The LIGHTest e-Procurement Pilot and PEPPOL

Pan-European Public Procurement Online – or PEPPOL for short – was a project funded in part by the European Commission aiming to provide 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 16 European countries, some of which have made its use mandatory. The project is now overseen by OpenPEPPOL AISBL, a not-for-profit organisation based in Belgium. It has around 250 members from across Europe, both governmental agencies as well as vendors and service providers.

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 organisation participating in PEPPOL chooses an access point that acts on their behalf for sending and receiving messages via the delivery network. Communication between an organisation 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 organisation to deliver the document.

Two directories facilitate this delivery. First, each organisation 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 organisation, a centralised directory, the Service Metadata Locator (SML) is employed.

**PEPPOL and LIGHT**

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 LIGHT, this strict single-root infrastructure can be replaced with a model where multiple CAs are authorised to create certificates through membership in a trust scheme. In addition, as PEPPOL BIS documents are signed ASiC containers, LIGHT's Automatic Trust Verifier (ATV) can directly be used by access points and organisations to verify trust into the sender or certain attributes atop the existing PEPPOL network without any changes.

**The Demonstration Scenario**

The pilot will demonstrate the use of LIGHT 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.

In the scenario, French Hospital will verify the authenticity of the invoice using LIGHT 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 LIGHT technology. Furthermore, all trust configuration for the steps will be done with the Policy Authoring and Visualisation Tools (WP6).

Extract from LIGHT deliverable D9.5.

**LIGHT** Developer’s Workshop

The LIGHT Developer’s Workshop was organised by TUBITAK at Shangri-La Bosphorus, Istanbul on 9th and 10th July 2019, with the contribution of project partners involved in the development of LIGHT components and piloting.

**The LIGHT** International Forum Workshop

From 27th – 30th May, a delegation from LIGHT (Heiko Roßnagel from Fraunhofer; Rachelle Sellung, Sven Wagner and Stephanie Weinhardt, from The University of Stuttgart; Stefan More and Lukas Alber from TU Graz) hosted the LIGHT International Forum Workshop in Baku, Azerbaijan.

The three-day event began with an introduction to the project and a close look at trust infrastructures and how they are developing digitalisation. Highlights from the workshop included sessions focusing on:

**Usability of Trust Policy Authoring Tools - Concept, Design and Evaluation**

Usability of policy authoring tools remains a challenge. However, in a user study, delegates were shown how LIGHT offers a new approach which has been developed based on a mental concept as opposed to design guidelines.

**Trust Scheme Publication Authority (TSPA)**

The concept of the TSPA and the different possibilities of publishing trust schemes were presented. The TSPA
is one of the key components of the LIGHTest reference architecture and is used in every verification process of an electronic transaction.

Delegates were also introduced to the use of DNS to make trust scheme membership claims discoverable by a verifier in an automated way. Also in this session, proof of concepts (PoC) regarding how the TSPA and further components of the LIGHTest infrastructure can be used were demonstrated for two possible application fields: PoC for a Trust Scheme for UNHCR and PoC for a predictive maintenance use case for sensor data verification in the IoT.

During the session delegates took a user perspective of the process, starting from an electronic transaction received by the central Automated Trust Verifier (ATV) component. It was demonstrated how the ATV processes this electronic transaction and makes a decision about its trust. In addition, delegates were shown how the ATV utilises components such as a trust policy, as well as several other LIGHTest components.

EEMA Annual Conference 2019

An Interactive Boardroom Session focusing on LIGHTest and entitled ‘Transforming the Way we see Trust’ was hosted by EEMA, during its Annual Conference at Microsoft in London on 19th June.

The morning session was Chaired by Rachelle Sellung of University of Stuttgart, who provided the business perspective, alongside Hans Graux an Attorney-at-law and Partner at Timelex who shared the legal considerations, and Martin Hoffmann of NLnet Labs who provided high level technical insight.

Automatic Trust Verification

This presentation featured an overview of the technical process of automated trust verification using LIGHTest.

Lightest Logo.pdf   2   03/11/2016   19:44
Produced by EEMA - WP11 Lead, LIGHTest