CREATING A EUROPEAN eHEALTH SPACE FOR CROSS-BORDER ePRESCRIPTION AND PATIENT SUMMARY SERVICES

Dimitrios G. Katehakis, Institute of Computer Science, Foundation for Research and Technology – Hellas, Greece, katehaki@ics.forth.gr

George Pangalos, Informatics and Information Security Laboratory, Aristotle University of Thessaloniki, Greece, pangalos@auth.gr

Andriana Prentza, Department of Digital Systems, University of Piraeus, Greece, aprentza@unipi.gr

Abstract

During the past few years, a lot of work has been done in establishing the necessary tools for providing cross-border Information and Communications Technologies (ICT) solutions for public services in Europe in domains of priority, including eHealth. Several Large Scale Pilot projects (LSPs), aiming towards the delivery of electronic cross-border services, have marked a first step in this direction. They have contributed towards ensuring interoperability, by providing new services and improving overall efficiency and effectiveness in a complex environment, making it easier for national companies to do business abroad and helping citizens when they cross borders, whether for tourism, pension or to work. This paper focuses on ongoing work in the Electronic Simple European Networked Services (e-SENS) Large Scale Pilot (LSP) project in the eHealth domain for improving those services through the integration of existing generic Building Blocks (BBs), outcomes of previous or current LSPs. It also aims to support reliable and secure exchange of medical data in a cross-border setting in order to support evolving interoperability, legal and security requirements. More specifically, the implementation of the cross-border ePrescription and Patient Summary (eP/ PS) use cases, in line with European Directive 2011/24/EU on patients' rights in cross-border healthcare, is examined. The need for consolidating the existing outcomes of non-health specific BBs is also outlined, together with related issues that need to be resolved for improving technical certainty and making it easier to use healthcare services abroad in cases of emergency.

Keywords: eHealth, Cross-border Public Services, Electronic Health Records, Interoperability, ICT Solutions, Patient Summary, ePrescription.

1 INTRODUCTION

Although several public eServices are available at national level, this is not always the case across borders. In order to help their development, a number of LSPs have been developed and run under the the Information and Communication Technologies Policy Support Programme (ICT-PSP) of the Competitiveness and Innovation Framework Programme (CIP) of the European Commission (ICT-PSP, 2015 and CIP, 2015), in five main areas: eID, eProcurement, eBusiness, eHealth and eJustice, to engage public authorities, service providers and research centres across the European Union (EU). LSPs pilot a number of solutions, or BBs, that enable cross-border digital services in those policy areas. Each such block consists of a number of components (common code) and uses a number of standards and specifications. They all also share a key characteristic: they are intended to be taken up as part of online services which make these online services cross-border enabled.

Four such LSPs have been completed so far (Digital Agenda, 2015):

- epSOS (European Patients – Smart Open Services) which was related to the exchange of clinical information, with initial focus on both Patient Summary (PS) and ePrescription/ eDispensation (eP/ eD) solutions (epSOS, 2015).

- PEPPOL (Pan-European Public Procurement Online) which has implemented technology standards for European governmental public electronic procurement (PEPPOL, 2015).
- STORK (Secure idenTity acrOss boRders linKed) which has developed a European eID interoperability platform that allows European citizens to log in to public services of other member states using the eID technology of their home country (STORK, 2015).
- SPOCS (Building the next generation Points of Single Contact) which has used the natural person eID solution developed by STORK as well as the Virtual Company Dossier (VCD) concept of PEPPOL for document containers and has generalized it to package company information for transmission to Points of Single Contact (PSC) in other countries (SPOCS, 2015).

Three other LSPs are also still currently running:

- STORK 2.0 that extends the scope of STORK to mandates and representation (e.g. of legal entities) and advances from eGovernment to private sector applications (STORK2.0, 2015).
- e-CODEX (e-Justice Communication via Online Data Exchange) that builds on and makes necessary changes to deliverables from SPOCS and the other pilots to fulfil its objectives for easy and secure access to legal information and procedures in other EU Member States (e-CODEX, 2015).
- e-SENS (Electronic Simple European Networked Services) aiming to consolidate and solidify the work done, to industrialise the solutions and to extend their potential to more and different domains (e-SENS TA, 2013). e-SENS focuses strongly on core BBs such as eID, e-Documents, e-Delivery, semantics and e-Signatures across the different LSP domains. These BBs aim to provide the foundation for the platform of "core services" for the eGovernment, cross-border, digital infrastructure foreseen in Regulation (EU) No 1316/ 2013 for establishing the Connecting Europe Facility (CEF) (REGULATION No 1316/ 2013, 2015).

This work puts focus on the ongoing activities for implementing e-SENS BBs in the eHealth domain, to facilitate cross-border eP/ PS services, in order to improve efficiency, cost-effectiveness, safety and confidence. The overall legal framework for the eHealth pilot for eP/ PS within the project is largely regulated by Directive 2011/ 24/ EU on the application of patients' rights in cross-border healthcare (DIRECTIVE 2011/ 24/ EU, 2015).

Section 2 (The Use Case Scenario for Cross-border ePrescription and Patient Summary Services) provides a brief description of the eP/ PS use case scenarios for cross-border services under consideration. Section 3 (Background Initiatives) describes specific relationship with prior LSPs and other domain initiatives. Section 4 (System Architecture and Use of e-SENS Building Blocks) illustrates how the already developed architecture of epSOS is being adapted to support the incorporation of cross-domain BBs. Section 5 (The e-SENS Pilot Implementation) presents the e-SENS pilot implementation in the eHealth domain and specifically for Greece. Finally, Section 6 (Discussion) concludes by presenting prospective issues and the open potential.

2 THE USE CASE SCENARIO FOR CROSS-BORDER EPRESCRIPTION AND PATIENT SUMMARY SERVICES

The specific use case describes how to support cross-border care for eP/ PS in line with Directive 2011/ 24/ EU on patients' rights in cross-border healthcare (e-SENS D5.4, 2015). Even if the use cases for eP and PS are different, their European background and motivation are similar. In consequence, these two use cases are introduced in a common perspective, although each one has a distinctive process description.

2.1 Process Description for Patient Summary

In the PS use case, the patient is a visitor to the country of care, for example someone on holiday, or attending a business meeting, or one that lives in one country but works in another. The health professional may have some information available from previous encounters, in which case the patient may have a patient record locally stored and possibly also a PS in the country of affiliation. Both sources of information could be consulted and updated by the health professional.

The following 'actors' compose the e-SENS use case for PS:

- A patient/ citizen who is seeking for healthcare treatment abroad.
- A healthcare professional or provider who is providing healthcare treatment. The healthcare professional is in the need to access remote patient electronic health record using the national infrastructure.
- Two National Contact Points (NCPs) and the epSOS Central Services (CS) for National Contact Point (NCP) configuration and terminology handling.
- Providers of trusted sources including national registries of citizens, patients and health professionals.

Also, the following conditions must be met before the PS use case can start:

- A patient/citizen requesting a healthcare professional for medical assistance abroad (Country B).
- A PS must exist in the patient/ citizen's country of affiliation (Country A).
- The healthcare professional is a person legally authorised in Country B to provide healthcare and is identified and authenticated in Country B.
- A mechanism to validate the identity of the patient at the Point of Care (PoC) has to be available.
- The health professional at Country B knows the identity of Country A.
- A health professional must be related to at least one Healthcare Professional Organization (HPO) or to a health authority.
- The patient/ citizen must provide consent (previously given or during the encounter) to the healthcare professional before health data is exchanged.
- There is a chain of trust between system actors in this process.
- The health professional must be able to access the "communication layout" that handles the PS in the European countries.

The use case begins when a healthcare professional in Country B receives a request for healthcare assistance from a patient/ citizen from Country A. The flow of events is as follows:

- Patient is identified.
- The health professional requests the validation of the identity of the patient.
- The request is conveyed to the patient's country of affiliation (Country A).
- Country A provides the (positive or negative) patient's identification confirmation.
- Country A provides the patient's identity and consent confirmation to the health professional.
- Once the identity of the patient is validated, the patient consent is verified.
- Once the identity of the patient is validated, the healthcare professional of Country B requests for the PS of Country A.
- If the PS exists, Country A provides the PS of Country A to the health professional.
- The PS of the patient/ citizen seeking for healthcare treatment abroad is displayed to the health professional.

If all the above pre-conditions are met, then the healthcare professional of Country B can have access to the PS of the patient in Country A. If the identity of the patient cannot be properly validated in Country A, then Country A informs Country B and subsequently the healthcare professional of the identification failure. If the PS of the patient does not exist or cannot be retrieved from Country A, then Country A informs Country B and subsequently the healthcare professional of the failure.

It is considered essential that related requirements be included in bilateral or multi-lateral agreements between partnering states (MS/ ACs) in order to maintain convergence. For real patient's health data to be exchanged there are also strong binding legal requirements, like for example the ones specified in the epSOS Legal Framework Agreements.

2.2 Process Description for ePrescription/ eDispensation

In the ePrescription (eP) case the patient context is similar to the PS case: The patient is visiting the country of care. If a prescribed medical product is not available abroad, the attending pharmacist may, depending on the circumstances, dispense a different brand or package size of a comparable and suita-

ble product to the patient. In case of a product being dispensed, the eDispensation (eD) document is returned to the country of affiliation, to allow the update of the corresponding ePrescription.

The following 'actors' compose the e-SENS use case for eP:

- A patient/ citizen who is seeking for having a medical product dispensed abroad.
- A pharmacist who is on duty to dispense the prescribed medical product. The pharmacist is in the need to fetch the remote ePrescription document record using the national infrastructure, and to submit the corresponding eD, once the medicine is dispensed.
- Two NCPs and the epSOS CS for NCP configuration and terminology handling.
- Providers of trusted sources including national registries of citizens, patients and health professionals.

Also, the following conditions must be met before the eP/ eD use case can start:

- A patient/ citizen requesting a pharmacist for having a medical product dispensed abroad (Country B).
- A valid for dispensation ePrescription document must exist in the patient/ citizen's country of affiliation (Country A).
- The pharmacist is a person legally authorised in Country B to dispense medical product and is identified and authenticated in Country B.
- A mechanism to validate the identity of the patient at the pharmacy has to be available.
- The pharmacist at Country B knows the identity of Country A.
- The patient/ citizen must provide consent (previously give or during the encounter) to the healthcare professional before health data is exchanged.
- There is a chain of trust between system actors in this process.
- The pharmacist must be able to access the "communication layer" that handles the ePrescription documents in the European countries.

The use case begins when a pharmacist in Country B receives a request for having prescribed a medical product from a patient/ citizen from Country A, who owns an ePrescription. The flow of events is as follows:

- Patient is identified.
- The pharmacist requests the validation of the identity of the patient.
- The request is conveyed to the patient's country of affiliation (Country A).
- Country A provides the (positive or negative) patient's identification confirmation.
- Country A provides the patient's identity and consent confirmation to the pharmacist.
- Once the identity of the patient is validated, the patient consent is verified.
- Once the identity of the patient is validated, the pharmacist of Country B requests for the list of valid ePrescription documents of Country A.
- If the ePrescriptions (ePs) exist, Country A provides the list of ePs of Country A to the pharmacist.
- The pharmacist selects the requested eP, accesses to the eP of the patient/ citizen seeking for having the medical product dispensed abroad.
- The pharmacist dispenses the medical product.
- The pharmacist generates eD.
- The eD document is transmitted using the NCP to Country A.

If all the above pre-conditions are met, then the pharmacist of Country B can have access to the eP of the patient in Country A. If the identity of the patient cannot be properly validated in Country A, then Country A informs Country B and subsequently the pharmacist of the identification failure. If the eP of the patient does not exist or cannot be retrieved from Country, then Country A informs Country B and subsequently the pharmacist of the failure.

As in the previous use case, it is considered essential that requirements be included in bilateral or multi-lateral agreements between partnering MS/ ACs in order to maintain convergence. Also, as in the PS use case, legal requirements are again crucial to assure the usage of real patient data. There is also a

need to assure compliance with the ePrescription EU guidelines adopted in 2014 (GUIDELINES ON eP, 2015).

3 BACKGROUND INITIATIVES

The following subsections present key background work and initiatives related to the deployment of cross-border eP/ PS services to support mobility and facilitate access to care across countries in the EU.

3.1 Smart Open Services for European Patients (epSOS)

The epSOS LSP (2008-2014) concentrated on proving that a reliable and secure exchange of medical data in a cross-border setting is actually possible and feasible. By the end of the project, up to 19 epSOS Participating Nations (PNs) launched their epSOS pilots.

The epSOS architecture has focused on the exchange of medical data in two primary use case settings: PS and eP/ eD. Ancillary value added services were implemented and piloted on top of the two primary use cases: Patient Access, Healthcare Encounter Report, and Medication-related Overview. Both, the primary use cases as well as the added-value services primarily feature clinical challenges. However, substantial parts of the non-functional requirements, in particular regarding data protection, confidentiality, and information-security aspects, had to be specifically approached by the eHealth domain, since none of the – at the time available- solutions provided effective answers to the challenges faced by the eHealth domain that could fit for the purpose of cross-border care services.

The fundamental epSOS architecture is depicted in Figure 1.

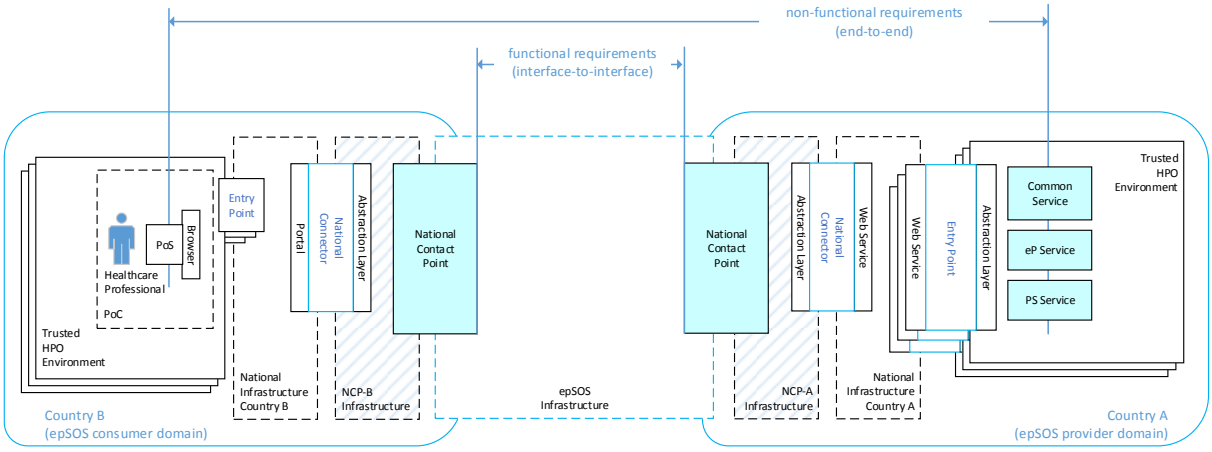

Figure 1. Fundamental epSOS architecture.

The central portion of Figure 1 signifies the heart of the epSOS architecture: the NCPs of the countries of affiliation (NCP-A) and care (NCP-B). Those systems have been deployed by each active participating nation and served as the primary contact to each Member State (MS). Their duties and responsibilities are described in the epSOS Legal Sustainability Recommendations. The NCPs are furthermore anchor points for cross-border interoperability as their exposed interfaces are commonly agreed upon by all PNs. The NCPs also serve as trust anchors, brokers (although exclusively trusting their own actors) and bootstrapper (through member state agreements an existing regulation) as well as serving as specific entry/ exit points for applicable legislation and jurisdiction. The right-hand side shows the country of affiliation or country A, representing the primary data location of the patient as well as the provision points for the epSOS business services, such as eP/ PS. These services and the connected national infrastructure of country A provide the information on patients and can unambiguously identify them.

While fully achieving its primary goal, as well as establishing a new eHealth ecosystem throughout the European MS/ ACs, it became apparent that several supporting functionalities and services might be

improved by already existing or currently developed tools and means, that may be used on different domains, provided they can adequately deliver an assertive solution for healthcare use cases and scenarios.

3.2 Secure Identity across Borders Linked (STORK)

The STORK LSP (2009-2012) provided an interoperability framework for eID natural person authentication in online processes (including a limited set of attributes often coming with eID tokens, like name, date of birth, or address). STORK 2.0 (2012-2015) extends by representation and mandates, and an enriched set of attributes through attribute providers. The interoperability framework is based on the Security Assertion Markup Language SAML 2.0 (OASIS SAML, 2015).

STORK is meant to be sector-independent. The high-level STORK and STORK 2.0 process is that authentication is always delegated to the citizens' infrastructure (either a Pan European Proxy Server – PEPS – component of the MS infrastructure or a Virtual Identity Provider – V-IDP – decentralized software component). The two deployment models "centralized PEPS"/ "decentralized V-IDP" are an MS decision. For the Service Provider, authentication requests get routed through Country B components (again V-IDP or PEPS depending on the MS deployment choice). Ad-hoc collaboration between the epSOS and the STORK LSP, called STepS (STORK meets epSOS subproject of STORK), revealed a significant potential of both initiatives complementing each other alongside with a very beneficial side effect of implicitly consolidating the solutions towards common basic infrastructure for shared tasks. The new specifications of STORK 2.0 are now allowing a realistic re-use of concepts and blocks.

STORK can augment existing epSOS patient identification, as the patient's eID tokens can provide a high level of assurance of patient's unique identification. Traits can be augmented through STORK and STORK 2.0 attribute provision.

Operating STORK at a PoC is challenging, if for example eID tokens have requirements on the IT environment, like card readers, drivers, etc. Mobile eID can play a major role to overcome that. While STORK itself is agnostic to the actual eID credential, the ubiquitous nature of mobile phones together with its zero-footprint characteristic (not imposing requirements on the computing environment other than e.g. a browser), may allow use at a PoC.

3.3 Shaping the Future of Electronic Identity (FutureID)

The FutureID project (2012-2015) (FutureID, 2015) is an Integration project partially funded under the ICT theme of the Cooperation Programme of the 7th Framework Programme of the European Commission. It builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims.

The FutureID infrastructure provides significant benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. FutureID allows application and service providers to easily integrate their existing services with the FutureID infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments.

This is expected to enable service providers to offer this technology to users as an alternative to username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology. For existing and emerging trust service providers and card issuers FutureID is expected to provide an integrative framework, which eases using their authentication and signature related products across Europe and beyond. To demonstrate the applicability of the developed technologies and the feasibility of the overall approach FutureID develops two pilot applications and is open for additional application services who want to use the innovative FutureID technology.

3.4 Other initiatives

A number of other initiatives have also been implemented recently. A European e-Health governance structure has been established at the political level (by Article 14 of the Directive 2011/ 24/ EU, through the eHealth Network – eHN, (eHN, 2015)); at the strategic level (via the eHealth Governance Initiative – eHGI (eHGI, 2015) – a follow-up to the Calliope Thematic Network (CALLIOPE, 2015)); and at the operational level through various projects (epSOS, NETC@RDS/ENED, etc. (NETC@ARDS and ENED, 2015)).

The implemented LSPs have already proven that providing cross-border services can be made simpler. In numerous domains, technical BBs have been developed and piloted that enable seamless cross-border services. The underlying technology to support cross-border eP/ PS usually relies heavily on CS for publishing and processing cross-border configuration information. The Expanding Health Data Interoperability Services – EXPAND – (EXPAND, 2015) initiative is the guardian of several such epSOS assets as well as assets from other European project that have ended. In that scope, the EXPAND Thematic Network provides governance and support whenever an in progress project aims to fulfil its goals by building on top of those assets. Another major objective of EXPAND is to handover to CEF (CEF, 2015) a set of mature eHealth assets that could be used as baseline for the CEF eHealth Digital Service Infrastructure (DSI). EXPAND also operates as a steering committee for eHealth use case pilots (like PS or eP), assuring the correct alignment with epSOS requirements and recommendations, as well as the foreseen directives for the CEF eHealth DSI.

It is noteworthy that during epSOS lifetime at least two proofs of concept have been implemented: the FETNCP and the OpenNCP (OpenNCP, 2015). All the countries planning to pilot e-SENS have adopted the OpenNCP implementation. e-SENS pilots also consider OpenNCP as the foundation for the pilots' implementation and operation. The e-SENS pilots also encourage a deep integration of innovative e-SENS BBs as supporting technology of the OpenNCP. They also commit to driving the evolution of the OpenNCP regarding maturity, applicability, and innovation, while no constraints are put in any other NCP implementation.

4 System Architecture and Use of e-SENS Building Blocks

Figure 2 outlines the proposed eHealth infrastructure by e-SENS which extends the existing epSOS based architecture with supplemental components provided by e-SENS, as well as the systems topology by defining the interrelations and orchestration of the supplements. Some of the newly integrated components are highlighted in orange and only feature their most common integration means (such as a web service or user agent).

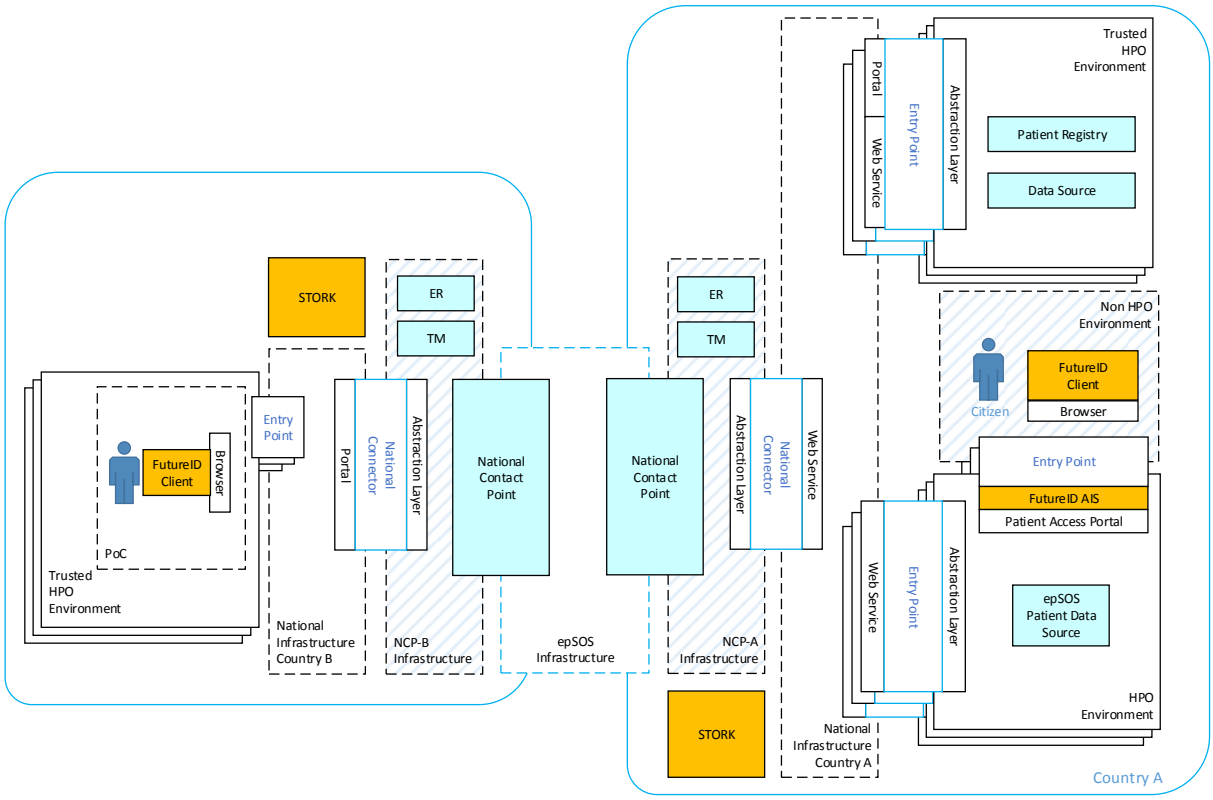

Figure 2. The e-SENS global eP/ PS use case architecture.

The STORK back-end module is depicted as a component within the national infrastructure of the respective countries. The functionality and provision of eID functionality of the FutureID client is immediately supported by the existing services of STORK. Any STORK-intrinsic interactions between the countries are performed over the existing STORK backbone and therefore they are not depicted within the diagram. The Transformation Manager (TM) deals with the transcoding and translation of information embedded in the clinical documents. The Entity Registries (ER) provide directory services towards the stakeholders, such as identity/ property information about a health professional or patient. The ER includes the specific registers, such as the patient or health professional registry as well as the meta directory services that combines and provides the services of multiple local registries for a common data access. The Abstraction Layers are pieces of system integration facilitators that bridge the gap between legacy backend systems and the e-SENS eHealth solution. The environments delimit the regulatory protected realms of the stakeholders with "Trusted HPO" environments benefitting from special legal protection (for instance professional discretion and confiscation protection). The Data Sources (DS) accommodate the clinical data repositories of a country. The FutureID Client is a component designed to operate within the User Agent (such as a Web Browser) at the PoC or the citizen's IT. Its primary functionality is to extend the capabilities of formerly incompliant IT towards the application of advanced eID, trust, and security functionality directly within the realm of the user.

4.1 Common interaction patterns

The eP/ PS use case is based on two generic interaction patterns. The primary interaction for exchanging a PS is the "Request of Data" pattern of Figure 3, in which a healthcare professional within country B is requesting a singular currently active instance of a clinical document, such as a single PS from country A.

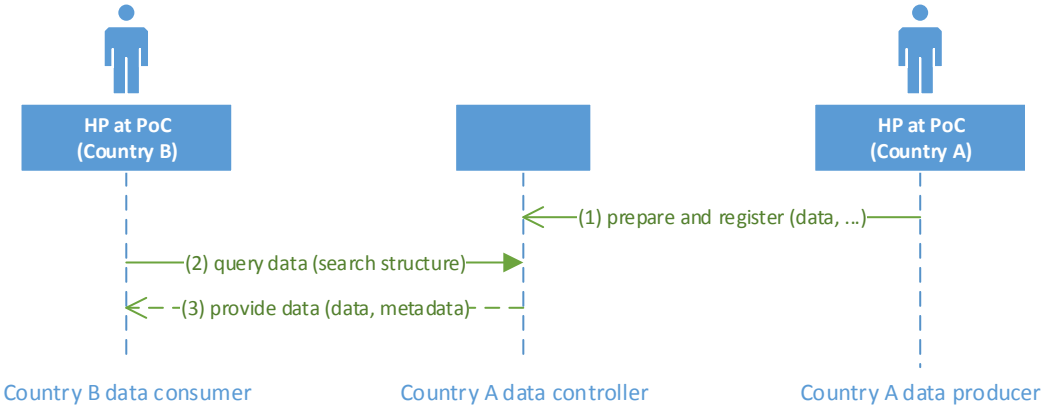

Figure 3: "Request of Data" interaction pattern.

However, whenever a larger/ selective number of documents or instances are requested or different versions of medical data are available that still preserve clinical value, the rather simplistic "Request of Data" interaction pattern of Figure 3 is unable to accommodate this request efficiently and effectively. Therefore, a second interaction pattern is established that enables the healthcare professional to selectively request a subset or collection of medical documents: "Request Overview and Pick Details" (Figure 4). Using this pattern, the healthcare professional in Country B is firstly requesting an overview about all available medical documents about a particular patient and is then able to selectively retrieve the currently relevant. This interaction pattern usually applies more to ePs as those traditionally are provided as multiple atomic clinical documents.

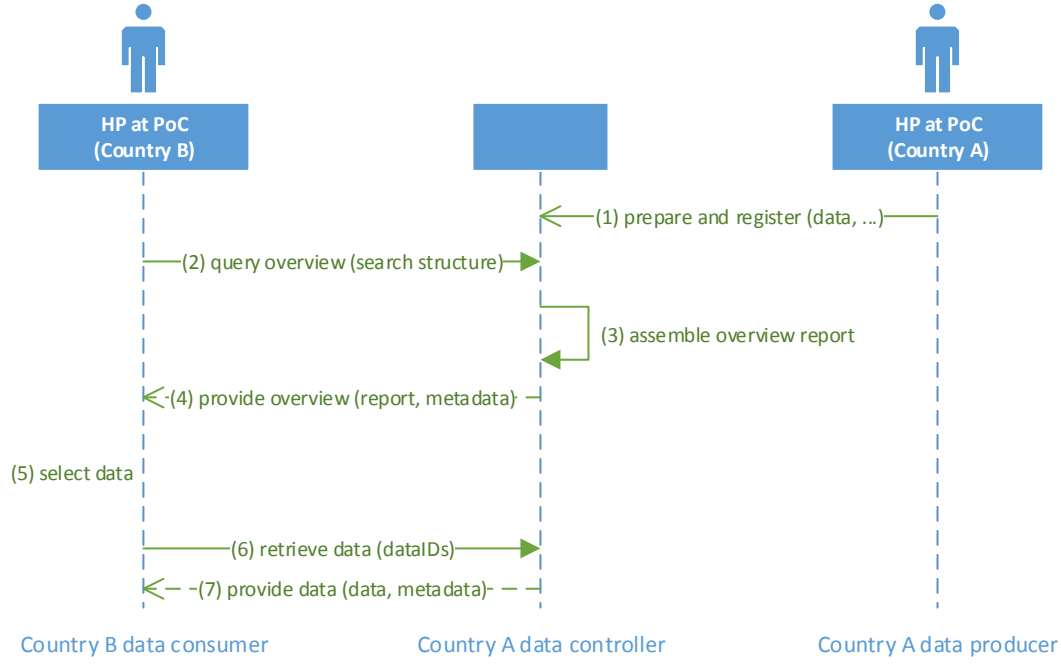

Figure 4: "Request Overview and Pick Details" interaction pattern.

The full context of the operations can be consolidated into the "Application Architecture" Interaction Pattern is depicted in Figure 5.

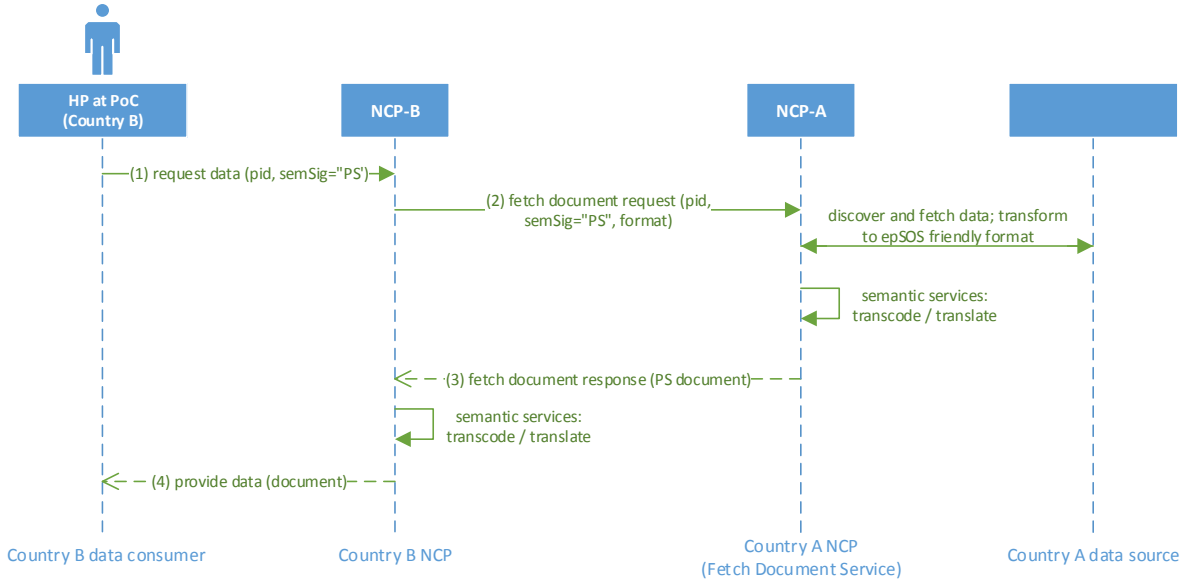

Figure 5: "Application Architecture" interaction pattern for medical data exchange.

4.2 Use of e-SENS Building Blocks

It is envisioned that the usage of the cross-domains e-SENS BBs will provide interoperable and stable solutions that will improve existing epSOS services. Such BBs could be the cross-border electronic identification of patients, the reduction of the managerial and administrative operation overhead, the appropriate capture of digital evidences of exchange, the update of the rather dated security safe-guards, the cross-border encoding and transporting security context, etc. Each one of these, linked with the injection of an e-SENS Building Block (BB) supporting technology to further facilitate the secure exchange of eP/ PS, is discussed briefly in the following sub-sections.

4.2.1 eID for patient identification

Although the original epSOS components responsible with the processing of manual and electronic identification have been designed to be replaced by more appropriate and robust means, a post-alignment of the subsequent healthcare standards, profiles, and interaction patterns is advisable. While this alignment primarily serves the technical domain as well as carrying towards a more robust provision of data protection aspects, some notable side effects with benefits for the piloting nations are anticipated:

- In cases in which the "global" patient identifier of a particular patient is returned immediately or is automatically matched to the national equivalent through the eID means, the epSOS-internal patient identification workflow may be completely skipped.
- The regulatory burden of a positive and correct patient identification and unambiguous linkage of data is currently an organizational burden of the treating healthcare professional who is required to confirm the identity material as presented by the patient as well as the integrity of the link between that material and the patient referenced in the returned medical data.
- The proper provision and application of the highly diverging identification means is a fundamental prerequisite of any successful and meaningful exchange of medical data. However, this operational burden is currently absorbed by the treating healthcare professional, despite their unfamiliarity with the various national means of identification. The eID may relief the healthcare professional of this burden and consequently remove a significant obstacle towards user acceptance.
- In addition to pure delivery of eID, most token carrier and national eID means support advanced security safeguards, including the generation of cryptographic session/ transaction keys or pseudonyms. Those may be applied to the healthcare transactions to raise the overall confidentiality as well as putting the data subject in a position to effectively exercise the rights granted under the respective national and pan-European legislation.

The means for establishing a robust patient identification within epSOS is based on several technological and organisational prerequisites originally designed and specified in order to accommodate national specialties, unavailability of suitable technology, and the former absence of pan-European procedures to identify and authenticate patients in a cross-border scenario. The e-SENS eID BB is set to overcome the inefficiency and merely fundamental robustness of the original epSOS process by establishing the means to operate purely electronic identification for not only identifying but ideally authenticating patients for the clinical workflows, while preserving a full compatibility with the existing epSOS technology.

The new e-SENS electronic identification process, as supporting technology for the e-SENS eP/ PS use case, is based on the generic interaction pattern for patient identification and authentication. The patient is identified by electronic means against an eID Provider (STORK/ FutureID) returning a unique eID for the patient itself. The healthcare professional's software reuses this identifier to: either obtain the sectorial eHealth patient identifier by performing the corresponding Integrating the Healthcare Enterprise (IHE) Cross-Community Patient Discovery (XCPD) transaction (IHE XCPD, 2015), or, immediately applies the obtained eID directly for the medical data request if the obtained patient identifier already qualifies as a sectorial eHealth patient identifier.

Once the patient is univocally identified (through a traditional XCPD workflow) or authenticated (through an e-SENS eID workflow) in the remote country, healthcare professional obtains an epSOS based Treatment Relationship Confirmation Assertion TRC(A) from the NCP-B. Using the Identity Assertion (IdA) and the TRC(A), any epSOS transaction can then be performed, as depicted in Figure 6.

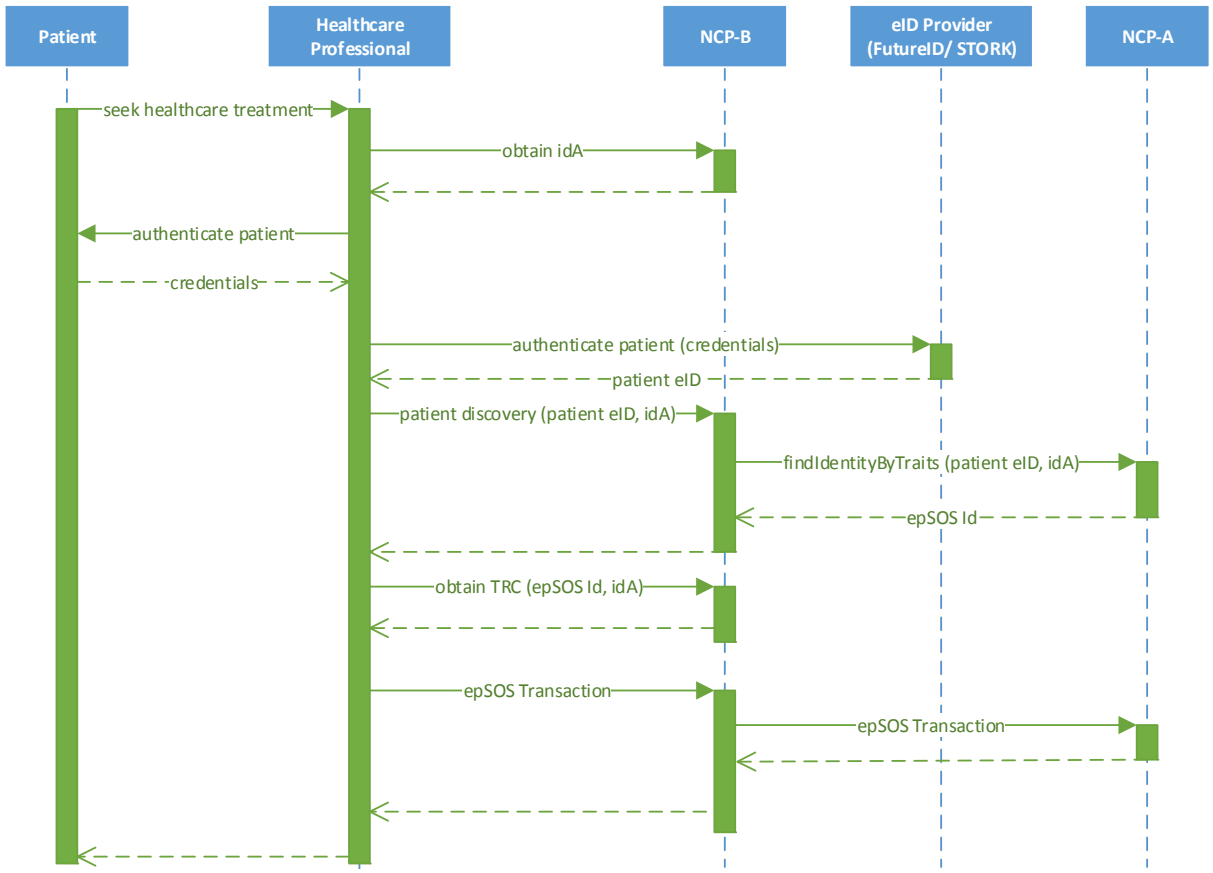

Figure 6: Generic e-SENS eID flow of events.

Medical data must only be disclosed or shared after the patient was identified and authenticated with sufficient accuracy (with respect to Country A demands). Each Country B data consumer as the intended recipient of medical data must identify and authenticate the patient with sufficient accuracy. A

Country B data producer must identify and authenticate the patient with sufficient accuracy before releasing medical information about that patient to a country A data consumer. On successful identification, country A must issue a unique patient identifier that can be used for further transactions on the patient's medical data. Country A may restrict the usability of this identifier to a certain time span or to a certain requestor.

Patient identification is of highest priority. This is why the EU through the eIDAS Regulation (eIDAS, 2015) aims at boosting the user convenience, trust and confidence, while keeping pace with technological developments, promoting innovation and stimulating competition. Following the formal adoption of the Regulation, related delegated/implementing acts will be developed. This will be accompanied by the necessary policy, standardisation and communication activities at the EU and International levels to ensure understanding and a positive environment for the acceptance and wide uptake of the new legislative framework.

4.2.2 Metadata Locator Service for end point detection

epSOS is using CS for addressing this issue. A capability lookup can provide metadata about the communication partner's interoperability capabilities on all levels defined in the European Interoperability Framework (EIF) for legal, organizational, process, semantic and technical interoperability levels. The metadata can be used to dynamically set interoperability parameters and ambitions between the sender and receiver.

Central Configuration services although not very highly prioritized, are considered to be background infrastructure and a priority when looking at infrastructure redundancy with view to CEF adoption. Therefore the adoption of the e-SENS capability lookup BB lies within its scope. E-SENS will use the Simple Metadata Publisher (SMP) developed by PEPPOL and generalized and standardized by OASIS (OASIS SMP, 2015).

The sender can retrieve the information necessary for setting up an interoperability process. The Service Metadata Publisher stores the interoperability metadata, which enables routing of documents received from a sender to the correct recipient. SMP service metadata is a combination of information on the end entity recipient (its identifier, supported business documents and processes in which it accepts those documents) and the gateway (metadata which includes technical configuration information on the receiving endpoint, such as the transport protocol and its address). Every community participant is registered in only one SMP registry.

4.2.3 Non-repudiation for patient access to audit trails

Non-repudiation services are also necessary 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. While patient access to audit trail is considered to be of high priority for collecting end-to-end evidence chains, epSOS does not provide non-repudiation information in the infrastructure and non-repudiation of origin and receipt can be manually obtained by (un)signed audit trails.

The epSOS means on Audit Trail and Non-Repudiation have been established with the scope and needs of an LSP in mind. That is:

- avoidance of any immediate implementation burden for the piloting MS/ ACs,
- isolation from existing national solutions including non-exposed national infrastructure,
- data source for evaluation purposes, namely the epSOS Automatic data Collector, and
- strong separation between the concerns of the MS involved in the medical exchange (epSOS Country A is protecting the concerns of its assigned patients, epSOS Country B is protecting its health professionals and treatment context).

Non-repudiation aspects in a real-life four-corner model (production system) are not a trivial task. The International Standards Organization and International Electrotechnical Commission (ISO/ IEC) 13888-3 standard (ISO/ IEC, 2015) defines four types of non-repudiation tokens, namely non-repudiation of origin, of receipt, of delivery, and of submission. These tokens (or evidence) are not

used in the same way for all the sectors. In fact, non-repudiation of delivery and submission are defined where delivery agents are used (e.g., store-and-forward message exchange pattern).

Content of non-repudiation tokens is defined to be sector-specific, and not to be defined project-wide. epSOS transactions are defined for NCP to NCP communications only, in a synchronous fashion, thus requiring mandatory non-repudiation of receipt tokens (namely, the audit trails) and optional non-repudiation of origin (digital signatures). The new use case aims at enhancing the epSOS approach with a more formal account of Evidence, thus enabling the epSOS LSP to have European Telecommunications Standards Institute (ETSI) Registered Electronic Mail (REM) evidences (ETSI REM, 2015), guaranteeing the sustainability of the other project's evidence emitter, even re-using the same software. Adding non-repudiation is also expected to improve security.

4.2.4 eSignatures for authenticating arbitrary artefacts

epSOS documents are not digitally signed and therefore more advanced electronic signature facilities are required that exceed the capabilities of the technical systems provided by epSOS. Consequently, the consolidated BB of e-SENS regarding eSignatures that combines functionality of STORK, FutureID as well as the current regulatory reality set forth by eIDAS is improving the original capabilities.

The e-SENS eSignature BB can provide: (i) assertion and authenticated attribute signatures, (ii) time stamp signatures for non-repudiation, and (iii) optional document signatures as currently assumed required by some piloting nations.

Not signed artefacts are considered to be of mixed prioritization. It has therefore been suggested to remain out of scope from the initial e-SENS piloting plans, since it requires use case extension and has an IHE dependency (since this BB behaviour is not yet accepted by IHE).

4.2.5 Trust Establishment for end-to-end security and security relaxation

Trust establishment is a key task, both during bootstrapping and operational stages. In epSOS trust establishment is implemented by using Trust-service Status Lists (TSLs) and NCP-service Status Lists (NSLs) containing remote certificates chains used to validate security means (e.g., validating SAML assertions, mutual authentication on TLS channels). During the epSOS operations, the Security Expert Group (SEG) had to aprove some ‘relaxation’ and amendments to the original epSOS security specifications, mainly due to the impossibility to find suitable certification authorities able to issue the required certificates.

The e-SENS Trust Services Solution Architectural Template (SAT) aims at providing a specification for cross-border and cross-sector trust establishment and certificate layouts following strictly the eIDAS regulation. Once it is finalized, its findings will enable the eHealth domain to overcome the abovementioned relaxations and align to the eIDAS. End-2-end security and security relaxation is considered to be of mixed-to-low prioritization.

5 THE E-SENS PILOT IMPLEMENTATION

5.1 The eHealth pilot implementation plan

The e-SENS eHealth pilot implementation will support cross border care for Patient Summaries and ePrescriptions, in line with Directive 2011/ 24/ EU on patients' rights in cross-border healthcare. The first set of e-SENS pilots is already under implementation and cross-border piloting is expected to become operational in June 2015.

In the PS case, the patient is a visitor to the country of treatment, for example someone on holiday, one attending a business meeting, or one that lives in one country but works in another. The health professional may have some information available from previous encounters, in which case the patient may have a patient record locally stored and possibly also a PS in the country of origin. Both sources of

information could be consulted and updated by the health professional. In the eP case the patient context is similar to the PS case, e.g., the patient is visiting the country of treatment. If a prescribed medical product is not available abroad, the attending pharmacist may, depending on the circumstances, dispense a different brand or package size of a comparable product to the patient. In case of a product being dispensed, the eD document is returned to the country of affiliation, to allow the update of the corresponding ePrescription.

Even though most of the MS piloting in e-SENS have already piloted PS and eP services during epSOS, the process described assumes that the plan is agnostic about previous experiences in piloting these services, in order to allow new MS/ ACs to come also on board.

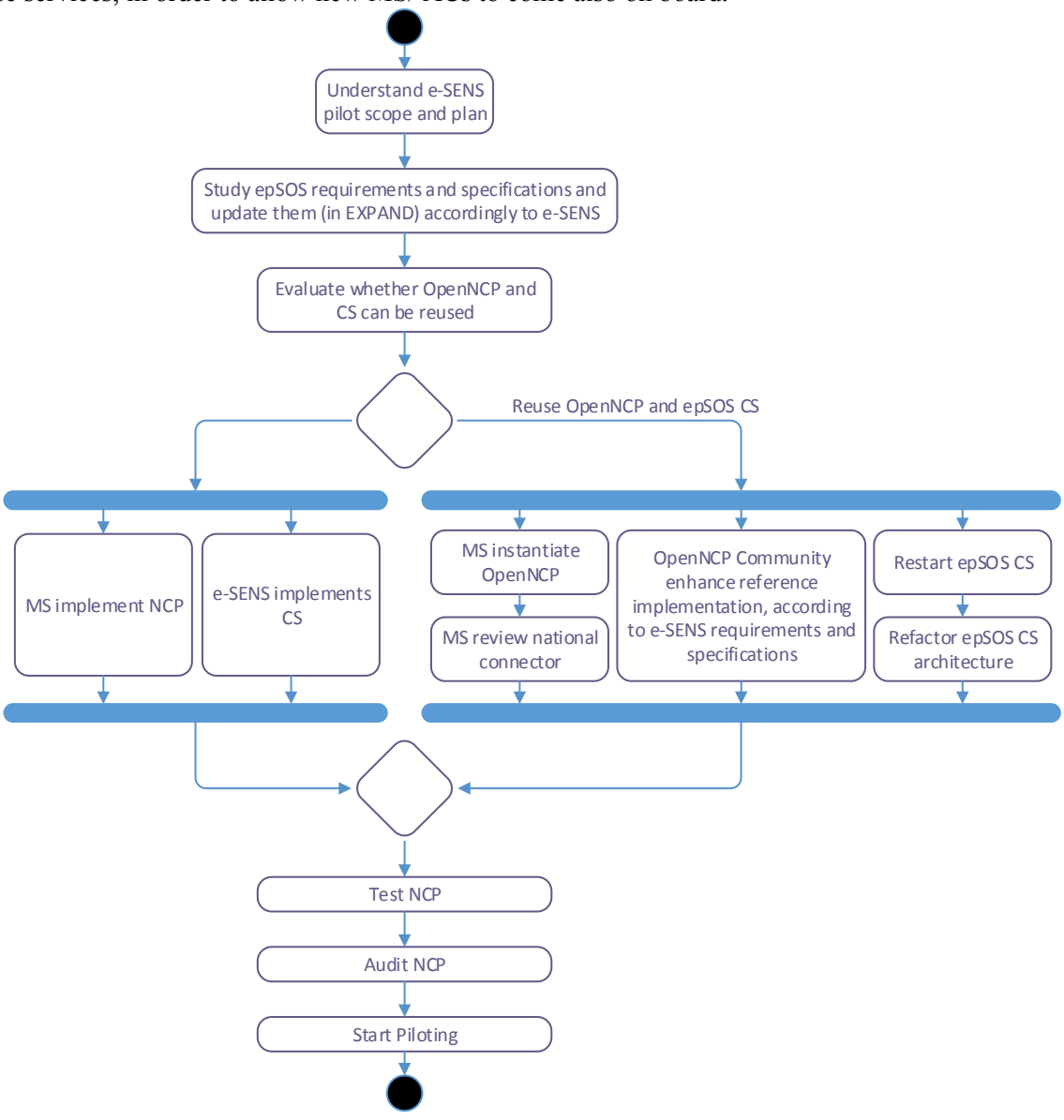

Figure 7: e-SENS eP/ PS Summary Pilot Plan.

The e-SENS pilot plan is organized in four distinct phases, each of one having a clear purpose and outcome. An overview of the e-SENS eP/ PS Summary Pilot Plan is shown in Figure 7.

(i) Phase 1: Baselining. Its purpose is to provide a clear picture of the pilot implementation plan in order to assure the unbiased comprehension by all involved, the effort it demands from each single stakeholder, understand the changes and their impact on assets, as well as to understand the de-

pendencies and risks. Its outcome is an agreement between all stakeholders in providing in time all the needed means foreseen in the Pilot Plan.

(ii) Phase 2: Restart Piloting. Its purpose is to re-establish the baseline conditions (e.g. necessary CS) for MS to Pilot the PS and eP use cases and to enhance the NCP reference implementation according to the e-SENS requirements. Its objective is to restart PS and eP pilots in the new e-SENS environment and specifications.

(iii) Phase 3: CS refactoring. Its purpose is to refactor the CS architecture and operation paradigm to the e-SENS specifications, including Trust Services. Its objective is to deploy the new architecture and operation paradigm for configuration services, based on specifications for cross-border and cross-sector trust establishment and certificate layouts according to the eIDAS regulation.

(iv) Phase 4: Patient eID. Its purpose is to implement an enhanced Patient identification scheme based on Electronic tokens and improve the liability and the user friendliness of the current (manual) process. The objective is to release for MS adoption, a new version of the NCP reference implementation that combines two methods of patient identification: a manual one (as it was on epSOS), and an electronic one (according to the e-SENS eID BB).

A revised epSOS testing strategy will also be applied to e-SENS eHealth eP/ PS pilots before they go live (and it covers legal, security, semantic, organisational and technical aspects).

5.2 The national pilot plan for Greece

The piloting in e-SENS is the next step for Greece to foster European wide cross-border eHealth services and a logical next step to the epSOS pilot services. The Greek pilot is included in the first set of pilots to become operational in June 2015. The first use-case to be implemented will be cross-border eP.

Greece is a country with a high influx of tourists throughout the year. The opportunity to dispense electronic prescriptions and access patient summaries from other countries in a Greek pharmacy and health care facilities respectively is a great advantage. The priorities for piloting in e-SENS in Greece are determined at the political level by the priorities of the state and the readiness of the national pilot partners to support such priorities. Within e-SENS, Greece will implement the eP/ PS use cases.

Greece has already piloted in the framework of epSOS ePrescription as country of treatment for the patients (country B). National cross border initiatives are focusing on expanding current services to services as country of affiliation for eP and also initially as country B for PS. In anticipation of the latter, the epSOS national implementation team has already implemented and tested the epSOS MTC which is necessary for the semantic transformation of the PS. However, the needed legal and organizational framework for electronic health records, currently in process of development, will need to be secured before Greece can expand into the eP/ PS use case beyond pre-production. It is also understood that the e-SENS eHealth pilot will take place initially with test data only. E-SENS extensions to be piloted need to be able to follow existing current situation in Greece, especially in the eID domain where end to end security via smart card technology for example is not supported. As such a STORK based eID approach seems to be more in-line with future developments.

Greece has implemented the epSOS open NCP and will maintain the NCP with any further extensions whether delivered in e-SENS or in other projects (such as EXPAND). It is anticipated that the currently expressed political commitment will also result in sustainable operation of the NCP under the legal agreements to be established within the Subgroup. The provision of the current cross border pilot services and the future extensions will take place within the framework of existing European regulations. Both eP and electronic patient records are regulated by national legislation.

Greece is expected be able to go live at pre-production with simulated data by the end of 2015. It is also expected to be ready to go operational immediately after all domain and national pre-conditions are met. It is desirable that action with actual users is taken in advance of deployment, possibly within CEF.

Once the solution has been tested and validated, it will run in pre-production environment. This phase includes the following actions:

- Installation of pre-production testing environment
- VPN Connections
- Certificate Management
- Training of pilot participants
- Management and monitoring of the running/ operation phase of the pilot
- Pilot environment maintenance – improvement of pilot implementation
- Helpdesk support (1st level)
- Assessment and evaluation of the pilot at national level

The national PS service was foreseen to be launched in 2015; it is therefore likely that Greece may participate in e-SENS with a full PS- country A, B service. It is however desirable that action with actual users is taken in advance of deployment, possibly within CEF. Greece is both a highly touristic destination and has also a highly digitized health sector. Embedding e-SENS/epSOS functionalities into the local apps is likely to increase doctors' buy-in and active collaboration.

6 DISCUSSION

This paper has focused on the ongoing work in the e-SENS project for improving ICT based cross-border solutions for public services in Europe in domains of priority, including eHealth. This is implemented mainly through the integration of existing generic BBs that support reliable and secure exchange of medical data in cross-border settings. An evolving architecture, to accommodate cross-domain BBs within the continuously evolving European eHealth space and to support cross-border services for eP/ PS has been presented.

It is anticipated that the eHealth domain will greatly benefit from mitigating non-domain concerns, such as eID, trust anchors, trust bootstrapping, crypto-management, and baseline infrastructure security towards other domains that are authoritatively responsible of providing those exact measures. Even so, deep assessment is necessary in order to deeply understand the legal, organizational, semantic and technical interoperability framework that has been established in the last fifteen years in Europe. Such assessments may provide evidence that, what in principle are non-domain concerns (e.g. baseline infrastructure), may in fact be tightly tied to domain requirements or pre-conditions (e.g. metadata profiling).

A core foundation and a set of basic principles are also necessary to realise interoperability between MS/ ACs. Although a lot of work has been done in this respect, there is still a need for consolidating the existing BBs and testing technical and legal issues. The European Interoperability Framework (EIF) (EIF, 2015) and the current LSPs already marked a first step in this direction. The next step is now required to unlock the potential of cross-border services and define the standards to enable cross-border services.

Specifications that are being developed in e-SENS are expected to contribute to the implementation of the European Interoperability Framework (EIF) for basic cross-border public services in Europe. In this way, e-SENS prepares the ground for the future Digital Service Infrastructures under the Connecting Europe Framework program (CEF).

Acknowledgements

Work reported in this paper is partially supported by the European Commission and specifically by the Information and Communication Technologies Policy Support Programme (ICT-PSP) of the Competi-

tiveness and Innovation Framework Programme (CIP) under the e-SENS project ("Electronic Simple European Networked Services", contract number 325211, http://www.esens.eu). The authors would like to explicitly acknowledge significant contributions from Sören Bittins (FOKUS, Germany), Massimiliano Masi (FMH, Austria), Marcello Melgara (LISPA, Italy), Licínio Kustra Mano (SPMS, Portugal), and Francois Wisniewski (LIST, Luxembourg). 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

CALLIOPE. CALL for InterOPErability: Creating a European coordination network for eHealth interoperability implementation. [cited 24 April 2015]. http://www.calliope-network.eu

CEF. Connecting Europe Facility. [cited 24 April 2015]. http://ec.europa.eu/digital-agenda/en/connecting-europe-facility

CIP. European Commission Competitiveness and Innovation Programme. [cited 24 April 2015]. http://ec.europa.eu/cip/

DIGITAL AGENDA for Europe, Cross-border solutions. [cited 24 April 2015]. https://ec.europa.eu/digital-agenda/en/large-scale-pilot-projects

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 [PDF]. [cited 03 April 2015]. Available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:en:PDF

eHN. eHealth Network. [cited 21 April 2015]. http://ec.europa.eu/health/ehealth/policy/network/index_en.htm

eHGI. The European eHealth Governance Initiative. [cited 24 April 2015]. http://www.ehgi.eu/default.aspx

eIDAS. REGULATION 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 23 April 2015]. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

EIF. Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services', 'European Interoperability Framework (EIF) for European public services' [PDF]. Bruxelles, le 16.12.2010 COM(2010) 744 final. [cited 03 March 2015]. Available from: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

EIRA. The European Interoperability Reference Architecture. [cited 22 April 2015]. https://joinup.ec.europa.eu/asset/eia/description

ENED. European Network for Electronic Data exchange in the health care sector. [cited 24 April 2015]. http://www.ened.eu/

epSOS. European Patients – Smart Open Services, Making Healthcare Better. [cited 24 April 2015]. http://www.epsos.eu/

ETSI REM. European Telecommunications Standards Institute, 'Registered Electronic Mail (eDelivery): TS 102 640 (multipart)'.

EXPAND. Expanding Health Data Interoperability Services. [cited 22 April 2015]. http://www.expandproject.eu/

e-CODEX. e-Justice Communication via Online Data Exchange, Making Justice Faster. [cited 24 April 2015]. http://www.e-codex.eu/

Electronic Simple European Networked Services (e-SENS), Moving Services Forward. [cited 24 April 2015]. http://www.esens.eu/

e-SENS TA. E-SENS Technical Annex, 2013, e-SENS Project, Contract number 325211.

e-SENS D5.4. e-SENS Deliverable D5.4: Second-wave Update of Plans and Status of Domain and National Pilots

e-SENS SAT. e-SENS Solution Architecture Template Trust Serviced. [cited 01 May 2015]. http://wiki.ds.unipi.gr/display/ESENS/SAT+-+Trust+Services

FutureID. Shaping the Future of Electronic Identity. [cited 22 April 2015]. http://www.futureid.eu/

GUIDELINES ON eP. 'Guidelines on ePrescriptions dataset for electronic exchange under Cross-Border Directive 2011/ 24/ EU' [PDF] of the European Commission. Release 1. 2014-11-18. [cited 03 March 2015]. Available from: http://ec.europa.eu/health/ehealth/docs/eprescription_guidelines_en.pdf

ICT-PSP European Commission Information and Communication Technologies Policy Support Programme. [cited 02 May 2015]. http://ec.europa.eu/cip/ict-psp/index_en.htm

IHE XCPD. Integrating the Healthcare Enterprise (IHE) ITI Technical Committee. IHE IT Infrastructure Technical Framework Supplement, 'Cross-Community Patient Discovery (XCPD)' [PDF]. Trial Implementation. 2011-08-19. [cited 03 May 2015]. Available from Internet: http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCPD_Rev2-3_TI_2011-08_19.pdf

ISO/ IEC International Standards Organization and International Electrotechnical Commission 2009, 'Information Technology – Security techniques – Non-repudiation – Part 3: Non-Repudiation mechanisms using asymmetric techniques', ISO/ IEC 13888-3:2009(en).

NETC@RDS. A step towards the electronic EHIC. [cited 24 April 2015]. http://www.netcards-project.com/

OASIS SAML. OASIS Security Services. [cited 24 April 2015]. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

OASIS SMP. The OASIS SMP Specification. [cited 30 April 2015]. https://www.oasis-open.org/committees/document.php?document_id=53763&wg_abbrev=bdxr

OpenNCP Community Home. [cited 24 April 2015]. https://openncp.atlassian.net/wiki/display/ncp/OpenNCP+Community+Home

PEPPOL. Pan-European Public Procurement Online, Making Procurement Better. [cited 24 April 2015]. http://www.peppol.eu/

REGULATION No 1316/ 2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010 Text with EEA relevance. [cited 24 April 2015]. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013R1316

SPOCS. Building the next generation Points of Single Contact, Making Business Easier. [cited 24 April 2015]. http://www.eu-spocs.eu/

STORK. Secure idenTity acrOss boRders linKed, Making Access Smarter. [cited 24 April 2015]. https://www.eid-stork.eu/

STORK2.0. Secure idenTity acrOss boRders linKed 2.0, Making Access Smarter. [cited 24 April 2015]. https://www.eid-stork2.eu/