D4.5

Open Source Client Library and Server Tools for Trust Translation

Document Identification	
Date	30.08.2018
Status	Final
Version	Version 1.0

Related WP	WP2, WP3, WP5	**Related Deliverable(s)**	D3.4, D3.2, D5.4, D4.1, D4.3, D4.2
Lead Authors	Javier Presa, Miguel Mateo Montero	**Dissemination Level**	PU
Lead Participants	ATOS	**Contributors**	TUG
Reviewers	DTU, FHG		

This document is issued within the frame and for the purpose of the LIGHT*est* project. LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No 700321.

1. Executive Summary

The aim of this document is to provide a brief description of the library developed to support the Trust Translation Authority according to the work done it work package 3, 4 and 5.

The document contains a chapter (5) with the mentioned description of the software components from the general architecture. This release constitutes a base of the TTA functionality that which evolution and improvement will continue during the integration of the Pilots. This code is released under Apache license.

2. Document Information

2.1 Contributors

Name	Partner
Javier Presa	Atos
Miguel A. Mateo	Atos
Miryam Villegas	Atos
Martin Hoffmann	NLNET

2.2 History

Version	Date	Author	Changes
0.1	13.08.2018	Miguel A. Mateo	First release
0.2	14.08.2018	Miryam Villegas	Atos internal review
1.0	27.08.2018	Miguel Mateo Javier Presa	Final version after reviewers' comments

3. Table of Contents

1. Executive Summary 2

2. Document Information 3
2.1 Contributors 3
2.2 History 3

3. Table of Contents 4
3.1 Table of Figures 4
3.2 Table of Acronyms 4

4. Scope of the Deliverable 5

5. TTA Programmatic Modules 6
5.1 DNSSEC/DANE 6
5.2 File Server 7
5.3 Data Base 7
5.4 Business Logic and REST API 7
5.5 TrustTranslationBuilder 8

6. References 10

7. Project Description 11

3.1 Table of Figures

Figure 1: Functional components of the TTA (from D4.2) 6

3.2 Table of Acronyms

DANE	DNS-based Authentication of Named Entities
DNSSEC	Domain Name System Security Extension
REST	REpresentational State Transfer
TTA	Trust Translation Authority

4. Scope of the Deliverable

This deliverable presents a brief description of the Open Source Client Library and Server Tools for the Trust Translation Authority.

The source code of the TTA can be found at:

https://gitlab.atosresearch.eu/ari/LIGHTEST-pub

The details of the technical infrastructure can be found in D8.1 [1]

5. TTA Programmatic Modules

In order to have a general view of the components of the TTA, the following figure is included, extracted from D4.2 [1]:

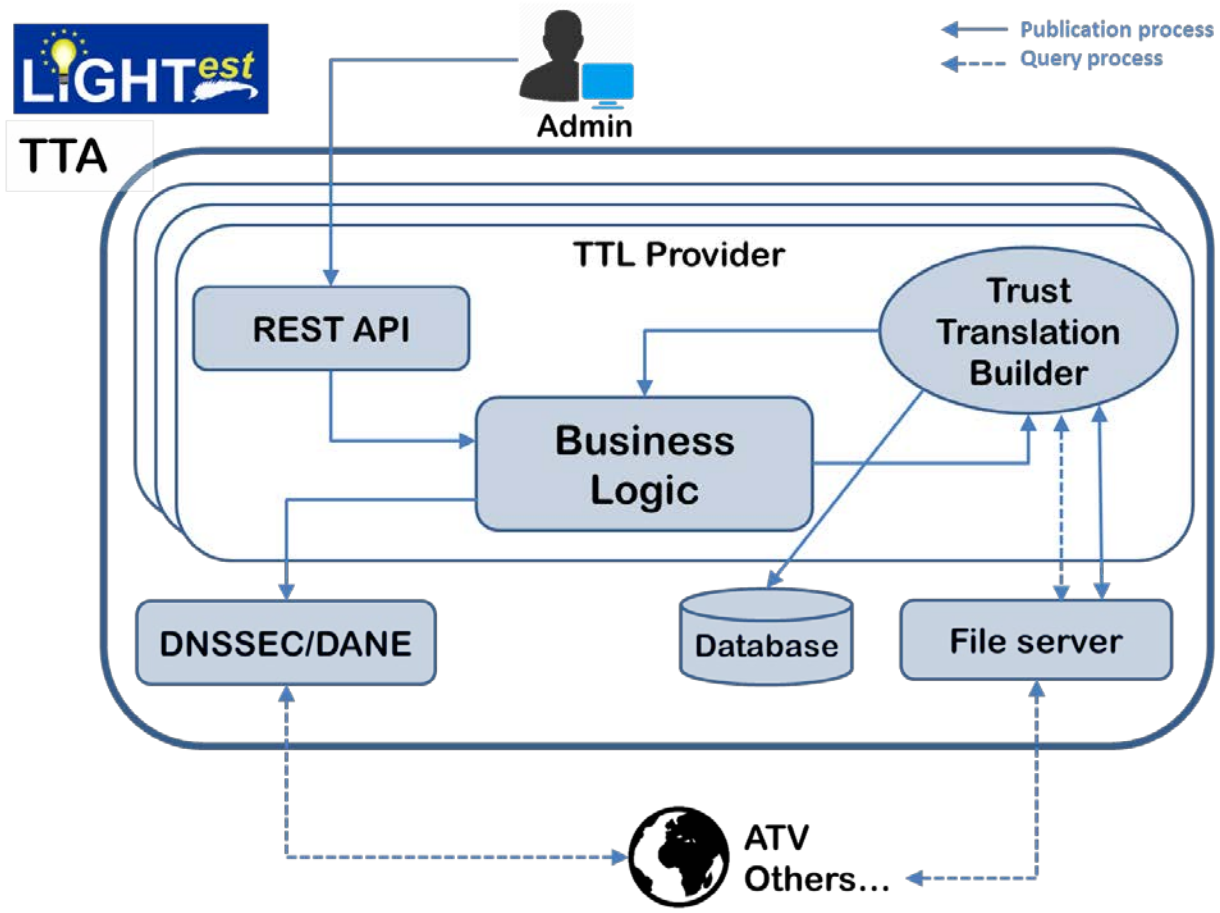

Figure 1: Functional components of the TTA (from D4.2)

As shown, a TTA consists of two different parts: at least one or more Trust Translation List Provider and the DNS Server component. Within each TTL Provider there are some components in charge of the generation and publication of the Trust Translation Lists. On the other hand, the DNS side manages the discovery of these Trust Translation Lists.

The modules that belong to these main components of TTA are:

5.1 DNSSEC/DANE

This component, which fulfils with the discovery functionality of the TTA, consists of a DNS server from NLNET and a REST API management interface, with the following methods:

- PUT names/<scheme-name>/translation

  Updates the pointer to the Trust Translation List published by the trust scheme identified by <scheme-name>. The request has to have the following content:

url	a string containing the URL of the trust service status list of this trust scheme.
certificate	an optional list of DaneCertificate objects describing the certificate used for signing the trust service status list. If this field is missing, no DANE records will be published.

- DELETE names/<scheme-name>/translation

  Deletes the pointer to the trust translation list. The request has no content.

5.2 File Server

The aim of this component is to make publicly available the files containing the translation declaration. In this case, for the sake of simplicity and robustness, it is used a TOMCAT [2] application server which can be easily configured as file server. This server will manage the storage of the files.

5.3 Data Base

Although this component is included in the architecture to support secondary functions, it has been added to provide failure tolerance functions. For the implementation, a non-relational data base has been chosen.

5.4 Business Logic and REST API

These functional blocks provide the management interface and business logic of the TTL Provider. In the first release of the TTL Provider, these two functionalities are integrated into the same component:

- Repository:
  - https://gitlab.atosresearch.eu/ari/LIGHTEST-pub/tree/master/LIGHTEST/blogic

- Packages:
  - com.ari.api:
    - Class BLogicApi: this class implements both modules: the REST API and also the Business Logic. Because the REST API is the data input procedure of the Business Logic, both are programmed in the same class.

5.5 TrustTranslationBuilder

This functional block performs the task of building Trust Translation declaration files and publish them in the file server. It consists of three software modules.

- Components:
  - **dao**: this module performs the parsing and storage procedures of trust translations declarations.
    - Repository:
      - https://gitlab.atosresearch.eu/ari/LIGHTEST-pub/tree/master/LIGHTEST/dao
    - Packages:
      - com.ari.api
        - REST API implementation
      - Server
        - Http server
  - **fileManager**: this module builds the declaration files of trust translation in XML and TPL formats.
    - Repository:
      - https://gitlab.atosresearch.eu/ari/LIGHTEST-pub/tree/master/LIGHTEST/fileManager
    - Packages:
      - com.ari.api
        - REST API implementation
      - com.ari.builders
        - TPL and XML files builders
      - Security
        - Signer file (to be defined)
  - **lightestCommons**: this library provides common functionality to other modules such as:
    - configuration.
    - data base connectors.
    - data model containers.
    - Repository:
      - https://gitlab.atosresearch.eu/ari/LIGHTEST-pub/tree/master/LIGHTEST/lightestCommons
    - Packages:
      - com.ari.conf
        - Configuration functionality
      - com.ari.connector.db

    - data base connector (MongoDB)
- com.ari.cte
    - constants
- com.ari.model
    - parser and data model for trust translation agreements provisioned through the business logic module
- com.ari.etsiModel
    - parser and data model for trust schemes. ETSI TS 102 231 [3] https://www.etsi.org/deliver/etsi_ts/102200_102299/102231/03.01.02_60/ts_102231v030102p.pdf

      this package has been developed to provide support to translation where the service provider is a factor.

6. References

[1] The LIGHTest Project, «D8.1 Technical Infrastructure for Development and Testing,» Project Deliverable, 2018.

[2] The LIGHTest Project, «D4.2- Conceptual Framework for Trust Scheme Translation (II),» Project Deliverable, 2018.

[3] «TOMCAT application Server,» [En línea]. Available: http://tomcat.apache.org/.

[4] E. S. a. I. (ESI), Provision of harmonized Trust-service status information, 2009.

7. Project Description

LIGHTest project to build a global trust infrastructure that enables electronic transactions in a wide variety of applications

An ever increasing number of transactions are conducted virtually over the Internet. How can you be sure that the person making the transaction is who they say they are? The EU-funded project LIGHTest addresses this issue by creating a global trust infrastructure. It will provide a solution that allows one to distinguish legitimate identities from frauds. This is key in being able to bring an efficiency of electronic transactions to a wide application field ranging from simple verification of electronic signatures, over eProcurement, eJustice, eHealth, and law enforcement, up to the verification of trust in sensors and devices in the Internet of Things.

Traditionally, we often knew our business partners personally, which meant that impersonation and fraud were uncommon. Whether regarding the single European market place or on a Global scale, there is an increasing amount of electronic transactions that are becoming a part of peoples everyday lives, where decisions on establishing who is on the other end of the transaction is important. Clearly, it is necessary to have assistance from authorities to certify trustworthy electronic identities. This has already been done. For example, the EC and Member States have legally binding electronic signatures. But how can we query such authorities in a secure manner? With the current lack of a worldwide standard for publishing and querying trust information, this would be a prohibitively complex leading to verifiers having to deal with a high number of formats and protocols.

The EU-funded LIGHTest project attempts to solve this problem by building a global trust infrastructure where arbitrary authorities can publish their trust information. Setting up a global infrastructure is an ambitious objective; however, given the already existing infrastructure, organization, governance and security standards of the Internet Domain Name System, it is with confidence that this is possible. The EC and Member States can use this to publish lists of qualified trust services, as business registrars and authorities can in health, law enforcement and justice. In the private sector, this can be used to establish trust in inter-banking, international trade, shipping, business reputation and credit rating. Companies, administrations, and citizens can then use LIGHTest open source software to easily query this trust information to verify trust in simple signed documents or multi-faceted complex transactions.

The three-year LIGHTest project starts on September 1st and has an estimated cost of almost 9 Million Euros. It is partially funded by the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321. The LIGHTest consortium consists of 14 partners from 9 European countries and is coordinated by Fraunhofer-Gesellschaft. To reach out beyond Europe, LIGHTest attempts to build up a global community based on international standards and open source software.

The partners are ATOS (ES), Time Lex (BE), Technische Universität Graz (AT), EEMA (BE), G&D (DE), Danmarks tekniske Universitet (DK), TUBITAK (TR), Universität Stuttgart (DE), Open Identity Exchange (GB), NLNet Labs (NL), CORREOS (ES), IBM Danmark (DK) and Ubisecure (FI). The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.

The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.