04

Interoperability Infrastructure Services to Enable Operational Secure Cross-Border eHealth Services in Europe

Dimitrios G. Katehakis[1], João Gonçalves[2], Massimiliano Masi[3], Sören Bittins[4]

[1] Foundation for Research and Technology – Hellas, Greece
[2] Shared Services of the Ministry of Health, Portugal
[3] Tiani "Spirit" GmbH, Austria
[4] Fraunhofer FOKUS, Germany

Abstract

Safeguarding patient safety, patient rights, and preserving trust are crucial components of providing high quality medical treatments across borders. This work presents technological improvements needed in order to address certain reliability and quality challenges towards enabling seamless care between European healthcare systems. More specifically, it introduces incremental, cross-sectorial advancements to facilitate cross-border access to health services within European Union and associated countries (EU) and to enhance the technology used with cross-domain technical building blocks (BBs) to support non-repudiation, capability lookup, service location, and electronic identification (eID). Non-repudiation registers any attempted access to a patient's protected health information and provides evidence for dis-putes resolution. Service location and capability lookup provide trusted, secure, and efficient mutual configuration for national contact points for eHealth. EID provides the proper authen-tication strength for patients when seeking health care in a cooperating EU member state, as well as safeguarding their fundamental access rights. The evolution of the reference imple-mentation for the national contact point for eHealth (NCPeH), named OpenNCP, is examined, in alignment with the Connecting Europe Facility (CEF) BBs framework. The case of cross-border electronic prescription (eP) and patient summary (PS) services is presented and the use of related international interoperability standards is discussed, together with recommendations for future work.

Keywords

Electronic Identification, Capability Lookup, Service location, Non-repudiation, Electronic Delivery, Cross-border Public Services, Electronic Prescription, Patient Summary.

Correspondence to:
Dimitrios G. Katehakis
Foundation for Research and Technology – Hellas, Institute of Computer Science
N. Plastira 100, Vassilika Vouton, GR-700 13 Heraklion, Greece
katehaki@ics.forth.gr

1. Introduction

Directive 2011/ 24/ EU [1] regulates patients' rights to cross-border care and makes provision for the continuity of their care through a shared PS and the deployment of eP. It also creates the initial legal framework for cross-border care in the EU and establishes the need of a digital infrastructure for the cross-border exchange of health data. The deployment of eHealth solu-tions for eP/ PS is expected to increase safety and quality of care throughout the EU, by en-suring continuity of care across borders and by providing immediate clinical information needed for unplanned care. Greater knowledge of patients' clinical characteristics and treat-ment is expected to improve clinical decision-making [2]. What is envisioned is fewer concerns about possible adverse interactions with current treatment and health conditions (allergies, drug interaction, etc.) and the provision of safer healthcare, in cases of emergency or on occasional basis abroad.

Work presented in this paper was conducted within the context of the Electronic Simple Eu-ropean Networked Services (e-SENS) [3] Large Scale Pilot (LSP) project (2013-2017) and is built on top of assets developed in previous LSP projects to provide common solutions for seamless public service delivery across borders [4]. The project, during its four years of oper-ation, succeeded in creating a pan-European set of IT building blocks for digital public services that embrace both national and sectorial diversity and facilitate interoperability. Focus is on the ongoing activities for implementing non-domain specific solutions in the eHealth domain, to facilitate cross-border eP/ PS services, in order to improve efficiency, cost-effectiveness, safety, and confidence. In other words, work presented, among others, advanced the application of patient rights in Europe in terms of medical records, and e-Prescription by dealing with critical patient safety issues, which require coordinated involvement of experienced stakeholders in Health Service deployment.

Structure of presented work is as follows: Background Section presents the approach followed for improving the NCPeH reference implementation, its relation to accepted architectural ap-proaches, as well as links to related initiatives. Incorporation of cross-domain reusable tech-nical components to provide enhanced, better quality eHealth services for eP/ PS is described in the Results Section. This work introduces digital infrastructure services for non-repudiation (to support evidence emission when backend systems exchange documents, data and/ or mes-sages through access points), service location and capability lookup (to facilitate electronic document exchange across borders), and eID (to enable the use of IDs across countries in the EU). It also presents prospective issues and recommendations for future work. Finally, the Discussion Section concludes and presents work scheduled ahead.

2. Background

The methodology for having non-domain specific BB solutions, outcomes of previous or cur-rent LSP projects, incorporated within the European Patient Smart Open Services (epSOS) [5] infrastructure and consisted of several core phases, further evolved under EXPAND project workings [6]. Starting with the creation of an inventory of existing practices (and solutions) within countries and across the EU and the definition of generic functional requirements for basic cross-sector services, available solutions were pre-selected, following consultation with countries interested in enabling cross-border eP/ PS at an operational level [7]. Based on con-solidated results from other domains, solutions were improved, and generic modules were developed to extend their usage in order to capture the eHealth domain requirements in alignment with member states' priorities. Testing and operating these, common solutions, in selected operational scenarios were the next steps. Based on these experiences, produced specifications were incorporated in the reference implementation for NCPeH [8], which was to be used to support national authorities in the implementation, deployment and maintenance of secure eHealth infrastructures and services for the secure exchange of patient information across borders.

The eHealth domain uses the Integrating the Healthcare Enterprise (IHE) process [9] as foun-dation for building project architectures and evaluating vendors or open source implementation to use. In fact, such process enables Information Technology (IT) software architects to have their system architecture "emerging" by selecting those IHE profiles matching their clinical requirements. An IHE profile defines a set of *actors* and *transactions* that solve one or more specific clinical use cases. Profiles can be *merged* with other profiles allowing the construction of complex software systems devised for the health IT sector. IT software suppliers implement the profiles and participate in testing events named *Connectathons* performing interoperability and conformance testing. After passing the connectathon, vendors and their products are listed in a public registry, where each project coordinator may search for imple-mentations compliant with the profiles selected in the architecting phase. The IHE process is not a substitute of an Enterprise Architecture, which has a broader scope: it enforces the pro-ject continuum, enforces measures to evaluate the return of investments, engages stakeholders at various levels, and identifies several viewpoints of the complex IT system.

The EU commission started the European Interoperability Framework (EIF) [10] as an enter-prise architecture-based framework targeted to the promotion of integration of IT services amongst the EU member states. Following that, ISA2 [11] introduced a reference architecture for guidance for the public administration in producing interoperable public services, the Eu-ropean Interoperability Reference Architecture (EIRA). Being a guideline, the viewpoints of the EIF-EIRA are high level, to give room to IT architects to define and implements technical aspects. As a follow-up for these needs, e-SENS created and implemented such technical viewpoints of the EIF-EIRA, in the e-SENS-

EIRA. EIF and e-SENS embrace the TOGAF enterprise architecture model [12]. In particular, e-SENS tailored the TOGAF architecture development method (ADM) creating specific BBs upon the requirements initially provided by the different domains (i.e. eHealth, eJustice, eProcurement, eAgriculture, etc.). The eHealth domain aimed at enhancing the already defined use cases (for eP and PS) by leveraging on the outcome of the e-SENS EIRA, and providing inputs to it, effectively contributing in four BBs: non-repudiation, capability lookup, service location, and eID. The e-SENS meta-model [13] defines a building block (BB) as a set of capabilities that are leveraged in cross-border eServices; in particular BBs are assembled in business process to realize eServices. This latter sentence has been considered crucial for the IHE process of the eHealth domain: the Business Process used to realize the eP/ PS services is the IHE merge operation. EIRA identifies three levels of BBs: the solution architecture template (SAT) containing the business processes assembling a set of blocks to provide business needs, an architectural BB (ABB) describing the intention and specification of a given capability, and the solution BB (SBB) describing the solution realizing a specific ABB.

Projects like epSOS, EXPAND, e-SENS and eStandards [14] have worked in trying to resolve European level compatibility and sustainability of the underlying national infrastructures re-quired to support the reliable and secure exchange of medical data, as well as the readiness to address continuously evolving interoperability, legal and security requirements in a cross-border setting. PS guidelines on data that can be exchanged electronically across borders [15] provide the first draft of the guidelines. Their purpose is not only to describe what data is to be included in the PS but also to assess the implications of adopting such a PS in practice, especially regarding organizational, technical and semantic requirements. The eP guidelines adopted in 2014 [16] indicate areas where further work is required in order to ensure that clin-ical need and patient safety requirements are taken into account.

Regulation (EU) No 910/ 2014, commonly known as eIDAS [17], aims at providing a com-mon, pan-European authentication scheme for notifiable eID, enabling national eID being properly consumed by service providers across the EU, regardless of where it was issued or is operated. EIDAS provides with legal grounds for the mutual recognition of eIDs across bor-ders [18]. The idea is to create technical gateways that broker trust across Europe by issuing, authenticating, translating, certifying, and maintaining eID and their relevant attributes.

As of January 2016, the OpenNCP [19] governance model shifted under the direct responsi-bility of the European Commission, Directorate General for Health and Food Safety (DG SANTE). The goal set was to move the epSOS eHealth pilot OpenNCP into the global Euro-pean CEF framework project under the umbrella of a CEF Digital Service Infrastructure (DSI), the eHealth DSI. Priorities set regarding cross-border eP/ PS relate to the improvement of existing cross-sectorial BB solutions to become operational ready so that member states can adopt them. In this context, all related integration is conducted within the OpenNCP framework, which is the selected NCPeH reference implementation to support cross-border eP/ PS.

3. Results

Outcomes of work conducted for non-repudiation, capability lookup, serviced location, and eID are presented in the following subsections including the rationale behind each BB's adop-tion, development made for their incorporation in OpenNCP, issues resolved, status, and out-look.

3.1 Non-repudiation

The e-SENS access control white paper [20] defines *"Non-repudiation services are mandated 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 the event or action".* The exchange of non-repudiation artifacts (tokens, or evidence) is defined as non-repudiation protocol. The need of having non-repudiation services emerged since the beginning of the epSOS project, but then left unimplemented due to piloting relaxations. The epSOS solution aimed at having audit trail and node authentication (ATNA) [21], achieved by means of mutual transport layer security (TLS). Audit trails is a mean to reach non-repudiation sufficient for the pilot. Unfortunately, the IHE ATNA profile leverages the syslog protocol [22] to send audits to the storage, named audit record repository (ARR). Audits are sent before an event occurs and when the event is occurred, e.g., before sending a message, and when a message is received.
ATNA audits [23] defines the following data formats:
• Event Identification: what was done
• Active Participant Identification: by whom
• Network Access Point identification: initiated from where
• Audit Source Identification: using which server
• Participant Object Identification: to what record
Audit trails are effectively reliable data sent over unreliable channels. Audits are designed on a best-effort principle: the audit creator and the ARR cooperate together to safely store the data, but without any guarantee.

In [24] the authors highlight the need of the following basic non-repudiation evidence: the non-repudiation of origin (NRO), of submission (NRS), of delivery (NRD) and of receipt (NRR). Moreover, [25] defines properties that non-repudiation protocols shall meet. In particular, three are defined:

- Efficiency: if no error occurs, non-repudiation services shall not intervene
- Timeliness: if a transaction has been terminated (or delayed) parties will know the sta-tus of a transaction eventually
- Fairness: each party holds the expected items at the end of the protocol run. In particular, fairness is subsequently divided in
  - Strong, when the exchange is completed, sender A can prove to an arbitrator that recipient B has received (or still can receive) the item, without any further need of cooperation from either B or any trusted third party.
  - Weak, when the exchange is completed, A can prove that B has received (or still can receive) the item, or otherwise an affidavit can be presented to demon-strate that B misbehaved or a network failure occurred.
  - Eventually Strong, when fairness is ensured within the system but the provi-sion that additional assumptions about the participating parties are made.

ATNA audit trails do not respect the above defined properties.

The non-repudiation ABB provides a flexible and horizontal model to generate and emit elec-tronic evidence used for non-repudiation purposes, based on each domain respective regula-tions and technological needs. The non-repudiation ABB enables different domains to imple-ment their own non-repudiation protocol with the properties needed to achieve their business needs.

The core of the e-SENS solution is the evidence emitter (EE) ABB. This BB defines an actor which is designed to act upon self-defined events and that, based on the execution policy, de-fines the syntax of the evidence to be stored based on the ISO 13888 standard [26]. Since ISO specifies an abstract notation for the definition of non-repudiation evidence, the EE ABB in-troduces a mapping between the standard and the extensible markup language (XML) notation derived by ETSI REM [27]. It is worth noticing that REM evidence has been devised for the exchange of registered emails, and thus the full standard comes with a specific security model. The EE ABB inherits only the XML syntax of the evidence. The non-repudiation ABB is composed by the following capabilities realization, as shown in *Figure 1.*

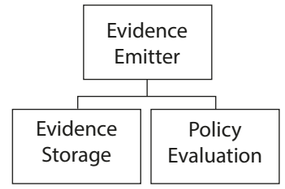

Figure 1: Evidence Emitter ABB relationships with other ABBs

The Evidence Storage provides a request/ response protocol that interfaces to a storage engine of any kind (e.g., a Revision Safe Archive). The policy evaluation provides the functional requirements on how an extensible access control markup language (XACML) [28] policy can be used to generate evidence, and the PerHop protocol [29] defines an eventually strong fair protocol for a web-service infrastructure.

XACML policies provides a flexible way to encode organizational constraints into XML format. XACML defines a policy programming language that evaluates an execution context to provide an authorization decision and return obligations that a policy enforcement point (PEP) shall execute. XACML has been proposed as a way to encode the Pol field of the non-repudiation token, effectively formalizing the execution scenario of the non-repudiation protocol. The field in the evidence can be considered the unique policy id in the XACML policy repository. The policy obligations encode non-repudiation values that the PEP (merged as the evidence emitter) will include in the evidence XML enabling for different non-repudiation specific messages.

The EE ABB has been formally proved by using a model-checking approach, using Casper + FDR [30][31].

3.2 Service Location and Capability Lookup

In cross-border eHealth, the central configuration services (CCS) are a way towards achieving NCPeH fully automated configuration. CCS are thus used to create, share and maintain in a secure environment some common data needed by the NCPeH to establish business transactions, e.g. web services endpoints and certificates. During the epSOS LSP, CCS was specified as "virtual central services", i.e. the configuration information of each NCPeH was

distributed by itself in its own infrastructure, being discoverable and reachable through hypertext transfer protocol (HTTP) queries to domain name system (DNS) served pointers. Albeit having a specification, its compliant implementation was never materialized. Instead, an ad-hoc solution was set up. The latter was based on a publish-polling mechanism of ETSI trusted service list (TSL) [32] files adapted for eHealth specificities, also called NCP service status list (NSL). On one side one of the NCPeH would create and publish its NSL file in a central shared folder through secured file transfer protocol (SFTP), while on the other side the other NCPeH would periodically poll the central folder in order to synchronize (through secure HTTP) the former's NSL file in its internal configurations.

Apart from being a process where the time-based polling was frequently dropped in favor of manual triggering, the configuration information provided through NSL files was limited to static data like endpoints and certificates. This was limiting the sharing of information such as the international search masks (the set of a country's identification traits used for cross-border patient identification) and other kinds of complex information that could require a more flexible data model to be accommodated. In order to internationalize formally isolated national certification authorities, it has been adopted the direct brokered trust model [33]. The remote NCPeh would self-configure using remote data signed by the national competent authority governing the country's NCPeH, anchoring a verifiable trust chain by relying on the trust service provider direct trust as formally made possible by [34] and each NCPeH would act as the trust broker between the national infrastructure it's protecting and the other NCPeH.

This picture paved the way for e-SENS introducing the Service Location and Capability Lookup BBs [35][36] as a standardized solution for eHealth CCS. These two BBs, coming from the eDelivery architectural solution [37], fit on the four-corner model on which cross-border eHealth is based: corners 2 and 3 being the NCPeH, while 1 and 4 being their related national infrastructures. Both BBs act on corners 2 and 3. The service location BB enables the dynamic discovery of the location of other NCPeH-declared interoperability capabilities. The capability lookup BB enables the publishing and fetching of the latter. Together they automate the peer's dynamic discovery and fetch of NCPeH self-declared capabilities (metadata). These two BBs are built on top of open standards - the OASIS business document metadata service location (BDX-Location) and service metadata publishing (BDX-SMP) [38][39], which are themselves a product of a generalization and consolidation of specifications created for the purpose of another European LSP project, PEPPOL [40], thus promoting their cross-sectorial use. These two BBs leverage an infrastructure based on three core components (servers): service metadata publisher (SMP), service metadata locator (SML) and DNS. With SML and DNS, the dynamic delegation discovery system (DDDS) pattern [41], targeted by BDX-Location is set up. This allows:

- the usage of URI-enabled naming authority pointer (U-NAPTR) DNS resource records to point to URLs of specific types of metadata services (SMP) upon a lookup, and
- the creation and update of DNS records through SML, triggered by requests on the SMP.

With SMP, the XML metadata following the data model defined by BDX-SMP is exposed in a RESTful way under the DNS-served URLs. *Figure 2* depicts the high-level overall use case.

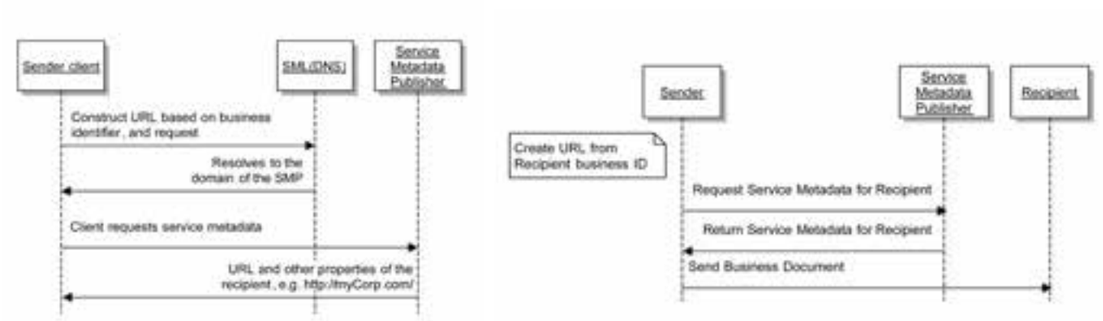

Figure 2: On the left: discovery of a peer's metadata. On the right: fetch and usage of the metadata. [42]

The integration of this BB into the OpenNCP reference implementation starts with a mapping between the NSL and SMP data models, to later completely replace it – as well as the TSL-editor tool used to create the former – by a new web client aligned with OASIS standards and the SMP server interface specification from CEF eDelivery DSI, capable of creating BDX-SMP metadata, applying the eHealth national authority signature and publishing the metadata in the SMP/ SML/ DNS centralized infrastructure. The appropriate standardized security measures are set up, as shown in *Figure 3.*

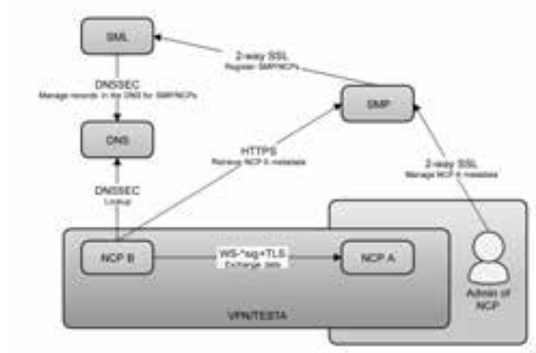

Figure 3: eHealth security infrastructure [43]

The adoption of these BB has been specified by a change proposal [44] aimed to amend the eHealth DSI specifications and to be included in the set of eHealth DSI artefacts to be consid-ered by member states. These BB have also been subject to some conformance testing under the supervision of IHE in EXPANDathon 2015 [45] and IHE-Europe Connectathon 2016 [46], and were also piloted in e-SENS.
The OASIS standards adopted in eHealth were also graded by the e-SENS BB maturity as-sessment workgroup, with BDX-SMP having been considered as "sufficiently mature for fur-ther promotion and adoption" [47] and BDX-Location as "essential for cross-border services" [48].

In the scope of the CEF eHealth DSI, DG-SANTE is foreseen to be the owner of the eHealth central SMP server, keeping straight collaboration with the CEF eDelivery DSI (DG-DIGIT) for the cross-domain SML and DNS components. While initially foreseen as a completely centralized infrastructure, effort can be put by Member States in decentralizing the SMP com-ponent, to progressively have national SMP servers instead of the central one. SML and DNS are envisioned to be kept centralized, as a way to support multiple business domains.

No major issues have been found regarding the adoption of these standards in eHealth. Still there is a path towards its full integration.

3.3 Electronic Identification

Strong electronic identification (eID) within the eHealth domain is motivated by two primary goals: patient safety as well as protection against illegitimate disclosure of medical data. Al-most every national health system features one or more types of eID and the relevant national regulation and norms effectively govern its appropriate regional application. This, however, yields a pan-European eID landscape of various fairly isolated and incompatible eID solu-tions.

Typical technical issues hinder an efficient eID harmonization, such as the need for various smartcard drivers and middleware, the inability to reach foreign security services (e.g. elec-tronic signature services, etc.), or the inability to deploy non-certified software (drivers, ap-plets, scripts, etc.) onto highly regulated medical systems, especially at the point of care (PoC). In addition to specific technical issues, the most critical field of work is the mainte-nance of the legitimate-use of a national eID means across borders. Many were, from an ad-ministrative and legal perspective, not designed to facilitate or support an international medical data exchange and impose unjust burdens or specific environmental requirements incompatible with the organization of work on/ in the foreign health systems.

The e-SENS project attempted to address many of the issues through a gradual migration from purely organizational patient identification facilities, through strong smartcard-based authentication and authorization towards full reliance on virtual authentication schemes, in particular eIDAS eID. In a first step, the eHealth team of the project designed a software component that harmonized the means to operate routine smartcard functions, such as elec-tronic signatures, authentication or data extraction, while simultaneously eliminating any need for specific drivers or middleware. Instead, a singular ISO24727-3 [49] compliant middleware encapsulates and provides access to all card functions regardless of the type of the supported eID token. Smartcards integrate through configuration items, CardInfo files, which define the general structure, capabilities, and record locations of a card *(Figure 4).*

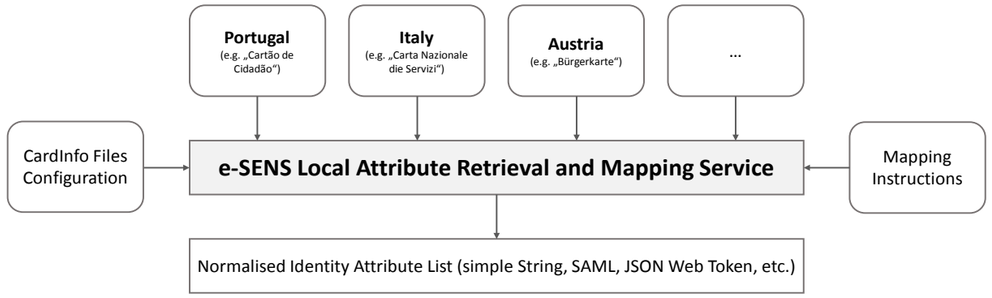

Figure 4: e-SENS Local Attribute Retrieval and Mapping Service (LARMS)

This configuration is assisted by specific mapping rules that link the proprietary information as stored on the card into a mutually shared general information model *(Figure 5)*.

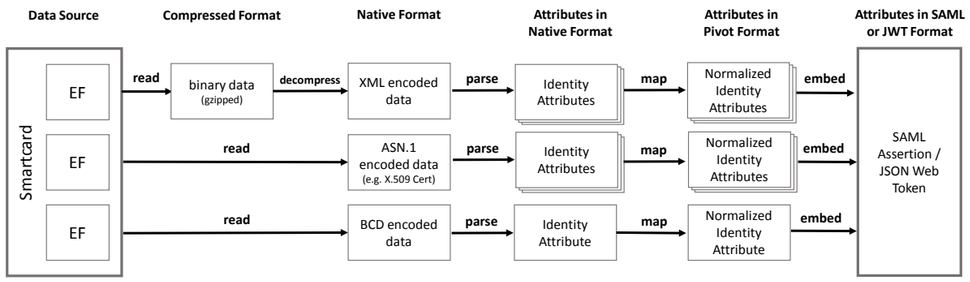

Figure 5: LARMS provides this functionality as the basic access means for any smartcard.

The operating burden has been minimized further by compiling the CardInfo files into card recognition trees that enable an auto-detection and subsequent auto-configuration of the e-SENS eID components for any supported eID token. The e-SENS Local Authentication Mod-ule (LAM) provides access to the higher card functions, such as protected authentication or the application of electronic signatures using digital certificates stored on and protected by the smartcard. The orchestration of LARMS and LAM to work complimentary of each other ena-bles the local providence of electronically signed assertion that contain authenticated attributes of the patient. Both, LARMS and LAM generate an entirely harmonized output of the extracted information in either IHE XUA [50] compliant SAML 2.0 Assertions or JSON Web Token (JWT) [51] for REST-oriented environments. Those authentications can be requested through WS-Trust Request Security Token (RST) messages [52], while the application and validation electronic signatures for both, assertions and consumer documents, are accessible in compliance to the OASIS digital signature services (DSS) [53].

In a second evolution, all of the above functionality and the card-processing framework were isolated from each other into individual, independent services and were subsequently separat-ed into a loosely coupled software ecosystem, the e-SENS eHealth eID Components. The latter can be either tightly integrated into existing eHealth services or operated as supporting services alongside with the existing solutions. The end-user portion of the service framework is compiled into a comprehensive, authenticity, and integrity-safeguarded Java WebStart (JWS) package that can be temporarily deployed and launched at the PoC through the Java Network Launching Protocol (JNLP). The package either contains its initial configuration or dynamically retrieves all relevant configuration items at runtime through SML. The e-SENS eHealth eID Components have been fully integrated into the NCPeH.

The e-SENS eHealth eID Components were tested towards compliance and usability through several international testing events as well as by simulating healthcare encounters with medical professionals. While the consolidation of technology and the greatly increased degree of security were confirmed, the underlying technology of smartcards itself was considered to have hit a glass ceiling: no further developments for this technology were anticipated to yield critical improvements towards usability or security in particular in reference to mobile appli-cations. Consequently, the e-SENS project evaluated other upcoming candidate technologies in order to virtualize the eID token itself for a more streamlined, user-friendly, and universally deployable solution. The CEF eID BB [54], or eIDAS eID, was quickly identified as the most promising solution component, not only because of the standardized way of transporting au-thentications between the relevant parties but in particular due to the stable legal framework encompassing the eIDAS eID service. The latter enabled the eHealth domain to shed the en-tirely redundant maintenance of a separate eID ecosystem with the heavyweight overhead of governing the legal stability of highly-regulated exchanges between mutually dependent parties and eID solutions as well as their pending national constraints in favor of the eIDAS regu-lation.

While the technology mandated by eIDAS eID and its ancillary trust services is fundamentally compatible with the routine solutions of the eHealth domain, some legal and organizational issues hindered a swift integration. The two major obstacles during the e-SENS project were the premature termination of an eIDAS eID workflow and the lack of injecting an additional attribute into the eIDAS minimum data set (MDS) benefitting of all routine protection means of eIDAS eID. The first concern addresses the need to have the legitimate authentication available to all relevant stakeholders, even after a patient has been successfully authenticated in the foreign country. For eIDAS eID, the authentication workflow terminates here, while the eHealth domain relies on this authentication being send back to the patients' country of affili-ation to serve as an authenticated supporting token for the national access control systems in the determination of whether the disclosure request for protected health information is indeed legitimate and authorized. The other issue relates to the mandatory expressiveness of the eI-DAS data structure to perform an identification. For a regular eGovernment use case, the mandatory attributes, such as name, date of birth, and address are sufficient to univocally identify a citizen. A patient, and – more precisely – the assigned medical records, however, are usually exclusively identified by the patient identifier instead of general demographics. While patient mapping services naturally exist, an authenticated patient identifier needs to be available at a very early point in the workflow – the initial patient registration in the foreign country – and at the very late point of authorizing a medical data disclosure in the patients' country of affiliation. Consequently, the inclusion of the patient identifier in the eIDAS eID SAML Assertion is of utmost importance for the eHealth domain.

The first issue was successfully tackled by grouping the eIDAS eID SAML Assertion as an additional protection token in a policy-push fashion with the clinical transaction, while the second concerns caused an extension to the eIDAS Nodes and Connectors in compliance with the eIDAS implementing acts [55]. An eHealth application is now able to retrieve the SAML metadata of an eIDAS Node and scan for the existence and definition of an additional attribute, the patient identifier. As long as this attribute is published, the eIDAS Connector then requests not only the MDS but also this attribute. The back-office systems of the operating countries are responsible for populating the patient identifier and for preserving the overall authentication assurance level (AAL) of the resulting eIDAS SAML assertion *(Figure 6)*.

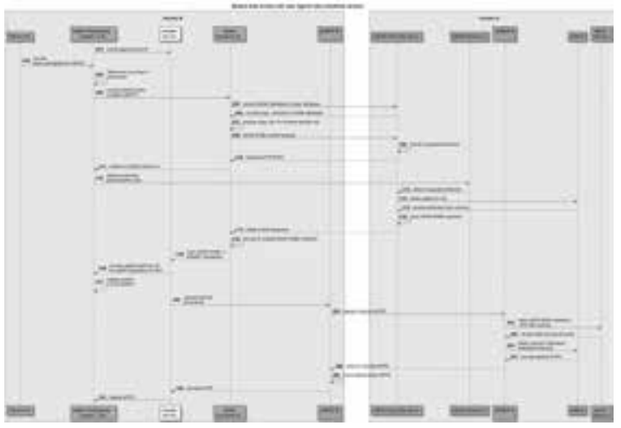

Figure 6: Medical Data Access with User Agents

The e-SENS project developed an eIDAS Connector that bridged the requirements of the eHealth domain with the capabilities of eIDAS eID and integrated a technology demonstrator into the NCPeH to enable production-level piloting between Austria, Italy, and Greece.

The piloting generated immediate first-hand experiences and ultimately confirmed the general fitness for use of eIDAS eID for the eHealth domain for real-world cross-border eHealth ser-vices. Some room for mutual improvement, especially regarding the usability of the solution, has been identified. The most pressing issue are the alignment of legal instruments that cur-rently work in concurrence instead of complimenting each other: the patient consent is the fundamental instrument legitimating any medical data disclosure and includes specific provi-sions for technology that is used to regulate the disclosure. eIDAS eID relies on a similar con-cept to satisfy the requirements of the relevant regulation and mandates the citizen to explicit-ly select all attributes that are authorized to be disclosed. This strained the piloting efforts since every eIDAS-activated eHealth identification required two independent but redundant and exhaustingly specific consents to be issued in close proximity. Succeeding in merging both legal instruments into one would streamline the eID process, critically increase usability without eroding any patient right to confidentiality and disclosure control, while benefitting from the general legal stability and security of the eIDAS framework.

4. Discussion

Work presented in this paper has advanced the application of patient rights in Europe in terms of medical records, and e-Prescription by dealing with critical patient safety issues, which require coordinated involvement of experienced stakeholders in Health Service deployment. Issues addressed included patient identification, locating capabilities of remote services, to-gether with addressing liability issues to support non-repudiation on a more solid ground to enable and support efficiently the delivery of cross-border healthcare.

It is proposed that the analysis and evolution of the potentially outdated original epSOS secu-rity architecture and its associated tools is continued with a particular emphasis on the specific impacts as mandated through eIDAS. The e-SENS project has kick-started that process by providing solutions towards three critical open issues – namely eID, documentation of digital evidences & dispute regulation, as well as trust bootstrapping & mutual configuration – as a blueprint for further work that needs to be performed. On top of technical outcomes, recommendations for relevant policy level actions such as eID solutions supporting eIDAS, have also been handed over to the EU member states community of the joint action supporting the eHealth Network (JASEHN) [56].

Developing safe and high-quality eHealth services across borders in the EU requires coordi-nated work by several member states at multiple levels (technical, semantic, organizational, legal and political). The work presented addressed reliability and quality challenges and intro-duced security improvements for better and safer cross-border eHealth services. Prospects for operational services are high, and outcomes of the work presented succeeded in making the ICT infrastructure inherited by epSOS more sustainable and more stable. Outcomes of this work (a set of mature eHealth assets) have already become part of the CEF [57] eHealth DSI Interoperability Specifications [58].

Their implementation by member states is (already) being funded by the EU through current [59] and future Generic Services Calls, paving the way for operational services to be enabled under the CEF programme. National/ Regional initiatives concentrate on specific business needs according, e.g., to local regulations. The inception of new Cross-Border health applica-tion, to facilitate the internationalization of such existing national services, is currently driven by the eHealth DSI. Already several proposals have been approved for the deployment of Generic Cross Border Services in Malta, France, Portugal, Finland, Cyprus, Italy, Luxembourg, Greece, Ireland, Estonia, Croatia, Sweden, Germany, Czech Republic, Austria and Hungary [60]. Future work is already in progress.

Acknowledgements
The European Commission, and more specifically the Information and Communication Technologies Policy Support Programme (ICT-PSP) of the Competitiveness and Innovation Framework Programme (CIP), partially supported work reported in this paper, under the e-SENS project (contract number 325211). The authors would like to thank all members of the e-SENS project eP/ PS working group for contributions to the work presented. Any opinions, results, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of e-SENS or the European Commission.

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 [cited 2017 May 29]. Available from: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32011L0024
[2] Moharra M, Almazán C, Decool M, Nilsson A L, Allegretti N, Seven M. Implementation of a cross-border health service: physician and pharmacists' opinions from the epSOS project. Family Practice, 2015, 32(5), 564-567.
[3] Electronic Simple European Networked Services [cited 2017 August 1]. Available from: https://www.esens.eu/
[4] Wisniewski F, Katehakis D G, Masi M, Bittins S. Improving Cross-Border European ePrescription and Patient Summary Services through e-SENS Cross-Sectorial Building Blocks, in Global Telemedicine and eHealth Updates: Knowledge Resources, Volume 9, 2016, International Society for Telemedicine & eHealth (Editors: Malina Jordanova and Frank Lievens), pp. 234-238.
[5] European Patient Smart Open Services [cited 2017 August 1]. Available from: http://www.epsos.eu/
[6] EXPAND: Deploying sustainable cross-border eHealth services in the EU [cited 2017 August 1]. Available from: https://ec.europa.eu/digital-single-market/en/news/expand-deploying-sustainable-cross-border-ehealth-services-eu
[7] E-SENS (2015). D5.4-2: Second-wave Update of Plans and Status of Domain and National Pilots in eHealth, [cited 2017 May 29]. Available from: https://www.esens.eu/sites/default/files/e-SENS_D5.4-2_e-Health.pdf
[8] eHealth Network (2015). Guideline on an Organisational Framework for eHealth National Contact Point, Brussels, [cited 2017 May 26]. Available from: http://ec.europa.eu/health/ehealth/docs/ev_20151123_co01_en.pdf
[9] IHE Process [cited 2017 May 29]. Available from: http://www.ihe.net/IHE_Process/
[10] European Interoperability Framework (EIF) [cited 2017 August 1]. Available from: https://ec.europa.eu/isa2/eif
[11] ISA2 [cited 2017 August 1]. Available from: https://ec.europa.eu/isa2/
[12] TOGAF version 9.1 [cited 2017 June 6]. Available from: http://www.opengroup.org/architecture/togaf/
[13] e-SENS Metamodel [cited 2017 May 30]. Available from: http://wiki.ds.unipi.gr/display/ESENS/eSENS+Metamodel/
[14] eStandards [cited 2017 August 1]. Available from: http://www.estandards-project.eu/
[15] eHealth Network (2013). Guidelines on minimum/ nonexhaustive patient summary dataset for electronic exchange in accordance with the cross-border Directive 2011/ 24/ EU. European Commission, Version 1.0. [cited 2017 May 26]. Available from: http://ec.europa.eu/health/ehealth/docs/guidelines_patient_summary_en.pdf
[16] eHealth Network (2014). Guidelines on ePrescriptions dataset for electronic exchange under Cross-Border Directive 2011/ 24/ EU. European Commission, Release 1. [cited 2017 May 26]. Available from: http://ec.europa.eu/health/ehealth/docs/eprescription_guidelines_en.pdf
[17] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [cited 2017 May 30]. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[18] Iglezakis I. Legal Issues of Identity Management in eGovernment. Social Science Research Network. Social Science Research Network, 2015. [cited 2017 May 26]. Available from: http://ssrn.com/abstract=2690374
[19] Fonseca M, Karkaletsis K, Cruz I, Berler A, Oliveira I C. OpenNCP: a novel framework to foster cross-border e-Health services. In Cornet R, et al, Studies in Health Technology and Informatics, vol. 210: Digi-tal Healthcare Empowering Europeans (pp. 617-621), Amsterdam, 2015. [cited 2017 May 26]. Available from: http://person.hst.aau.dk/ska/MIE2015/Papers/SHTI210-0617.pdf
[20] E-SENS Whitepaper. Non-Repudiation [cited 2017 May 30]. Available from: http://wiki.ds.unipi.gr/display/ESENS/Whitepaper+-+Non+Repudiation
[21] IHE, Audit Trail and Node Authentication [cited 2017 May 30]. Available from: http://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication
[22] Network Working Group, Request for Comments: 5424 [cited 2017 May 30]. Available from: https://tools.ietf.org/html/rfc5424
[23] Network Working Group, Request for Comments: 3881 [cited 2017 May 30]. Available from: https://tools.ietf.org/rfc/rfc3881.txt
[24] Onieva J, Zhou J. Secure Multi-Party Non-Repudiation Protocols and Applications, Springer-Verlag, 2008
[25] Asokan A. Fairness in Electronic Commerce, [cited 2017 June 6]. Available from: https://www.researchgate.net/publication/2281851_Fairness_in_Electronic_Commerce
[26] ISO/IEC 13888-3, IT Security Techniques, Non-Repudiation – Part 3: Mechanisms using asymettric techniques
[27] ETSI TS 102 640-2 V2.2.1, Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM [cited 2017 May 30]. Available from: http://www.etsi.org/deliver/etsi_ts/102600_102699/10264002/02.02.01_60/ts_10264002v020201p.pdf
[28] OASIS XACML v2.0, [cited 2017 June 6]. Available from: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[29] Aranha H, Masi M. The E-SENS PerHop protocol, [cited 2017 June 6]. Available from: http://wiki.ds.unipi.gr/display/ESENS/PR+-+PerHopProtocol
[30] Lowe G. Casper: a Compiler for the Analysis of Security Protocols, [cited 2017 June 6]. Available from: http://www.cs.ox.ac.uk/gavin.lowe/Security/Casper/casper.ps
[31] FDR, The CSP Refinement checker, [cited 2017 June 6]. Available from: https://www.cs.ox.ac.uk/projects/fdr/
[32] ETSI TS 102 231 V3.1.2 (2009-12), Electronic Signatures and Infrastructures (ESI); Provision of harmo-nized Trust-service status information. [cited 2017 May 28]. Available from: http://www.etsi.org/deliver/etsi_ts/102200_102299/102231/03.01.02_60/ts_102231v030102p.pdf
[33] OASIS WS-Trust 1.3, [cited 2017 August 1]. Available from: http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html
[34] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Commu-nity framework for electronic signatures; [cited 2017 May 30]. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093
[35] eSENS Reference Architecture [Internet]. ABB - Service Location. [cited 2017 May 28]. Available from: http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Service+Location+-+1.1.0
[36] eSENS Reference Architecture [Internet]. ABB - Capability Lookup. [cited 2017 May 28]. Available from: http://wiki.ds.unipi.gr/display/ESENS/ABB+-+Capability+Lookup+-+1.6.0
[37] CEF Digital Home [Internet]. eDelivery: Supporting secure and reliable exchange of data and documents. [cited 2017 June 7]. Available from: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery
[38] OASIS [Internet]. Business Document Metadata Service Location Version 1.0. Candidate OASIS Standard 01. [cited 2017 May 28]. Available from: http://docs.oasis-open.org/bdxr/BDX-Location/v1.0/BDX-Location-v1.0.html
[39] OASIS [Internet]. Service Metadata Publishing (SMP) Version 1.0. Candidate OASIS Standard 01. [cited 2017 May 28]. Available from: http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/bdx-smp-v1.0.html
[40] PEPPOL: Pan-European Public Procurement Online [cited 2017 August 1]. Available from: https://peppol.eu/
[41] Network Working Group, Request for Comments: 3401 [cited 2017 June 7]. Available from: https://tools.ietf.org/html/rfc3401
[42] OASIS. Service Metadata Publishing (SMP) Version 1.0, Committee Specification 03, 30 June 2016. [cited 2017 June 7]. Available from: http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/cs03/bdx-smp-v1.0-cs03.html
[43] Ferial A. SML/SMP/eDelivery PKI Impact Assessment for the CEF eHealth DSI [Internet]. Version 1.1. 2015 [cited 2017 May 28]. Available from: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210473/Impact%20assessment%20v1%201.pdf?version=1&modificationDate=1481557941264&api=v2
[44] Masi M, Cunha J. eHealth DSI Change Proposal - Add SMP/SML capabilities [Internet]. Version 1.0. 2017 [cited 2017 May 28]. Available from: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210522/CP-eHealthDSI-002_SMP%20SMLCapabilities_v1.0.pdf?version=1&modificationDate=1488205346718&api=v2
[45] EXPANDathon - Lisbon, December 2015 [cited 2017 August 1]. Available from: https://gazelle.ihe.net/content/expandathon-lisbon-december-2015
[46] IHE-Europe Connectathon 2016, RuhrCongress Bochum, April 11-15, 2016 [cited 2017 August 1]. Avail-able from: http://connectathon.ihe-europe.net/connectathon/bochum-2016
[47] Verhoosel J, Roes J, Tepandi J, Vallner U, Cirnu C, Zamfiroiu A, Rotuna C, Celik V, Adalier O, Karabat C. D3.2 Assessment on the maturity of building blocks: second cycle [Internet]. Version 2.0. 2015 [cited 2017 May 28]. Available from: https://www.esens.eu/sites/default/files/e-sens_d3.2_part2.pdf
[48] Verhoosel J, Roes J, Tepandi J, Vallner U, Cirnu C, Ilioudis C, Papanikolaou A, Stassis A, Kingstedt A, Forsberg M, Pedersen S, Isaksson H, Santesson S, Alcaide A, Celik V, Adalier O, Karabat C. D3.2 As-sessment on the maturity of building blocks: first cycle [Internet]. Version 1.0. 2014 [cited 2017 May 28]. Available from: https://www.esens.eu/fileadmin/images/user-uploads/e-SENS_D3.2_Assessment_on_the_maturity_of_building_blocks.pdf
[49] ISO/IEC 24727-3:2008, Identification cards -- Integrated circuit card programming interfaces -- Part 3: Application interface [cited 2017 May 30]. Available from: https://www.iso.org/standard/43809.html
[50] IHE Initiative: Cross Enterprise User Assertion (XUA), [cited 2017 June 7]. Available from: http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf , sec 3.40.
[51] IHE Initiative: Internet User Authorization, [cited 2017 June 7]. Available from: http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_IUA.pdf
[52] OASIS, Web Service Trust, version 1.4, [cited 2017 June 7]. Available from: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/os/ws-trust-1.4-errata01-os-complete.html
[53] OASIS, Digital Signature Services [Internet], [cited 2017 June 7]. Available from: https://www.oasis-open.org/standards#dssv1.0
[54] CEF Digital Home [Internet]. eID: Helping public and private Service Providers extend the use of their online services to citizens from other European countries. [cited 2017 June 7]. Available from: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery
[55] eIDAS - Implementing Acts [Internet]. [cited 2017 May 30]. Available from: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID
[56] JASEHN Joint Action to Support the eHealth Network [cited 2017 August 3]. Available from: http://jasehn.eu/
[57] Connecting Europe Facility [cited 2017 August 1]. Available from: https://ec.europa.eu/inea/en/connecting-europe-facility
[58] eHealth DSI Interoperability Specifications [cited 2017 May 29]. Available from: https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Specifications
[59] CEF-TC-2017-2: eHealth [cited 2017 August 1]. Available from: https://ec.europa.eu/inea/sites/inea/files/2017-2_ehealth_calltext_superfinal_060517_.pdf
[60] CEF-TC-2015-2: List of Selected Proposals [cited 2017 August 1]. Available from: https://ec.europa.eu/inea/sites/inea/files/cef-tc-2015-2.pdf