Challenges of eID interoperability: The STORK project

Herbert Leitold

A-SIT, Secure Information Technology Center - Austria,
Inffeldgasse 16a, 8010 Graz, Austria
Herbert.Leitold@a-sit.at

Abstract. Secure means of identification and authentication is key to many services such as in e-government or e-commerce. Several countries have issued national electronic identity (eID) infrastructure to support such services. These initiatives however have often emerged as national islands; using eID cross-border has not been on the agenda in most cases. This creates electronic barriers. The Large Scale Pilot STORK aims at taking down such barriers by developing an interoperability framework between national eID solutions. The framework is tested in six concrete cross-border applications. In this paper, an overview of the STORK architecture and the pilot applications is given.

Keywords: electronic identity, eID, STORK

1 Introduction

Who one is on the Internet is becoming an issue once sensitive or valuable data is being processed. Services that can be as diverse as filing a tax declaration online, inspecting one's electronic health record, or accessing a bank account online need secure means of unique identification and authentication. To address the need for secure electronic identities (eID) in e-government, many states launched national initiatives. A study carried out by the European Commission in 2007 and updated in 2009 showed that 13 out of 32 surveyed countries issued government supported eID cards, eight countries have mobile phone eID solutions, and 22 also have username/password approaches [1].

The national eID infrastructure often emerged in isolation, developed only to meet sectorial, regional, or national requirements. Using the eID tokens – whatever the technological implementation is (card, mobile phone, etc.)– across borders was no priority for most states. In the Internal Market this can be a significant barrier for prospering of electronic services. The European Union has recognized that deficiency early: In the Ministerial Conference of Manchester 2005 a political agreement has been reached that European citizen shall benefit from "*secure means of electronic identification that maximise user convenience while respecting data protection regulations*" within a five year timeframe [2]. The ministerial declaration also addressed the national responsibility and competences: "*Such means shall be made available under the responsibility of the Member States but recognised across the*

EU." Concrete Action plans followed the declaration [3] and the discussion between Member States and the European Commission on eID interoperability intensified.

A project as complex as to make heterogeneous national eID infrastructure interoperable, however, cannot be carried out just from pure desk research. Getting concrete experience in piloting the approaches in real world applications is advisable before making policy decisions. Such piloting shall make legal, operational or technical hurdles visible when deploying the concepts in practice. The project STORK[1] is such an attempt of piloting approaches. The project and its findings are described in this short paper.

2 Project Overview

STORK has been launched when fourteen EU and EEA Member States gathered together to form a consortium to bid for a Large Scale Pilot (LSP) grant under the European Commission Competiveness and Innovation (CIP) in the Information and Communication Technology Policy Support Programme (ICT-PSP) stream [4]. The STORK consortium has been extended to 17 partners in 2010[2].

The STORK LSP started as a so-called "type A LSP" in June 2008 and lasts for three years until May 2011. The idea of type A LSPs is to advance European key ICT policy areas by large scale projects driven by the Member States themselves and co-funded by the European Commission. Four such key areas have been defined in the CIP ICT-PSP Programme, eID being one key area that finally resulted in STORK[3].

The STORK project structure can be divided into three successive phases:

1. First came a taking stocks exercise. The purpose was to get in-depth insight into the national eID systems that need to be incorporated into the STORK eID interoperability framework. Legal, operational, and technical aspects have been investigated.
2. The second phase was to develop and implement common technical specifications. This phase resulted in the STORK eID interoperability framework. Its results are described in the next section 3.
3. As the proof of the pudding is in its eating, the interoperability framework has been deployed in several national production applications. Six such pilots have been defined. The pilots are sketched in section 4.

At time of writing this short paper, the first two phases have been completed and the third phase "piloting" has been launched. Deliverables – both specifications and its reference implementations – are in the public domain and can be accessed via the project web[1].

---

[1] STORK: Secure Identities Across Borders Linked, Project co-funded by the European Commission under contract INFSO-ICT-PSP-224993; https://www.eid-stork.eu

[2] The project started in 2008 with Austria, Belgium, Estonia, France, Germany Iceland, Italy, Luxemburg, Portugal, Slovenia, Spain, Sweden, The Netherlands, and United Kingdom. The 2010 extension included Finland, Lithuania, Norway, and Slovak Republic

[3] The three other key policy areas under ICT-PSP and STORK's sibling LSPs are eHealth (epSOS), electronic procurement (PEPPOL), and the Services Directive (SPOCS)

3 Architecture and Interoperability Models

The first issue the STORK project had to address was the heterogeneous nature of eID in Europe. One might think of eID being an ID card amended by smartcard or signature functions, an online banking access certificate, or non-PKI solutions such a SMS transaction numbers or simply a username password combination. All these eID technologies are deployed to access national or regional e-government services in Europe. Given the various technical implementations, the question of how to trust the other's systems comes upfront. The road followed by STORK was that the various eIDs are categorized into quality classes. This resulted in a Quality Authentication Assurance (QAA) scheme to map the Member States' eIDs to a common scheme. The QAA scheme is based on an IDABC proposal [5] and also compatible with the Liberty Identity Assurance Framework [6].

The STORK QAA model defines four levels ranging from "QAA-1: low assurance" to "QAA-4: high assurance". Assessing the QAA-level takes both the technical security of the eID token and the technical and organizational security of the issuance process into consideration. The model was developed so that secure signature-creation devices (SSCD) to create qualified electronic signatures and the issuance of qualified certificates compliant with the EU Signature Directive [7] meet the highest level QAA-4. A rationale is that legal recognition of qualified certificates is already given throughout the EU. It was felt that no higher requirements than for qualified signatures are needed for eID. The QAA-model is however defined, so that qualified certificates or SSCDs are no necessary condition to reach QAA-4.

Recognition of eID across borders and data protection are the two main legal issues to be addressed. The former – legal recognition of eID – is the scare exemption in Europe. While recognition of qualified certificates is given with the Signature Directive, just few Member States such as Austria yet recognize foreign identifiers and eID tokens. On the second issue – complying with data protection requirements – the project came to the conclusion that explicit user consent is the proper basis for legitimacy of cross-border eID processing. The user giving consent does not rule out all legal obstacles, as e.g. some states defined protection of national identifiers in a way that its cross-border use is prohibited[4]. The STORK project is however not meant to solve complex legal issues. Identifying and documenting legal issues is however a main purpose of the LSPs in order to prepare for sound policy actions beyond the LSP lifetime.

The main goal of the project STORK has been to develop common technical specifications for a cross-border interoperability framework. Two conceptual models "middleware" and "proxy" are covered and piloted:

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

In the middleware model the service provider (SP) 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-SP relation is just extended to foreign citizens. Each SP needs components

[4] This can e.g. be overcome in STORK by cryptographically deriving other identifiers

(middleware) that can handle foreign eID tokens (we call that service-provider-side middleware "SPware"). The user experience is as if she would access a SP in her home country, as the components to recognize her eID are integrated to the SP.

The proxy model centralizes integration of eID tokens by carrying out the authentication for the SP. This releases the SP 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. A single supranational proxy instance was out of question, STORK decided in favor of one proxy service per Member State that handles its own eIDs and SPs. We refer to the proxy as Pan-European Proxy Service (PEPS). Two components are needed: The S-PEPS is located in the country of the SP. The C-PEPS is located in the citizen country. The process is as follows: If a foreign citizen accesses a SP, the SP delegates authentication to the S-PEPS. The S-PEPS redirects the citizen to her home C-PEPS that carries out authentication of its citizens. Successful authentication is asserted back to the S-PEPS, that finally is asserting that back to the SP.

A remaining component in the architecture is referred to as virtual identity provider (V-IDP). This has been invented to bridge between the two conceptual models middleware and proxy. In a "middleware country" no central infrastructure (PEPS) is installed for privacy reasons. Thus the V-IDP has been introduced as a decentralized bridge. The V-IDP is installed either at the S-PEPS (for citizens from middleware countries accessing a SP in a PEPS country) or at the SP in a middleware country.

The overall scenario is illustrated in figure 1. The STORK common specifications defined the cross-border protocols between the C-PEPS, S-PEPS and V-IDP (that are indicated as black boxes in figure 1). Established national protocols with the SP or Identity Service providers may remain, as STORK does not impose changes in the established national infrastructure.

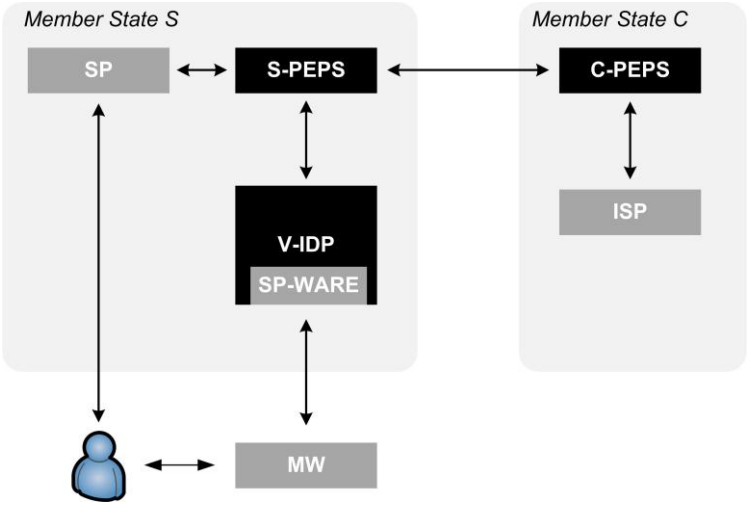

Fig. 1. STORK overall architecture showing both the "PEPS model" and the "middleware model"

For the common specifications STORK relied on existing standards. The Security Assertion Markup Language (SAML) version two has been chosen. A browser single sign on profile [8] using an HTTP post binding has been chosen. Amendments to the existing standards have been kept to a minimum. Such amendments are e.g. needed to communicate the QAA levels a SP needs as a minimum to provide service.

4 Pilots

The project has originally defined five pilots, each addressing a specific challenge related to eID. A sixth pilot has been defined in the course of the project. The six pilots are:

1. Cross-border Authentication Platform for Electronic Services
2. Safer Chat
3. Student Mobility
4. Electronic Delivery
5. Change of Address
6. A2A Services and ECAS integration

The main function needed in each pilot is authentication of the user. The first pilot *Cross-border Authentication Platform for Electronic Services* aims at integrating the STORK framework to e-government portals, thus allowing citizens to authenticate using their electronic eID. The portals piloting in STORK 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.

A specific challenge when deploying eID widely is that the strong identification that is usually needed in e-government is not necessary in all cases and sometimes even undesirable. Think e.g. of users that pseudonymously want to communicate in the Web. In the *Safer Chat* pilot juveniles shall communicate between themselves safely. The pilot is being carried out between several schools. The specific requirement is that in the authentication process the age group delivered by the eID is evaluated to grant access. Unique identification that is the basis of the other pilots is less important.

Student Mobility supports exchange of university students, e.g. under the Erasmus student exchange program. As most universities nowadays have electronic campus management systems giving services to their students, STORK shall be used to allow foreign students to enroll 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. Enrolment in university however usually needs accompanying documentation in addition to eID, such as transcripts of records. These are often not available electronically. A pre-enrolment process is piloted where the student is preliminarily granted access to the campus management system until the accompanying evidence is presented.

The fourth pilot's *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 the qualified signature functions that most existing smart-card based eIDs have.

To facilitate moving house across borders, the pilot *Change of Address* has been defined. In addition to authentication, the pilot has transfer of attributes, i.e. the address, as a specific requirement. This extends the other pilots by addressing attribute providers that may be different from the identity providers.

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.

Conclusions

STORK has brought seventeen EU and EEA Member States together to define an electronic identity (eID) framework to support 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 establishes 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 (SP). 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 defined to test the interoperability framework in real world environments. At the time of writing this paper, all six pilots have been launched and are operational. This gives confidence in the technical results. The piloting period of a few month is however too short to give sound results on user satisfaction, pilot stability, or protocol robustness. Such results are expected at the end of the piloting phase mid 2011.

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 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);*" [9]. Achieving such legal recognition together with the technical infrastructure that has been developed by STORK is expected a major leap on seamless eID use in Europe.

References

1. IDABC: Study on eID Interoperability for PEGS, European Commission, December 2009. http://ec.europa.eu/idabc/en/document/6484/5938/
2. Ministerial Declaration approved unanimously on 24 November 2005, Manchester, United Kingdom.
3. European Commission: i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, COM(2006) 173, 2006.
4. Project STORK: Secure Identities Across Borders Linked, INFSO-ICT-PSP-224993; https://www.eid-stork.eu
5. IDABC: eID Interoperability for PEGS - Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms, 2007.
6. Liberty Alliance Project: Liberty Identity Assurance Framework, 2007.
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. OASIS: Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, 2005.
9. European Commission: A Digital Agenda for Europe, COM(2010) 245, 2010