

Improving Cross-border European ePrescription and Patient Summary Services through e-SENS

Cross-sectorial Building Blocks

François Wisniewski¹, Dimitrios Katehakis²,
Massimiliano Masi³, Soeren Bittins⁴

¹ LIST, G. D. of Luxembourg, francois.wisniewski@list.lu

² Foundation for Research and Technology – Hellas, Greece,
katehaki@ics.forth.gr

³ Tiani Spirit, Austria, massimiliano.masi@tiani-spirit.com

⁴ Fraunhofer FOKUS, Germany, soeren.bittins@fokus.fraunhofer.de

Introduction

The cross-border healthcare services are now largely regulated by the Directive 2011/ 24/ EU [1] on the application of patients' rights. ePrescription and Patient Summary (eP/ PS) services are expected to be the first cross-border healthcare services to become operational in real life by some European Union (EU) countries, starting 2017, with the support of the Connecting Europe Facility (CEF) [2]. The Electronic Simple European Networked Services (e-SENS) project (2013-2016) provides solutions for seamless public service delivery across borders by developing infrastructure for interoperability, adaptable to different domains (like e-Justice, e-Procurement, and Business Lifecycle), using the results of previous Large Scale Pilot (LSP) projects, and more specifically those of e-CODEX [3], SPOCS [4], STORK [5], PEPPOL [6], and the more specific to eHealth ePSOS [7].

Method

During the first year of the e-SENS project, each domain listed their business requirements for priority use cases, together with technical solutions adopted in the past to meet these requirements. e-SENS consolidated and analyzed the maturity of each technology and packed the most relevant ones into generic components, called Building Blocks (BBs), that can be used across different domains. The Building Block (BB) continuum is guaranteed by the e-SENS architectural approach, strictly based on TOGAF [8]. Each BB has an *architectural* view (ABB), and a *solution* view (SBB) to guarantee both the architectural as well as the operational continuum.

As far as eP/ PS is concerned, e-SENS has tried to mitigate issues related to missing evidence, patient identification, central configuration services refactoring, and end-2-end security (which are linked to several BBs). Patient identification was considered to be of the highest priority for EU

Member States as well as patient access to audit trails. Central configuration services are considered to be background infrastructure and a priority when looking at infrastructure redundancy with view to CEF adoption.

Based on the elicited business requirements for eP/ PS, the e-SENS eHealth domain took benefits of three cross-sectorial BBs among the ones identified by the project to be part of the e-SENS reference architecture [9]: *Evidence Emitter*, *Electronic Identification (eID)*, *Service Location*, and *Capability Lookup*. Each BB has been implemented in the OpenNCP reference implementation framework for a National Contact Point for eHealth (NCPeH) [10]. The participating Member States – Austria, Greece, Italy, Luxembourg, Portugal and Spain – installed and localized this reference-implementation in their NCPeH. IHE [11] provided the conformance testing procedure to perform these tests in IHE Connectathon (April 2015) and later in EXPANDATHON (December 2015).

Building Blocks and Benefits for the eHealth Domain

The *Evidence Emitter* BB provides a layer enabling actors to generate and emit electronic evidence used for non-repudiation purposes, in a cross-domain scenario. Non-repudiation services are mandate to generate, collect, maintain, make available, and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of an event or action. Several definitions and corresponding frameworks have been proposed to achieve the four fundamentals non-repudiation evidence, namely the *Non Repudiation of Origin*, *Submission*, *Delivery*, and *Receipt*. The Evidence Emitter fits in a per-hop non-repudiation mechanism where the tokens have the format defined by ISO 13888 [12] and are using the ETSI REM [13] standard. Its peculiarity relies on the abstract model implemented: each incoming/outgoing message is evaluated against a XACML policy [14] in a specific evaluation context (e.g. domain of application, data classification) and the resulting evaluated XACML policy obligations trigger the emitting of a domain-specific non-repudiation evidence, following domain-specific non-repudiation policies.

To ease the piloting operations, epSOS had relaxed the need for non-repudiation tokens. In fact, non-repudiation of origin and receipt had been implemented by using Audit Trails [15]. Although interoperability had been achieved, it did not fit into the definition of non-repudiation [12]. For these reasons, the e-SENS evidence emitter BB enables the epSOS NCPeH with non-repudiation tokens based on the standard ETSI REM, while preserving compliance with the Audit Trails: when a message reaches the NCPeH, or leave the NCPeH, the Evidence Emitter policy is evaluated and, based on

the type of the message, the specific REM and Audit Trail are emitted and stored.

The *eHealth eID* components primarily address the problem of the last mile on how to effectively and efficiently operate a multitude of eID token carriers, like smart cards, and their specific complex cryptographic material in a highly regulated but technically limited environment. The core tool deals with identifying, transforming, and mapping available token services and data onto a singular virtual ISO 24727-3 compliant middleware [16] to decouple a specific eID technology from its after-use as well as avoiding the need to install several middleware or drivers for each token type. Paired with Java Web Start technology, the tools are available to the health professional when needed, install and configure automatically, and are removed afterwards. Currently, international smart card-based services for authentication, authorization, and the patient-centric application of electronic signatures are operated with a planned extension for the inclusion of the European Authentication Scheme eIDAS [17] as well as smart phone-based mobile eID. A systemic integration into the epSOS-inspired OpenNCP eHealth gateways has been done in order to test-drive its functionality in real medical environments.

The *Service Location* BB provides a DNS-based query mechanism to locate capabilities of remote services. Once located, capabilities can be retrieved, and consumed using the definitions of the *Capability and Location Lookup* BB. The underlying standard is the OASIS SMP [18]. Such BB is widely used in production in the eProcurement domain, where a single-PKI trust model is in place. Authorities push their SMP-based metadata into servers that apply a signature (note that the processing model can be either centralized or distributed). The receiving party verifies the authenticity of the data by checking the signature of the server. The epSOS LSP provided an ad-hoc model based on ETSI TL files [19] for the definition of remote NCPeH configurations. This was a manual procedure: operators had to create the TL-like file, sign it, and submit into central configuration services, using the Secure File Transfer Protocol (SFTP). Daily a cron-job was on duty to fetch new TL files and configure the local NCPeH. This manual task has been proven to be inefficient and error prone, thus adopting the *Capability and Location Lookup* BB has been considered relevant. However, the integration presented several challenges. A different trust model (single public key infrastructure and direct brokered trust), a set of mandatory (mainly procurement-specific) elements, and a lack of extensibility of the SMP model are examples. The adoption of SMP firstly enables the NCPeH with a flexible method to retrieve dynamically remote configuration (that can be cached) improving the overall system performance, and secondly

improve the SMP specifications to open for cross-domain transactions. For this latter point, a change proposal has been submitted to the OASIS SMP.

Conclusion

The proposed solution improves on the technical solutions supporting the data protection, privacy and security process initiated in epSOS, through the use of technologies enabling stronger identification and authentication of the patient and improving on the usability of the technical solutions. The objective has been to facilitate cross-border access to EU eP/ PS services and to enhance the technology used with cross-domain technical BBs.

Cross-sectorial BB usage is expected to reduce cost of maintenance and allow the IT industry to be provided with open source solutions to be adopted in their own business services in order to improve efficiency, cost-effectiveness, and safety.

e-SENS results will be handed over to CEF in order to increase the value of the cross-border health services offer to citizens, health professionals, and public administration with fast, secure and seamless electronic access to medical information in the appropriate language.

Acknowledgment

This work has been co-funded by the European Commission (ICT Policy Support Program) and participating Member States through the e-SENS project (contract number 325211, <http://www.esens.eu>). The Authors thank the OpenNCP community for its contribution to the work presented.

References

- [1] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024>
- [2] Connecting Europe Facility, <https://ec.europa.eu/digital-agenda/en/connecting-europe-facility>
- [3] e-Justice Communication via Online Data Exchange, Making Justice Faster, <http://www.e-codex.eu/>
- [4] Building the next generation Points of Single Contact, Making Business Easier, <http://www.eu-spocs.eu/>
- [5] Secure idenTity acrOss boRders linKed 2.0, Making Access Smarter, <https://www.eid-stork2.eu/>
- [6] Pan-European Public Procurement Online, Making Procurement Better, <http://www.peppol.eu/>
- [7] European Patients – Smart Open Services, Making Healthcare Better, <http://www.epsos.eu/>
- [8] TOGAF, an Open Group standard, <http://www.opengroup.org/subjectareas/enterprise/togaf>
- [9] eSENS Reference Architecture, <http://wiki.ds.unipi.gr/display/ESENS/eSENS+Reference+Architecture>

- [10] Guideline on an Organisational Framework for eHealth National Contact Point, eHealth Network, http://ec.europa.eu/health/ehealth/docs/ev_20151123_co01_en.pdf
- [11] Integrating the Healthcare Enterprise, <http://www.ihe.net/>
- [12] ISO/IEC 13888:2010, Information Technology, Security Techniques, Non Repudiation
- [13] F. Ruggeri, European Telecommunications Standards Institute (ETSI) Specifications for Registered E-Mail (REM), ISSE, Springer, 2009, pp 242-254
- [14] The eXtensible Access Control Markup Language, XACML, <https://www.oasis-open.org/standards#xacmlv2.0>
- [15] RFC 3881, G. Marshall, Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications, The Internet Engineering Task Force, September 2004, <https://tools.ietf.org/html/rfc3881>
- [16] ISO/IEC 24727-3:2008, Identification cards -- Integrated circuit card programming interfaces -- Part 3: Application interface
- [17] REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
- [18] OASIS Service Metadata Publishing (SMP) Version 1.0, Committee Specification 01, 18 December 2014, <https://docs.oasis-open.org/bdxc/bdx-smp/v1.0/bdx-smp-v1.0.html>
- [19] European Telecommunications Standards Institute (ETSI) TS 119 612, v1.1.1, Electronic Signature and Infrastructure (ESI), Trust Lists.



François WISNIEWSKI is graduated with a master in Biomedical Engineering from the University of Medicine in Nancy/France. He worked as research engineer in several eHealth R&D projects in Europe. He is now Partnership Officer engineer at the Luxembourg Institute of Science and Technology and focuses his work to develop the eHealth and wellbeing activities.



Dimitrios G. KATEHAKIS is the Head of the Center for eHealth Applications and Services at the Institute of Computer Science of FORTH. He has been scientific responsible for several projects related to the development and deployment of IT software for the healthcare sector. Currently he coordinates the ePrescription and Patient Summary workgroup of the e-SENS project.



Massimiliano MASI, Information Security Architect at Tiani "Spirit" GmbH. He received his Ph.D. in Computer Science from the University of Florence in 2012. He contributed to the development of eHealth projects in Europe, United States, and in Africa, such as epSOS, e-SENS, and IHE security profiles.



IT Architect & Strategic Project Coordinator at the Fraunhofer FOKUS. Soeren BITTINS is taking the lead regarding the aspects of data protection/privacy, standardisation, interoperability and regulatory alignment of innovative technology at an international scope.