D9.1

eCorreos: Requirements, Scenarios and Demo Data

Document Identification	
Date	30.05.2018
Status	Final
Version	Version 1.0

Related WP	WP9	**Related Deliverable(s)**	D2.8, D2.13, D3.5, D4.5., D5.5, D7.3, D8.1, D8.5, D8.10, D8.11, D9.2, D9.4, D9.6, D9.8, D10.1
Lead Authors	Javier Salazar (CORREOS), Victor Martin (CORREOS), Carlos Balot (CORREOS)	**Dissemination Level**	**PU**
Lead Participants	CORREOS	**Contributors**	ATOS, TUBITAK, GS, FHG, G&D, OIX, IBM, TIL, TUG
Reviewers	ATOS, USTUTT		

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

In order to demonstrate the technical feasibility of using LIGHTest technology in a real-world scenario, Correos has envisioned a pilot within its suite of digital cloud services (eCorreos). Testing some LIGHTest components on eCorreos eNotification (*My Notifications*), eDelivery (*My Mailbox*) and/or eCorreos eID (*Correos ID*) services will check some of the major features of LIGHTest in an operational environment. The objectives for WP9 are:

1. Demonstrate LIGHTest in an operational environment.
2. Demonstrate the ease of trust-list-enabling diverse existing systems.
3. Effectively use scheme translation – to be determined how that will fit this pilot.
4. Demonstrate the ease of authoring individual trust policies.
5. Demonstrate automatic trust verification of electronic transactions.
6. Demonstrate the use of delegations as part of automatic trust verification (most likely this will be only demonstrated within the IBM eProcurement pilot).
7. Demonstrate how LIGHTest enables easy validation of signatures without the use of validation authorities.

Out of this set of objectives, T9.1 related to Correos pilot will cover few or several of them. This is further explained on chapter "4.2 Pilot scenarios introduction and LIGHTest features associated ".

This is the first deliverable (D9.1) in the CORREOS Pilot demonstration task, and its aim is to present and analyse of the Requirements, Scenarios and Demo Data for that pilot. All along the document there will be information referenced from other different work packages. Likewise, there is a set of similar information within both of the analogous deliverables of the pilots: D9.1 (this one) and D9.5 [1] (also mentioned as PEPPOL IBM pilot).

Further on this document, the reader will navigate through all the information needed to understand how the eCommunications pilot is envisioned. Starting with a list of the requirements that might be of interest for developing such pilot, include an introduction first and then a full description of the pilots scenarios environment. As final closure of the document, there are a chapter describing the necessary demo data and some of the conclusions after definition of the pilot.

2. Document Information

2.1 Contributors

Name	Partner
Victor Martin	CORREOS
Carlos Balot	CORREOS
Rosario Encinas	CORREOS
Javier Salazar	CORREOS
Ramon Castrejon	CORREOS
Rogelio Menez	CORREOS
Ivan Martín	CORREOS
Javier Presa	ATOS
Miguel Angel Mateo	ATOS
Miryam Villegas	ATOS
Alberto Crespo	ATOS
Burçin BOZKURT GÜNAY	TUBITAK
Olamide Omolola	TUG
Rachelle Sellung	USTUTT
Sven Wagner	USTUTT
Frank-Michael Kamm	G+D
Hans Graux	TLX

2.2 History

Version	Date	Author	Changes
0.1	14-02-2018	Javier Salazar	Initial creation of the document based on all info received by all CORREOS members.
0.2	10-04-2018	Javier Salazar, Carlos Balot	Adding further information and fulfillment of the topics, as well as information from Stuttgart pilots Workshop meeting. Also added the first version made by ATOS.
0.3	27-04-2018	Carlos Balot	Adding information agreed at Stuttgart Pilots Workshop.
0.4	14-05-2018	Victor Martin	Adding information gathered from: TUG.
0.5	18-05-2018	Javier Salazar, Victor Martin	Version with all partners' comments & collaborations (TUBITAK, ATOS, CORREOS, FHG, USTUTT).
0.6	21-05-2018	Javier Salazar	ATOS latest comments and recommendations.
0.7	23-05-2018	Hans Graux	Addition of minor comments in relation to ethics and legal compliance, notably data protection
0.8	24-05-2018	Carlos Balot	Final draft version of the document for internal reviewers (USTUTT & ATOS).
1.0	29-05-2018	Javier Salazar	Final version to EC with internal reviewers comments

3. Table of Contents

3.1 Table of Figures

3.2 Table of Tables

N/A

3.3 Table of Acronyms

Term	Meaning	Reference
LoA	Level of Assurance	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_LoA_Mapping.pdf?__blob=publicationFile&v=4
ATV	Automatic Trust Verifier	
GDPR	General Data Protection Regulation	https://www.eugdpr.org/
API	Application Programming Interface	
REST API	Representational State Transfer API	https://en.wikipedia.org/wiki/Representational_state_transfer
TRL7	Technology Readiness Level	https://en.wikipedia.org/wiki/Technology_readiness_level
DNS	Domain Name System	
DNSSEC	DNS Security Extensions	https://es.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
DANE	DNS-Based Authentication of Named Entities	https://www.internetsociety.org/resources/deploy360/dane/
NTLM	Windows Challenge/Response	https://msdn.microsoft.com/es-es/library/windows/desktop/aa378749(v=vs.85).aspx
LDAP	Lightweight Directory Access Protocol	https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
HTTPS	HTTP Secure	https://en.wikipedia.org/wiki/HTTPS
OTP	One Time Password	
sTLD / gTLD	*s*ponsored Top-Level Domains / *g*eneric Top-Level Domains	https://en.wikipedia.org/wiki/Top-level_domain
eIDAS	REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions	https://www.eid.as/home/
NIST	National Institute of Standards and Technology	https://www.nist.gov/

4. Requirements

The specific scenarios that will be proposed further on this document, include LIGHTest integration as APIs calling at any point of the service. Specifically, it'll be called at moments where it would add value to any business transaction. This pilot is mainly focus on market-check of the ATV access door as way to sell the LIGHTest as a trust service.

Moreover, it'll be interesting that LIGHTest is capable to offer a quick and easy check with any due Level of Assurance (LoA) policy and give some kind of assurance of the check to infrastructure customer. It was proposed that this assurance could be shown as a "badge" of LIGHTest checked.

LIGHTest will be tested in the Minder platform provided by TUBITAK. However, the conformance and interoperability tests will be carried out in the pre-production phase. Therefore, within the pilot phase (which is at the LIGHTest production phase) it is not planned to test the components using the Minder testbed.

4.1 Analysis of the Functionality that is Relevant

The pilots plan to take into consideration all of the requirements that were developed in Deliverable D2.3 [2] and D2.10 [3]. The requirements were developed to ensure that a wide and diverse spectrum of requests was considered regarding the technical and market needs. With that, there are five identified categories. The five categories are the following: Functional Requirements, Privacy Requirements, Security and Accountability Requirements, Usability Requirements and Economic Requirements. Further categories of requirements regarding Societal, Legal and Ethical Requirements will be explored in Deliverable 2.10 [3]. Regarding each category, there is an established structure and methodological reason that is tailored to the needs of each perspective.

As mentioned above, the Pilots will consider all of the requirements provided in D2.3 [2] and D2.10 [3]. With that, it is not expected that all of the requirements will be necessary or applicable to each pilot as they are very detailed use cases, where the requirements were made in a broader sense. With that, within the pilots work package are reviewed the requirements and depict which are a 'may, must, should, not applicable' as decided in D2.3 [2]. The "selection" of the requirements from D2.3 [2] can be found below. Further, the Correos Pilot has some first impressions to, which requirements will be applied in which way. These impressions are subject to change as development progresses.

In WP2, the Task 2.8 "*Evaluation*" will evaluate and access all of the requirements, also on a pilot level.

4.1.1 Functional Requirements

No.	FR-01.00- Performance
Description	LIGHTest SHOULD provide results in time relative to the complexity and amount of required information.

No.	FR-02.00- DP: Can be integrated with DNSSEC
Description	A Delegation Publisher MUST operate an off-the-shelf DNS Name Server with DNSSEC extension.

No.	FR-03.00- ATV: Verify Trust (1)
Description	The Automatic Trust Verifier (ATV) MUST be able to take an Electronic Transaction and Trust Policy as input.

No.	FR-03.01- ATV: Verify Trust (2)
Description	The ATV MUST provide outputs, if the Electronic Transaction is trustworthy [y/n] and highly recommended with explanation of its reasoning (in particular if not trustworthy). It uses a pluggable parser for Electronic Transactions as sub-component.

No.	FR-03.02- ATV: Verification Process Receipt
Description	The Automatic Trust Verifier MUST provide a receipt for every verification process.

No.	FR-03.03- ATV: Data Integrity
Description	The Automatic Trust Verifier MUST verify the integrity of the data it uses in the trust verification process.

No.	FR-04.00- Applications for non-technical verifiers (1)
Description	Provide an application for non-technical verifiers to easily understand and author individual trust policies.

No.	FR-04.01- Applications for non-technical verifiers (2)
Description	Provide automatic means for verifiers to verify the trustworthiness of complex electronic transactions.

No.	FR-05.00- TSPA: Can be integrated with DNSSEC
Description	The Trust Scheme Publication Authority MUST be able to operate an off-the-shelf DNS Name Server with the DNSSEC extension

No.	FR-05.01- TSPA: Trust List Flexibility
Description	LIGHTest MUST be able to publish multiple Trust Lists under different sub-domains of the Authority domain name

No.	FR-05.02- TSPA: Utilities to Load selected Trust Lists
Description	The utilities that parse selected Trust List formats MUST be able to be written or loaded into an equivalent DNS Zone files

No.	FR-06.00- TTA: Can be integrated with DNSSEC
Description	A Trust Translation Authority MUST operate a standard DNS Name Server with DNSSEC extension

No.	FR-06.01- TTA: Trust Data Flexibility
Description	A server publishes multiple Trust Lists under different sub-domains of the Authority's domain name

No.	FR-06.02- TTA: Utilities to Load selected Trust Translation Data
Description	The utilities parse and query input data and write or load equivalent DNS Zone files. The "zone file writer" sub-component can be used for multiple utilities and expose a conceptual view (reference to D2.14).

No.	FR-06.03- TTA: Formats
Description	The Trust Translation Publisher MUST be able to accept trust translation lists of all the required formats, such as Boolean, ordinal, and tuple-based.
	Note: *This formats have to be further defined within the development of the pilots, it may be used one or more of the formats.*

No.	FR-06.04- TTA: User interface
Description	The Trust Translation Publisher MUST provide an interface, either GUI or API or both, to create and edit trust translation lists.

No.	FR-06.05- TTA: Uniform interface
Description	The Trust Translation Publisher SHOULD provide a uniform interface feel to the user as the publication and delegation interfaces.

No.	FR-06.06- TTA: Discoverability
Description	The Trust Translation Publisher MUST implement the required functionalities to make the translation lists discoverable through DNS according to the required URL formats.

No.	FR-06.07- TTA: Interface
Description	The Trust Translation Authority MUST be able to accept trust translation lists of all the required formats, such as Boolean, ordinal, and tuple-based.

No.	FR-06.08- TTA: Interface
Description	The Trust Translation Authority MUST provide an interface, either GUI or API, to create and edit trust translation lists.

No.	FR-07.00- Policy Authoring and Visualization Tools Use Acceptability
Description	Policy Authoring and Visualization Tools MUST be an interactive software (e.g. one or several desktop/web applications) that make it easy for non-technical users to visualize and edit a Trust Policy.

No.	FR-08.00- Individual Trust Policy
Description	LIGHTest Trust Policy MUST provide formal instructions how to validate trustworthiness of a given type of transaction. It always states which Trust Lists from which Authorities should be used.

No.	FR-08.01- Individual Trust Policy: Flexibility
Description	The LIGHTest Individual Trust Policy MUST be able to interpret LIGHTest Trust Policy Language

No.	FR-08.02- Individual Trust Policy: Interface
Description	The Policy authoring tool MUST have a user-friendly interface for non-technical users

No.	FR-08.03- Individual Trust Policy: Creation
Description	The Policy Authoring tool MUST be able to create and edit Trust policies

No.	FR-09.00- Global Trust Lists
Description	LIGHTest Infrastructure SHOULD develop the concept and infrastructure for global trust lists.

No.	FR-10.00- Mechanisms for Publication and Querying Trust Lists
Description	Provide the mechanisms that SHOULD have the ability for the publication and querying of trust lists with the same convenience that OCSP brings to revocation lists.

No.	FR-10.01- Mechanisms for determining individual assurance levels
Description	Provide a component that SHOULD determine individual assurance levels that is easy to integrate in arbitrary applications and systems.

No.	FR-10.02- Mechanisms for translating foreign Trust Schemes
Description	Provide the mechanisms SHOULD translate foreign trust schemes into the context of the local jurisdiction

No.	FR-10.03- Mechanisms for publishing delegations/mandates and trust-related attributes
Description	Provide the mechanisms SHOULD publish delegations/mandates and trust-related attributes for easy querying.

No.	FR-11.00- Uniform Interface
Description	The publishers for lists, translation, and delegation SHOULD provide a uniform interface feel to the user.

4.1.2 Privacy Requirements

No.	PR-03.00- Unlinkability
Description	The Pilots using Components of the LIGHTEST Reference Architecture MUST support the privacy protection goal of unlinkability. They MUST ensure that privacy-relevant data cannot be linked across privacy domains that are constituted by a common purpose and context.

No.	PR-03.01- Purpose limitation (lawfulness and fairness)
Description	Any personal data SHOULD be collected only for specified, explicit, lawful, and fair purposes and not further processed in a way incompatible with those purposes. The personal data SHOULD be adequate, relevant and limited to what is necessary for the purposes for which they are processed. In particular, the specific purposes for which personal data are processed SHOULD be explicit and legitimate and determined at the time of the collection of the personal data.

No.	PR-03.02- Sensitivity awareness
Description	Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation MUST be prohibited, unless one of the conditions listed in Article 9 of GDPR applies.

No.	PR-04.00- Data minimization
Description	Any personal data collected MUST be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

No.	PR-04.01- Minimal registration data
Description	As a corollary of the Data minimization requirement, any data required to use the LIGHTest services by any actor SHOULD NOT include any identifiable data, and any identifier SHOULD be randomly generated.

No.	PR0-5.00- Transparency
Description	Any personal data collected MUST be processed in a transparent manner in relation to the Data Subject: information MUST be provided to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons SHOULD be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

No.	PR-05.04- Transparency towards actors
Description	All outcomes of authentication, authorization, delegation, and identity and attribute management processes, including any automated decision-making, MUST be visible (transparent) for the relevant actor whose electronic transaction is being processed.

No.	PR-05.05- Notification
Description	If personal data are obtained from the Data Subject, the Data Controller MUST provide the Data Subject with the information described in Article 13 of GDPR. If any personal data have not been obtained from the Data Subject, the Data Controller MUST provide the Data Subject with the information described in Article 14 of GDPR. The controller MUST communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Articles 16, 17(1) and 18 of GDPR to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller MUST inform the Data Subject about those recipients if the Data Subject requests it.

No.	PR-06.00- Intervenability
Description	The Pilots using Components of the LIGHTEST Reference Architecture MUST support the privacy protection goal of intervenability. Data subjects MUST be provided with the opportunity to have control over how their personal data is processed.

No.	PR-08.00- Storage trustworthiness and accountability
Description	If any personal data are collected for the LIGHTest pilots, the pilots MUST provide a trustworthy storage for them preserving their authenticity, where only authorized persons would be allowed to make changes and new entries. Each Data Controller and, where applicable, the controller's representative, MUST maintain a record of processing activities under its responsibility. That record shall contain all of the information specified in Article 30 of GDPR.

4.1.3 Security and Accountability Requirements

The Security and Accountability Requirements are internal to the LIGHTest infrastructure processing and are not visible the users of the technology. Any pilot, specifically for this document the Correos pilot (T9.1), should not check or test this set of requirements.

4.1.4 Usability Requirements

No.	UR-01.00- High Usability

Description	Usability and understanding of services and applications SHOULD be a main benefit to the End-Users. Given that End-Users, may have a wide range of competence with this technology it is important to make it as simple and usable as possible.

No.	UR-01.02- Learnability
Description	Learnability is an important Usability Design Principle. In this case even more important, because most users have little knowledge of the topic. So first of all, they have to learn how the system works.

No.	UR-02.00- Usable Tools
Description	In order for users to achieve higher Usability with the Trust Policies, LIGHTest MUST provide Usable Tools to assist in better understanding of Trust Policies.

No.	UR-03.01- User readable terminology
Description	All terminology (Labels, Buttons, Messages etc.) must be understandable for users with little technical understanding, users new to the software and the subject. Example: Instead of encrypted email – „Secret message for...“or „email only readable for…“

No.	UR-04.00- Team to answer queries
Description	Having a team available to answer questions and queries from end-users as and when they arise.

No.	UR-05.00- User Experience
Description	Building on Usability, the LIGHTest Project should consider User Experience to guarantee good user acceptance. Especially the basic human needs security and competence are important factors in designing a security system. Ideally the System is able to address those Needs to create a good User Experience.

No.	UR-07.00- Easy to grasp metaphors
Description	Often security software uses metaphors which aren't easy to understand or are even misunderstood (for example the metaphor for public and private key). Easier to understand and grasp metaphors would help the users to understand the whole concept of the topic on a high Level.

No.	UR-08.00- Transparency

Description	There is no need for the user to understand to whole system and every little detail that happens in the background. But the system UI must be transparent enough so the user can understand the overall concept and therefore understand what's happening and what he/she is supposed to do. At any given point the system should be transparent enough whilst not overstraining the user.

No.	UR-09.00- Minimalistic / simple User Interface Design
Description	It is found that with security sensible transactions users prefer a simple and minimalistic User Interface, so that they can focus on important tasks and realize what is happening. So every clutter or non-relevant information must be excluded from the UI.

No.	UR-10.00- Empowered Users
Description	Users must always feel in control of the things happening in the UI.

No.	UR-11.00- Error handling
Description	In all predictable cases the system must hinder the user to make mistakes. But the system shouldn't just block an operation. Instead it should explain to the user why this operation isn't available at the Moment. Same with mistakes. If there's an error, or the user makes a mistake the system must provide clear and understandable cause, also giving the user clear instruction on how to fix it.

No.	UR-12.00- Cognitive load
Description	Cognitive load must be minimized as much as possible. Security is a secondary task for the user. If the user has to remember too much or has to execute too many tasks, the user won't return to the system. There should be as little to remember as possible and as little to execute to achieve the desired goal.

4.1.5 Economic Requirements

No.	ER-01.00- Support of various business models
Description	Different stakeholders and scenarios need different business models. There is no business model that fits all applications. Therefore, LIGHTest MUST support various business models and applications. Refer to the Stakeholder analysis.

No.	ER-01.03- Support for various pricing models and strategies

Description	The willingness to pay by different users varies, depending on the use case. In order to build a sustainable business model, users and providers have to be approached in different ways / levels in order to absorb their willingness to pay. Therefore, LIGHTest MUST support price differentiation according to the different willingness to pay individual stakeholders for the different applications.

No.	ER-01.04- Supports different deployment models
Description	Different stakeholders and different scenarios require different deployment models (Public Institutions, Private Corporations, Citizens). There is no deployment model (Trust Policy) that fits all applications. Therefore, LIGHTest MUST support a wide range of application models for different applications.

No.	ER-02.00- Provide value for all stakeholders involved
Description	Many stakeholders are relatively satisfied with the currently used trust use case solutions and trust management. In order for the relevant stakeholders to use LIGHTest, they MUST to be offered added value. Examples of 'added-value' could be either having additional merit, increased user-friendliness, security or data protection benefits, improved usability, greater convenience, financial benefits. Refer to Use Cases for specific examples.

No.	ER-03.01- Support of Various Trust Objectives
Description	LIGHTest MUST support various types Trust Frameworks, Policies, Schemes, and Lists to enable the networking of different stakeholders. The aim is to promote cross-border cooperation with the ultimate objective of optimizing trust management and more efficient.

No.	ER-03.02- Support of Existing Trust Frameworks, Lists, Policies, Schemes
Description	With a large variety of pre-existing Trust Frameworks, Lists, Policies, and Schemes, LIGHTest MUST be flexible enough to utilize and support already existing works.

No.	ER-04.00- Global Application
Description	The market for Trust Management is global. A unique selling point for LIGHTest, is that it works globally and on a large scale. Therefore, the LIGHTest SHOULD be globally applicable. Related to: Societal Requirements

No.	ER-06.00- Easy Adoption
Description	LIGHTest MUST establish and consider adoption factors of the users and the market. This MUST be done at all levels of development.

No.	ER-06.01- Flexibility and Acceptance of Individual Trust Applications
Description	LIGHTest MUST allow for each entity to be able to make their own choices and have the ability to design their own rules and regulations whether it is with the used Trust Framework, Policies, Schemes, or Lists.

No.	ER-07.00- Neutrality
Description	Similar to the grid neutrality, the entourage ecosystem SHOULD NOT ensure individual players' preference, but a transparent neutrality of all participants.

4.1.6 Legal and Ethics Requirements

No.	LE-01.00 – Implementation of an appropriate contractual framework
Description	In order to satisfy the privacy requirements as outlined in section 4.1.2., and also to address legal issues in relation to the use of the TSPA, TTA and ATV, a contractual framework needs to be established between Correos and the entity operating the TSPA, TTA and ATV. If Correos will operate these itself, no contractual framework will be needed as the data remains under Correos' control; otherwise a contract is mandatory.

No.	LE-02.00 – Implementation of an appropriate transparency notice (privacy policy) towards end users of the pilot scenarios
Description	In order to ensure that end users are informed in relation to the use of their personal data, a privacy notice needs to be put in place that satisfies the requirements of the GDPR. Such a notice is not necessary if the services will be piloted only with fake data; otherwise a notice is mandatory.

No.	LE-02.00 – Implementation of appropriate terms and conditions towards end users
Description	In order to ensure that the legal responsibilities and assurances (if any) are clear to end users, terms and conditions need to be put in place that satisfiy the requirements of the eIDAS Regulation, eCommerce legislation and (if applicable) consumer protection rules. Terms and conditions are not necessary if the services will be piloted only with fake data; otherwise they are mandatory.

4.2 Pilot scenarios introduction and LIGHTest features associated

Correos pilot focuses on trust within eCommunications (eDelivery and eNotification) mostly, but eID authentication scenario will also be analysed and explained further in this document. Those 3 possible scenarios will be explained, but not forcefully implemented all of them, as integration has to be fully designed to ensure feasibility of each scenario.

As introduced before, automatic trust verification is the key feature of interest, as it can work as a "trust-check API" (through the ATV). Correos is a service provider and the services within the eCorreos suite could benefit from a somehow verified/certified double-check for electronic transactions.

Figure 1: What is eCorreos

Three different possible scenarios will be explained afterwards, a briefing explanation is as follows:

- **My Mailbox ("*Mi Buzón*")** is a digital service for citizens, companies and governments enabling them to send and receive documentation. Information is stored with all legal guarantees and high security standards. Sender and receiver are validated and uniquely identified by Correos. Individuals subscribe to any verified business/government agency to start receiving trusted information. LIGHTest ATV would be used to inform users about document **eDelivery** LoA, and LoA translation in the case of non-national companies.

- **My Notifications ("*Mis Notificaciones*")** is a digital service foreseeing centralization and management of governmental **eNotifications** for one or several individuals or legal entities. In such secured and trusted communications, it would be useful to offer value by double-checking with a certified entity in Europe that such communication is done accordingly to current legislation.

- **Correos ID** provides secured **digital IDs** to citizens, businesses and governments. It's a trusted third party to validate identity attributes, raising third parties trust on individuals. This service is used as authenticator for internal to Correos and external applications,

LIGHTest may help checking this transaction/action taking by the user and ensure is compliant with a specific trust policy.

However, these scenarios are subject to changes due to business requirements and/or strategic changes with the digital suite of Correos (eCorreos). Aim of the project is to at least test 2 out of the 3 scenarios presented in this document, ensuring the infrastructure testing in a real environment.

The reference architecture for LIGHTest is reproduced below for reference in the following discussion. These scenarios include the use of Trust Schemes (TSPA - WP3) and Trust Scheme Translation (TTA - WP4) together with the Automatic Trust Verifier (ATV - WP6)[1]. This will, most likely mean, that it'll have to exist a first call to TTA and TSPA APIs to prepare the LIGHTest-Correos information/resources in which the transaction validation will be done through the ATV. This will be further analysed along this document.

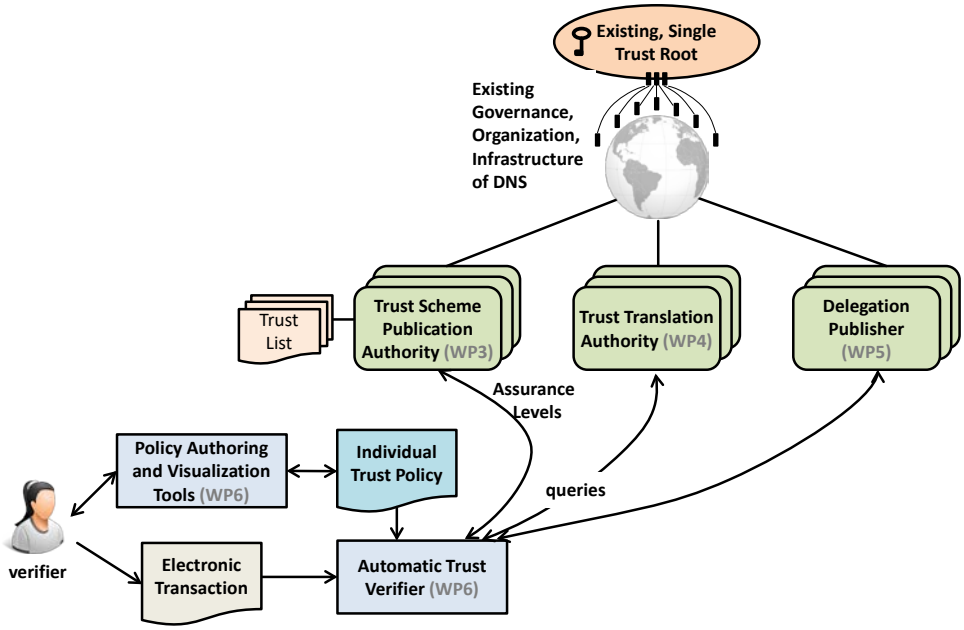


Figure 2: Reference architecture for LIGHTest

As extracted from the general objectives of the project, list of pilot specific objectives is:

O9.1 Demonstrate LIGHTest in an operational environment (TRL7)
O9.2 Demonstrate the ease of trust-list-enabling diverse existing systems
O9.3 Demonstrate LIGHTest integration of foreign trust schemes through scheme translation

[1] to be confirmed further on depending on the chosen scenarios.

O9.4 Demonstrate the ease of authoring individual trust policies
O9.5 Demonstrate automatic trust verification of electronic transactions
O9.6 Demonstrate the use of delegations as part of automatic trust verification
O9.7 Demonstrate how LIGHTest enables easy validation of signatures without the use of validation authorities.

From this objective below are listed the ones will be tested within the eCorreos pilot:

- ✓ O9.1 Demonstrate LIGHTest in an operational environment (TRL7)
- ✓ O9.2 Demonstrate the ease of trust-list-enabling diverse existing systems
- ✓ O9.5 Demonstrate automatic trust verification of electronic transactions
- ✓ O9.7 Demonstrate how LIGHTest enables easy validation of signatures without the use of validation authorities.

4.2.1 Which existing trust schemes should be used

Regarding the setup of the pilot environment, it was agreed to at least be included by WP3 leaders the schemes for eIDAS validation of transactions, as the project is developed under the European commission framework. Additionally it'll be evaluated if some type of agreement can be done with the representative body of the European Commission regarding the eIDAS policy, as it'll add an extra layer of trust (as business perspective it could be even created a "CE-LIGHTest validated badge").

Furthermore, if possible it should be included the policies mentioned all along the project, such as related ISOs or NIST policy for electronic transactions. Moreover, empowering the first usage of the infrastructure and business adoption.

4.2.2 Which components of the existing LIGHTest system are necessary

As already stated in 4.2 Pilot scenarios introduction and LIGHTest features associated introduction, and briefly speaking, LIGHTest components will provide two kinds of APIs:

- APIs towards Administrator users, to maintain the bilateral agreements (publishing trust translation lists). To be expected to use the TSPA and TTA APIs. Most likely used rarely and at least once before using the ATV, as a configuration for all Correos Pilot environment.
- API towards ATV, to provide trust validation over electronic transactions based on policies and the schemes already uploaded to LIGHTest (including eCorreos schemes and WP3 standard schemes explained before).

Automatic Trust Verifier (ATV)

Automatic Trust Verifier takes an Electronic Transaction and Trust Policy as input, outputs trustworthy [yes/no], possibly with explanation of its reasoning (in particular if not trustworthy). It uses a pluggable parser for Electronic Transactions as sub-component. The ATV will usually require input about trust scheme from the Trust Scheme Publication Authority, optionally require input from the Delegation Publisher and the Trust Translation Authority for delegation verification, and trust translations. These optional requirements are dependent on the specifications given in the trust policy.

Trust Scheme Publication Authority (TSPA)

The Trust Scheme Publication Authority (TSPA) provides the infrastructure for the Publication of Trust Schemes as well as for the Discovery and Verification of Trust Scheme Memberships. For this purpose, the conceptual framework consists of two components; a DNS Name Server with DNSSEC extension and a Trust Scheme Provider. The DNS Name Server is used for the discovery of associated Trust Scheme and Trust Scheme Provider and the Trust Scheme Provider contains the signed trust list indicating if the Issuer operates under the specific Trust Scheme.

More information about TSPA can be found in D3.1 [4], D3.3 [5] & D3.4 [6].

Trust Translation Authority (TTA)

Once the ATV has fetched the Trust Scheme under which an entity claims to operate, if the given Trust Scheme is not valid for the transaction under study, ATV with the assistance of the TSPA can set the appropriate level of the trust Scheme associated to the entity and request to the TTA if there exists another Trust Scheme which validate the transaction that is equivalent to the one of the entity. In other words, whether there is a signed agreement with another Trust Scheme to validate the transaction.

In order to fulfil with this operation, TTA provides two different interfaces, the very first interface is a REST API for the provisioning of the TTA. This interface is designed to manage, into the TTA, translation agreements between Trust Schemes. With this interface an Administrator can create new agreements and modify them. It should be taken into account that once an agreement is created it is not possible to delete it, as it is possible that, although the validity period of the agreement has finished, ATV could need to verify transactions done in the past or affected by this agreement. Also, it is possible that beyond the validity period of the agreement, it can be valid for a specific policy in the ATV.

The second interface is offered to the ATV in order to discover Trust Translation Agreements. It is a DNS interface with DNSSEC and DANE extensions in order to offer mechanism to validate the information provided.

More information about TTA can be found in D4.1 [7], D4.3 [8] and D4.4 [9]

4.2.3 Which existing application-specific infrastructure is available from Correos infrastructure

eCorreos is a cloud-based suite of services that aims to deliver digital trusted services to citizens in Spain. Such environment will be available to market-check LIGHTest, consequently to discover the benefits of using an additional trust management DNS infrastructure and its market acceptance.

The suite of services uses a backbone IdP which is based on: Kerberos, NTLM, LDAP and Group policy. This backbone, “My Identity” B2C infrastructure, is the environment that communicates to any integrated service through Web Services (WS) using OTPs and an OAuth2 (Open ID Connect) customization. These integrated services can be either applications within the eCorreos suite or external apps, using specific APIs.

Services infrastructure has 2 live environments, accessible externally: production and pre-production. Additionally it got several local development environments for the teams working on it. For the purposes of this pilot, everything will most likely be deployed in pre-production environment, as live production environment cannot be a subject of testing research based applications (due to internal policy).

Web front end is HTTPS secured plus .post domain secure policies. .Post is a sponsored top-level domain (sTLD) available exclusively for the postal sector. It is the first gTLD to be 100% secured by DNSSEC. It aims to integrate the physical, financial and electronic dimensions of postal services to enable and facilitate ePost, eFinance, eCommerce and eGovernment services. .Post domains are sponsored by the UPU (Universal Postal Union), a specialized agency of the United Nations that coordinates postal policies among member nations.

The specific scenarios that will be proposed further on this document, include LIGHTest integration as APIs calling at any point of the service. Specifically, it’ll be called at moments where it would add value to any business transaction. This pilot is mainly focus on market-check of the ATV access door as way to sell the LIGHTest as a trust service. Therefore, LIGHTest will be used through the ATV, but also the APIs provided by the TSPA and TTA to publish the correspondent trust schemes and the related translations (the first time for setup and only after if the trust scheme of Correos changes).

4.2.4 Which real or fake stakeholders need to be involved to demonstrate the targeted objectives

The pilots will be working closely with WP10 and WP2 on how to demonstrate and exploit stakeholders during the development process and the impact that could evolve after. This will be done in both a theoretical and applied way.

A first insight to the stakeholder's involved in the pilots from a theoretical perspective will be provided in Task 2.8 "*Evaluation*" and D2.12 [10]. This will tend to more of the analysis of potential 'fake' stakeholders. In task 2.8, it will take the preceding stakeholder analysis given in D2.3 [2] and in D10.1 [11] and apply those results to a more concentrated and defined use case of the pilots.

Likewise, this analysis will be done in order to enhance the understanding of the pilots potential and exploit opportunities, taking into consideration the perspectives of real potential stakeholders. During the final year of the project, the pilots will be a focus of an International Forum meeting with the stakeholders, in order to establish a more applied and realistic perspective of the stakeholder for the pilots.

As a first approach and depending on each of the scenarios these are the necessary stakeholders to be represented for each mentioned Correos scenarios:

- My Mailbox: fake/real (opportunity to any consortium member to get onboard and test/use Correos service) company to subscribe to.
- My Notifications: need to create a fake government agency or to convince a real one to test.
- Correos ID: create a set of fake/real (is currently open to any person, so the consortium members could be the testers) users to access any due service.

4.3 Mobile ID specific requirements

The mobile ID component could be used for strong authentication of a customer (with the FIDO protocol and biometrics or PIN or card-based authentication) and to couple the authentication credentials to a user identity/identification. The main value is that you will get a direct cryptographic link between the results of an onboarding/identification session (not part of the mobile ID solution) and the strong authentication credentials of the user and that the ID provider is not needed anymore after an initial registration.

The flow could be the following (to be determined further on the project):

1. The user registers on eCorreos and can now use the smartphone (with biometrics or PIN) for (*passwordless*) strong authentication based on the FIDO protocol. Without

further identification, the user could for example access services that require a low level of any due LoA.
2. For identification the user is redirected to an IdP.
3. The IdP makes an attestation of the identity attributes and generates a certificate over the FIDO public key of the user.
4. Finally, eCorreos has a direct link between the customer identity and the FIDO key used for strong authentication. From now on the customer can simply authenticate with the smartphone.

This approach would require some integration work between the IdP, the LIGHTest infrastructure and the FIDO part, but for demo purposes this could be handled by an intermediate server that takes over the control of the flow. Since this is a high level of effort work, should only be done if appears meaningful and used in the demo.

For a potential productive rollout there is already a commercial platform available as a basis for the FIDO part (without the integration to LIGHTest). It uses the smartphone as FIDO authenticator and provides authenticators for fingerprint, face and voice biometrics (and PIN as fallback).

5. Scenarios

Within the context of the T9.1, there will be analysed 3 different scenarios. Implementation of each scenario would be subject of further valuation and most likely 2 out of 3 of them will be finally tested.

As introduced in chapter "*4.2 Pilot scenarios introduction and LIGHTest features associated*" the three possible scenarios tries to cover three different aspects of eIDAS regulation: trust services (eDelivery, eNotification) and electronic identity (eID).

Below will be described each scenario and its use case deeply in detail, including infrastructure slide by each one that was introduced before and presented in the General Meeting of Seville from March 2018. This is intended to open the possibilities of LIGHTest business test and not to narrow the possibilities when the infrastructure is ready and further analysis can be done.

All applications are hosted within a cloud-based platform and interconnected by an ecosystem of APIs. More specifically:

- ✓ Correos ID is a web based (responsive to any device).
- ✓ My Mailbox is web and native iOS and Android app based.
- ✓ My Notifications is desktop based, with a web consultation frontend.

All of them are subject to continuous improvement and changes depending on market/business needs. Those are mature services offered by Correos in Spain that most likely will tend to increase the amount of platforms in which it can be accessed.

5.1 My Mailbox - eDelivery scenario

As explained before in this document My Mailbox ("*Mi Buzón*") is a digital service for citizens, companies and governments enabling them to send and receive documentation. Information is stored with all legal guarantees and high security standards. Sender and receiver are validated and uniquely identified by Correos. Individuals subscribe to any verified business/government agency to start receiving trusted information.

By means of LIGHTest, Correos service will validate that the entity sending a document operates under a known Trusted Scheme (eIDAS, NIST, etc.); querying, through the ATV, first to the TSPA to fetch the metadata of the Trusted Scheme claimed and check if it enables the sender, and second if it is necessary to query TTA to look for an equivalent trust scheme level which enables the sender. Moreover, LIGHTest ATV would be used to inform users about document eDelivery LoA, and possible LoA translation in the case of non-national companies.

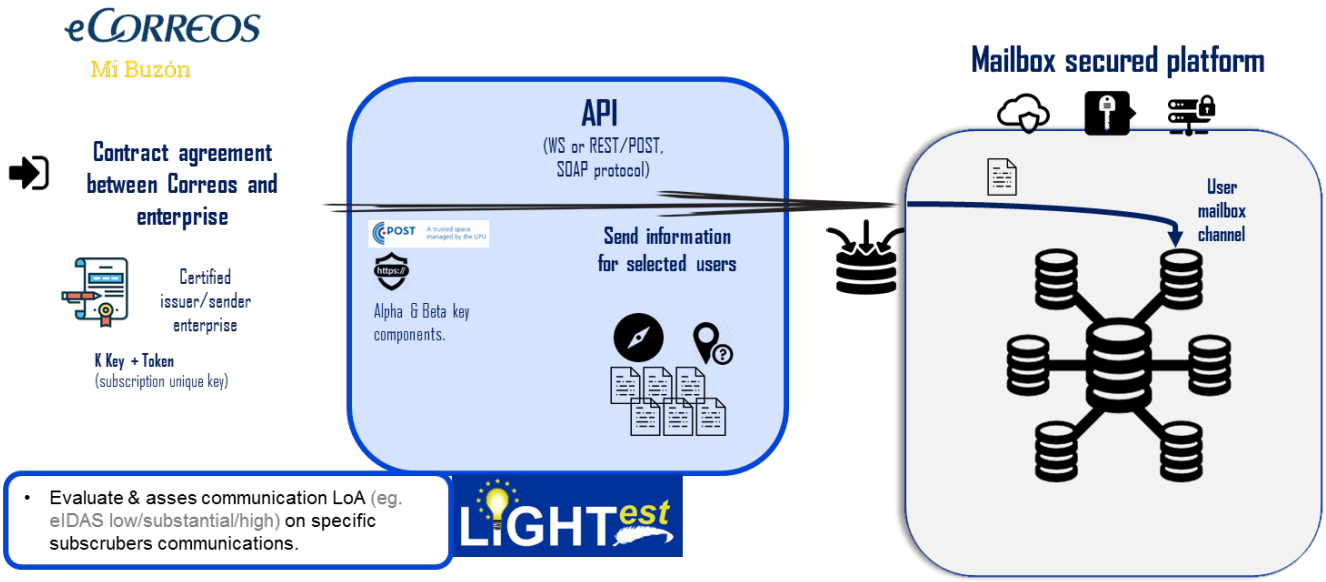
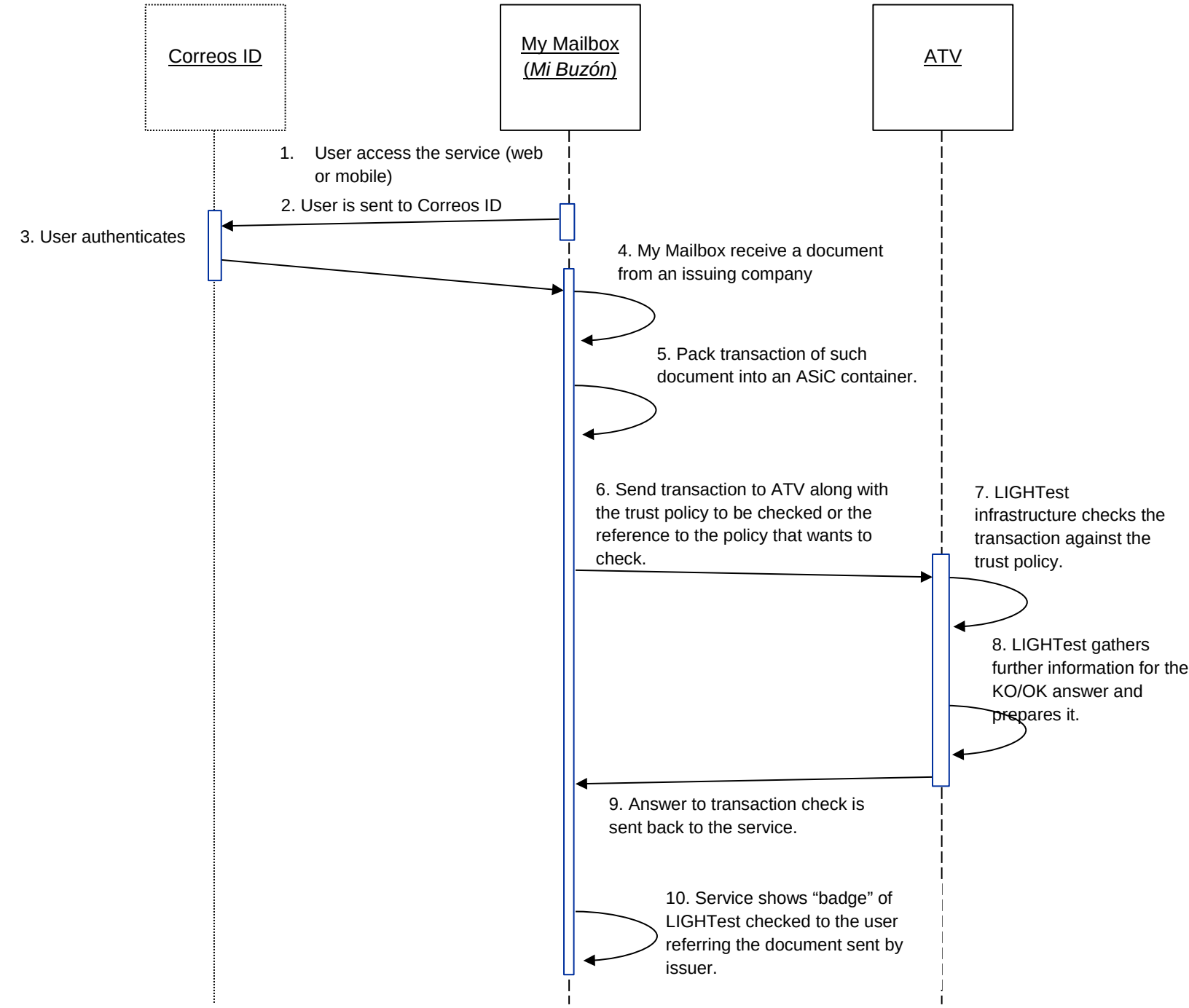


Figure 3: My Mailbox infrastructure description


Correos ID
My Mailbox (Mi Buzón)
ATV
1. User access the service (web or mobile)
2. User is sent to Correos ID
3. User authenticates
4. My Mailbox receive a document from an issuing company
5. Pack transaction of such document into an ASiC container.
6. Send transaction to ATV along with the trust policy to be checked or the reference to the policy that wants to check.
7. LIGHTest infrastructure checks the transaction against the trust policy.
8. LIGHTest gathers further information for the KO/OK answer and prepares it.
9. Answer to transaction check is sent back to the service.
10. Service shows “badge” of LIGHTest checked to the user referring the document sent by issuer.

5.2 My Notifications - eNotifications scenario

As explained before in this document My Notifications ("*Mis Notificaciones*") is a digital service foreseeing centralization and management of governmental eNotifications for one or several individuals or legal entities. In such secured and trusted communications, would be useful to offer value by double-checking with a certified entity in Europe that such communication is done accordingly to current legislation.

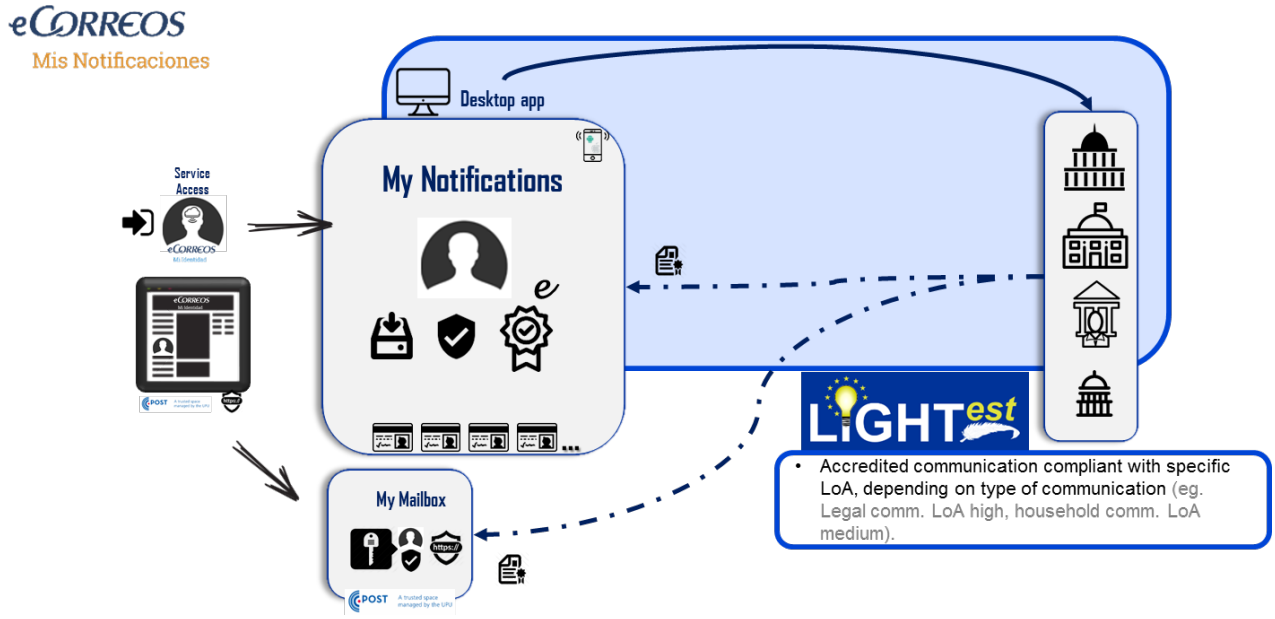
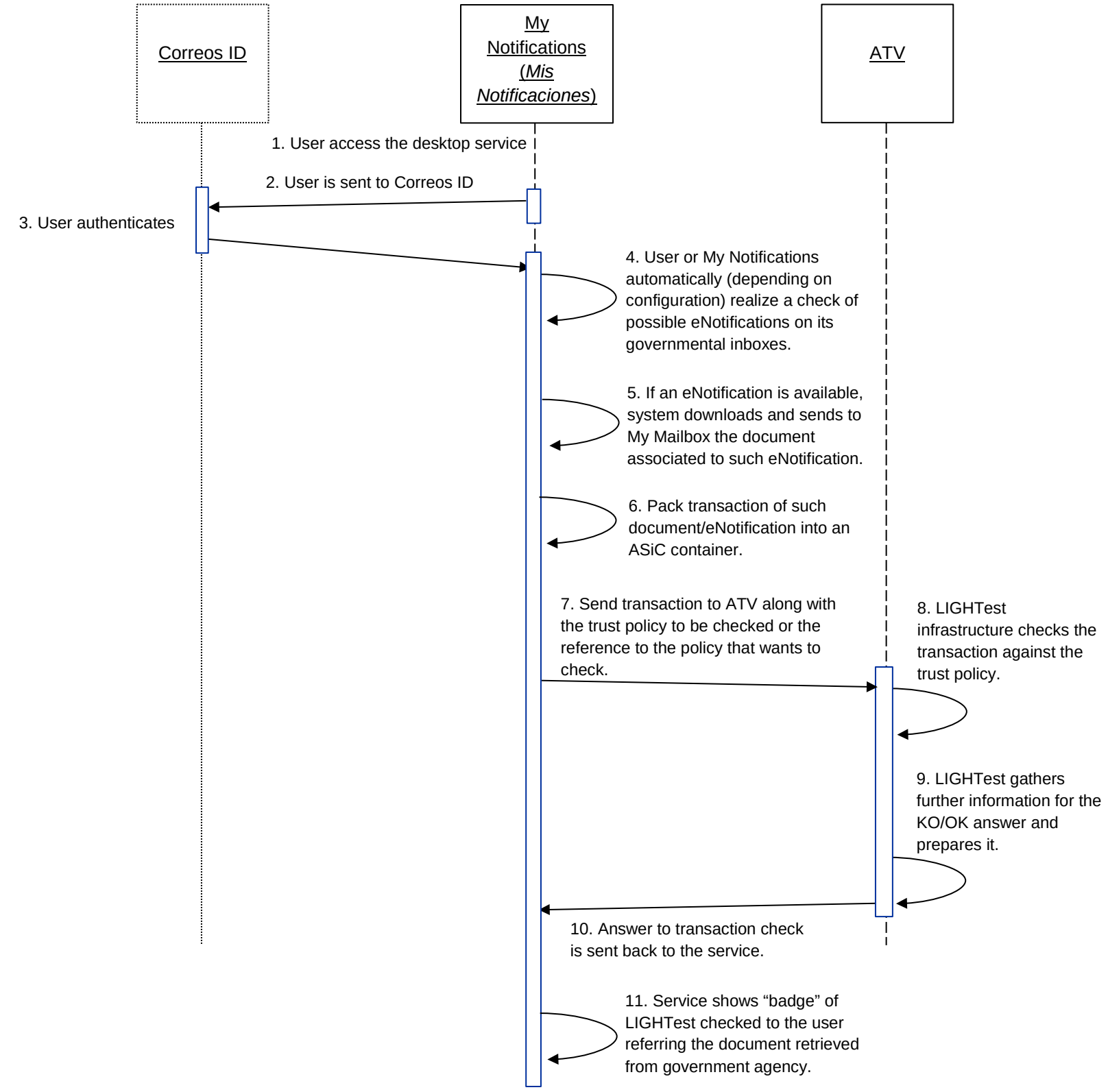


Figure 4: My Notifications infrastructure description


Correos ID
My Notifications (*Mis Notificaciones*)
ATV
1. User access the desktop service
2. User is sent to Correos ID
3. User authenticates
4. User or My Notifications automatically (depending on configuration) realize a check of possible eNotifications on its governmental inboxes.
5. If an eNotification is available, system downloads and sends to My Mailbox the document associated to such eNotification.
6. Pack transaction of such document/eNotification into an ASiC container.
7. Send transaction to ATV along with the trust policy to be checked or the reference to the policy that wants to check.
8. LIGHTest infrastructure checks the transaction against the trust policy.
9. LIGHTest gathers further information for the KO/OK answer and prepares it.
10. Answer to transaction check is sent back to the service.
11. Service shows “badge” of LIGHTest checked to the user referring the document retrieved from government agency.

5.3 Correos ID – eID authentication scenario

As explained before in this document Correos ID provides secured digital IDs to citizens, businesses and governments. It is a trusted third party to validate identity attributes, raising third parties trust on individuals. This service is used as authenticator for internal to Correos and external applications; LIGHTest may help checking this transaction/action taking by the user and ensure its compliance with a specific trust policy.

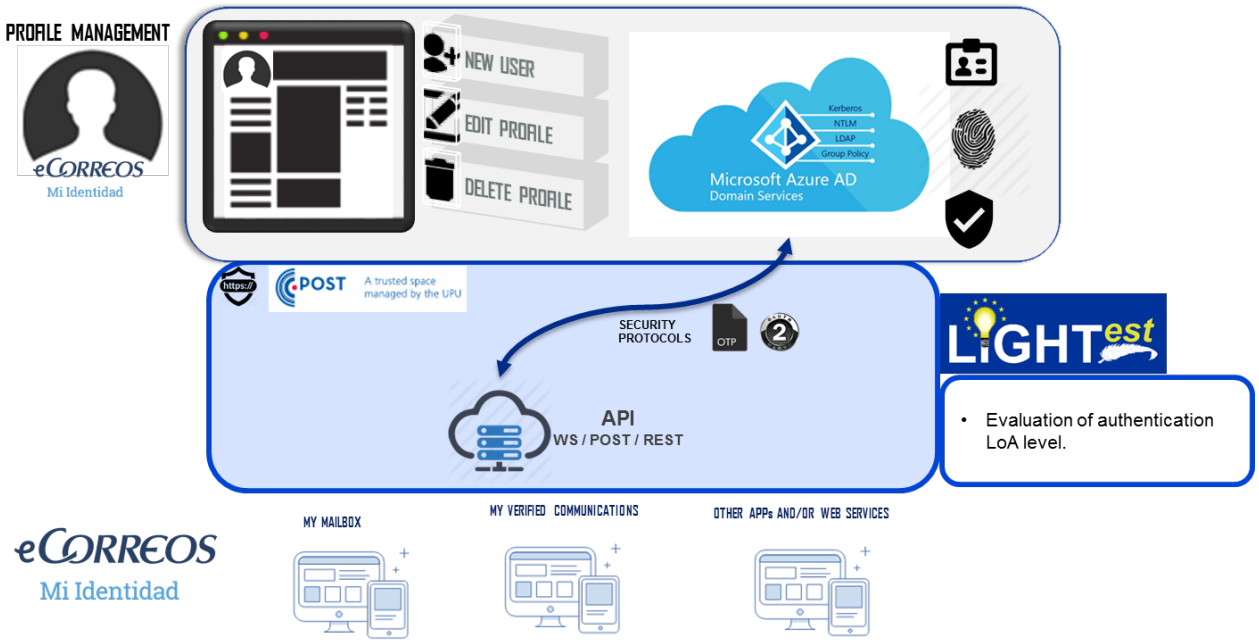
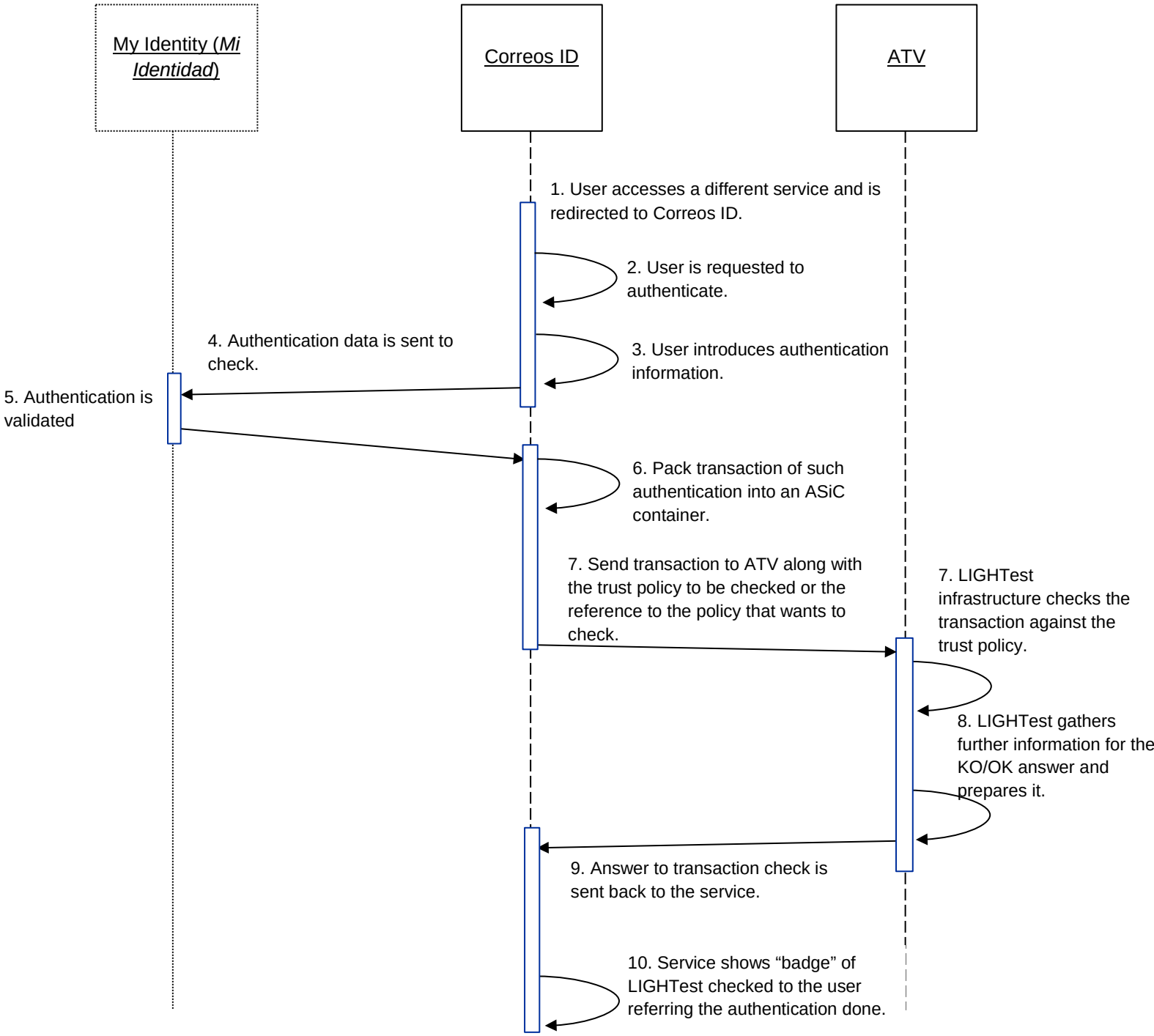


Figure 5: Correos ID infrastructure description


My Identity (*Mi Identidad*)
Correos ID
ATV
1. User accesses a different service and is redirected to Correos ID.
2. User is requested to authenticate.
3. User introduces authentication information.
4. Authentication data is sent to check.
5. Authentication is validated
6. Pack transaction of such authentication into an ASiC container.
7. Send transaction to ATV along with the trust policy to be checked or the reference to the policy that wants to check.
7. LIGHTest infrastructure checks the transaction against the trust policy.
8. LIGHTest gathers further information for the KO/OK answer and prepares it.
9. Answer to transaction check is sent back to the service.
10. Service shows “badge” of LIGHTest checked to the user referring the authentication done.

6. Demo Data

There is several data that will be need and that will have to be produced specifically for the pilot. At this point, it is not necessary to define specifically the data to use, but to identify the sets that will be necessary by each component of LIGHTest:

- DNS entries in the TSPA (as trust lists that includes the issuers for the stated scheme). Please refer to existing standard on trust lists - ETSI TS 119 612.
- Trust Scheme Identifier.
- Translation of DNS entries in the TTA for cross-border LoA translation.
- Trust Policies that can be automatically executed in the ATV (for all parties).
- ASiC packed transactions that can be given as input to the ATV (for all scenarios), including PKI infrastructure for the signing of the electronic transaction.

For trust policy definition please refer to the deliverable WP3 D3.4 - Section 6.3 [6]. In ETSI TS 119 612, the trust scheme policy is specified as part of the information section in the overall structure of trusted lists. Hereby, several tags provide information on the trust scheme policy.

7. End Summary

Requirements analysis done within the first part of the document has shown that a deeper analysis would be of interest. Such analysis, may be done within coming deliverables, would consist on an applied analysis of how the Correos Pilot will cover or address the requirements listed in this deliverable. Such extension will increase clarity and will narrow the target to be achieved within the LIGHTest pilot.

After analysis and definition of the scenarios, the consortium has devised the possible uses of LIGHTest. However, this needs a further detailed review and preparation that will be done in the coming deliverables. As research project, options were tried to keep open, to not exclude possible business cases for the project. Furthermore, the scenarios presented are subject to changes as the detailed analysis and reviews keep going, and development of the project continues.

Likewise, demo data has to be prepared based on the categorization of sets done within the document. This is better to be done when testing scenarios are specified and data starts to be necessary, data creation before the scenarios are completely defined and “closed”, could potentially mean a duplication of work when test phase starts.

8. References

[1] the LIGHTest Project, D9.5 - e-Procurement: Requirements, Scenarios and Demo Data, Project Deliverable, 2018.

[2] The LIGHTest Project, D2.3 - Requirements and Use Cases, Project Deliverable, 2017.

[3] The LIGHTest Project, D2.10 - Legal, ethical and societal requirements and constraints (1), Project Deliverable, 2017.

[4] The LIGHTest Project, D3.1 - Conceptual Framework for Trust Schemes (1), Project Deliverable, 2017.

[5] The LIGHTest Project, D3.3 - DNS-based Publication of Trust Schemes, Project Deliverable, 2018.

[6] The LIGHTest Project, D3.4 - Discovery of Trust SCheme Publication Authorities, Project Deliverable, 2018.

[7] The LIGHTest Project, D4.1 - Conceptual Framework for Trust Scheme Translation, Project Deliverable, 2017.

[8] The LIGHTest Project, D4.3 - DNS-based Publication of Trust Translation Schemes, Project Deliverable, 2017.

[9] The LIGHTest Project, D4.4 - Discovery of Trust Translation Authorities, Project Deliverable.

[10] The LIGHTest Project, D2.12 - Evaluation report (1), Project Deliverable, 2018.

[11] The LIGHTest Project, D10.1 - Business Plan (1), Project Deliverable, 2017.

9. 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), Sociedad Estatal de Correos y Telégrafos (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.