D9.5

E-Procurement: Requirements, Scenarios and Demo Data

Document Identification	
Date	29.05.2018
Status	Final
Version	Version 1.0

Related WP	WP 9	**Related Deliverable(s)**	D2.3, D2.10
Lead Authors	David Hixon (IBM), Niels Pagh (IBM)	**Dissemination Level**	PU
Lead Participants	IBM	**Contributors**	USTUTT, FHG, NLNET
Reviewers	DTU, USTUTT		

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

This document and its content are the property of the *Lightest* Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the *Lightest* Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the *Lightest* Partners.

Each *Lightest* Partner may use this document in conformity with the *Lightest* Consortium Grant Agreement provisions.

1. Executive Summary

In order to demonstrate the technical feasibility of using LIGHTest technology in a real-world scenario, IBM has devised a pilot that will exercise the major features of LIGHTest in an operational environment. The objectives of the pilot are:

1. Demonstrate LIGHTest in an operational environment.
2. Demonstrate the ease of trust-list-enabling diverse existing systems.
3. Demonstrate the ease of authoring individual trust policies.
4. Demonstrate automatic trust verification of electronic transactions.
5. Demonstrate the use of delegations as part of automatic trust verification.
6. Demonstrate how LIGHTest enables easy validation of signatures without the use of validation authorities.

The context of the pilot is the OpenPEPPOL initiative in Europe to facilitate cross border public procurement in the European Union. OpenPEPPOL is a consortium of European government agencies and private companies that work to enable European businesses to easily deal electronically with any European public-sector buyers in their procurement processes. This helps the Member States as well because it increases the opportunities for competition for government contracts and thereby provides better value for tax payers' money.

Within the OpenPEPPOL context, IBM will specifically demonstrate the use of LIGHTest technology in the e-invoicing domain. The PEPPOL e-invoice process is a five-step message exchange where trust decisions are applied to three out of the five steps. The trust schemes used at each point are different. Finally, delegation of trust is incorporated into the scenario in the context of cloud services. Combined, these applications demonstrate the feasibility and usefulness of the LIGHTest technology in a real-world, European environment.

This deliverable is the first of a series of deliverables accompanying the E-Procurement Pilot. It presents an analysis of the requirements, scenarios, and demo data for that pilot.

2. Document Information

2.1 Contributors

Name	Partner
David Hixon	IBM
Martin Hoffmann	NLNET
Sreedhar Janaswamy	IBM
Niels Pagh	IBM
Heiko Roßnagel	FHG
Rachelle Sellung	USTUTT
Sven Wagner	USTUTT

2.2 History

Version	Date	Author	Changes
0.1	05-02-2018	Niels Pagh	
0.2	13-02-2018	Niels Pagh	
0.6	17-04-2018	David Hixon	Requirements etc.
0.7	15-05-2018	Sven Wagner	
0.9	23-05-2018	Martin Hoffmann	
1.0	29-05-2018	Martin Hoffmann	Include reviews

3. Table of Contents

3.1 Table of Figures

3.2 Table of Acronyms

AISBL	Association internationale sans but lucratif
API	Application Programming Interface
ASiC	Associated Signature Container
ATV	Automatic Trust Verifier
BIS	Business Interoperability Specification
CA	Certificate Authority
CSR	Certificate Signing Request
D	Deliverable
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DP	Delegation Provider
GA	Grant Agreement
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
eIDAS	electronic Identification, Authentication and Trust Services
EC	European Commission
EU	European Union
IBM	International Business Machines Corporation
ID	Identifier
OCSP	Online Certificate Status Protocol
PEPPOL	Pan-European Public Procurement On-Line
PKI	Public Key Infrastructure
SHA	Secure Hash Algorithm
SML	Service Metadata Locator
SMP	Service Metadata Publisher
TIA	Transport Infrastructure Agreement
TLS	Transport Layer Security
TSPA	Trust Scheme Publication Authority

UI	User Interface
WP	Work package

4. Scope of the Deliverable

This deliverable D9.5 introduces the pilot scenario for the LIGHTest E-Procurement Pilot and studies the requirements, relevant LIGHTest components, and demo data for this pilot.

In Section 5, the pilot scenario is introduced, which includes a section on PEPPOL in general, the use of LIGHTest technology in PEPPOL, and the demonstration scenario.

Section 6 develops the requirements for the pilot. After assessing the features of the LIGHTest project to be demonstrated by the pilot, the section derives the pilot's requirements from those of LIGHTest at large, divided into functional, privacy security, usability, and economic requirements. The section reviews the objectives of the pilot and relates them to the integration into the PEPPOL network. It concludes with an analysis of the stakeholders involved in the pilot.

In Section 7, the use cases in the pilot are introduced. There are two use cases where LIGHTest technology is integrated into the existing PEPPOL infrastructure: one for access point verification, and one for delegation of document signing to access point provider.

In Section 8, the demo data which is necessary for the pilot is identified. In general, this data is either already publicly available or fictitious data will have to be generated. Necessary data includes payload data (i.e. transmitted documents), digital identities for all entities, and data for the trust scheme, trust delegation, and trust policy.

5. Pilot Scenario

The E-Procurement Pilot integrates LIGHTest in a PEPPOL e-invoicing infrastructure and application scenario 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 with flexible scenarios. PEPPOL is the EU's e-procurement infrastructure and is very appropriate for setting up and running pilot scenarios with LIGHTest components that are meant to be incorporated either as a gateway service or directly into the application systems which have chosen to use PEPPOL as their prime infrastructure. The LIGHTest components will be activated and integrated in different pilot scenarios.

5.1 PEPPOL

Pan-European Public Procurement On-Line – or PEPPOL for short – was a project funded in part by the European Commission aiming at providing the technical standards to enable businesses to participate electronically in procurement of all European government institutions in a uniform way. The project ran from 2008 to 2012. Today, PEPPOL is in use in sixteen European countries, some of which made its use mandatory. The project is now overseen by OpenPEPPOL AISBL, a not-for-profit organization based in Belgium. It has around 250 members from across Europe, both governmental agencies as well as vendors and service providers). [1]

PEPPOL does not constitute an e-procurement platform of its own but rather provides the technical and legal means to allow interoperation between existing platforms. Specifically, it provides three components:

- the PEPPOL e-Delivery Network, a network for securely and reliably exchanging messages between participating entities,
- PEPPOL 'BIS' Specification, a specification of standardized document formats for procurement processes, and
- PEPPOL Transport Infrastructure Agreements (TIA), providing the legal framework for communication between the many connected parties.

The LIGHTest e-Procurement Pilot focuses on the e-delivery network.

This network operates on an open four-corner model, shown in Figure 1. In this model, each organization participating in PEPPOL chooses an access point that acts on their behalf for sending and receiving messages via the delivery network. Communication between an organization and their access point is not regulated by PEPPOL and can happen in whatever form they agree on to accommodate existing systems or procedures. The access point makes sure that documents submitted are either already valid PEPPOL BIS documents or translates them. It then uses the PEPPOL e-delivery network to communicate with the access point chosen by the receiving organization to deliver the document.

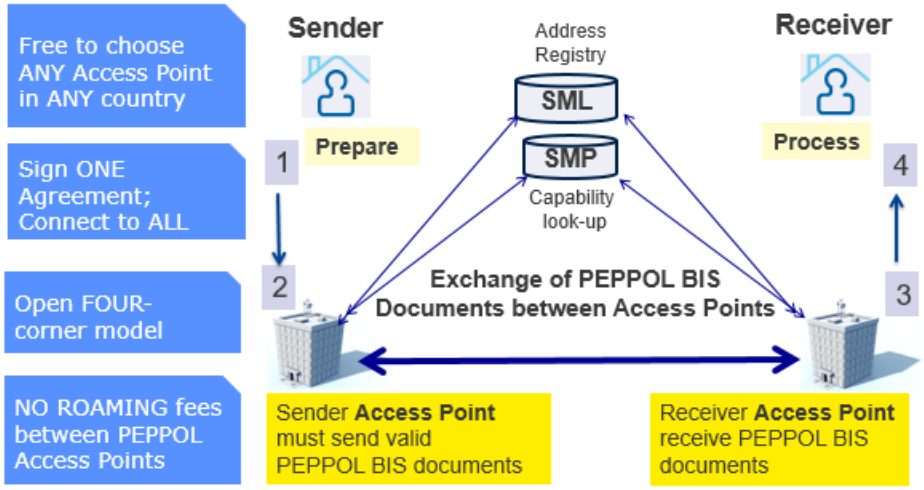


Figure 1: PEPPOL four-corner model. [2]

Two directories facilitate this delivery. First, each organization publishes their receiving capabilities, contact information, and other information through a Service Metadata Publisher (SMP). This publisher is typically operated by the access point directly. To find the SMP responsible for a given organization, a centralized directory, the Service Metadata Locator (SML) is employed.

5.2 PEPPOL and LIGHTest

To ensure security and integrity of the network, PEPPOL heavily relies on public key infrastructure (PKI). All access points and SMP providers receive a digital certificate which they use to identify themselves in communication. These certificates are created based on trusted certificate authority (CA) operated by PEPPOL itself. Currently, verification in the network relies on distributing the CA and intermediary certificates between all access points. With LIGHTest, this strict single-root infrastructure can be replaced with a model where multiple CAs are authorized to create certificates through membership in a trust scheme.

In addition, as PEPPOL BIS documents are signed ASiC containers, LIGHTest's Automatic Trust Verifier (ATV) can directly be used by access points and organizations to verify trust into the sender or certain attributes atop the existing PEPPOL network without any changes.

5.3 The Demonstration Scenario

The pilot will demonstrate the use of LIGHTest technology in a cross-border, healthcare scenario. There will be a fictitious sender named *German Medical Device Company* in Germany that will send an invoice to *French Hospital,* a hospital in France for 200 insulin pumps over the PEPPOL network, using the PEPPOL specifications. Preparing and signing message according

to the PEPPOL specifications is complex and the *German Medical Device Company* will delegate the packaging and signing of their invoices to IBM.

In the scenario, *French Hospital* will verify the authenticity of the invoice using LIGHTest technology (Trust Scheme Publication, WP3, and Automatic Trust Verification, WP6) and acknowledge the receipt of the invoice to the sender as specified in the PEPPOL specifications. This is a multi-step process involving multiple message flows. Many of the steps have trust operations and all trust operations (other than TLS 1.2 authentication) will be done using LIGHTest technology. Furthermore, all trust configuration for the steps will be done with the Policy Authoring and Visualization Tools (WP6).

6. Requirements

6.1 LIGHTest Features Demonstrated by the Pilot

Various documents are exchanged in PEPPOL on two levels; participating organizations exchange documents while, below, access points exchange message. In both levels, authenticity of exchanged data is established using digital signature. Therefore, Automatic Trust Verification and the underlying Trust Scheme Publication are of primary interest for the pilot. IBM is a service provider and our customers require the capability to delegate the signing and verification of digital signatures to us, so Trust Delegation is also crucial.

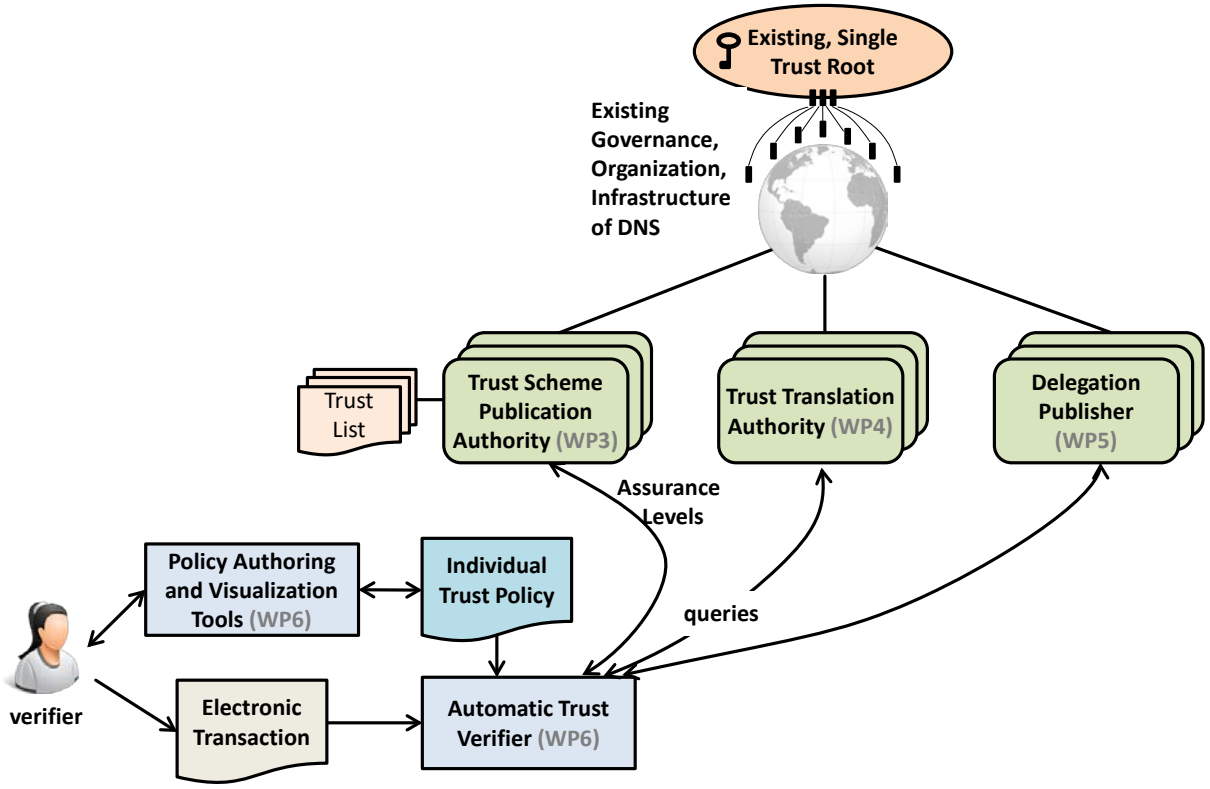


Figure 2: The LIGHTest reference architecture (see D2.14 (The LIGHTest Project, 2017))

Specifically, from the components of LIGHTest's architecture as show in Figure 2, the pilot will demonstrate the use of Trust Scheme Publication (WP3), Trust Delegation (WP5), Automatic Trust Verifier (WP6) and Policy Authoring and Visualization Tools (WP 6).

6.2 Analysis of the Relevant Project Requirements

The pilots take into consideration all of the requirements that were developed in deliverables D2.3 [3] and D2.10 [4]. These requirements ensure that a wide and diverse spectrum of requests are considered regarding the technical and market needs. D2.3 identified five

categories: 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 D2.10. Regarding each category, there is an established structure and methodological reasoning that is tailored to the needs of each perspective.

While the pilots will consider all requirements from all categories provided in D2.3 and D2.10, it is not expected that all of them will be necessary or applicable as these pilots implement very detailed use cases while the requirements were developed for all of the LIGHTest project.

With that in mind, the following sections recapitulate the requirements found in D2.3 and provide a first analysis of their applicability to the E-Procurement Pilot. This analysis will be repeated throughout the development process, providing a refined impression. This continuous review will provide input for WP2's task 2.8 which evaluates and assesses all the requirements for the entire LIGHTest project.

6.2.1 Functional Requirements

The Functional Requirements represent the guidelines and necessary functions of each of the components defined in the LIGHTest Reference Architecture in D2.14 [5]. Consequently, they are grouped by the LIGHTest component they refer to.

As the E-Procurement Pilot does not demonstrate all LIGHTest components, only a subset of the overall functional requirements is applicable. In particular, the complete category FR-06 as well as some requirements from category FR-10 do not apply as they deal with the Trust Translation Authority and Derived Mobile IDs both of which are not part of the E-Procurement Pilot.

The applicable requirements are provided in the following overview.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.2.2 Privacy Requirements

The Privacy Requirements reflect the principles set out in the EU General Data Protection Regulation. The following requirements apply to the pilot.

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.
Note	The E-Procurement Pilot will verify if the purposes are explained and legitimate at the time of collection.

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

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

No.	PR-04.01- Minimal registration data
Description	As a corollary of the Data minimization requirement, any data required to use the LIGHTest services by any actor SHOULD NOT include any identifiable data, and any identifier SHOULD be randomly generated.
Note	The E-Procurement Pilot will verify the statement “any data required to use the LIGHTest services by any actor SHOULD NOT include any identifiable data”.

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

No.	PR-05.04- Transparency towards actors

Description	All outcomes of authentication, authorization, delegation, and identity and attribute management processes, including any automated decision-making, MUST be visible (transparent) for the relevant actor whose electronic transaction is being processed.

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

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

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

6.2.3 Security and Accountability Requirements

The Security and Accountability Requirements are internal to the LIGHTest infrastructure processing and are not visible the users of the technology. The IBM e-Invoicing pilot will not be able to verify these requirements.

6.2.4 Usability Requirements

The Usability Requirements ensure that LIGHTest components can be used by their users effectively, efficiently, and satisfactory. The following Usability Requirements are relevant for the pilot.

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

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

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

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

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

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

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

No.	UR-08.00- Transparency
Description	There is no need for the user to understand to whole system and every little detail that happens in the background. But the system UI must be transparent enough so the user can understand the overall concept and therefore understand what’s happening and what he/she is supposed to do. At any given point the system should be

	transparent enough whilst not overstraining the user.

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

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

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

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

6.2.5 Economic Requirements

The E-Procurement Pilot demonstrates LIGHTest in one specific market namely the procurement or supply chain market. Due to this focus, the Economic Requirements will be applied only to this one market and the related business model. In consequence, the requirements dealing with the wide-range applicability of LIGHTest, such as ER-01.00 "Support of various business models," do not apply to the pilot.

This limitation leaves the following requirements.

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-02.00- Provide value for all stakeholders involved
Description	Many stakeholders are relatively satisfied with the currently used trust use case solutions and trust management. In order for the relevant stakeholders to use LIGHTest, they MUST to be offered added value. Examples of 'added-value' could be either having additional merit, increased user-friendliness, security or data protection benefits, improved usability, greater convenience, financial benefits. Refer to Use Cases for specific examples.

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

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

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

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

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

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

6.3 Review of Pilot Objectives

Within the LIGHTest project, the pilots are intended to achieve seven objectives. The E-Procurement Pilot will contribute to these objectives as follows:

O9.1 Demonstrate LIGHTest in an operational environment (TRL7)

OpenPEPPOL is an organization with around 250 members (government agencies and vendors/service providers) across Europe. It is well known, well established and has been in production for many years. The E-Procurement Pilot will take place in this mature environment proving that it is operational in production B2B applications.

O9.2 Demonstrate the ease of trust-list-enabling diverse existing systems

The pilot will explore trust-list enabling three different trust schemes in a single message flow:

- the trust scheme used for signing documents by the sender,
- the trust scheme used for propagating messages between PEPPOL e-delivery access points, and finally
- the trust scheme used by the receiver in signing the acknowledgement documents.

By introducing LIGHTest to these different levels of the existing system, the pilot will demonstrate the ease of enabling diverse existing schemes.

O9.3 Demonstrate LIGHTest integration of foreign trust schemes through scheme translation

This will not be addressed as part of the E-Procurement Pilot. Integration of foreign trust schemes will, however, be demonstrated by the Correos Pilot.

O9.4 Demonstrate the ease of authoring individual trust policies

As part of the pilot, trust policies will be created for three different entities, namely the IBM access point, the French access point, and *French Hospital*). As these have differing requirements resulting in different policies of differing complexity, creating these policies will demonstrate the ease of authoring policies using the Policy Authoring and Visualization Tool.

O9.5 Demonstrate automatic trust verification of electronic transactions

The E-Procurement Pilot will demonstrate automatic trust verification at three different points in a five-step message flow:

- verification of the invoice sent by *German Medical Device Company* by *French Hospital*,
- verification of Sender's Access Point by Receiver's Access Point while sending the invoice, and
- verification of Receiver's Access Point by Sender's Access Point while sending the acknowledgement document.

O9.6 Demonstrate the use of delegations as part of automatic trust verification

In the E-Procurement Pilot, *German Medical Device Company* will delegate signing of their invoice to their access point. The access point will sign the invoice with their own private key and when *French Hospital* authenticates the invoice, the authentication will rely on the fact that *German Medical Device Company* has delegated signing authority to their access point.

O9.7 Demonstrate how LIGHTest enables easy validation of signatures without the use of validation authorities:

By introducing the Automatic Trust Verifier into in the validation of access points, the pilot will relieve the system from its dependence on a sole central root certificate authority.

6.4 Integration with PEPPOL

As the pilot will integrate LIGHTest components with the existing PEPPOL infrastructure, a number of points will have to be considered.

6.4.1 Existing Trust Schemes Used in the Pilot

To authenticate messages exchanged between access points as part of the PEPPOL e-delivery network no trust scheme is currently in use. Instead, the network relies on a straightforward public-key infrastructure based on a single root certificate.

Documents exchanged between participating organizations, however, can be signed with any certificate and greatly benefits from verification via a trust scheme. As such verification is left to the discretion of the access point or receiving organization, pretty much any trust scheme these parties deem applicable can be used. Since PEPPOL is used for procurement within the European Union, the European eIDAS trust scheme – or a scheme qualifying as equivalent – is likely to be required for verification of the digital entities behind the exchanged documents.

6.4.2 Components of the Existing System Necessary

The pilot will integrate with the existing PEPPOL e-delivery network. Of the components in this network, briefly introduced in section 5.2, theses will be used:

- access points for the sender and receiver,
- Service Metadata Publisher (SMP) of these two access points,
- Service Metadata Locator (SML),
- participating organizations, represented by *German Medical Device Company* and *French Hospital*.

6.4.3 Existing Application-specific Infrastructure Available for the Pilot

For the pilot, the infrastructure of OpenPEPPOL will be used. The LIGHTest components that need to be integrated with this infrastructure, specifically the Automatic Trust Verifier, will either be integrated as gateway services or embedded directly into the affected application systems.

6.5 Stakeholders Involved in the Demonstration

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

A first insight into the stakeholders involved in the pilots from a theoretical perspective will be provided in Task 2.8 and deliverable D2.12. It will take the preceding stakeholder analysis given in deliverables D2.3 and D10.1 and apply those results to a more concentrated and defined use case of the pilots, focusing on fictitious stakeholders. In order to transform this theoretical analysis into an understanding of the pilots' potential for real stakeholders, the International Forum will place particular focus on the pilots during the final year of the project.

Based on the methodology introduced in section 10.3 of deliverable D2.3 [3] the following provides an early impression on potential stakeholders relevant to the E-Procurement Pilot.

6.5.1 Active Stakeholders

The most obvious stakeholders are those involved directly in the demonstration. These are two fictitious organizations exchanging documents as well as the PEPPOL access point providers they have selected.

OpenPEPPOL, the organization overseeing the PEPPOL e-delivery network, is involved as a governing entity as well as a provider of some of the networks essential infrastructure, such as the central SML service and the certificate authority providing trust service for the network.

Slightly more removed yet essential are the trust service providers that issue the digital identities for the participating organizations as providers of an essential part of the LIGHTest infrastructure exploited by the pilot.

6.5.2 Enabling Stakeholders

As PEPPOL has been created to facilitate procurement of governmental agencies in the European Union, these agencies have an enabling stake in the demonstration as well as the European Commission in its desire to foster the digital market within the Union.

6.5.3 Internal Stakeholders

As the pilot demonstrates a number of core benefits of LIGHTest, all project partners have a strong interest and role.

7. Use Cases in the Pilot

The E-Procurement Pilot comprises two concrete use cases that will greatly benefit from integration of LIGHTest technology into the existing PEPPOL infrastructure.

7.1 Access Point Verification

The first use case shows the value of the LIGHTest trust list publication infrastructure. PEPPOL acts as its own certificate authority and certifies access points to the PEPPOL network. Upon successfully completing the certification process, an access point submits a certificate signing request (CSR) to the OpenPEPPOL authority which creates a certificate signed within the PEPPOL trust chain. Every PEPPOL message must be signed using such a PEPPOL signed certificate. Every message received by an OpenPEPPOL access point must be authenticated by verifying that it is properly signed using the embedded certificate and that the signing certificate is itself signed by within the OpenPEPPOL trust chain.

The OpenPEPPOL root and intermediate certificates were originally signed using the SHA-1 signing algorithm. At some point in time, the SHA-1 algorithm was demonstrated to be breakable and it became imperative that everyone (including OpenPEPPOL) migrate to using SHA-2 algorithms. Unfortunately, there are hundreds of access points, upon which thousands of trading partners depend, which have the current SHA-1 trust chain installed. How then to effect the change to SHA-2 without shutting down the entire OpenPEPPOL network and coordinating the actions of hundreds of access points to swap out the SHA-1 certificates with the SHA-2 certificates?

OpenPEPPOL hasn't announced their specific plan yet, but it would really have to be a four-phase plan. First, they need to tell all the access points that they are moving SHA-2, re-sign every certificate with the new trust chain, and distribute all the newly signed certificates. In the second phase, they need to give all the access points time to load the new certificates alongside the old certificates so that they sign using SHA1 but can verify either SHA1 or SHA2. This may require programming changes to some of the access points, so they need to be given time to modify and test their systems. Once all the access points confirm that they have both sets of trust chains loaded and can sign and verify using either, then phase three begins where all the access points are told to start using the SHA2 certificates to sign messages. The fact that all access points can handle either trust chain means that it is not necessary for the access points to synchronize their changes during this phase. Finally, after some period of time, the access points can be told to disable support for SHA1 and delete the old certificates. OpenPEPPOL is currently assessing that this would likely be a six-month process.

Contrast that with how the update of the root certificate would proceed with LIGHTest. No access point would have the trust chain loaded, so there is need to redistribute the updated CA certificates and wait for every access point to load it, nor do access points have to modify their code to support multiple trust chains. Verification is handled by the ATV, which automatically

knows which trust chain to apply and where to go to get it, so support for multiple trust chains is already there. All that needs to be done if for OpenPEPPOL to re-sign the access point certificates and distribute them. Access points do not need to synchronize, and they can swap out the old certificates at a time that is convenient for them. A six-month process with much higher risk is replaced by a one-week process with low risk.

The same applies to a potential case where a root certificate needs to be replaced either because of a routine certificate replacement or because the private key of the current certificate is compromised. In particular, in the latter case a six-month process is hardly acceptable and quick exchange is of the essence.

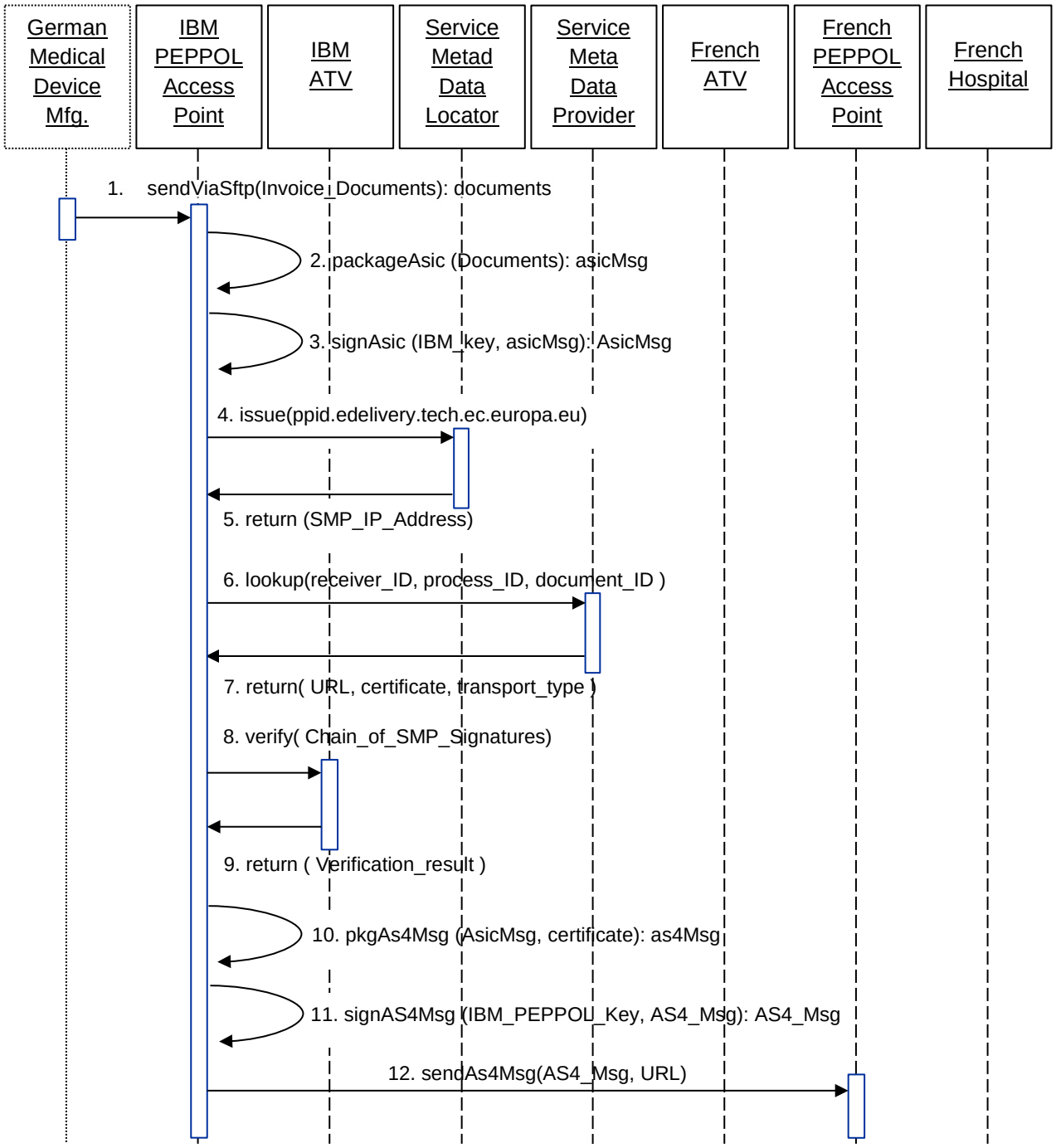
7.2 Delegation of Document Signing to Access Point Provider

A second use case demonstrates the use of delegation and delegation authorities in a cloud environment.

IBM customers contract with IBM to handle the complexities of business-to-business message processing. In the PEPPOL BIS, ASiC containers are used which are complex to prepare and are expected to be signed by the owner of the documents inside the container. Unfortunately, without divulging their private key, there is no way for IBM to sign the for them. With delegation however, IBM customers can delegate the signing of ASiC containers “that contain invoices and document related to invoices” to IBM. The receiver of the ASiC container can use a delegation provider to verify that IBM had the authority, on the date of the signing, to sign invoices and invoice related documents for our customer. This allows our customer and IBM to avoid a serious security risk.

7.3 Message Flows

Figure 3 shows the flow of messages through the PEPPOL infrastructure that has been enhanced with LIGHTest components as it would appear in both uses cases of the pilot.


German Medical Device Mfg.
IBM PEPPOL Access Point
IBM ATV
Service Metad Data Locator
Service Meta Data Provider
French ATV
French PEPPOL Access Point
French Hospital
1. sendViaSftp(Invoice, Documents): documents
2. packageAsic (Documents): asicMsg
3. signAsic (IBM_key, asicMsg): AsicMsg
4. issue(ppid.edelivery.tech.ec.europa.eu)
5. return (SMP_IP_Address)
6. lookup(receiver_ID, process_ID, document_ID)
7. return(URL, certificate, transport_type)
8. verify(Chain_of_SMP_Signatures)
9. return (Verification_result)
10. pkgAs4Msg (AsicMsg, certificate): as4Msg
11. signAS4Msg (IBM_PEPPOL_Key, AS4_Msg): AS4_Msg
12. sendAs4Msg(AS4_Msg, URL)

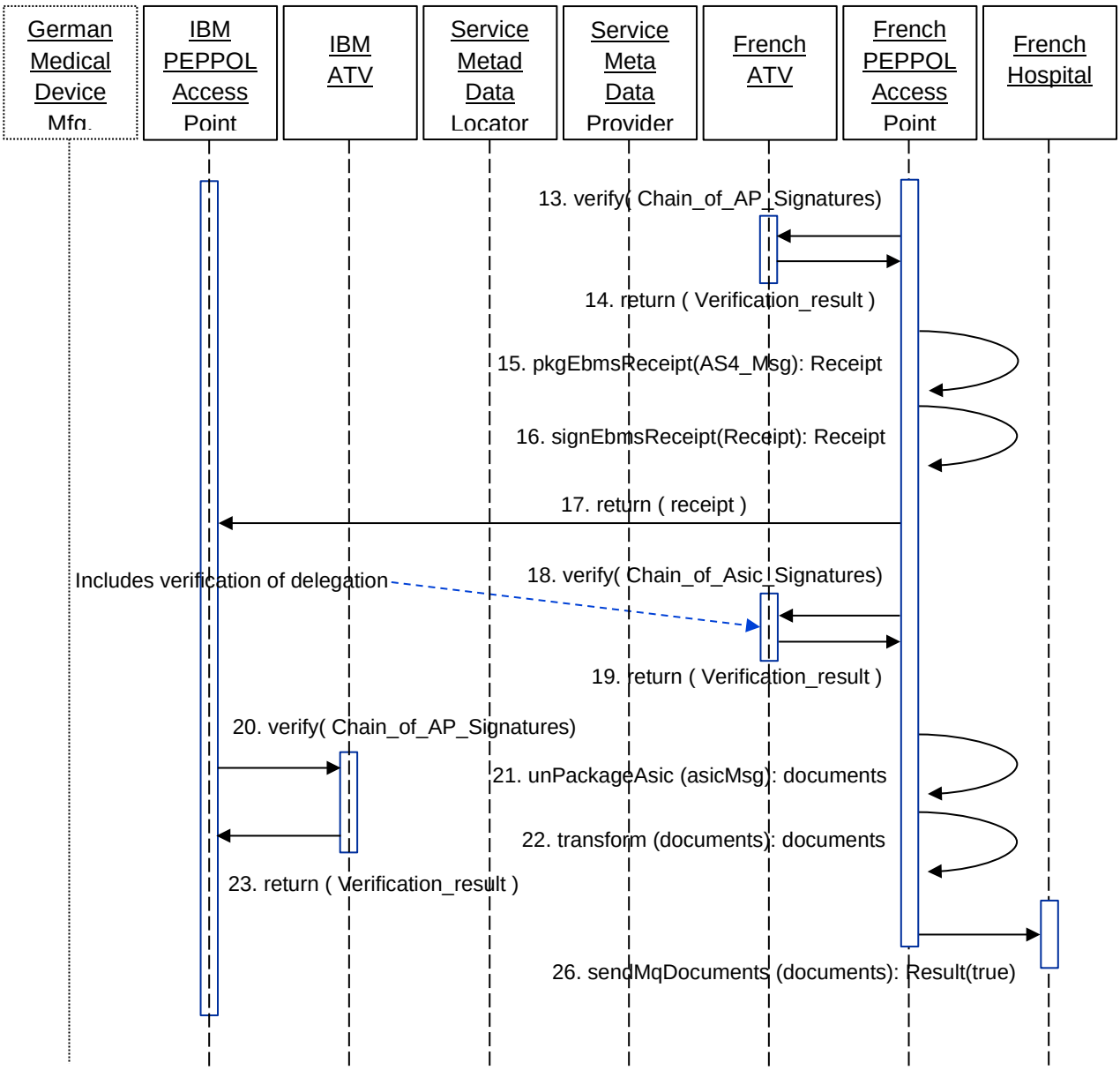


Figure 3. Trust related steps in document flows for Open PEPPOL in LIGHTest

8. Demo Data

This chapter identifies the data that is necessary as part of the pilot. Part of the data, particularly that relating to the existing infrastructure, does already exist and will be used in the pilot. All of this data is already publicly available. Additional data pertaining to fictitious and newly established entities will have to be created and subsequently will not be real-world data. As this data does not identify any real organizations or transactions, it will be made available as part of the pilot demonstration.

The data can roughly be placed into these categories:

- payload data, i.e., documents transmitted via the PEPPOL e-distribution network,
- digital identities representing the various entities, real and fictitious, participating in the pilot,
- the data necessary for the trust schemes employed,
- the data necessary for trust delegation, and
- trust policies used as input for trust verification.

The following sections provide a closed look at these categories.

8.1 Payload Data

The overall goal of the pilot scenario is to transmit an invoice issued by *German Medical Device Company* to *French Hospital.* As both these entities are fictitious as is the transaction for which the invoice is being issued, this invoice needs to be manufactured as part of the pilot.

In addition, *French Hospital* will reply with an acknowledgement document confirming the arrival of that invoice. Similarly to the invoice itself, this document will be created as part of the pilot.

8.2 Digital Identities of Participating Entities

All the entities participating in the pilot are identified by and authenticate themselves with public key certificates. Depending on the role of the entity, these certificates have to be created and signed by certain certificate authority (CA).

8.2.1 Participating Organizations

The demonstration scenario identifies two fictitious organizations, *German Medical Device Company* and *French Hospital.* Each will be identified by a digital identity issued by a qualified trust service. If the organizations were real European entities, these qualified digital identities would be issued under the eIDAS trust scheme. Since the pilot, however, uses fictitious entities, this is not an option.

8.2.2 PEPPOL E-Delivery Network

Four entities of the PEPPOL e-delivery network will play a role in the pilot:

- IBM PEPPOL Access Point,
- French PEPPOL Access Point,
- French PEPPOL Access Point's SMP,
- SML.

See section 5.1 for a brief descriptions of their roles.

All of these entities are identified by public key certificates issued by the PEPPOL certificate authority. As existing entities will be used, these certificates already exist.

In addition, all will receive extra certificates as part of the first pilot use case. These certificates will be issued by a new certificate authority. This CA will be created as part of the pilot.

8.2.3 Trust Schemes

Two trust schemes are used in the pilot.

The first use case employs a trust scheme to verify the identity of PEPPOL entities. This trust scheme does not yet exist and will be created as part of the pilot. Both the existing and the newly created PEPPOL certificate authorities will be recognized trust services under this scheme.

For the second use case, a trust scheme is used to verify the identity of the two participating organizations. As mentioned above, this trust scheme would be the European eIDAS were the participating entities real European organizations. Since they are not, a fictitious trust scheme including fictitious trust services needs to be created as part of the demonstration. This scheme will, however, be modeled closely after the real eIDAS scheme.

Each trust scheme requires the same data: a trust service status list that provides information about the trust services and their CA certificates recognized by the scheme, a certificated used to sign this trust service status list, and a set of DNS records allowing discovery of the list as well as signature validation. These DNS records will need to be placed in several DNS zones. The trust scheme requires a zone containing the domain name used to identify the scheme. Similarly, each recognized trust service needs a zone containing the domain name it uses to identify itself.

8.2.4 Trust Delegation

As part of the second use case of the pilot, *German Medical Device Company* delegates authority to sign invoices to *IBM PEPPOL Access Point*. This delegation needs to be created as part of the pilot.

8.2.5 Trust Policies

The two pilot use cases require two trust policies.

For use case one, a trust policy needs to be defined that verifies the identity of another access point and SMP in the PEPPOL e-delivery network. This policy employs the PEPPOL trust scheme and simply verifies trust scheme membership.

In the second use case, the ATV is used to verify the trustworthiness of the transmitted invoice. The trust policy for this case is more complex. It not only needs to consider whether the sender's digital identity has been issued via a qualified trust service under the trusted scheme but also valid trust delegations from the sender to the signing party.

9. Summary and Conclusion

This deliverable D9.5 is the first deliverable for the pilot demonstration of E-Procurement, where LIGHTest technology is integrated into the existing PEPPOL infrastructure. It defines the requirements, relevant LIGHTest components, and demo data for this pilot. From the LIGHTest reference architecture, the pilot will in particular demonstrate the use of the Trust Scheme Publication, Trust Delegation, Automatic Trust Verifier and Policy Authoring and Visualization Tools.

The demonstration scenario is a cross-border, healthcare scenario, with a fictitious medical device company in Germany sending an invoice to a hospital in France over the PEPPOL network. For this scenario there is one use case for access point verification, and one use case for delegation of document signing to access point provider.

For the demo data, which are necessary for the pilot, either already publicly available will be used or fictitious data will be generated for the remaining ones.

The LIGHTest components, requirements, and demo data for this pilot and the developed use cases will be continuously reviewed and updated if necessary as development progresses.

10. References

[1] OpenPEPPOL AISBL. About OpenPEPPOL. https://peppol.eu/about-openpeppol/.

[2] OpenPEPPOL AISBL. PEPPOL eDelivery Network – An Overview. https://peppol.eu/what-is-peppol/peppol-transport-infrastructure/

[3] The LIGHTest Project. D2.3 – Requirements and Use Cases. Project Deliverable, April 2017.

[4] The LIGHTest Project. D2.10 – Legal, Ethical and Societal Requirements and Constraints (1). Project Deliverable, August 2017.

[5] The LIGHTest Project. D2.14 – Reference Architecture. Project Deliverable, February 2017.

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

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