Bernd Zwattendorfer, Thomas Zefferer, Arne Tauber - "E-ID Meets E-Health on a Pan-European Level" - Proceedings of the IADIS International Conference e-Health, 2011, pp. 97-104

E-ID MEETS E-HEALTH ON A PAN-EUROPEAN LEVEL

Bernd Zwattendorfer
Graz University of Technology, E-Government Innovation Center, EGIZ
Inffeldgasse 16a, 8010 Graz, Austria

Thomas Zefferer
Graz University of Technology, E-Government Innovation Center, EGIZ
Inffeldgasse 16a, 8010 Graz, Austria

Arne Tauber
Graz University of Technology, E-Government Innovation Center, EGIZ
Inffeldgasse 16a, 8010 Graz, Austria

ABSTRACT

Information and communication technologies are more and more becoming an inherent part of our life. This is particularly manifested in the fields of electronic government and electronic health care. Identification, authentication, and data privacy protection are the key elements to ensure both secure and reliable transactions and trust in the applied technologies. So far, European governments and public administrations have rolled out eID (electronic identity) solutions and put in place proper eHealth infrastructures that are tailored to national needs. Globalization and the opening of the EU internal market have raised the demand for interoperable solutions across national borders in order to allow citizens to use own eGovernment and eHealth infrastructures also abroad. For this reason, the European Commission has started several initiatives with the aim to establish interoperability between different national solutions. The large scale pilot STORK strives for the goal to enable mutual recognition of electronic IDs between EU Member States. Another large scale pilot called epSOS provides a pan-European framework for the secure and reliable exchange of patient health data. In this paper we review and compare both large scale pilots from several perspectives. We further investigate how synergies between both pilots can be exploited so that epSOS can reap the benefits of STORK to replace paper-based identification procedures with a fully-fledged electronic one.

KEYWORDS

eID, electronic identity, eHealth, STORK, epSOS

1. INTRODUCTION

The emergence of information and communication technologies (ICT) has had a significant influence on various parts of our daily life. Since nowadays more and more transactions are processed online, secure and reliable user identification over the Internet has become an important topic. One popular field of application is eGovernment, where eIDs are used to unambiguously identify citizens within administrative and governmental procedures (Siddhartha, A. 2008). Another area that has been heavily influenced by ICT during the past years is healthcare. The utilization of information and communication technologies in the context of healthcare services has been commonly known under the term eHealth.

Both, in the field of eID and in the area of eHealth various independent approaches and solutions have been developed during the past years and decades. These solutions are mostly tailored to the requirements of a certain country. Hence, interoperability between different solutions is often not ensured by their nature. With the increasing mobility of people, interoperability has become a significant demand. The European Union has already reacted on this and is currently supporting several large scale pilots (LSP) that aim to improve interoperability of existing solutions on a pan-European level. In the field of eID, the LSP STORK (Secure Identity Across Borders Linked) (Ivkovic, M. et al 2009) attempts to establish a pan-European interoperability infrastructure for the mutual recognition of eIDs across EU Member State boundaries.

Similarly, the LSP epSOS (European Patients Smart Open Services) (epSOS, 2010) aims to facilitate cross-border activities in the context of eHealth services.

Although, the LSPs STORK and epSOS run independently from each other, both rely on the two basic concepts *'user identification and authentication'* and *'electronic signatures'* within their proposed use cases. Therefore, it is meaningful to search for synergies between the two LSPs in order to reap the benefits from each other and to achieve better results in a more cohesive and efficient way. In this paper we identify these synergies and show how they can be used to improve the pilots. By discussing several use cases we further show how these synergies could be turned into concrete results, which all users can benefit from.

To provide the reader with a comprehensive understanding of the topic, the remainder of this paper is structured as follows. Section 2 introduces the two LSPs STORK and epSOS, describes the projects' main goals and reports on already observable results. Subsequently, in Section 3 a comparison of the two projects is made. Synergies that may be exploited to fill certain gaps are identified and discussed in Section 4. Possible solutions implementing and using the identified synergies are introduced in Section 5. Finally, conclusions are drawn.

2. THE EUROPEAN LSPS STORK AND EPSOS

During the past years, eID and eHealth have turned out to be more and more topics of increasing importance and interest. Due to the advancing globalization and the opening of the European internal market, the demand for interoperability between different closed systems has been increased to the same degree. Especially in the European Union, several attempts are currently made to improve the compatibility of Member State specific solutions in the fields of eID and eHealth. In this section, basic concepts and objectives of the two LSPs STORK and epSOS, which aim to tackle the issue of eID and eHealth interoperability, are briefly introduced.

2.1. LSP 'Secure Identity Across Borders Linked (STORK)'

With the increasing need for secure and reliable authentication mechanisms over the Internet, most European countries have rolled out their own eID infrastructures in the last years. Missing central coordination and varying national legal requirements have led to significant differences in current country-specific solutions. Due to these differences, interoperability between EU Member States eID solutions is not ensured by their nature, which in turn makes cross-border user authentication a hard task.

STORK aims to tackle this issue by establishing a cross-border interoperability framework that builds upon already existing national eID solutions. In this way, subsidiarity of EU Member States is ensured and national solutions remain untouched. At the same time, interoperability with foreign eID systems is established. The STORK interoperability framework comprises two different authentication models. Applying the so-called *'middleware model'* service providers integrate all foreign eIDs using a country specific middleware. Alternatively, the STORK framework also supports a *'proxy model'*. Following this approach, each country runs a single gateway – a so called *'Pan-European Proxy Service (PEPS)'*. Cross-border transactions are delegated from Service Providers (SP) to their national PEPS instances, which act as gateway and subsequently forward the transaction to the responsible foreign country's PEPS. The actual eID authentication process itself is carried out in the citizen's home country. Finally, the obtained identification and authentication data is again returned through the PEPS infrastructure back to the requesting Service Provider.

Several EU Member States like Austria or Germany rely on the middleware model due to scalability issues, or liability and data protection policies. In this paper, however, we focus on the proxy model, since it has turned out that this model has a higher potential for synergies with the epSOS project.

The proposed STORK authentication framework has already been implemented and is currently evaluated by several pilot applications (Leitold, H. and Zwattendorfer, B. 2010). Experiences that have been gained so far have shown the ability of the proxy model to enable secure and reliable cross-border user authentication.

Figure 1 illustrates a typical STORK authentication process of a European citizen (originating from country B) at a Service Provider (SP) located in a foreign country A on an abstract level. In this cross-border scenario, both countries (Member State A and B) rely on the PEPS approach. In a first step, the citizen of MS B wants to access a certain application at the Service Provider located in MS A using her eID. Starting the

cross-border authentication process, the Service Provider contacts its national PEPS A instance. PEPS A forwards the authentication request to the citizen country PEPS B instance where the authentication process actually takes place using domestic Identity Providers (IdP) and/or Attribute Providers (AP). After having successfully authenticated the citizen, PEPS B assembles the identity data into an authentication token and transfers this token back to PEPS A. In this process step, PEPS B asserts PEPS A that the citizen has successfully authenticated with a certain quality at a certain point in time. In a final step, PEPS A returns the identity and authentication information to the requesting SP where access to the service is granted or denied for the foreign user.

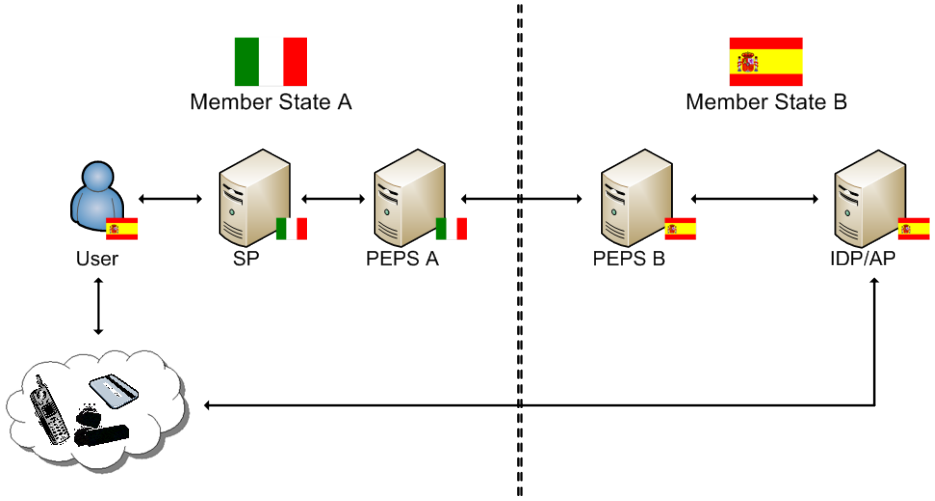

Figure 1. STORK Authentication Process

2.2. LSP 'European Patients Smart Open Services (epSOS)'

While STORK aims to make existing eID solutions interoperable, the goal of the large scale pilot epSOS is to achieve interoperability for eHealth services on a pan-European level. In particular, epSOS aims *'to develop a practical eHealth framework and ICT infrastructure that will enable secure access to patient health information, particularly with respect to a basic Patient Summary (PS) and ePrescription (eP, including eDispensation - eD), between European healthcare systems'* (epSOS 2010).

According to (Heider, G. 2010), *'the main functionality of the epSOS LSP environment is the provision of patient health data stored in patient's home country to a health care professional providing health service in a foreign country'*. Besides the secure and reliable transmission of patient health data, identification has been identified as a key element of the epSOS LSP. Reliable identification and authentication mechanisms are vital to unambiguously identify patients and to ensure that privacy-sensitive health data is protected and accessed by authorized health care professionals (HCP) only. Even though identification is a vital prerequisite, the main objective of epSOS is the cross-border provision of patient health data. Basic building blocks of the infrastructure proposed by epSOS are the so called National Contact Points (NCP) that act as interfaces between different national eHealth infrastructures. According to (Kolitsi, Z. and Wilson, P. 2010), an *'epSOS NCP is identifiable in both the epSOS domain and in its national domain, acts as communication gateway, and establishes a Circle of Trust amongst national Trusted Domains'*.

At a high level view, Figure 2 illustrates a typical identification process within the epSOS project. Currently, the identification process of e.g. a patient of Member State B takes place at the Point of Care[1] (PoC) in Member State A and is carried out by an authorized HCP. In the example of patient identification, the HCP is responsible for verifying the foreign patient's identity by checking a passport, driving license or health insurance card. To additionally check whether the patient allows the cross-border transfer of her sensitive health data between institutions of Member States A and B, the HCP needs to verify certain patient's identification data in the patient's home country. In a first step the HCP submits the patient identity verification request through her PoC to the NCP of Member State A. NCP A then forwards the identity

[1] A point of care (PoC) defines a hospital, a medical office or any other point where a patient could receive healthcare.

verification request to the NCP of Member State B where the patient originally comes from. At NCP B the identification data is verified using national infrastructures. Having successfully verified the patient's identity, a special Patient ID uniquely identifying the patient within the epSOS context is returned from NCP B to NCP A and finally to the HCP stationed at PoC.

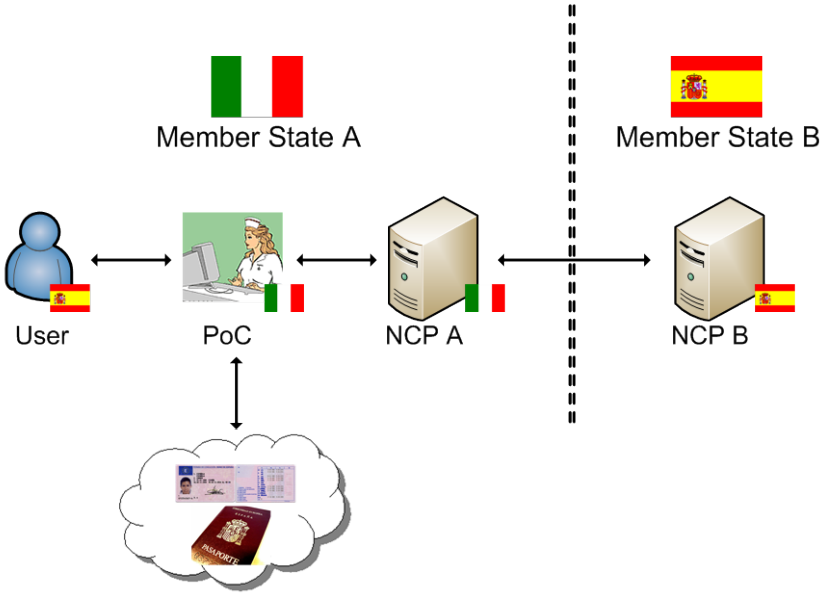

Figure 2. epSOS Overview

The conceptual similarity between an NCP and PEPS, which is a major component in the STORK infrastructure, is evident. A comparison of the frameworks that have been developed in STORK and epSOS is given in the next section.

3. COMPARISON

The interoperability objectives of the two LSPs STORK and epSOS are very similar. Both projects aim to establish interoperability between country specific solutions rolled out on the large scale. In this section, we look at similarities between STORK and epSOS in more detail and analyze their significant differences in order to facilitate the identification of potential synergies.

The most apparent similarity between STORK and epSOS is their operating principle: both large scale pilots aim to facilitate the secure and reliable cross-border data exchange between EU Member States while retaining already existing country specific infrastructures. The architectures of STORK and epSOS are basically comparable as being illustrated in Figure 3. Both LSPs rely on national gateways, through which cross-border data exchanges are processed. All gateway instances belong to a so called Circle of Trust that is based on agreed policies of a particular governance structure in order to mutually establish trust relationships. In STORK, these gateways are called PEPS, while epSOS refers to these components as NCP. Nevertheless, the basic intention of using one single gateway per EU Member State is the same in both LSPs.

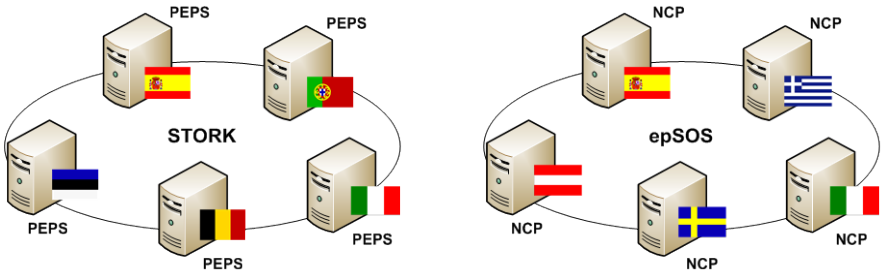

Figure 3. Comparison of basic STORK and epSOS architectures

In both projects, data is exchanged but not shared between different Member States. Thus, the requested information is forwarded by the involved gateways for temporary use only, but is never stored in the foreign country's infrastructure. Besides the overall architecture, the conceptual and technical design of those gateways is very similar. Both, the PEPS and NCP concepts internally rely on a platform independent model and make use of web standards based on XML for cross-border communication and data exchange.

Besides these similarities, there are also some significant differences. One apparent difference is the kind of information being exchanged across borders. While STORK basically exchanges only simple attributes, epSOS proposes the exchange and transformation of complex documents. Another major difference is the use case. While STORK supports the cross-border identification and authentication of citizens only, epSOS additionally aims at the cross-border exchange of patient health data. Even if both LSPs rely on a common XML-based transport protocol, further differences can be found on message level. For instance, STORK only supports a request/response messaging mechanism, whereas epSOS additionally relies on a notification message. However, for identification and authentication both projects rely on the well-established Security Assertion Markup Language (SAML) standard (Cantor, S. et al 2005).

Even though STORK and epSOS have some apparent similarities, also several significant differences between these two LSPs have been identified. Nevertheless, there is much potential to use synergies between these projects. The following section identifies potential synergies by sketching appropriate use cases.

4. SYNERGIES

This section identifies common use cases and shows on an abstract level how STORK and epSOS processes can be combined together so that epSOS can benefit from the outcome and findings of STORK. Thus, examples are given on how cross border electronic identification can be successfully integrated into the eHealth world of epSOS.

By having a deeper look at the STORK uses cases and protocols, the following epSOS scenarios could be realized using STORK functionality (Campari, C. et al 2010):

1. Patient identification
2. HCP authentication
3. Patient consent signature
4. Signature verification of foreign signed prescriptions

4.1 Patient identification

Within the epSOS world - before being medically treated by a HCP - the patient needs to be uniquely identified. Currently, epSOS foresees identification using paper-based documents only. By the help of STORK, patients from foreign countries could be identified using their national electronic ID. The only things required are Internet access, a web browser, and a token reader (depending on the underlying technology of the eID) at the point of care (PoC).

Figure 4 illustrates a successful epSOS patient identification process based on the STORK architecture. In this example, the traditional authentication process used in epSOS is enhanced by supporting foreign eIDs. For that, no major modifications are required. The traditional epSOS authentication process is just enhanced

by a fully-fledged electronic one. From a STORK perspective, the national NCP acts as simple service provider, which triggers the cross-border authentication process. The Patient-ID received via STORK can still be used for verification at the citizen country NCP. Thus, no adaption is necessary in the actual epSOS process flow.

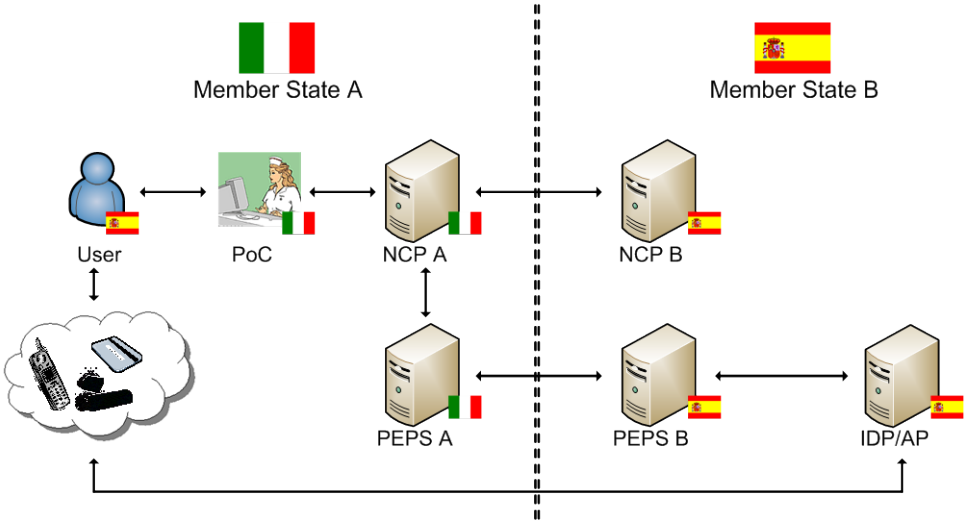

Figure 4. Foreign Citizen Authentication in epSOS using STORK

4.2 HCP authentication

The use case of HCP authentication is very similar to the use case of patient identification; hence we continue without a detailed analysis. In addition to a unique ID for the HCP also authorization attributes are requested during authentication. These authorization attributes specify a certain role and guarantee that the HCP has the appropriate rights and profession to medically treat the patient (e.g. to prescribe medicine for recovery). A HCP authentication is usually started directly from the epSOS web portal.

4.3 Patient consent signature

A major objective of epSOS is the access to patient's data across borders. For such a data exchange, an additional permission by the patient is required. epSOS manages this additional authorization requirement by relying on a patient's consent. Thus the patient explicitly gives her consent for cross-border data transfer, which is verified by the NCP. By combining both LSPs, the create-signature functionality of foreign eIDs through STORK could be used for signing the patient's consent. In this scenario, the process flow steps and the modules involved are equal to the ones shown in Figure 4. There is no change in the process flow, only the exchanged data is different.

4.4 Signature verification of foreign signed prescriptions

In this scenario, it is assumed that some kind of medicine needs to be dispensed to patient A in country B. However, the medicine to dispense has already been prescribed in country A and patient A has an electronic prescription for it. The aim of this use case is to verify an electronic prescription (issued by a HCP in country A) in country B. For that, the functionality of a national PEPS could be enhanced by signature verification to verify the ePrescription's signature.

5. IMPLEMENTATION PROPOSALS

Identification, authentication and electronic signatures are key elements of the eHealth sector. Secure identification and authentication of patients or HCPs is also an essential part of epSOS. Electronic signatures are helpful for securing and authenticating cross-border data exchange of patient summaries or electronic prescriptions. Section 4 has identified common use cases where STORK and its developed eID interoperability framework could support epSOS in its processes. This section goes a little bit more into detail and tries to point out how a liaison between STORK and epSOS could be achieved.

5.1 Identification and authentication

epSOS defines uses cases where unique identification and authentication of patients or HCPs is required. Currently, the identification process of e.g. a patient by a HCP is based on traditional ID documents such as passports or driving licenses. However, for retrieving a unique patient identifier also STORK could be used. STORK has already developed and implemented a framework for identification and authentication across borders. In its common interface specification (Alcalde-Moraño, J. et al 2010) STORK has defined an attribute reflecting an eIdentifier which could simply be used as PatientID in the epSOS context. If required, also a new attribute could be defined. The STORK protocol has been specified open and flexible in such a way that new attributes can be introduced easily. Therefore, no change in the original message format would be necessary, only an agreement on organizational level of both projects. This easy adoption of new attributes can also be used for HCP authentication and authorization. In epSOS, HCPs must have appropriate rights or roles to e.g. access foreign patient data. Those roles could be mapped to STORK attributes and transferred to the requesting PoC.

STORK functionality should be easily integrable into an epSOS portal because both, STORK and the current epSOS authentication services rely on the SAML Web SSO profile (Hughes, J. et al 2005). However, both projects build upon a different set of SAML bindings and protocols. Thus, a common agreement on used bindings and protocols needs to be negotiated between both projects. Additionally, the contents of the exchanged assertions need to be defined in detail in order to be accepted by the respective services.

5.2 Signature creation and verification

Several epSOS use cases rely on the secure exchange of documents across borders, such as the transfer of patient data or electronic prescriptions. To guarantee the authenticity of those documents electronic signatures are applied. Nowadays, most eID tokens can be used to create electronic signatures. The STORK interface specification supports the creation of electronic signatures on documents using the STORK protocol. This functionality could be used in epSOS for e.g. patient's consent signing. Since STORK supports signing of arbitrary XML data, no special amendments for epSOS would be required.

Usually, besides signature creation, it's essential to verify documents that are signed. Currently, STORK does not support the verification of digital signatures but only the validity check of digital certificates. However, it would be advantageous to enhance the current implemented certificate validation request/response protocol to additionally support signature verification. To keep the verification process similar to the creation process, in STORK just an additional attribute indicating a signature verification request needs be introduced. At the moment, signature creation within STORK is based on the OASIS DSS protocol (Pope, N. and Carlos Cruellas, J. 2007) thus also signature verification should follow this standard.

6. CONCLUSION

Secure identification and authentication play important roles in daily live when using online services. Especially in applications where sensitive data is transferred or processed, security is an inevitable requirement. Popular fields where unique identification is required are e.g. the eGovernment or eHealth sectors. Currently, most applications in these fields are designed to satisfy certain needs of one country only

and cross-border communication is limited. However, the European commission has started several initiatives and research projects to overcome these interoperability issues. The LSP STORK focuses on the interoperability of national EU Member States' eID solutions. Similarly, the project epSOS aims on facilitating the exchange of patient or health data across borders.

Although both projects are carried out independently, several synergies can be identified. The most apparent similarity between STORK and epSOS is probably their basic architecture. Both projects rely on a single gateway per Member State – a so-called PEPS in STORK terminology and a NCP in the epSOS world. Those gateways are responsible for the cross-border data exchange and hide the national and country-specific solutions. Nevertheless, also differences between both projects exist since STORK focuses on the secure exchange of simple identification data, whereas epSOS tries to facilitate the cross-border exchange of complete documents.

However, both projects can be combined to enhance certain general use cases to full online services. For example, for patient identification the epSOS concept currently relies on paper-based IDs only. To avoid such a media break, we have shown how the STORK framework could be integrated into the epSOS architecture to support the recognition of foreign electronic IDs, too. This could be easily achieved since both projects base on well-established standards such as SAML. In general, the use of standards and open interfaces is essential for re-using concepts in other projects and establishing interoperability.

REFERENCES

Conference paper or contributed volume

Ivkovic, M. and Leitold H. and Rössler T. 2009. Interoperable elektronische Identität in Europa, *In 7. Information Security Konferenz*, Krems, Austria pp. 175–190

Leitold, H. and Zwattendorfer, B. 2010. STORK: Architecture, Implementation and Pilots, *In ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference*, Berlin Germany, pp. 131-142.

Deliverable

Alcalde-Moraño, J. et al, 2010. *D5.8.3b Interface Specification*. STORK consortium

Heider G., 2010. *D3.6.2 Final identity management specification definition*. epSOS consortium

Kolitsi Z. and Wilson P., 2010. *D2.1.2 Legal and Regulatory Constraints on epSOS Design- Participating Member States*. epSOS consortium

Journal

Siddhartha, A., 2008. National e-ID card schemes: A European overview. *In Information Security Technical Report*, vol. 13, pp 46-53

Report

Campari, C. et al, 2010. *Report on Common Specifications for eHealth LSP*. STORK consortium

Specification

Cantor, S. et al, 2005. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard

Hughes, J. et al, 2005. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard

Pope, N. and Carlos Cruellas, J., 2007. *Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0*. OASIS Standard

Web Page

epSOS, 2010. epSOS – European patients smart open services. http://www.epsos.eu/about-epsos.html