Secure Cross-Border eHealth Services in Europe

Dimitrios G. Katehakis1, João Gonçalves2, Massimiliano Masi3, Sören Bittins4
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 disputes resolution. Service location and capability lookup provide trusted, secure, and efficient mutual configuration for national contact points for eHealth. EID provides the proper authentication 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 implementation for the national contact point for eHealth (NCPhE), 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.

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 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 solutions for eP/PS is expected to increase safety and quality of care throughout the EU, by ensuring continuity of care across borders and by providing immediate clinical information needed for unplanned care. Greater knowledge of patient’s clinical characteristics and treatment 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 European 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 operation, 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 confidentiality. 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.

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 NCPhE [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 foundation 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 trans-actions 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-rompe 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-
Audit trail and node authentication (ATNA) [21], achieved by the epSOS project, but then left unimplemented due to non-repudiation services emerged since the beginning of is defined as non-repudiation protocol. The need of having exchange of non-repudiation artifacts (tokens, or evidence) the occurrence or non-occurrence of the event or action”.

The maintain, make available, and validate evidence concerning repudiation services are mandated to generate, collect, operational ready so that member states can adopt them. Priorities set in the OpenNCP framework, which is the selected NCPeH framework project under the umbrella of a CEF Digital Service Infrastructure (DSI), the eHealth DSI. Priorities set by 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-pan CEF framework project under the umbrella of a CEF Digital Service Infrastructure (DSI), the eHealth DSI. Priorities set regarding cross-border ePS 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 ePS guidelines adopted in 2014 [16] indicate areas where further work is required in order to ensure that clinical need and patient safety requirements are taken into account.

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-pan CEF framework project under the umbrella of a CEF Digital Service Infrastructure (DSI), the eHealth DSI. Priorities set regarding cross-border ePS 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.

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 pilots 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 status 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 demonstrate that B misbehaved or a network failure occurred.
- Eventually Strong, when fairness is ensured within the system but the proviso 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 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). This entity 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-roduces 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.

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 Po field of the non-repudiation token, effectively formalizing the execution scenario of the non-repudiation protocol. The field in 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) files adapted for eHealth specificities, also called NCPEH service status list (NSSL). On one side one of the NCPEH would create and publish its NSSL 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 NSSL 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 NSSL 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 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 ESP project, PEPPOL [40], thus promoting their cross-sectorial use. These two BBs leverage an infrastructure based on three core components (servers): metadata service 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 XM 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.

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.

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, applets, 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 maintenance 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 ISO/24727-3 (49) compliant smartcard 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 2: On the left: discovery of a peer’s metadata. On the right: fetch and usage of the metadata. [42]
The operating burden has been minimized further by compiling the Cardinfo files into card recognition trees that enable an auto-detection and subsequent auto-configura-
tion of the e-SENS eID components for any supported eID token. The e-SENS Local Authentication Mod-ule (LAM) pro-
vides 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-blis the local providence of electronically signed assertion that contain identifica-
tion attributes of the patient. Both, LARMS and LAM generate an entirely harmonized output of the extracted information in either X.509 [50] compliant SAML 2.0 Assertions or JSON Web Token (JWT) [51] for REST-oriented environ-
ments. Those authentications can be requested through WC-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 subsequent-
ly separated 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
includes 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 encoun-
ters 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 par-
ticular in reference to mobile applications. 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 transport-
ing authentication or the application of electronic signatures between the relevant parties but in partic-
ular 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 min-
imum 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 affiliation 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 au-
thorized. The other issue relates to the mandatory expres-
siveness of the eIDAS data structure to perform an identifi-
cation. For a regular eGovernment use case, the mandatory
attributes, such as name, date of birth, and address are suf-
cient to univocally identify a citizen. A patient, and – more precisely – the assigned medical records, however, are usu-
ally 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 identi-
 fier and for preserving the overall authentication assurance level (AAL) of the resulting eIDAS SAML assertion
(Figure 6).
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 NCPhl to enable production-level piloting between Austria, Italy, and Greece.

The piloting generated immediate first-hand experiences and ultimately confirmed the general fit for use of eIDAS eID for the eHealth domain for real-world cross-border eHealth services. 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 currently work in concurrence instead of complementing each other: the patient consent.

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-rit architecture and associated tools continues to be 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 intra-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 eIDAS framework.

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 application-ica, 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-PS) 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

[27] ETSI TS 102 640-2 V2.2.1, Electronic Signatures and Infrastructure (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/102640_102649/102640v02.00_01/0 ts_102640v0202p00.pdf