QUESTION SECTION: Client/ATV to the TTA
;_translate._trust.loa4.eid.iso29115.org.   IN   URI
;; ANSWER SECTION: from the TTA
_translate._trust.loa4.eid.iso29115.org.    IN   URI https://lightest.eu/ttl_LoA4iso29115_1.tpl
```

check validity of information

```
;; QUESTION SECTION: Verifying authenticity
;_translate._trust.etimestamp.eidas.eu.   IN   SMIMEA

;; ANSWER SECTION:
_translate._trust.etimestamp.eidas.eu.   IN   SMIMEA  <SMIMEA record data>
```

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

Trust Translation Scheme Representation

- Translations in TPL and XML formats
- a ternary list of (trustPolicy, sourceSchema, targetSchema).

```
translate_identity(EIDAS, FIDOUAF_1_5) :-
    extract(EIDAS, schemename, eidas),
    extract(FIDOUAF_1_5, schemename, fidouaf_1_5),
    translate_qual(EIDAS, FIDOUAF_1_5).
translate_qual(EIDAS, FIDOUAF_1_5) :-
    extract(EIDAS, eIdentity_level, qualified),
    extract(FIDOUAF_1_5, userVerification, ″Fingerprint″),
    extract(FIDOUAF_1_5, userVerificationUp, ″5″),
```

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

Discovery of Trust Translation Lists

- Example: eIDAS eTimestamp
  - DNS query to discover trust translation lists
    - ; QUESTION SECTION: Client/ATV to the TTA
      ;_translate._trust.etimestamp.eidas.eu. IN **URI**

      ; ANSWER SECTION: from the TTA
      - https://lightest.eu/ttl_qualifiedTimestampEidas1.tpl
      - https://lightest.eu/ttl_qualifiedTimestampEidasN.tpl
      - https://lightest.eu/ttl_qualifiedTimestampEidas1.xml
      - https://lightest.eu/ttl_qualifiedTimestampEidasN.xml

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

Verification of the Signed Translation Lists

- Example eIDAS eTimestamp
  - DNS query to discover certificate constraints

```
;; QUESTION SECTION:
;_translate._trust.etimestamp.eidas.eu IN  SMIMEA
;; ANSWER SECTION:

;_translate._trust.etimestamp.eidas.eu 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

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

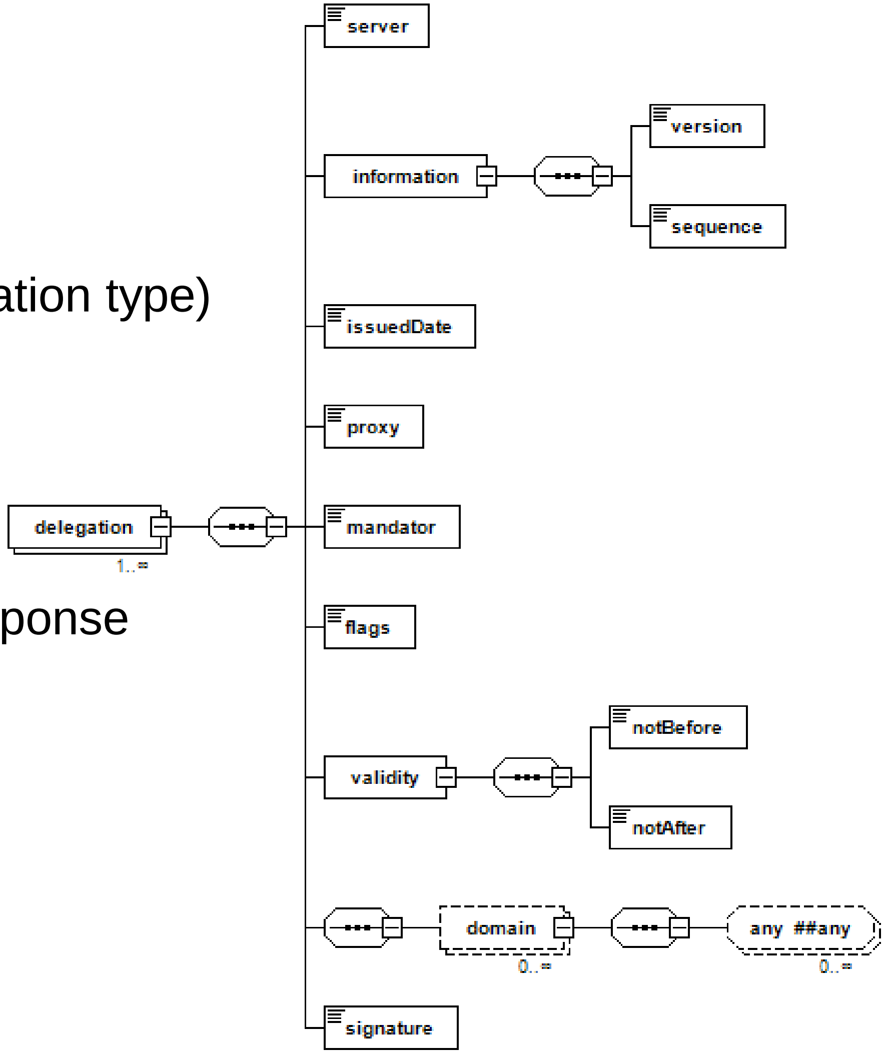
Delegation Provider

- **Open Source Client Library and Server Tools (available on IAK Git) that aim to design**
  - **A conceptual framework** to represent delegations
  - Delegations to be **published/queried**
  - **The discovery** of Trust Translation Authorities.
- **Legal Toolbox**, publicly available soon (M36 of the project),
  - Cross-Border **Legal Compliance and Validity** of this delegations publishing

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

Design of a Conceptual Framework for Delegations

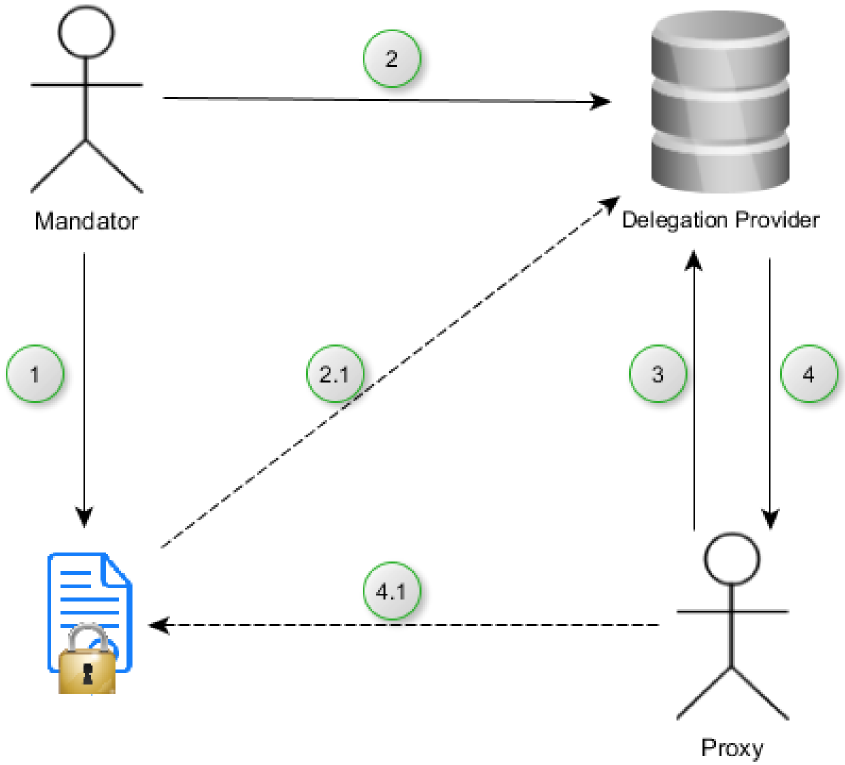
- Views on different projects and scientific publications
- Defines possible types of delegations (bilateral, substitution, delegation type)
- Data format defined
- Revocation of a delegation
    - Revocation with OCSP
    - Delegation Provider gets a delegation to sign the OCSP response



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

Design of Publication of Delegations

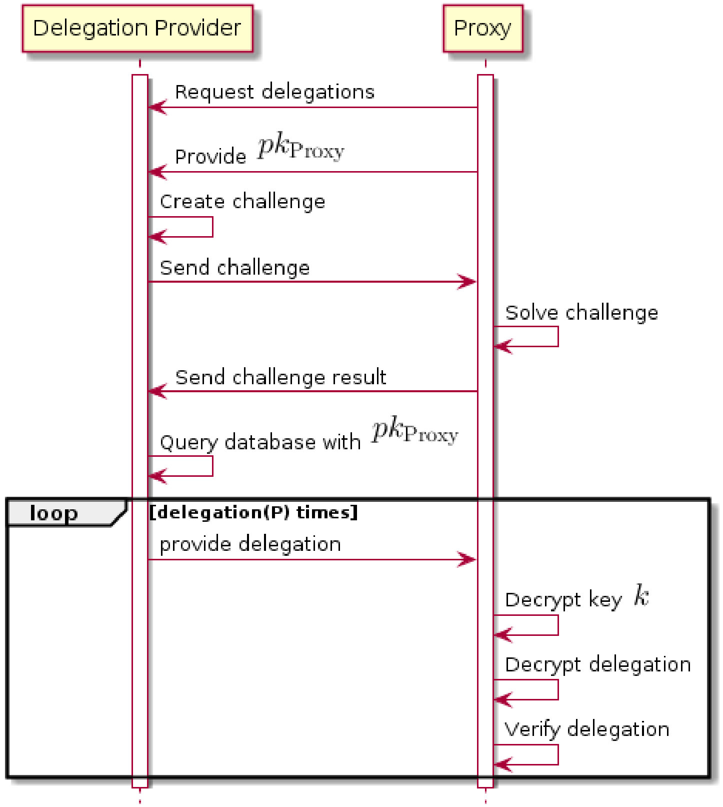
- Mandator
  - Creates delegation
  - Signs the delegation
  - Creates encryption key for the delegation
  - Encrypts generated key with Proxy’s public key
  - Uploads delegation and encryption key to delegation provider



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

Discovery of Delegations

- Proxy
  - Requests delegations
  - Provides public key
- Delegation Provider
  - Generates challenge
  - Sends challenge to proxy
- Proxy
  - Solves challenge
  - Sends result back
- Delegation Provider
  - Sends delegations to Proxy



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

How to Integrate and Test Components

- Sources can be obtained via IAIK GitLab at https://extgit.iaik.tugraz.at/LIGHTest/
- Each component uses/provides a REST API
    - TSPA to handle Trust Schemes that
        - Passes the information to the DNS server to create/update/delete entries
        - Stores the Trust Scheme information
    - TTA to handle Trust Translation Schemes that
        - Passes the information to the DNS server to create/update/delete entries
        - Stores the Trust Translation Scheme and Aggreement information
    - DP
        - To create/update/delete entries
        - Stores delegation data

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

Integration and Conformance Testing of components in LIGHT*est*

- Main objective
  - Render all LIGHT^{est} components mature and robust in order to reach TRL7.
  - Performs evaluations whether the products are in compliance with the defined specifications
- Iterative approach
  - 3 iterations are held
- Automated testing using Minder

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

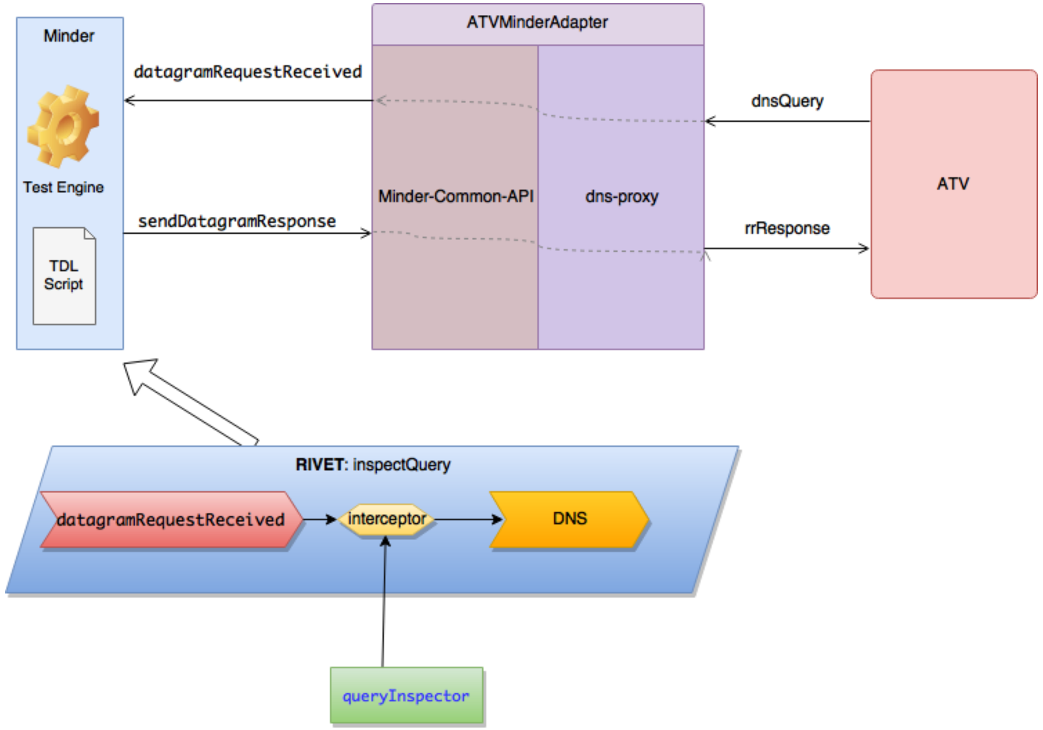
How to Integrate and Test Components

- **Minder** Conformance and Interoperability Testbed is used for the testing architecture
- Implemented in e-SENS EU Project
- Open Source Testbed confirmed by CEF and available on: https://joinup.ec.europa.eu/solution/minder-conformance-and-interoperability-testbed
- Ability to create-group-edit-execute test stories (or more formally test assertions converted to test cases) and inspect and publish reports and logs
- Minder Test Definition Language (MTDL, an extensible SCALA-based scripting language) including the use of external Java library dependencies

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

How to Integrate and Test Components

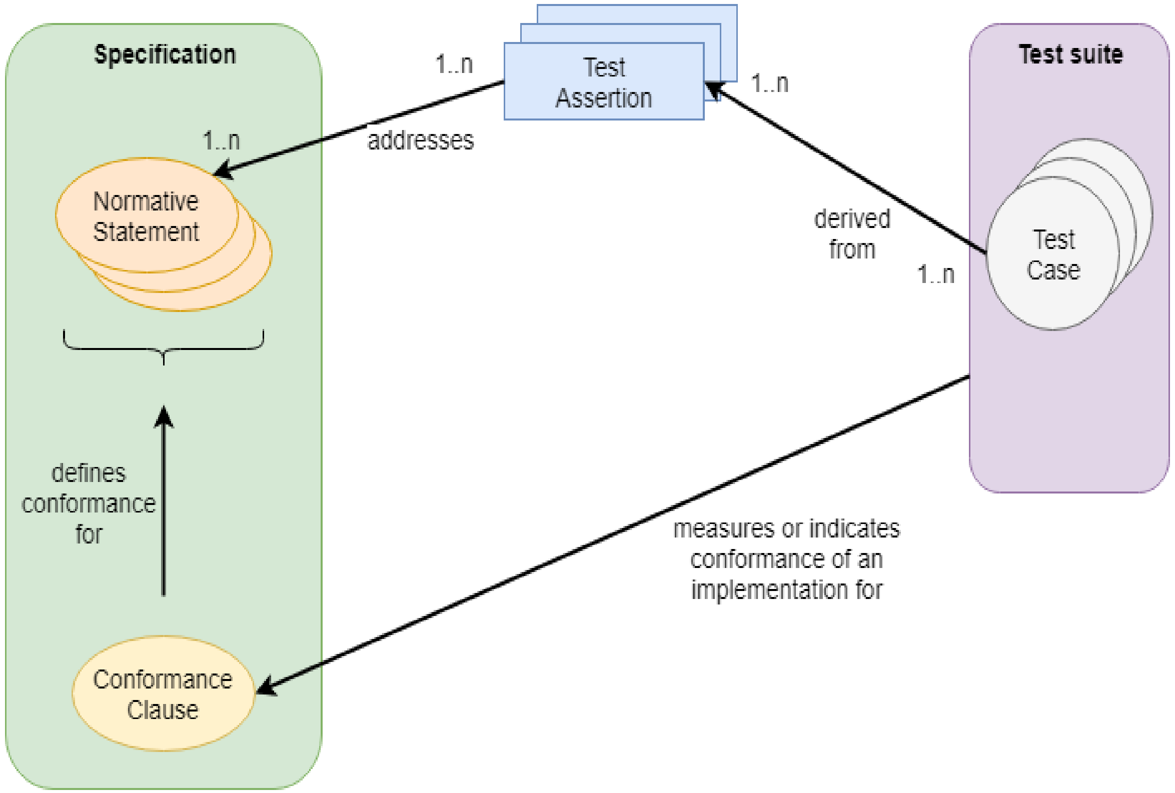
- **Minder** is compliant with GITB (Global e-Business Interoperability Test Bed methodologies)
- Focuses on methodologies and architectures that support e-business standards assessment and testing activities from early stages of business standards development from:
  - implementation and
  - Implementation → deployment of large-scale solutions.



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

Integration and Conformance Testing of components in LIGHT^{est}

- Automate
- Testing Methodology is based on OASIS Test Assertion Model

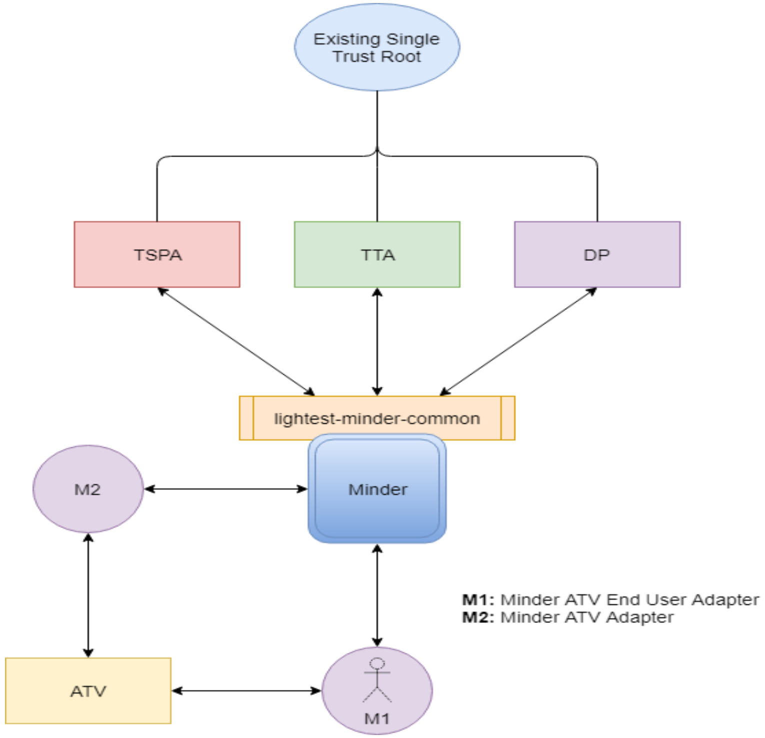


© LIGHT^{est} Consortium

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

Minder Testbed Applied Architecture

- The architecture&scenarios based on the design documentation is base on
  - Querying of Trust Scheme Membership
  - Querying of Trust Translation List
  - Discovering of Trust Delegation
  - Publishing of Trust Delegation Test Scenario
- Minder Test Manager is implemented to handle test case and suite execution



M1: Minder ATV End User Adapter
M2: Minder ATV Adapter

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

Conformance and Interoperability Testing Iterations

- TSPA
    - 18 Normative Statements :
    - 11 Test Assertions derived from normative statements
    - 20 Test Cases derived from assertions
- TTA
    - 15 Normative Statements
    - 15 Test Assertions
    - 25 Test cases
- DP
    - 13 Normative Statements
    - 15 Test Assertions
    - 18 Test cases

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

Conformance and Interoperability Testing in Summary

- Technical Infrastructure Setup – DNS with DNSSEC setup for the components
- Deployment and Integrating of LIGHT^{est} components for testing
- Test Assertions and Test Cases extraction from:
    - Use cases = Integration Test
    - Requirements = Conformance and Interoperability Tests
- Test Executions and Report Generations
- Defect correction and Re-Execution of Tests automatically with minimum effort

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

Contact Us

www.lightest-community.org
info@lightest-community.org
@LIGHTest_trust
www.linkedin.com/groups/12017516

LIGHTest COMMUNITY

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