D2.13

Evaluation Report (2)

Document Identification	
Date	12.11.19
Status	Final
Version	1.0

Related WP	WP 2	**Related Deliverable(s)**	D2.2, D2.12
Lead Authors	Rachelle Sellung (USTUTT)	**Dissemination Level**	PU
Lead Participants	USTUTT, FHG, DTU, ATOS, UBISECURE, CORREOS, UPRC	**Contributors**	Please see List of Contributors Below
Reviewers	EEMA, NLNET		

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 goal of this deliverable is to evaluate the requirements for the LIGHTest project that were established in D2.3. With regards to the establishment of requirements, this is done by first defining five categories of requirements that will give a full perspective of what is needed to achieve the highest level of success. Next, there are three driving artefacts in the LIGHTest project. The three artefacts are the Reference Architecture, Implementation, and the Pilots. With that, each established requirement will need to rank the level of importance in reference to each of these artefacts. As this is a two-part deliverable, the deliverable D2.12 Evaluation (1) focused on the evaluation of the Reference Architecture Artefact and this deliverable will focus on the evaluation of the Implementation and Pilots Artefacts.

2. Document Information

2.1 Contributors

Name	Partner
Rachelle Sellung	USTUTT
Stephanie Weinhardt	USTUTT
Sven Wagner	USTUTT
Mohamed Ali Masmoudi	FHG
Heiko Rossnagel	FHG
Sebastian Mordersheim	DTU
Andreas Victor Hess	DTU
Anders Schlichtkrull	DTU
Javier Presa Cordero	ATOS
Alberto Miranda Garcia	ATOS
Javier Gomez Salazar	CORREOS
Charles Sederholm	UBISECURE
Jesse Kurtto	UBISECURE
Andriana Prentza	UPRC

2.2 History

Version	Date	Author	Changes
0.1	01.07.2019	USTUTT	Established First draft and outline of the deliverable
0.2	23.07.2019	USTUTT	Draft of Delieverable to partners

0.4	29.08.2019	USTUTT, All Partners	Updated Draft of Requirements and evaluations of artefacts
0.5	13.09.2019	USTUTT, All partners	Integrated new updates on Evaluations
0.6	27.09.2019	USTUTT, All Partners	New Evaluations updates on Artefacts
0.7	25.10.2019	USTUTT, All partners	Updates on Evaluations
0.8	11.11.2019	USTUTT	Review and Final Updates
0,9	12.11.2019	USTUTT	Updates Pilot evaluations,
0.95	21.11.2019	USTUTT/All	Insert Reviewers comments and remarks, update last drafts
1.0	26.11.2019	USTUTT	Finalize Document

2.3 Table of Figures

2.4 Table of Contents

3. Introduction

This deliverable looks to explore what basic high-level requirements are needed for LIGHTest. These high-level requirements are guidelines regarding what aspects LIGHTest Should be aware of throughout the duration of the project. Further, this deliverable is the follow up to the Requirements and Use Case Deliverable D2.3 and D2.12 Evaluation (1). With that, all methodologies of requirements and the requirements themselves have been agreed upon in the first year of the project and accepted as high-level requirements.

As stated in D2.3 Requirements and Use Case deliverable (The LIGHTest Project, 2017) , a wide and diverse spectrum of high-level requirements for LIGHTest was established and included five 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 was explored in Deliverable 2.10. Regarding each category, there is an established structure and methodological reason that is tailored to the needs of each perspective. This varies from category to category as each disciplinary has a wide array of different methods and perspectives.

Further, each requirement was considered on three different artefacts; the Reference Architecture, Implementation, and the Pilot Level. The importance of establishing artefacts is to be aware that throughout the development process, that there are different guidelines for different stages. While observing a larger picture, the guidelines should be aware from the beginning even if they won't be initiated until later stages. For the Reference Architecture artefact, this is a more abstract and technical perspective of the processes of what the LIGHTest Infrastructure can achieve. This artefact was heavily reliant on deliverable 2.14, where the components and processes of the LIGHTest Reference Architecture was elaborated on. For the Implementation artefact, this regards a more concrete perspective of the different ways that the LIGHTest Reference Architecture is executed or used. For this, it has been decided to evaluate the LIGHTest Automatic Trust Verifier (ATV) tool for the implementation artefact. Further, the Pilots Artefact refer to high-level requirements that are specifically for the LIGHTest Pilots. The Pilots are the proof-of-concept use cases that are implemented within the duration of the project. They are very specific and implement in their own way the Reference Architecture.

Within this consideration, it was necessary to state the importance for each of these levels per requirements. Following the IETF terminology, each requirement states on each artefact level (The Reference Architecture, Implementation, and The Pilots) whether it is a 'MUST, MAY, SHOULD, or NOT APPLICABLE' requirement. Please find below in Table 1 a summary of the terminology. In addition, in the establishment of the requirements description in D2.3 may include the classification within the description text. This classification remains in the description text of the requirment, however, it is possible that the classification was adjusted depending on the artefact being evaluated, which is stated in each Classification of X Artefact. There are many

reasons for this simply since each artefact is unique and as the artefact becomes more specific the requirement itself may be either not applicable or another classification.

Table 1 IETF Classification Summary

Level of Importance	IETF Definition
MUST	This word, or the terms "REQUIRED" or "SHALL", mean that the Definition is an absolute requirement of the specification.
MAY	This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor May choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor May omit the same item. An implementation which does not include a particular option must be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option must be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the Option provides.)
SHOULD	This word, or the adjective "RECOMMENDED", mean that there May exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course

The structure for each requirements section are as followed. They go briefly over the methodology that was used for each set of requirements and then explains how they evaluated that set of requirements for the reference architecture artefact. With that, each evaluated requirement has a result; it is “Passed”, “Neutral”, “Not Passed”, or “Not Applicable”, and a remarks section. A requirement is Passed, if it already applies to the current status, or if it is possible to be applied in the future. A requirement is Neutral in the case we can’t detect the current status yet, Not Passed if it isn’t applied and can’t be applied in the future and Not Applicable is if the requirement is not applicable for the specific Artefact being evaluated. These definitions may have slight adaptations depending on which discipline category is being evaluated.

The second part of this two-part deliverable will follow the same structure when evaluating the last two artefacts, the Implementation and the Pilots.

The structure of this deliverable is the following: Section 4 focuses on the evaluation of the Functional Requirements; Section 5 regards the Privacy Requirements; Section 6 looks at the evaluation of Security and Accountability Requirements; Section 7 the Usability Requirements; Section 8 looks at the Economic Requirements evaluation, and then to conclude the deliverable there is a Conclusion in Section 9.

4. Functional Requirements Evaluation

The Functional Requirements were constructed in a fairly simple and organized manner. They were derived and built off of the guidelines and necessary functions of each component as defined in the Reference Architecture, D2.14. With that, the requirements are divided into sub-categories of their components. The considered components are the following; Trust Service Publication Authority, Trust Translation Authority, Delegation Publisher, Automated Trust Verifier, Individual Trust Policy, etc. The process was to go through each component and to find what requirements or basic high-level guidelines would be necessary to ensure that the overall LIGHTest Infrastructure would lead to a successful deployment, usage and general feasibility.

4.1 Requirements Evaluation

4.1.1 Implementation

Understanding functional requirements as the way in which a solution should behave and the specification of what is needed for its development, these requirements were defined in D2.3[1] taking into account those observable characteristics that any stakeholder affected wishes to be contained in the system. A stakeholder is an interested party affected by the project that is developed. For the definition of this set of requirements, was taken into account stakeholders affected only by functional aspects.

The functional requirements were evaluated in the frame of the concept of the reference architecture. As the reference architecture has had some changes and adaptations since the establishment of the requirements there are also some slight changes to the functional requirements for the reference architecture. These amendments are typically in regards to the processes of the Delegation Publisher and the use of DNSEC. Please find the updated requirements for the artefacts in this section (FR-3.00-FR-3.04) and the previous version of functional requirements in the D2.3 Requirements and Use Case deliverable.

FR-01.00	**Performance**
Description	LIGHTest SHOULD provide results in time relative to the complexity and amount of required information
Classification on Implementation	MUST
Result	**PASSED**

[1] D2.3 Requirements and Use Cases. Version 0.7, 07/04/2017.

Remarks	

FR-02.00	**A Single Generic Solution**
Description	In order for LIGHTest to be successful, there MUST be a single generic solution or alternative to what is already existing. This would be in the form of Qualified Signature, Authentication credentials/Identity Providers, Signed Software, FIDO device Attestation, etc.
Classification on Implementation	SHOULD
Result	**PASSED**
Remarks	

FR-03.00	**DP: Integrateable with DNSSEC**
Description	A Delegation Publisher MUST operate an off-the-shelf DNS Name Server with DNSSEC extension.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	Although the actual design does not use DNS entries for publication and discovery, it makes sense to have DNSSEC extensions on, to verify the correct server as the delegation provider.

FR-03.01	**DP: Trust List Flexibility**
Description	LIGHTest MUST be able to publish multiple delegations at a Delegation Publisher.
Classification on Implementation	MUST
Result	**PASSED**

Remarks	

FR-03.02	**DP: Utilities to load selected Delegation Data**
Description	The utilities parse and query input data and write or load equivalent delegations to the Delegation Provider.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-03.03	**DP: Interface**
Description	The Delegation publisher MUST provide an interface to create and edit delegations. The interface could either be GUI or an API.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-03.04	**DP: Multiple Formats**
Description	The delegation publisher MUST be able to publish delegations of different formats.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-04.00	**ATV: Verify Trust (1)**

Description	Automatic Trust Verifier MUST be able to take an Electronic Transaction and Trust Policy as input.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-04.01	**ATV: Verify Trust (2)**
Description	The ATV MUST provide outputs, if the Electronic Transaction is trustworthy [y/n] and optionally with explanation of its reasoning (in particular if not trustworthy). It uses a pluggable parser for Electronic Transactions as sub-component.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-04.02	**ATV: Verification Process Receipt**
Description	The Automatic Trust Verifier MUST provide receipt for every verification process
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-04.03	**ATV: Data Integrity**
Description	The Automatic Trust Verifier MUST verify the integrity of the data it uses in the trust verification process
Classification on Implementation	MUST

Result	**PASSED**
Remarks	

FR-05.00	**Applications for non-technical verifiers (1)**
Description	Provide an application for non-technical verifiers to easily understand and author individual trust policies.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-05.01	**Applications for non-technical verifiers (2)**
Description	Provide automatic means for verifiers to verify the trustworthiness of complex electronic transactions.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-06.00	**TSPA: Integrateable with DNSSEC**
Description	The Trust Scheme Publication Authority MUST be able to operate an off-the-shelf DNS Name Server with the DNSSEC extension
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-06.01	**TSPA: Trust List Flexibility**

Description	LIGHTest MUST be able to publish multiple Trust Lists under different sub-domains of the Authority domain name
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-06.02	**TSPA: Utilities to Load selected Trust Lists**
Description	The utilities parse selected Trust List formats MUST be able to be written or loaded into an equivalent DNS Zone files
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-07.00	**TTA: Integratable with DNSSEC**
Description	A Trust Translation Authority MUST operate a standard DNS Name Server with DNSSEC extension
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-07.01	**TTA: Trust Data Flexibility**
Description	A server publishes multiple Trust Lists under different sub-domains of the Authority's domain name
Classification on Implementation	MUST
Result	**PASSED**

Remarks	

FR-07.02	**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
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-07.03	**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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-07.04	**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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-07.05	**TTA: Uniform interface**

Description	The Trust Translation Publisher SHOULD provide a uniform interface user experience as the publication and delegation interfaces.
Classification on Implementation	SHOULD
Result	**NOT APPLICABLE**
Remarks	

FR-07.06	**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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-07.07	**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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-07.08	**TTA: Interface**
Description	The Trust Translation Authority MUST provide an interface, either GUI or API, to create and edit trust translation lists.
Classification on Implementation	MUST

Result	**PASSED**
Remarks	

FR-08.00	**Policy Authoring and Visualization Tools Use Acceptability**
Description	Policy Authoring and Visualization Tools MUST be an interactive software (e.g. one of several desktop/web applications) That makes it easy for non-technical users to visualize and edit a Trust Policy.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-09.00	**Individual Trust Policy**
Description	LIGHTest Trust Policy MUST provide formal instructions how to validate trustworthiness of a given type of a transaction. It always states which Trust Lists from which Authorities Should be used.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-09.01	**Individual Trust Policy: Flexibility**
Description	The LIGHTest Individual Trust Policy MUST be able to interpret LIGHTest Trust Policy Language
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-09.02	Individual Trust Policy: Interface
Description	The Policy authoring tool MUST have a user-friendly interface for non-technical use
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-09.03	Individual Trust Policy: Creation
Description	The Policy Authoring tool MUST be able to create and edit Trust policies
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-10.00	Global Trust Lists
Description	Develop the concept and infrastructure for global trust lists.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

FR-11.00	Mechanisms for Publication and Querying Trust Lists
Description	Provide the mechanisms for the publication and querying of trust lists with the same convenience that OCSP brings to revocation lists.
Classification on Implementation	MUST

Result	**PASSED**
Remarks	

FR-11.01	**Mechanisms for determining individual assurance levels**
Description	Provide a component to determine individual assurance levels that is easy to integrate in arbitrary applications and systems.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-11.02	**Mechanisms for translating foreign Trust Schemes**
Description	Provide the mechanisms to translate foreign trust schemes into the context of the local jurisdiction
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-11.03	**Mechanisms for publishing delegations/mandates and trust-related attributes**
Description	Provide the mechanisms to publish delegations/mandates and trust-related attributes for easy querying.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-11.04	**Mechanisms for Derived MobileIDs**
Description	Provide mechanisms to derive trusted mobile identities from other credentials such as government eIDs.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

FR-12.00	**Uniform Interface**
Description	The publishers for lists, translation, and delegation SHOULD provide a uniform interface user experience.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

4.1.2 Pilots

As stated already in section 4.1.1 for implementation, functional requirements are understood as the way in which a solution should behave and the specification of what is needed for its development. These requirements were defined in D2.3[2] taking into account those observable characteristics that any stakeholder affected wishes to be contained in the system.
As proof-of-concept use cases, the two pilots, Correos Pilot and UPRC Pilot, are implemented within the duration of the project. They are very specific and implement in their own way the Reference Architecture. This is very similar for any stakeholder affected by the project that is developed. This means that not all components of the Reference Architecture are required for each project. For example, in the UPRC Pilot there is currently no translation scenario implemented, but it can implemented in the future. And in in Correos Pilot there is currently no delegation scenario implemented, but it can implemented in the future. Therefore, also the set of requirements varies for each pilot. If a specific requirement is currently not fulfilled in a pilot but could be implemented and fulfilled in the future it is stated as neutral. In this section, for the definition of this set of requirements, was taken into account stakeholders affected only by

[2] D2.3 Requirements and Use Cases. Version 0.7, 07/04/2017.

functional aspects. Furthermore, for both pilots the functional requirements regarding the "internal" LIGHTest infrastructure (e.g. TSPA, TTA, DP), which is used by the pilots, are evaluated in the implementation analysis and not in the pilot evaluation. Therefore, these requirements (e.g. FR06.00 – FR07.06, or FR09.00-FR11.04 are evaluated as "not applicable" in this pilot analysis.

The functional requirements were evaluated in the frame of the concept of the reference architecture. As stated already in section 4.1.1 for implementation, the reference architecture has had some changes and adaptations since the establishment of the requirements there are also some slight changes to the functional requirements for the reference architecture. These amendments are typically in regards to the processes of the Delegation Publisher and the use of DNSEC. Please find the updated requirements for the artefacts in this section (FR-3.00-FR-3.04) and the previous version of functional requirements in the D2.3 Requirements and Use Case deliverable.

FR-01.00	**Performance**
Description	LIGHTest SHOULD provide results in time relative to the complexity and amount of required information
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

FR-02.00	**A Single Generic Solution**
Description	In order for LIGHTest to be successful, there MUST be a single generic solution or alternative to what is already existing. This would be in the form of Qualified Signature, Authentication credentials/Identity Providers, Signed Software, FIDO device Attestation, etc.

Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-03.00	**DP: Integrateable with DNSSEC**
Description	A Delegation Publisher MUST operate an off-the-shelf DNS Name Server with DNSSEC extension.
Classification on Pilots	MUST
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	In The Correos Pilot there is currently no delegation scenario implemented, but it can implemented in the future.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Although the actual design does not use DNS entries for publication and discovery, it makes sense to have DNSSEC extensions on, to verify the correct server as the delegation provider.

FR-03.01	**DP: Trust List Flexibility**

Description	LIGHTest MUST be able to publish multiple delegations at a Delegation Publisher.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-03.02	**DP: Utilities to load selected Delegation Data**
Description	The utilities parse and query input data and write or load equivalent delegations to the Delegation Provider.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	In The Correos Pilot there is currently no delegation scenario implemented, but it can implemented in the future.
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-03.03	**DP: Interface**
Description	The Delegation publisher MUST provide an interface to create and edit delegations. The interface could either be GUI or an API.

Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	In The Correos Pilot there is currently no delegation scenario implemented, but it can implemented in the future
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

FR-03.04	**DP: Multiple Formats**
Description	The delegation publisher MUST be able to publish delegations of different formats.
Classification on Pilots	SHOULD
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	In The Correos Pilot there is currently no delegation scenario implemented, but it can implemented in the future.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	

FR-04.00	**ATV: Verify Trust (1)**
Description	Automatic Trust Verifier MUST be able to take an Electronic Transaction and Trust Policy as input.
Classification on Pilots	MUST

Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

FR-04.01	**ATV: Verify Trust (2)**
Description	The ATV MUST provide outputs, if the Electronic Transaction is trustworthy [y/n] and optionally with explanation of its reasoning (in particular if not trustworthy). It uses a pluggable parser for Electronic Transactions as sub-component.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-04.02	**ATV: Verification Process Receipt**
Description	The Automatic Trust Verifier MUST provide receipt for every verification process
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**

Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

FR-04.03	**ATV: Data Integrity**
Description	The Automatic Trust Verifier MUST verify the integrity of the data it uses in the trust verification process
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

FR-05.00	**Applications for non-technical verifiers (1)**
Description	Provide an application for non-technical verifiers to easily understand and author individual trust policies.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	In The Correos Pilot trust policies are defined by Correos experts. There is currently no scenario having non-technical verifiers, but it can implemented in the future.

Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	

FR-05.01	**Applications for non-technical verifiers (2)**
Description	Provide automatic means for verifiers to verify the trustworthiness of complex electronic transactions.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

FR-06.00	**TSPA: Integrateable with DNSSEC**
Description	The Trust Scheme Publication Authority MUST be able to operate an off-the-shelf DNS Name Server with the DNSSEC extension
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**

Comments for The UPRC Pilot	

FR-06.01	**TSPA: Trust List Flexibility**
Description	LIGHTest MUST be able to publish multiple Trust Lists under different sub-domains of the Authority domain name
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-06.02	**TSPA: Utilities to Load selected Trust Lists**
Description	The utilities parse selected Trust List formats MUST be able to be written or loaded into an equivalent DNS Zone files
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-07.00	TTA: Integratable with DNSSEC
Description	A Trust Translation Authority MUST operate a standard DNS Name Server with DNSSEC extension
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-07.01	TTA: Trust Data Flexibility
Description	A server publishes multiple Trust Lists under different sub-domains of the Authority's domain name
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-07.02	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
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-07.03	**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.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-07.04	**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.

Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-07.05	**TTA: Uniform interface**
Description	The Trust Translation Publisher SHOULD provide a uniform interface user experience as the publication and delegation interfaces.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-07.06	**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.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No

Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-07.07	**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.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	TTA is implemented. However “only” trust translation lists for boolean, and ordinal formats are accepeted currently; tuple-based format can be added in the future
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-07.08	**TTA: Interface**
Description	The Trust Translation Authority MUST provide an interface, either GUI or API, to create and edit trust translation lists.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**NEUTRAL**

Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	In The UPRC Pilot there is currently no translation scenario implemented, but it can implemented in the future.

FR-08.00	**Policy Authoring and Visualization Tools Use Acceptability**
Description	Policy Authoring and Visualization Tools MUST be an interactive software (e.g. one of several desktop/web applications) That makes it easy for non-technical users to visualize and edit a Trust Policy.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	In The Correos Pilot trust policies are defined by Correos experts. There is currently no scenario having non-technical verifiers, but it can implemented in the future.
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-09.00	**Individual Trust Policy**
Description	LIGHTest Trust Policy MUST provide formal instructions how to validate trustworthiness of a given type of a transaction. It always states which Trust Lists from which Authorities Should be used.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**

Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-09.01	**Individual Trust Policy: Flexibility**
Description	The LIGHTest Individual Trust Policy MUST be able to interpret LIGHTest Trust Policy Language
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-09.02	**Individual Trust Policy: Interface**
Description	The Policy authoring tool MUST have a user-friendly interface for non-technical use
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**

Comments for The UPRC Pilot	

FR-09.03	**Individual Trust Policy: Creation**
Description	The Policy Authoring tool MUST be able to create and edit Trust policies
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-10.00	**Global Trust Lists**
Description	Develop the concept and infrastructure for global trust lists.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-11.00	Mechanisms for Publication and Querying Trust Lists
Description	Provide the mechanisms for the publication and querying of trust lists with the same convenience that OCSP brings to revocation lists.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-11.01	Mechanisms for determining individual assurance levels
Description	Provide a component to determine individual assurance levels that is easy to integrate in arbitrary applications and systems.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-11.02	Mechanisms for translating foreign Trust Schemes

Description	Provide the mechanisms to translate foreign trust schemes into the context of the local jurisdiction
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-11.03	**Mechanisms for publishing delegations/mandates and trust-related attributes**
Description	Provide the mechanisms to publish delegations/mandates and trust-related attributes for easy querying.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-11.04	**Mechanisms for Derived MobileIDs**
Description	Provide mechanisms to derive trusted mobile identities from other credentials such as government eIDs.

Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

FR-12.00	**Uniform Interface**
Description	The publishers for lists, translation, and delegation SHOULD provide a uniform interface user experience.
Classification on Pilots	SHOULD
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

5. Privacy Requirements

As stated in the previous deliverable (D 2.12), the methodology followed to analyze the privacy requirements is based on the principles set out in the EU General Data Protection Regulation.

Although in LIGHT^{est} there is no collection/storing of personal data per se, and any processing of personal data is limited to specific cases in the delegation domain, during the collection of the requirements, we focused on a minimum set that can reliably cover these special cases.

The privacy requirements should influence the conceptual design during the definition of reference architecture phase (already done) and the subsequent implementation and the specific application contexts of the pilots.

In this second phase of the evaluation, after reviewing the architecture, components, use cases and identify the requirements, we need to continue with the implementation and pilots' scenarios.

In this regard, the assumption made during the evaluation of the architecture artefact (D2.12) is still valid and needed to be highlighted again, that all information provided in the trust lists, trust translation lists, and delegation lists are already compliant with GDPR, meaning they either do not contain any personal information at all or that personal information is present for purposes that are GDPR-legitimate.

5.1 Requirements Evaluation

5.1.1 Implementation

Technically speaking, during the codification of the components of LIGHT^{est}, there is no feasible way to detect or prevent inappropriate use of the trust services as a programming language cannot prevent one to write illegal or unethical programs. It is barely impossible to detect during the implementation phase, there will be personal information stored in the trust lists.

During this step, we assumed the trust lists and trust translation lists will not contain any sensible data as they will contain information related to trust schemes and levels of those trust schemes. For the delegation lists it may occur a name of a delegate (as a natural person) appears publicly, and this can be privacy relevant, but this case is considered in GDPR.

The ATV will in general work on a transaction that contains more information, and for avoiding any privacy issues on the side of the ATV, we make again explicitly the following requirements as in the D2.12. This creates duplication in the content of both deliverables, but also ensures that this section can be read and understood as standalone:

1. The ATV MUST not store of information except for caching of information obtained from DNS-Servers and trust lists, trust translation lists or trust delegation lists. Rather, the ATV is a program that evaluates whether an electronic transaction satisfies a policy and returns the result of this evaluation with a detailed transcript.

2. The user of the ATV is who decides what to do with the result that the ATV returns if they decide to keep it, it is their responsibility to defend whether this is correct with regards to GDPR.
3. During the evaluation of the ATV implementation it will be checked that the ATV complies with the first point, in terms of not storing information other than caching of certificate information from trust (translation) lists. Also we will check that the ATV does not make any communication other than lookups of certificates, trust schemes, trust translation schemes and delegation schemes according to the policy that it is evaluating.

The classification of the privacy requirements was done based on the aforementioned explanations and taking into account the previous classification of the architecture artefact, as the classifications should keep consistency along the life-cycle of the project. Requirements labelled as MUST have to be implemented and its implementation verified, giving the LIGHT^{est} platform the needed tools for applying adequate security measures and providing an assessment framework for the pilots that will use the LIGHT^{est} infrastructure. In case of “SHOULD”, those are requirements that focus on communicating an important issue to the developers in order to achieve privacy protection goals, but it is undefined the way to do so in the form of a verifiable requirement. We mark as "Assumption" in the remarks all those requirements that are satisfied due to the assumptions denote above.

No.	**PR-01.00- Privacy by design**
Description	The LIGHT^{est} project MUST protect any personal data it collects or processes according to the definition of personal data in the GDPR and any data controllers of such personal data within LIGHT^{est} MUST, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, which are designed to implement data-protection principles in an effective manner, and to integrate the necessary safeguards into the processing in order to meet the requirements of GDPR and protect the rights of data subjects.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption (see section **Fehler! Verweisquelle konnte nicht gefunden werden.**)

No.	**PR-01.01- No revocable privacy**
Description	Actors MUST NOT be subject to any mechanism that revokes their privacy. This includes backdoors, key-escrow or similar concepts that ultimately places control of an actor in the hands of a third party.

Classification on Implementation	MUST NOT
Result	**PASSED**
Remarks	There are no such escrow techniques implemented.

No.	**PR-02.00- Privacy by default**
Description	Any personal data Controller within LIGHTest boundaries MUST implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption

No.	**PR-02.01- Privacy-friendly settings**
Description	All preferences, configuration, and other settings, SHOULD use the most privacy-friendly settings as the default settings, where technically feasible in a compatible way with the use of existing DNSSEC technology. Changes from the defaults and their implications on users' privacy SHOULD be both clearly documented and conveyed to the actor making the change.
Classification on Implementation	SHOULD
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption

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.
Classification on Implementation	MUST
Result	**NOT APPLICABLE**
Remarks	It is not applicable on this level but on pilot level.

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.
Classification on Implementation	SHOULD
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption

No.	**PR-03.02- Purpose limitation (sensitivity)**
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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by Assumption

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
Classification on Implementation	MUST
Result	**PASSED**
Remarks	By assumption and research on accountability

No.	**PR-04.01- Minimal registration data**
Description	Data required to use the LIGHTest services by any actor SHOULD NOT include any identifiable data, and any identifier SHOULD be randomly generated.
Classification on Implementation	SHOULD
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption

No.	**PR-04.02- Limited storage time**
Description	Any personal data collected MUST be kept in a form which permits identification of the owner for no longer than is necessary for the purposes for which the personal data are processed; personal data May be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of GDPR subject to implementation of the appropriate technical and organizational measures required by GDPR in order to safeguard the rights and freedoms of the data subject.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption and research on accountability

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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption and research on accountability

No.	**PR-05.01- Owner explicit delegation**
Description	When a delegation process is implemented, actors MUST explicitly be involved in it.
Classification on Implementation	MUST
Result	**NEUTRAL**
Remarks	A delegation can only take place if the delegator chooses to perform a delegation; however, the delegate is not necessarily involved as an active participant in the delegation process (i.e. agreeing to be delegate). However, the delegate will be notified of the delegation, and this seems completely sufficient.

No.	**PR-05.02- Limited re-delegation**
Description	Delegations SHOULD NOT be delegable in turn, unless strictly required by the nature of the service provided and with the consent of the original actor.
Classification on Implementation	SHOULD NOT
Result	**PASSED**
Remarks	In fact, chains of delegations are currently possible, even though limited. In practice it seems often reasonable to have some limited form of re-delegation (e.g., following the hierarchy in a company), so we may choose to allow it despite this privacy goal,

	so that PR-05.02 would not be fulfilled. Also, it is of course possible to simply forbid re-delegation as part of a trust delegation policy.

No.	**PR-05.03- Transparent delegation overlap**
Description	When being informed about a delegation request, actors SHOULD explicitly be warned, if applicable, if any part of the LIGHTest pilot that the delegation requests concern, is already the subject of delegation.
Classification on Implementation	SHOULD
Result	**NOT APPLICABLE**
Remarks	It is not applicable on this level but on pilot level.

No.	**PR-05.04- Transparency towards actors**
Description	All outcomes of authentication, authorization, delegation, and identity and attribute management processes MUST be visible (transparent) for the relevant actor whose electronic transaction is being processed.
Classification on Implementation	MUST
Result	**NOT APPLICABLE**
Remarks	It is not applicable on this level but on pilot level.

No.	**PR-05.05- Notification**
Description	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.
Classification on Implementation	MUST

Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption

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.
Classification on Implementation	MUST
Result	**NOT APPLICABLE**
Remarks	As the requirement stated, this is applicable on pilot level.

No.	**PR-06.01- Right to be forgotten**
Description	If any personal data are collected, the owner MUST have the right to obtain from the Data Controller the erasure of personal data concerning her/him without undue delay and the Data Controller MUST have the obligation to erase personal data without undue delay, if any of the grounds from Article 17 of GDPR applies.
Classification on Implementation	MUST
Result	**NOT APPLICABLE**
Remarks	It is not applicable on this level but on pilot level.

No.	**PR-06.02- Right to restriction of processing**
Description	The owner MUST have the right to obtain from the Data Controller the restriction of the processing of personal data, if any of the grounds from Article 18 of GDPR applies.
Classification on Implementation	MUST
Result	**PASSED**

Remarks	Tools implemented to fulfill the requirement entirely

No.	**PR-06.03- Right to object**
Description	The Data Subject MUST have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1) of GDPR, including profiling based on those provisions. The Data Controller MUST no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	Tools implemented to fulfill the requirement entirely

No.	**PR-06.04- Right to data portability**
Description	The Data Subject SHOULD have the right to receive the personal data concerning him or her, which he or she has provided to a Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided, where the conditions specified in Article 20 of GDPR are met.
Classification on Implementation	SHOULD
Result	**NOT APPLICABLE**
Remarks	It is not under LIGHTest´s implementation scope

No.	**PR-07.00- Accuracy**
Description	Any personal data collected MUST be accurate and, where necessary, kept up to date; every reasonable step MUST be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, will be erased or rectified without delay.

Classification on Implementation	MUST
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption and research on accountability

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.
Classification on Implementation	MUST
Result	**NOT APPLICABLE**
Remarks	Generally, LIGHTest components themselves should not store information, so this requirement should normally not apply (see the assumptions in Section **Fehler! Verweisquelle konnte nicht gefunden werden.**).

No.	**PR-09.00- Integrity and confidentiality**
Description	Any personal data collected MUST be processed in a way that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage; the Data Controller MUST implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, and when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller MUST communicate the personal data breach to the Data Subject without undue delay.
Classification on Implementation	MUST
Result	**NOT APPLICABLE**
Remarks	It is not applicable on this level of implementation but on pilot level during the deployment phase.

No.	PR-09.01- Anonymization for statistics
Description	Data SHOULD be anonymized, if applicable, and gathered together in order to be processed for statistical analysis
Classification on Implementation	SHOULD
Result	**PASSED**
Remarks	Tools implemented to fulfill the requirement entirely

No.	PR-09.02- Key privacy
Description	If a public-key encryption scheme is implemented, it SHOULD provide key privacy if applicable. Key privacy is a security property of public-key encryption algorithms that requires that ciphertexts produced by an encryption algorithm do not leak any information about which public key was used to produce the ciphertext.
Classification on Implementation	SHOULD
Result	**NOT APPLICABLE**
Remarks	No need to fulfill this requirement as there is no public-key encryption scheme implemented.

No.	PR-09.03- Private process outcomes
Description	Information on all process outcomes SHOULD NOT be available to anyone else, unless required by the nature of the service provided and with the consent of the original actor.
Classification on Implementation	SHOULD NOT
Result	**NOT APPLICABLE**
Remarks	It is not applicable on this level but on pilot level.

No.	PR-09.04- Private metadata
Description	The metadata used to reference encrypted data stored in the LIGHT^{est} pilots SHOULD NOT reveal information regarding the actors.

Classification on Implementation	SHOULD NOT
Result	**NOT APPLICABLE**
Remarks	No need to fulfill this requirement as there is no encryption of data implemented in the LIGHTest component.

No.	**PR-09.05- Private policies**
Description	Authorization and delegation policies/preferences stored in LIGHTest SHOULD NOT reveal information regarding the actors.
Classification on Implementation	SHOULD NOT
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption

No.	**PR-10.00- International Personal Data Transfer**
Description	The Data Controller MUST provide information in the event of a personal data transfer to third countries or international organizations, taking into account that a transfer to “a third country or an international organization May take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection.” (EU Data Protection Article 45)
Classification on Implementation	MUST
Result	**PASSED**
Remarks	This requirement is fulfilled entirely by assumption.

No.	**PR-47.00- Data Economy**
Description	LIGHTest SHOULD store as few data as possible
Classification on Implementation	SHOULD

Result	**PASSED**
Remarks	Requirement fulfilled entirely during implementation as the number of data structures was minimized.

5.1.1 Pilots

When using the LIGHT^{est} infrastructure in live environment, operational measures applied play a more important role than the design or implementation specifications and proper procedures for meeting specifically privacy demands have to put in place when the deployment is being performed.

Therefore, it is needed to make some assumptions on the way LIGHT^{est} is rolled out on the pilots 'scenarios, with respect to privacy requirements, meaning it is being deployed in a context where GDPR and related regulations are already respected, and we can give the guarantee that LIGHT^{est} will not introduce any GDPR problems. These are almost the same assumptions made during the implementation steps but adapted to the two different scenarios of the pilots.

The classification of the privacy requirements in the demonstrators´ scenario have been assigned analyzing the impact of the privacy principles on the personal data transferred or managed among the different components involved in the execution of the pilot. We focused on another important aspect of privacy, in addition to data minimization, the possibility for users of LIGHT^{est} to be in control of their data at any time. This implies a sufficient understanding of the data processing procedures during the life-cycle of the pilots and in particular of the privacy risks and how to react upon them, even assuming LIGHT^{est} is not really concerned with any privacy problems, since, as explained before, trust lists are essentially public information and that not contain any personal data.

The need to take into account the previous classification during implementation is obvious but not strictly the same. Actually, requirements classified as "MAY" are optional, i.e., they are desirable but not necessary and could be applicable for improving the privacy preserving principles but some of them are marked as MUST in implementation step. As in the previous step, requirements marked with "Assumption" in the remarks are all those requirements that are satisfied due to the assumptions denote above (see Section **Fehler! Verweisquelle konnte nicht gefunden werden.**)

No.	**PR-01.00- Privacy by design**
Description	The LIGHT^{est} project MUST protect any personal data it collects or processes according to the definition of personal data in the GDPR and any data controllers of such personal data within LIGHT^{est} MUST, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, which are designed to implement data-protection principles in an

	effective manner, and to integrate the necessary safeguards into the processing in order to meet the requirements of GDPR and protect the rights of data subjects.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption (see section **Fehler! Verweisquelle konnte nicht gefunden werden.**)
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This requirement is fulfilled entirely by assumption (see section **Fehler! Verweisquelle konnte nicht gefunden werden.**)

No.	**PR-01.01- No revocable privacy**
Description	Actors MUST NOT be subject to any mechanism that revokes their privacy. This includes backdoors, key-escrow or similar concepts that ultimately places control of an actor in the hands of a third party.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	There are no such escrow techniques implemented.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	There are no such escrow techniques implemented.

No.	**PR-02.00- Privacy by default**
Description	Any personal data Controller within LIGHTest boundaries MUST implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes

Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This requirement is fulfilled entirely by assumption.

No.	**PR-02.01- Privacy-friendly settings**
Description	All preferences, configuration, and other settings, SHOULD use the most privacy-friendly settings as the default settings, where technically feasible in a compatible way with the use of existing DNSSEC technology. Changes from the defaults and their implications on users' privacy SHOULD be both clearly documented and conveyed to the actor making the change.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This requirement is fulfilled entirely by assumption.

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.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil entirely this requirement.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil entirely this requirement.

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.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This requirement is fulfilled entirely by assumption.

No.	PR-03.02- Purpose limitation (sensitivity)
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.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This requirement is fulfilled entirely by assumption.

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

Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption and research on accountability
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This requirement is fulfilled entirely by assumption and research on accountability

No.	**PR-04.01- Minimal registration data**
Description	Data required to use the LIGHTest services by any actor SHOULD NOT include any identifiable data, and any identifier SHOULD be randomly generated.
Classification on Pilot	SHOULD
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This requirement is fulfilled entirely by assumption

No.	**PR-04.02- Limited storage time**
Description	Any personal data collected MUST be kept in a form which permits identification of the owner for no longer than is necessary for the purposes for which the personal data are processed; personal data May be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of GDPR subject to implementation of the appropriate technical and organizational measures required by GDPR in order to safeguard the rights and freedoms of the data subject.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**

Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption and research on accountability
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This requirement is fulfilled entirely by assumption and research on accountability

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.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	During the pilots, the system users will be informed about their rights according to GDPR
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	During the pilots, the users will be informed about their rights according to GDPR

No.	**PR-05.01- Owner explicit delegation**
Description	When a delegation process is implemented, actors MUST explicitly be involved in it.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	The system is designed for fulfilling the requirement in the future but it is not fully fulfilled now.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**

Comments for The UPRC Pilot	A delegation can only take place if the delegator chooses to perform a delegation; however the delegate is not necessarily involved as an active participant in the delegation process (i.e. agreeing to be delegate). However, the delegate will be notified of the delegation, and this seems completely sufficient.

No.	**PR-05.02- Limited re-delegation**
Description	Delegations SHOULD NOT be delegable in turn, unless strictly required by the nature of the service provided and with the consent of the original actor.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	The system is designed for fulfilling the requirement in the future but it is not fully fulfilled now.
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	There will be no re-delegation during the execution of this pilot

No.	**PR-05.03- Transparent delegation overlap**
Description	When being informed about a delegation request, actors SHOULD explicitly be warned, if applicable, if any part of the LIGHTest pilot that the delegation requests concern, is already the subject of delegation.
Classification on Pilot	SHOULD
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	The system is designed for fulfilling the requirement in the future but it is not fully fulfilled now.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

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

Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption and research on accountability
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	The system is designed for fulfilling the requirement in the future but it is not fully fulfilled now.

No.	**PR-05.05- Notification**
Description	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.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption and research on accountability
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	The system is designed for fulfilling the requirement in the future but it is not fully fulfilled now.

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.
Classification on Pilot	MUST

Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil the requirement entirely

No.	**PR-06.01- Right to be forgotten**
Description	If any personal data are collected, the owner MUST have the right to obtain from the Data Controller the erasure of personal data concerning her/him without undue delay and the Data Controller MUST have the obligation to erase personal data without undue delay, if any of the grounds from Article 17 of GDPR applies.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil the requirement entirely

No.	**PR-06.02- Right to restriction of processing**
Description	The owner MUST have the right to obtain from the Data Controller the restriction of the processing of personal data, if any of the grounds from Article 18 of GDPR applies.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil the requirement entirely

No.	**PR-06.03- Right to object**

Description	The Data Subject MUST have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1) of GDPR, including profiling based on those provisions. The Data Controller MUST no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil the requirement entirely

No.	**PR-06.04- Right to data portability**
Description	The Data Subject SHOULD have the right to receive the personal data concerning him or her, which he or she has provided to a Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided, where the conditions specified in Article 20 of GDPR are met.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil the requirement entirely

No.	**PR-07.00- Accuracy**
Description	Any personal data collected MUST be accurate and, where necessary, kept up to date; every reasonable step MUST be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, will be erased or rectified without delay.

Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption and research on accountability
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This requirement is fulfilled entirely by assumption and research on accountability

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.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil the requirement entirely

No.	**PR-09.00- Integrity and confidentiality**
Description	Any personal data collected MUST be processed in a way that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage; the Data Controller MUST implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, and when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller MUST communicate the personal data breach to the Data Subject without undue delay.
Classification on Pilot	MAY

Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil the requirement entirely

No.	**PR-09.01- Anonymization for statistics**
Description	Data SHOULD be anonymized, if applicable, and gathered together in order to be processed for statistical analysis
Classification on Pilot	SHOULD
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	This requirement cannot be applicable in this scenario

No.	**PR-09.02- Key privacy**
Description	If a public-key encryption scheme is implemented, it SHOULD provide key privacy if applicable. Key privacy is a security property of public-key encryption algorithms that requires that cipher texts produced by an encryption algorithm do not leak any information about which public key was used to produce the cipher text.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil the requirement entirely

No.	**PR-09.03- Private process outcomes**

Description	Information on all process outcomes SHOULD NOT be available to anyone else, unless required by the nature of the service provided and with the consent of the original actor.
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil the requirement entirely

No.	**PR-09.04- Private metadata**
Description	The metadata used to reference encrypted data stored in the LIGHTest pilots SHOULD NOT reveal information regarding the actors.
Classification on Pilot	SHOULD NOT
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	This requirement cannot be applicable in this scenario

No.	**PR-09.05- Private policies**
Description	Authorization and delegation policies/preferences stored in LIGHTest SHOULD NOT reveal information regarding the actors.
Classification on Pilots	SHOULD NOT
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This requirement is fulfilled entirely by assumption
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	This requirement cannot be applicable in this scenario

No.	PR-10.00- International Personal Data Transfer
Description	The Data Controller MUST provide information in the event of a personal data transfer to third countries or international organizations, taking into account that a transfer to “a third country or an international organization May take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection.” (EU Data Protection Article 45)
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	The system is designed for fulfilling the requirement in the future but it is not fully fulfilled now.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This requirement is fulfilled entirely by assumption

No.	PR-47.00- Data Economy
Description	LIGHTest SHOULD store as few data as possible
Classification on Pilot	MAY
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Tools implemented to fulfil the requirement entirely
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Tools implemented to fulfil the requirement entirely

6. Security and Accountability Requirements

Security as a term is one that for many has some intuitive meaning, but for which there is no specific meaning that everyone agrees on. Therefore, when dealing with computer security in practice, it is customary to define a number of separate goals that define the intended meaning for a particular system. Then the system is said to be secure when the goals are satisfied. With this approach, the meaning of "secure" is made specific; but there is also an added advantage, which is the usual advantage of dividing a task into multiple distinct steps that can be completed independently.

The process of deriving the security and accountability requirements (SAR) is based on this approach. Instead of goals, we define five security principles from which the SAR Should follow:

Title	Description
Channels	The LIGHT^{est} components MUST use the best (most secure) channels that are technically feasible and not violating privacy goals. These channels SHOULD include protection against man-in-the middle, replay, reflection and similar protocol level attacks. This SHOULD be achieved by using protocols like TLS, DNSSEC, and DANE.
Inter-component communication	When components communicate with each other, this is either on the same physical system or virtualized. The principle of virtualization is that by crypto it Should be ensured to be equivalent to the setup on the same machine except for failures of the communication medium (-> that is an issue of availability).
Storage	Storage of data MUST be minimal -- i.e. there is a clearly documented need -- and it MUST be protected against unauthorized reading, writing, and loss/destruction. Any backups MUST adhere to these protections, and the amount of backups, if any, MUST be explicitly assessed.
Availability	Protection against classical denial of service attacks SHOULD be achieved to the level provided -- without opening additional vulnerabilities -- by protocols like TLS, DNSSEC, and DANE. Resource access limitations MUST be implemented to protect against workload problems. An analysis for robustness SHOULD be provided in the style of the Quality Calculus.
Accountability	Any LIGHT^{est} component that makes decisions (trust decisions, issuing certificates) MUST be able to defend such decisions by presenting all the artifacts (like certificates) on the basis of which the decision was made. When data storage is necessary to achieve this, it MUST adhere to the general requirements for storage.

The principles can be thought of as requirements on their own, as each is accompanied by a concise description of what is required for the topic addressed. At the same time these principles partition the SAR. So all the following SAR requirements can be thought of specializations/concretizations of one or more of these principles. In this way, the principles provide a succinct, high-level description of what the larger body of requirements should express, while the sub-requirements express details on a low-level.

This makes for an effective tool in designing a requirement set because the process of separating the sub-requirements categories, forces the sub-requirements to match with the principles; or, in other words, it forces the low-level details to match with the high-level intuition. When a sub-requirement does not fit, it could mean that the overall vision is wrong and that the principles Should be adjusted; or it could mean that the sub-requirement Should be dropped, because it does not match the overall vision. It is also possible that a sub-requirement fits with multiple principles. This can be because the requirement is too incoherent and needs to be refined or split up; or it can be because the principles overlap, in which case they Should be adjusted.

Another advantage of dividing requirements into categories like this is that it makes it apparent when some area or topic has received too little attention. In that case, there Should be too few or too weak sub-requirements for one particular principle. This is an important mechanism because it leads to strengthening the design by adding more content, which – together with the other mechanisms that tend to trim it – leads to a feedback loop.

This methodology is applied here because it is well suited to a dynamic design process. Whenever the design is changed – be it on a very specific level, like the addition of a new requirement, or on a higher level – it is much easier to check if the change is coherent with the rest of the design. More importantly, this methodology is applied because it is particularly well suited to security, being an inherently divisible notion.

Security as a term is one that for many has some intuitive meaning, but for which there is no specific meaning that everyone agrees on. Therefore, when dealing with computer security in practice, it is customary to define a number of separate goals that define the intended meaning for a particular system. Then the system is said to be secure when the goals are satisfied. With this approach, the meaning of "secure" is made specific; but there is also an added advantage, which is the usual advantage of dividing a task into multiple distinct steps that can be completed independently.

The process of deriving the security and accountability requirements (SAR) is based on this approach. Instead of goals, we define five security principles from which the SAR Should follow:

Title	Description

Channels	The LIGHT^{est} components MUST use the best (most secure) channels that are technically feasible and not violating privacy goals. These channels SHOULD include protection against man-in-the middle, replay, reflection and similar protocol level attacks. This SHOULD be achieved by using protocols like TLS, DNSSEC, and DANE.
Inter-component communication	When components communicate with each other, this is either on the same physical system or virtualized. The principle of virtualization is that by crypto it Should be ensured to be equivalent to the setup on the same machine except for failures of the communication medium (-> that is an issue of availability).
Storage	Storage of data MUST be minimal -- i.e. there is a clearly documented need -- and it MUST be protected against unauthorized reading, writing, and loss/destruction. Any backups MUST adhere to these protections, and the amount of backups, if any, MUST be explicitly assessed.
Availability	Protection against classical denial of service attacks SHOULD be achieved to the level provided -- without opening additional vulnerabilities -- by protocols like TLS, DNSSEC, and DANE. Resource access limitations MUST be implemented to protect against workload problems. An analysis for robustness SHOULD be provided in the style of the Quality Calculus.
Accountability	Any LIGHT^{est} component that makes decisions (trust decisions, issuing certificates) MUST be able to defend such decisions by presenting all the artifacts (like certificates) on the basis of which the decision was made. When data storage is necessary to achieve this, it MUST adhere to the general requirements for storage.

The principles can be thought of as requirements on their own, as each is accompanied by a concise description of what is required for the topic addressed. At the same time these principles partition the SAR. So all the following SAR requirements can be thought of specializations/concretizations of one or more of these principles. In this way, the principles provide a succinct, high-level description of what the larger body of requirements Should express, while the sub-requirements express details on a low-level.

This makes for an effective tool in designing a requirement set because the process of separating the sub-requirements categories, forces the sub-requirements to match with the principles; or, in other words, it forces the low-level details to match with the high-level intuition. When a sub-requirement does not fit, it could mean that the overall vision is wrong and that the principles Should be adjusted; or it could mean that the sub-requirement Should be dropped, because it does not match the overall vision. It is also possible that a sub-requirement fits with multiple principles. This can be because the requirement is too incoherent and needs to be

refined or split up; or it can be because the principles overlap, in which case they Should be adjusted.

Another advantage of dividing requirements into categories like this is that it makes it apparent when some area or topic has received too little attention. In that case, there Should be too few or too weak sub-requirements for one particular principle. This is an important mechanism because it leads to strengthening the design by adding more content, which – together with the other mechanisms that tend to trim it – leads to a feedback loop.

This methodology is applied here because it is well suited to a dynamic design process. Whenever the design is changed – be it on a very specific level, like the addition of a new requirement, or on a higher level – it is much easier to check if the change is coherent with the rest of the design. More importantly, this methodology is applied because it is particularly well suited to security, being an inherently divisible notion.

6.1 Requirements Evaluation

6.1.1 Implementation

Security is classically defined as consisting of Confidentiality (or Secrecy), Integrity (including Authentication/Agreement) and Availability (absence of Denial of Service and the like). In particular Integrity, i.e., the reliability of data, is the most crucial goal for any trust infrastructure: if it were possible for any attacker to manipulate any data relevant to the processing of trust policies, all trust guarantees are in question. For this very reason, there is a particular focus on integrity and authentication that goes far beyond a "simple" security evaluation. Related to this are in particular questions of (formal) accountability, i.e., that we can produce proofs of correct decisions that can be later verified by a third party, e.g., in a legal dispute. Since achieving these security properties is a particular focus of the project, we label them with "Focus" below in the comments. For the implementation it is in particular important that it satisfies these requirements and so an in depth evaluation has been carried out. As a result of this evaluation we can conclude that the implementation indeed satisfies these requirements.

The architecture evaluation deliverable (D2.12) described the possibility of using formal verification to support some of the security and accountability concepts. The concepts of accountability and the integrity of trust decisions are now supported by formal verification: The ATV can for a positive trust decision produce a special transcript that encodes the given policy, query and the interactions with servers etc. A separate and formally verified tool, RPx, can then independently check that the positive decision was correct. Another important aspect for the evaluation is the compositionality aspect that the DTU partner is focusing on: that we can design, reason about, test, and verify components in isolation so that their composition to a large system does not break. This is in particular crucial to ensure that one dishonest (i.e., untrustworthy) participant cannot destroy the trust in the whole system. Thus, when one component fails (not only in terms of function but also security and trust), the impact on other components should be minimal if any. Also much of this aspect is current research at DTU and we simply label this as "Compositionality" in the remarks as goals where the architecture haslaid some ground work.

In the following we mark a requirement as “PASSED” if the implementation fully fulfills the requirement. If the implementation currently does not fulfill the requirement but it is possible that it might fulfill it in the future then the requirement is marked as “Neutral”. Finally, if the implementation does not fulfill the requirement then the requirement is marked “NOT PASSED”. Whenever we have an additional remark on how our decision was made then we have justified the decision in the Remark field.

Compared to the evaluation at the architecture level, some requirements got new classifications on the implementation level. The reason for these changes is for the most part that some requirements were not applicable at the architecture level---and so they were previously classified as “NOT APPLICABLE”---whereas they are applicable on the implementation level. Note, however, that some requirements are only applicable on the pilot level, and so for these requirements the result on the implementation level is “Not Applicable”.

No.	**SAR-01.00- Channels**
Description	The LIGHTest components MUST use the best (most secure) channels that are technically feasible and not violating privacy goals. These channels SHOULD include protection against man-in-the middle, replay, reflection and similar protocol level attacks. This SHOULD be achieved by using protocols like TLS, DNSSEC, and DANE.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	We have discovered that this requirement is a bit stronger than intended. In particular, it is often feasible that endpoints authenticate themselves where that authentication is Not Applicable for security, e.g., when querying a server for public information, it is not necessary that the client authenticates itself. If authentication would not be in conflict with any privacy goals, then a lack of authentication would strictly speaking violate this requirement.

No.	**SAR-01.01- Confidentiality: Secure Channel**
Description	(Confidentiality – Secure Channel) Lightest Services MUST communicate on secure channel in order to protect channel data from eavesdropping
Classification on Implementation	MUST
Result	**NOT PASSED**
Remarks	The lookups by the ATV on trust list servers are by default not encrypted, e.g., with TLS, even though that would be technically possible. Using an unencrypted connection bears the risk of an eavesdropper to monitor what trust list entries a party is looking

	up. We consider the privacy risk, however, quite low. It was therefore a deliberate design decision not to insist on TLS channels, and thus violate this requirement.

No.	**SAR-01.02- Confidentiality: Data Protection**
Description	Lightest services MUST maintain the confidentiality of the data subject to protection that are sent between components.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	This is actually indirectly achieved, see the evaluation on the privacy goals. Actually, there is a minor leak of data protection: an attacker observing the traffic between an ATV and trust list servers can observe who is accessing which credentials. However this is the credential of a certificate provider, not of a participating party, so this is a very minor leakage.

No.	**SAR-01.03- Confidentiality: Session data protection**
Description	Lightest components MUST ensure that the any session data subject to protection (person-related data or session keys) are deleted after session finishes.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	According to our assumptions, LIGHTest components generally will not store data, but only processes them. However, for delegation providers and LIGHTest run-services (pilot level) this MUST be evaluated. However, the delegation provider store data that could be considered session data and person-related, but it is stored encrypted.

No.	**SAR-01.04- Confidentiality: Key Material/Credential Protection**
Description	Lightest services MUST enforce all key materials and credentials are held confidential at rest.
Classification on Implementation	MUST
Result	**NEUTRAL**
Remarks	According to our assumptions, LIGHTest components generally will not store data, but only processes them. However, for delegation providers and LIGHTest run-services (pilot level) this MUST be evaluated. The ATV does not use any private cryptographic material. The delegation provider and the ASIC creator do, but the user is responsible for how to store this (since the material is not created---just used---by the tools). The Zone Manager, however, has a private key for DNSSEC signing which is stored as is in a database with no precautions of any kind, and

	so does not fulfill this requirement yet, but this could be rectified in the future. For these reasons we have decided to mark it as "NEUTRAL".

No.	**SAR-01.05- Confidentiality: Replay Protection**
Description	Request and response messages MUST be replay protected and if a replay occurs Lightest components MUST be able to detect.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	Focus. Note that this requirement Should actually be labeled an authentication/integrity goal since replay/freshness are part of injective agreement, not secrecy.

No.	**SAR-01.06- Confidentiality**
Description	Any confidentiality issue that occurs in one Lightest component MUST not affect other Lightest components.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	Compositionality

No.	**SAR-01.07- Integrity: Data Integrity**
Description	All components of Lightest MUST protect the integrity of Data Subject's Personal Data, Audits, metadata and log files both in retention and processes (authentication, authorization, delegation, transporting, identity and attribute management). Only the authorized entities MUST be able to correct and remove the Personal Data with the condition of informing the Data Subject.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	Focus

No.	**SAR-01.08- Integrity: Error Handling**
Description	Lightest components MUST detect a data and system integrity error and take the necessary actions (E.g. closing current session, re-authentication, informing the Data Subject, informing concerned Member State(s)' supervisory body(ies) etc.) to prevent possible treats.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**

Remarks	

No.	**SAR-02.00- Inter-component communication**
Description	When components communicate with each other, this is either on the same physical system or virtualized. The principle of virtualization is that by crypto it SHOULD be ensured to be equivalent to the setup on the same machine except for failures of the communication medium (-> that is an issue of availability).
Classification on Implementation	SHOULD
Result	**NOT APPLICABLE**
Remarks	

No.	**SAR-02.01- Integrity: Component Relations**
Description	Lightest components MUST ensure that the breaking the integrity of one system component will not cause “single point of failure” that can lead to integrity failures in other components.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	Compositionality

No.	**SAR-02.02- Availability: Single Point of Failure**
Description	The LIGHTest system MUST not have, or have as minimal, single point of failures. The critical system nodes and bottleneck regions MUST have multiple instances that are supported by powerful load balancers.
Classification on Implementation	MUST NOT
Result	**NEUTRAL**
Remarks	The design actually allows for redundancy, but it is currently not part of the implementation. However, we give a "NEUTRAL" for this anyway since the DNS components are already designed to be very resilient infrastructure elements, and we can simply demand that other servers that host public information’s like trust lists to be implemented and deployed in the same way.

No.	**SAR-03.00- Storage**

Description	Storage of data MUST be minimal -- i.e. there is a clearly documented need -- and it MUST be protected against unauthorized reading, writing, and loss/destruction. Any backups MUST adhere to these protections, and the amount of backups, if any, MUST be explicitly assessed.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	This is actually now covered by the requirements we have made at the beginning of the privacy section, that the ATV does not store itself any transcript. Rather, the transcript is returned by the ATV and it is the responsibility of the organization running the ATV to decide what to do with the data (e.g. discard after a certain period of time) and to ensure that it is handled in a safe and GDPR-compliant way.

No.	**SAR-03.01- Logging and Auditing**
Description	The overall LIGHTest system MUST establish a logging and auditing infrastructure that is able to audit system and component failures, to detect suspicious system behavior and that can be used to trigger according alerts and countermeasures to maintain secure system functionality. The logging and auditing infrastructure MUST be in accordance with privacy regulations and requirements.
Classification on Implementation	MUST
Result	**NOT APPLICABLE**
Remarks	LIGHTest performs logging (in particular, the ATV), but in a transparent way as explained in the introduction of the privacy evaluation, i.e., the LIGHTest components produce a trace of what has happened that they don't retain but rather just return to the entity deploying the component. Therefore, the security, integrity, and privacy of these logging information's is the responsibility of the parties deploying LIGHTest. In particular, they have to comply with whatever regulations is applicable for their business and/or service contracts.

No.	**SAR-03.02- Logging and Auditing: Event association**
Description	For audit events resulting from actions of identified users, all LIGHTest backend components MUST be able to associate each event with the identity of the user that caused the event, in compliance with the LIGHTest privacy requirements.
Classification on Implementation	MUST
Result	**NOT APPLICABLE**

Remarks	LIGHTest performs logging (in particular, the ATV), but in a transparent way as explained in the introduction of the privacy evaluation, i.e., the LIGHTest components produce a trace of what has happened that they don't retain but rather just return to the entity deploying the component. Therefore, the security, integrity, and privacy of these logging information's is the responsibility of the parties deploying LIGHTest. In particular, they have to comply with whatever regulations is applicable for their business and/or service contracts.

No.	**SAR-03.03- Logging and Auditing: Access rights**
Description	All LIGHTest components that generate audit records MUST prohibit all entities read access to the records except for those entities that have been granted explicit access.
Classification on Implementation	MUST
Result	**NOT APPLICABLE**
Remarks	LIGHTest performs logging (in particular, the ATV), but in a transparent way as explained in the introduction of the privacy evaluation, i.e., the LIGHTest components produce a trace of what has happened that they don't retain but rather just return to the entity deploying the component. Therefore, the security, integrity, and privacy of these logging information's is the responsibility of the parties deploying LIGHTest. In particular, they have to comply with whatever regulations is applicable for their business and/or service contracts.

No.	**SAR-03.04- Logging and Auditing: Integrity protection**
Description	Access to all audit records by LIGHTest components or system administrators SHOULD be recorded and stored with integrity protection in an access-restricted storage space.
Classification on Implementation	SHOULD
Result	**NOT APPLICABLE**
Remarks	LIGHTest performs logging (in particular, the ATV), but in a transparent way as explained in the introduction of the privacy evaluation, i.e., the LIGHTest components produce a trace of what has happened that they don't retain but rather just return to the entity deploying the component. Therefore, the security, integrity, and privacy of these logging information's is the responsibility of the parties deploying LIGHTest. In particular, they have to comply with whatever regulations is applicable for their business and/or service contracts.

No.	**SAR-04.00- Availability**

Description	Protection against classical denial of service attacks SHOULD be achieved to the level provided -- without opening additional vulnerabilities -- by protocols like TLS, DNSSEC, and DANE. Resource access limitations MUST be implemented to protect against workload problems. An analysis for robustness SHOULD be provided in the style of the Quality Calculus
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	DTU's opinion: We do not see these availability goals as the responsibility of the ATV – also the following availability goals here. Hence we have set the classification to MAY. If there are any protections in the ATV they are very welcome, but we do not see that they are required.

No.	**SAR-04.01- Availability: Failover Backup**
Description	The LIGHTest system components MUST have a Failover backup mechanism. The databases, operation history and system components MUST be backed up in a failover system which will back up the main system during a critical failure.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

No.	**SAR-04.02- Availability: Emergency Operation Mode**
Description	The LIGHTest system MUST expose an emergency operation mode which supports availability of critical system services during emergency system support, maintenance and upgrades which May require limited functionality during the process.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

No.	**SAR-04.03- Availability: Availability Optimization**
Description	The availability of the overall system does not mean that the availability of every component SHOULD be 100% all the time. Therefore, the availability equation of the overall system and the coefficients of each particular component MUST be determined optimally to reduce the costs while keeping the goal at maximum.

Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

No.	**SAR-04.04- Availability: Execution Power**
Description	The LIGHTest services MUST have sufficient execution power to take actions for various use cases.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

No.	**SAR-04.05- Availability: Downtime Power**
Description	The components that require downtime during their regular process or maintenance MUST be identified and made sure that they don't affect the availability of the overall system.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

No.	**SAR-05.00- Accountability**
Description	Any LIGHTest component that makes decisions (trust decisions, issuing certificates) MUST be able to defend such decisions by presenting all the artifacts (like certificates) on the basis of which the decision was made. When data storage is necessary to achieve this, it MUST adhere to the general requirements for storage.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	Focus

No.	**SAR-05.01- Integrity of Trust Decisions**

Description	LIGHTest shall provide a clear recipe for its decisions. All-important data to verify the decision MUST be stored for later verification.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	Focus

No.	**SAR-10.00- Integrity: System Integrity**
Description	All Lightest components MUST ensure that integrity of installed software on them are protected against modifications. Therefore, Lightest project MUST provide an attestation mechanism for its service providers from booting to software layer and user owned devices.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

No.	**SAR-20.00- Logging and Auditing: Monitoring**
Description	The LIGHTest backend components MUST be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential security violation.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

No.	**SAR-21.00- Logging and Auditing: Suspicious activity**
Description	The LIGHTest backend components SHOULD be able to maintain profiles of system usage in compliance with the privacy requirements that allow the detection of any suspicious user activity. In case of detection of a suspicious activity, an alert to the system administrator SHOULD be triggered. Depending on the level of severity, a user authentication May be blocked until the detected issue is resolved.
Classification on Implementation	SHOULD
Result	**NOT APPLICABLE**

Remarks	

No.	**SAR-22.00- Logging and Auditing: Security violation**
Description	The LIGHTest backend components SHOULD have available a heuristic method to detect well known attacks and intrusion scenarios. Upon detection, the affected component SHOULD inform the other components about the security violation and terminate further service activities. Additionally, it SHOULD trigger an alert to the system administrator.
Classification on Implementation	SHOULD
Result	**NOT APPLICABLE**
Remarks	

No.	**SAR-26.00- Minimal data usage**
Description	The data stored in the system for decision making SHOULD be kept to a minimum.
Classification on Implementation	SHOULD
Result	**NOT APPLICABLE**
Remarks	

No.	**SAR-27.00- Authentication**
Description	The Delegation Publisher MUST provide a means of authenticating the delegations before they are published
Classification on Implementation	MUST
Result	**PASSED**
Remarks	Provisions; this MUST also (in addition to the specified requirement) include discovery and revocation

No.	**SAR-27.01- Authorization**
Description	Only authorized personnel can edit or publish delegations
Classification on Implementation	MUST

Result	**PASSED**
Remarks	Provisions

6.1.2 Pilots

The classifications of the pilot requirements are generally the same as on the implementation level, except for most of the requirements that concern availability and the requirements SAR-10.00 and SAR-20.00. These are properties that concern the deployment of the LIGHTest systems and so they are important for the pilots. We have therefore increased the classification levels for SAR-10.00 and SAR-20.00 as well as most of the availability requirements.

In the following we mark a requirement as “PASSED” if the pilots fully fulfill the requirement. If the pilots currently do not fulfill the requirement but it is possible that they might fulfill it in the future then the requirement is marked as “Neutral”. Finally, if the pilots do not fulfill the requirement then the requirement is marked “NOT PASSED”. Whenever we have an additional remark on how our decision was made then we have justified the decision in the Remark field.

No.	**SAR-01.00- Channels**
Description	The LIGHTest components MUST use the best (most secure) channels that are technically feasible and not violating privacy goals. These channels SHOULD include protection against man-in-the middle, replay, reflection and similar protocol level attacks. This SHOULD be achieved by using protocols like TLS, DNSSEC, and DANE.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-01.01- Confidentiality: Secure Channel**
Description	(Confidentiality – Secure Channel) Lightest Services MUST communicate on secure channel in order to protect channel data from eavesdropping
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes

Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-01.02- Confidentiality: Data Protection**
Description	Lightest services MUST maintain the confidentiality of the data subject to protection that are sent between components.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	This is actually indirectly achieved, see the evaluation on the privacy goals.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	This is actually indirectly achieved, see the evaluation on the privacy goals.

-

No.	**SAR-01.03- Confidentiality: Session data protection**
Description	Lightest components MUST ensure that the any session data subject to protection (person-related data or session keys) are deleted after session finishes.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-01.04- Confidentiality: Key Material/Credential Protection**
Description	Lightest services MUST enforce all key materials and credentials are held confidential at rest.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes

Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	According to our assumptions, LIGHTest components generally will not store data, but only processes them. However, for delegation providers and LIGHTest run-services (pilot level) this MUST be evaluated.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	According to our assumptions, LIGHTest components generally will not store data, but only processes them. However, for delegation providers and LIGHTest run-services (pilot level) this MUST be evaluated.

-

No.	**SAR-01.05- Confidentiality: Replay Protection**
Description	Request and response messages MUST be replay protected and if a replay occurs Lightest components MUST be able to detect.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	Note that this requirement Should actually be labeled an authentication/integrity goal since replay/freshness are part of injective agreement, not secrecy.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Note that this requirement Should actually be labeled an authentication/integrity goal since replay/freshness are part of injective agreement, not secrecy.

-

No.	**SAR-01.06- Confidentiality**
Description	Any confidentiality issue that occurs in one Lightest component MUST not affect other Lightest components.
Classification on Pilot	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-01.07- Integrity: Data Integrity**

Description	All components of Lightest MUST protect the integrity of Data Subject's Personal Data, Audits, metadata and log files both in retention and processes (authentication, authorization, delegation, transporting, identity and attribute management). Only the authorized entities MUST be able to correct and remove the Personal Data with the condition of informing the Data Subject.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-01.08- Integrity: Error Handling**
Description	Lightest components MUST detect a data and system integrity error and take the necessary actions (E.g. closing current session, re-authentication, informing the Data Subject, informing concerned Member State(s)' supervisory body(ies) etc.) to prevent possible treats.
Classification on Pilot	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

-

No.	**SAR-02.00- Inter-component communication**
Description	When components communicate with each other, this is either on the same physical system or virtualized. The principle of virtualization is that by crypto it Should be ensured to be equivalent to the setup on the same machine except for failures of the communication medium (-> that is an issue of availability).
Classification on Pilot	SHOULD
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**

Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

-

No.	**SAR-02.01- Integrity: Component Relations**
Description	Lightest components MUST ensure that the breaking the integrity of one system component will not cause “single point of failure” that can lead to integrity failures in other components.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**NEUTRAL**
Comments for the Correos Pilot	If an intruder is able to break the integrity of a component this does not help to break the integrity of other components. However, some components—like trust lists—are heavily depended upon by other components and thus an integrity breach can have far reaching consequences. Therefore, we would like to classify this as neutral, because we cannot reasonably prevent the consequences of such a breach.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	If an intruder is able to break the integrity of a component this does not help to break the integrity of other components. However, some components—like trust lists—are heavily depended upon by other components and thus an integrity breach can have far reaching consequences. Therefore, we would like to classify this as neutral, because we cannot reasonably prevent the consequences of such a breach.

-

No.	**SAR-02.02- Availability: Single Point of Failure**
Description	The LIGHTest system MUST not have, or have as minimal, single point of failures. The critical system nodes and bottleneck regions MUST have multiple instances that are supported by powerful load balancers.
Classification on Pilots	MUST NOT
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	Only relevant for The UPRC Pilot (PEPPOL). In the Correos Pilot (eCorreos) the user will still be able to use the eCorreos even in a case where LIGHTest has a failure – the user will just not have the guarantee of LIGHTest. Moreover, only

	in The UPRC Pilot (PEPPOL) is the deployment in a remote fashion.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Only relevant for The UPRC Pilot (PEPPOL). In the Correos Pilot (eCorreos) the user will still be able to use the eCorreos even in a case where LIGHTest has a failure – the user will just not have the guarantee of LIGHTest. Moreover, only in The UPRC Pilot (PEPPOL) is the deployment in a remote fashion.

-

No.	**SAR-03.00- Storage**
Description	Storage of data MUST be minimal -- i.e. there is a clearly documented need -- and it MUST be protected against unauthorized reading, writing, and loss/destruction. Any backups MUST adhere to these protections, and the amount of backups, if any, MUST be explicitly assessed.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-03.01- Logging and Auditing**
Description	The overall LIGHTest system MUST establish a logging and auditing infrastructure that is able to audit system and component failures, to detect suspicious system behaviour and that can be used to trigger according alerts and countermeasures to maintain secure system functionality. The logging and auditing infrastructure MUST be in accordance with privacy regulations and requirements.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	

-

No.	SAR-03.02- Logging and Auditing: Event association
Description	For audit events resulting from actions of identified users, all LIGHTest backend components MUST be able to associate each event with the identity of the user that caused the event, in compliance with the LIGHTest privacy requirements.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NOT PASSED**
Comments for The UPRC Pilot	The PEPPOL community requires that no logging occurs in any form, so this requirement cannot be satisfied.

-

No.	SAR-03.03- Logging and Auditing:Access rights
Description	All LIGHTest components that generate audit records MUST prohibit all entities read access to the records except for those entities that have been granted explicit access.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NOT PASSED**
Comments for The UPRC Pilot	The PEPPOL community requires that no logging occurs in any form, so this requirement cannot be satisfied.

-

No.	SAR-03.04- Logging and Auditing: Integrity protection
Description	Access to all audit records by LIGHTest components or system administrators SHOULD be recorded and stored with integrity protection in an access-restricted storage space.
Classification on Pilots	SHOULD
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	

Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NOT PASSED**
Comments for The UPRC Pilot	The PEPPOL community requires that no logging occurs in any form, so this requirement cannot be satisfied.

-

No.	**SAR-04.00- Availability**
Description	Protection against classical denial of service attacks SHOULD be achieved to the level provided -- without opening additional vulnerabilities -- by protocols like TLS, DNSSEC, and DANE. Resource access limitations MUST be implemented to protect against workload problems. An analysis for robustness SHOULD be provided in the style of the Quality Calculus
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	Only relevant for The UPRC Pilot (PEPPOL). In The Correos Pilot (eCorreos) the user will still be able to use the eCorreos even in a case where LIGHTest has a failure – the user will just not have the guarantee of LIGHTest. Moreover, only in The UPRC Pilot (PEPPOL) is the deployment in a remote fashion. And this also holds for most of the following availability goals for which we do not make the remark.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	Only relevant for The UPRC Pilot (PEPPOL). In The Correos Pilot (eCorreos) the user will still be able to use the eCorreos even in a case where LIGHTest has a failure – the user will just not have the guarantee of LIGHTest. Moreover, only in The UPRC Pilot (PEPPOL) is the deployment in a remote fashion. And this also holds for most of the following availability goals for which we do not make the remark.

-

No.	**SAR-04.01- Availability: Failover Backup**
Description	The LIGHTest system components MUST have a Failover backup mechanism. The databases, operation history and system components MUST be backed up in a failover system which will back up the main system during a critical failure.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**

Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-04.02- Availability: Emergency Operation Mode**
Description	The LIGHTest system MUST expose a emergency operation mode which supports availability of critical system services during emergency system support, maintenance and upgrades which May require limited functionality during the process.
Classification on Pilots	MAY
Relevant for the Correos Pilot	No
Result for the Correos Pilot	**NOT APPLICABLE**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

-

No.	**SAR-04.03- Availability: Availability Optimization**
Description	The availability of the overall system does not mean that the availability of every component Should be 100% all the time. Therefore, the availability equation of the overall system and the coefficients of each particular component MUST be determined optimally to reduce the costs while keeping the goal at maximum.
Classification on Pilots	MUST
Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	PEPPOL: unclear how to answer this

-

No.	**SAR-04.04- Availability: Execution Power**
Description	The LIGHTest services MUST have sufficient execution power to take actions for various use cases.
Classification on Pilots	MUST

Relevant for the Correos Pilot	Yes
Result for the Correos Pilot	**PASSED**
Comments for the Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-04.05- Availability: Downtime Power**
Description	The components that require downtime during their regular process or maintenance MUST be identified and made sure that they don't affect the availability of the overall system.
Classification on Pilots	MUST
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-05.00- Accountability**
Description	Any LIGHTest component that makes decisions (trust decisions, issuing certificates) MUST be able to defend such decisions by presenting all the artifacts (like certificates) on the basis of which the decision was made. When data storage is necessary to achieve this, it MUST adhere to the general requirements for storage.
Classification on Pilots	MUST
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-05.01- Integrity of Trust Decisions**

Description	LIGHTest shall provide a clear recipe for its decisions. All important data to verify the decision MUST be stored for later verification.
Classification on Pilots	MUST
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**NEUTRAL**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	

-

No.	**SAR-10.00- Integrity: System Integrity**
Description	All Lightest components MUST ensure that integrity of installed software on them are protected against modifications. Therefore, Lightest project MUST provide an attestation mechanism for its service providers from booting to software layer and user owned devices.
Classification on Pilots	MUST
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**NEUTRAL**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

-

No.	**SAR-20.00- Logging and Auditing: Monitoring**
Description	The LIGHTest backend components MUST be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential security violation.
Classification on Pilots	MUST
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	SAR-21.00- Logging and Auditing: Suspicious activity
Description	The LIGHTest backend components SHOULD be able to maintain profiles of system usage in compliance with the privacy requirements that allow the detection of any suspicious user activity. In case of detection of a suspicious activity, an alert to the system administrator SHOULD be triggered. Depending on the level of severity, a user authentication May be blocked until the detected issue is resolved.
Classification on Pilots	SHOULD
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	SAR-22.00- Logging and Auditing: Security violation
Description	The LIGHTest backend components SHOULD have available a heuristic method to detect well known attacks and intrusion scenarios. Upon detection, the affected component SHOULD inform the other components about the security violation and terminate further service activities. Additionally, it SHOULD trigger an alert to the system administrator.
Classification on Pilots	SHOULD
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	SAR-26.00- Minimal data usage
Description	The data stored in the system for decision making SHOULD be kept to a minimum.
Classification on Pilots	SHOULD
Relevant for The Correos Pilot	Yes

Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

-

No.	**SAR-27.00- Authentication**
Description	The Delegation Publisher MUST provide a means of authenticating the delegations before they are published
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	This is a requirement on the delegation publisher and is therefore obviously not relevant for the pilots.
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	This is a requirement on the delegation publisher and is therefore obviously not relevant for the pilots.

-

No.	**SAR-27.01- Authorization**
Description	Only authorized personnel can edit or publish delegations
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	Only relevant for The UPRC Pilot (PEPPOL) because The Correos The Correos Piloturrently does not make use of delegation.
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

7. Usability Requirements

Usability is the extent to which a product can be used by specific users in a specific context of use, to reach specific goals effectively, efficiently and satisfactory. Usability is a key indicator of product quality and in the design process, it plays an important role in ensuring that a product is easy and pleasant to use.

The ISO 9241-11 specifies Usability Core Requirements to meet the Usability definition. Usability core requirements are effectiveness, efficiency and the users' satisfaction.

To refine those Core Requirements the ISO 9241-110 defines seven aspects of these general ergonomic principles: Suitability for the task, Suitability for learning, Suitability for individualization, Conformity with user expectations, Self-descriptiveness, Controllability and Error tolerance.

Based on the Usability definition, Nielsen (2012) defines five quality components of usability:

1. Learnability: The ease of performing basic tasks for the first time
2. Efficiency: The speed of performing tasks once a user has experience using the system
3. Memorability: The ability to remember the interface's components
4. Errors: The regularity and severity of, and recovery from, error
5. Satisfaction: The overall pleasantness of the product

The claim of today's product design is not just to have a usable User Interface, but also that users are having a positive Experience with the product. User Experience (UX) as described by Hassenzahl (2008) is a momentary, evaluative feeling (positive or negative) when using technical products and services. A positive UX occurs by satisfying basic human needs. These needs are self-esteem, competence, competition, physicalness, security, stimulation, relatedness and popularity. Designing a good user experience is important as it engages and delights the user and builds trust.

One of the LIGHT^{est} project's goals is to provide a usable and well-designed client; therefore, guidelines for Trust and Knowledge based on the common Usability principles and requirements have to be considered. Crucial guidelines, considered in the Usability Requirements in 7.1, are:

1. Usability Requirements for Security Tools (Whitten and Tygar, 1999)
2. Freiburg Usability guidelines (Gerd tom Markotten, 2004)
3. Guidelines for Secure Interaction Design (Yee, 2004)
4. Principles and Patterns to Align Usability and Security (Garfinkel, 2005)

5. Idea for Heuristic Evaluation for IT Security Management Tools (Jaferian et al., 2011)

7.1 Requirements Evaluation

7.1.1 Implementation

The following section presents the results of the usability evaluation on the implementation and pilot's level. The usability evaluation stretches over the entire duration of the project. From definition, analysis and re-categorization of the requirements towards the actual evaluation, each step was and is important and not to be neglected to receive satisfying evaluation results. The usability evaluation aims at providing a realistic view of how the requirements would be interfrated and applied to the artefacts.

The test strategy for the usability evaluation combines two basic evaluation methods.

One method is a combination of a heuristic evaluation and a walkthrough, also referred as "heuristic walkthrough". The heuritistic evaluation is a qualitative method that uses usability principles (the heuristics) to check the overall usability of the product. Walkthrough simply says, that experts are checking the whole system how the design principles were applied and where they can find opportunities to improve the system. A heuristic walkthrough is cheap and easy to conduct. It provides qualitative feedback and good results. Nevertheless, it Should never be the sole evaluation, because experts are biased and well trained. Therefor it does not replace a usability evaluation with end users (Sarodnick & Brau, 2011).

The other method is a usability evaluation with end users containing several usability evaluation methods.

The following section shows the results from the heuristic walkthrough and the usability evaluation considering the implementation.

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.
Classification on Implementation	NOT APPLICABLE
Result	**NOT APPLICABLE**
Remarks	

UR-01.01	**Established Usability Guidelines and Principles**

Description	The User Interface MUST consider established Usability Guidelines and Principles to assure an easy to use product and overall Usability.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

UR-01.02	**Learnability**
Description	Learnability is an important Usability Design Principle. In this case, it is even more important, because most users have little knowledge of the topic. So, first of all they have to learn how the system works.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

UR-03.00	**Commonality of Language**
Description	Ensure that global language requirements are taken into account, including languages that use special characters.

Classification on Implementation	MUST
Result	**PASSED**
Remarks	

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…“
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

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.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

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.
Classification on Implementation	SHOULD

Result	**PASSED**
Remarks	

UR-06.00	**Adaptive User Interface**
Description	The User Interface for the LIGHTest Project MUST be adaptive, so the content shows well on small screens as well on big ones.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

UR-07.00	**Easy to grasp metaphors**
Description	Often security software uses metaphors, which are not 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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

UR-08.00	**Transparency**
Description	There is no need for the user to understand the 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.
Classification on Implementation	MUST

Result	**PASSED**
Remarks	

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 stuff and realize what is happening. So every clutter or non-relevant information MUST be excluded from the UI.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

UR-10.00	**Empowered Users**
Description	Users MUST always feel in control of the things happening in the UI.
Classification on Implementation	MAY
Result	**NOT APPLICABLE**
Remarks	

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.
Classification on Implementation	MUST

Result	**PASSED**
Remarks	

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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

7.1.2 Pilots

Considering the usability requirements for the LIGHTest pilots all of them are "NOT APPLICABLE". This is due to the fact that the pilots are only using LIGHTest in the backend, but are not implementing the LIGHTest tools themselves as stated in the concept Deliverable D6.3. Therefore, there is not a direct user interaction with a LIGHTest User Interface.

The Pilots User Interfaces are Interfaces from the companies and there would be the need to evaluate those in a usability evaluation to be able to say if they do meet the usability requirements or not. As this is not a part of the LIGHTest project, no usability evaluation was conducted with the Pilots user interfaces.

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.
Classification on Pilots	MAY
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**

Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

UR-01.01	**Established Usability Guidelines and Principles**
Description	The User Interface MUST consider established Usability Guidelines and Principles to assure an easy to use product and overall Usability.
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

UR-01.02	**Learnability**
Description	Learnability is an important Usability Design Principle. In this case, it is even more important, because most users have little knowledge of the topic. So, first of all they have to learn how the system works.
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	

Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

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.
Classification on Pilots	MAY
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

UR-03.00	**Commonality of Language**
Description	Ensure that global language requirements are taken into account, including languages that use special characters.
Classification on Pilots	MAY
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**

Comments for The UPRC Pilot	

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…“
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

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.
Classification on Pilots	MAY
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

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.
Classification on Pilots	SHOULD
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

UR-06.00	Adaptive User Interface
Description	The User Interface for the LIGHTest Project MUST be adaptive, so the content shows well on small screens as well on big ones.
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

UR-07.00	Easy to grasp metaphors

Description	Often security software uses metaphors, which are not 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.
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

UR-08.00	**Transparency**
Description	There is no need for the user to understand the 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.
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

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 stuff and realize what is happening. So every clutter or non-relevant information MUST be excluded from the UI.
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

UR-10.00	Empowered Users
Description	Users MUST always feel in control of the things happening in the UI.
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

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.
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

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.
Classification on Pilots	MUST
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

8. Economic Requirements

The Economic Requirements were derived after a process of three preliminary steps. First, we identified and explored various relevant socio-economic theories that could be important to the different markets of interest for LIGHTest, such as, the identity management market, cloud and big data analytics market, and for internet of things market, etc. We built off what was learned and explored in the (Projekt, 2013) and built a LIGHTest aimed theoretical foundation. Second, we considered the overview of the markets that were defined as a peak interest for LIGHTest in the proposal stage. With that, we established an early stage stakeholder analysis that will be developed in future deliverables and work packages. After the process described above, we developed high-level economic requirements that ensures that the LIGHTest Artefacts are aware of the needs throughout the process what is needed post-project and to prepare the basic necessities to be open to the market and its stakeholders.

The Economic Requirements in this deliverable constitute as a guideline for the development of LIGHTest. These requirements have set the foundation of what should be evaluated. This section consists of two evaluations of artefacts. The first is the Implementation artefact, which is the ATV. The second evaluation is of the artefacts, the pilots.

8.1 Requirements Evaluation

8.1.1 Implementation

Once all Economic Requirements are set, it is necessary to classify them according to the level of importance in reference to both the implementation and pilot artefacts.

Since the implementation point of view is focused on the automatic trust verifier (ATV), we need to think about how the economic requirements could impact in the diverse markets for LIGHTest that were analysed previously in D2.3((The LIGHTest Project, 2017). It means to evaluate those requirements looking at the needs of the current market, and its stakeholders, and giving them the corresponding value under the environment of the Implementation Artefact.

Once the requirement is classified, this was followed in a second step by a detailed examination of the requirements specifications' key parts. As the Implementation artefact, the ATV, is not a 'market ready' product, it is considered in a more conceptual manner. If the Implementation artefact states that it is economic requirements are oriented to a future stage of the project where the LIGHTest will be on the market, and the following evaluation of the requirements took this into account.

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 (The LIGHTest Project, 2017).
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

ER-01.01	Support for different sources of income/compensation
Description	LIGHTest and its elements consume financial resources during operation. Therefore, LIGHTest MUST make it possible to generate a sustainable income/compensation which is large enough to cover the necessary financial resources. Nevertheless, not all stakeholders May be financially burdened (possibly free of charge for individual stakeholders). Therefore, LIGHTest MUST support the use of different sources of income/compensation.
Classification on Implementation	MUST
Result	**NEUTRAL**
Remarks	

ER-01.02	Support of different models of revenue distribution
Description	LIGHTest and its elements consume financial resources during operation. Therefore, a sustainable income MUST be generated, which is to be provided to the stakeholders involved in order to cover these financial resources. Nevertheless, not all stakeholders and users can be burdened (in the absence of adequate payment). Therefore, not all of the components involved in LIGHTest can generate sales. For this reason, LIGHTest MUST support various forms of revenue distribution between the operators of the components required for operation. This MUST be supported functionally by appropriate billing mechanisms
Classification on Implementation	SHOULD
Result	**NEUTRAL**
Remarks	Due to the flexible nature of the architecture, supporting different sources of incomes, there are no constraints found during evaluation to support appropriate billing mechanisms in the future.

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
Classification on Implementation	MUST
Result	**NEUTRAL**
Remarks	

ER-01.04	**Supports different deployment models**
Description	Different stakeholders and different scenarios require different deployment models (Public Institutions, Private Corporations, and 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
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

ER-03.00	**Trust Framework independence**
Description	Trust Management uses a wide variety of different forms of Trust Frameworks, Schemes, Policies, and Lists. LIGHTest MUST be designed to support as many platforms as possible.

Classification on Implementation	MUST
Result	**PASSED**
Remarks	

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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

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
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

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
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

ER-04.01	**Industry-independent set-up**
Description	LIGHTest MUST be sector-independent, as it allows for the participation of companies from different industries. In addition, it supports the development of inter-industry cooperation models, which can provide an all-encompassing range of solutions

Classification on Implementation	MUST
Result	**PASSED**
Remarks	

ER-05.00	**Organizational Interoperability**
Description	LIGHTest SHOULD allow for organizational interoperability. The goal of this interoperability level is to establish a common generic Trust Policy, List, and Scheme concepts. Related to Functional Requirements.
Classification on Implementation	SHOULD
Result	**PASSED**
Remarks	

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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

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.
Classification on Implementation	MUST
Result	**PASSED**
Remarks	

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.

Classification on Implementation	SHOULD NOT
Result	**PASSED**
Remarks	

8.1.2 Pilots

The Economic Requirements take the same approach as in the other requirement evaluations of artefacts.However, the pilots have another situation than our other artefacts. Each pilot is implemented in a different way. The Correos pilot is integrated into and a tool for their customers and the UPRC pilot is implemented as a back end application of PEPPOL tool. The classification of the economic requirements focus on the priority of each general economic requirement and the evaluation focuses on whether or not the Correos Pilot can fulfil the requirement as Passed, it implies that it has fulfilled the requirement or has the potential to fulfil it in the future. If the requirement is neutral, then it is not able to declare if it fulfills the requirement yet or not. If the requirement is not passed, the pilot has not completed the requirement. If the requirement is not applicable, it is explained in the comments on an ad hoc basis.

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 (The LIGHTest Project, 2017).
Classification on Pilots	MUST
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

ER-01.01	**Support for different sources of income/compensation**
Description	LIGHTest and its elements consume financial resources during operation. Therefore, LIGHTest MUST make it possible to generate a sustainable income/compensation which is large

	enough to cover the necessary financial resources. Nevertheless, not all stakeholders May be financially burdened (possibly free of charge for individual stakeholders). Therefore, LIGHTest MUST support the use of different sources of income/compensation.
Classification on Pilots	MUST
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	

ER-01.02	**Support of different models of revenue distribution**
Description	LIGHTest and its elements consume financial resources during operation. Therefore, a sustainable income MUST be generated, which is to be provided to the stakeholders involved in order to cover these financial resources. Nevertheless, not all stakeholders and users can be burdened (in the absence of adequate payment). Therefore, not all of the components involved in LIGHTest can generate sales. For this reason, LIGHTest MUST support various forms of revenue distribution between the operators of the components required for operation. This MUST be supported functionally by appropriate billing mechanisms
Classification on Pilots	SHOULD
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	

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
Classification on Pilots	MUST

Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

ER-01.04	**Supports different deployment models**
Description	Different stakeholders and different scenarios require different deployment models (Public Institutions, Private Corporations, and 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
Classification on Pilots	MAY
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

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 convienence, financial benefits. Refer to Use Cases for specific examples.
Classification on Pilots	MAY
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

ER-03.00	Trust Framework independence
Description	Trust Management uses a wide variety of different forms of Trust Frameworks, Schemes, Policies, and Lists. LIGHTest MUST be designed to support as many platforms as possible.
Classification on Pilots	MAY
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

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.
Classification on Pilots	MAY
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

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
Classification on Pilots	MAY
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**

Comments for The UPRC Pilot	

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
Classification on Pilots	SHOULD
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

ER-04.01	**Industry-independent set-up**
Description	LIGHTest MUST be sector-independent, as it allows for the participation of companies from different industries. In addition, it supports the development of inter-industry cooperation models, which can provide an all-encompassing range of solutions
Classification on Pilots	MAY
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**PASSED**
Comments for The UPRC Pilot	

ER-05.00	**Organizational Interoperability**
Description	LIGHTest SHOULD allow for organizational interoperability. The goal of this interoperability level is to establish a common generic Trust Policy, List, and Scheme concepts. Related to Functional Requirements.
Classification on Pilots	SHOULD
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	

Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

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.
Classification on Pilots	MAY
Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

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.
Classification on Pilots	MAY
Relevant for The Correos Pilot	No
Result for The Correos Pilot	**NOT APPLICABLE**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	No
Result for The UPRC Pilot	**NOT APPLICABLE**
Comments for The UPRC Pilot	

ER-07.00	**Neutrality**
Description	Similar to the grid neutrality, the LIGHTest ecosystem SHOULD NOT ensure individual players' preference, but a transparent neutrality of all participants.
Classification on Pilots	SHOULD NOT

Relevant for The Correos Pilot	Yes
Result for The Correos Pilot	**PASSED**
Comments for The Correos Pilot	
Relevant for The UPRC Pilot	Yes
Result for The UPRC Pilot	**NEUTRAL**
Comments for The UPRC Pilot	

9. Conclusion

This deliverable reviewed all of the sets of requirements that were established in D2.3. This included requirement categories such as, Functional, Privacy, Security and Accountability, Usability, and Economic. As this is a two part deliverable, this first deliverable evaluates only one artefact, the Reference Architecture. The second part of the deliverable evaluates the Implemenation and Pilots artefacts. Overall the results of every category was very positive for the Implementation and Pilots artefacts.

9.1 Overall Evaluation of Each Artefact

9.1.1 Implementation

Below, we can see that for the implementation that it was largley passed despite i fit was classified as a May, Must, or Should requirement and only a small fraction of them were deemed not passed. The diagram below shows out of a total of 132 requirements how many were classified as should, may, or must requirements and of those classifications which were evaluated with a passing, neutral, not passed, or not applicable result. There was 36 requirments that were classified as not applicable for the evaluation leaving 96 requirements applicable for evaluation. Of those 96 requirements, 88 (92 percent) were passed for the entire implementation artefact as shown in the pie chart below (Figure 2: Overall Evaluation Results of Applicable Requirementsfor the Implementation).

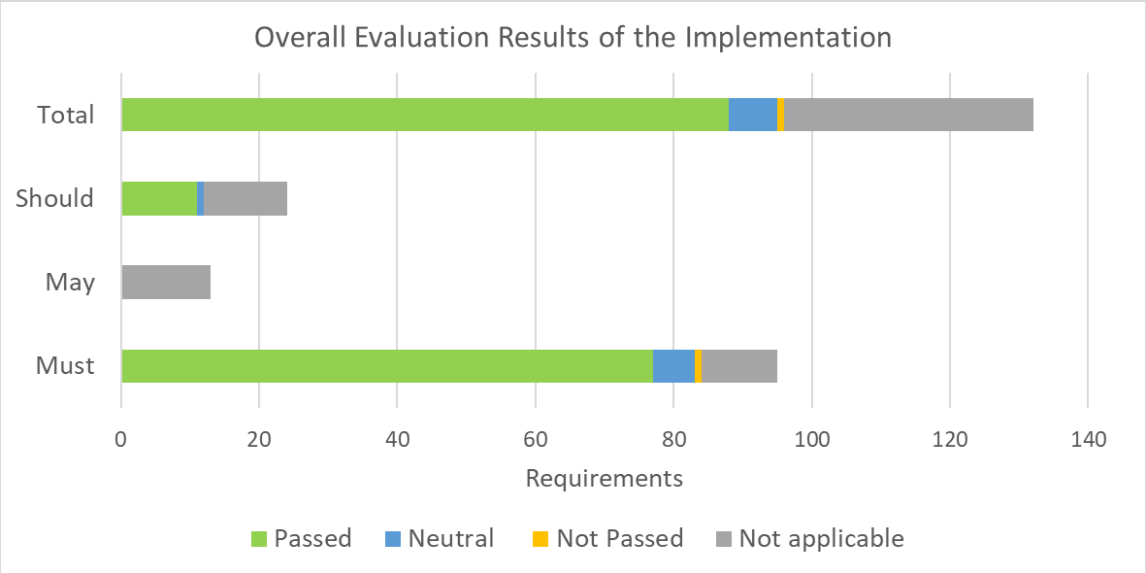

Figure 1: Overall Evaluation Results of the Implementation

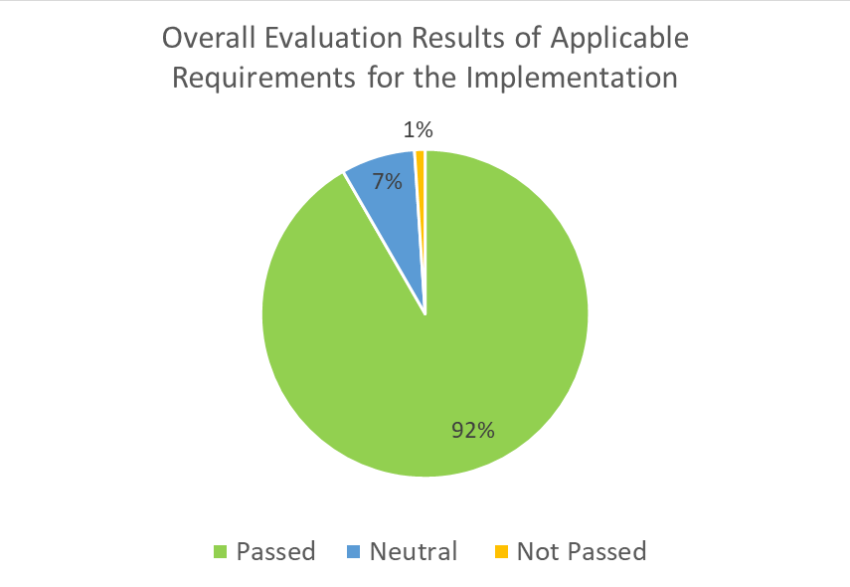

Figure 2: Overall Evaluation Results of Applicable Requirementsfor the Implementation

9.1.2 Correo's Pilot

For the Correo's Pilot Artefact, each classified requirement had a majority being passed. Even though there was more not applicable requirements, of the applicable requirements 83 percent were passed and 17 percent resulted in neutral.

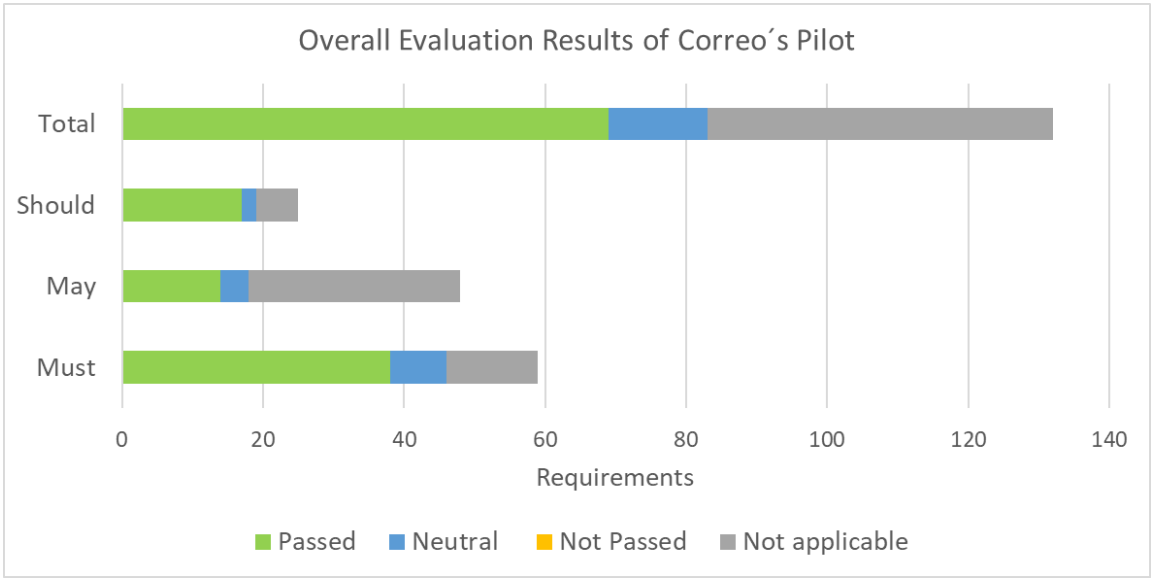

Figure 3: Overall Evaluation Results of Correo´s Pilot

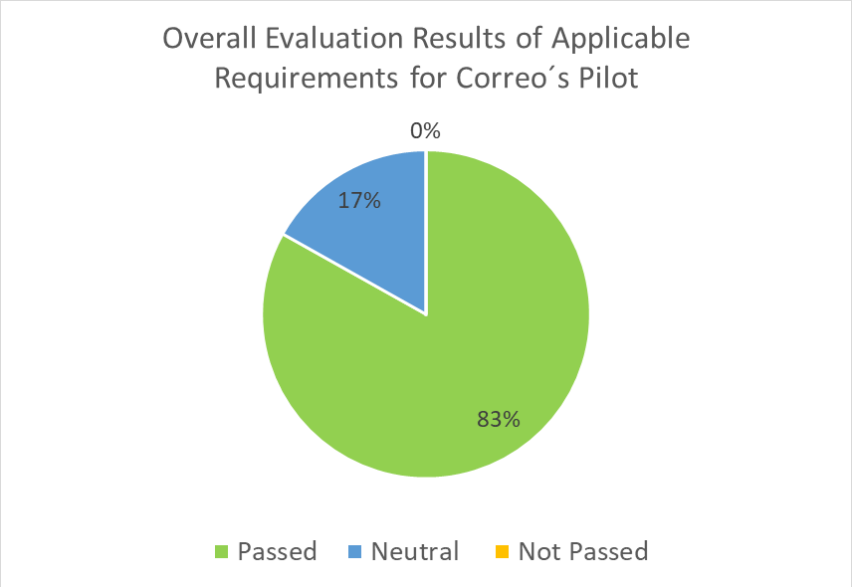

Figure 4: Overall Evaluation Results of Applicable Requirements for Correo's Pilot

9.1.3 UPRC's Pilot

The UPRC requiements also had a succesful majority of results. Of all applicable requirements for the UPRC pilot, 82 percent were evaluated as passing. There was 14 percent that received a Neutral score and 4 percent being Not Passed. Overall, this is still optimistic results for a pilot meeting interdisciplinary requirements.

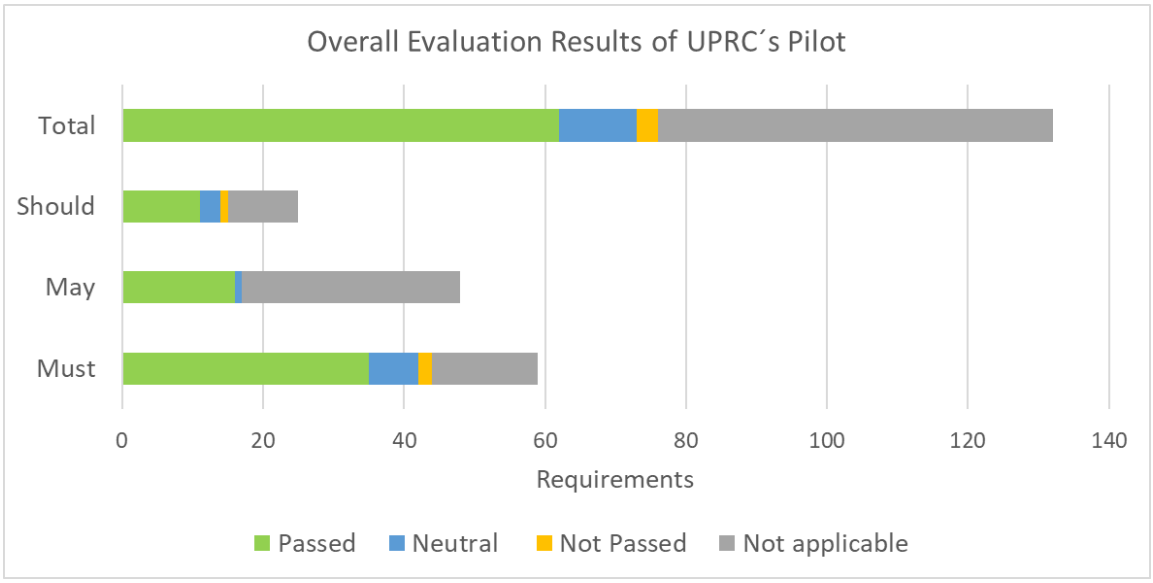

Figure 5: Overall Evaluation Results of UPRC´s Pilot

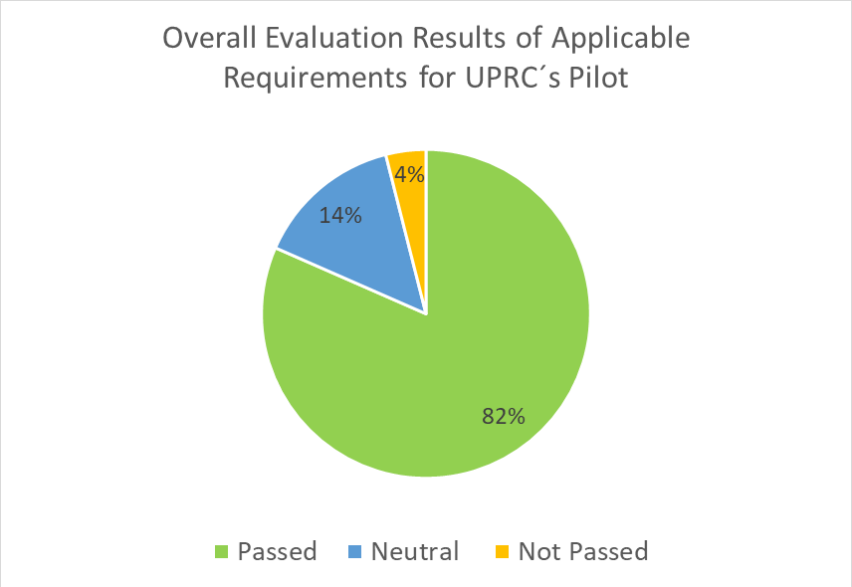

Figure 6: Overall Evaluation Results of Applicable Requirements for UPRC's Pilot

9.2 Functional Requirements Evaluation

9.2.1 Implementation

Regarding the evaluation of the Implementation, there was positive results. All MUST Requriements were passed. All MAY Requirements were not applicable regarding the intention of the Implementation. Of the SHOULD requirements, one was rated as passed and the other was rated as not applicable. With that, below one can see that 100 percent of the applicable Functional Requirements were passed. Regarding the evaluation of the Implementation, there was positive results.

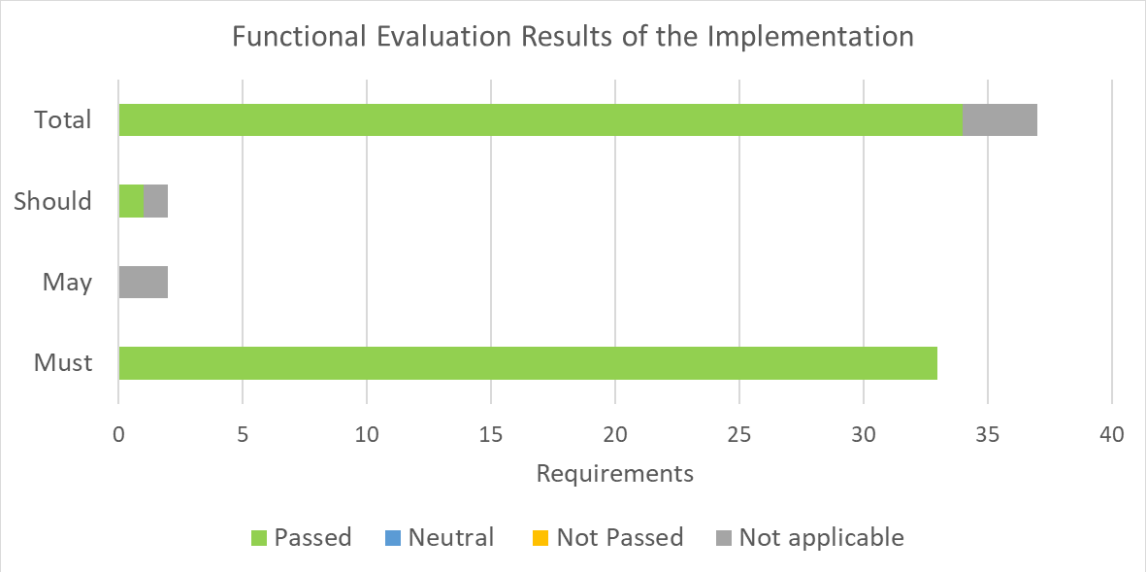

Figure 7: Functional Evaluation Results of the Implementation

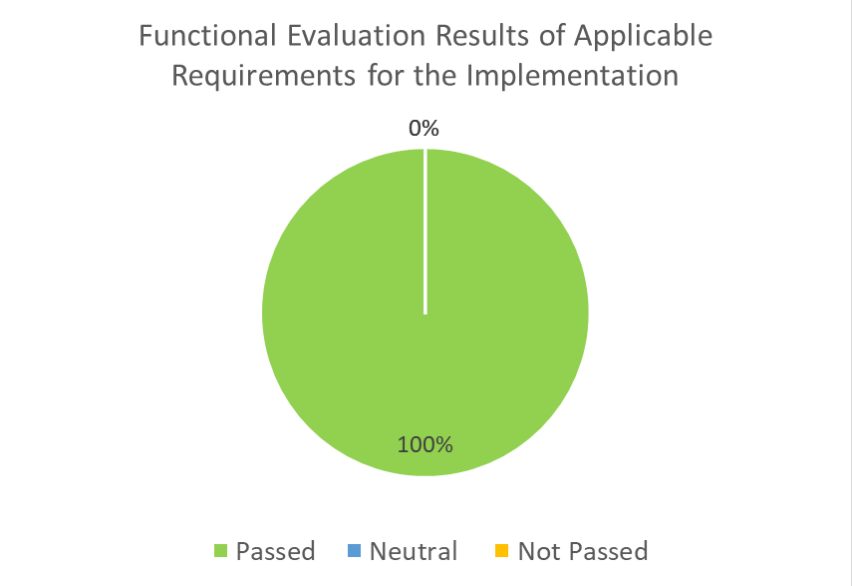

Figure 8: Functional Evaluation Results of Applicable Requirements for the Implementation

9.2.2 Correos Pilot

Regarding the evaluation of the Correos Pilot, there was positive results. Of 11 MUST Requirement, 6 were passed and 5 were neutral. Of 24 MAY Requirements, only one was neutral while the rest was deemed not applicable regarding the intention of the Correos Pilot. Of

the 2 SHOULD Requirements, 1 was passed while the other was neutral. With that, below one can see that 50 percent of the applicable Functional Requirements were passed, while the other 50 percent were neutral.

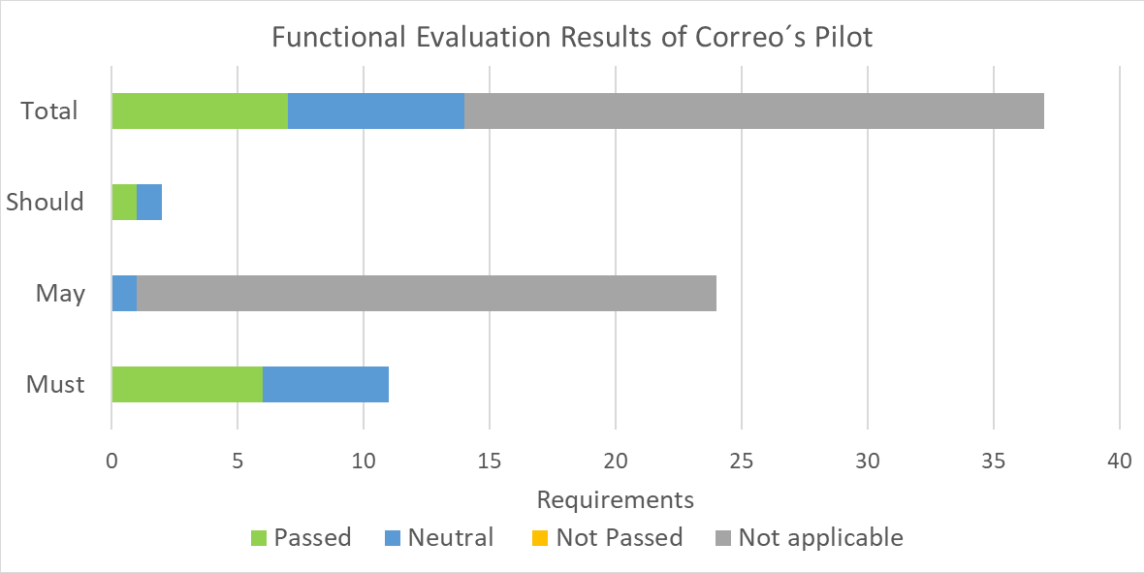

Figure 9: Functional Evaluation Results of Correo´s Pilot

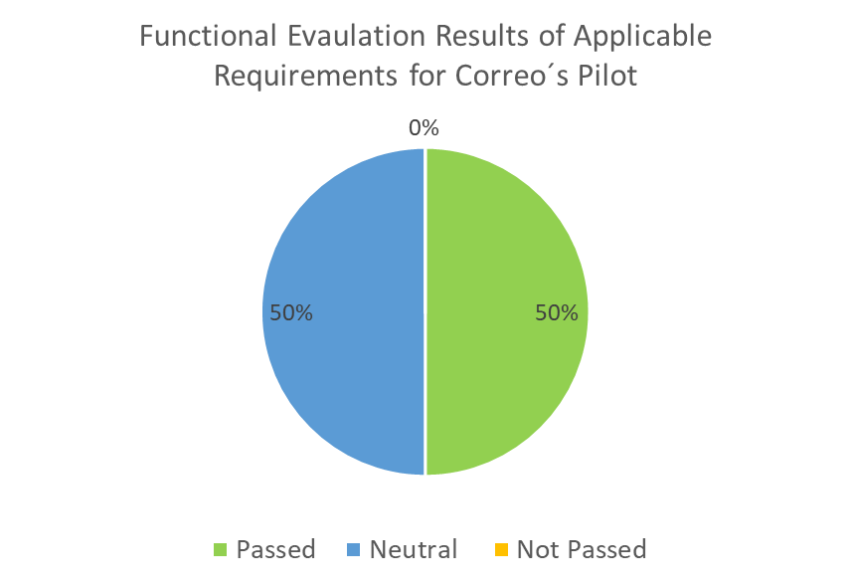

Figure 10: Functional Evaluation Results of Applicable Requirements for Correo´s Pilot

9.2.3 UPRC Pilot

Regarding the evaluation of the UPRC Pilot, there was positive results. Of 11 MUST Requirements, 7 were passed, 1 was neutral, while the rest was not applicable. All MAY Requirements were not applicable regarding the intention of the UPRC Pilot. Of the 2 SHOULD Requirements, 1 was passed and 1 was neutral. With that, below one can see that 80 percent of the applicable Functional Requirements were passed, while 20 percent were neutral.

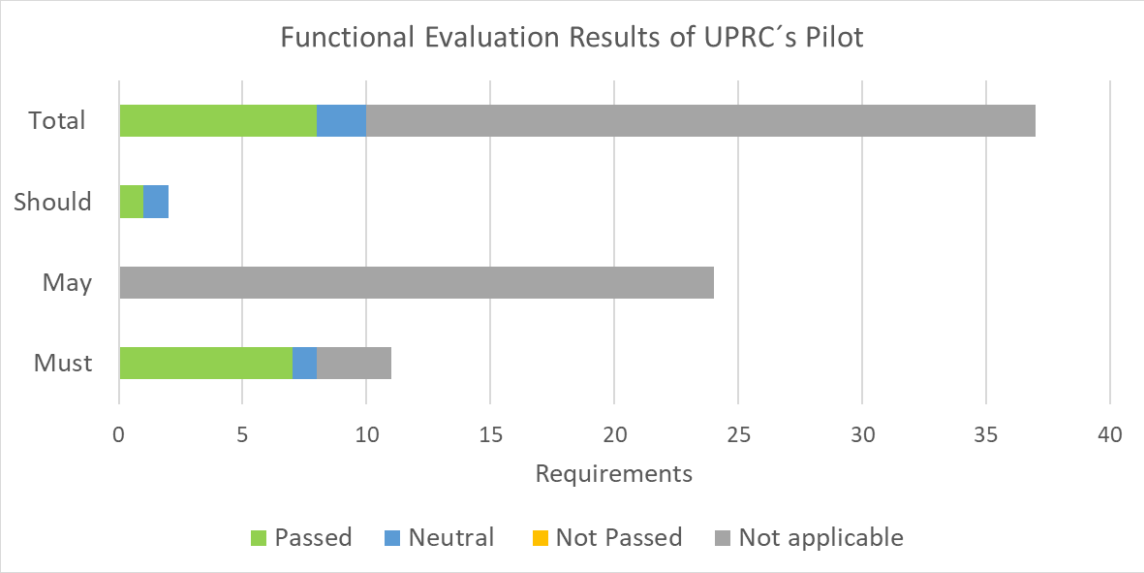

Figure 11: Functional Evaluation Results of UPRC´s Pilot

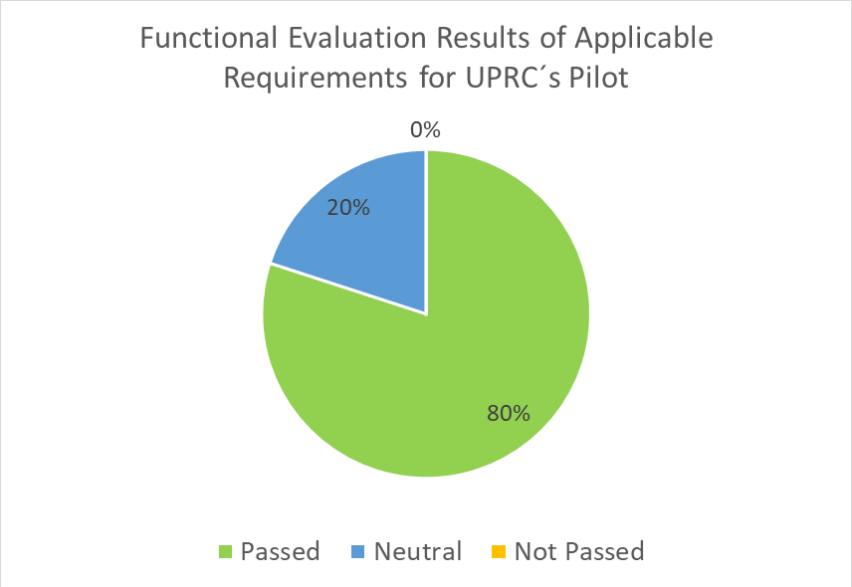

Figure 12: Functional Evaluation Results of Applicable Requirements for UPRC´s Pilot

9.3 Privacy Requirement Evaluation

9.3.1 Implementation

Regarding the evaluation of the Implementation, there was positive results. Of 20 MUST Requirements, 12 were passed, 1 was neutral, while 7 were Not Applicable. Of 12 SHOULD Requirements, 7 were passed and 5 were Not Applicable regarding the intention of the Implementation. With that, below one can see that 95 percent of the applicable Privacy Requirements were passed, while 5 percent were neutral.

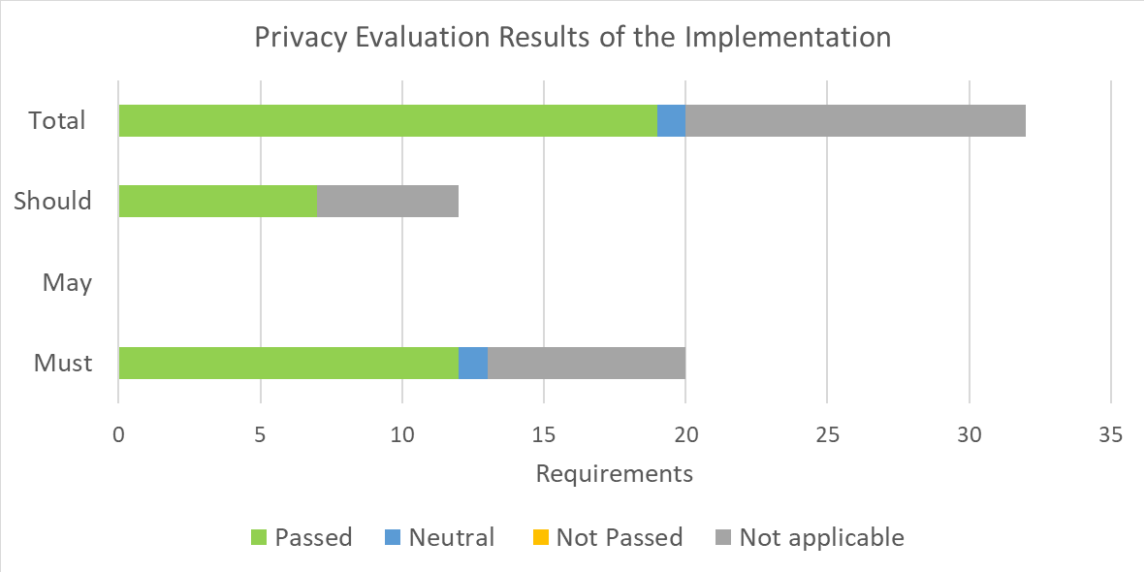

Figure 13: Privacy Evaluation Results of the Implementation

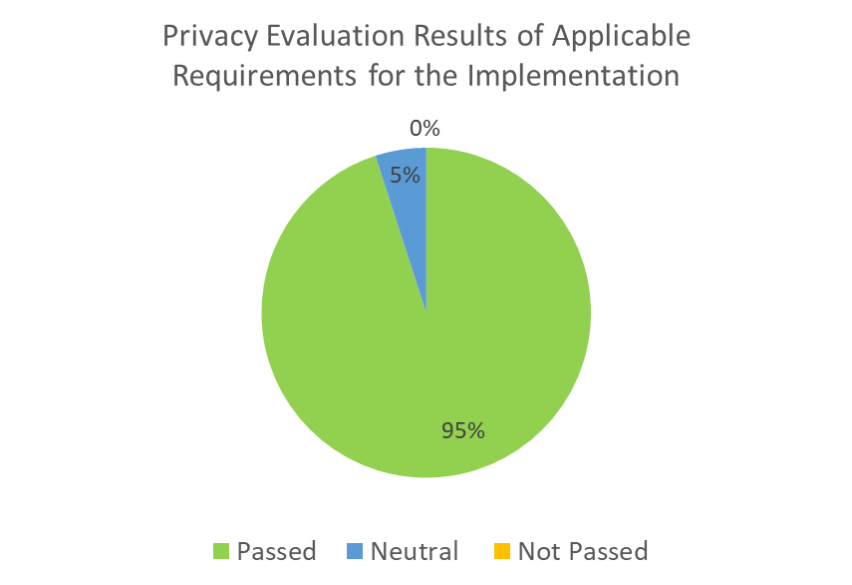

Figure 14: Privacy Evaluation Results of Applicable Requirements for the Implementation

9.3.2 Correos Pilot

Regarding the evaluation of the Correos Pilot, there was positive results. All MUST Requirements were passed. Of 17 MAY Requirements, 14 were passed and the rest were neutral regarding the intention of the Correos Pilot. Of the 5 SHOULD Requirements, 4 were passed and 1 was deemed neutral. With that, below one can see that 87 percent of the applicable Privacy Requirements were passed, while 13 percent were neutral.

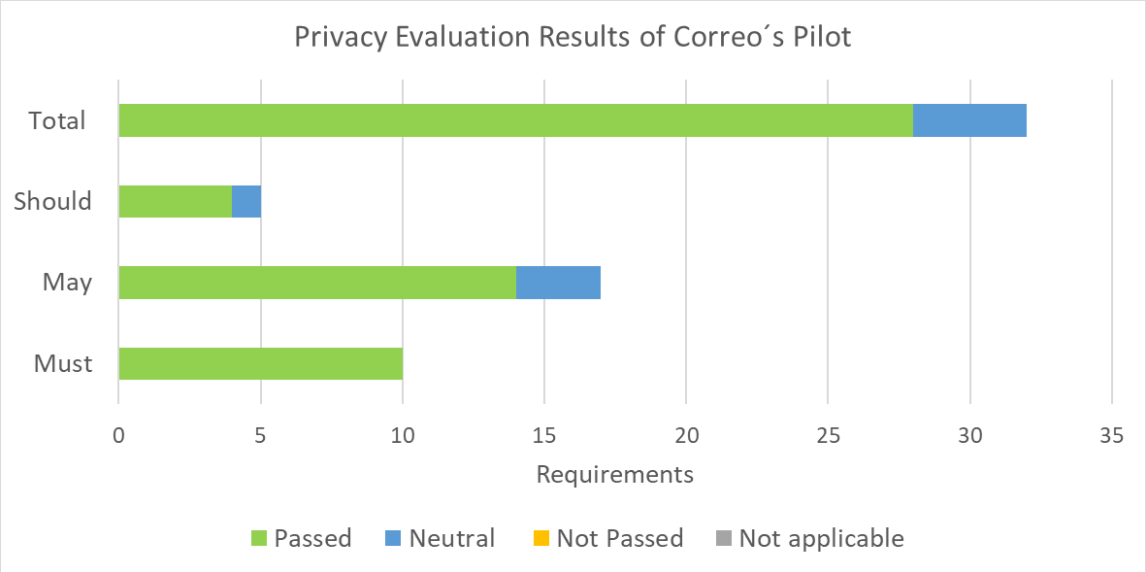

Figure 15: Privacy Evaluation Results of Correo´s Pilot Overview

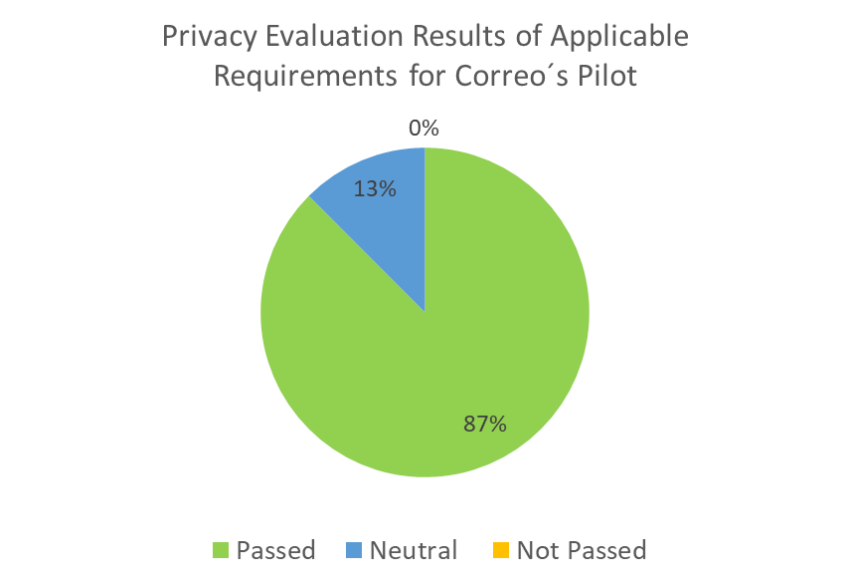

Figure 16: Privacy Evaluation Results of Applicable Requirements for Correo´s Pilot

9.3.3 UPRC Pilot

Regarding the evaluation of the UPRC Pilot, there was positive results. Of 10 MUST Requriements, 9 were passed and 1 was neutral. Of 17 MAY Requirements, 15 were passed, 1 was neutral and 1 was deemed Not Applicable regarding the intention of the UPRC Pilot. Of the 5 SHOULD Requriements, 13 were passed and 1 was deemed Not Applicable. With that, below one can see that 93 percent of the applicable Privacy Requirements were passed, while 7 percent were neutral.

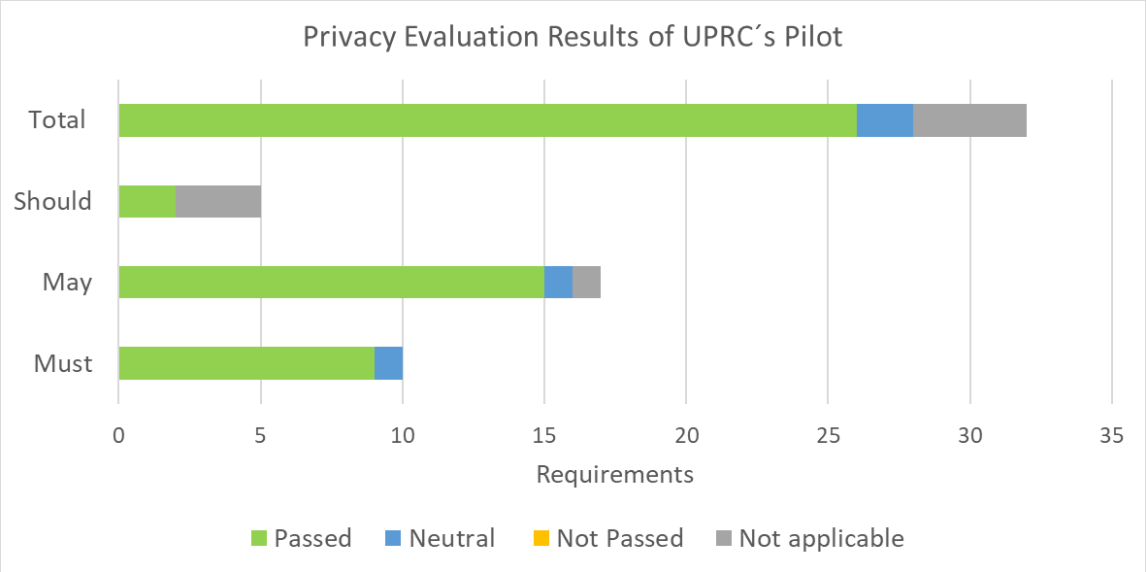

Figure 17: Privacy Evaluation Results of UPRC´s Pilot

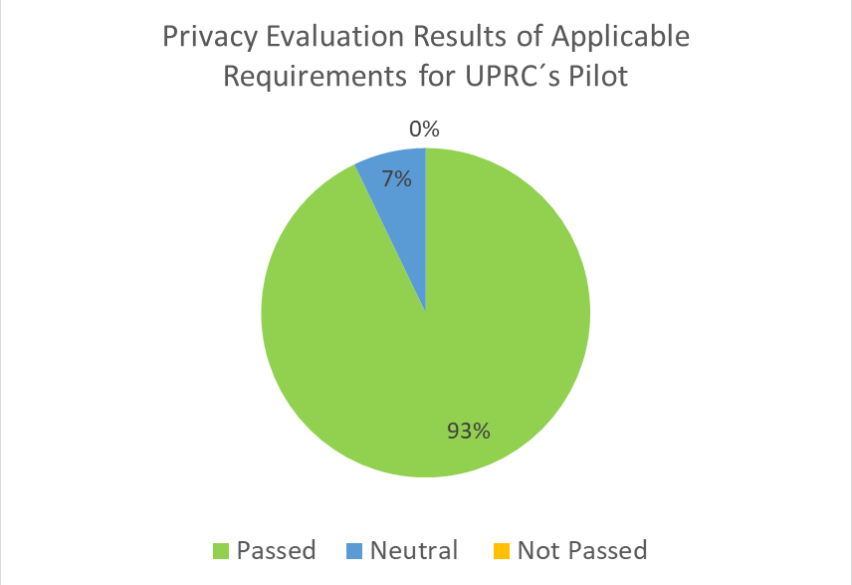

Figure 18: Privacy Evaluation Results of Applicable Requirements for UPRC´s Pilot

9.4 Security and Accountablility Evaluation

9.4.1 Implementation

Regarding the evaluation of the Implementation, there was positive results. Of 19 MUST Requriements, 12 were passed, 3 were neutral, 3 were Not Applicable and only 1 was not passed. None of the MAY and SHOULD Requirements were applicable regarding the intention of the Implementation. With that, below one can see that 75 percent of the applicable Security and Accountability Requirements were passed, while 19 percent were neutral and 6 percent not passed.

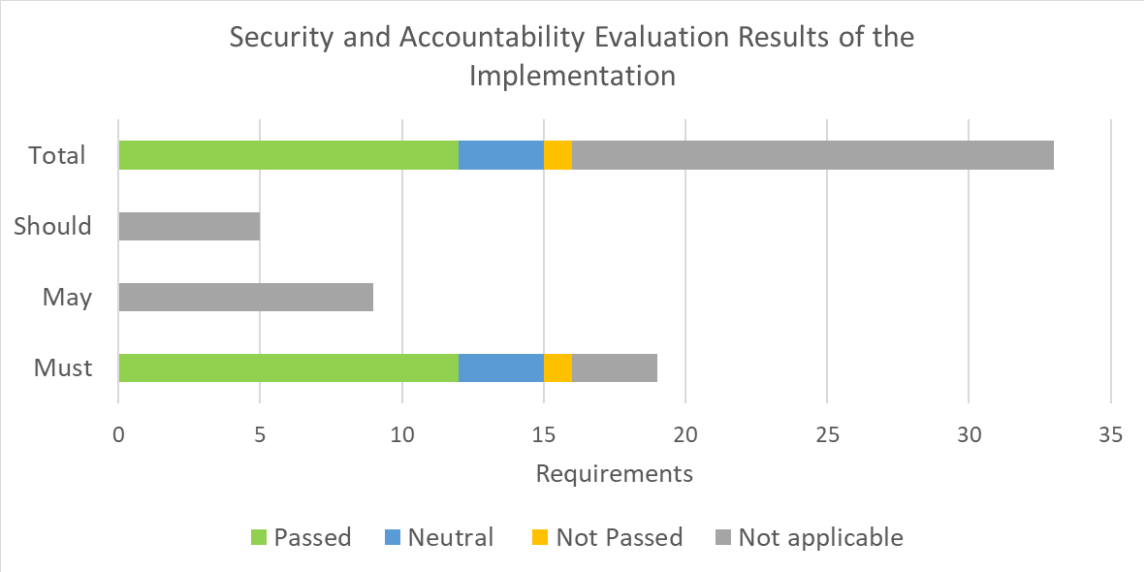

Figure 19: Security and Accountability Evaluation Results of the Implementation Overview

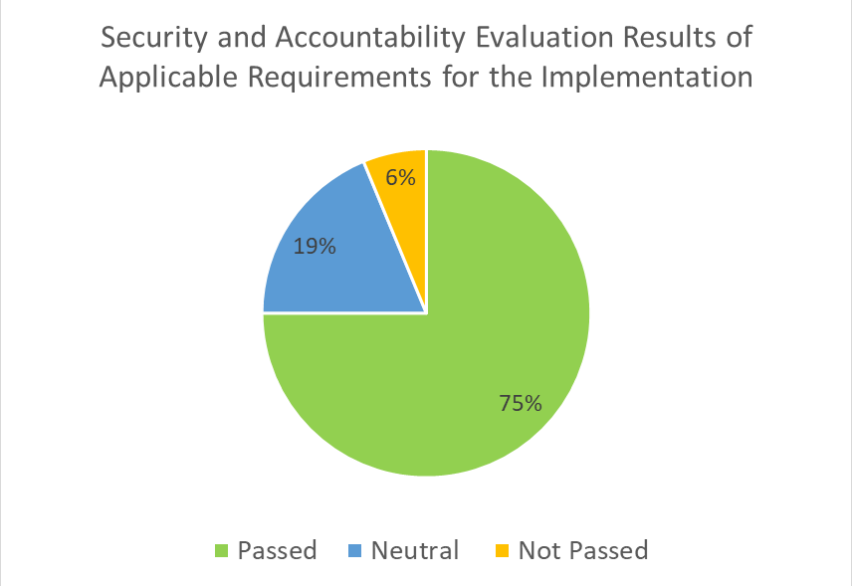

Figure 20: Security and Accountability Evaluation Results of Applicable Requirements for the Implementation

9.4.2 Correos Pilot

Regarding the evaluation of the Correos Pilot, there was positive results. Of 25 MUST Requirements, 19 were passed, while 3 were neutral and 3 were deemed Not Applicable. None of the MAY Requirements were applicable regarding the intention of the Correos Pilot. Of the 5 SHOULD Requirements, 80 percent were passed and 20% were deemed Not Applicable. With

that, below one can see that 88 percent of the applicable Security and Accountability Requirements were passed, while 12 percent were neutral.

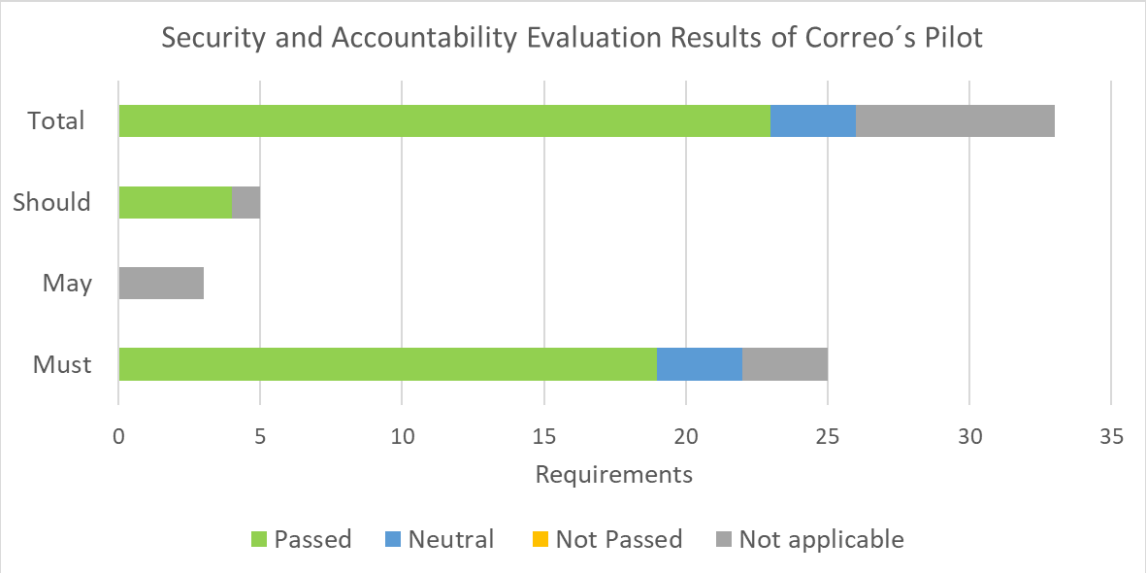

Figure 21: Security and Accountability Evaluation Results of Correo´s Pilot

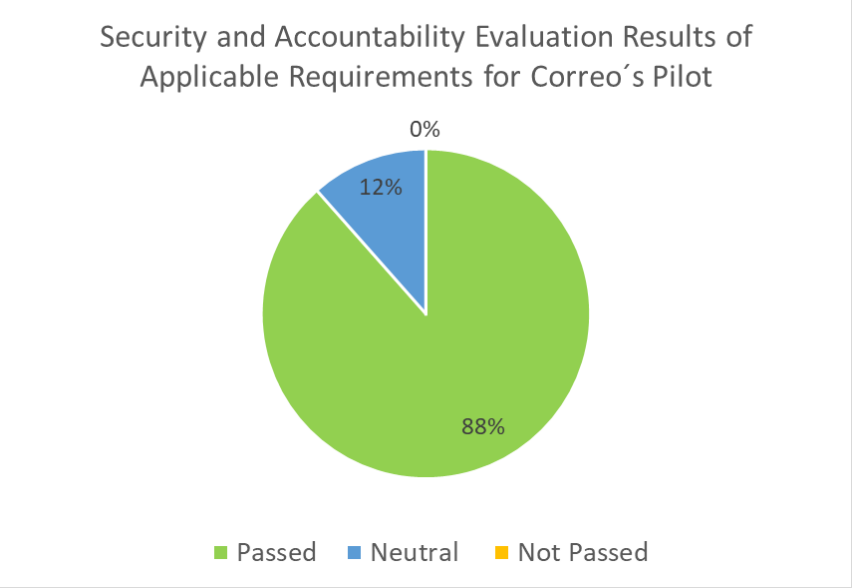

Figure 22: Security and Accountability Evaluation Results of Applicable Requirements for Correo´s Pilot

9.4.3 UPRC Pilot

Regarding the evaluation of the UPRC Pilot, there was positive results. Of 25 MUST Requriements,16 were passed, 5 were neutral, 2 were not passed and 2 were deemed Not Applicable.Of 3 MAY Requirements, 2 were Not applicable while 1 was applicable regarding the intention of the Correos Pilot. Of the 5 SHOULD Requriements, 60 percent were passed, while 20 percent were not passed and the rest were deemed Not Applicable. With that, below one can see that 71 percent of the applicable Security and Accountability Requirements were passed, while 18 percent were neutral and 11% were not passed.

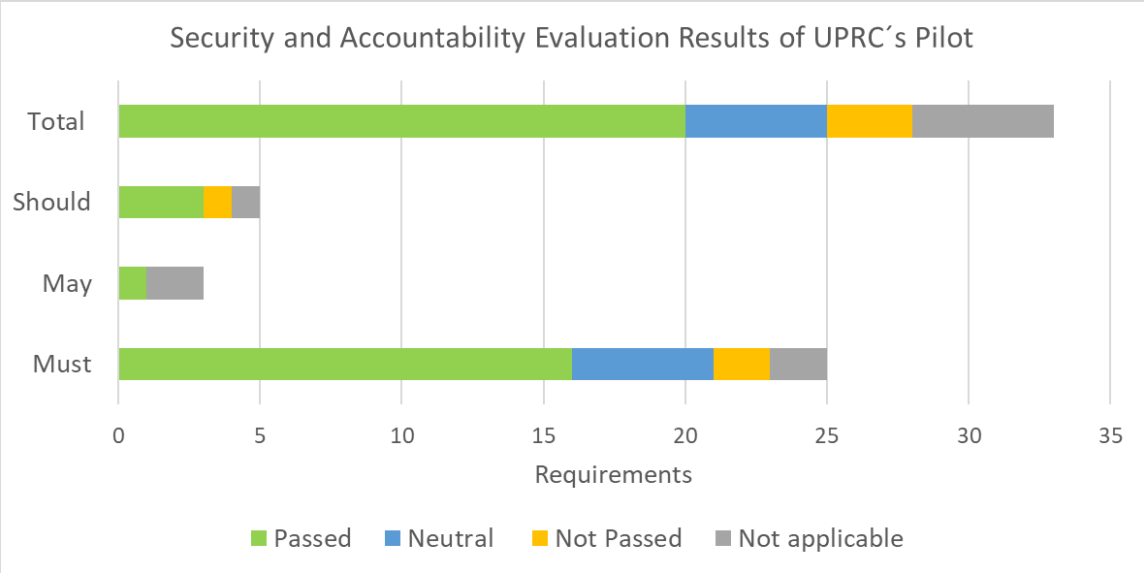

Figure 23: Security and Accountability Evaluation Results of UPRC´s Pilot

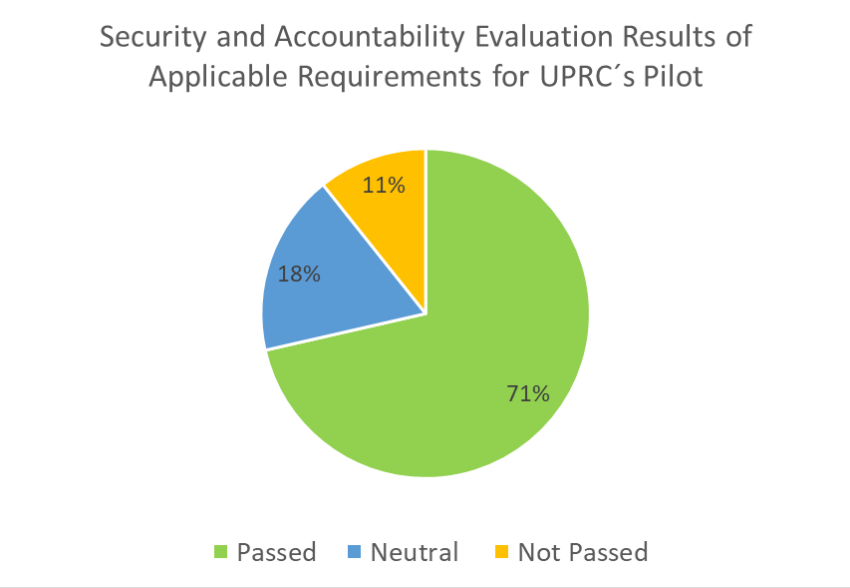

Figure 24: Security and Accountability Evaluation Results of Applicable Requirements for UPRC´s Pilot

9.5 Usability Requirements Evaluation

9.5.1 Implementation

Regarding the evaluation of the Implementation, there was positive results. Of 11 MUST Requirements, 10 were passed and 1 was Not Applicable. None of the MAY Requirements were applicable regarding the intention of the Implementation. The only SHOULD Requirement was passed. With that, below one can see that 100 percent of the applicable Usability Requirements were passed.

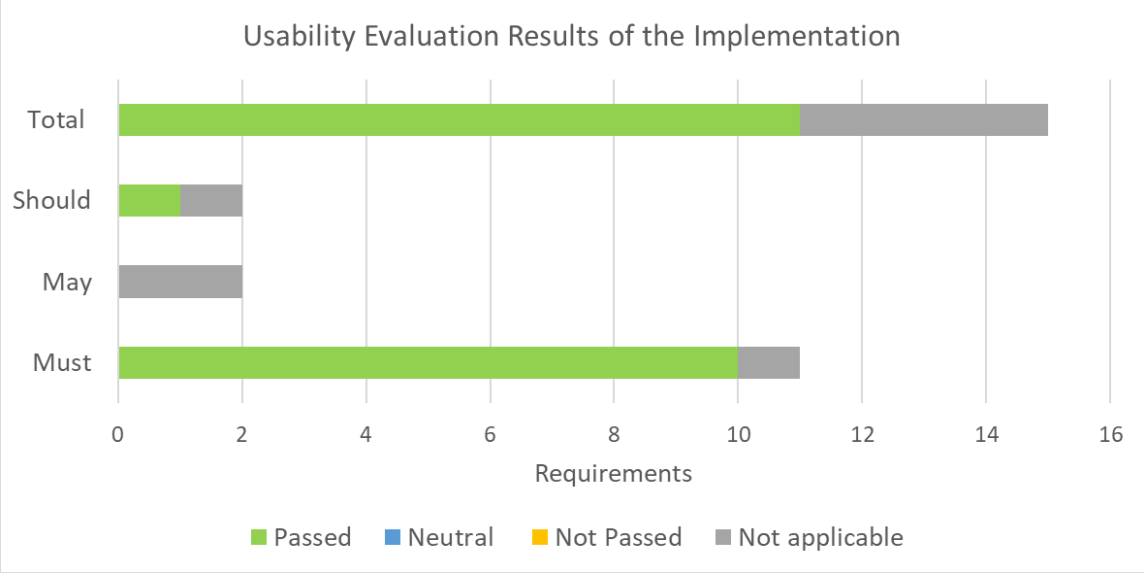

Figure 25: Usability Evaluation Results of the Implementation

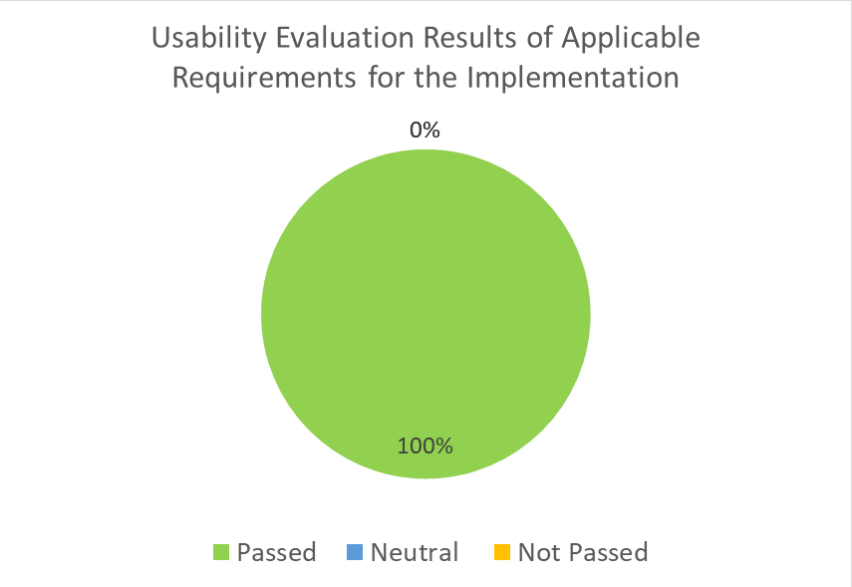

Figure 26: Usability Evaluation Results of Applicable Requirements for the Implementation

9.5.2 Correos Pilot

None of the Requirements were applicable regarding the intention of the Correos Pilot.

9.5.3 UPRC Pilot

None of the Requirements were applicable regarding the intention of the UPRC Pilot

9.6 Economic Requirements Evaluation

This section depicts overall optimistic results for the high level Economic Requirements. This section will give an overview of the evaluation results for the Implementation Artefact and each Pilot Artefact.

9.6.1 Implementation

Regarding the evaluation of the Implementation, there was positive results. Of the 12 MUST requirements, 10 were based and 2 were neutral. There were no MAY requirements. Of the 3 SHOULD Requirements, 2 were passed and 1 was Neutral. Overall, 80 percent of all requirements were fully passed and 20 percent were deemed neutral.

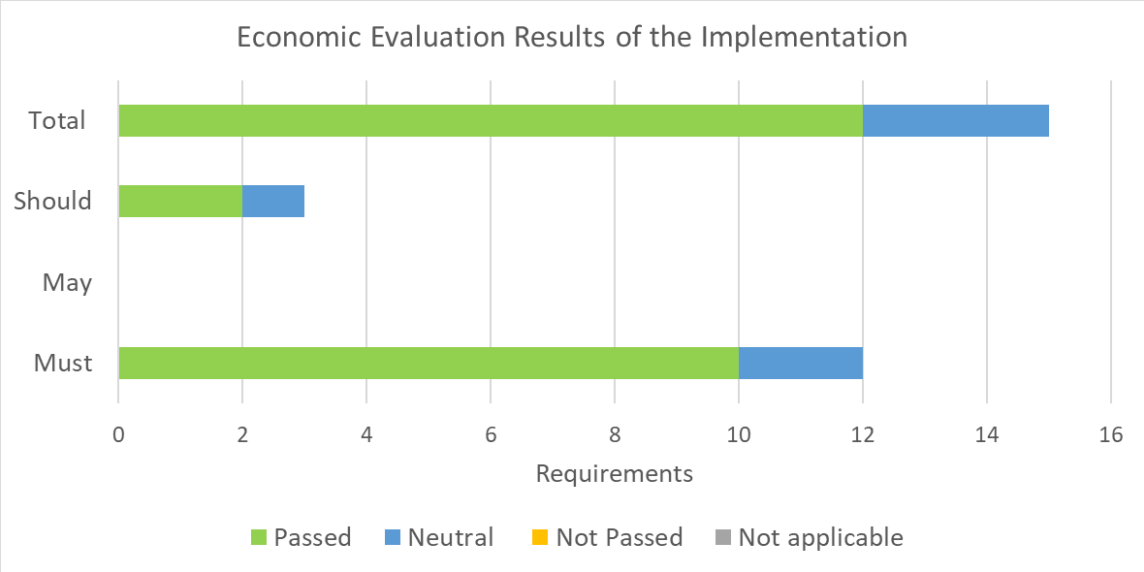

Figure 27: Economic Evaluation Results of the Implementation Overview

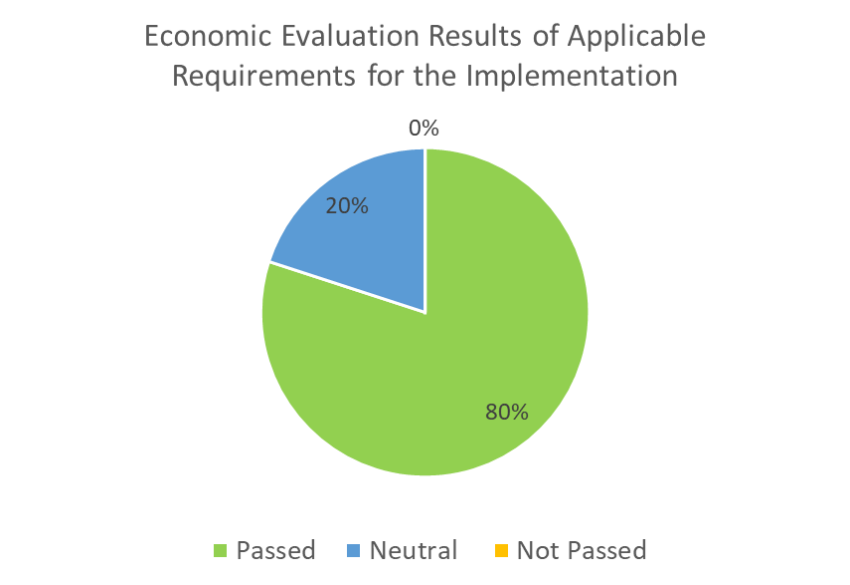

Figure 28: Economic Evaluation Results of Applicable Requirements for the Implementation

9.6.2 Correos Pilot

The Correos Pilot showed very positive results as all applicable requirements were deemed passed, including 3 MUST, 1 MAY, and 7 SHOULD requirements. There were 4 requirements that were deemed not applicable.

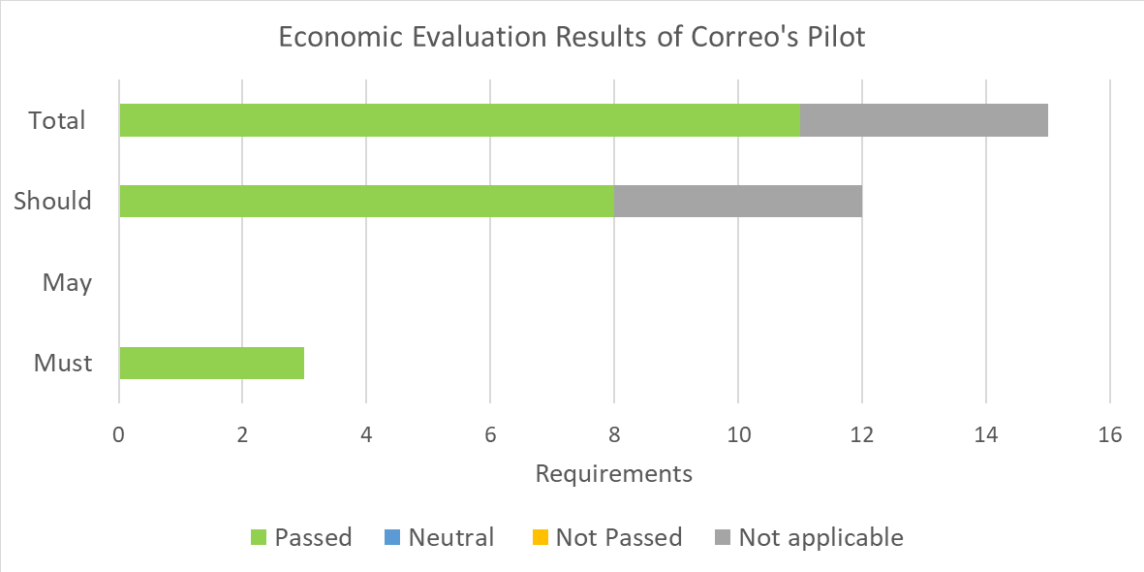

Figure 29: Economic Evaluation Results of Correo´s Pilot

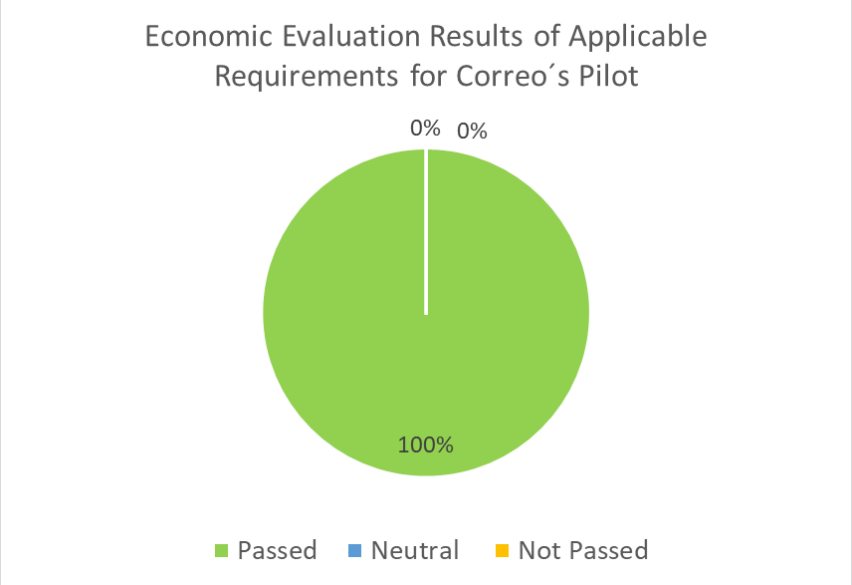

Figure 30: Economic Evaluation Results of Applicable Requirements for Correo´s Pilot

9.6.3 UPRC Pilot

The UPRC Pilot had postive results as well. All MUST requirements were passed. 80 Percent of the Applicable requirements were passed, 20 percent were rated as netural. There was 5 of 15 requirements that were deemed not applicable.

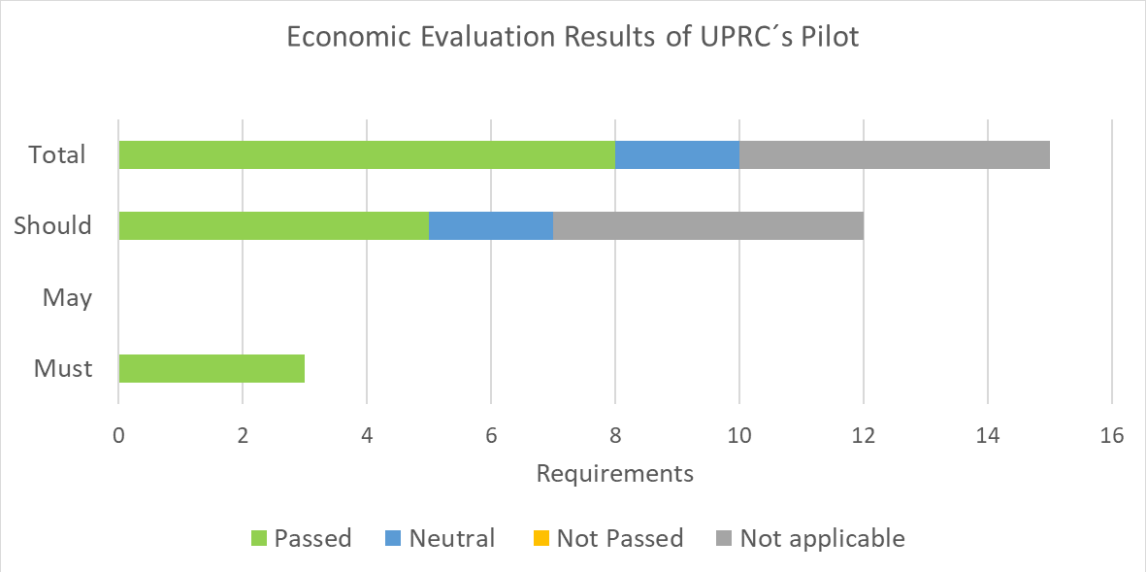

Figure 31: Economic Evaluation Results of UPRC´s Pilot

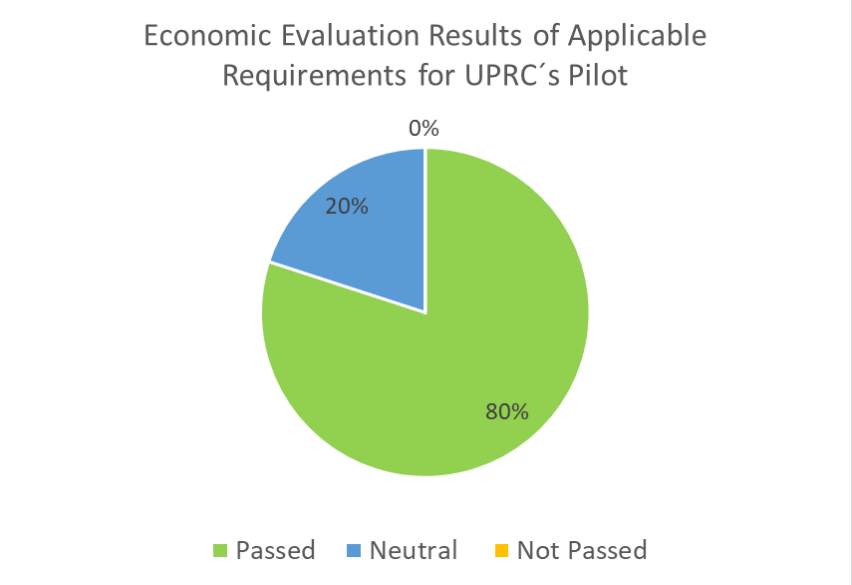

Figure 32: Economic Evaluation Results of Applicable Requirements for UPRC´s Pilot

10. References

Anon., 2012. *University of Twente - "Alphabetic list of Theories".* [Online]
Available at: http://www.utwente.nl/cw/theorieenoverzicht/Alphabetic%20list%20of%20theories/

ENSIA, 2015. *Privacy and Data Protection by Design.* [Online]
Available at: www.ensia.europa.eu/publications/privacy-and-data-protection-by-design

Freeman, R., 1984. *Strategic Management: A Stakeholder Approach.* s.l.:Cambridge: Ballinger Publishing Co..

idc, 2014. [Online]
Available at: http://www.idc.com/downloads/idc_market_in_a_minute_iot_infographic.pdf

J. Vom Brocke, A. S. B. K. R. A. C., 2009. *"Reconstructing the giant: on the importance of rigour in documenting the literature searching process.* Verona: s.n.

marketsandmarkets, 2013. [Online]
Available at: http://www.marketsandmarkets.com/PressReleases/personal-cloud.asp

Pouloudi, A., 1999. *Aspects of the Stakeholder Concept and their Implications for Information Systems Development," in Proceedings of the 32nd Hawaii International Conference on System Sciences, 1999, vol. 1999..* s.l.:s.n.

prnewswire, 2013. [Online]
Available at: http://www.prnewswire.com/news-releases/global-identity-and-access-management-iam-market-report-2013-2018-231458581.html

Projekt, S., 2013. *Skidentity Projekt Website.* [Online]
Available at: http://www.skidentity.de/

prweb, 2013. [Online]
Available at: http://www.prweb.com/releases/cloud-analytics/market/prweb10591613.htm

Sarodnick, F. & Brau, H., 2011. *Methoden der Usability Evaluation - Wissenschaftliche Grundlagen und praktische Anwendung.* 2 ed. Bern: Verlag Hans Huber.

smitherspira, 2014. [Online]
Available at: http://www.smitherspira.com/products/market-reports/security/personal-id/personal-identification-information-2019

strategymrc, 2014. [Online]
Available at: http://www.strategymrc.com/report/global-digital-signature-market-outlook-2014-2022

The LIGHTest Project, 2017. *D.2.3 Requirements and Use Cases.* s.l.:Project deliverable.

thepaypers, 2013. [Online]
Available at: http://www.thepaypers.com/e-invoicing-scf-e-procurement/e-invoicing-market-to-grow-at-a-23-3-cagr-by-2018-report/755088-24

University, B. Y., 2012. *Brigham Young University- "IS Theory".* [Online]
Available at: http://istheory.byu.edu/wiki/Main_Page

11. 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), Ubisecure (FI), and University of Piraeus Research Center – UPRC (GR). The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.