Zwattendorfer, B.; Sumelong, I.; Leitold, H., "Middleware architecture for cross-border eID,"
Eighth International Conference on Information Assurance and Security (IAS), pp. 303-308
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6412419&isnumber=6412367

Middleware Architecture for Cross-Border eID

Bernd Zwattendorfer
E-Government Innovation Center
Graz University of Technology
Graz, Austria
Bernd.Zwattendorfer@egiz.gv.at

Ivo Sumelong
OpenLimit SignCubes GmbH
Berlin, Germany
Ivo.Sumelong@openlimit.com

Herbert Leitold
Secure Information Technology
Center (A-SIT)
Graz, Austria
Herbert.Leitold@a-sit.at

***Abstract*— Many European states have issued electronic identities (eID) to its citizens since the early 2000s. Several have reached full coverage and usually high assurance credentials, such as smartcards, USB crypto tokens, or mobile phone eIDs are used. This lead to an impressive security infrastructure to authenticate at online services that, however, evolved as national silos – interoperability was no priority for a while. To overcome this, 18 European states have joined forces in the large scale pilot STORK. A SAML-based technical solution for cross-border eID federation between states has been designed, implemented, and finally piloted in a number of production services. In this paper we present the STORK middleware architecture that has been developed by Austria and Germany. Its main characteristic is a decentralized deployment that gives some end-to-end security and privacy advantages, but also needs particular attention to meet scalability challenges. This is compared to the STORK proxy model, an alternative centralized deployment approach that was chosen by other states. Federation between the two architectures is described, with particular attention to security and privacy aspects.**

Keywords- eID, electronic identity, middleware, STORK, interoperability

I. INTRODUCTION

The European Commission has recently (June 2012) published the proposal for an EU regulation on Internal Market electronic identification and trust services [1]. Pending upcoming political discussion in the Parliament and the Council to advance the proposal to a legal act, it is expected to establish a missing link on pan-European eID federation. This missing link is a legal basis for mutual recognition of national eIDs. The political will to advance to cross-border recognized eID already dates back to the Manchester Ministerial declaration 2005 [2]. This will has been further reinforced in the Malmö Ministerial declaration [3]. In fact, provisions for secure cross-border electronic services for EU citizens and businesses have already emerged from just a "desire" to a "must": An example is the EU Services Directive [4] that – in the services sector – grants a right for filing applications electronically from abroad. Such a right advances eGovernment from a voluntary provision to a public authorities' obligation. This also has implications on information security – think of how to uniquely and securely identify and authenticate unknown foreign citizens or businesses upon their first application.

The political decision is however facing technical and organizational reality. It already has reached a pretty complex and heterogeneous state when the Manchester declaration [2] has been filed: Early adopters like Austria, Belgium, Estonia, Finland, or Italy started issuing smart cards to each citizen around 2003 and reached full penetration around 2005. Not that other countries like Germany, Lithuania, Portugal, or Spain just followed, also further credential technologies got widely deployed like mobile phone based eID, software certificates, or one time passwords. For an overview of "higher assurance" credentials in the European market we refer to a European Commission study carried out for 32 states in 2009 [5].

To prepare the policy measures on mutual recognition and to get some hands-on experience with eID federation in such a heterogeneous environment, the European Commission together with 18 European states launched a large scale pilot "STORK" (Secure idenTities acRoss boRders linKed) in 2008. The basic idea was to gain experience and to see in real production environments, where issues arise or one even might get stuck. Uncertainties that have driven the piloting idea have inter alia been trust framework considerations, security concerns, questions of accountability and liability, data protection or legal issues rooted in the procedural laws service providers need to meet. A governing principle of STORK was that the federation infrastructure shall not change existing national eID solutions, but shall be built as an interoperability layer on top of those. This recognizes the national responsibility of citizen identifications as a core sovereign act.

One building block of STORK is the so-called "middleware model" (MW). It is an interoperability framework that has been developed by Austria and Germany, as it best fits the user-centric eID infrastructure of those countries, but it is also appealing from an end-to-end security and privacy perspective. This paper discusses the middleware architecture. The remainder of the paper is structured as follows: In section II we sketch the most prominent identity frameworks as related work. We start discussing STORK in section III where the basic framework is described and the two interoperability models are explained. These models are referred to as "Middleware" (MW) and "Pan-European Proxy Service" (PEPS). The core part of the paper is section IV and section V which gets into the details the architecture and the implementation of the MW model. Security measures are discussed. Finally, we give lessons learned and draw conclusions.

II. Related Work

Identity management is no new topic. Numerous identity management initiatives and systems already exist and have evolved over the past years. We briefly introduce a couple of systems that gained importance either due its broad use, or as they established relevant standards.

Kerberos [6] for example was one of the earliest systems allowing secure and uniform authentication in unsecure TCP/IP networks. Due to the increasing popularity of the WWW the need for secure identity management systems arose also on application level and on the Web. One such system supporting central authentication and single sign-on (SSO) for several services on the Web was Microsoft Passport[1] (latterly called Windows Live ID). This system is seen as an example for a central identity model.

Other identity management systems came up such as the Liberty Alliance Project [2] (that evolved to the Kantara initiative [3]) or Shibboleth. Both projects follow a decentralized architecture and allow SSO based on identity federation. Whereas the Liberty Alliance Project focused on federating enterprises, Shibboleth [4] targeted on inter-connecting universities. Both projects influenced the development of the current version of the Security Assertion Markup Language (SAML 2.0) [7]. SAML has been developed by OASIS and defines one of the most important standards dealing with SSO and identity federation. A similar framework constitutes WS-Federation [8], being part of the WS-Security framework. Another decentralized authentication system defines OpenID[5]. OpenID is similar to the Liberty Alliance systems but uses URL-based identities for authentication.

Identity management and in particular unique identification plays an important role for governments. The USA introduced its National Strategy for Trusted Identities in Cyberspace (NSTIC) [9] in 2011. It aims on the creation of a secure and trusted identity ecosystem facilitating access to public and private sector services. Several countries – especially in Europe – have already rolled-out national eID solutions for eGovernment or eBusiness. Those eID solutions follow different approaches. The user-centric approach based on stronger authentication mechanisms is applied with secure tokens such as smart cards or mobile phones. Other approaches federate between authentication gateways or use central authentication gateways as identity provider. Most national eID solutions rely on a Public Key Infrastructure (PKI) and the X.509 standard. The IDABC eID country reports [5] give a comprehensive overview of national eID solutions in Europe.

[1] http://www.passport.net

[2] http://www.projectliberty.org

[3] http://kantarainitiative.org

[4] http://shibboleth.net

[5] http://openid.net

III. STORK Interoperability Models

This section gives an introduction to the STORK framework and its interoperability models. The aim of the STORK framework was to achieve cross-border eID interoperability agnostic from underlying technologies or infrastructures. Hence, the STORK framework takes already existing national eID solutions as a basis and builds an interoperability layer on top of it.

The STORK framework defines two models, the so-called PEPS model (Pan-European Proxy Service) and the MW model (Middleware):

The PEPS model is a proxy-based approach with identity intermediaries. A national gateway (the PEPS) serves as single interface to other countries and encapsulates specifics of the national eID infrastructure (i.e., the communication to service providers, identity providers, and/or attribute providers). Additionally, the PEPS implements the protocols and functionality for cross-border authentication. In a cross-border authentication process, the PEPS is an intermediary between the service provider and the actual (foreign) identity provider. The PEPS asserts the service provider that a user has been successfully and properly authenticated by a foreign identity provider. A PEPS can either act as so-called S-PEPS (PEPS in the state of the service provider) or as C-PEPS (PEPS in the state of the citizen). An S-PEPS communicates with the service provider and the corresponding C-PEPS thus depicts an intermediary between those two entities. In comparison, a C-PEPS receives authentication requests from an S-PEPS and triggers the identification and authentication process at an identity and/or attribute provider. The advantage of this proxy model is that each PEPS only needs to serve its national eID infrastructure and the common STORK protocol [10] for cross-border communication. Thus, in a cross-border scenario specifics of the national eID infrastructure are hidden from other involved entities of other countries. This also hides national or proprietary protocols from other countries, as the PEPS leverages to the common cross-border STORK protocol.

In the user-centric MW model users directly authenticate at the service provider. This means that the service provider itself supports all desired identification and authentication methods. For supporting the middleware model, service providers install and deploy a so-called server-side middleware (VIDP – Virtual Identity Provider), which is operated in the service provider's infrastructure. It particularly preserves privacy because identity data are stored in the user's domain and no intermediaries are involved. Another advantage of this model is end-to-end security, as the user's eID (such as a smart card) can establish a direct communication channel to the service provider. A drawback is, however, that service providers need to integrate the various protocols and eIDs of foreign countries. We will discuss in section V how this has been met.

STORK implemented both models PEPS and MW, and its combinations. I.e., citizens from MW countries can authenticate at service providers of PEPS countries and vice versa. Basically, four different STORK interoperability models can be distinguished (PEPS-PEPS, MW-MW, PEPS-MW and MW-PEPS). Details on these four interoperability models can be found in [11]. In fact, common specifications and protocols have been designed so that STORK is seen as s single framework that supports both central and decentralized deployment. Identity and authentication data exchange is based on the well-known and standardized Security Assertion Markup Language (SAML). Details on the protocol for cross-border data exchange are given in the STORK interface specification [10]. Aside authentication protocols, STORK defined quality authentication assurance (QAA) levels. It assigns each eID to one of four QAA classes. This is similar to levels of assurance (LOA) in other frameworks. QAA is not further discussed in this paper.

IV. MIDDLEWARE ARCHITECTURE

The middleware model represents the decentralized deployment option of STORK. It has merit from an end-to-end security and from a privacy perspective. It however faces the scalability challenge that service providers need to support several (possibly many) foreign eID tokens that can be based on different protocols. This asks for a modular and scalable architecture. This section describes the modular architecture of the VIDP, the main entity of the STORK middleware approach.

The MW model has been developed by Austria and Germany – both countries operating their national eID in a MW model: Austria has a national eID solution based on the MW concept and supporting several smartcards and mobile phone eID in use since 2003 (Austrian Citizen Card [12]). Germany has set up a MW infrastructure for the so-called "*neuer Personalausweis*" (nPA) [13] on national level in 2010. Figure 1 illustrates the common MW architecture.

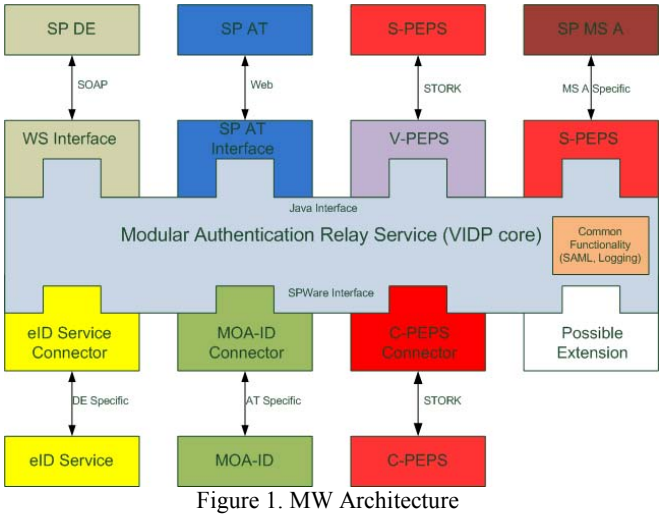

Figure 1. MW Architecture

To satisfy modularity and scalability requirements, it consists of a common component (Modular Authentication Relay Service (MARS)) that can be extended by plug-ins and plug-ons for the national eID and SPWare protocols. Within STORK, national eID components are called SPWare. To integrate new countries' eIDs, two MARS-interfaces need to be implemented: (1) the Java Interface and (2) the SPWare Interface. Modules implementing the Java Interface handle incoming authentication requests of service providers (SP). These authentication requests are transformed and routed to the desired SPWare Connectors. The SPWare Connectors implement the SPWare interface and define connectors to the national MW module (SPWare). Figure 1 illustrates the SPWare Connectors to the German MW (eID Service) and the Austrian MW (MOA-ID).

Countries following the PEPS approach are also supported by this architecture. In this case the so-called C-PEPS Connector acts as SPWare Connector, which forwards an authentication request to the respective country PEPS (C-PEPS). Subsequently, the user authenticates at the according national PEPS which in turn wraps the identification and authentication data into a SAML token and returns it to the VIDP. The VIDP verifies the validity of this token and transmits the data through the respective national interface back to the requesting service provider. The modular approach does not only provide the opportunity to easily integrate other countries' authentication systems but furthermore allows the conversion and restructuring of the VIDP to an entire PEPS. This means that both models, MW and PEPS, can be implemented using this architecture. The realization can simply be achieved by utilizing and invoking the modules S-PEPS and C-PEPS Connector together.

The implementation of this architecture contains the following components:

WS Interface: This SOAP-based interface is used for receiving authentication requests of German service providers.

SP AT Interface: This interface is Web-based and supports authentication requests of Austrian service providers.

V-PEPS: Via this interface the VIDP receives STORK authentication request messages from an S-PEPS.

eID Service Connector: This connector is responsible for the communication between the VIDP and the German eID service, which constitutes the national German MW solution (SPWare).

MOA-ID Connector: This connector forwards and transforms an authentication request to the Austrian national middleware MOA-ID (SPWare).

C-PEPS Connector: The C-PEPS connector is the endpoint of the VIDP for outgoing and incoming messages to and from a C-PEPS. By the help of this connector, users originating from a PEPS country get the ability to authenticate at service providers supporting the MW model.

V. IMPLEMENTATION AND DEPLOYMENT

This chapter describes the implementation and deployment of the common middleware architecture (VIDP) and discusses scalability and security aspects. The software implementation of the MW architecture, which is based on J2EE[6] reference components and has been developed by Austria and Germany, is presented.

A. *Implementation of the MW Architecture*

This section describes the actual implementation of the STORK middleware. To guarantee high flexibility and dynamics for the implementation, EJBs[7] (Enterprise Java Beans) web services technologies had been chosen. Smooth interfaces were defined to allow flexibility for decoupling individual modules and dynamic deployment. Modules can simply be added or removed during runtime.

Figure 2 illustrates the component diagram of the implemented middleware architecture. To achieve great dynamism and flexibility the implementation has been split into three separate deployable modules: VIDP-Services, VIDP-SPWare and VIDP module.

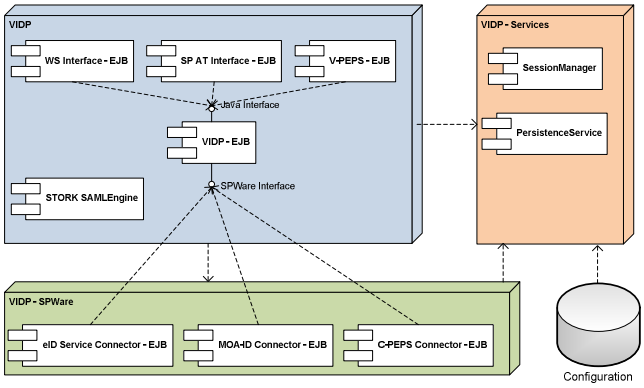

Figure 2. Component Diagram of the STORK Middleware

The VIDP-Services module is responsible for common or support tasks, e.g. managing authentication sessions or handling the communication with the external database. The database holds all required configuration information for the individual modules and components.

The VIDP-SPWare module contains the country-specific SPWare Connector components. These connectors handle the communication with the respective national MW module (SPWare) or the respective C-PEPS, if a PEPS country is involved in the authentication process. All connectors are modeled as EJBs. For configurations, the VIDP-SPWare module accesses the VIDP-Services module.

The VIDP module constitutes the main module of the MW implementation. The routing functionality is implemented in the VIDP-EJB component. The service provider specific authentication interfaces are also modeled as EJB components. The national MW connector modules (SPWare Connectors) are included in the VIDP-SPWare module and thus the VIDP only connects to them. The separate STORK SAMLEngine component handles all tasks related to the common STORK interface protocol, which is based on SAML. Again, for configurations also the VIDP module relies on the VIDP-Services module.

The middleware implementation shown in Figure 2 allows a flexible arrangement of the modules for deployment. Depending on availability of resources or other desired properties such as flexibility or maintenance efforts, different deployment strategies (Coupled or Loose Deployment) can be chosen. When choosing a coupled deployment, all VIDP modules (VIDP-Services, VIDP-SPWare, VIDP) are deployed on a common server instance. Within a loose deployment model, the VIDP modules such as VIDP-Services or VIDP-SPWare can be deployed individually as single and distributed instances. Moreover, static or dynamic extensibility of the VIDP is supported. In this context, the term dynamic means that modules (e.g. C-PEPS Connector, VIDP-SPWare) can easily be added or removed during runtime without negatively influencing the complete VIDP operation.

B. *Security*

Security plays a major role in the STORK context as well as in its framework implementations. Personal data of EU citizens are transmitted across borders, are processed, and are temporarily stored. These personal data define valuable assets, which must be particularly protected. STORK had a dedicated security team that defined security requirements and principles [14]. These have as well been implemented by the VIDP.

The interfaces between entities or components define the critical parts where impersonation or a loss of security can occur. Figure 3 illustrates the critical interfaces of the VIDP which must be especially protected.

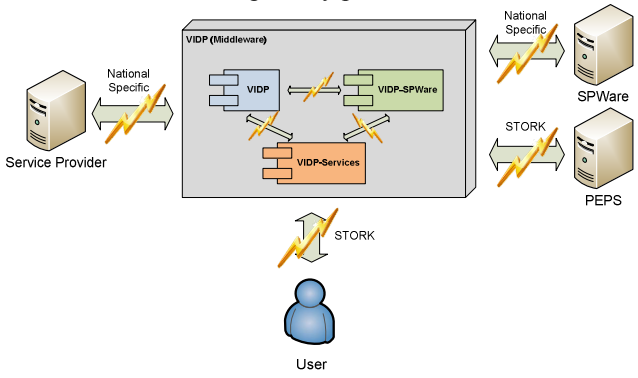

Figure 3. VIDP critical interfaces

Critical interfaces can be identified internally and externally to the VIDP. The protection of internal interfaces is especially important if a loose deployment option is preferred, where the VIDP implementation components (VIDP-Services, VIDP-SPWare, VIDP) are distributed. The

[6] http://www.oracle.com/technetwork/java/javaee/tech/index.html

[7] http://www.oracle.com/technetwork/java/index-jsp-140203.html

external interfaces must be protected in every situation where an external entity of the VIDP (e.g. Service Provider or PEPS) is involved. In other words, whenever personal data leave the VIDP and are transferred to another entity the data must appropriately be protected. In the following we describe how these external and internal interfaces were secured.

1) VIDP External Interfaces

This sub-section identifies the critical external interfaces of the VIDP and shows how the predefined security requirements of STORK were met.

SP ⇔ VIDP Interface:

Via this interface data are transferred between a national service provider and the VIDP. In the MW model, the general idea is that the VIDP is directly installed in the SP domain to enable end-to-end security between the user and the service provider. Thus, there are no further security requirements that must be fulfilled for the VIDP except for the SP itself. In fact, the VIDP can be seen as being a part of the SP. However, the SP has to ensure that the internal SP-VIDP connection is secured properly.

In case this SP-VIDP interface is externalized, the VIDP needs to support the security functions of the national specific service provider interface and its protocol. The current VIDP implementation supports national SP interfaces of Austria and Germany. The connection between an Austrian SP interface and the VIDP is secured by the use of TLS/SSL certificates. The German SP interface is Web service-based and requires a mutually secured and authenticated TLS communication channel.

VIDP ⇔ SPWare Interface:

Identification and authentication data are exchanged between the VIDP and the national MW module (SPWare) through this interface. According to the main idea of the MW model, all supported national MW modules are installed close to the VIDP within the SP domain. Hence, this interface can be assumed as SP internal interface which does not require higher protection than the SP domain itself. However, in case of externalization of this interface (as illustrated in Figure 3) the data passing through must be appropriately protected. Similar to the SP-VIDP interface, the current VIDP implementation supports connections to the Austrian and German national MW module. Both countries rely on a mutually authenticated TLS communication channel for data transfer between the VIDP and the SPWare.

VIDP ⇔ PEPS Interface:

This interface implemented by the VIDP relies on the common STORK interface specification [10] and its protocol. The common STORK protocol is used for the secure data transfer between a VIDP and a PEPS. Since this protocol bases on SAML 2.0 also all security related functionality is aligned to this well-established standard. In particular, for data transfer between STORK entities the SAML Web SSO Profile with the HTTP Post Binding is used. Thereby, all in- and outgoing messages must be properly digitally signed using the XML-DSig syntax. Digital signatures ensure message integrity, non-repudiation and authenticity. Authenticity can be guaranteed because only digital certificates issued for STORK entities are trusted.

To further improve security, the STORK specification allows to encrypt parts (especially user data) of the transmitted messages. For encrypting such parts, the XML Encryption syntax can be used. In addition, instead of the SAML Web SSO Profile the SAML Holder-of-Key (HoK) Profile [15] may be used. This profile ensures a stronger authentication and security context between the identifying and authenticating provider, the service provider, and the user's client. This higher strength is based on client's presentation of the same X.509 certificate, which results from the TLS handshake, to both providers. However, the HoK Profile is currently not widely adopted in standard components, e.g. Web browsers.

VIDP ⇔ User Interface:

Through this interface, required interactions between the user and the VIDP are handled. The user accesses this interface by a standard Web browser. To guarantee a high level of security, all connections to the VIDP are secured by the use of TLS/SSL. Users are able to verify the authenticity of the VIDP by checking the corresponding X.509 certificate.

In general, users are not required to enter any data into a Web page or form presented by the VIDP. However, all input messages or input data are validated by the VIDP against syntax, range, length, etc. to prevent e.g. cross-site scripting attacks. Additionally, during the implementation and testing phase the developers considered several Web application security issues, especially the ones presented by the OWASP [16].

2) VIDP Internal Interfaces

The VIDP internal interfaces constitute those interfaces between the three VIDP implementation components (VIDP-Services, VIDP-SPWare, VIDP). For the VIDP internal interfaces security issues only come into play if a loose deployment option for the VIDP is chosen. In this deployment option, the VIDP implementation components can be deployed remotely and distributed for achieving higher flexibility and scalability.

For implementing the VIDP the EJB technology has been chosen. This shifts application security aspects to the server implementation hosting the VIDP. This simplification holds especially for a coupled deployment of the VIDP individual components, but it cannot be relied on when applying a distributed (loose) deployment model. To achieve the same level of security independent of the deployment option, so-called security gateways were implemented protecting the remote communication between the three VIDP implementation components.

Those security gateways are modular available and are responsible and were especially designed for supporting individual security functions such as authentication and

authorization, signature or encryption services, or preventing denial-of-service (DOS) attacks. Authentication between components is based on mutual SSL/TLS authentication. For authorization between the individual components the well-known Role Based Access Control (RBAC) models and Attribute Based Access Control (ABAC) models are supported. Again, for signature and encryption functionality the XML-DSig and the XML-Enc standard had been chosen. The DOS protection security gateway only allows a maximum number of requests to a VIDP implementation component during a certain time frame. In addition to these security service gateways, gateways supporting supplementary functionality such as schema validation or message logging for auditing purposes had been implemented.

VI. CONCLUSIONS

We presented a secure identification and authentication architecture (Virtual Identity Provider – VIDP) that is based on the so-called middleware (MW) approach of STORK. This architecture supports cross-border identification and authentication of different eIDs of various EU Member States. In general, the STORK project defines two basic approaches for national eID infrastructure interoperability, the MW approach and the PEPS approach. In comparison to the PEPS model, main advantages of the MW approach are end-to-end security and liability as there is no intermediary between the user and the service provider.

The MW architecture has been developed by Austria and Germany and was implemented based on J2EE components. Thereby, emphasis lay on dynamic configurations, dynamic deployment, security, and the support of popular database and application servers. The implementation has been tested and evaluated in the six STORK pilot applications. These are productive environments, such as national eGovernment portal or the STORK Safer Chat pilot [17].

STORK was a success, as cross-border acceptance of national eIDs could be successfully demonstrated in real environments. However, while STORK showed that cross-border eID interoperability is technically feasible, some hindering issues still remain open for future investigations. Issues on organizational level are for example the mapping of personal identifiers from national registers between countries. Another issue is harmonization of legislation as e.g. eID registration procedures vary between countries. Furthermore, in terms of acceptance of individual credentials for authentication still some work needs to be done. For instance, to qualitatively ensure the authentication levels proposed by STORK some independent auditing and validation procedures would be required. [17]

Nevertheless, the STORK results on cross-border eID for natural persons are taken up by a follow-up project STORK 2.0 [8] that further elaborates on mandates and representation, such as representing a legal person. The lessons learned, in particular that technology is not the hindering factor of cross-border eID, but the lacking trust framework such as lacking mutual recognition, influenced ongoing European policy measures. The main is a proposed European Community legal framework for eID [1]. Furthermore, the gained experience of developing STORK could also have implications for other evolving efforts such as NSTIC.

[8] http://www.eid-stork2.eu

REFERENCES

[1] European Commission: Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, COM(2012) 238/2.

[2] European Union: Ministerial Declaration, Manchester, United Kingdom, on 24 November 2005

[3] European Commission: Ministerial Declaration on eGovern-ment approved unanimously, Malmö, 18 November 2009

[4] European Union: Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market

[5] European Commission - IDABC. 2009. eID Interoperability for PEGS: Update of Country Profiles.

[6] Neuman, C., Yu, T., Hartman, S. and Raeburn, K. 2005. "The Kerberos Network Authentication Service (V5)". RFC 4120. Internet Engineering Task Force (IETF)

[7] Lockhart, H. and Campbell, B. 2008. "Security Assertion Markup Language (SAML) V2.0 Technical Overview". OASIS Committee

[8] Kaler, C. and McIntosh, M. 2009. "Web Services Federation Language (WS-Federation) Version 1.2". OASIS Standard.

[9] The White House. 2011. National Strategy for Trusted Identities in Cyberspace (NSTIC)

[10] Alcalde-Morano, J., Hernández-Ardieta, J.L., Johnston, A., Martinez, D., Zwattendorfer, B., and Stern, M. 2011. "D5.8.3b Interface Specification". STORK Deliverable

[11] H. Leitold and B. Zwattendorfer, "STORK: Architecture, Implementation and Pilots". in ISSE 2010, pp. 131-142. 2010.

[12] Leitold, H., Hollosi, A., and Posch, R. 2002. "Security Architecture of the Austrian Citizen Card Concept". In Proceedings of the 18th Annual Computer Security Applications Conference (2002)

[13] Ferderal Office for Information Security (BSI). 2009. eCard-API-Framework (BSI TR-03112)

[14] Stern, M. 2011. "D5.8.3d Security Principles and Best Practices". STORK Deliverable

[15] Lockhart, H. and Hardjono, D. 2010. "SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0". OASIS Committee Specification 02.

[16] The Open Web Application Security Project (OWASP). 2010. "OWASP Top 10 - 2010 - The Ten Most Critical Web Application Security Risks".

[17] Knall, T., Tauber, A., Zefferer, T., Zwattendorfer, B., Axfjord, A., Bjarnason, H.: "Secure and Privacy-preserving Cross-border Authentication: the STORK Pilot "SaferChat"". In Proceedings of the Conference on Electronic Government and the Information Systems Perspective (EGOVIS 2011), pp. 94-106

[18] Koulolias, V., Kountzeris, A., Leitold, H., Zwattendorfer, B., Crespo, A., Stern, M. , "STORK e-privacy and security," In 5th Internationl Conference on Network and System Security (NSS) 2011, pp.234-238