

---

# 12 eID Interoperability

*Ioannis Krontiris, Herbert Leitold, Reinhard Posch, Kai Rannenberg*

*eIDs have simplified the lives of many Europeans. But what happens when they travel to another Member State? Unfortunately, the benefits of eIDs disappear, when citizens try to use their own country's eID to access another country's services. In this chapter, we emphasize the importance of interoperability between national eIDs and discuss the complexity of the problem. Then we present the STORK<sup>1</sup> project and what it has achieved so far in developing specifications and testing out interoperability in real world situations. Finally we conclude with some open issues and future directions.*

## 12.1 Introduction

Throughout the EU, some 30 million national electronic identifier (eID) cards are being used by citizens to access a variety of public services, such as claiming social security and unemployment benefits or filing tax returns. However, several barriers to the free movement of citizens still exist in the EU. For example, accessing public services that require identification, while working or living in another country is not easy. Providing eID interoperability will facilitate this situation by enabling businesses and citizens to securely use their national eIDs and receive services from public administrations, while living or travelling in any Member State. So, interoperability can simplify administrative formalities by providing online access to public services across EU borders. This can be achieved through the development of common specifications for secure and mutual recognition of national eIDs between participating countries.

The necessity for interoperable eIDs has been recognized in the i2010 eGovernment Action Plan [Com06] that followed the 2005 Manchester Ministerial Declaration. The document emphasizes that interoperability and electronic identity are “key enablers” for eGovernment in general. Interoperability of eIDs is essential for achieving the freedom of goods, services and capital. It can reduce administrative burden throughout Europe and therefore lead to a better competitive position of the EU-zone.

Also in the recent Digital Agenda for Europe [Com10], communicated by the European Commission, the role of eGovernment services is emphasized as a key factor towards

---

<sup>1</sup> Secure idenTity acrOss boRders linKed, [www.eid-stork.eu](http://www.eid-stork.eu)

achieving the social and economic goals of Europe for the future. In particular, it remarks that the future public online services will rely on effective and interoperable identity management and authentication frameworks and tools across borders. Therefore, Member States should make eGovernment services fully interoperable and enable common cross-border public online services by 2015.

The STORK project is such an attempt to test eID interoperability in real world situations. It is a Large Scale Pilot co-funded by the European Commission under the CIP ICT-PSP Framework Programme.<sup>1</sup> In STORK a group of fourteen EU/EEA Member States,<sup>2</sup> in the course of the project extended by four further states,<sup>3</sup> develops common specifications, implements them and tests them in six concrete pilot applications. STORK started in June 2008 and lasts for three years. STORK's objectives are to develop widespread rules and specifications to assist mutual recognition of eIDs across national borders, to test secure and easy-to-use eID solutions for citizens and businesses in real life environments and to interact with other EU initiatives to maximize the usefulness of eID services.

In this chapter, we will first introduce a general authentication process model (Section 12.2). In Section 12.3 we take a look at the complex nature of interoperability by exploring the different requirements it poses on the legal, social and technical sphere. In Section 12.4 we emphasize on the privacy aspects of interoperability and discuss some threats. In Section 12.5 we present some details of the STORK project and how it has managed to address several of the requirements of the first section. In Section 12.6, we discuss open issues and future directions for identity management that could have influence on how we see interoperability today, before we conclude in Section 12.7.

## 12.2 Authentication Process Model

Before we proceed to framing the requirements for interoperability, it is helpful to briefly review the authentication reference model, described by IDABC [IDA07a]. IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens)<sup>4</sup> is a project managed by the European Commission that has published recommendations and developed common solutions in order to improve the electronic communication within the public sector.

Conceptually the authentication of an entity requires 2 main phases:

- the Registration phase, which is the process by which a user gains a token/credential such as a username or digital certificate for subsequent authentication;

---

<sup>1</sup> Competitiveness and Innovations Programme, ICT Policy Support Programme, [http://ec.europa.eu/information\\_society/activities/ict\\_psp/](http://ec.europa.eu/information_society/activities/ict_psp/)

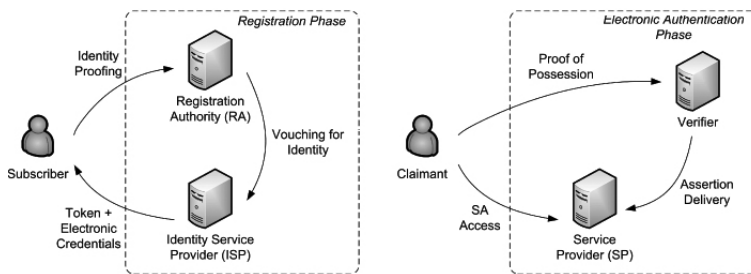
<sup>2</sup> STORK started 2008 with Austria, Belgium, Estonia, France, Germany Iceland, Italy, Luxemburg, Portugal, Slovenia, Spain, Sweden, The Netherlands, and United Kingdom.

<sup>3</sup> The 2010 extension included Finland, Lithuania, Norway, and Slovak Republic.

<sup>4</sup> <http://ec.europa.eu/idabc/>

- the Electronic Authentication phase, also called Proof of Possession (or PoP), during which the electronic identity of the claimant is verified.

As shown in Figure 12.1, during the registration phase, the subscriber (or claimant) refers to a Registration Authority (RA) to claim an identifier. That is, the RA must ensure that the subscriber identification corresponds to a real entity and that the subscriber is indeed subscribed to some Identity Service Provider (ISP). The ISP gives the subscriber an eID to be used in an authentication process and issues credentials to bind that token to the identity. In the simplest and perhaps the most common case, the RA and ISP are separate functions of the same entity and the process takes place at a government institute of the subscriber's home country.



**Figure 12.1** Authentication Process Model

During an authenticated online transaction, the claimant, i.e. the user, uses the token and credentials obtained in the previous phase to access a service. The Service Provider (SP) is the one who determines what credentials need to be provided, in order to grant the claimant access. It is therefore the SP who determines the required authentication level for getting access. If the SP cannot verify the used eID by himself, a Verifier will need to assure the SP that the used eID belongs to the claimant and is authentic.

In this case, the claimant must authenticate his identity by demonstrating the possession and control of an eID token and/or credential to the Verifier. This is called Proof of Possession (PoP). The electronic object created by the Verifier to convey this result is called an assertion. The Verifier passes along the assertion about the eID token or provides an attribute of the claimant to the SP. Then the SP uses the authenticated identity and other factors to make access control or authorization decisions.

In an international context, the SP is an organization situated in a Member State different than the Member State that has assigned the eID. In this case, the SP may need to verify the eID at the Verifier in a different Member State. Hence, cross border transfer of an eID occurs between the SP and the Verifier. Let us emphasize here that in addition to a formal eID, the cross-border exchange may also include other attributes (for example that someone is a student), not directly deduced from the authentication of that formal eID.

## 12.3 Requirements for Interoperability

As has been highlighted in the literature [LW01, MMMW01] already, interoperability is not to be confused with compatibility between heterogeneous systems. Of course there is a big inherent technical part that focuses on how to set up the information flow properly between associated processes in order to offer a service. This compatibility, or by others called interconnectivity, is a necessary requirement for interoperability, but not sufficient. The much broader goal to achieve is to encourage the sharing of information between people and organizations within the ICT environment.

The Roadmap to a pan-European interoperability framework [EU06] presented a series of building blocks that need to be brought in place in order to put pan-European eID into practice. These building blocks include:

- **Fundamental requirements:** a consistent eIDM terminology, creation and maintenance of user trust and awareness, and the realization of a personal data ownership/stewardship model that also takes into account privacy requirements mapped on a Member State level.
- **Infrastructural requirements:** a clear conceptual framework (including common specifications), the definition of authentication levels, choice of data formats and standardization issues, implementation of role and mandate management, information security and legal issues (including data quality and liability).
- **Usability requirements:** validation of solution models and business models, cooperation between public and private sectors and ensuring a harmonious user experience.

The above set of requirements gives us a hint on the multiple levels that interoperability refers to. Next we analyze some of the most important requirements from the above categories.

### 12.3.1 Fundamental Requirements

#### *User Trust and Awareness*

Without trust (in the framework's security) and awareness (of its basic operating principles and the resulting guarantees) the system is likely to remain unused, or be viewed as an intrusion rather than as an enabler. The end users should be willing to confide in the eID framework. To this end, concrete standards of security and privacy protection should be defined on a European level. These standards must be defined, observed by the system, evaluated continuously and communicated to the user base in an understandable manner to ensure user trust.

#### *Data ownership of the individual*

It is important that users have sufficient control and awareness of which of their personal data a service provider will obtain access to, keeping into account the proportionality principle of the Data Protection Directive and the Privacy and Electronic Commu-

nications Directive. Data control also implies active involvement in issuing, extending, restricting and withdrawing of credentials, as well as in management of personal data (including accessing and updating personal data to a maximum extent), in order to ensure that data in official authentic sources remains as accurate as possible.

#### *Partial Identities*

As it is pointed out in [HBC+04], we need to understand that individuals operate in different contexts, where they act using different “Partial Identities”. Contexts can be for example the relation to a doctor or a service provider in private life or the relation to an employer in professional life. These contexts are in principle separate and individuals might not want to give up the privacy they enjoy currently without interoperable systems. It should be individuals who decide in which context they will act and whether or not individual information could be shared across the contexts.

### 12.3.2 Infrastructural Requirements

#### *Authentication Interoperability*

Each country currently has its own way to deal with authentication. This means that neither the authentication profiles, nor the underlying mechanisms, nor the methods to identify the “right” profile are currently aligned. For each country, the reliability and trust levels of the authentication solutions used depend on the needs of specific applications, the policy preferences and socio-cultural considerations.

The following list shows how different eIDs are in the Member States and shows some illustrative examples. It is not supposed to be complete.

- *Identity management*

Some Member States use a national identifier flat in all sectors (e.g., Belgian RRN-number,<sup>1</sup> Estonian Personal Identification Code), others have sector-specific identifiers derived from a unique source (e.g. Austria), and other states consider persistent identifiers unconstitutional (e.g. Germany).

- *eID issuers*

eIDs can be issued by the public sector (Spanish DNIe card; Portuguese eID card), but can be also private sector borne (Swedish BankID). Government-borne eID can be issued by the central government (Italian Carta d’identità elettronica, CIE) or on the regional level (Italian Carta Nazionale dei Servizi, CNS).

- *Engagement*

Some Member States issue eIDs on a mandatory ID card and reach full coverage (e.g. Belgian or Estonian eID card), others have tokens reaching full coverage but activation as eID is voluntarily decided by the citizen (e.g. Austrian health insurance card) and others allow eIDs to be taken from the market (e.g. Slovenian Posta@ca or Austrian bank cards).

---

<sup>1</sup> Rijksregister – Régistre National

- *Technology*

eIDs range from username-password (DigiD in The Netherlands or UK Government Gateway), to SMS transaction numbers (DigiD) and software certificates, mobile eIDs (Austria, Estonia), and smartcards and qualified certificates.

- *Variety*

The categories above represent no clear-cut distinction between Member States. As the repeated mentioning of some Member States in the examples shows, some states have various combinations of issuers from private sector and public sector, support both eIDs on mandatory ID cards and alternative means, and have different technologies and security levels.

Once eIDs leave the comfort zone of qualified certificates, where mutual recognition and liability are defined in the Signature Directive, trust in the others' system becomes an issue. Currently there is no assurance mechanism in place that could allow building this trust between countries. The setup of a common set of authentication profiles would support interoperability and trust. If there is a common understanding about the levels of assurance, then interoperability is ensured.

In general, the challenge in defining different assurance levels is the ability to measure the "quality" of different authentication solutions and compare them with each other. Each assurance level describes the degree to which a service provider in an electronic transaction can be confident that the identity information actually represents the entity referred in this information. This is influenced by several organizational factors, such as the registration, issuance and revocation of identities or the record keeping and auditing. Also some technical factors, such as the type or strength of the authentication credentials and protocols are of importance here.

Several approaches to define levels of trustworthiness for authentication mechanisms have been proposed in recent years, indicating the importance of such a concept. IDABC's authentication levels report [IDA07b] consists of the following components:

- four authentication assurance levels, in terms of risk and potential damage in case of abuse
- a definition of registration requirements for solutions at each level
- a definition of authentication requirements for solutions at each level.

The IDABC proposal bases the definition of authentication assurance levels on the consequences of an authentication error and misuse of credentials. The possible risks and possible damages from an abuse of the authentication method, as well as the likelihood of those risks are taken into account. The higher the perceived risk, the higher the level of assurance should be. Lower risk authentication requests require low assurance, whereas higher risk authentication requests require more stringent assurance.

### *Legal Issues*

Legal materials related to eIDs are the EC Treaty defining responsibilities of the Member States and the EU institutions, but also a number of Directives. In particular, since most of the data exchanged in citizen-government interactions are to be considered personal

data, the processing of such data is subject to the Data Protection Directive. Since many Member States use qualified certificates in their eIDs, a number of legal issues are handled by the eSignature Directive 1999/93/EC. Finally, since we target to offer cross-border services, the Services Directive 2006/123/EC is also related.

The above Directives give a common legal basis. Complexity increases, if national laws without community grounds are the basis. Let us give two examples of legal issues that need to be addressed:

- *Identity Numbers*

Many eIDs contain identifiers that are based on, or are equal to, national identification numbers (e.g., Estonian Personal Identification Code, Dutch BurgerService-Number (BSN), Spanish DNI number). In most countries, the use of these numbers is restricted and regulated by law. This in effect means that they cannot be processed in cross-border eGovernment interactions that include storage. Overall, there are significant differences in the Member States regarding (national) identifiers and the restrictions on the use of these numbers.

- *Attributes*

The eIDs in Member States differ in the amount and nature of the attributes they contain. It may be the case that an eID contains only the identifier's BSN (e.g. the Dutch DigiID) or a large number of personal information (as it is the case in Portugal). Whether the attributes present in the eID may be used in pan-European eGovernment services also varies according to the Member States. For some eIDs access to the attributes is locked to guarantee that they can be read only with the holder's consent.

## 12.4 Privacy Considerations

We have already mentioned some aspects of privacy throughout our discussion so far, but here we want to treat this topic separately, as we consider it to be of ultimate importance for the success of any interoperability solution.

First of all, in the transfer of identity information with regard to natural persons, adherence to privacy regulations becomes particularly important. This implies specifically:

- that the user is duly informed of the scope of the transaction, i.e., of which identity information is transferred to the application owner and for which purposes the data will be processed (notice)
- that the application provider does not request or process more identity data than strictly required for the purposes of his application (minimal disclosure)
- that the user is given optimum control over the identity information which is finally transferred to the application owner (control)
- that the user is duly informed about the way in which he can exercise his/her rights resulting from the Data Protection regulations.

Accordingly, privacy violations can emerge both from data collection and data processing. Surveillance and interrogation are threats related to information collection. Aggregation, identification, secondary use such as for profiling and exposure are some of the threats related to data processing. To protect against these threats, current Privacy Enhancing Technologies (PETs) provide anonymity on application layer and support pseudonyms and help users to control access to their personal data.

Allowing users to control access to their personal data is not always easy to provide. For example, the Authentication Process Model described in Section 12.2 follows a federation strategy, which is ISP-centric. That means, for any given interaction between the user and the SP, a back channel authentication process takes place between the SP and the ISP of the user's home country. Consequently, the ISP is aware of the services that the user accesses in another member state and is able to make conclusions on his activities. Linking these activities, the profile that the user keeps in this country can easily be revealed.

An approach that overcomes this problem was described in [CPR09], where the SP informs the user's agent about the identity information required. The user's agent presents that information to the user through a specialized agent, called a claims selector. Should the user instruct the claims selector to release the required claims, it contacts the ISP, which in its turn determines what claims it should issue. Resulting claims are returned to the claims selector, which forwards them to the SP. This way, the link between the SP and the ISP is broken, by the intervention of the user.

## 12.5 STORK

In the considerations made so far it was emphasized that eID interoperability is not just a technical issue. Legal, operational, and socio-cultural aspects build the environment that technology needs as a support. It is important to realize that these legal, operational, and technical aspects are interdependent and they cannot be addressed separately. This complex situation asks for scrutinizing approaches in a sufficiently large real world situation. The goal is to gain confidence and to make sure that issues are made out well before a long-term solution is implemented.

The underlying assumption of STORK is that the national eID infrastructures should not be changed. In fact, these cannot easily be altered, given the enormous investments already made nationally in most EU Member States. Cross-border interoperability shall build on top of the existing infrastructures.

We present the STORK project in the following subsections. Firstly, the six pilot applications are presented. The pilots are the project's core, as they shall point out strengths and weaknesses of approaches and lead to the lessons learned. We continue by discussing the legal issues that have been made out. These in fact are among the main obstacles to cross-border eID use. A discussion of operational aspects follows. This includes a sketch of various national eID approaches and how the different security levels are addressed. Further operational aspects, intervened with legal considerations, are the

concrete interoperability models – also taking liability and data protection aspects into consideration. These considerations led to the concrete interoperability models chosen and implemented by STORK, which are described in a subsection on the technical solutions. This section on STORK is concluded by addressing issues that likely remain open beyond STORK.

### 12.5.1 Pilot Applications

The main objective of STORK is to test its eID interoperability solution in real world cross-border applications. Six such applications have been defined, each characterized by specific requirements:

- Cross-border Authentication platform for electronic services
- Safer Chat
- Student Mobility
- Electronic Delivery
- Change of Address
- A2A services and ECAS integration.

#### **STORK Pilots**

The first pilot *cross-border authentication platform for electronic services* aims at integrating the STORK framework to eGovernment 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 personalized eGovernment services.

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 like it is the basis of the other pilots is less important.

*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, 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.

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 most smartcard based eIDs offer.

To facilitate moving 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.

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 to communicate among themselves and with the 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.

Given the requirements stemming from the pilots, the main use cases STORK has implemented are the natural person authentication and the attribute transfer. The former *authentication* is needed by all pilots and shall be based on unique identification. The latter *attribute transfer* spans various attributes and is needed by Safer Chat (age claim), Electronic Delivery (signed proof of receipt), and Change of Address (address).

### 12.5.2 Legal Environment and Data Protection

Among the first activities that have been carried out by STORK was taking stock of the legal situation in the participating Member States. The purpose was not to create an exhaustive list of legal issues on interoperability, but to provide an analysis that can serve as a framework for the legal requirements for pan-European eID. The exercise relied on several sources. One was a comprehensive study on eID for pan-European Government Services (PEGS) that had been carried out by IDABC in 2007 and was updated in 2009 [IDA09]. Other sources were the *Signposts paper towards eGovernment 2010* [eU05] and the *Roadmap for a pan-European eIDM Framework* [eU06] that have been prepared by the eID ad-hoc group under the i2010 initiatives. Related Directives and national laws have also been analyzed.

On data protection, the main finding was that *“The most important ground to make the processing of personal data across state borders legitimate is unambiguous consent of the data subject (the claimant), because legal obligations (as meant in art. 7(c) [of Directive 93/46/EC]) are unlikely to exist in a pan-European context.”* Thus, consent of the citizen is the basis STORK relies on in its implementation. The analysis also stated that getting consent is not much of a problem, when data is provided by the citizen. When collecting data from attribute providers, the citizen needs to be presented these data too and the citizen has to give consent.

The Signature Directive defines that one anchor of trust that is grounded on an established legal basis is liability related to qualified certificates, as well as its mutual recognition and the recognition of secure signature-creation devices (SSCD) (something that many eID tokens are). As it will be further discussed in Section 12.5.3, qualified signatures and SSCDs represent the highest assurance level used in STORK.

The Services Directive was addressed in detail by the Large Scale Pilot SPOCS<sup>1</sup>, but it is also important for STORK, as it obliges Member States in its Article 8 to allow for electronic applications. Identification is an important enabler.

---

<sup>1</sup> Simple Procedures Online for Cross-border Services ([www.eu-spocs.eu](http://www.eu-spocs.eu))

Concerning the national laws restricting the use of national identification numbers, an option that has been suggested in STORK is to derive a new identifier from the national number using one-way transformations, which in its derived form can be used in cross-border interactions. The system implemented by Austria for sector-specific identifiers has been stated as a model.

Finally, an aspect that needs to be considered in any project is the following question: In case something goes wrong, who is liable? If the eID is based on qualified certificates, the Signature Directive gives a sound basis for liability related to these certificates. The legal analysis then states: “*In the case where no qualified certificates are used or available, liability issues in pan-European eGovernment services are much more complex and need further analysis.*” In fact, a liability regime is hard to establish between Member States, as it may lead to state contracts and involve parliamentary processes.

### 12.5.3 Operational aspects and Security Levels

STORK operates in an environment, which is characterized by a heterogeneous ecosystem in various dimensions. The overview in Section 12.3.2 showed that eIDs can vary in the technical security levels offered. STORK developed a Quality Authentication Assurance (QAA) scheme to map the Member States’ eIDs to a common scheme.

The QAA scheme is based on the IDABC proposal [IDA07b], which we presented in Section 12.2. It is also compatible with the Liberty Identity Assurance Framework [LAP07]. A similar approach has been taken by NIST SP 800-63 [SP800-63], which defines four assurance levels with similar criteria, so that a mapping should be possible.

An eID’s STORK QAA level is determined by both requirements on the *registration phase* and requirements on the *electronic authentication phase*:

- For the registration phase the quality levels of the *identification procedure*, the *credential issuing procedure*, and the *entity issuing the credential* are assessed. Factors used inter alia are what assertions about the identity of a claimant are presented and how these assertions are validated (quality of the identification procedure), how the identity of the claimant is verified ranging to physical presence of the claimant (quality of credential issuance), and which level of government agreement, supervision or accreditation the organizations involved have (quality of the entity issuing the credential).
- For the electronic authentication phase the *robustness of the credential* and the *security of the authentication mechanism* are assessed. This inter alia distinguishes between username and passwords, on-time password generators, software certificates, and qualified certificates that are based on hardware tokens or SSCDs (robustness of the credential). A further factor is whether the protocols protect against guessing, eavesdropping, hijacking, replay, or man-in-the-middle attacks (security of the authentication mechanism).

The STORK QAA system defines four levels that range from *low or no assurance* (STORK QAA level 1) to *high assurance* (STORK QAA level 4). The levels have been defined so that a qualified signature, as defined in the Signature Directive, meets QAA level 4, although

a qualified signature is not a necessary condition to reach QAA level 4. This gives some technology neutrality. An eID needs to meet the highest quality levels for both the registration phase and the electronic authentication phase to reach the highest overall level (QAA level 4). If the quality of either phase is lower, the overall QAA level degrades.

The concept followed by STORK is that the service provider requests a certain QAA level. The service provider might base this decision on legal requirements or a risk assessment. Any eID, which meets at least the level requested by the service provider, can be used to access the service.

The security of the eID token is an important, but not the only aspect that determines the overall system security. The secure implementations of the interoperability components are discussed in Section 12.5.4. Their secure operation and their secure integration into the service providers' environment are equally important.

STORK therefore defined a set of security principles and best practices to follow. The methodology followed was to carry out a threat analysis, derive security objectives that counter these threats, and define security functions that implement these objectives. Technical security recommendations resulted from this process. As public sector service providers usually already follow security best practices – either based on international or on national standards – and as imposing a specific approach touches Member State sovereignty, a pragmatic approach has been followed: Both determining the QAA level of an eID credential and the secure implementation and operation of the components, have been declared by the Member States in a self-assessment.

A fundamental operational question was how an interoperability layer can be achieved. As we mentioned before, since the eID ad-hoc group established under the i2010 initiative, two models prevailed for interoperability and STORK aimed to pilot both: the middleware model and the proxy model:

- In the *middleware model* a citizen directly authenticates at the service provider.
- In the *proxy model* authentication is delegated to a separate entity.

In the middleware model the service provider remains responsible both from a data protection perspective (as the data controller) and from an official liability perspective (no responsibility and thus no liability is shifted to a third party). The citizen-to-service-provider relation is just extended to foreign citizens. Each service provider however needs components (middleware) that can handle foreign eID tokens.

The proxy model centralizes integration of eID tokens by carrying out the authentication for the service provider. This releases the service provider from any integration of foreign eID tokens, but introduces an intermediary – the proxy – in data protection aspects (being a data controller or processor) and a liability shift at least for the authentication process. As a single supranational proxy instance was out of question, STORK decided in favour of one proxy service per Member State that handles its own eIDs and service providers.

The selection of which model fits best a Member State gets into its administrative culture and existing eID infrastructure. Austria and Germany have chosen the middleware

approach, which is also considered by France. The other Member States opted for the proxy approach. Their technical implementation and how interoperability is achieved across the models is discussed in the next section.

### 12.5.4 Technical Solutions and Interoperability Models

The *proxy* and *middleware* interoperability models have initially been discussed in a technology-neutral approach, not deciding on or not precluding any specific protocol. Generic process flows for authentication, attribute transfer, and electronic signature and certificate validation have been developed to visualize the basic cross-border processes.

In STORK the proxy is referred to as Pan-European Proxy Service (PEPS), a term introduced by a common specifications effort of the IDABC eID interoperability study [IDA07a]. Middleware (MW) refers to the combination of software used by the client to interface with the eID token and software used by the service provider to integrate eID into their processes – the latter software component referred to as *SP-ware*.

Figure 12.2 depicts all components required in a STORK-enabled scenario. The components that are Member State specific are coloured grey, while the common STORK components are coloured black [Sto09]. In what follows, we will explain the functionality and interconnectivity of these components for different processes.

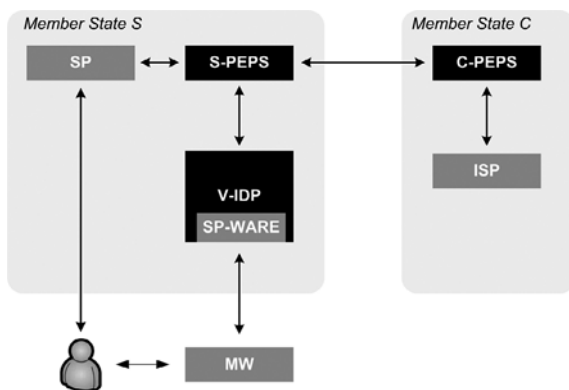
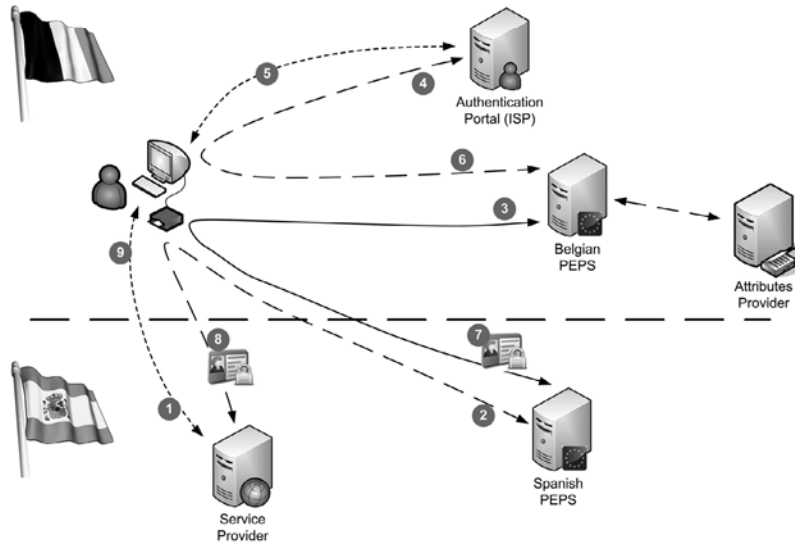


Figure 12.2 STORK System Overview

#### *Pan European Proxy Service*

A Pan-European Proxy Service (PEPS) serves two functions: On the one hand, it carries out the authentication and attribute collection for a Member State's eIDs and attribute providers. It asserts its citizen's eID and attributes to foreign Member States. We refer to these functions interfacing to a Member State's citizens as *C-PEPS*. The second function of a Member State's PEPS is asserting foreign eIDs to the service providers established in its territory. This function is referred to as *S-PEPS*. Splitting the functions is sensible, as in a certain transaction, a PEPS either acts as *S-PEPS* (when a foreign citizen accesses a



**Figure 12.3** Authentication example based on PEPS

domestic service provider) or as C-PEPS (when a citizen accesses a foreign service provider). A circle of trust is established between the service providers and the S-PEPS, foreign Member States need to trust the C-PEPS.

To give an example of the process in the pure PEPS model, i.e., when a citizen from a “PEPS country” accesses a service provider from another “PEPS country”, let’s assume a Belgium student, who wants to enrol to a Spanish university. Then the process, also depicted in Figure 12.3, is as follows:

- 1) The Belgian student accesses the Spanish university’s campus management system via a web browser. She selects to authenticate as a Belgian citizen using STORK.
- 2) The Spanish university redirects the student’s browser to the Spanish PEPS as its trusted entity in the STORK framework and requests authentication at a certain QAA level. Let’s assume that the service needs QAA level 3 and that the service also needs the student’s name as an attribute. Both the QAA-request and the attribute-request are embedded into the authentication request.
- 3) The Spanish PEPS (actually its S-PEPS part) redirects the authentication request to the Belgian PEPS being the trusted foreign component in the STORK framework. The Spanish PEPS digitally signs the request.
- 4) The student’s browser is redirected now to the Belgian PEPS (actually its C-PEPS part), which authenticates the Belgian student. Authentication can be done at the PEPS itself or can be delegated to the authentication portal of an identity service provider. This depends on the national eID infrastructure.
- 5) The student presents her eID card and enters the authentication PIN. As the Belgian eID is QAA level 4, the required eID authentication level is met. The name as requested attribute can also be provided, as it is stored on the Belgian eID. A citizen’s

unique identifier is needed – let's assume for simplicity that the Belgian national RNR-number is used.

- 6) Prior to further processing, the student needs to give consent to forward the data to the service provider. All relevant data, i.e. the identifier, the student's name and the Spanish university as recipient are displayed.
- 7) After having authenticated the student and having got her consent, the Belgian C-PEPS creates an authentication response that contains the identifier, the QAA level and the name as requested attribute. The authentication response is signed by the Belgian C-PEPS and returned to the Spanish S-PEPS.
- 8) The Spanish S-PEPS verifies the Belgian C-PEPS's signature, digitally signs the authentication response itself, and returns it to the Spanish university.
- 9) The Spanish university verifies the Spanish S-PEPS's signature and grants the student access to the campus management system.

In its common specifications, STORK has defined the protocols for the cross-border transactions. The national eID infrastructure is not changed. While Member States may decide to use STORK protocols also nationally, the communication between the service provider and the S-PEPS (Step 2 and Steps 8 and 9) or between identity service providers and the C-PEPS (Step 4) usually is a national protocol.

The trust relationship in the pure PEPS model is between the service provider and the S-PEPS, and between the PEPSs. Note, that the authentication responses are re-signed at the PEPS. This is because the service provider has a trust-relationship only with its S-PEPS, but none with the foreign C-PEPS. It is required that the PEPSs are well protected to prevent attackers from taking over a PEPS and creating false authentication responses. Holder-of-the-key protocol bindings could be used to prevent man-in-the-middle attacks, but, due to lack of implementation of such bindings in widely used browsers, this is not supported in the pilots.

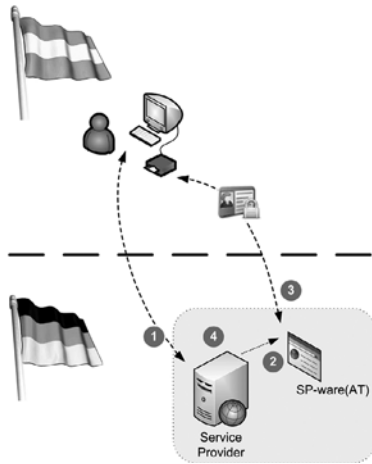
In our example we assumed that the Belgian national identifier *RNR-number* is transferred cross-borders. As discussed in Section 12.3.2, using national identifiers across borders may not be possible. STORK defines protocols to apply the one-way functions discussed as a solution for those cases. Identifiers can be derived per receiving Member State up to the granularity of service-specific identifiers. Whether these functions are used, depends on the national situation.

#### *The middleware model*

The pure middleware model, i.e. a citizen from a “middleware country” accessing a service provider in another “middleware country”, usually is based on an infrastructure where the service provider integrates eID without intermediaries. A middleware component, previously referred to as *SP-ware*, is used. In STORK the national SP-wares are combined so that the service provider replaces the existing national SP-ware by an STORK-enhanced SP-ware. Taking an Austrian migrant worker accessing a German eGovernment portal as an example, the process is as follows:

- 1) The Austrian accesses the German portal and selects to authenticate as an Austrian citizen. Let's assume a QAA level 4 is needed. As in the previous PEPS example, we assume that the service needs the name as attribute.
- 2) The German portal activates the Austrian part of its SP-ware by creating an authentication request asking for a QAA level 4 and the name.
- 3) The SP-ware asks the citizen to enter his citizen card. In the Austrian case this can either be a smartcard or a mobile phone eID, both supporting QAA level 4. The citizen then authenticates, the name is stored on the citizen card.
- 4) Consent by the citizen is given as in the domestic case.
- 5) The SP-ware verifies the authentication, and creates the authentication response. This may be transformed to a protocol supported by the service and the citizen is granted access.

The pure middleware scenario is illustrated in Figure 12.4. The fact that the SP-ware is operated by each service provider is indicated by a box. The middleware providing access to the eID token is either installed at the citizen's PC, or included in the SP-ware using minimum footprint technologies (e.g. applets).



**Figure 12.4** Authentication example based on middleware

Similar as with the PEPS model, the existing national protocols remain unchanged, even though convergence to common middleware protocols is a desire. Thus, in the general case the communication between the foreign eID token and the SP-ware (Step 3 above) and the one between the service and the SP-ware (Step 5) are not covered by the STORK common specifications.

As the SP-ware is operated under the service provider's responsibility, no liability shifts or third party processing are given. Note, that in the pure middleware model just attributes stored in the eID token are supported. The basic assumption is that no intermedi-

aries, such as a third-party attribute provider, are introduced into the citizen-to-service-provider relationship. End-to-end security between the citizen's domain and the service provider's domain is the objective.

#### *The PEPS-middleware model*

While the *pure PEPS model* and the *pure middleware model* are rather straightforward, as the same basic assumptions and concepts are applied at both ends of the cross-border transaction, the situation becomes a little tricky, if the crossovers are to be handled, i.e. a citizen from a "middleware country" accessing a service provider from a "PEPS country" and vice versa. Here, depending on the case, either the citizen using a middleware approach communicates with a component hosted under responsibility of a PEPS, or the service provider in a middleware country directly accesses a PEPS:

- The notion of a *virtual identity provider (V-IDP)* has been introduced for cases where a citizen from a "middleware country" accesses a service provider from a PEPS country. The V-IDP is hosted under responsibility of the PEPS and hosts the various SP-ware implementing the protocols with the client eID middleware. The PEPS interfaces with the V-IDP as if it were a single identity service provider. If the citizen accesses the service provider, it selects authentication as a foreigner. The service provider redirects to its S-PEPS (as in Steps 1 and 2 in the pure PEPS scenario above). The S-PEPS, instead of redirecting to a foreign C-PEPS, redirects to its V-IDP. The V-IDP activates the SP-ware and authenticates the citizen (as in Steps 3 and 4 in the pure middleware case). The SP-ware returns the authentication response to the S-PEPS which digitally signs it and returns it to the service provider (as in Step 5 in the pure middleware case and Steps 8 and 9 in the pure PEPS scenario). This scenario is shown on the left side of Figure 12.5 for an Austrian citizen accessing a Spanish service provider.
- If a citizen from a PEPS country accesses a service provider from a middleware country, she selects authentication as a foreign citizen using STORK (as in Step 1 in the pure middleware model). Then, the SP-ware, instead of directly interfacing to a middleware (Step 2 in the pure middleware model), redirects to the foreign C-PEPS that carries out the authentication (Steps 4 to 7 in the pure PEPS model). The right side of Figure 12.5 illustrates this for a Belgian citizen and a German service provider.

Both situations keep fundamental principles at both ends intact: The "PEPS country" has decoupled the potential complexity of foreign eID tokens via its PEPS – at the price of hosting a V-IDP as an additional component. The "middleware country" does not need to operate central components that rise privacy connotations of government being capable of tracking citizen movements – at the price of end-to-end security being terminated at a foreign PEPS, not at the citizen environment or the service provider.

In defining the protocols, STORK succeeded to design the interface specifications so that the V-IDP to S-PEPS protocols and the SP-ware to C-PEPS protocols are the same as the C-PEPS to S-PEPS protocols. Thus, the STORK architecture may technically be looked at as a single interoperability framework that either is deployed in a centralized approach (PEPS), or in a distributed environment (middleware).

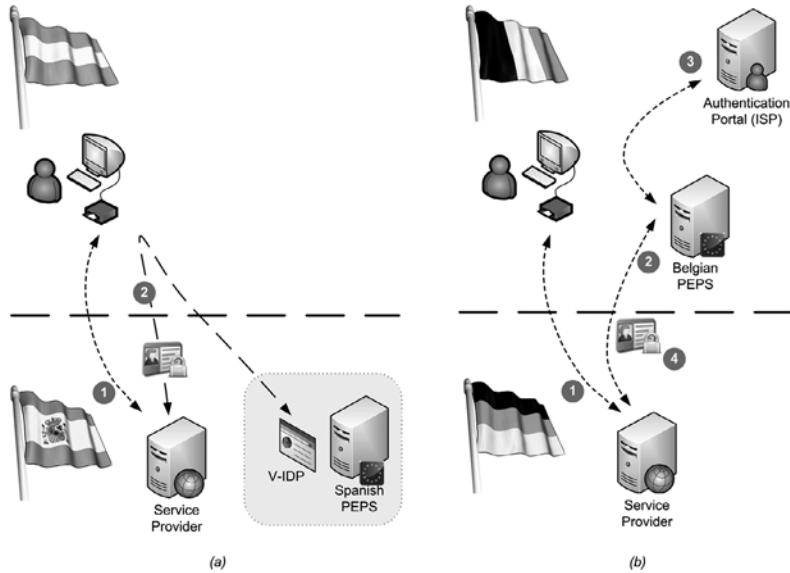


Figure 12.5 Combined PEPS-middleware model

At the beginning of this sub-section we have discussed that the processes had initially been defined technology neutral. Different protocols such as the Security Assertion Markup Language (SAML) or the Web Services standards family (WS-\*) could have fulfilled the requirements of the generic processes described above. A survey carried out amongst the participating Member States showed that eleven out of fourteen Member States either already used SAML (seven Member States) or planned to implement SAML (four Member States). As a consequence, SAML 2.0 has been chosen in the STORK common specifications. The Web Browser single-sign on (SSO) profile [OASIS05b] and HTTP POST binding [OASIS05a] have been selected. The latter for data protection reasons, as all communication is transferred via the user's browser.

## 12.6 Open Issues and Future Directions

STORK achieved a lot. It however would be naïve to assume that all aspects of a multi-disciplinary topic as complex as cross-border eID interoperability can be solved in its entirety by a single project. At time of writing this chapter the STORK pilots just launched. Thus any lessons learned are preliminary and do not yet take the users' and application providers' feedback into consideration.

The technological part of STORK shows that the chosen solutions are feasible, since even in the early stage, the pilots are operational. The integration into service providers worked and the cross-border testing carried out gives confidence in the common specifications that have been developed and implemented. This integration covered both *proxy* and *middleware* models, as well as its combinations.

### 12.6.1 Application Integration

STORK is embedded into an ecosystem of comparable Large Scale Pilots that address other key policy areas. This includes the projects epSOS on eHealth, PEPPOL on eProcurement, or SPOCS on the Services Directive. eIDs are playing an important role in several of them. A challenge being addressed by continuous collaboration efforts is that basic elements can be applied to each other. eIDs as addressed by STORK are such a basic element. Intense collaboration is done by the *STORK meets epSOS (STeps)* activity that aims at testing STORK results in the eHealth domain. The purpose is to carry out interoperability field tests to prove that STORK can be applied to domains other than the eGovernment domain that STORK primarily has been focused on in its own pilot applications.

The main focus of the STORK pilots was on eGovernment applications. To foster eID take up, synergies with private sector applications and eBusiness may be sought. This has not been covered by STORK and may be challenging on scalability, international relations beyond the EU, or data protection in relation to identifiers.

### 12.6.2 Representation and Mandates

An aspect that is important for eGovernment processes, but has not been addressed by STORK, is representation and mandates. STORK is limited to eID of natural persons. Many processes are however entered by a legal person represented by a natural person, e.g. the CEO representing a company. Lacking widespread national solutions,<sup>1</sup> representation and mandates remain to be solved after STORK.

### 12.6.3 Mutual Recognition of Foreign eIDs

What STORK could not solve in its limited timeframe, and in fact did not claim to solve, are legal issues in relation to mutual recognition of foreign eIDs. Lacking a community framework such as given with the Signature Directive, unilateral activities are to be relied on. An already established legal basis for recognition of foreign eID – as e.g. given in the Austrian eGovernment Act – is the rare exemption. The need of a vehicle to support mutual recognition is therefore recognized in the European Commission's Communication on the Digital Agenda [Com10] that states in its Key Action 16: *Propose by 2012 a Council and Parliament Decision to ensure mutual recognition of eidentification and eAuthentication 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).*

### 12.6.4 User-centric Identity Management

The so-called user-centric identity management systems, which focus on the users' rather than the service providers' perspective, have increasingly gained popularity in

---

<sup>1</sup> IDABC Study on eID Interoperability for PEGS (2009) states that out of 32 countries just two – Austria and Belgium – have a mandate/authorization management that can be called systematic.

the past few years. This approach lets users choose, for example, what personal data to disclose under various conditions, and which credentials to present in response to authentication or attribute requests.

User-centric identity management – also referred to as Personal Identity Frameworks (PIF) or Identity 2.0 – focuses on user empowerment in sharing personal information and self-determination in establishing relationships with relying parties. User-centricity distinguishes itself from other notions of identity management by emphasizing that the user maintains control over “what, where, when, and to whom” a user’s identity attributes are released.

In user-centric identity architectures, individuals present the credentials of their choice for authentication at online services. Instead of the vendor-to-vendor systems integration and trust contracts of federation, service providers or relying parties authenticate a visitor by relying on the identity services of an identity service provider of the visitor’s choice. Relying parties may not accept all identity service providers, but in general, the choice of who authenticates the identity lies with the user.

There are already some developments towards the realization of the vision for a personalized identity ecosystem. The STORK architecture in its conception and goals can provide a basis, on which the government-controlled identity registries can be accessible, not only for cross-border eID interoperability for authentication to eGovernment services but for a large scope of possible transactions that would require data verification against authoritative sources. Some of the services envisaged within the INDI ecosystem may soon become offers from government agencies.

## 12.7 Conclusion

At the same time as more European states develop electronic identity cards for identity management, the European Union has been pushing its interoperability agenda as part of its aim to support the mobility of EU citizens and develop for them seamless provision of services, no matter where their location in Europe is. Our aim in this chapter was to develop an understanding of the term interoperability for eIDs across Europe. We argued that the success of an interoperable system would involve not only technical, but also legal and regulatory components, as well as behavioural and cultural aspects. In the second part of the chapter, we presented the solutions proposed by STORK and gave concrete examples from the test pilots currently being deployed. The future looks even more challenging, as interoperability should be extended to integrate private sector applications and eBusiness, as well as cover a more user-centric approach of identity management, according to the current trends.