Digital Enlightenment Yearbook 2012
J. Bus et al. (Eds.)
IOS Press, 2012

doi:10.3233/978-1-61499-057-4-289

STORK - Technical Approach and Privacy

Herbert LEITOLD[a,1] and Reinhard POSCH[b]
[a]*A-SIT, Secure Information Technology Center, Austria*
[b]*Federal CIO, Federal Chancellery, Austria*

Abstract. In this paper we describe the STORK Large Scale Pilot (LSP). STORK has been a project driven by eighteen European Union (EU) and European Economic Area (EEA) Member States (MS). The objective was to develop an interoperability framework to enable cross-border use of national electronic identity (eID) solutions. The framework has been tested in six pilots that involved MS and European Commission production environments. The paper describes the technical STORK solution that supports eID federation both in centralized and in decentralized deployment models. We refer to these as Pan-European Proxy Service (PEPS) for centralized deployment, as middleware (MW) for the decentralized deployment, respectively. The paper puts particular attention to security and privacy aspects.

Keywords. electronic identity, identity federation, eID interoperability

Introduction

Who one is on the Internet and its corroboration becomes important, once valuable or sensitive information gets exchanged. We refer to an electronic representation of the “who one is” as electronic identity (eID). The corroboration of a claimed identity is referred to as authentication or entity authentication.

For traditional face-to-face situations, governments provide means that offer high assurance into the claimant’s identity. Examples of such means are identity cards, driving licenses, or passports. We regularly use these in public administration to provide evidence of our identity, but also in private sector services such as when opening a bank account. Even state borders are no barrier, as state-issued identity documents get recognized when renting a car, boarding a plane, or verifying the holder of a credit card.

With the advent of the Internet, governments started in the late 1990s to issue electronic complements to traditional identity documents. The purpose was to offer secure means of entity authentication in e-government or in e-commerce. Some countries amended existing identity cards by a smart card. Examples are BELPIC in Belgium, ID KAART in Estonia, or “neuer Personalausweis” in Germany. Other states reuse e-authentication infrastructure existing in the private sector. An example is BankID in Sweden where a citizen’s Internet banking credential can be used as eID for e-government services. Further states use both public sector borne and private sector borne credentials as national eID. An example of this is the Austrian citizen card concept that inter alia embraces private sector issued bank cards and mobile phones, as

[1] Corresponding Author: Herbert Leitold, Secure Information Technology Center A-SIT, Inffeldgasse 16a, A-8010 Graz, Austria. Herbert.Leitold@a-sit.at

well as state-issued cards such as health insurance cards or public servants' service cards. For an overview of the various solutions in the EU and beyond we refer to the European Commission study on eID Interoperability for Pan-European Government Services (PEGS) [1].

When comparing traditional identity documents with eID, two observations can be made: First, for eID the frequency of use is in many cases still in ramp-up phases mainly attracting early adopters or those which have frequent government contacts within certain sectors or professions. Most national eID initiatives have not yet reached mass day to day usage by large portions of its citizens. Note however, that the day to day use of traditional ID cards is as infrequent. A second observation is that national eID to a large extent have evolved as national silos. Cross-border recognition has rarely been considered when designing the systems.[2] As eID is an enabler of services in particular from home or from distance, national silos create the risk of hindering a European digital market. A decade of experience made with eID deployment by those MS that started early, together with a situation that national silos haven't yet hardened with broad mass usage, leaves the window of opportunity open to advance to pan-European eID use.

Europe has recognized early that seamless use of eID across borders has to be addressed. The Manchester Ministerial Declaration [2] already in 2005 asked 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*". This has been further emphasized in 2010 by the Digital Agenda for Europe [3] that defined two Key Actions on a Community legal basis for cross-border recognition of eID and eAuthentication. The two Key Actions are Key Action 3 "*In 2011 propose a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems;*" and Key Action 16 "*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);*". Note, that the Manchester Ministerial Declaration gave particular attention to data protection and that the Digital Agenda for Europe keeps eID open for being issued by either the public sector or the private sector.

Both the Manchester Ministerial Declaration and the Digital Agenda for Europe recognize the states' responsibility in issuance of eID. The purpose is not to harmonize, but to respect national responsibility and sovereignty and to preserve the investment in national infrastructure. Thus, interoperability between existing systems is to be achieved that, given short technology cycles, also is robust and resilient enough to be enhanced by future solutions.

Given that national eID systems are already heterogeneous in various dimensions – the technological[3], the operational[4], and the legal[5] dimension – it is advisable to first

[2] To the authors' best knowledge, the only country that included recognition of foreign eID in both the legal environment and the technical and organizational eID infrastructure from the beginning is Austria.

[3] Some states rely on smartcards, e.g. Belgium or Germany. Others use username-password with (optional) SMS authentication, e.g. the DigID system in the Netherlands. Further MS use various technologies in parallel, such as Austria and Estonia where smartcard and mobile phone eID can be chosen.

test promising solutions in production environments. This shall scrutinize approaches in practice and to see whether and where one gets stuck when leveraging eID service to a cross-border context. Such piloting in large scale production environments has been stimulated by the European Commission by co-funding so-called Large Scale Pilots (LSPs) under the Competitiveness and Innovation Framework Programme (CIP), Information and Communication Technology Policy Support Programme (ICT-PSP).

The LSP piloting cross-border eID is Secure idenTities acrOss boRders linKed (STORK)[6]. The project and its results are described in the remainder of this paper. Therefore, section 1 gives an overview of the project and discusses the six pilots that did validate the interoperability solution. In section 2 the conceptual basis of results are sketched. This consists of a so-called Quality Authentication Assurance (QAA) model and the conceptual interoperability model. The latter comprises centralized deployment, decentralized deployment, and its combination. Section 3 continues by discussing the main outcome of STORK. These are common specification and its reference implementation as open source software. The important aspects of information security and privacy are discussed in section 4. The two interoperability models PEPS and MW are compared and advantages and challenges resulting from the specifics of each model are explained. The section also discusses the outcome of a consultation done with the Article 29 Data Protection Working Party. This initiative discussed the STORK data protection measures with the European Data Protection Authorities. Finally, conclusions are given.

1. STORK Overview and its Pilots

The STORK project started in May 2008 with an original duration of three years[7]. As a so-called "pilot A" it had been driven by EU Member States (MS). The project started with 14 EU and EEA states[8] and an overall budget of € 20 million. In 2010 an extension by four further MS[9] and to a budget of € 26 million took place. Under the CIP ICT-PSP co-funding regime, 50 % of the project costs have been co-funded by the European Commission, 50 % is borne by the project partners.

The overall idea was to define a framework that does not change the existing national eID infrastructure, but does define an eID interoperability layer on top of the national systems that supports cross-border use.

In a nutshell, the project has been structured in three phases:

[4] For instance, eID can be issued on the federal level, e.g. in Belgium or Portugal with national ID cards. Other countries may have eID issued either on the state or on the regional level. An example is Italy where the Carta d'identità elettronica (CIE) is issued by the Ministry of Interior, Carta Nazionale dei Servizi (CNS) is issued by the regions. Other states rely on private sector issuance such as BankID in Sweden.

[5] Examples of legal differences are restriction on national identifiers: Whereas some states such as Spain allow using identifiers across sectors, others like Austria use sector-specific identifiers. While many states rely on life-long persistent identifiers, that is e.g. considered unconstitutional in Germany. Other legal differences are that in some states an activated eID is issued to each citizen, such as in Belgium or Estonia; in other states such as Austria activation of eID is voluntary and at the discretion of the citizen.

[6] STORK is an EU co-funded project under contract INFSO-ICT-PSP-224993

[7] The project has later been extended from 36 months duration to 43 months, i.e. until end of 2011.

[8] The 14 states that started in 2008 have been Austria, Belgium, Estonia, France, Germany, Iceland, Italy, Luxemburg, Portugal, Slovenia, Spain, Sweden, The Netherlands, and United Kingdom.

[9] The extension in 2010 included Finland, Greece, Lithuania, and Slovak Republic.

- In the first project year, common specifications for the eID interoperability framework have been developed.
- In the second year, the common specifications have been implemented and deployed into the national pilot systems.
- The third year was devoted to piloting the framework.

The target was to deploy and pilot in production systems. This to maximize lessons learned, as less compromise or weakening requirements under pilot assumptions is expected, once service providers have to deploy in their production environment. Service provider rather will ask for close-to production quality which increases confidence in the general applicability of pilot results.

The STORK cornerstones are thus the six pilots, each having specific requirements:

- The first pilot *Cross-Border Authentication Platform for Electronic Services* aimed at integrating the STORK framework to e-government portals, thus allowing citizens to authenticate using their eID. The portals did 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 personalized e-government services.
- In the *Safer Chat* pilot juveniles could communicate with peers within their age range safely. The pilot has been carried out between several schools. The specific requirement was 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.
- *Student Mobility* supported 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 could be used to allow foreign students to enroll from abroad using their eID and to access the campus management system’s services during their stay. The prime requirement is authentication, as in the first pilot on cross-border authentication.
- The fourth pilot *Electronic Delivery* objective was 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 enabled cross-border tests of signature-functions that most national eIDs have.
- To facilitate moving house across borders, the pilot *Change of Address* has been defined. In addition to authentication, the pilot had transfer of attributes, i.e. the address, as a requirement. An interesting aspect was that – in addition to the population registers – further authorities could be connected and automatically be informed of an address change. Examples are employment centers or billing addresses for the electrical supply companies.
- 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 European institutions. Piloting

administration-to-administration (A2A) services with national eIDs was a STORK objective. The pilot A2A Services and ECAS integration serves this objective by linking up STORK to ECAS.

In the course of the project, the ambition stretched beyond these pilots. One example is the continuous liaison with the STORK sibling pilot European patients' Smart Open Services (epSOS) on cross-border e-health. As e-health has immanent need of secure authentication, a "STORK meets epSOS" (STepS) liaison activity has been defined in order to ensure that e-government and e-health do not deviate on eID aspects. A discussion of STepS that led to field tests is given in [5]. A further example is using STORK in Point of Single Contacts in relation to the EU Services Directive [6]. This has e.g. been implemented by Spain.

2. QAA Scheme and Conceptual Interoperability Models

In this section we present two fundamental aspects of the STORK project: The first aspect is a Quality Authentication Assurance (QAA) framework that has been defined as the basis of a trust framework between the MS. This QAA model is described in sub-section 2.1. The second aspect is how interoperability based on heterogeneous national eID is approached. Two basic models have been defined which can either be centralized or a decentralized. The two models are referred to as PEPS and middleware and are described in sub-sections 2.2 and 2.3. The component that bridges between the two models is referred to as virtual identity provider (V-IDP) and is discussed in sub-section 2.4.

2.1. Quality Authentication Assurance Model

A basis for cross-border use of eID is trust in the other MS's systems. To date, no formal basis for such trust exists for eID, such as e.g. given for the international acceptance of passports or for the EEA-wide recognition of qualified certificates under the EU Signature Directive [7]. When considering the different implementations of national eID systems – ranging from simple username-password to smartcards – means to assess the quality of a credential used cross-borders are needed.

The idea is to assign each authentication credential an assurance level. A service provider can than request authentication based on the minimum assurance level needed for its particular service. Similar schemes have been established as levels of assurance (LoA) by the US administration [8] – further specified by the National Institute of Standards and Technologies (NIST) [9]. Under the European Commission's Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC) programme, a similar scheme was proposed in [10].

STORK based its QAA scheme [11] on the proposal done by IDABC [10]. As in the IDABC scheme, as well as in the US work [8] and [9], the STORK model consists of four levels. This is sketched in Table 1.

Table 1. Overview of STORK QAA levels

STORK QAA Level	Description
1	Low or minimal assurance
2	Low assurance
3	Substantial assurance
4	High assurance

To give a little more detail, the four STORK QAA levels are summarized as (QAA descriptions quoted from its specification in [11]):

- STORK QAA level 1 is the lowest assurance level; it either assures a minimal confidence in the asserted identity or no confidence at all. Identity credentials are accepted without any form of verification. If the subscriber provides an e-mail address, the only check that is performed is the verification of the correctness of the e-mail address. This level is appropriate when negative consequences that result from an erroneous authentication have a very low or a negligible impact. This level suits recognized on-line services implementing either a minimal set of security protection mechanisms or no set at all.
- STORK QAA level 2 defines the level used by those services where damage from a misappropriation of a real-word identity has a low impact. Even if the claimants are not required to appear physically during the registration, their real-word identities must be validated and a token issued by a body subjected to specific governmental agreement. Identity tokens must be delivered with accuracy and security guarantees. Sufficiently robust authentication protocols must be used during the electronic authentication phase.
- STORK QAA Level 3 defines the level used by services that may suffer substantial damages in case of an identity misuse. The registration of an identity is processed with methods that unambiguously and with a high level of certainty identify the claimant. The identity providers are supervised or accredited by the government. The credentials delivered are at least soft certificates or hard certificates. The authentication mechanisms used in the remote authentication phase are robust.
- STORK QAA Level 4 is the highest assurance level and addresses those services where damage caused by an identity misuse might have a heavy impact. The registration requires at least once (i.e., the very first time of the request but not for a later renewal) either the physical presence of the claimant or a physical meeting with the claimant (e.g., a certificate is requested on-line, delivered at home, and deployed in the hands of the claimant after a physical check of his/her identity). Alternatively, in case of on-line registration, a claimant identity is validated using trusted e-signatures. Annex II of the Signature Directive [7] leaves the details of identity verification to national law. Therefore, level 4 is fulfilled if the national legal requirements for issuing a qualified certificate have been met. Furthermore, the identity provider must be a qualified entity according to the Annex II of the e-signature Directive. The certificates are hard certificates qualified according to the Annex I of the e-signature Directive. The most robust authentication mechanisms are used during the authentication phase.

To categorize eID, criteria for both the registration and the authentication phase have been defined. For registration, criteria are further divided into those for initially identifying the citizen (e.g., whether physical presence or official documents are requested), for registering the credential (e.g., whether the credential is downloaded or handed over in person), and for the entity issuing the credentials (e.g., whether government supervision applies). For the authentication phase, criteria comprise the credential type (e.g., username-password, software certificates, or hardware crypto tokens) and its technical methods (e.g., challenge-response, symmetric, or asymmetric cryptography), as well as its robustness (e.g., resistant against guessing, spoofing, or man-in-the-middle attacks). This division is shown in figure 1.

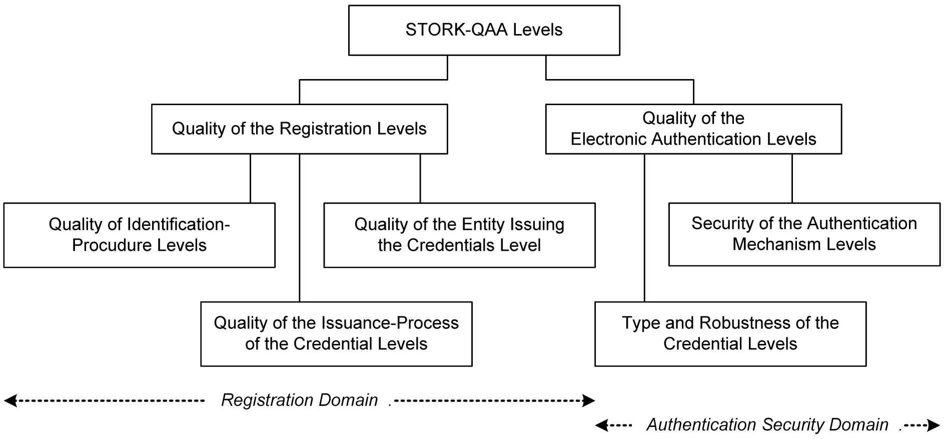
STORK-QAA Levels
Quality of the Registration Levels
Quality of the Electronic Authentication Levels
Quality of Identification-Procudure Levels
Quality of the Entity Issuing the Credentials Level
Security of the Authentication Mechanism Levels
Quality of the Issuance-Process of the Credential Levels
Type and Robustness of the Credential Levels
Registration Domain
Authentication Security Domain

Figure 1. STORK QAA mapping concept (from [11]).
Each MS assigns its eID credentials to one of the four STORK QAA levels

To reach the highest QAA level (STORK QAA level 4) each of the domains, registration and authentication security, as well as their sub-categories need to meet highest standards. QAA has been defined so that existing credentials that support qualified electronic signatures also fulfill QAA level 4. A rationale of aligning with the Signature Directive [7] is that it already defines security measures that lead to mutual recognition across the EEA. Qualified signature are however no necessary condition for QAA level 4 – credentials not supporting qualified signatures can reach it as well.

2.2. Centralized Deployment - PEPS

The first interoperability model defined and piloted in STORK is assuming that each MS operates a central gateway that serves both its citizens' eID credentials and its service provider (SP). We refer to such a gateway as Pan-European Proxy Service (PEPS). As serving the citizen credentials and handling the SP are different functions, we further distinguish between a C-PEPS (handling citizen's eID credential) and an S-PEPS (interfacing to the SP). The conceptual model is illustrated in figure 2.

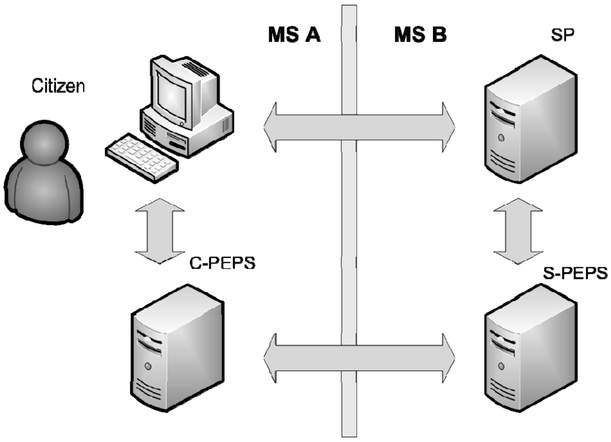

Figure 2. STORK centralized – PEPS model (from [4])

We refer to Member State A (MS A) as the state which has issued an eID to the citizen, i.e. usually the citizen is a MS A resident. The foreign SP is located in MS B. When the citizen accesses a foreign service that requires authentication, the SP delegates the authentication process to her S-PEPS. The SP's request to the S-PEPS contains the minimum QAA level required and mandatory or optional attributes needed by the service (e.g., mandatory name and date of birth to provide service, and optionally the residence). Delegation to the S-PEPS is done via the Web-browser, i.e. the citizen is redirected to the S-PEPS. At the S-PEPS, the citizen selects the country of origin (i.e., MS A) and is than further redirected to the C-PEPS (cross-border). The actual citizen authentication takes place either directly at the C-PEPS or at an Identity Provider's (IdP's) authentication service in MS . In addition, attribute providers may be involved to collect the attributes, such as an address register for the citizen's residence. The MS A C-PEPS asserts to the S-PEPS in MS B a successful authentication, the QAA-level associated with the citizen credential used, and the provided attributes. Finally, the S-PEPS asserts authentication to the SP that grants the citizen access to the application.

Figure 2 and the process description illustrate that the PEPS model is characterized by segmented trust relationships: SPs trust their national S-PEPS. A C-PEPS trusts its national IdPs. The cross-border trust relationship is established between the C-PEPS and the S-PEPS. A further discussion of security and data protection aspects of the centralized PEPS model is given in section 4.

2.3. Decentralized Deployment - Middleware

The alternative deployment model is to avoid centralized components and to provide interoperability at the SP. The idea is based on the situation that national eID integration at service providers is usually supported by some sort of middleware that de-couples the legacy service from handling of eID token protocols. In the STORK context, such SP-side middleware has been referred to as "SPware". Usually, also a client-side middleware (MW) does the integration of the credential (e.g., a smartcard) into the citizen's PC operating system.

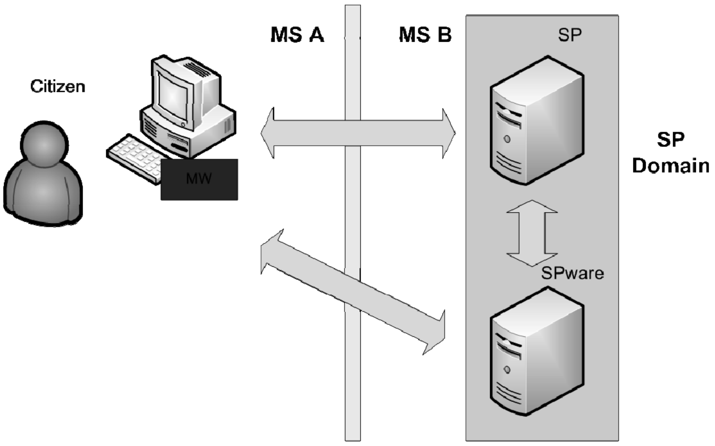

Figure 3. STORK decentralized – MW model (from [4])

The MW scenario is illustrated in figure 3. Leveraging that scenario cross-border without introducing additional central infrastructure means that the server-side middleware needs to incorporate the national protocols used for the various eIDs.

2.4. Combination – V-IDP

With two conceptional models interoperability within each is not a big deal, as each follows similar basic assumptions. The deployment is limited to technical implementation of common protocols. The challenge however is to bridge between the two, as the underlying assumptions are different. We distinguish between two situations, as follows:

- A citizen from a “MW-country” accessing a SP from a “PEPS-country”
- A citizen from a “PEPS-country” accessing a SP from a “MW-country”

In the first scenario, the underlying assumption is that in the citizen’s country of origin MS A no central component “C-PEPS” exists and the SP provides the citizen credential integration using SPware. The SP’s assumption however is that a central component “S-PEPS” provides an authentication gateway hiding foreign specifics. The S-PEPS may also provide the authentication gateway to national IdPs. The idea thus was to introduce a further component at the S-PEPS that mimics an IdP protocol, but integrates the protocols of all “MW-countries”. This component has been referred to a “virtual IdP” (V-IDP). The V-IDP thus needs to integrate all the server-side middleware (SPware) of MW-countries. At the S-PEPS the situation is as if it accesses a C-PEPS, that however is operated in the SP’s country MS B, not in the citizen’s country of origin MS A.

The approach meets both requirements: The MW-country MS A that may not be able to provide central authentications gateways for legal reasons can still authenticate at the foreign environment, though at a central component – which however is obviously legally possible in the SP-country MS B, as PEPS is such a central component anyhow. The overall architecture of this scenario is illustrated in figure 4.

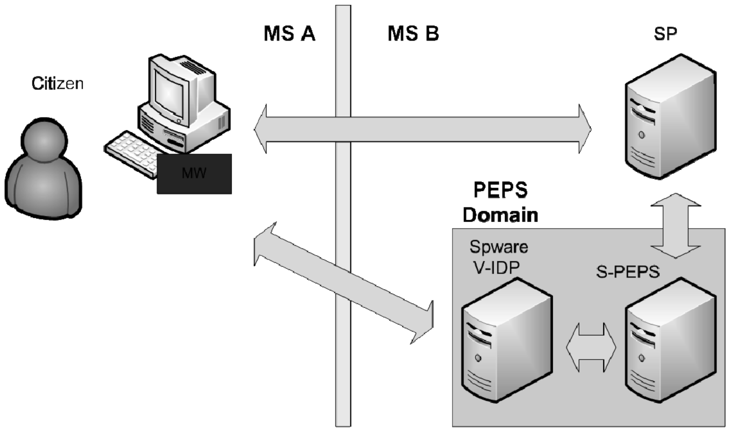

Figure 4. STORK V-IDP – citizen from a “MW-country” accessing a “PEPS-country”

The second bridging scenario is when a citizen that origins from a “PEPS-country” authenticates at an “MW-country”. Here the SP operates a SPware component interfacing with the national eID. The citizen authentication is delegated to a C-PEPS. The approach thus is that the SPware is extended by the C-PEPS protocol. Thus the citizen authenticates at the C-PEPS as in the PEPS model. The authentication assertion is however directly provided to the SP’s domain, not redirected via a further PEPS. What changes for the C-PEPS is that instead of interfacing to a single S-PEPS instance per foreign MS B, an arbitrary number of SPs may request authentication. The overall scenario is shown in figure 5.

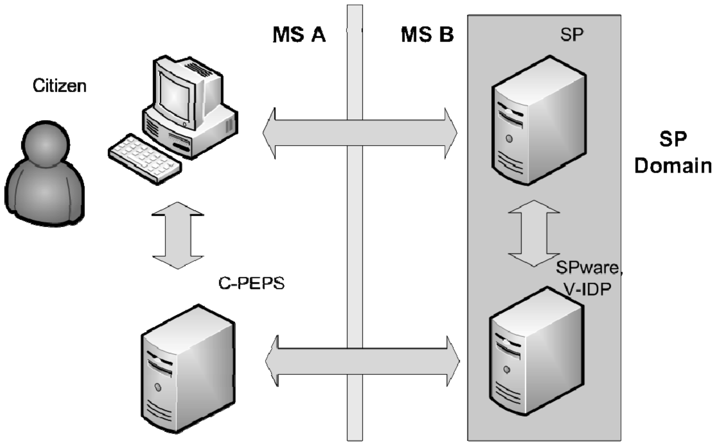

Figure 5. STORK V-IDP – citizen from a “PEPS-country” accessing a “MW-country”

To streamline the terminology used, the term “SPware” has been eliminated and the term “V-IDP” is used whenever a middleware is involved. This reduces the STORK architecture to three components and interfaces, as follows:

- The *C-PEPS* is a central authentication gateway that interfaces to the citizen’s eID credential (probably via an IdP).

- The *S-PEPS* asserts successful authentication to an SP
- The *V-IDP* provides a bridging component that (depending on the case) interfaces to the citizen eID credential, the C-PEPS, or the S-PEPS. This is done whenever a decentralized approach is desired and where central authentication gateways are not possible.

The main outcome of STORK has been common specifications of these three components and its implementation. This is described in the following section.

3. Common Specifications and Technical Components

An underlying principle of STORK was to use open standards and to provide free open source reference implementations of its specifications. With respect to open standards in identity federation, two main families exist: The Security Assertion Markup Language (SAML) [12] and the Web Services family (WS*) that build on Web Services Security (WS-Security) [13], such as Web Service Trust (WS-Trust) [14], etc. In addition, open specifications of identity federation initiatives exist, such as specifications for OpenID.

STORK has chosen SAML version 2.0 as the basis of its common specifications. The SAML profiles and bindings used by STORK are:

- HTTP Post Binding [15]
- Web Browser SSO Profile [16]
- Holder of Key Web Browser SSO Profile [17] (as an optional supplement to the Web Browser SSO Profile)

While SAML 2.0 provides the basis, the STORK interface specifications contain some extensions that are needed to implement the overall infrastructure, such as introducing the QAA levels. The main extensions that have been included in the `samlp:Extensions` element of the SAML authentication request, are:

- The QAA Level which indicates the quality of authentication required for the subject (cf. section 2.1). This is a mandatory extension.
- Optional indications send by the SP on whether the identifier received might be shared within the sector, across sectors, or cross-borders.
- Optional attributes requested by the SP. Such attributes might for instance be the name, the date of birth, or the residence, but also may be extended to arbitrary further attributes needed by a sector to provide service.

The main element in the SAML Assertion in the authentication response is the "eIdentifier" that is transferred as a `saml2:Attribute`. In addition, the attributes requested by the SP are delivered. The SAML response is electronically signed.

The STORK common specifications consist of the following documents that all are publicly available:

- A brief overview document "Technical Design for PEPS, MW models and interoperability" (STORK deliverable D5.8.3) [18]. That overview summarizes the common specification documents that follow.
- The overall architecture describing the PEPS and MW models is given in the "Software Architecture Design" (D5.8.3a) [19].
- The main specification is the "Interface Specifications" (D5.8.3b) [20]. This document defines the SAML 2.0 protocol and extension used by STORK.

- An open source PEPS reference implementation is described in the "Software Design for PEPS architecture" document (D5.8.3c) [21].
- The V-IDP implementation is specified in "Software Design for MW architecture for MW architecture" (D5.8.3e) [23].
- Finally, the document "Security Principles and Best Practices" (D5.8.3d) [22] defines common principles for secure development and operations.

For both PEPS and V-IDP reference implementations are provided in Java. The PEPS architecture is illustrated in figure 6. A PEPS consists of two main components, an "Authentication PEPS" and a "Validation PEPS", as follows:

- The Authentication PEPS consists of a SAML engine and three components implementing the main PEPS interfaces: (1) The "AUSPEPS" component manages the authentication process between a SP and the S-PEPS. Authentication requests from a SP are received at this component and authentication responses are returned to the calling SP. (2) The "AUCPEPS" component provides the inbound functionality of a C-PEPS. Authentication request messages sent from a S-PEPS are received and handled. Responses containing citizen's identity and authentication data are returned to the requesting S-PEPS. The "Specific PEPS" component covers country specific functionality to 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 Validation PEPS implements the business logic for digital certificate validation. The main sub-components include an online certificate status protocol (OCSP) engine. The OCSP responder is in charge of handling OCSP requests either sent from a SP or a partner PEPS. The OCSP Client component is responsible for generating OCSP requests for certificate validation to be sent to a partner PEPS. The OCSP Engine implements methods for the generation and processing of OCSP request and response messages.

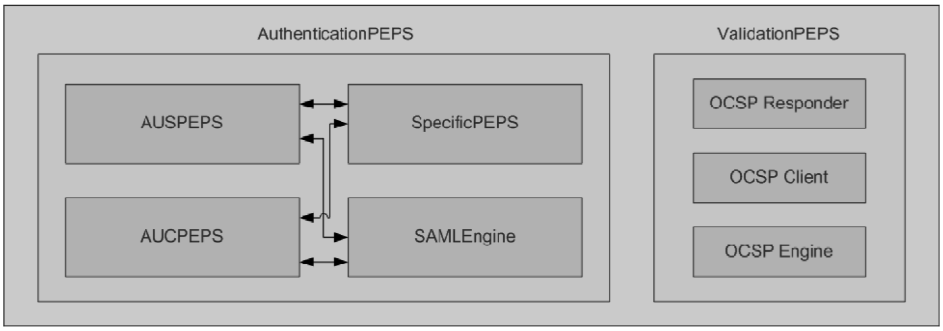

Figure 6. PEPS architecture (from [4])

The V-IDP architecture is shown in figure 7. As the V-IDP needs to host different national components, i.e. SPware that implements different national protocols, a scalable architecture has to be developed. The core component is referred to as Modular Authentication Relay Service (MARS). The MARS can dynamically link national components as Plug-In or Plug-On.

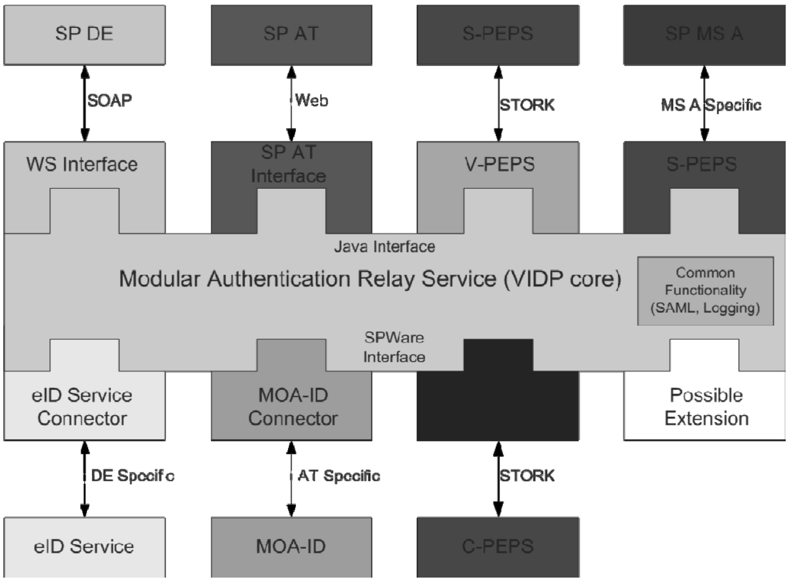

Figure 7. V-IDP architecture (from [4])

The MARS core provides common functionality such as logging, configuration or SAML message generation. The components shown on the top of the V-IDP core in figure 7 define so-called "Plug-Ons". They are responsible for mapping various authentication requests from service providers or S-PEPSs to a common Java interface. The Plug-Ons can either be Web Service-based (SOAP) or can be a Web server component. The components shown at the bottom of the V-IDP core in figure 7 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 two countries that have opted for the MW model in STORK are Austria and Germany (see also section 4.). Thus, the current implementation of this V-IDP architecture needs to at least support Austrian and German middleware, as well as the PEPS connectors. It consists of the following components:

- The "WS Interface" is used by German SPs and is SOAP-based.
- The "SP AT interface" is a Web interface for supporting Austrian legacy service providers.
- The "V-PEPS" component receives SAML authentication request messages from a S-PEPS and forwards the message to the V-IDP.
- The "eIDService Connector" is a Plug-In that handles the communication with the German eID service.
- A "MOA-ID Connector" delegates an authentication request to the Austrian server-side middleware MOA-ID.
- With the "C-PEPS Connector" citizens of PEPS countries can be authenticated at SPs relying on a MW model (cf. section 2.2, figure 5)

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. Further details of the V-IDP architecture are given in [24].

4. Security and Data Protection

Security and data protection have been major considerations throughout the development of STORK [25]. When comparing the models PEPS and MW, an obvious difference that has an impact on security and privacy is that an intermediary is introduced in the PEPS model. This has consequences with respect to trust relationships, end-to-end security capabilities, or liability. A summary is given in the following table 2 and further discussed in this section.

Table 2. Overview of STORK QAA levels

Criterion	Middleware	PEPS
scalability	challenge with many eID tokens	easy due to single cross-border interface
trust relations	direct: citizen – SP	segmented: citizen – PEPS – PEPS – SP
security perimeter	end-to-end	terminates at intermediary (segment)
liability	remains at SP	potential liability shift
data controller	SP	SP or PEPS operator

Transmission of personal electronic identifiers of general use is privacy sensitive. Misuse can lead to profiling or linking of otherwise unrelated cases of the citizen. The Data Protection Directive [26] foresees several grounds for legitimacy of processing of personal data, such as the unambiguous consent of the data subject, the processing being necessary for the performance of a contract to which the data subject is party, or compliance with a legal obligation to which the controller is subject. The legal assessment within STORK [27] has identified consent of the data subject as the only general enough grounds for an infrastructure like STORK aims to establish. STORK defined two types of consent the operator of a component (the PEPS or the SP in the middleware model) can choose to apply: (1) Data type consent is provided before data collection. For instance, the citizen consents to transfer her address before a residence register is queried. (2) Data value consent is applied after the data has been collected, but before it is transmitted cross-border. In the example used before, consent is not just asked for transferring the address (whatever the residence register as attribute provider delivers as address), but the actual values such as the street name and the number are displayed to the citizen before consent is given.

A further issue to be tackled was the use of identifiers. States often restrict the use of national identifiers. This is done for privacy reasons and also rooted in the Data Protection Directive [26] that asks EU Member States to "*... determine the conditions under which a national identification number or any other identifier of general application may be processed*". Such restrictions however may limit or even inhibit the use of eID and national identifiers cross-borders. To overcome this, the STORK legal assessment [27] suggested to cryptographically transforming identifiers for cross-border use from the national identifiers, similar as Austria derives sector-specific identifiers from a unique base identifier [28]. The STORK security specifications [22] further define cryptographic schemes to transform to country-specific, service-provider-specific, or application-specific personal identifiers. Such measures can allow the cross-border use of national identification schemes where legal obstacles for such use are given. The application of such measures is however at the discretion of the data controller, depending on its legal obligations.

In any case the territorial principle of the Data Protection Directive applies. I.e., that national law of the establishment of the data controller applies. In terms of the Directive, each Member State applies its national provisions to the processing of personal data where "*the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State*". On the different approaches of using identifiers (cf. footnote 5 in section 1), this means that if a state uses its national identifiers flat across sectors, STORK assumes that also a foreign identifier may be used this way in that particular state. This irrespective from different rules applying in the citizen's country of origin. Vice versa, if a state has provisions for deriving sector-specific identification, such data protection measures need to be applied for foreign identifiers as well. Again, this needs to be done even if these identifiers may be used flat across sectors in the country of origin.

On the technical security, state-of-the-art protection of data transmitted is applied. Given that STORK is browser-based, HTTPS has been defined. In addition, the security provisions [22] define best practices on secure operations. The security aspect is however one where the two models middleware and PEPS distinguish: In the middleware model, technical provisions for end-to-end security between the citizen and the SP can be implemented, as no intermediary is in the trust-chain. The middleware model has been chosen by Austria and Germany. With the Austrian citizen card a qualified electronic signature is applied by the citizen to an authentication statement. This qualified electronic signature can be verified by the SPs in their domain. This provides end-to-end security. The German eID "neuer Personalausweis" uses card-verifiable certificates where the SPware "eID service" operated by the SP establishes a cryptographic channel to the card. This also provides technical end-to-end security. eID tokens of "PEPS countries" provide similar mechanisms, such as using the eID for providing client-certificates in SSL-connections or providing qualified certificates. The PEPS model, however, is based on the assumption that the PEPS hides national specifics and acts as a single entry point. Thus, the channel that is technically secured by the eID token terminates at the IdP or the C-PEPS[10]. The PEPS vouches for having validated the authentication. This leads to segmented security perimeters: Technical security is provided between the eID token and the C-PEPS (or the IdP), the C-PEPSs and S-PEPSs of the states build a circle of trust by means of the SAML signing certificates, and finally technical security measures exist between the S-PEPS and the SP. In order to reduce the risk of man-in-the-middle attacks, a holder of the key SAML profile [17] has been specified as an option in [20].

The segmented trust relationship may lead to liability shifts: In the MW model, the SP operates the components that accept the various eID. In case of compromise, either the eID issuer can be held liable for breaching its obligations[11], or the SP remains liable. Thus no liability shifts. In the PEPS model, however, liability may shift: In case a PEPS gets compromised, false identities may get created. As neither the eID issuer nor the SP have means to recognize that, they cannot be held liable.

Taking end-to-end security and liability into account, it becomes obvious that the decision of opting for the PEPS model or the MW model is no straightforward one, but is a tradeoff between various factors: The MW model comes with some challenges in integrating the various eIDs, but leads to a clearer situation on liability and extends technical end-to-end security to the cross-border case[12]. In the PEPS model, eID

[10] Whether the link technically secured by the eID token terminates at the IdP or the C-PEPS depends on whether eID integration and, thus, authentication is done at the C-PEPS, or whether delegated to an IdP.

[11] In case of qualified certificates, liability of the eID issuer is defined in the Signature Directive [7].

[12] End-to-end security between the eID token and the SP holds for the "pure" middleware model between two MW-countries. In the communication with a PEPS country, the secure channel established by the eID token terminates at the V-IDP hosted at the C-PEPS (cf. figure 4).

integration is limited to the national eID (at the C-PEPS), specifics of foreign eID are hidden from both the S-PEPS and the SP. This comes with the PEPS as central component needing particular attention both security-wise and data-protection-wise.

A central question on data protection assessments is who the controller is. This question is easily answered in the MW model: As authentication is provided directly at the SP without an intermediary, the SP remains the controller. A PEPS however can be argued either as a controller or as a processor. The data processor can be the C-PEPS acting on behalf of the IdP as controller, the S-PEPS acting on behalf of the SP as controller, respectively. Whether the PEPS is a controller or a processor has some consequences: The main is that the "processing on behalf" of a processor needs some sort of basis, such as contract. Establishing many bilateral contracts with SPs may however be a hindering factor of take-up of an infrastructure like STORK. The STORK consortium did not come to a conclusion if a PEPS is a controller or a processor.

The STORK consortium did a consultation with the Article 29 Data Protection Working Party under the Data Protection Directive [26]. Art. 29 WP gave some recommendations [29], in principle the privacy measures of STORK have been seen positive. On the question of controller vs. processor, Art. 29 WP however was inconclusive as well, stating a "dilemma" and "*Therefore controllers that use a PEPS and provider of PEPS services will have to decide if they consider themselves as controller or processor under the Directive 95/46 and contact their national DPA to confirm this for example during a notification procedure.*" [29].

5. Conclusions

STORK has brought eighteen EU and EEA Member States together to define a framework that supports seamless eID use across borders. The idea was to make use of the existing national eID programmes and to build an interoperability layer on top of it. Two models have been investigated – the Pan-European Proxy Service (PEPS) model and the middleware model. The PEPS model is based on central national authentication gateways, thus aiming at interoperability by dedicated services installed for the cross-border case. The middleware model integrates the various eID tokens technically into common modules deployed at the service provider, i.e. the application the citizen authenticates to. Both models take explicit user consent as the basis for legitimacy of data processing and transfer, thus – aside technical measures – establishing consent as the root to data protection compliance. Six pilots have been carried out from mid-2010 to end of 2011 to test the interoperability framework in real world environments.

While the pilots have shown the technical feasibility of the interoperability solution, there have been gaps: The main are that a sustainability solution for the infrastructure is not yet given and the missing legal basis for cross-border eID. On sustainability, the European Commission's Interoperability Solutions for European Public Administrations (ISA) programme has a STORK sustainability action in its 2011 Work Programme [30]. The ISA work item consists of governance, coordination, standardization, software maintenance, and support activities.

The Large Scale Pilots are expected to give valuable input into related policy actions. A major one in the eID field is advancing legal recognition of eID across borders. This is expected from the EU Digital Agenda that in its Key Action 3 defines to "*In 2011 propose a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure* *eAuthentication systems;*", as well as in Key Action 16 defines 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);*" [3]. Achieving such legal recognition together with the technical infrastructure that has been developed by STORK is expected to become a major leap on seamless eID use in Europe.

References

[1] H. Graux, J. Majava, E. Meyvis: Analysis & assessment report. In: *Study on eID Interoperability for PEGS: Update of Country Profiles*. IDABC European eGovernment Services, European Commission, 2009.

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

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

[4] H. Leitold, B. Zwattendorfer, STORK: Architecture, Implementation and Pilots, In: *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference*, Vieweg+Teubner, 131 – 142, 2010.

[5] B. Zwattendorfer, T. Zefferer, A. Tauber, E-ID Meets E-Health on a Pan-European Level, In: *Proceedings of the IADIS International Conference e-Health 2011,* 97-104, 2011.

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

[7] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[8] Executive Office of the President, *E-Authentication Guidance for Federal agencies*, OMB Memorandum M-04-04, 2003.

[9] W. E. Burr, D. F. Dodson, W. T. Polk, *Electronic Authentication Guideline*, NIST Special Publication 800-63, 2006.

[10] European Commission, *Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms*, IDABC – European e-Government Service, 2007.

[11] B. Hulsebosch, G. Lenzini, and H. Eertink, *Quality authenticator scheme*, STORK deliverable D2.3, 2009.

[12] S. Cantor, J. Kemp, R. Philpott, E. Maler, *Assertions and Protocols for the OASIS Security Assertion Markup Language* (SAML) V2.0, OASIS Standard, 2005.

[13] A. Nadalin. C. Kaler, P. Hallam-Baker, R. Monzillo, *Web Services Security: SOAP Message Security 1.0* (WS-Security 2004), OASIS Standard, 2004.

[14] A. Nadalin, M. Goodner, M. Gudgin, A. Barbir, H. Granquist, *WS-Trust 1.4*, OASIS Standard, 2009.

[15] S. Cantor, F. Hirsch, J. Kemp, R, Philpott, E. Maler, *Bindings for the OASIS Security Assertion Markup Language* (SAML) V2.0, OASIS Standard, 2005.

[16] J. Hughes, S. Cantor, J. Hodges, F. Hirsch, P. Mishra, R. Philpott, E. Maler, *Profiles for the OASIS Security Assertion Markup Language* (SAML) V2.0, OASIS Standard, 2005.

[17] N. Klingenstein, T. Scavo, *Profiles for the OASIS Security Assertion Markup Language* (SAML) V2.0, OASIS Committee Specification, 2010.

[18] J. Heppe, *Technical Design for PEPS, MW models and interoperability*, STORK deliverable D5.8.3 overview document, 2011.

[19] D. Berbecaru, E. Jorquera, J. Alcalde-Moraño, R. Portela, W. Bauer, B. Zwattendorfer, J. Eichholz, T. Schneider, *Software Architecture Design*, STORK deliverable D5.8.3a, 2011.

[20] J. Alcalde-Moraño, J. López Hernández-Ardieta, A. Johnston, D. Martinez, B. Zwattendorfer, M. Stern, J. Heppe, *Interface Specifications*, STORK deliverable D5.8.3b, 2010.

[21] D. Berbecaru, J. Alcalde-Moraño, J. L. Hernández-Ardieta, R. Portela, R. Ferreira, *Software Design for PEPS architecture*, STORK deliverable D5.8.3c, 2011.

[22] M. Stern, *Security Principles and Best Practices*, STORK deliverable D5.8.3d, 2011.

[23] I. Sumelong, A. Lunkeit, B. Zwattendorfer, T. Schneider, *Software Design for MW architecture for MW architecture*, STORK deliverable D5.8.3e, 2011.

[24] B. Zwattendorfer, I. Sumelong, Interoperable Middleware-Architektur für sichere, länderübergreifende Identifizierung und Authentifizierung, *In: Tagungsband zum 12. Deutschen IT-Sicherheitskongress*, 175-189, 2011.

[25] V. Koulolias, A. Kountzeris, A. Crespo, H. Leitold, B. Zwattendorfer, M. Stern, STORK e-Privacy and Security, *In: Proceedings of 5th International Conference on Network and System Security (NSS)*, 234-238, 2011.

[26] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[27] R. Leenes, B. Priem, C. van de Wiel, K. Owczynik, Report on Legal Interoperability, STORK deliverable D2.2, 2009.

[28] Austrian E-Government Act: Federal Act on Provisions Facilitating Electronic Communications with Public Bodies. In: Austrian Federal Law Gazette, part I, Nr. 10/2004; last amended part I, Nr. 111/2010.

[29] Article 29 Data Protection Working Party, Written report of the Article 29 Data Protection Working Party on STORK, Biometrics & eGovernment Subgroup, Ref. Ares(2011)424406, 2011.

[30] European Commission, ISA Work Programme, First revision 2011.