D2.3

Requirements and Use Cases

Document Identification	
Date	28.04.2017
Status	Final
Version	Version 1.0

Related WP	WP 2	**Related Deliverable(s)**	D2.2
Lead Authors	Rachelle Sellung (USTUTT)	**Dissemination Level**	PU
Lead Participants	USTUTT	**Contributors**	Please see List of Contributors Below
Reviewers	Hans Graux (TIL), Martin Hoffmann (NLNET)		

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

1. Executive Summary

This goal of this deliverable is to establish requirements and uses cases for the LIGHTest project. 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 potential 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 requirements will need to rank the level of importance in reference to each of these artefacts. The process and definition of these tasks will be elaborated in the introduction. With regards to the establishment of use cases, this deliverable will also entail a chapter dedicated to various use cases that could demonstrate the strengths and possibilities for LIGHTest.

2. Document Information

2.1 Contributors

Name	Partner
Rachelle Sellung	USTUTT
Michael Kubach	USTUTT
Stephanie Weinhardt	USTUTT
Benjamin Bader	FHG
Heiko Roßnagel	FHG
Lorenzo Rosa	ATOS
Alberto Crespo Garcia	ATOS
Miryam Villegas Jimenez	ATOS
Rosario M Encinas Bayan	CORREOS
Niels Pagh-Rasmussen	IBM
Muhammet Yildiz	TUBITAK
Elif Ustundag Soykan	TUBITAK
Burcin Bozkurt	TUBITAK
Melis Ozgur Cetinkaya Demir	TUBITAK
Edona Fasllija	TUBITAK
Berkay Topcu	TUBITAK
Çağatay KARABAT	TUBITAK
Charles Sederholm	GS
Sebastian Alexander Mödersheim	DTU
Sue Dawes	OIX
Peter Lipp	TUG

Stefan More	TUG
Jesse Kurtto	GS
Rasmus Birkel	DTU
Michelle Parkes	OIX
Georg Wagner	TUG
Jon Shamah	EEMA
Lorraine Spector	EEMA
Roger Dean	EEMA
Carlos Balot Toldra	CORREOS
Victor Martin Gonzalez de Haro	CORREOS
Javier Salazar Gomez	CORREOS

2.2 History

Version	Date	Author	Changes
0.01	01.10.2016	USTUTT	Outline of Deliverable
0.02	01.11.16		Partners started to developing methodology and requirements
0.03	28.02.17	ALL	Partners gave first draft of requriements for reference architecture
0.04	17.03.17	ALL	Partners provided first draft of all requriements and methodology
0.05	05.04.17	ALL	Final Methodology and Requriements
0.06	05.04.17	ALL, USTUTT	Insertation of Use Cases
0.07	07.04.17	USTUTT	Expansion of Use cases and Stakeholder Analysis
0.08	27.04.17	ALL	Instert reviewers comments and adaptations
0.09	28.04.17	USTUTT	Minor Corrections
1.00	27.04.17	USTUTT	Final Version

3. Table of Contents

3.1 Table of Figures

3.2 Table of Acronyms

API	Application Programming Interface
ATV	Automatic Trust Verifier
B2B	Business to Business
B2C	Business to Customer
BYOD	Bring your own device
CAA	Certification Authority Authorization
CAGR	Compund Annual Growth Rate
DA	Delegation Authority
DANE	DNS-based Authentication of Named Entities
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoA	Description of Work
DP	Delegation Publisher
DPD	Delegated Path Discovery
DPV	Delegated Path Validation
EAPO	European Account Preservation Order
EC	European Comission
ER	Economic Requirements
EU	European Union
FPKI	Federal Public-Key-Infrastructure
FR	Functional Requirements
FVEY	5 Eyes
G2C	Government to consumer
G2P	Government to people
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
ICT	Information and Communication Technology
IETF	Internet Enginering Task Force
IoT	Internet of things
IP	Internet Protocol
IPv6	Internet Protocol Version 6
MS	Member State
NGO	Non-governmental Organization
OCSP	Online Certificate Status Protocol
PKI	Public-key Infrastructure

PR	Privacy Requirements
RFC	Request for Comments (from IETF and ISOC)
SAML	Security Assertion Markup Language
SAR	Security and Accountability Requirements
SCVP	Server-based Certificate Validation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SWOT	Strengths, Weaknesses, Opportunities and Threats
TIC	Trust Infrastructure Consumer
TIP	Trust Infrastructure Provider
TLS	Transport Layer Security
TRL	Technology Readiness Level
TSPA	Trust Scheme Publication Authority
TTA	Trust Translation Authority
UI	User Interface
UR	Usability Requirements
US	United States
USA	United States of America
UX	User Experience
WP	Workpackage

4. Introduction

This deliverable looks to explore what basic high-level requirements are needed for LIGHTest. These high-level requirements should be seen as guidelines regarding what aspects LIGHTest should be aware of throughout the duration of the project. For a deeper more specific set of Requirements, please refer to the detailed requirements that are given in WP3, WP4, WP5, WP6, and WP7.

In order to achieve a wide and diverse spectrum of high-level requirements for LIGHTest, there are five identified categories. The five categories are the following; Functional Requirements, Privacy Requirements, Security and Accountability Requirements, Usability Requirements and Economic Requirements. Further categories of requirements regarding Societal, Legal and Ethical Requirements will be explored in Deliverable 2.10. 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 applied to 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. The Implementation artefact relies on what is achieved in work package 6. 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. Each of the requirements mentioned in this deliverable, regarded each of these artefacts on the LIGHTest Requirements Wiki. This Wiki will be used through out the entirety of the project and succeed as the living version of the requirements as the LIGHTest Infrastructure develops.

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.

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

With that, the structure of the deliverable will proceed as follows. Each category will be presented with a sub section that explains their methodology and their structure, along with a sub section dedicated to the requirements at this stage of the project. The order of the categories in the deliverable are: Functional Requirements, Privacy Requirements, Security and Accountability Requirements, Usability Requirements, and Economic Requirements. After the requirements, there will be an overview of the market, an early stakeholder analysis, and a uses cases that will follow.

5. Functional Requirements

The Functional Requirements were constructed in a fairly simple and organized manner. They were derived and built off of the guidelines and necessary functions defined for each component defined in the Reference Architecture, D2.14. With that, the requirements are defined as applying to sub-categories of the architectural components. The regarded 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. This was done due to the fact that the LIGHTest Infrastructure builds on the existing DNS infrastructure and therefore has some limitations due to functional abilities. Further, the basic LIGHTest Infrastrucuture was already approved in the proposal phase and the general functionality of it. With that, the proceeding functional requriements set to provide a guidline of functionality along with maintaining the constraints of the already existing DNS infrastrucuture and what was agreed upon in the proposal phase.

5.1 Requirements

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

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

No.	FR-02.01- DP: Trust List Flexibility
Description	LIGHTest components MUST be able to publish multiple delegations under different sub-domains of the organization’s domain name

No.	FR-02.02- DP: Utilities to Load selected Delegation Data
Description	The utilities parse (as described in D2.14) 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

No.	FR-02.03- DP: Interface

Description	The delegation publisher MUST provide an interface to create and edit delegations. The interface could either be a GUI or an API.

No.	FR-02.04- DP: Multiple Formats
Description	The delegations publisher MUST be able to publish delegations of different formats.

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

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

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

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

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

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

No.	FR-05.00- TSPA: 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

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

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

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

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

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

No.	FR-06.03- TTA: Formats
Description	The Trust Translation Publisher MUST be able to accept trust translation lists of all the required formats, such as Boolean, ordinal, and tuple-based.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

No.	FR-10.04- Mechanisms for Derived MobileIDs
Description	Provide mechanisms SHOULD derive trusted mobile identities from other credentials such as government eIDs.

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

6. Privacy Requirements

The methodology we follow to gather the privacy requirements is based on the principles set out in the EU General Data Protection Regulation.

We recognize that in the LIGHTest infrastructure itself no personal data collection will occur. Any personal data processing will be purely incidental and limited to special cases like delegations and the parsing and verification of transactions in the Automated Trust Verifier; even in such cases, the LIGHTest infrastructure is a tool that may lead to personal data processing outside the infrastructure and outside the context of the LIGHTest project, rather than as an inherent part of it. Therefore, we focus on a minimum set of requirements that can reliably cover these special cases.

The strategy is based first on an analysis of the text, with the aim of identifying broader categories of requirements set out in the single articles of GDPR, which provide the justification for each category. This led to the identification of 10 principal categories of requirements, and these categories are used as models to group the requirements in a homogenous and coherent way. In particular, we have followed the Privacy by Design principle of the GDPR in this project by: (i) implementing proper security measures within the infrastructure and (ii) performing assessments on privacy requirements, and providing an assessment framework for any pilots that will use the LIGHTest infrastructure (which can be used both for the LIGHTest pilots themselves and for any use cases outside the LIGHTest context).

In addition to the GDPR-related principles, we also include in the framework the complementary privacy goals of “unlinkability” and “intervenability” [1], to reflect privacy concerns more clearly. In particular, the unlinkability principle “is defined as the property that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context.”The intervenability principle “is defined as the property that intervention is possible concerning all ongoing or planned privacy-relevant data processing.” [1]

The second step will be to review the architecture, components, and use cases and identify the emerging requirements according to each category. This will be followed by a revision and pruning of the requirements list, to obtain the minimum achievable set. This will be done by merging similar requirements of different components and use cases and considering the ability to reach each requirement in the project time frame, justified by taking into account the target use cases for the pilots, the exploitation outcomes sought, and the TRLs set out in the DoA. (ENISA, Janurary 2015)

6.1 Requirements

No.	PR-01.00- Privacy by design
Description	The LIGHTest 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 LIGHTest 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 organisational 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.

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.

No.	PR-02.00- Privacy by default
Description	Any personal data Controller within LIGHTest boundaries MUST implement appropriate technical and organisational 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.

No.	PR-02.01- Privacy-friendly settings
Description	As a corollary of the Privacy by default requirement, 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.

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

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

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

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

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

No.	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 organisational measures required by GDPR in order to safeguard the rights and freedoms of the data subject.

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

No.	PR-05.01- Owner explicit delegation
Description	When a delegation process is implemented, actors MUST explicitly be involved in it.

No.	PR-05.02- Limited re-delegation
Description	Delegations SHOULD NOT be delegatable in turn, unless strictly required by the nature of the service provided and with the consent of the original actor.

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.

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

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

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

No.	PR-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.

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.

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 defence of legal claims.

No.	PR-06.04- Right to data portability
Description	The Data Subject shall 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.

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.

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.

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 unauthorised or unlawful processing and against accidental loss, destruction or damage; the Data Controller MUST implement appropriate technical and organisational 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.

No.	PR-09.01- Anonymization for statistics
Description	Data SHOULD be anonymized, if applicable, prior to being processed for statistical analysis

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.

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.

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.

No.	PR-09.05- Private policies
Description	Authorization and delegation policies/preferences stored in LIGHTest SHOULD NOT reveal information regarding the actors.

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 only take place under the circumstances defined in the GDPR.

7. 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, 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 by protocols like TLS, DNSSEC, and DANE, without opening additional vulnerabilities. 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 later 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 SAR 3.XX 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 every other requirement among the SAR is associated to exactly one of the principles, and becomes, in a sense, a sub-requirement. 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.

7.1 Requirements

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, DANE.

No.	SAR-01.01- Confidentiality: Secure Channel
Description	(Confidentiality – Secure Channel) Lightest Services should communicate on secure channel in order to protect channel data from eavesdropping

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.

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.

No.	SAR-01.04- Confidentiality: Key Material/Credential Protection
Description	Lightest services must enforce all secret key materials and credentials are held confidential at rest.

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.

No.	SAR-01.06- Confidentiality
Description	Any confidentiality issue that occurs in one Lightest component must not affect other Lightest components.

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.

No.	SAR-01.08- Integrity: Error Handling
Description	Lightest components must detect a data and system integrity error and make it possible to 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 threats.

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).

No.	SAR-02.01- Integrity: Component Relations
Description	LIGHTest components must ensure that breaking the integrity of one system component will not lead to integrity failures in other components.

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.

No.	SAR-03.01- Logging and Auditing
Description	The LIGHTest system components MUST establish a logging and auditing infrastructure that is able to audit system and component failures. The logging and auditing infrastructure MUST be in accordance with privacy regulations and requirements.

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.

No.	SAR-03.03- Logging and Auditing:Access rights
Description	All LIGHTest components that generate audit records MUST only allow read access to these records to entities that have been granted access explicitly.

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.

No.	SAR-04.00- Availability
Description	Protection against classical denial of service attacks SHOULD be achieved to the level provided by protocols like TLS, DNSSEC, and DANE, without opening additional vulnerabilities. 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.

No.	SAR-04.01- Availability: Failover Backup
Description	LIGHTest system components that do not have an emergency operation mode as specified in SAR 4.02 must have a Failover backup mechanism. There must be a failover system to take over functionality in the event of a component failure.

No.	SAR-04.02- Availability: Emergency Operation Mode
Description	LIGHTest system components that do not have a failover backup mechanism as specified in SAR 4.01 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.

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.

No.	SAR-04.04- Availability: Execution Power
Description	Deployed LIGHTest components must have sufficient computing power to perform their function.

No.	SAR-04.05- Maintenance
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.

No.	SAR-04.06- Availability: Single Point of Failure
Description	The LIGHTest system SHOULD not have single points of failure.

No.	SAR-05.00- Accountability
Description	Any LIGHTest component that makes decisions (trust decisions, issuing certificates) MUST later 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 SAR 3.XX requirements for storage.

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.

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.

No.	SAR-27.00- Authentication
Description	The Delegation Publisher MUST provide a means of authenticating the delegations before they are published

No.	SAR-27.01- Authorization
Description	Only authorized personnel can edit or publish delegations

8. Usability Requirements

Usability is the extent in 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 considerd. Crucial guidelines, considered in the Usability Requirements in 8.1, 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)

8.1 Requirements

No.	UR-01.00- High Usability
Description	Usability and understanding of services and applications SHOULD be a main benefit to the End-Users. Given that End-Users, may have a wide range of competence with this technology it is important to make it as simple and usabile as possible.

No.	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.

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

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

No.	UR-03.00- Commonality of Language
Description	Ensure that global language requirements are taken into account, including languages that use special characters.

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

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

No.	UR-05.00- User Experience

Description	Building on Usability, the LIGHTest Project should consider User Experience to guarantee good user acceptance. Especially the basic human needs security and competence are important factors in designing a security system. Ideally the System is able to adress those Needs to create a good User Experience.

No.	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.

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

No.	UR-08.00- Transparency
Description	There is no need for the user to understand to whole system and every little detail that happens in the background. But the system UI must be transparent enough so the user can understand the overall concept and therefore understand what's happening and what he/she is supposed to do. At any given point the system should be transparent enough whilst not overstraining the user.

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

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

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

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

9. 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 (SkIDentity-Project, 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. These two items can be seen at length in section ten of this document. 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 stake holders. The Economic Requirements in this deliverable constitute as a guideline for the development of LIGHTest. At the end of the project, they can serve as a tool to evaluate the project results.

9.1 Requirements

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

No.	ER-01.01- 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.

No.	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

No.	ER-01.03- Support for various pricing models and strategies
Description	The willingness to pay by different users varies, depending on the use case. In order to build a sustainable business model, users and providers have to be approached in different ways / levels in order to absorb their willingness to pay. Therefore, LIGHTest MUST support price differentiation according to the different willingness to pay individual stakeholders for the different applications.

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

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

No.	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.

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

No.	ER-03.02- Support of Exisiting 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 exisiting works.

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

No.	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

No.	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 Requriements.

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

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

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

10. Overview of Market, Stakeholder Anaylsis, and Use Cases

The LIGHTest Infrastructure is a technology that can be used in many different respects. It is a tool that can be applied to many different industries and applications. While it is still relatively early in the project, all of the added values or purposes of the Use Cases are not as distinguished. The following section will simply highlight an overview of the potential markets of interest for LIGHTest, an Early Stage Stakeholder Analysis, and a wide range and variety of differnet Use Cases for LIGHTest.

10.1 General Functions of LIGHTest

The general functions of LIGHTest, Trust Services, Trust Translations, and Trust Delegation. These three basic functions can be applied in a multitude of different ways and in various channels.

For Trust Services, LIGHTest can be used to verify published information on Trust Lists. The published information could be names, certificates, objects, things, basically anything. The Trust List, is a list of items that could be verified. For instance, if we wanted to verify that person XYZ has a Drivers Liscence in USA, it would be possible to use LIGHTest to check the published list 'List of Valid Drivers Liscence in the USA' that was published by the USA Department of Motor Vehicles. This function uses the Trust Publication Authority (TSPA).

For Trust Translations, LIGHTest can be used in a cross borders or translation scenario where some items may transfer into a different kind of item in other scenarios. Simply said, this would imply that object A on List 1 would be translated to object 2 on List B. For example, if the University of New York gave Max Mustermann a final grade of a 4.0 in the USA, which is equivilant to an A., this could be translated using LIGHTest Trust Translation services into the German Education Scale of a 1.0, which is equivelant to an A in Germany. This function uses the Trust Translation Authority (TTA).

For Trust Delegation, LIGHTest could be used in a variety of delegation scenarios or simply to check or verify the delegation. An example of this function, would be to check if an employee has the delegation rights from a company to purchase items in the companies' name. LIGHTest would check if the employee is on the Companies published Delegation list of Employees with Purchasing Rights. This function uses the Delegation Authority. (DA)

10.2 Overview of Potential Markets of Interest

There is a diversity of potential markets with a lot of agile global players for the LIGHTest project, which shows the range and importance of it in a clear way. The aim is to realise the opportunities and to avoid the threats to generate a high level of benefit. Further, we see that LIGHTest can be very well suited for facilitating trust publication, validation and translation in any ICT domain and that we reasonable expect growth figures in these domians to reflect the potential of LIGHTest. With that, this section depicts and overview of potential markets, their

size, opportunities, threats and main players, the following examples are presented are based on a SWOT-analysis that was done in the proposal phase:

In the market of 'Identity and Access Management software (on premise, cloud and hybrid)' an expected growth from 2013 to 2018 makes 15.1%, running at 7300 million euros only in 2018 (prnewswire, 2013). Increasingly growing usage of web/cloud-based applications as well as user convenience and cost reduction give a lot of opportunities of further development to this market. Restraints may be found in trust in eDAS providers and in integration and compatibility requirements i.e. for federated Single Sign-On and acceptance of multiple credentials. Among the main players in the market are i.e. Oracle, Dell, Intel, Siemens, HP, ATOS.

An estimated compound annual growth rate (CAGR) of the market 'Cloud / Big Data analytics' from 2013 to 2018 is 25.8%, growing up to 11550 million euros by 2018 (prweb, 2013). Cost advantage as well as easy installation and fast deployment are the most important drivers of this market. Another trigger of this progress is growth of structured and unstructured data in the area. Nevertheless, trust issues and security and data availability can come up as restraints in the market. Major players in this market are Birst, Kognitio, Adaptive Planning, IBM, HP, Oracle, BIME, Cloud9 Analytics, GoodData, Google, Host Analytics and Microsoft.

The market of 'Personal cloud' shows CAGR of 45.61% from 2013 to 2018 (marketsandmarkets, 2013). Such opportunities and drivers as making personal cloud appealing to business users, remote access, BYOD and mobile workforce, as well as the need to address privacy and security make this market particularly active and expanding. Alongside the above-mentioned advantages that provide success to the area, the market has some restraints, among which vendor lock-in, interoperability and bandwidth can be named. The 'Personal cloud' market consists of such major players as Amazon, Apple, Google, Seagate, Box, Microsoft, Dropbox, Engyte, Buffalo Technology, and Sygarsync.

'E-invoicing (eProcurement)' market has an expected growth of 23.3% from 2013 to 2018 (thepaypers, 2013). Cost savings, greater transparency, as well as enhanced Inventory Management and shortened Communication Cycle Times let the market expand further. However, resistance to change and lack of widely accepted solution are some of the biggest restraints to the introduction of e-Procurement to the public sector. Ariba, ComerceOne, Oracle, SAP, IBM are the main players in the market of 'E-invoicing (eProcurement)'.

In the market of 'Secured digital communication & communication', especially in the area of eID, eDelivery and related markets, from 2014 to 2019 an expected growth is 2.6%, growing up to 9.1 billion dollars annually (smitherspira, 2014). Such opportunities as developing financial services based on eIDs, integration of online and offline experiences in the Internet of Things, and revenues on new services based on eID, eDelivery, eProof, etc. are the main triggers of growth of this particular market. However, there are risks that it may be difficult or not possible at all to adapt quickly to new opportunities and to earn the trust in Digital Security Services. Major players in this market are postal operators, express mail companies, financial services (major banks), and eRetailors (Amazon, Alibaba).

Regarding the potential market 'Digital signature in dematerialization', its CAGR makes 6.17% (as of 2014), reaching 25.37 billion dollars by 2022 (strategymrc, 2014). Cost reduction, increased efficiency, throughput and competitiveness, as well as improved usability and security are the main drivers and opportunities that ensure progress of this market. Nonetheless, there are also some restraints to its development: integration with existing systems, acceptance of B2C and B2B, implementation cost, legal basis and security issues. The major players in the 'Digital signature in dematerialization' market are Opentrust, D-Trust, Adobe Echosign, ARX CoSign and DocuSign.

'Internet of Things' market expect an annual growth rate of 17.5% from 2014 to 2020, reaching 28.1 billion dollars in 2020 (idc, 2014). Such opportunities and drivers as the necessity to manage trust of participating de-vices at very large scale and to establish trust across organization boundaries as well as the support for applications that are naturally global stimulate market growth. The restraints here might be scalability, interoperability of trust management solutions and security issues. The 'Internet of Things' market consists of such major players as ARM, Bosch, Cisco, Ericsson, General Electric, Google, Atmel, IBM, Intel, Microsoft, Oracle, PTC, SAP, etc.

10.3 Early Stage Stakeholder Analysis

This section will elaborate on the starting development of the stakeholder analysis for LIGHTest. We anticipate that this analysis will develop and become clearer as the project progresses. This section will lay out some founding methodologies that were considered and the process. As stated above, this analysis is expected to be further developed in WP10.

10.3.1 Core Literature Methodology

Stakeholder analysis shifts the focus of research from isolated artifacts (e.g. the organization) towards the entities it depends on. Following (Freeman, 1984), a stakeholder can be defined "in an organization" as "any group or individual who can affect or is affected by the achievement of the organizations objectives" (Freeman, 1984). (Pouloudi, 1999) mentions, that by this definition the relationship between stakeholders and organizations "marks a double line of influence", since the "organization reacts to environmental influences, which means that the position of the stakeholders is affected by the decisions taken by the organizations in question " and the stakeholders, being active elements in this organization influence the organization "according to their interests and use their power to influence the organization in the direction they desire" (Pouloudi, 1999). By following this definition one is able to examine the "external organizational environment" and to explore "how an organization can manage multiple stakeholder relationships" (Pouloudi, 1999). This allows for derivations, such as shaping management decisions. Since different stakeholders shape and direct the organization according to their own needs, managerial decisions "should not be exclusively based on the requirements of either the managers, or the stockholders, or the customers. Instead "an ethical organization should take into account the interests of other stakeholders who are affected by these decisions" (Pouloudi, 1999). In (Pouloudi, 1999) different aspects of the stakeholder theory are being introduced, including descriptive, instrumental and normative views on stakeholder analysis:

Descriptive

Describes an organization and enables for analysis of “the corporation as a constellation of cooperative and competitive interests possessing intrinsic value” (Pouloudi, 1999).

Instrumental

Connections between the “practice of stakeholder management and the achievement of various corporate performance goals” (Pouloudi, 1999) can be examined, if any exist. This also includes the definition of the relationship between stakeholders and organizations, as a “double line of influence” (Pouloudi, 1999).

Normative

Forms the basis for stakeholder theory, by accepting the following ideas: “stakeholders are persons or groups with legitimate interests in procedural and / or substantive aspects of corporate activity and the interests of all stakeholders are of intrinsic value” (Pouloudi, 1999).

10.3.2 Approach

The approach of stakeholder analysis can be very interesting for Trust Management, since these technologies are not isolated artefacts, but rather entities which benefit and suffer from its surrounding ecosystem. Therefore, stakeholder analysis is an important and thus considerable approach for analyzing the market potentials for electronic Trust Management.

Some of the main benefits of developing and establishing a stakeholder analysis is to be able to identify the the key players or participants for this LIGHTest Infrastrucuture and technology. The stakeholder analysis in this deliverable, is considered to be a simple stakeholder analysis.

First, it is important to start the process of identifying the stakeholders. Second, it would be necessary to start to go deeper into understanding the different identified stakeholders and to start mapping and understanding their position for LIGHTest. This could include but is not limited to evaluating their degrees of influence, degree of importance, and their evaluating their points of interest and prioritizing them. Third, in order to strengthen the analysis it would be beneficial to directly interact with stakeholders and to reevaluate the analysis and potentially consider a more modelled framework of analysis as conducting an Expected Stakeholder Model.

Until now, we have defined three groups of stakeholders, which can be seen in Figure 1 below. First, we have the Active Stakeholder, who are stakeholders that take part in the LIGHTest Technologies. This implies that they are either apart of the ‘consumption’ of LIGHTest services, where they use the LIGHTest Infrastructure. Further, they could be apart of the ‘providing’ aspect of LIGHTest Services. This implies that they are either providing the LIGHTest Infrastrucuture, which entails the maitenence and continuous development of LIGHTest Infrastructure or be a provider as in a Provider of the LIGHTest Services to the LIGHTest consumers. Second, we have Enabling Stakeholders, who add or provide to the expansion and use of the LIGHTest Technology. In detail, this relies on those who would be apart of dissimenation of the the technology, such as, the media. In other terms, this could be Public Institutions that make a policy, subsidy, or a kind of regulation that would ‘promote’ or nudge consumers and providers into using the LIGHTest Infrastructure. Third, we have internal stakeholders, who are involved in the creation and establishment of LIGHTest. Of course, there are many ways to distribute the different types and categories of stakeholders, however, for this stage of the project this seems like the first analysis of what the potential stakeholders could be.

Figure 1 Overview of Stakeholders

10.4 Prospective Use Cases for LIGHTest

This section first elaborates on the process used to understand and to test each use case that is listed. Following is a list of use cases, along with a brief descriptions. Future use cases will be added to the LIGHTest wiki and further analysis may be extended in WP10.

When understanding each use case, we depicted three roles that are important to verifying a use case. These three roles and their relationships are important in the establishment of a use case. They correspond with the Stakeholders found in the Stakeholder Analysis in section 10.2. As seen in the Figure 2 below, the three roles are; Trust Infrastructure Provider, Trust Infrastrucuture Consumer, and End Consumer.

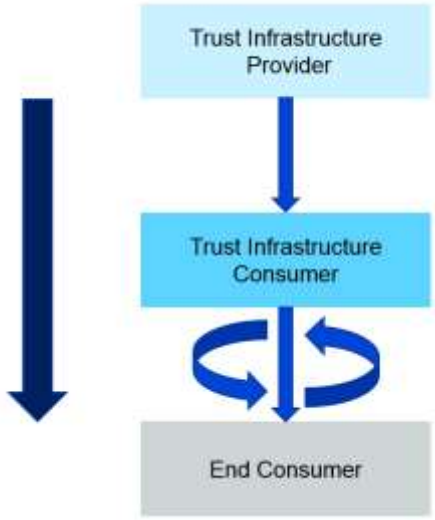

Figure 2 Active Stakeholder Roles and Relations

First, the Trust Infrastructure Provider would have the role of providing the LIGHTest technology as a service. This would imply that they are in control and responsible for the implementation of LIGHTest into their trust services. The Trust Infrastructure Provider (TIP) is in control of providing the technical aspects of the LIGHTest Infrastrucuture technology. The technical aspects are in regards to the basic functionality of LIGHTest Infrastructure. The TIP is not responsible for collecting the information or trust lists, but to just to provide a means of how to use them in the LIGHTest Infrastructure. The involved Stakeholders in the TIP are those in the Active Stakeholders and Trust (Infrastrucuture) Provider section.

Second, the Trust Infrastructure Consumer (TIC) is the consumer of the LIGHTest Infrastructure, but a provider to the End User. Further, it is in the role of providing the trust lists that is refered to in the LIGHTest Infrastructure. The TIC is the direct face to the End User. The Trust Infrastructure Provider and the Trust Infrastructure Consumer can, but does not need to be the same entity. The involved Stakeholders in the TIC are those in the Active Stakeholder and the End Consumer section OR the Trusted Entities (the End Consumers) in the stakeholders of the Trusted (Infrastructure) Provider section. Simply said, this is a role that can be tied into either of the other roles or stand alone.

Third, the End User is who ever is using the provided service. They are not involved in the technical funcitionality of the LIGHTest Infrastructure, but simply use the provided services. The involved Stakeholders in the End User are the Active Stakeholders and the End Consumer.

Following is a list of the potential Use cases for LIGHTest. They are organized by whether they are aimed at Private, Public Sector, and both. This is a list of potential use cases that were established in an early stage in the project. With that, there are many other use cases that

LIGHTest is expected to attribute to. Within the scope of the project, LIGHTest will test the use cases in the two pilots; e-Correos and e-Procurement. In addition, LIGHTest will be tested in the Predictive Maitnence use case.

Regarding the Use Cases themselves, there are some trends that can be noticed when observing the use cases for the LIGHTest Infrastructure. First, the LIGHTest Infrastructure is a tool that is for optimizing a process or an existing organizational structure. It is not a tool that is set out to re-establish or replace some process or technology, but to make it more efficient, convenient and flexible. The LIGHTest Infrastructure sets to highlight the Pareto Optimum. This is to be extended and further developed as the project continues and in WP10.

Please find below a first collection of use cases for LIGHTest.

1. Private Sector	Access Control for IoT and Assisstants Data
Description	Publish a list for 'Trusted Information Agents' that are associated with different services and applications of what has permissable access to supply or review data Plaintext: Control the Data that different IoT devices or Assisstants are sharing or communicating with one another. Works for providing and rejecting Access (TSPA)

2. Private Sector	NewsTrust
Description	News Trust provides a chain of trust for news stories to ensure that a news item comes from a trusted source. As a news item is generated it is signed by the originator. If the item is utilised by a news service, it can examine the trust chain from the origination and determine if the path is via trustworthy agencies. This implies that every news agency has the ability to verify its source rather than blindly repeating a story that it receives. In greater detail, there would be ‘first hand’ or primary news source agencies that would provide a list of their trusted sources. With that, the end readers or secondary news agencies could then verify the articial and whether it came from a trusted source. (TSPA)

3. Private Sector	Purchasing Order
Description	Companies often delegates the permission to sign for a purchasing order in their name to employees of certain positions or rights. This process could be checked through LIGHTest and the Delegation Authority, to make sure that the employee is on the delegated list of the Companies. LIGHTest Component: (DA)

4. Private Sector	Trust services for the credit card industry
Description	The credit cards industry was built up on a contractual basis by the banking industry, which also built aits global infrastructure for it. LIGHTest can be effectively promoted as a flexible infrastructure to validate the communications between the business partners in a cross-border environment and validate trust in credit card transactions. Trust services involved: eID, eSignature, eSeal, eTimestamp, Web certificates. (TSPA, TTA)

5. Private Sector	Shipping Insurance and other shipping documentation
Description	In regards of the shipping industry, LIGHTest could assist in the process verifying shipping insurance. Specifically when it comes to container insurance, which needs a variety of different insurances and other forms of documentation in order to ship to different ports world wide. For instance, one could check each container and see who it was insured by, where it is shiping from, when, and other informations. It could make use of lists, such as, Lloyds List of Intelligence service and others. (TSPA)

6. Private Sector	Predictive Maitenence
Description	In the use case “end to end sensors” authentic sensor data are generated and transferred via Industrial Data Space (Industrial-Data-Space-e.V., 2017). Within this use case, there is a scenario “predictive maintenance”, which describes a business process using these sensor data for pre-emptive maintenance decisions. This means the supplier can react to a possible problem with a manufacturing system before an actual failure of the system occurs. The supplier can react earlier by e.g. ordering spare parts or sending out a service technician to adjust machine parameters to prolong the machine’s lifetime and/or reduce the machine’s downtime. The advantages of “predictive maintenance” require some additional and specific security measures. When sensor data leaves the manufactures domain, it has to be guaranteed that no production details are transmitted. Therefore, before transmission a filtering of the data is required to provide only the necessary data for the supplier. In addition, the communication flow between the manufacturer and the supplier has to be confidential, integrity protected and authentic. In many cases a manufacturing system was constructed and is maintained not only by one but by several suppliers. In these cases it is important that each supplier can access his own and only his own sensors. For this purpose, an access control verifier is required to assign sensor and corresponding supplier. (TSPA)

7. Private Sector	Trusted Billing
Description	In perspective of B2B, Mega+ corp. is a customer of ACME Inc. with monthly billing. Unexpectedly, Mega+ receives an ordinary looking invoice from ACME, but with the bank details changed from an account in Germany to an account in Panama. This

	change would be trivial to be flagged and then subject to automatic verification against the list of trusted banks from ACME. This is very similar to DANE and the DNS CAA extension (*mandatory after Sep 2017*) for the WebPKI This Use Case could be further used in situations of G2C or G2P (TSPA)
8. Private Sector	e-Procurement Pilot Use Case
Description	The E-Procurement Pilot integrates LIGHTest in a PEPPOL e-Invoicing infrastructure and application sce-nario where IBM will be responsible for inclusion of the applications that are relevant for the pilot scope. IBM is at present using the IBM PEPPOL services for its own e-invoicing--which gives room for use of flexi-ble scenarios. PEPPOL is the EU e-invoicing infrastructure and is very appropriate for setting up and running pilot scenarios with LIGHTest components that are meant to be 'built-in' either as a Gateway service or di-rectly in the application systems which have chosen to use PEPPOL as their prime infrastructure. The LIGHTest service will be activated and integrated in different pilot scenarios. The pilot will (i) demonstrate the ease of integrating LIGHTest in existing applications and gateways, (ii) ex-plore the alternatives of integrating LIGHTest as a business application feature or as a service from a PEPPOL or eSENS GW, (iii) and demonstrate the delegation-enabling of an application. For the latter purpose LIGHTest will be used validate seals directly, as well as use delegation based on LIGHTest delegation publisher operated by a business register as well as a by the invoice issuer to authorize its employees to issue invoices. (TSPA, DA)
9. Private Sector	Data Traffic Routing
Description	As the new GDPR legislation is coming into effect next year, digital privacy is going to have an unpreceded role for any company operating in the EU or handling EU citizens' personal information. With LIGHTest, it would be possible to control that data is only transmitted within the EU. Companies' web applications could follow a published list of routes for the data, ensuring that the new regulation is complied with. From a technical perspective, this is an opportunity to implement secure IP source routing in IPv6. The older IPv4 standard itself has source routing built in, but it is disabled by default due to severe security issues. The trust list would dictate a mandatory, trusted route. This would help managing ever growing Internet traffic, ensure that data never leaves the EU and even keep private data out of the FVEY (5 Eyes) analytics dragnet. (TSPA)
10. Public Sector	Business register
Description	In Europe and other countries, the source for business mandates are business registers. SMEs lose money due to other companies refusing to pay invoices, because they were signed by a person not registered as representative; LIGHTest

	can avoid this by leveraging the value of DNS. LIGHTest can exploit the flexibility of the business register and stress that it is making the business register functionality available and expanding it. LIGHTest can offer a level of trust at least the same as DNSSEC registration. The business model would be to offer extended validation services, and it could be built on top of the LIGHTest infrastructure. Trust services involved: eSignatures, eSeals. Related to the Purchasing Order Use Case. (DA)

11. Public Sector	eVoting
Description	Electronic voting is a trending topic of discussion for many countries and states, especially in the sense of online voting as it would make voting much more convient for many citizens. However, in order for electronic voting to work a trusted system is needed and this system could be LIGHTest. (TSPA)

12. Public Sector	US Federal PKI trust chain generation
Description	This use case shows how one can be the trust chain between two FPKI end-points as a supplement to existing SCVP. Currently the Federal PKI has a large number of servers and the pathway between any two end-points can traverse many servers belonging to many agencies. In order to manage the revocation, the SCVP protocol is used. (IETF RFC 5055 and RFC 5276). This path discovery uses the SCVP tool from HIDGlobal. However the rules management is very basic. It is envisioned that LIGHTest might be able to supplement that product "ActivID Validation Authority - Delegated Path Discovery (DPD) and Delegated Path Validation (DPV)" with advanced rules mediation and might be incorporated into the product. The suggested route would be liaison with HIDGlobal to explore the potential use-case further. (TSPA)

13. Public Sector	LIGHTest-eSENS-eConfirmation Use Case
Description	The e-SENS e-Confirmation domain use caseconsists of the cross border issuance and verification of a Provisional Replacement Certificate for a patient who applies to a medical facility in a need for medical treatment. For instance, there could be a check of what is covered by the Health Insurance from Germany for a certain procedure that is done in the USA. (TSPA, TTA)

14. Public Sector	A Proposed Use Case for LIGHTest Project: eSENS eJustice Pilot
Description	eSENS is an EU funded project that aims to improve the Digital Market through ICT solutions. One of the Building Blocks of eSENS is eJustice domain that is scoped with 2 use cases for piloting: Matrimonial Matters and Parental Responsibility and European Account Preservation Order.

	Matrimonial Matters and Parental Responsibility pilot aims recognition and enforcement of a cross-border judgment on matrimonial matters or parental responsibility, on rights of access and international child abduction with grant of political visibility and increase the international mobility. In a more simplified explanation, a citizen in of Member State (MS) may register to her own Member State's or another Member State's judgment for divorce, separation, annual of the marriage, parental responsibility, abduction of children and etc. Moreover, the citizen may also request pending the case in her own Member State or in another Member State. European Account Preservation Order pilot aims to create a European bank account preservation order (EAPO) to ease the recovery of cross-border debts for both citizens and businesses will only block the debtor's account but not allow money to be paid out to the creditor and be directed against specific accounts. (TSPA)
15. Public Sector	Trusted Open (Government) Data
Description	Governments increasingly publish data collected and/or processed in open formats, to be used by industry, communities or other government entities. LIGHTest could be used to ensure the integrity (and authenticity) of the published data, even across borders. (TSPA)
16. Public Sector	Transcript Translation
Description	Every Country has their own grading system, when students study abroad it is common to recieve a grade on a different scale. Therefore, it could be possible to use LIGHTest's trust translation services, to be able to refer to the translation between the grades of the different systems. This could also be used with (TTA)
17. Public Sector	Military Personnel
Description	Military personal and veterans across North America are entitled to services and benefits across multiple sectors. Organisers such as retailers use the ID.me trust list to determine that the individual they are talking to has indeed served or is currently serving. The military individual is issued with a password-based single and multi-factor credential across Assurance Levels 1, 2 and 3. All identities can be verified remotely and won't expose any personally identifiable information. The individual fills in a full or partial social security number which will then be compared with authoritative databases such as a bank or university. At the moment that is undertaken using a SAML protocol to return a response, however LIGHTest could provide an easier way of verifying the military individual by comparing their data to available trust lists. There is also the potential that this could work across borders, as international retail outlets could extend discounts to military personnel in other countries from their

	residence. This use case could be applied to similar scenarios such as the student/teacher discounts. (TTA,TSPA)
18. Public Sector	Cross-governement offical communications
Description	The LIGHTest Infrastructure could provide a system that could be used to verify international communications to be sent within the EU, such as traffic fines, health notifications, etc. Related to Use Case: Trusted Open (Government) Data (TSPA, TTA)
19. Private-&Public Sector	Secure Online Banking- Protection from Phishing on Websites
Description	It is not unheard of to be scammed on an Internet website that didn't have the proper security measures and was weak to phishing or other Internet attacks. Common juicy targets include identity theft, and stealing online banking credentials. With LIGHTest, it would be possible to allow users to surf the web more securely by making phishing attacks against banks and other sensitive sites. From a technical stand-point, this could be done by having your bank provide a list of trusted CAs that the end user can know for sure that their privacy is not being attacked using a compromised CA, like for example in the notorious DigiNotar case. (TSPA)
20. Private-& Public Sector	Cross-Border Certification
Description	There exists a variety of different certifications. For example, training certificates, other forms of non-government education, government certificates (birth certificates, tax certificates). This certifications may be country specific, or specific to a certain domain. Obviously there is also a huge field of fake certificates, but also fake certification authorities. LIGHTest could be used to (i) ensure trust in those certifications and (ii) translate those certifications between different countries, domains, ... As an extension, this could also be applied to devices (re: safety certifications). (This is related to the Trump University use case.) (TSPA+TTA)

21. Private- & Public Sector	Notary
Description	In order to prove the validity of certificates provided from a foreign country, it is a common process to need a notary from a Bank or Public Authority that proves that it is in fact a real document. This could be done through LIGHTest. This can be open to be used also in the Private Sector, for verifying different work certificates. (TSPA)

22. Private- & Public Sector	IoT Trust Management (A)
Description	Organizing IoT devices to communicate and work with one another based on their certifications of a trusted (3rd, Independent, 2nd) Party. (E.g. Bosch Certified IoT devices, BSI, or NGOs) (TSPA)

23. Private- & Public Sector	IoT Trust Management (B)
Description	Organizing IoT Assisstants to communicate and work with one another based on their certifications of a trusted (3rd, Independent, 2nd) Party. (E.g. Bosch Certified IoT devices, BSI, or NGOs). (TSPA)

24. Private- & Public Sector	Individual IoT Trust Management
Description	A person or company wants to enforce a company or organizational policy. This policy is transfered into a list of what IoT devices are allowed or have permission to be used according to company policy. Therefore, it would be possible for IoT devices to connect or be used in the company, they only have to be on the trusted IoT list of devices. (TSPA)

25. Private- & Public sector	CORREOS.MyMailbox
Description	Any government agency, organization or enterprise will sign an agreement with Correos and so became a "certified" sender of documents to users. After the agreement is signed, the enterprise/organization/government will receive a unique subscription key (with a non-visible token on each transaction/communication), so they'll spontaneously or periodically send documents to any amount of users. (ALL)

26. Private- & Public Sector	CORREOS.MyVerifiedCommunications
Description	Any registered user (or representative of a company) would choose to send a document to any chosen person. The communication will be stored on a trusted platform. Likewise events through all process will be tracked. Notifications (SMTP or SMS) including a link to the document will be sent to the addressee. (TSPA)

27. Private- & Public Sector	CORREOS.MyNotifications
Description	Users can access to register through MyIdentity platform, they will be required to introduce any additional information missing on Myidentity profile. Afterwards user will need to download the desktop app and install it in their PC. Each time they access their app, they'll need to login with MyIdentity. Automatically it'll appear some government agencies that may publish documents to any user. Communication between user and goverment agency will be done through electronic certificate (has to be configured in the app). (TSPA)

28. Private- & Public Sector	Export / Import Control
Description	This Use case would simplify the export / import control processes. It would do so by the following. It would make the export/import check lists more effiecient by being able to check through LIGHTests different published lists on what is allowed to be Imported/Exported from different Countries and the requirements needed to make it work. LIGHTest Component: TSPA. (TSPA)

29. Private- & Public Sector	Allergens Information
Description	Regulation (EU) No 1169/2011 defines that allergens have to be highlighted. To highlight the allergens in an efficient ways an letter can be used. Each member state can define own letters for allergens. This creates a wide variety of letters throughout the member states of the european union. An interested user could use LIGHTest to translate allergenes from one scheme into another. (TSPA)

30. Private- & Public Sector	Cross Borders Banking
Description	Delivery of services that require data flows across multiple legal jurisdictions can be difficult for private sector companies. People today live international lives, often working or being educated across national borders. Opening a bank account in

another country can be difficult and slow and users would need to assert trustworthy data about themselves to support an application for a new financial service. Where additional data is required by the financial institute, with the users consent and control to enable an account to be opened in line with regulatory obligations, LIGHTest may be able to help with this cross border verification. This fits into the 'Supporting Trust Services' scope of the project. (TSPA)

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), IBM Danmark (DK) and Globalsign (FI). The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.