Herbert Leitold, Bernd Zwattendorfer - "STORK: Architecture, Implementation and Pilots" - ISSE 2010 Securing Electronic Business Processes, 2010, pp.131-142
URL: http://link.springer.com/chapter/10.1007%2F978-3-8348-9788-6_13
The original publication is available at www.springerlink.com

STORK: Architecture, Implementation and Pilots

Herbert Leitold[1] · Bernd Zwattendorfer[2]

[1] Secure Information Technology Center - Austria, A-SIT
Herbert.Leitold@a-sit.at

[2] Graz University of Technology, E-Government Innovation Center, EGIZ
Bernd.Zwattendorfer@egiz.v.at

Abstract

Who one is on the Internet turns out essential once sensitive information is exchanged or transactions of value are carried out. Electronic identification and identity management provide the solutions. Governments are important players in the area, having a tradition of providing qualified means of identification of their citizens. However, migration to electronic identities often developed as national islands that are based on one country's domestic legal, administrative and socio-cultural tradition. Once the citizens are crossing borders electronically, these islands need to get connected and interoperability becomes an issue.

The project STORK is an EU Large Scale Pilot driven by 17 EU/EEA Member States and the European Commission. The project promises to bridge national eID islands by developing and testing common specifications for electronic identity interoperability. Taking the existing national infrastructures as a basis, models have been developed for the cross-border interoperability framework. The framework is tested in six real-world pilot applications.

This paper describes the project STORK. It discusses the interoperability models that have been developed. These are the "proxy model" that introduces national identity gateways and the "middleware model" that is limited to a client to service provider relationship. Rationales for selecting a particular model are given and the principle architecture of STORK is discussed.

1 Introduction

Electronic identity (eID) is understood as key-enabler for a variety of services on the Internet. Once the identity of communicating entities is established with a level of certainty matching the value associated with the service, the communication partners can gain the confidence and trust needed for concluding the transaction. Such transactions can range from social networks to get in touch with friends, to buying a book at an online shop, to have a look at one's stock deposit and to trade a few shares, to file a tax declaration, or to access one's medical data in an electronic health record. In each case authentication is involved, i.e. claiming an identity and proving it true. As the examples also show, value associated with a transaction can be pecuniary in case of e-commerce, legal duties in case of e-government, or can touch fundamental data protection questions when in e-health sensitive data is involved.

The more we get active on the Internet and the more value transactions get carried out, the higher the importance of high levels of assurance by secure means of authentication linked to qualified identities gets. E-government is such an area where high assurance in the citizen's

identity may be needed. Several states therefore as early as in the late 1990's started to plan and to develop electronic identity systems and beginning of the 2000's started to deploy them.

Examples of early developments are the Austrian Citizen Card, the Belgian BelPIC, the Estonian eID card, the Italian CIE and CNS cards, or the Finnish FineiD. Other countries followed with mass roll-outs such as Portugal and Spain. A study that has been carried out by the European Commission under IDABC and that recently has been amended shows that that 13 out of 32 surveyed countries issue eID cards – as the smartcard examples just given [GrMM09]. Other countries provide eID via authentication portals using username passwords such as the UK Government Gateway or DigiD (that may be complemented with SMS transaction codes) in The Netherlands. Further countries rely on PKI software certificates and/or base their eID on banking authentication systems such as the Swedish BankID. Some deploy mobile solutions as in Austria and Estonia and several countries have combinations of these methods.

Given this diversity of technologies and given that solutions that have been deployed about a decade ago and are still in operation it is not too hard to guess that interoperability is a concern. Solutions evolved in their national environment under its legal and administrative constraints, thus carrying national specifics. The EU recognised early that this can hamper the Common Market in an Information Society. In 2005 the Manchester Ministerial Declaration gave a political message by stating that "*By 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations. Such means shall be made available under the responsibility of the Member States but recognised across the EU*" [Manc05].

Note, that the Manchester Declaration does not put technology in its epicentre, but emphasises user convenience, security, and data protection and points to the need of mutual recognition. Cross-border eID interoperability is a complex and multi-disciplinary issue covering legal, operational and technical aspects. A vehicle to clear the bar of the Manchester Declaration and to get hands-on experience with the issues involved is to test concepts in real world applications on a large-enough scale. This has been initiated by the European Commission by co-funding an eID Large Scale Pilot under the Competitiveness and Innovations Framework Programme, ICT Policy Support Programme (CIP, ICT-PSP). STORK – which stands for *S*ecure identi*T*y acr*O*ss bo*R*ders lin*K*ed – is the eID Large Scale Pilot that origins from this initiative.

STORK is introduced in the remainder of this paper. In section 2 the project objectives are discussed. These are to develop common specifications for an interoperability framework and – as the prime objective – to test its implementation in six concrete cross-border applications. These pilot applications are also briefly described in this section. Section 3 sketches the legal and operational aspects that had to be tackled. In the main part of the paper – section 4 – the interoperability models that have been developed are described. These are the "proxy model", the "middleware model", and its combinations. The architecture of STORK is described in section 5 and, finally, conclusions are drawn.

2 Goals of STORK

STORK brought together fourteen EU/EEA Member States in 2008 which then has been enhanced by three further Member States in 2010[1]. The aim of the consortium has been to take

[1] Austria, Belgium, Estonia, France, Germany, Iceland, Italy, Luxemburg, Portugal, Slovenia, Spain, Sweden, The Netherlands, and United Kingdom; later extended by Finland, Lithuania, Norway, and Slovak Republic.

their national eID systems as a basis and to develop and build an interoperability framework on top of it. The underlying assumption of STORK is that the national electronic identity systems remain unchanged – note the huge investments that would be at stake if an infrastructure rolled out nation-wide and integrated in many of service providers would need to be changed.

In a three year journey, the goals of STORK are to get clarity on how the legal and operational issues (discussed in the next section 3) can be addressed. This comprised the first phase of the project. A major goal was to develop the technical specifications to enable cross-border interoperability (discussed in section 4) and to implement these (section 5). This phase covered the second project year.

The proof of the pudding is in its eating. The main and final phase of the STORK project is to deploy its interoperability framework to six real-world applications. This phase shall establish the lessons learned, to see where the concepts are successful, or where we might got stuck, respectively. The pilots shall run for one year in the period from mid 2010 to mid 2011. The six pilots are:

1. The first pilot *Cross-Border Authentication Platform for Electronic Services* aims at integrating the STORK framework to e-government portals, thus allowing citizens to authenticate using their electronic eID. The portals can range from sector-specific portals such as the Belgian “Limosa” application for migrant workers to regional portals serving various sectors such as the Baden-Württemberg “service-bw” portal or national portals as the Austrian “myhelp.gv” for personalised e-government services.
2. In the *Safer Chat* pilot juveniles shall communicate between themselves safely. The pilot will be carried out between several schools. The specific requirement is that in the authentication process the age group delivered by the eID is evaluated to grant access. Unique identification that is the basis of the other pilots is less important.
3. *Student Mobility* supports exchange of university students, e.g. under the Erasmus exchange program. As many universities nowadays have electronic campus management systems giving services to their students, STORK shall be used to allow foreign students to enrol from abroad using their eID and to access the campus management system’s services during their stay, respectively. The prime requirement is authentication, as in the first pilot on cross-border authentication.
4. The fourth pilot *Electronic Delivery* objective is cross-border qualified delivery, replacing registered letters. On the one hand, delivering cross-border requires protocol conversions between the national delivery standards. On the other hand, qualified delivery usually asks for signed proof of receipts. The latter – signed proof of receipts – is the specific requirement in this pilot. This enables cross-border tests of signature-functions that most smart-card based eIDs have.
5. To facilitate moving house across borders, the pilot *Change of Address* has been defined. In addition to authentication, the pilot has transfer of attributes, i.e. the address, as a requirement.
6. The *European Commission Authentication Service* (ECAS) is an authentication platform that serves an ecosystem of applications that are operated by the European Commission. Member States use these services to communicate among themselves and with the European Commission. Piloting administration-to-administration (A2A) services with national eIDs is an STORK objective. The pilot A2A Services and ECAS integration serves this objective by linking up STORK to ECAS.

3 Legal and operational aspects

An initial activity of STORK was taking stocks of the legal and operational eID environment. Major findings can be summarised by three categories: Firstly, the use of national identifiers. Secondly, data protection and legitimacy of cross-border processing of electronic identity and, finally, the security and assurance levels associated with eID tokens. These three aspects are summarised in this section.

Personal identifiers are the basis of identity management. Some countries use unique citizen identifiers across sectors, such as citizen register numbers in Belgium or Estonia or the tax number (codici fiscale) in Italy. Austria derives sector-specific identifiers from a unique source taken from the residents register. Germany uses service-provider-specific identifiers, unique identifiers are however not provided, as it would be unconstitutional to have such persistent citizen identification. Regulations on the use of national identifiers exist in most countries and restrict their use. These restrictions can lead to situations where using the identifiers is only possible in the country of origin, cross-border use is prohibited in several cases. A solution proposed by STORK is to apply one-way functions to the base identifiers and thus to derive identifiers that can be used abroad. Whether such a scheme is used is on the discretion of the country: In STORK e.g. Austria and Belgium apply a cryptographic transformation of national identifiers.

Data protection is key to enable cross-border eID. The EU Data Protection Directive – and thus national laws implementing it – gives several options to make processing of personal data legitimate. These include situations where the processing is necessary to perform a contract to which the data subjects is party, or where the processing is necessary to perform a legal obligation of the data controller. The legal analysis by STORK however argued it unlikely that such situations exist in all situations STORK aims to cover. Therefore, STORK relies on consent of the citizen as the basis for legitimacy of the data processing. Personal data that are to be transferred as well as the receiver of these data are shown to the user. The user has to give explicit consent prior to personal data being communicated.

The national eIDs in STORK can range from username-password schemes, via software certificates to smart cards and qualified certificates. To categorise these, STORK has developed a Quality Authenticator Assurance (QAA) consisting of four levels. These levels range from low assurance (QAA level 1) to high assurance (QAA level 4), the latter e.g. given with qualified certificates. The idea followed is that the Service Provider requests a certain QAA level needed for the particular service. Service is granted, if the citizen's eID token matches or exceeds the requested level.

4 Interoperability Framework

The project is based on two lines of thoughts on how an interoperability framework can be build: (1) In the first approach, the service provider integrates all foreign eID tokens using a middleware. We refer to this approach as "*middleware model*". (2) In the second approach, cross-border eID transactions are delegated to a national gateway – a proxy – that hides the specifics of national eID tokens and infrastructure from other countries. We refer to this as "*proxy model*".

The advantage of the middleware model is that a clear user-to-service provider relationship is given from a data protection and from a liability perspective: No intermediaries are involved that liability might be shifted to, or that the personal data is transferred to. End-to-end security

between the citizen domain and the service provider domain can be technically granted, as the middleware can make use of the eID token's security functions. A drawback however is that maintaining the middleware needs support of the eID issuers, as each eID needs to be integrated and modifications are needed once generations change or new token types get into use. Such changes in the middleware need to be rolled out to service providers.

The advantage of the proxy model is that the proxy serves just its national eID tokens and its national service providers. In the cross-border case the communication is leveraged to a common proxy-to-proxy protocol. This advantage however comes with a situation where the proxy steps into the citizen to service provider relationship. This can lead to a liability shift. From a data protection perspective, the proxy becomes a data processor or data controller. The trust-relationship is established between two proxies, and between a proxy and an end-entity (citizen or service provider). Thus, an entity asserts a fact (such as the authentication of a citizen) towards its direct neighbour (e.g., one proxy to another proxy, but in that case not to the end entity). This leads to point-to-point trust relationships asking for properly securing the intermediaries, as a compromised proxy might intercept data or impersonate users.

The following sub-sections discuss the two models and its combinations in detail.

4.1 Conceptual Models

The national eID solutions deployed in their domestic infrastructure, such as citizen cards or central authentication portals, are based on different models or frameworks. This sub-section bases on the general interoperability concepts discussed above and describes the two models Pan-European Proxy Service (PEPS) and Middleware (MW) in a cross-border context. This also builds the basis for interoperability within the STORK architecture. [EJL+10]

4.1.1 PEPS Model

The PEPS bundles several services required for a cross-border eID solution and hides the complexity and specifics of national solutions form other countries. The services provided by a PEPS include the identification and authentication at identity providers, the additional retrieval of identity attributes, or the secure transfer of the identity information to service providers (SP) [MaGr07]. **Fig. 1** illustrates the PEPS Model in a logical view.

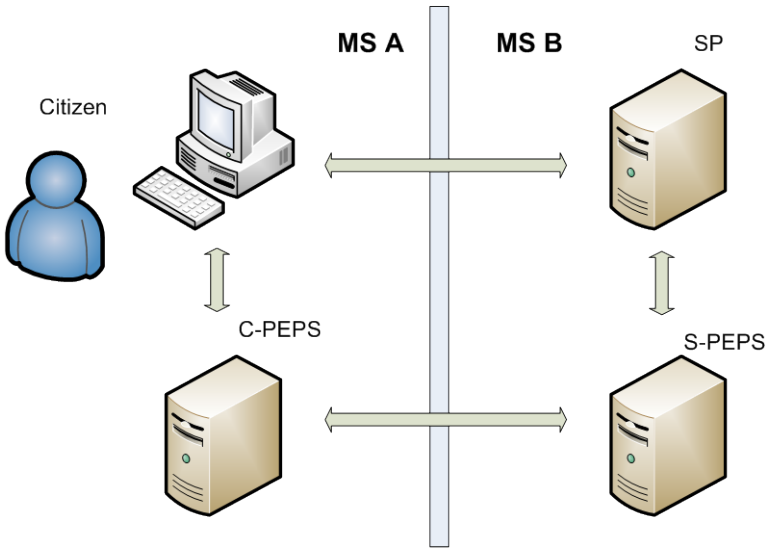

Fig. 1: PEPS Model

In the scenario shown in the figure, MS A as well as MS B host its own PEPS server. The PEPS server defines a central and single[2] instance responsible for the communication with identity providers and attribute providers and for the transfer of identity information across borders. Additionally, a connection and trust relationship between the PEPS and its own country service providers exists. In this model the PEPS asserts the SP that a citizen presenting the requested identity information has been successfully authenticated at a needed authentication level. Since there are several parties involved where data can be transformed, trust relationships and security are established on a point-to-point basis.

A PEPS can act as so-called S-PEPS (PEPS in the Service Provider's country) or C-PEPS (PEPS in the citizen's origin country). The S-PEPS communicates with the SP requesting authentication and the C-PEPS, thus acting as intermediary between SP and C-PEPS. The C-PEPS retrieves requests from a calling S-PEPS and triggers the identification and authentication for a citizen at an identity and/or attribute provider.

4.1.2 MW model

In the MW (Middleware) model a citizen directly authenticates at a service provider. The citizen remains the owner of the data and the service provider is the data controller. Identity data is usually stored on a secure token, e.g. smart cards, and will only be released if the user gives his consent to do so, e.g. by entering a PIN. No intermediary is in the path between the citizen and the service provider. **Fig. 2** illustrates the MW model.

[2] Considering scalability, the load of this instance can be shared and balanced among a couple servers.

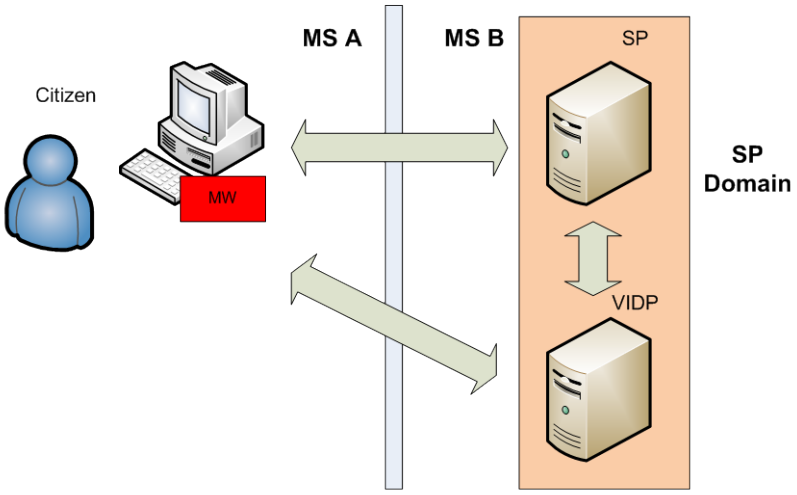

Fig. 2: MW Model

The MW model consists of two pieces of software, one running on the user's PC (referred to as client-middleware) and one running on the service provider's system (server-side middleware – referred to as virtual identity provider VIDP). Generally, the client-middleware handles the communication with the secure token and the server-side middleware. The server-side middleware is responsible for transmitting the identity information retrieved from the token to the SP application. The MW model can ensure end-to-end security.

4.2 Interoperability Scenarios

The conceptual interoperability model of the STORK project combines the PEPS and the MW model. The aim of STORK has been the design and development of a common architecture and framework to enable citizens' of PEPS and MW countries secure cross-border authentication. The Security Assertion Markup Language [SAML] has been chosen for transferring eID and authentication data between the models. The message exchange format has been specified in Deliverable D5.8.1b [ALJ+09]. By combining both models, four different cross-border scenarios can be distinguished that are discussed in the following subsections.

4.2.1 PEPS – PEPS Scenario

In this scenario, a citizen from a PEPS country wants to authenticate at a service provider in another PEPS country. The SP delegates the authentication process to its S-PEPS which in turn forwards the request to the citizen's origin C-PEPS. The C-PEPS triggers the actual authentication process with the user by invoking the appropriate identity and attribute provider. If authentication was successful, the C-PEPS assembles a so-called SAML assertion containing the requested identity data, wraps it into a SAML Response message and returns it to the S-PEPS. The S-PEPS verifies the assertion and forwards the citizen to the SP that grants or denies access to the requested resource. Following the point-to-point trust relationship, the messages are validated at each receiver, re-signed and forwarded to the next hop.

4.2.2 PEPS – MW Scenario

In this interoperability scenario a citizen from a MW country wants to use services from a SP located in a PEPS country. The first steps (SP forwarding the request to the S-PEPS) are equal to the scenario above. However, instead of transferring the request to the C-PEPS the citizen is redirected to the so-called virtual identity provider (VIDP) which is installed in the S-PEPS

domain and which manages the MW authentication. Depending on the citizen's home country, the VIDP delegates the authentication process to the national server-side middleware. After successful authentication, the VIDP assembles a SAML Response according to the common STORK format and transfers it to the requesting S-PEPS. Again, the S-PEPS forwards the response information to the SP. The end-to-end security assumption of the MW model terminates at the VIDP as if it was a service provider in the pure middleware model. The VIDP to S-PEPS and the S-PEPS to SP communication follow a point-to-point trust relationship.

4.2.3 MW – MW Scenario

A citizen from a MW country wants to authenticate at a SP located in another MW country. In this case, the VIDP is directly located in the SP domain. As in the previous scenario, the VIDP calls the appropriate server-side middleware for actual citizen authentication. As in the two other scenarios, the VIDP assembles an SAML Response message to be returned to the SP.

4.2.4 MW – PEPS Scenario

In the last of the four combinations a citizen from a PEPS country wants to authenticate at a SP in a MW country. The VIDP in the SP domain assembles an appropriate STORK request and transmits the authentication request to the C-PEPS of the citizen's country. Equal to the PEPS-PEPS scenario, the C-PEPS invokes the identity and attribute provider. Having successfully authenticated the citizen, the C-PEPS returns the response containing the authentication data to the requesting VIDP. The VIDP verifies the response message and redirects the user back to the SP.

5 Implementation Architecture

Besides the design of a conceptual architecture another aim of the STORK project's common specifications has been the implementation of the interoperability framework. The implemented components are used in the pilots acting as enabler for cross-border identification and authentication.

5.1 PEPS Architecture

Fig. 3 illustrates the basic architecture of a PEPS server, including the functionality for authentication (*AuthenticationPEPS*) and validation (*ValidationPEPS*).

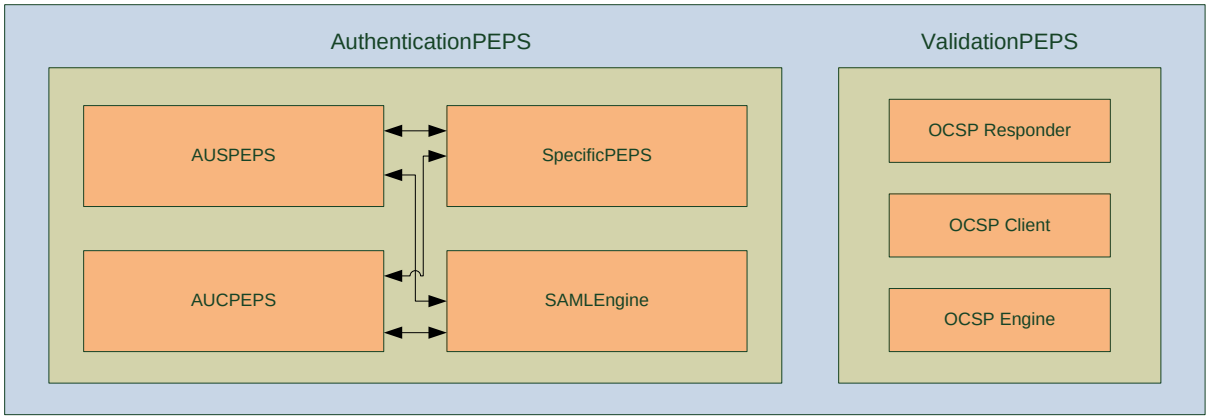

Fig. 3: PEPS Architecture

Both functionalities, S-PEPS and C-PEPS, are implemented in the same component. That means, a PEPS can either act as S-PEPS or C-PEPS or can support both functionalities. Details on the PEPS architecture can be found in Deliverable D5.8.1c of the STORK project [BAL+09].

5.1.1 Authentication PEPS

The *AuthenticationPEPS* consists of four main components – the *AUSPEPS*, the *AUSCPEPS*, the *SpecificPEPS*, and the *SAMLEngine*.

The *AUSPEPS* Component manages the authentication process between a SP and a S-PEPS. Authentication requests from a service provider are received at this component whereas authentication responses are returned to the calling SP.

The *AUCPEPS* component reflects the inbound functionality of a C-PEPS. Authentication request messages sent from a S-PEPS are received and handled by this component. Furthermore, responses containing either citizen's identity and authentication data or an error message are returned to the requesting S-PEPS.

The *SpecificPEPS* component covers country specific functionality and must be implemented by each PEPS country. The Specific PEPS component is in charge of communicating with national identity providers and attribute providers and the translation of the identity information and national protocol into the common STORK format.

The *SAMLEngine* component encapsulates all SAML related functionality necessary for STORK processing. This engine supports methods for the generation and validation of SAML AuthnRequest and SAML Response messages as well as methods for digitally signing or verifying them.

5.1.2 Validation PEPS

The *ValidationPEPS* implements the business logic for digital certificate validation. The main sub-components include an online certificate status protocol (OCSP) engine as well as an OCSP client and responder. The *OCSP responder* is in charge of handling OCSP requests either sent from a SP or a partner PEPS. Additionally, the responder generates OCSP responses to be returned to the requesting entity. The *OCSP Client* component is responsible for generating OCSP requests for certificate validation to be sent to a partner PEPS. Similar to the

SAMLEngine component the *OCSP Engine* implements methods for the generation and processing of OCSP request and response messages.

5.2 MW Architecture

The general idea behind common middleware architecture is the use of various different middleware approaches through a consistent interface. On lower level, an example for such an interface would be the eCARD-API developed by the German BSI [BSI09] and used with the German electronic ID card. The aim of this API is the provision of a unique interface for applications to use card-based services without needing specific and detailed knowledge about the various smart cards.

The MW architecture developed within STORK tracks the same aim but on a higher level. **Fig. 4** illustrates this modular architecture.

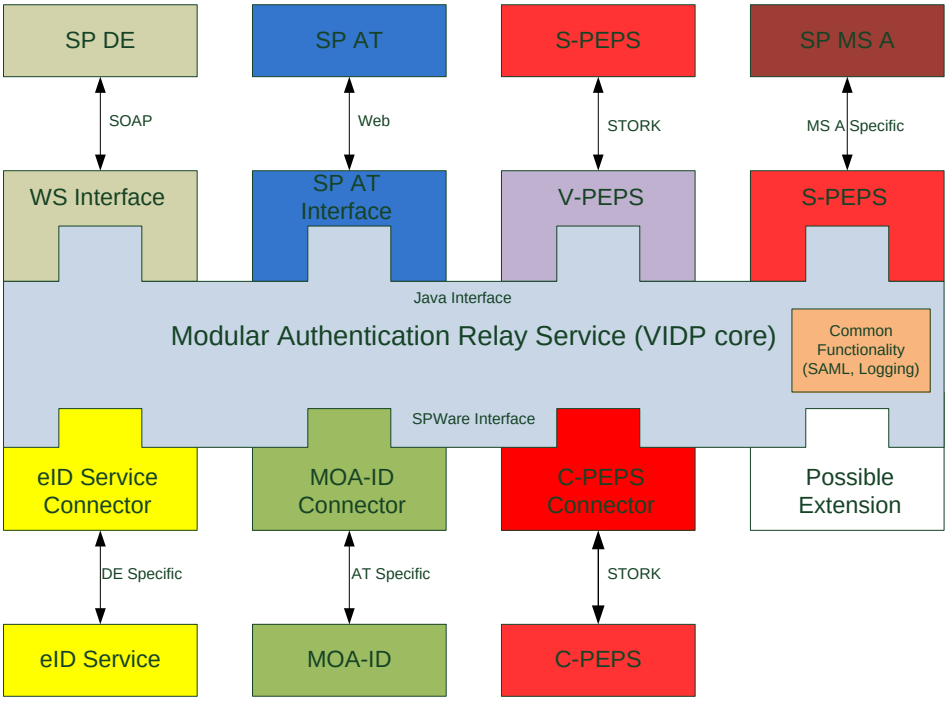

Fig. 4: MW Architecture "MARS"

The VIDP core – Modular Authentication Relay Service (MARS) – provides common functionality such as logging, configuration or SAML message generation. The components on the top of the VIDP core define so-called "Plug-Ons". They are responsible for mapping various authentication requests from service providers or S-PEPSs from different countries to a common Java interface. The Plug-Ons can either be Web Service-based (SOAP) or a Web server component. The components shown at the bottom of the VIDP core are so-called "Plug-Ins" that process the connection to different national server-side middleware components or to a C-PEPS in case MW-PEPS authentication is desired.

The current implementation of this architecture provides the following components:

- WS Interface: This interface is used by German service providers and is SOAP-based.
- SP AT interface: Web interface for supporting Austrian legacy service providers.

- V-PEPS: This component receives SAML AuthnRequest messages from a S-PEPS and forwards the message to the VIDP.
- eIDService Connector: This Plug-In handles the communication with the German eID service.
- MOA-ID Connector: This connector delegates an authentication request to the Austrian server-side middleware MOA-ID.
- C-PEPS Connector: With this module citizens of PEPS countries can be authenticated at service providers relying on a MW model.

The modular design of this architecture also allows the realization of an S-PEPS or C-PEPS. For this, the Plug-On covering the S-PEPS functionality must be implemented. Details on the MW architecture can be found in Deliverable D5.8.1a [BJA+09].

6 Conclusion

STORK is a Large Scale Pilot aiming at cross-border interoperability of eID. The basic assumption is to build a technological infrastructure on top of existing national eID infrastructure. Two models are followed by countries in STORK – proxy and middleware. The decision of which model to follow depends on the country. It may be based on weighing liability, scalability, data protection and end-to-end security considerations.

The technical infrastructure has been developed and deployed to six pilot applications. At time of writing this paper, the pilots just launched. Thus, no lessons learned can be derived at this early stage. What is known is that pilots operate proving the technology feasible. The main issue to be tackled for a sustainable cross-border eID ecosystem is mutual recognition. This is in particular the case if no community basis for mutual recognition can be relied on, such as the Signature Directive for the recognition of qualified certificates.

Actually, STORK is not the end of a journey, rather a first leap: By demonstrating core elements of the Manchester Declaration [Manc05] STORK has contributed to this challenging objective. The lessons learned from STORK and its pilots can serve as valuable basis for Key Action 16 of the Digital Agenda where the Commission aims to *"propose by 2012 a Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector)"* [Comm10].

References

[ALJ+09] Alcalde-Morano, Joaquín; López Hernández-Ardieta, Jorge; Johnston, Adrian; Martinez, Daniel; Zwattendorfer, Bernd; Stern, Marc: D5.8.1b Interface Specification, STORK Deliverable, 2009

[BAL+09] Berbecaru, Diana; Alcalde-Morano, Joaquín; López Hernández-Ardieta, Jorge; Portela, Renato; Ferreira, Ricardo: D5.8.1c Software Design. STORK Deliverable, 2009

[BJA+09] Berbecaru, Diana; Jorquera, Eva; Alcalde-Morano, Joaquín; Portela, Renato; Bauer, Wolfgang; Zwattendorfer, Bernd; Eichholz, Jan; Schneider, Tim: D5.8.1a Software Architecture Design. STORK Deliverable, 2009

[BSI09] Bundesamt für Sicherheit in der Informationstechnik (BSI): Das eCard-API-Framework (BSI TR-03112), 2009

[Comm10] European Commission: A Digital Agenda for Europe, COM(2010) 245, 2010

[EJL+10] Eichholz, Jan; Johnston, Adrian; Leitold, Herbert; Stern, Marc; Heppe, John: D5.1 Evaluation and assessment of existing reference models and common specs, STORK Deliverable, 2010

[GrMM09] Graux Hans, Majava Jarkko, Meyvis Eric: Analysis & assessment report. In: Study on eID Interoperability for PEGS: Update of Country Profiles. IDABC European eGovernment Services, European Commission, 2009

[MaGr07] Majava, Jarkko; Graux, Hans: Common specifications for eID interoperability in the eGovernment context. In: eID Interoperability for PEGS. Editor: IDABC European eGovernment Services, European Commission, 2007, p. 25.

[Manc05] Ministerial Declaration approved unanimously on 24 November 2005, Manchester, United Kingdom Presidency of the EU, 2005

[SAML] Security Assertion Markup Language (SAML), OASIS Security Services (SAML) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Index

Electronic identity, eID, STORK