Federating e-identities across Europe, or how to build cross-border e-services

# Federating e-identities across Europe, or how to build cross-border e-services

Diana Berbecaru[1], Antonio Lioy[1], Marco Mezzalama[1],
Giorgio Santiano[2], Enrico Venuto[2], Marco Oreglia[2]

*[1]Dip. di Automatica e Informatica*
*[2] Integrazione Processi e Sistemi Informativi*
*Politecnico di Torino,*
*Corso Duca degli Abruzzi 24, 10129, Torino, Italy*
*first.last @ polito.it*

*This work discusses the main challenges and requirements of technical and legal authentication interoperability in e-services involving organizations from different countries. We present the Stork cross-border authentication framework that satisfies these requirements by establishing interoperability between existing European national eID infrastructures in a federated manner. As a sample application, we present the pilot for Student Mobility that has been developed to evaluate and demonstrate the functionality of the Stork authentication framework.*

## 1. Introduction

During the last decade a lot of effort has been spent to permit on-line execution of several public administration tasks, to reduce costs and save time. Examples are obtaining marital status, birth certificates, or residence attestations or submitting income tax declarations or paying bills online.

Typically, to access an on-line public or private service (e.g. offered by universities, public offices or private companies), a citizen needs first to register directly with the entity providing the service, named the *Service Provider (SP)*. During the registration phase, the SP requires and stores several attributes associated with the citizen (e.g. name, surname, address, age) as well as his unique national identifier, like fiscal code or social security number. The SP must then use additional mechanisms to check that the asserted attributes correspond to the identity claimed by the user, for example by sending via surface mail part of an access password to his home address. Also at registration time, the SP creates and associates the citizen to his credentials (e.g. username and password) that can later be used for authentication purposes.

Credentials come in various forms; apart from the trivial reusable passwords, higher security levels may be obtained by using one-time passwords and cryptographic tokens (like smart-cards). Tokens often contain identification data (e.g., photo or biometric data) and user profile data (e.g., the user ID inside an

organization) in addition to the base cryptographic material (e.g., a digital certificate and the corresponding private key). These tokens are used for authentication and/or digital signing purposes, and are considered more secure than authentication based on username and passwords.

Note that in this simple model, the "producer" of the user profile is also its "consumer", as the SP itself implements the services requiring the authentication credentials created upon user registration. As a consequence, very often the credential issued by one provider is not automatically recognized by other SPs. Thus nowadays users end up with several different credentials to access various e-services: this creates confusion, opens the way to various attacks, and makes difficult the control of personal data.

Since the above model is costly and inefficient both for users and SPs, the *federated identity management (FIM)* model has been proposed in recent years, allowing users to register and authenticate once and then access various resources across several different domains. In this model, the user registers his identity or profile with one organization (called the *Identity Provider, IDP*), yet manages to access the services offered by other SPs without any further registration. User profiles maintained by one organization can be trusted by another organization, provided that the two organizations established a relationship, called also a "Circle of Trust". Several different FIM solutions have emerged over the last couple of years such as Microsoft's Passport [Mic], Liberty Alliance [Liberty], Security Assertion Markup Language (SAML) [OASIS], Cardspace [Infocard] and OpenID [OpenID].

Using FIM in practice, especially in cross-border scenarios, is not only a matter of technology. As the number of IDP and SP increases, the number of trust relationships to be established and maintained becomes quickly unmanageable. Moreover, as explained in [ENISA], when the IDP and the SP belong to different countries (as in a cross-border authentication scenario, where the SP is in country B whereas the IDP is in country A), the SP is actually governed by different laws and business rules than the ones holding for the IDP. Moreover, the IDP and the SP might even use different technologies which may be incompatible [Arora].

In a converging European society, missing interoperability between national *electronic identity (eID)* infrastructures threatens to compromise the success of electronic cross-border services. The European Commission has therefore launched several large scale pilots to address the key issues of technical and legal interoperability of electronic identities to facilitate citizens' access to e-services across the EU. These initiatives are explicitly mentioned in the e-Government action plan [ECeGov] as enablers of a single European digital market, which is one of the main goals of the European Digital Agenda [ECDigitalAgenda].

To overcome the eID interoperability issues and facilitate secure cross-border authentication, the European project Stork [Stork] implemented a pan-European infrastructure which allows cross-border recognition of national eID solutions. It is important to note that Stork is not introducing any new type of authentication token or registration procedure, rather it uses what is already established in each European country as a legally valid eID. These various eIDs

are mapped to one of four assurance levels defined in Stork to express the reliability of the authentication credentials and registration process.

To validate this approach, Stork is running various cross-border pilots. We'll describe here the Student Mobility application that allows citizens from several EU countries to use their own national eID for on-line application at various universities, including the Politecnico di Torino in Italy. For Italian citizens, this permits the use of various eID, including the CNS (National e-Services Card), CRS (Regional e-Services Card), and CIE (Electronic Identity Card).

The remainder of this paper is organized as follows: Section 2 gives an overview of the basic FIM concepts, Section 3 presents the Stork framework and its operation for a generic cross-border e-service, Section 4 describes the Stork Student Mobility pilot, and Section 5 draws the conclusions.

## 2. Basic FIM Concepts

Whenever a human is involved in identity interactions, the federated model involves four logical components [Maler]: the user, the user agent (UA, such as a browser or other software application running on a PC, a mobile phone or any other electronic device), the SP, and the IDP (typically a web site that authenticates the users by using credentials such as usernames and passwords or digital certificates).

The main protocols proposed so far for FIM implementation are: OpenID, SAML, which ties into the Liberty Alliance Identity Web Service Framework standard, and the Identity Selector Interoperability Profile specification (often referred as InfoCard) underlying Windows Cardspace. The salient feature of most of these protocols is that they only require a standard web browser as UA while the providers may use several federation protocols, depending on the relationships between partners. Since SAML is a very extensible open standard, it is often used as a basis for several architectures with specific extensions. For example, various protocols of the Liberty Alliance project [Hodges] as well as the Shibboleth project [Shibboleth] build on SAML. The SAML protocol functionality is simple: when the user accesses via the user agent a service provided by an SP, the SP creates an authentication request in SAML format and redirects the user to the IDP to authenticate the user.

Once the user has been authenticated (e.g., by means of username/password or digital certificates), the IDP acting as a SAML Authority creates a SAML assertion in XML format, which is valid for a specific time interval and contains a declaration about the date and method of authentication. In addition, the assertion can include other attribute statements besides the authentication information. Each attribute statement can contain one or more attributes, each of which has associated a name in a specific format. The IDP typically signs the assertion to guarantee its authenticity and integrity. The protocol allows also encrypting the assertion to guarantee its confidentiality. The authentication response containing the issued SAML assertion is sent to the SP using a SAML binding. For example, in case of the web browser Single Sign On (SSO) profile [Cantor] the HTTP POST binding is commonly used, which means the SAML assertion is sent through the user's browser with the HTTP POST

method. Finally, the SP verifies the SAML assertion, including the digital signature applied on the assertion and its temporal validity. If the verification succeeds, the SP provides the requested service to the user.

As part of a federation configuration, the SP must establish a trust relationship with its partner IDP, typically via manual out-of-band exchange of certificates used to protect the SAML messages. Thus, each SP will end up with a list of partner IDP certificates. The SP accepts SAML protocol messages from a partner IDP if the certificate used to sign the SAML assertion validates the signature against its trusted list.

Additionally, the SP might require that the user is authenticated using strong authentication methods (such as a smart-card) in order to grant him access to particular services. Consequently, the SP should individually agree with each IDP about the meaning and the format of the authentication level required by the SP in certain service contexts.

## 3. The Stork Interoperability Framework

The Stork framework performs a number of basic functions, such as the retrieval of the person's eID and related attributes and the transport of these attributes to a trusted SP.

These services could be either offered by a national proxy server, named PEPS (Pan-European Proxy Services), or they could be provided directly by a dedicated software, which is named Identity Middleware. Thus, the Stork architecture supports two approaches – the proxy (or PEPS-based) approach and the middleware approach – and each European Member State (MS) country can freely decide which one to support. The middleware approach is specifically suitable for those cases in which the smart-card is used for user authentication, as detailed in [Tauber]. Both the PEPS-based and the middleware approach use the SAML 2.0 standard as foundation for authentication and user attribute transfer. However, the SAML format has been extended to support user-related attributes significant for access control services.

A European MS adopting the proxy approach will run a PEPS server, which is part of a centralized European infrastructure used to connect the national identity infrastructures. Each PEPS has two interfaces: the interface used for communicating with the SPs and the IDPs in his own country is MS-specific (thus its implementation is left at MS' choice), whereas the interface used for communicating with the other PEPS servers, based on SAML 2.0, was developed in the project itself. In the Stork framework, the SP contacts its own national PEPS to ask for user authentication and (on the other hand) the IDP will respond to its national PEPS about user authentication requests originating from that PEPS. In addition, in Stork, the SAML authentication request contains an indication of proper authentication assurance level required to get access to an SP service. Currently, four authentication assurance levels are defined, which are related to the assurance required for the user's identity: level 1 (providing minimal assurance) indicates that the user can be authenticated via reusable passwords, level 2 (providing low assurance) demands use of identity

Tokens (software or hardware) and One Time Passwords (OTPs), in a level 3 authentication (providing a substantial assurance) the OTPs are still tolerated, but identity tokens are strongly recommended, whereas in a level 4 authentication only strong crypto tokens (like smart cards with qualified certificates) are accepted.

Let's consider the case – shown in Fig. 1 – of a person trying to access a remote service (provided by a foreign SP) when both countries adopted the proxy approach. The PEPS in the SP country is named also S-PEPS, whereas the PEPS in the citizen's country is named C-PEPS.

To access a web-based service, the user is first asked to authenticate (step 1). As the SP is connected to Stork, it creates a SAML authentication request containing the attributes required for the service and sends it to the S-PEPS through the UA (step 2). In addition, the SP or the S-PEPS provides the citizen with a web page to select the citizen's originating country. Based on this information the citizen is redirected to her national C-PEPS. Upon country selection, the S-PEPS constructs a signed SAML request containing the required attributes mapped to Stork format, which is sent (through the user's browser) to the C-PEPS (step 3).

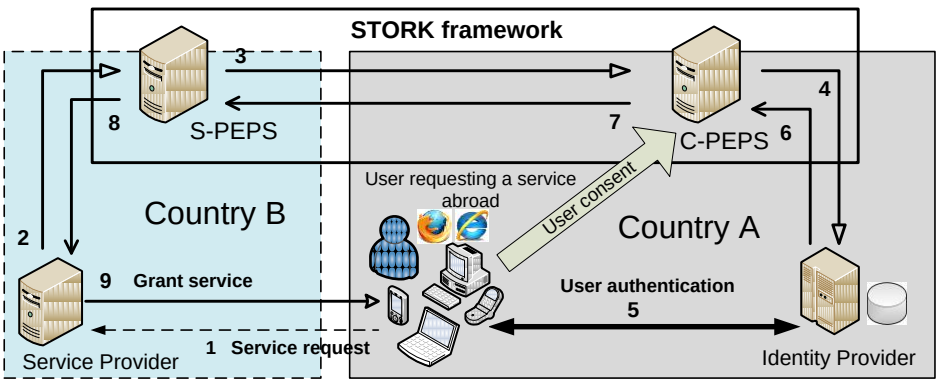


**Fig.1 – Using the Stork framework (PEPS-based) in a cross-border e-service.**

The C-PEPS selects the appropriate national IDP for user authentication and creates an authentication request where the user attributes required are mapped from the Stork format to the format recognized by the IDP, and sends it to the IDP (step 4). In step 5, the IDP performs the authentication exchange with the user and returns the appropriate response to the C-PEPS (step 6). After validating the response, the C-PEPS maps the received attributes to the Stork format, and (if necessary) derives additional attributes (e.g. "ageOver" derived from birthDate, or an pan-European eID uniquely identifying the person abroad derived from the national electronic identifier) for privacy protection purposes. In addition, the C-PEPS requires also the user's consent to forward his attributes to the S-PEPS. Finally, the C-PEPS creates a signed SAML response (containing the user attributes values) and sends the response to the

S-PEPS through the UA with the HTTP POST method (step 7). The S-PEPS performs similar operations as the C-PEPS, and sends subsequently the newly created SAML response to the SP (step 8), where the certified attributes are extracted and verified to eventually grant access to the requested service (step 9).

The main innovation features of Stork can be summarized as follows:

- the possibility for an European citizen to use her own national e-identity (in whatever form it is, e.g. one-time password, code provided via a mobile phone, smart-card) when accessing a foreign web-based service provided by a service provider connected to Stork;
- the possibility (for a SP) to automatically identify a user from a foreign country and have this identification be performed with a specified level of assurance.
- the possibility to automatically retrieve specific attributes about the user (like name or age) so that she does not need to enter them. Since these attributes are certified by the national eID infrastructures of the European countries participating in the project, the user cannot lie (and this fact is very important for the provider offering the service and requesting identification of the user).
- the high scalability of the Stork infrastructure allowing a SP and an IDP in an European country to easily interconnect with the other providers in the other Member States through the Stork infrastructure.

In addition, a prototype service has been also implemented allowing validation of digital certificates through Stork. This service is of crucial importance for applications or services exploiting digital certificates, like the creation and verification of electronic signatures.

## 4. Building the Student Mobility e-service with Stork

Based on Stork, we designed and implemented a flexible and scalable student mobility service, allowing both foreign students to apply on-line at Politecnico di Torino using their own national credentials, as well as Italian citizen to apply online at foreign universities integrated in the Stork framework.

Our contribution is twofold. First we integrated in Stork our service for foreign student application at the Politecnico di Torino, and the architecture of this service is illustrated in Fig. 2. On the other hand, we also integrated a real IDP with Stork (as shown in Fig. 3), allowing citizens that have previously registered at Politecnico di Torino's IDP or that have a smart card issued by our organization [PiemonteCard] to access other cross-border on-line services at foreign universities connected to Stork. Examples of such services are access to eLearning platform for students and teachers or applying online to Erasmus programs. As explained in Section 3, the Service Provider portal contains the protected on-line application that can be accessed via common web browsers and requires user authentication.

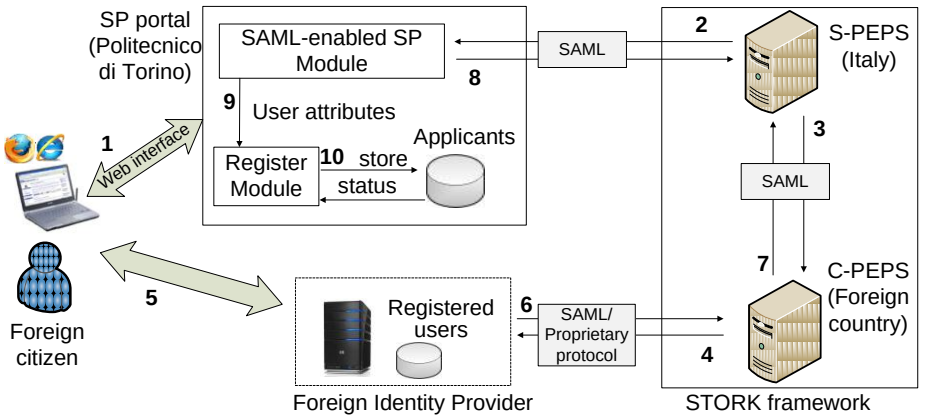


**Fig.2 – Integrating the Stork framework into Apply@polito web portal.**

*Integrating the Stork framework into Politecnico di Torino's Apply@polito web portal*. To allow foreign students to apply online at our university, we developed a web-based application running at the university's portal (as shown in Fig. 2), which has been derived from the Demo SP provided in Stork. This application is actually a web application running on an application server such as Apache Tomcat [Tomcat], and it contains several basic components: a web interface initially accessed by the users to apply on-line at our university indicating that the procedure can be fulfilled using their national credentials; a SAML engine (based on OpenSAML [OpenSAML]) allowing the SP to construct SAML authentication requests and to extract user attributes from the SAML authentication responses received from the national PEPS; configuration files containing data required to digitally sign the SAML messages, to indicate the location of the S-PEPS, and the list of user attributes that can be required through Stork. When the user accesses the portal, he will be presented with a web page (step 1) in which he can choose to perform his Application@polito with an European eID. Next, he is presented a page indicating the attributes required to complete the application, some of these attributes are mandatory (i.e. the Given Name, the Surname, the eIdentifier and the date of birth), whereas other are optional (i.e. the residence address, the country of birth, the nationality, the e-mail address and the gender). At the next step, the user is asked to select his country of origin. On selecting the country, the SAML authentication request is sent first to the S-PEPS (step 2) and subsequently to the C-PEPS running in the foreign country (step 3). The format of the messages exchanged in these steps is specified in [Alcalde-Moraño]. At the C-PEPS, the user is required to either authenticate directly (since some PEPS servers embed this functionality in the national proxy) or he is redirected to a specific national IDP (step 4) to complete authentication (step 5). The communication protocol used between IDP and C-PEPS is often based on SAML but it can be even a proprietary protocol (as described in Section 3). The authentication response is sent back through the Stork framework to the SP, where the

dedicated web application extracts the required attributes and pass them to a Registration module (step 9) in charge with storing the data into a relational database, such as an Oracle database (step 10).

The experimental setup put in place for this service consists of a SP machine running the web application derived from the Stork Demo SP application, and the PEPS machine running the PEPS package developed in the project, which contains also a SAML engine based and a set of Java servlets handling the SAML requests and responses arriving from the SP and from the other PEPS respectively.

*Providing identity and attribute transfer service through Stork*. For this service, we set up a SAML-enabled IDP (as shown in Fig. 3) in charge with authenticating users using any of the three types of authentication methods that have been mapped to the Stork levels of assurance: the username/password (corresponding to level 2), the digital certificates saved in files, named also "soft" certificates (corresponding to level 3) and the digital certificates saved on smart cards (corresponding to level 4). In addition, the IDP is also in charge with providing user attributes, by extracting them from the dedicated database containing the students and teachers registered at the Politecnico di Torino. The IDP is connected to the national PEPS, so that assertions about authentication and user attributes are transferred to the foreign SPs through the Stork framework. In our experimental setup, the IDP machine runs the Shibboleth software (v2.0). We chose Shibboleth because it incorporates a SAML 2.0 engine and it permits easy management of the IDP functionality through dedicated configuration files. We extended the IDP functionality by integrating authentication with digital certificates (either stored in files or on smart-cards) besides the username/password authentication supported by default in the Shibboleth package.

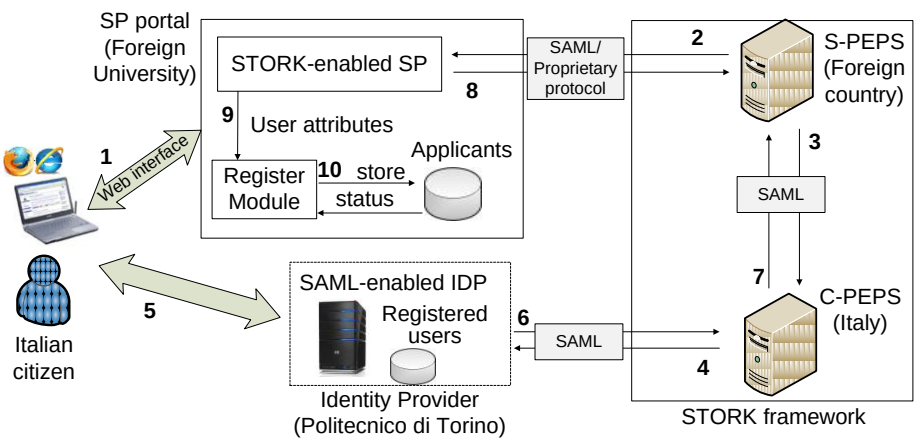


**Fig.3 – Providing identity and attribute transfer services through Stork.**

## 5. Conclusions

In this paper, we presented the European e-ID interoperability framework Stork, which offers scalable, secure and privacy-aware cross-border authentication for public and private e-services. Besides the technical aspects, it is important to note that Stork uses legally valid national electronic identifiers and puts the user in control of his personal data.

We have also reported about practical applicability of Stork, focussing on the pilot application for Student Mobility. It demonstrates the main features of Stork, such as integration with the national IDPs and SPs, and the technologies developed to simplify the implementation of a cross-border e-service, such as the one allowing people to apply on-line at European universities by using their own national credentials. The Student Mobility application is currently being piloted in universities from Italy, Austria, Spain, Portugal and Estonia. Our experience, gained in more than nine months of use in a production environment, indicates that Stork is a viable solution to implement cross-border e-services for European citizens.

**Acknowledgements.** This paper describes work that was developed in the framework of the EU co-funded project Stork (INFSO-ICT-PSP-224993, www.eid-stork.eu).

## References

[Alcalde-Moraño] Alcalde-Moraño J., Hernández-Ardieta J. L., Johnston A., Martinez D., Zwattendorfer B., Stern M., Heppe J., Stork deliverable D5.8.2b Interface Specification, October 2010.

[Arora] Arora S., National e-ID card schemes: A European overview, Information Security Technical Report, Vol. 13, Issue 2, 2008, 46–53.

[Shibboleth] Cantor S. (editor). Shibboleth architecture - Protocols and Profiles, http://shibboleth.internet2.edu/docs/internet2-maceshibboleth-arch-protocols-latest.pdf, Sept. 2005.

[Cantor] Cantor S., Kemp J., Philpott R., Maler E., Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0, in OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/samlprofiles-2.0-os.pdf, 15 March 2005.

[DigitalAgendaEurope] Digital Agenda for Europe, Communication from the Commision to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, August 2010, http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[ECeGov] European Commission: The European eGovernment Action Plan 2011-2015, COM(2010) 743, Brussels, 2010.

[ECDigitalAgenda] European Commission: A Digital Agenda for Europe, COM(2010) 215 final/2, Brussels (2010).

[ENISA] ENISA Risk Assessment Report: Security Issues in Cross-border Electronic Authentication, February 2010.

[Hodges] Hodges J, Wason T, Liberty architecture overview, 2003.

[InfoCard] Microsoft. Identity Selector Interoperability Profile V1.0, http://download.microsoft.com/download/1/1/a/11ac6505-e4c0-4e05-987c-6f1d31855cd2/Identity-Selector-Interop-Profile-v1.pdf, September 2007.

[ISA] Interoperability solutions for European public administrations (ISA) (OJ L 260, 3.10.2009, p. 20). ISA replaces the IDABC programme (Interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (OJ L 181, 18.5.2004, p. 25).

[Liberty] Liberty Alliance. Identity web services framework 2.0, http://www.projectliberty.org, 2006.

[Maler] Maler E., Reed D., The venn of identity: Options and issues in federated identity management. IEEE Security & Privacy, pages 16–23, March/April 2008.

[Mic] Microsoft. Windows Live ID/Passport Network, https://accountservices.passport.net/ppnetworkhome.srf?vv=700&lc=1031.

[OASIS] OASIS. OpenID Authentication 2.0 - Final. Assertions and Protocols for the OASIS Security Markup Language (SAML) v2.0, OASIS Standard, http://www.oasis-open.org/apps/org/workgroup/security/, March 2005.

[OpenID] OpenID Foundation. OpenID Authentication 2.0. Final, December 5, 2007. http://openid.net/specs/openid-authentication-2_0.html.

[OpenSAML] OpenSAML libraries, https://spaces.internet2.edu/display/ OpenSAML/Home.

[PiemonteCard] Piemonte University System Smart Card. https://didattica.polito.it/segreteria/sportello/en/Smartcard.html, 2011.

[Stork] Secure Identity Across Borders Linked (Stork) project - Towards pan-European recognition of electronic IDs (eIDs) (2008-2011), http://www.eid-stork.eu

[Tauber] Tauber A., Zwattendorfer B., Zefferer T., Mazhari Y., Chamakiotis E., Towards Interoperability: An Architecture for Pan-European eID-Based Authentication Services, in Proc. of EGOVIS 2010, Bilbao, Spain, LNCS Vol. 6267/2010, 120-133.