Transforming Government: People, Process and Policy

Research note: A European ehealth space for moving cross-border eprescription and patient summary services forward

Dimitrios G. Katehakis George Pangalos Andriana Prentza

Received 1 October 2015
Revised 29 January 2016
7 April 2016
Accepted 12 April 2016

Research note

A European ehealth space for moving cross-border eprescription and patient summary services forward

Dimitrios G. Katehakis
Institute of Computer Science, Foundation for Research and Technology – Hellas, Heraklion, Greece
George Pangalos
Informatics and Information Security Laboratory, Aristotle University of Thessaloniki, Thessaloniki, Greece, and
Andriana Prentza
Department of Digital Systems, University of Piraeus, Piraeus, Greece

Abstract

Purpose – The purpose of the paper is to present a framework for moving cross-border ePrescription (eP) and Patient Summary (PS) services forward, bearing in mind the needs and requirements of the European e-health space for cross-border eP and PS services, the limitations of the already developed solutions, as well as outcomes available from other domains.

Design/methodology/approach – The outcomes of previous and current large-scale pilot projects, aiming toward the delivery of electronic cross-border services, are examined. Integration of generic building blocks (BBs) is considered for the further development of cross-border eP and PS, in line with the European Directive on patients' rights in cross-border health care.

Findings – The e-health domain is expected to greatly benefit from mitigating non-domain concerns such as those for electronic identification, end point detection, non-repudiation and the use of electronic signatures and trust establishments for basic cross-border public services in Europe.

Research limitations/implications – Research limitations are related to the fact that electronic identification, electronic signature and semantic issues have not been fully addressed yet at a European level to support cross-border services.

Practical implications – Practical implications are related to the cooperation, European level compatibility and sustainability of the underlying national infrastructures required to support 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.

Originality/value – The need for consolidating the existing outcomes of non-health specific BBs is examined for two high-priority e-health services. Ongoing progress is presented, together with related

Work reported in this paper is partially supported by the European Commission and specifically by the ICT-PSP of the CIP under the e-SENS project ("Electronic Simple European Networked Services", contract number 325211, www.esens.eu). The authors would like to acknowledge 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.

Transforming Government: People, Process and Policy
Vol. 10 No. 3, 2016
pp. 478-504

1750-6166
DOI 10.1108/TG-07-2015-0032

issues that need to be resolved for improving technical certainty and making it easier to use health-care services abroad in cases of emergency.

Keywords Interoperability, Electronic health record, Cross-border public services, EHealth, ePrescription, Patient summary

Paper type Research paper

1. Introduction

The use of ePrescription and Patient Summary (eP/PS) services has been recognized as an important strategic policy to improve health care across Europe to support access to safe and high-quality, cross-border health care and promote cooperation on health care between Member States (MSs) (Tinholt *et al.*, 2013). Provisions related to the prior authorization of health care in another MS, the reimbursement of such health care and the removal of unjustified obstacles to achieving these aims are largely regulated by Directive 2011/24/EU on the application of patients' rights in cross-border health care (Quinn and De Hert, 2011; European Parliament and the Council of the European Union, 2011).

The application of the eP system in European countries has already resulted in significant changes toward better use of medications and utilization of resources and has proved to be a valuable tool for improving services and providing planning, control and transparency data for the health-care domain (Angelidis *et al.*, 2010; Pangalos *et al.*, 2013). This is because it has already proved that can help patients by providing easier prescription and medication pick-up procedures, fewer difficulties over prescription insurance coverage and an increase in patient safety (e.g. legible prescriptions can be checked for harmful interactions) (Hollingworth *et al.*, 2007). It can also help pharmacists by reducing the number of mistakes by misreads, increasing the time spent toward critical issues concerning drug therapy matters, providing a competitive advantage over other pharmacists who do not adopt ePrescribing and an overall simplification of the claiming procedure (eHealth Initiative, 2004). An eP system can also help physicians gain quick on-line access to patient information, better formulary adherence and alignment with guidelines, on-line notification of drug interactions and a review of the cost of prescription produced (Wang *et al.*, 2009). An eP system is also a valuable source of information for monitoring medication use. It provides an effective tool not only for the timely monitoring of patient safety and public health but also for reducing medication costs (Ammenwerth *et al.*, 2008). Information as for example on the type, volume and cost of prescribed drugs and the prescribing habits of doctors are available in real time. The system can also monitor and facilitate (e.g. by suggesting appropriate alternatives) the prescription of lower cost (including generic – off patent) drugs. The monitoring of the overall prescription process through the new system has also provided an effective tool for tackling the problem of over-prescribing, which has not only financial but also serious public health consequences (Miller *et al.*, 2005; AHRQ, 2007; Fischer *et al.*, 2008).

During the past several years many regional and national health-care networks have been deployed in Europe to support PS and electronic health record (EHR) solutions (Stroetmann *et al.*, 2011). The gains from EHR systems depend on meaningful sharing and rely on access to information regardless of place and time and from re-using information for multiple purposes (Dobrev *et al.*, 2010). Although there has been evidence of a modest number of benefits associated with structuring the current

patient history, including obtaining more complete clinical histories, improved accuracy of patient self-documented histories and better associated decision-making by professionals, further investigation is still required (Fernando *et al.*, 2012).

It is a fact that despite favorable attitudes toward both cross border eP/PS, multiple perceived barriers impede its incorporation and integration in clinical practice. There are varying interpretations and implementations of data protection and confidentiality laws in the 28 MSs of the European Union (EU). Infrastructures are not in place to support the system and stakeholders in some jurisdictions are reluctant to embrace e-health because of the high cost and the lack of security of the systems (Kierkegaard, 2013). MSs have varying degrees of health care policy, privacy enforcement and laws concerning data protection, telecommunication services and digital signature with regards to eP/PS.

This work puts focus on the ongoing activities for implementing non-domain specific solutions in the e-health domain to facilitate cross-border eP/PS services to improve efficiency, cost-effectiveness, safety and confidence. More specifically, it presents how the already developed European patients – Smart Open Services (epSOS) architecture (epSOS, 2015) is being adapted to support the incorporation of cross-domain building blocks (BBs), developed within the Electronic Simple European Networked Services (e-SENS) framework (e-SENS, 2016).

Work methodology together with key background initiatives for the development of cross-border services and the relevant e-health space for eP/PS under consideration are presented in Section 2 (Methodology). Section 3 (Results) describes the proposed system architecture and use of selected BBs, based on MS priorities. Section 4 (The e-SENS pilot implementation) discusses issues related to eP/PS piloting and specifically for Greece with a little more detail. Finally, Section 5 (Discussion) provides conclusions and some recommendations.

2. Methodology

Although several public e-services are available at national level, this is not always the case across borders. To help their development, a number of large-scale pilot (LSPs) projects have been developed and run under the Information and Communication Technologies Policy Support Programme (ICT-PSP) of the Competitiveness and Innovation Framework Programme (CIP) (CIP, 2016) of the European Commission (ICT-PSP, 2016) in five main areas – eID, eProcurement, eBusiness, e-health and e-Justice – to engage public authorities, service providers and research centers across the 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 (TOGAF, 2016). They all 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 (European Commission, 2016a):

(1) epSOS, which was related to the exchange of clinical information, with initial focus on both PS and eP/eDispensation (eP/eD) solutions (epSOS, 2016).

(2) Pan-European Public Procurement Online (PEPPOL), which has implemented technology standards for European governmental public electronic procurement (Mondorf *et al.*, 2010; Ølnes, 2012; PEPPOL, 2016).

(3) Secure idenTity acrOss boRders linKed (STORK), which has developed a European eID interoperability platform that allows European citizens to log in to public services of other MSs using the eID technology of their home country (Leitold and Zwattendorfer, 2011; STORK, 2016).

(4) Building the next generation points of single contact (SPOCS), which has used the natural person eID solution developed by STORK, as well as the virtual company dossier concept of PEPPOL for document containers, and has generalized it to package company information for transmission to Points of Single Contact in other countries (Rössler and Tauber, 2011; SPOCS, 2016).

Three other LSPs are also still currently running:

(1) STORK 2.0 that extends the scope of STORK to mandates and representation (e.g. of legal entities) and advances from e-government to private sector applications (Leitold *et al*., 2014; STORK 2.0 2016).

(2) e-Justice Communication via Online Data Exchange (e-CODEX) 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 MSs (Francesconi, 2012; e-CODEX, 2016).

(3) e-SENS aiming to consolidate and solidify the work done to industrialize the solutions and to extend their potential to more and different domains. e-SENS focuses strongly on core BBs such as eID, e-documents, e-delivery, semantics and eSignatures across the different LSP project domains. These BBs aim to provide the foundation for the platform of "core services" for the e-government, cross-border, digital infrastructure foreseen in Regulation (EU) No. 1,316/ 2013 for establishing the connecting Europe facility (CEF) (European Parliament and the Council of the European Union, 2013).

Although a lot of work has been done in creating a core foundation and some basic principles that are necessary for establishing interoperability between MSs, there is still a need for consolidating the existing BBs and testing technical and legal issues.

The methodology of the work is based on the e-SENS LSP approach toward the integration of existing generic BBs, outcomes of previous or current LSPs to be effectively used in resolving open issues for cross-border eP/PS. This approach consists of several core phases, starting with creating an inventory of existing practices and solutions within countries and across the EU, defining generic functional requirements for basic cross-sector services, developing specifications, operating and testing these common solutions in selected operational scenarios and on the basis of these experiences, finalizing the specifications. The pathway diagram demonstrating the various stages of the process (including testing, pilot enablement and handover) is depicted in Figure 1. E-SENS does not aim at exporting national solutions to the pan-EU level but seeks to create a common pan-European set of standards that are expected to embrace the national diversity and facilitate interoperability, thus respecting subsidiarity.

The e-health scenario for the eP/PS service use case describes how to support cross-border health care for eP/PS in line with the Patients' Rights Directive (2011/24/ EU). Even if the use cases for eP and PS are different, their European background and

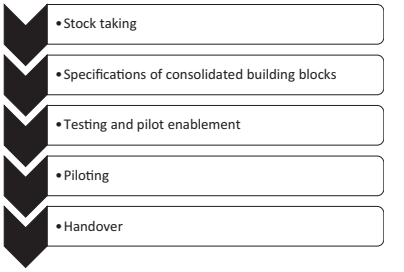

Figure 1.
e-SENS tasks

motivation are similar. In consequence, these two use cases are introduced in a common perspective, although each one has a distinctive process description. 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.

2.1 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, Health care 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 e-health domain because none of the – at the time available – solutions provided effective answers to the challenges faced by the e-health domain that could fit for the purpose of cross-border care services.

The central portion of Figure 2 signifies the heart of the epSOS architecture: the National Contact Points (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 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 MS 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 e-health ecosystem throughout the European MSs, it became apparent that several supporting

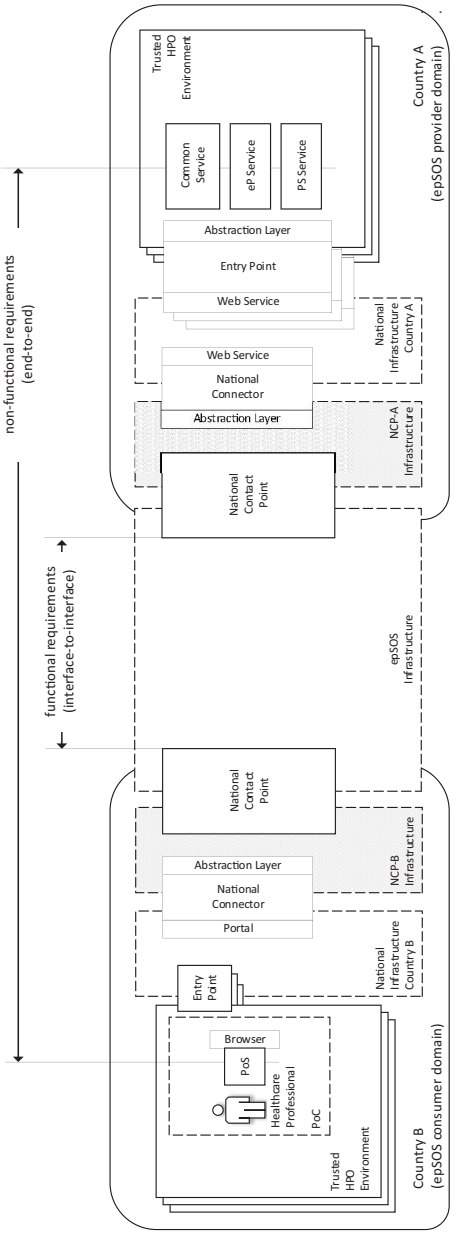

Figure 2.
Fundamental epSOS
architecture

functionalities and services could 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 health care use cases and scenarios.

2.1.1 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 use case under consideration for PS:

- A patient/citizen who is seeking for health-care treatment abroad.
- A health-care professional or provider (HP) who is providing health-care treatment. The health-care professional is in the need to access remote patient EHR using the national infrastructure.
- Two 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 health-care professional for medical assistance abroad (Country B).
- A PS must exist in the patient/citizen's country of affiliation (Country A).
- The health-care professional is a person legally authorized in Country B to provide health care 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 Health-care Professional Organization (HPO) or to a health authority.
- The patient/citizen must provide consent (previously given or during the encounter) to the health-care professional before health data are 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 health-care professional in Country B receives a request for health-care assistance from a patient/citizen from Country A. 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 health-care 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 health-care treatment abroad is displayed to the health professional.

If all the above pre-conditions are met, then the health-care 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 health-care 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 health-care professional of the failure.

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

2.1.2 Process description for e-prescription/eDispensation. In the eP use case, the patient context is similar to the PS use 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 suitable 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 eP.

The following "actors" compose the use case under consideration 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 eP 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 eP document must exist in the patient/citizen's country of affiliation (Country A).
- The pharmacist is a person legally authorized 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 health-care professional before health data are 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 eP 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 eP. 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 eP documents of Country A. If the ePs (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 MSs 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 eP EU guidelines adopted in 2014 (eHealth Network, 2014).

2.2 Secure identity across borders linked

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, such as 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, 2016a).

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

toward 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 because 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 such as 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.

2.3 Shaping the future of electronic identity

The FutureID project (2012-2015) (Cuijpers and Schroers, 2014; FutureID, 2016) 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.

2.4 Other initiatives

A number of related e-health initiatives have also been implemented recently. The e-health network, a European e-health governance structure (European Commission, 2016b), has been established at the political level to bring together national authorities responsible for e-health on a voluntary basis to work on common orientations in this area and to promote an interoperable and sustainable e-health implementation across Europe. At the strategic level, the European e-health Governance Initiative eHGI (Stroetmann *et al.*, 2011; eHGI, 2016) has developed strategies, priorities, recommendations and guidelines designed to deliver e-health

in Europe in a coordinated way. Finally at the operational level, projects such as NETC@RDS/ENED (Pagkalos *et al.*, 2010; NETC@ARDS, 2016; ENED, 2016) have worked, like epSOS, in trying to resolve European level compatibility and sustainability of the underlying national infrastructures required to support 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.

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) initiative is the guardian of several epSOS assets, as well as assets from other European project that have ended. In that scope, the EXPAND Thematic Network provides (EXPAND, 2016) 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 (2016) a set of mature e-health assets that could be used as baseline for the CEF e-health Digital Service Infrastructure (DSI). EXPAND also operates as a steering committee for e-health use case pilots (such as PS or eP), assuring the correct alignment with epSOS requirements and recommendations, as well as the foreseen directives for the CEF e-health DSI.

It is noteworthy that during epSOS lifetime, at least two proofs of concept have been implemented: the FETNCP and the OpenNCP (Fonseca *et al.*, 2015; OpenNCP, 2016). 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, whereas no constraints are put in any other NCP implementation.

3. Results

Based on the existing framework presented in Section 2, the eP/PS use case as described in epSOS and BBs originally designed for other domains, the next generation eP/PS infrastructure can be built based on cross-domain BBs to move the eP/PS services forward. This is done in the context of the evolving governance structures described above.

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

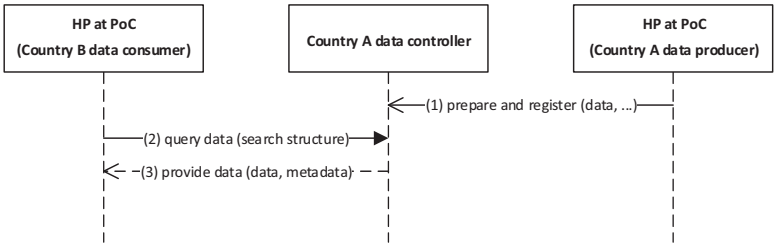

Figure 3.
"Request of Data" interaction pattern

health-care professional within Country B is requesting a singular currently active instance of a clinical document, such as a single PS from Country A.

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 health-care professional to selectively request a subset or collection of medical documents: "Request Overview and Pick Details" (Figure 4). Using this pattern, the health-care professional in Country B is first 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.

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

It is envisioned that the usage of cross-domain BBs will provide interoperable and stable solutions that will improve existing epSOS services. Such BBs could be the

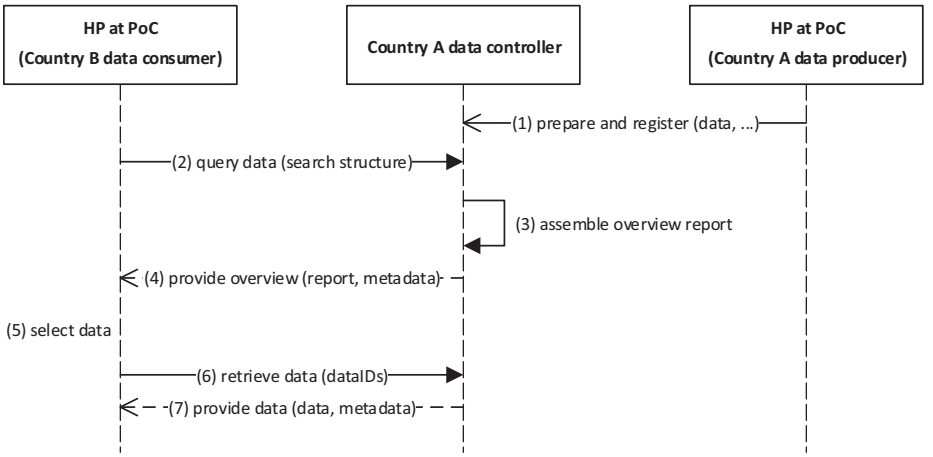

Figure 4.
"Request Overview and Pick Details" interaction pattern

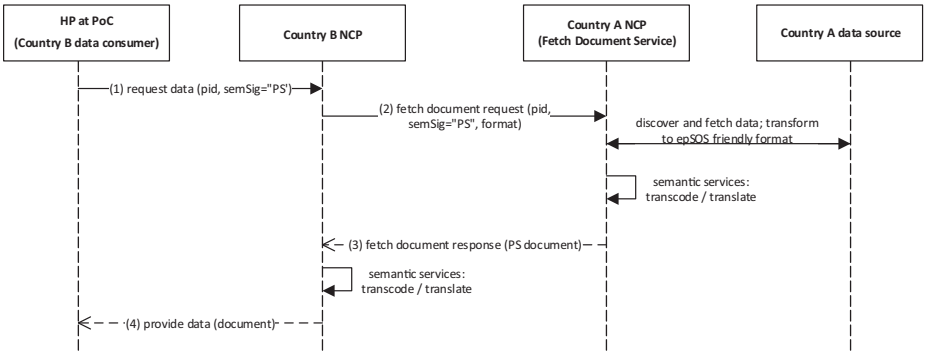

Figure 5.
"Application Architecture" interaction pattern for medical data exchange

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 safeguards, the cross-border encoding and transporting security context, etc. In other words, e-SENS BBs can be used to improve electronic patient identification, end point detection, non-repudiation, authenticating arbitrary artefacts and trust establishment for eP/PS.

Figure 6 outlines the proposed e-health infrastructure, which extends the existing epSOS based architecture with supplemental components that can be provided by e-SENS, as well as the system's 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).

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 toward 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 e-health solution. The

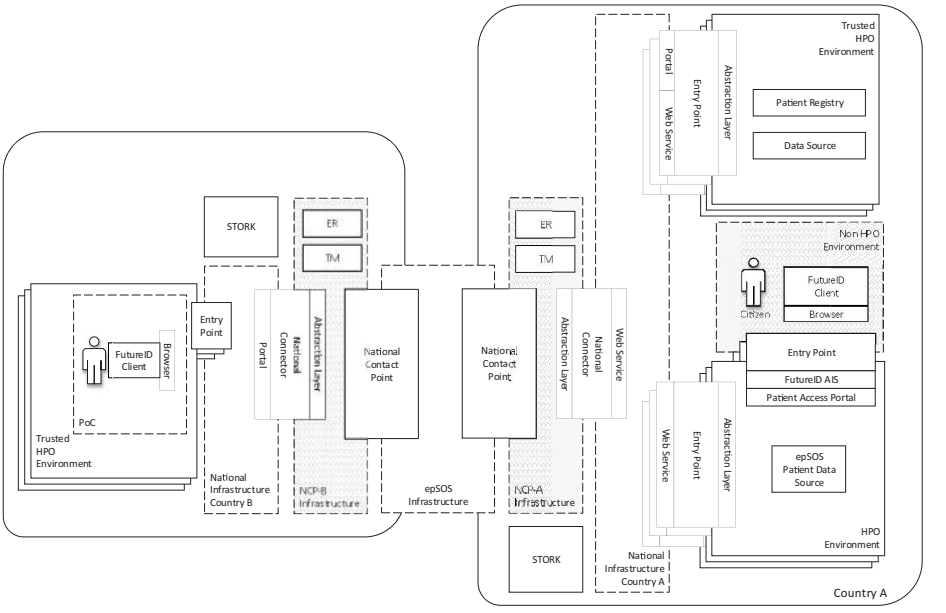

Figure 6.
The proposed global eP/PS use case architecture

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 toward the application of advanced eID, trust and security functionality directly within the realm of the user.

The facilitation of the secure exchange of eP/PS, with the injection of each non-domain specific BB supporting technology, is presented briefly in the following sub-sections.

3.1 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 health-care standards, profiles and interaction patterns is advisable. While this alignment primarily serves the technical domain, as well as carrying toward 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 health-care professional that 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 health-care professional, despite their unfamiliarity with the various national means of identification. The eID may relief the health-care professional of this burden and consequently remove a significant obstacle toward 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 health-care 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 organizational prerequisites originally designed and specified 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 proposed eID BB provides the overall architecture that defines a set of protocol, formats and data definitions to implement a cross-border authentication architecture that minimizes data disclosure and permits interoperability based on national standards. The goal is to allow business, citizens and government employees to use the presently widespread (national) identities in cross-border public and private services.

The new e-SENS electronic identification process, as supporting technology for the 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 health-care professional's software reuses this identifier to either obtain the sectorial e-health patient identifier by performing the corresponding Integrating the Healthcare Enterprise (IHE) Cross-Community Patient Discovery (XCPD) transaction (IHE, 2011; Bourqard and Le Gall, 2015) or immediately applies the obtained eID directly for the medical data request if the obtained patient identifier already qualifies as a sectorial e-health 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, health-care 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 7.

Medical data must only be disclosed or shared after the patient is identified and authenticated with sufficient accuracy (with respect to Country A demands). Each Country B data consumer because 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

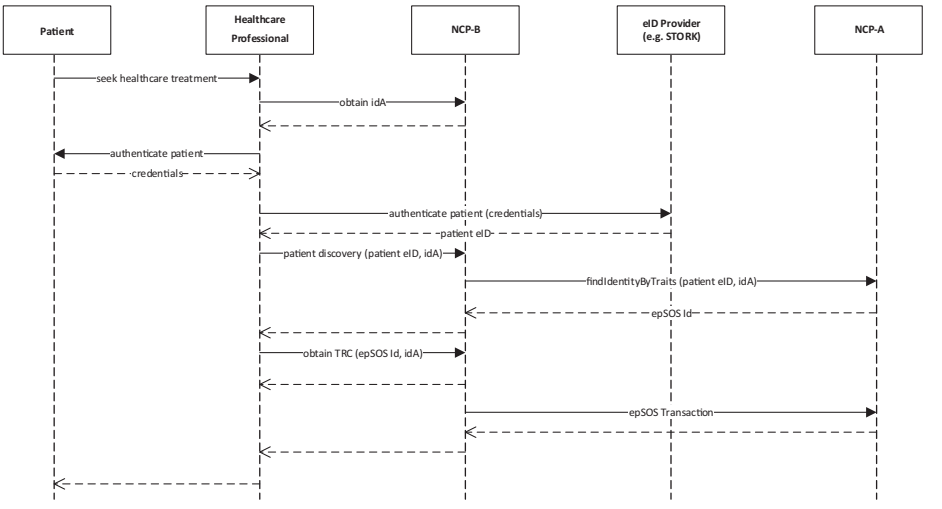

Figure 7.
Generic eID flow of events

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 considered to be of highest priority. This is why the EU through the eIDAS Regulation (European Parliament and the Council of the European Union, 2014) aims at boosting the user convenience, trust and confidence while keeping pace with technological developments, promoting innovation and stimulating competition.

3.2 Metadata locator service for end point detection

EpSOS uses 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) (Chena *et al.*, 2008; EIF, 2010) 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 are considered to be background infrastructure and a priority when looking at infrastructure redundancy with view to CEF adoption. The Service Metadata Locator (component from PEPPOL) can be exploited to evolve the epSOS CS rationale (architecture and services) by adopting e-SENS BBs such as Capability Lookup and Service Location. This step will have impact also at NCP level where refactoring will need to be made to allow the improved articulation model between NCPs. E-SENS will use the Simple Metadata Publisher (SMP) developed by PEPPOL and generalized and standardized by OASIS (2016b).

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).

3.3 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 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 MSs, 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) 13,888-3 standard (ISO/IEC, 2009) 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 have been 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 (Ruggieri, 2010), guaranteeing the sustainability of the other project's evidence emitter, even re-using the same software.

The e-SENS evidence emitter BB, enabling all the corners of the e-SENS four corner model to generate and emit electronic evidence used for non-repudiation purposes, has already been implemented and incorporated in NCP software. The OpenNCP Community has already released a new stable release, following the full integration of the e-SENS evidence emitter BB and the solution was presented and tested during the 15th European IHE Connectathon event (IHE, 2016).

3.4 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:

- assertion and authenticated attribute signatures;
- time stamp signatures for non-repudiation; and
- optional document signatures as currently assumed required by some piloting nations.

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

3.5 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 approve some "relaxation" and amendments to the original epSOS security

specifications, mainly because of the impossibility to find suitable certification authorities able to issue the required certificates.

Consumers and Providers of the interconnected distributed solutions must be able to rely on and validate the authenticity and trustworthiness of each service-provider carrying out electronic transactions; this implies mutual trust between nodes involved. 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 (Bovalis *et al.*, 2014; EIRA, 2016). Once it is finalized, its findings will enable the e-health 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, as far as e-health is concerned. It is currently under discussion.

4. The e-SENS pilot implementation for eP/PS

The e-SENS e-health pilot implementation will support cross border care for Patient Summaries and ePs, in line with Directive 2011/24/EU on patients' rights in cross-border health care. The first set of e-SENS pilots is already under implementation and cross-border piloting is expected to become operational as this paper is being prepared.

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, for example, 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 eP.

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 MSs to come also on board. Countries involved in e-SENS piloting include Greece, Italy, Luxembourg, Portugal and Spain.

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 8:

(1) *Phase 1*: Baselining. Its purpose is to provide a clear picture of the pilot implementation plan 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 dependencies and risks. Its outcome is an agreement between all stakeholders in providing in time all the needed means foreseen in the Pilot Plan.

(2) *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.

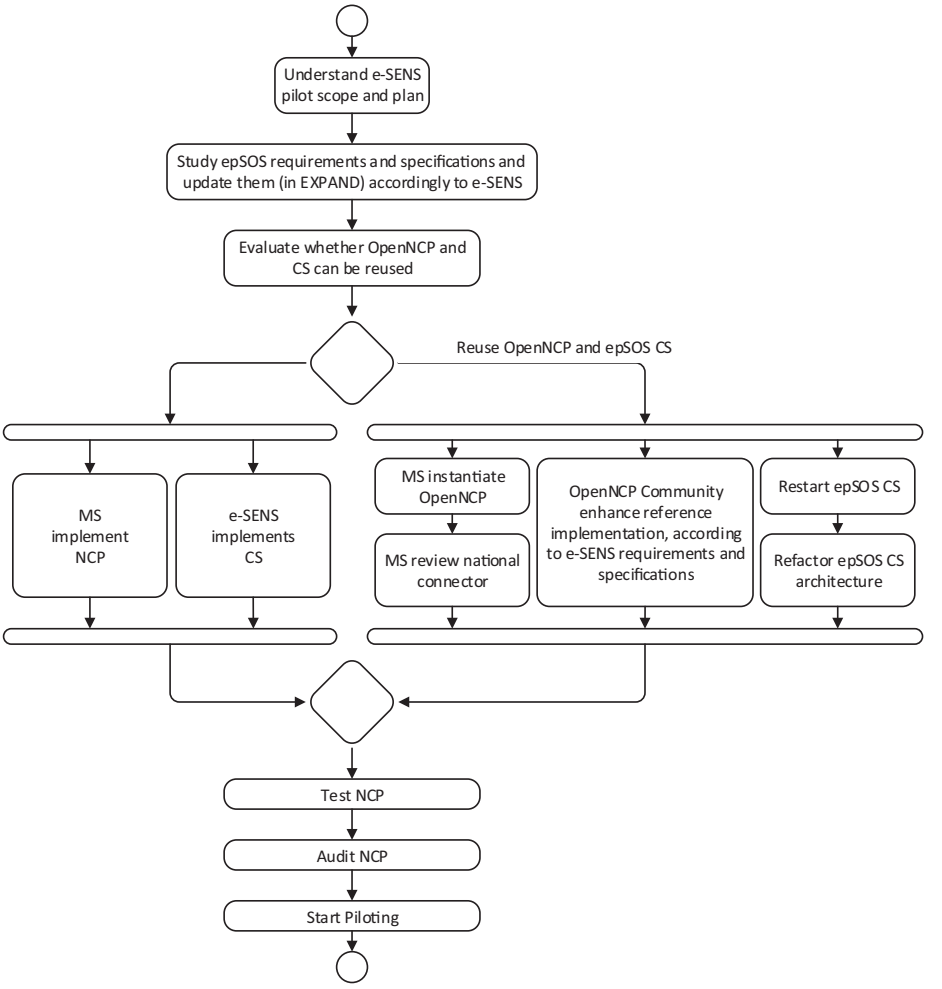

Figure 8.
e-SENS eP/PS Summary Pilot Plan

(3) *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.

(4) *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).

4.1 The national pilot plan for Greece

The piloting in e-SENS is the next step for Greece to foster European-wide, cross-border e-health services and a logical next step to the epSOS pilot services. The Greek pilot is included in the first set of pilots and 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 eP 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 Master Translation/Transcoding Catalogue (MTC) which is necessary for the semantic transformation of the PS. However, the needed legal and organizational framework for EHRs, 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 e-health 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 actions for the 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, helpdesk support (first level), and 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.

5. Discussion

An evolving architecture, to accommodate cross-domain BBs, within the continuously evolving European e-health space to support sustainable cross-border services for moving eP/PS services forward has been presented. It is quite evident that the e-health domain will greatly benefit from mitigating non-domain concerns for elDs, metadata locators, non-repudiation, eSignatures and trust establishment in a cross-border setting. Even so, deep assessment is necessary to understand the legal, organizational, semantic and technical interoperability framework that has been established in the past 15 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).

It is a fact that cross-border electronic identification, electronic signature and semantic issues have not been fully addressed yet at a European level. Following the formal adoption of the Regulation for common identification and authentication measures, related delegated/implementing acts will be developed. This will be accompanied by the necessary policy, standardization 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, and therefore common identification and authentication measures for e-health will be required. Some of the aspects the paper has dealt with may need to expand to other cross-border services that build upon services like eP/PS and require more complex solutions, like e.g. medication reimbursement.

The effective value of a cross-border health-care services such as eP/PS can be considered under different angles such as, for example, increased technical and semantic interoperability in terms of increased knowledge, enhanced legal and regulatory cooperation at bi-lateral and multilateral level, improved treatment of patients, overcoming communication barriers and allowing the transfer of meaningful information by a point of care to another placed in a different country, etc. Piloting activities are a key success factor to demonstrate the technical feasibility of the integrated single digital market. Specifications that are being developed in projects such as e-SENS are expected to contribute to the implementation of 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 CEF program. Ongoing efforts toward the consolidation of BBs such as eID, eDelivery and eSignature (outcomes of previous and currently running pilot projects) into a pan-European digital platform for cross-sector, interoperable eGovernment services are in progress.

6. Implications for policy makers

The establishment of the NCP systems and the set-up of the legal and administrative rules for making the services running have revealed critical paths and the need to elaborate solutions to be validated by the political level. Practical implications are related to cooperation, European level compatibility and sustainability of the underlying national infrastructures required to support reliable and secure exchange of medical data, as well as the readiness to address the continuously evolving interoperability, legal and security requirements in a cross-border setting. E-health interoperability challenges are familiar to all countries. For many years, each country has separately tried to address similar issues; however, each country lacks the resources

and skills needed to boost innovation and would benefit from joint effort aimed at addressing common challenges together.

National alignment is an important aspect and therefore a core foundation and a set of basic principles are also necessary to realize interoperability between MSs. This in turn has highlighted the need for action at Member State and European level to consider global and specific approaches to standardization. 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 for cross-border transactions. EIF and the current LSPs have already marked a first step in this direction.

References

AHRQ (2007), "Findings from the evaluation of e-prescribing pilot studies", AHRQ Publication No. 07-0047-EF, April 2007, The National Opinion Research Center (NORC) at the University of Chicago, Agency of Healthcare Research and Quality, US Department of Health and Human Services, available at: http://library.ahima.org/xpedio/groups/public/documents/government/bok1_034018.pdf (accessed April 2016).

Ammenwerth, E., Schnell, P., Machan, C. and Siebert, U. (2008), "The effect of electronic prescribing on medication errors and adverse drug events: a systematic review", *Journal of the American Medical Informatics Association*, Vol. 15 No. 5, pp. 585-600, available at: http://jamia.oxfordjournals.org/content/15/5/585.long (accessed April 2016).

Angelidis, P., Giest, S., Dumortier, J., Artmann, J. and Heywood, J. (2010), "eHealth strategies", European Commission, DG Information Society and Media, ICT for Health Unit, October.

Bourqard, K. and Le Gall, F. (2015), *Standards for Interoperability in Digital Health: Selection and Implementation in an eHealth Project, Requirements Engineering for Digital Health*, Springer International Publishing Switzerland, pp. 95-115, available at: http://link.springer.com/chapter/10.1007/978-3-319-09798-5_5 (accessed April 2016).

Bovalis, K., Peristeras, V., Abecasis, M., Abril-Jimenez, R., Alvarez Rodriguez, M., Gattegno, C., Karalopoulos, A., Sagias, I., Szekacs, S. and Wigard, S. (2014), "Promoting interoperability in Europe's E-government", *IEEE Computer*, Vol. 10 No. 1, pp. 25-33, doi: 10.1109/MC.2014.295.

CEF (2016), "Connecting Europe facility", Digital Agenda for Europe, A Europe 2020 Initiative, available at: http://ec.europa.eu/digital-agenda/en/connecting-europe-facility (accessed April 2016).

Chena, D., Doumeingtsb, G. and Vernadatc, F. (2008), "Architectures for enterprise integration and interoperability: past, present and future", *Computers in Industry*, Vol. 59 No. 7, pp. 647-659.

CIP (2016), "Competitiveness and innovation framework programme", European Commission, available at: http://ec.europa.eu/cip/ (accessed April 2016).

Cuijpers, C. and Schroers, J. (2014), "eIDAS as guideline for the development of a pan European eID framework in FutureID", *Open Identity Summit 2014, Gesellschaft für Informatik*, Vol. 23 No. 7, pp. 23-38.

Dobrev, A., Jones, T., Stroetmann, V., Stroetmann, K., Vatter, Y. and Peng, K. (2010), "Interoperable eHealth is worth it: securing benefits from electronic health records and e-prescribing", Information Society and Media Study Report, European Commission, available at: www.ifap.ru/library/book476.pdf (accessed April 2016).

e-CODEX (2016), "e-Justice communication via online data exchange, making justice faster", available at: www.e-codex.eu/ (accessed April 2016).

eHealth Initiative (2004), "Electronic prescribing: toward maximum value and rapid adoption: recommendations for optimal design and implementation to improve care, increase efficiency and reduce costs in ambulatory care", Washington, DC, 14 April, available at: www.providersedge.com/ehdocs/ehr_articles/Electronic_Prescribing-Toward_Maximum_Value_and_Rapid_Adoption.pdf (accessed April 2016).

eHealth Network (2014), "Guidelines on ePrescriptions dataset for electronic exchange under Cross-Border Directive 2011/24/EU", eHealth Network, European Commission, Release 1, available at: http://ec.europa.eu/health/ehealth/docs/eprescription_guidelines_en.pdf (accessed April 2016).

eHGI (2016), "The European eHealth governance initiative", available at: www.ehgi.eu/default.aspx (accessed April 2016).

EIF (2010), "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'", Bruxelles, le 16.12.2010 COM (2010) 744 final, available at: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf (accessed April 2016).

EIRA (2016), "The European Interoperability Reference Architecture (EIRA)", Interoperability Solutions for European Public Administrations (ISA) programme, European Commission, available at: https://joinup.ec.europa.eu/asset/eia/description (accessed April 2016).

ENED (2016), "European network for electronic data exchange in the health care sector", available at: www.ened.eu/ (accessed April 2016).

epSOS (2016), "European patients – smart open services, making healthcare better", available at: www.epsos.eu/ (accessed April 2016).

e-SENS (2016), "Electronic simple European Networked Services (e-SENS), moving services forward", available at: www.esens.eu/ (accessed April 2016).

European Commission (2016a), "Cross-border solutions", European Commission, Digital Agenda for Europe, available at: https://ec.europa.eu/digital-agenda/en/large-scale-pilot-projects (accessed April 2016).

European Commission (2016b), "eHealth network", European Commission, Directorate-General for Health and Food Safety, available at: http://ec.europa.eu/health/ehealth/policy/network/index_en.htm (accessed April 2016).

European Parliament and the Council of the European Union (2011), "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", Official Journal of the European Union, L 88, 4 April, pp. 45-65, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32011L0024 (accessed April 2016).

European Parliament and the Council of the European Union (2013), "Regulation (EU) 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", Official Journal of the European Union, L 348, 20 December, pp. 129-171, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013R1316 (accessed April 2016).

European Parliament and the Council of the European Union (2014), "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", Official Journal of the European Union, L 257, 28 August, pp. 73-114, available

at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG (accessed April 2016).

EXPAND (2016), "Expanding health data interoperability services", available at: www.expandproject.eu/ (accessed April 2016).

Fernando, B., Kalra, D., Morrison, Z., Byrne, E. and Sheikh, A. (2012), "Benefits and risks of structuring and/or coding the presenting patient history in the electronic health record: systematic review", *BMJ Quality & Safety*, Vol. 21 No. 4, pp. 337-346.

Fischer, M., Vogeli, C., Stedman, M., Ferris, T., Brookhart, A. and Weissman, J.S. (2008), "Effects of electronic prescribing with formulary decision support on medication use and cost", *Archives of Internal Medicine*, Vol. 168 No. 22, pp. 2433-2439, doi: 10.1001/archinte.168.22.2433.

Fonseca, M., Karkaletsis, K., Cruz, I., Berler, A. and Oliveira, I.C. (2015), "OpenNCP: a novel framework to foster cross-border e-Health services", Studies in Health Technology and Informatics, Digital Healthcare Empowering Europeans, Vol. 210, pp. 617-621.

Francesconi, E. (2012), "Supporting transnational judicial procedures between European member states: the e-codex project", *Frontiers in Artificial Intelligence and Applications*, Vol. 250, pp. 41-50.

FutureID (2016), "Shaping the future of electronic identity", available at: www.futureid.eu/ (accessed April 2016).

Hollingworth, W., Devine, E., Hansen, R., Lawless, N., Comstock, B., Wilson-Norton, J., Tharp, K. and Sullivan, S. (2007), "The impact of e-prescribing on prescriber and staff time in ambulatory care clinics: a time–motion study", *Journal of the American Medical Informatics Association*, Vol. 14 No. 6, pp. 722-730, November-December, available at: www.ncbi.nlm.nih.gov/pmc/articles/PMC2213487/ (accessed April 2016).

ICT-PSP (2016), "European commission information and communication technologies policy support programme", available at: http://ec.europa.eu/cip/ict-psp/index_en.htm (accessed April 2016).

IHE (2011), "Integrating the Healthcare Enterprise (IHE), IHE IT Infrastructure Technical framework supplement, Cross-Community Patient Discovery (XCPD) Trial Implementation", Integrating the Healthcare Enterprise (IHE), 19 August, available at: www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XCPD_Rev2-3_TI_2011-08_19.pdf (accessed April 2016).

IHE (2016), "Integrating the Healthcare Enterprise (IHE) connectathon", Integrating the Healthcare Enterprise (IHE), available at: http://connectathon.ihe-europe.net/ (accessed April 2016).

ISO/IEC (2009), "Information technology – security techniques – non-repudiation – Part 3: non-repudiation mechanisms using asymmetric techniques", ISO/IEC 13888-3:2009(en), International Standards Organization and International Electrotechnical Commission.

Kierkegaard, P. (2013), "E-Prescription across Europe", *Health and Technology*, Vol. 3 No. 3, pp. 205-219, available at: https://dx.doi.org/10.1007%2Fs12553-012-0037-0 (accessed April 2016).

Leitold, H., Lioy, A. and Ribeiro, C. (2014), "STORK 2.0: breaking new grounds on eID and mandates", Mesago Messe Frankfurt GmbH (Ed.), *Proceedings of ID World International Congress*, pp. 1-8, available at: https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=81827 (accessed April 2016).

Leitold, H. and Zwattendorfer, B. (2011), "STORK: architecture, implementation and pilots", *ISSE 2010 Securing Electronic Business Processes*, Vieweg+ Teubner, GmbH, Wiesbaden, pp. 131-142.

Miller, R., Gardner, R., Johnson, K. and Hripcsak, G. (2005), "Clinical decision support and electronic prescribing systems: a time for responsible thought and action", *Journal of the American Medical Informatics Association*, Vol. 12 No. 4, pp. 403-409, available at: www.ncbi.nlm.nih.gov/pmc/articles/PMC1174885/ (accessed April 2016).

Mondorf, A., Schmidt, D. and Wimmer, M. (2010), "Ensuring sustainable operation in complex environment: the PEPPOL project and its VCD system", Proceedings of Mediterranean Conference on Information Systems (MCIS), Paper 61, available at: http://aisel.aisnet.org/mcis2010/61 (accessed April 2016).

NETC@RDS (2016), "A step towards the electronic EHIC", available at: www.netcards-project.com/ (accessed April 2016).

OASIS (2016a), "OASIS security services (SAML) TC", available at: www.oasis-open.org/committees/tc_home.php?wg_abbrev=security (accessed April 2016).

OASIS (2016b), "OASIS Service Metadata Publishing (SMP) version 1.0", available at: http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/cs01/bdx-smp-v1.0-cs01.html (accessed April 2016).

Ølnes, J. (2012), "PEPPOL – experience from four years work on esignature interoperability", *ISSE 2012 Securing Electronic Business Processes*, Springer Fachmedien, Wiesbaden, pp. 282-295.

OpenNCP (2016), "OpenNCP community home", available at: https://openncp.atlassian.net/wiki/display/ncp/OpenNCP+Community+Home (accessed April 2016).

Pagkalos, I., Kortesis, S., Pangalos, G. and Hassapidou, M. (2010), "Deployment of the NETC@RDS service: a new step towards a European e-health space", *Proceedings of the 3rd International Conference on Biomedical Engineering and Informatics (BMEI)*, *Yantai*, *16-18 October*, Vol. 6, pp. 2511-2515, doi: 10.1109/BMEI.2010.5639699.

Pangalos, G., Asimakopoulos, D. and Pagkalos, I. (2013), "The new Greek national e-prescription system: an effective tool for improving quality of care and containing medication costs", *Informatics, Management and Technology in Healthcare*, Vol. 190 No. 1, pp. 13-17, doi: 10.3233/978-1-61499-276-9-13.

PEPPOL (2016), "Pan-European public procurement online, making procurement better", available at: www.peppol.eu/ (accessed April 2016).

Quinn, P. and De Hert, P. (2011), "The patients' rights directive (2011/24/EU) – providing (some) rights to EU residents seeking healthcare in other member states", *Computer Law & Security Review*, Vol. 27 No. 5, pp. 497-502, September, available at: www.sciencedirect.com/science/article/pii/S0267364911001221 (accessed April 2016).

Rössler, T. and Tauber, A. (2011), "The SPOCS interoperability framework: interoperability of edocuments and edelivery systems taken as example", *ISSE 2010 Securing Electronic Business Processes*, Vieweg + Teubner, GmbH, Wiesbaden, pp. 122-130.

Ruggieri, F. (2010), "ETSI specifications for registered e-mail REM", *ISSE 2009 Securing Electronic Business Processes*, Vieweg+ Teubner, Wiesbaden, pp. 242-254.

SPOCS (2016), "Building the next generation points of single contact, making business easier", available at: www.eu-spocs.eu/ (accessed April 2016).

STORK (2016), "Secure identity across borders linked, making access smarter", available at: www.eid-stork.eu/ (accessed April 2016).

STORK 2.0 (2016), "Secure identity across borders linked 2.0, making access smarter", available at: www.eid-stork2.eu/ (accessed April 2016).

Stroetmann, K., Artmann, K., Stroetmann, V., Protti, D., Dumortier, J., Giest, S., Walossek, U. and Whitehouse, D. (2011), "European countries on their journey towards national ehealth infrastructures", Final European progress report, European Commission, DG Information

Society and Media, ICT for Health Unit, available at: www.e-health-com.eu/fileadmin/user_upload/dateien/Downloads/eHealthStrategies_Final_Report.pdf (accessed April 2016).

Tinholt, D., Carrara, W., Tol, T., Foley, P., Graux, H. and Erdogan, E. (2013), "Study on analysis of the needs for cross-border services and assessment of the organisational, legal, technical and semantic barriers", European Commission – Directorate-General of Communications Networks, Content & Technology, doi: 10.2759/10003, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2310 (accessed April 2016).

TOGAF (2016), "The Open Group Architecture Forum (TOGAF) capability framework – building blocks", available at: http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html (accessed April 2016).

Wang, J., Patel, M., Schueth, A., Bradley, M., Wu, S., Crosson, J., Classman, P. and Bell, D. (2009), "Perceptions of standards-based electronic prescribing systems as implemented in outpatient primary care: a physician survey", *Journal of the American Medical Informatics Association*, Vol. 16 No. 4, pp. 493-502, July-August, available at: http://jamia.oxfordjournals.org/content/16/4/493.long (accessed April 2016).

About the authors

Dimitrios G. Katehakis is the Head of the Center for eHealth Applications and Services at the Institute of Computer Science of FORTH. He received his Electrical Engineering Diploma in Telecommunications and Electronics from the Technical University of Patras, Greece, and his Electrical Engineering MS in Computers from the University of Maryland at College Park. His work focuses on data integration analysis and the development of the appropriate health information infrastructure required for the provision of innovative, integrated Electronic Health Record (EHR) services. Since 2006, he has been scientific responsible for more than 200 commercial projects related to operational EHR systems in the National Health System of Greece. Current and past participation in projects co-funded by the EU include EURECA (FP7-ICT-2011.7 No 288048), EHR-Q-TN (7th Framework Programme), EHR-IMPLEMENT (DG SANCO), INFOBIOMED (IST/FP6-2002-IST-1-507585), PICNIC (IST-1999-10345), RETRANSPLANT (DGXIII – Health Telematics), TEMeTeN (DGXVI – RISI 2), HECTOR (DGXIII – Health Telematics) and CreteCT (Ministry of National Economy & INTERREG II). Past experience includes also working with the Medical School of the University of Maryland at Baltimore for the IONDT (US Federal), and MCR (MD State, Dept. of Health and Mental Hygiene – CDC) projects, as well as with the National Defence Ministry of Greece, the Association for Research, Technology and Training, and the Hellenic Telecommunications Organization (OTE). He has numerous publications, as well as presentations in international conferences and workshops. Currently he coordinates the ePrescription and PS workgroup of the e-SENS project (ICT-PSP/CIP). He is also a member of the BoD of HL7 Hellas. Dimitrios G. Katehakis is the corresponding author and can be contacted at: katehaki@ics.forth.gr

George Pangalos was born in Athens (GR). He received a BSc degree in mathematics from the University of Athens and a MSc and a PhD degree in computer science from the University of London (University College London, UK). Since 1990, he has been with the Faculty of Technology of the Aristotle University of Thessaloniki, Greece, where he is currently a professor in the Department of Electrical and Computer Engineering (ECE) and the director of the Informatics and Information Security laboratory of the same faculty. He has also taught in several universities in Greece and USA. His research interests include the areas of Information Systems Design and Implementation, Information System security, Database systems Security, Access control, e-Identification and e-Authentication, IT Forensics and IT security audit, internet security and secure internet transactions, Medical and Health Information Systems, e-Health and applications, Design Implementation and security of e-Government Applications. He has published over 200 articles in international scientific journals and conference proceedings. He has also been the author or co-author in several (more than 20) International and Greek books. He has also been

involved as project leader/expert in a significant number (more than 50) major international (mostly EU funded) research and development projects in the above areas. He has also participated as an expert evaluator, after an invitation from the EU, in the selection and the assessment of several (more than 20) EU projects and studies and the formulation of EU framework research programs (FP). He has also been for several years (2004-2012) the National Representative of Greece to the European Union's Security Research Program. He has been president and member of the board in several national and international scientific and professional bodies (President of the Greek Computer Society [NG], President of the Education and Research section of GCS, President and Member of the Board of the (Brussels based) European Informatics Association CECUA, Representative of Greece to the International Medical Informatics Association, Vice-President of the Greek Medical Informatics Association, etc.). He has also been director/CEO of several IT related organizations and departments (President of the Greek Centre for e-government Applications in Social Security and Health [IDIKA], President and CEO of the Regional Health System [PESY] of Thessaly, Director of the Informatics Institute and of the under and post graduate IT schools of the Greek Productivity Centre, Member of the AUTH research management committee, Co-founder and Director of the IT Support center of AUTH [1991-2001], etc.).

Andriana Prentza is an Associate Professor at the Department of Digital Systems of the University of Piraeus, Greece. She received her Diploma in Computer Engineering and Information Sciences and her MSc in Biomedical Engineering from the University of Patras, Greece, and her PhD degree in Biomedical Engineering from the Eindhoven University of Technology, Eindhoven, the Netherlands. She has been a Teaching/Research Assistant at the Department of Electrical Engineering of Eindhoven University of Technology and a senior Research Scientist at the Biomedical Engineering Laboratory of the Institute of Communication and Computer Systems of National Technical University of Athens, Athens, Greece. She has been very actively involved in a number of European (FP4, FP5, FP6, FP7) and National R&D programs focusing on Information Communication Technologies (ICT) projects and she serves as expert evaluator and reviewer for the European Commission and national research and development programs. She has published more than 90 scientific papers in peer-reviewed international journals, book chapters and conference proceedings. She is Associate Editor for the *IEEE Journal of Biomedical and Health Informatics* and serves as a reviewer for several other scientific journals. Her current research interests include Software Engineering techniques and methodologies for the development and evaluation of software systems and services in the areas of eGovernment, e-health and biomedicine. She is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE) and a member of the Technical Chamber of Greece. Since 2013, she is a member of the Horizon 2020, Advisory Group for Health, demographic change and well-being of the European Commission.