Identity federation beyond national borders: connecting the SIR service to the STORK infrastructure

A. Daryanani[1], J.P Gumbau[2], J. Heppe[3]

[1]Middleware Engineer, RedIRIS / red.es, Spain, ajay.daryanani@rediris.es. [2] Head of Office for Planning and Technology Forecast, Universitat Jaume I, Spain, gumbau@sg.uji.es. [3] Senior Consultant, Indra, Spain, jheppe@indra.es.

Keywords
STORK, SIR, cross-border, federation, digital identity, interoperability

1. ABSTRACT

Federated identity is a key topic in any organization nowadays. It has evolved from an in-campus test technology to nation-wide production services in only a few years, thanks to the growing user community, the standardization of protocols and the effort on establishing trust links between service and identity providers.

In Spain, RedIRIS (the Spanish National Research and Education Network) operates an identity federation called SIR. With the aim of broadening the services available for the community, RedIRIS is exploring the links with international initiatives, such as STORK. The STORK project (Secure idenTity acrOss boRders linKed) establishes a legal, organizational and technological platform, which will enable EU citizens to access e-government services by presenting their actual eID. The 29 participants from 14 countries in the consortium have defined and are implementing common specifications for mutual recognition of national electronic identities; in order to test these specifications, the project will deploy a platform on which different pilots will demonstrate the usefulness and viability of delivering cross-border electronic services in Europe. One of these pilots is called 'Student Mobility', that will enable students to get access to online administrative services offered by a particular University using their national eID card of origin.

This paper shows the design and implementation of the interconnection between the SIR federation and the Spanish national authentication service from STORK, fruit of the collaboration between CRUE (Spanish Conference of University Rectors), Universitat Jaume I de Castellón, RedIRIS and Indra.

2. BACKGROUND

The implementation of the Student Mobility pilot is not built from scratch, but relies on preexisting infrastructures that ease the integration for university services. Here we will analyze the Spanish academic federation SIR and the STORK infrastructure.

2.1. The SIR Service

SIR (Servicio de Identidad de RedIRIS) provides a single entry point to digital identity services for the Spanish academic community. It acts like a hub, connecting the local infrastructures to a central point of information exchange, and offers compatibility with several protocols on both IdP and SP sides: SAML1.1, SAML2, Shibboleth 1.3/2.x, eduGAIN and openID.

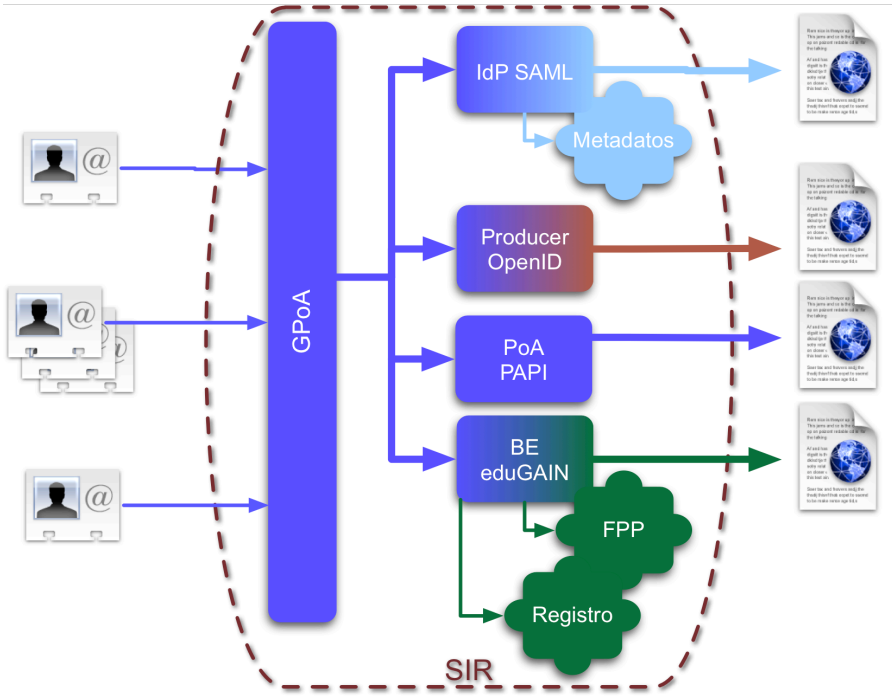

Figure 1. Technical view of the SIR service

With SIR, universities acting as Identity Providers (IdPs) have to deploy their connection to SIR only once; Service Providers (SPs) are made available to them seamlessly when they join the federation (of course, there should be some kind of agreement or contract between IdP and SP). RedIRIS takes care of enabling the appropriate connector for the SP and aggregating the metadata for the participants.

Universities can also act as SPs, offering their services to the federation: this is the case of University of Cordoba, which offers a dropbox-like service to the community; and of University Jaume I of Castellón, that has enabled federated access to their mediatheque. Following this model, Spanish members of the STORK pilot on Student Mobility will offer e-administration services to STORK users.

Joining SIR provides a range of benefits for both Service and Identity Providers:

- Access to a consolidated federation, with 54 IdPs and 118 SPs (as of April 2010)
- Seamless integration with the federation, thanks to the multiprotocol nature of SIR
- Support and advising for institutions affiliated to RedIRIS
- Centralized management of metadata and attribute mappings (on demand)
- Privacy preservation on both ends
- Independence of authentication mechanisms and LoAs (Levels of Assurance)
- Ad-hoc Discovery Service: when accessing a SP, users see a restricted list of IdPs (those who have an agreement with the SP)

2.2. The STORK project

The STORK project aims to establish an European eID Interoperability Platform that will allow European citizens to use their national eID to establish new e-relations across borders. The project will test cross-border user authentication by means of five pilot projects that will use existing government services in EU Member States. In time, the number of cross- border services available to European users will increase as more service providers become connected to the platform.

Thus in the future, citizens should be able to start a company, get their tax refund, or obtain their university papers without physical presence; all they will need to access these services is to enter their personal data using a national eID, and the STORK platform will obtain the required guarantee (authentication) from their government.

Most EU countries have already deployed national electronic citizen cards; citizens are becoming accustomed to them and are beginning to enjoy the benefits they offer. Other countries have opted for simpler solutions based on user ID and password, sometimes complemented with other identification mechanisms.

The goal of the project is not to replace any existing national infrastructure, but rather to take what is already available and to connect all the various authentication methods with transparency, in such a way that any of these methods will allow users to present their certified personal data to foreign administrations.

The Student Mobility pilot is intended to facilitate students' mobility across Europe. It will enable foreign students to get access to online administrative services offered by Universities using their national eID of origin for authentication and transfer of identity attributes. In Spain, these services include the enrolment for Erasmus students and registration of foreign students. In order to use them, a student will follow these steps:

- The student will access, for example, the registration page at Universitat Jaume I de Castellón
- The student will be shown a country list, and will choose his/her country (in this example, Estonia)
- The student will be redirected to the university country's PEPS (PanEuropean Proxy Service, the national STORK entry point); in this case, it will be the Spanish PEPS
- The student will be redirected to the Estonian PEPS transparently
- The student will authenticate by means of his/her credentials, and will give consent to the issuing and transfer of data
- Then, he/she will be redirected back to the Spanish PEPS, which will forward him/her to the university's registration page
- The registration page will check if the authentication has been successful, and act accordingly (by recording the user's data into the application, or asking him/her to enter the data manually)

3. CHALLENGES

Seven Spanish universities are part of the student mobility pilot of STORK. Therefore, in order to implement the pilot, some online services of these universities should be connected to the STORK infrastructure. Bearing in mind that most of them are already connected to the SIR service, it looks reasonable to implement only one connection between SIR and STORK.

Generally, connecting to SIR requires exchanging metadata documents and maybe a protocol adaptation; but in the case of STORK there are some more challenges:

- Protocol: STORK has defined an extension of SAML2 (SAML2-STORK), which isn't supported in the SIR federation
- Deployment: The SAML2-STORK engine has been developed in Java, while the SIR federation is based on PHP
- Attributes: Most Spanish institutions follow the iris-* and schac schemas to represent users and attributes in their directories, thus needing an adaptation to the specifications of STORK

To implement this, and after studying the two infrastructures, the most reasonable solution was to deploy a new protocol adaptor inside SIR, as an addition to the current ones. This connector would

have the ability to generate SAML2-STORK requests and receive SAML2-STORK responses, solving the protocol issue.

The next question is: how to implement this connector? Instead of writing a new connector from scratch for SAML2-STORK, it seemed reasonable to make use of the library being developed by the STORK consortium, therefore avoiding the re-implementation in PHP and providing a better maintenance of the interconnection, as any change in the SAML2-STORK profile will be reflected in the library.

This library is written in Java, thus creating the second challenge mentioned earlier as it needs to be used by a PHP class. The solution to this was to develop a simple web service, that can be instantiated by a PHP connector in SIR, and which will query the SAML2-STORK engine to create requests and validate responses.

Finally, there was the issue of attribute mappings: while STORK defines a set of attributes that can be used within their infrastructure, most Spanish universities follow the iris-* and schac schemas. It was decided that each university will make their choice, by doing the mapping locally, or asking SIR to do it for them.

4. ARCHITECTURE

A high level picture of the architecture is depicted in Figure 2, with special emphasis in the interconnection components (the SIR-STORK box)

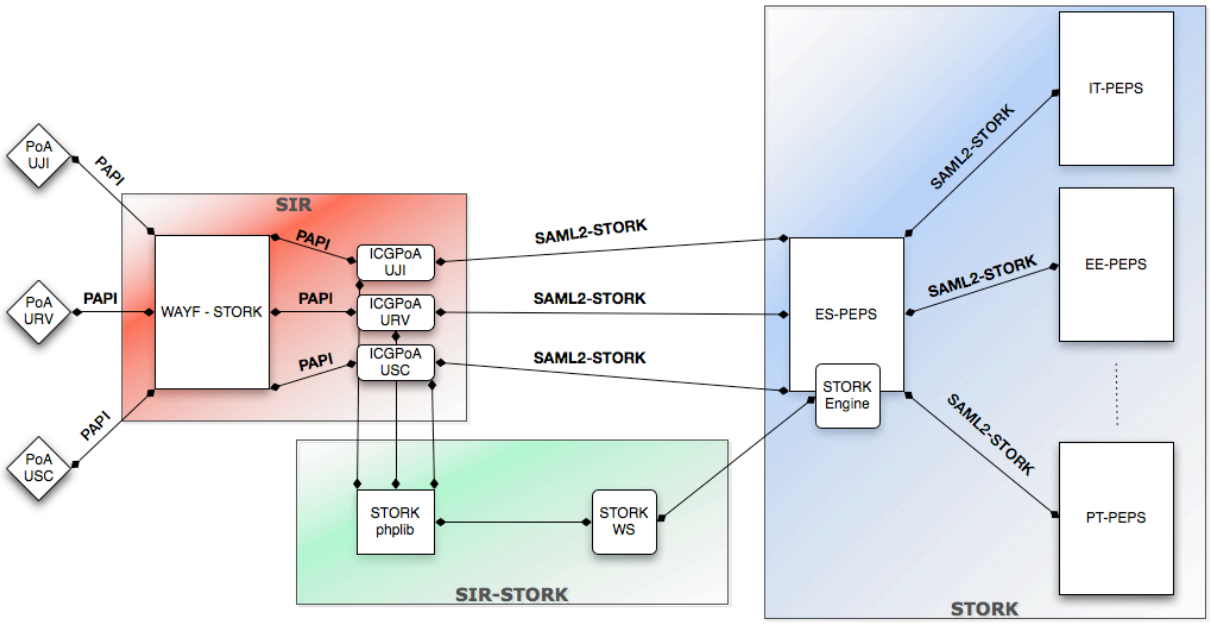

Figure 2. SIR-STORK interconnection architecture

To explain all the components, we will follow the same use case explained in the end of section 2.

- *The student will access, for example, the registration page at Universitat Jaume I de Castellón (UJI)*

  The service is protected by some kind of federation software (Service Provider software). In the PAPI protocol, which is the one being used to internally connect to SIR, this software is called PoA (Point of Access). So the PoA will redirect the user to SIR using the PAPI protocol.

  The image also shows other Spanish universities, to have a complete view of the architecture.

- *The student will be shown a country list, and will choose his/her country (in this example, Estonia)*

  The PEPS expects a destination country code in the request, so this decision must be taken before the request is created. Instead of including a country list in each service at each university, it has been decided to have a single list (WAYF-STORK) and deploy it inside SIR.

- *The student will be redirected to the university country's PEPS (PanEuropean Proxy Service, the national STORK entry point); in this case, it will be the Spanish PEPS*

  This is the core operation. The WAYF forwards the PAPI request to a very simple protocol connector between PAPI and SAML2-STORK, called ICGPoA (InterConnection Group-wide PoA); each university will have an ICGPoA, to have enough flexibility in what relates to attributes (which attributes each university expects, and with which mappings, can be defined here).

  The ICGPoA (PHP based) receives the PAPI request; then, it will call the STORK-phplib library, that has the objects and methods to provide STORK-SAML2 requests to the ICGPoA, and will use a web service to connect to the STORK Engine (Java based), who actually creates the request. After this request is made available to the ICGPoA, it will redirect the user to the Spanish PEPS, with the appropriate parameters defined in the SAML2-STORK specification and posting the request with it

- *The student will be redirected to the Estonian PEPS*

  The Spanish PEPS (ES-PEPS) receives the requests, checks for the destination country and redirects the user to the corresponding PEPS. This process is transparent to the user

- *The student will authenticate by means of his/her credentials, and will give consent to the issuing and transfer of data*

  Either wit username/password, software certificate, smartcard-based certificate or any other approved means, the user will authenticate and give his/her consent to the issuing of personal data

- *Then, he/she will be redirected back to the Spanish PEPS, which will forward him/her to the university's registration page*

  This is the other important operation in this flow: the ICGPoA receives a SAML2-STORK response, which is validated against the STORK Engine by means of the STORKphplib and the web service. A PHP object is made available to the ICGPoA, which can now adapt the response to the PAPI protocol as well as the attribute mapping (if necessary). The user is redirected back to the university.

- *The registration page will check if the authentication has been successful, and act accordingly (by recording the user's data into the application, or asking him/her to enter the data manually)*

  The PoA at UJI receives the PAPI response, and provides the result of the operation and the attributes to the registration page.

In the picture, the components (except the PoAs at each university) are separated in 3 big blocks: one for the SIR service components (developed by RedIRIS), another for the STORK project components (developed by the STORK consortium) and the last one that are particular to the interconnection between them (developed by Indra). It is worth noting that, while the Student Mobility pilot is in its early stages, the SIR service that is being used lives in parallel to the production one. In the near future, the WAYF for STORK will be integrated with the production WAYF for SIR (that currently includes IdPs from the Spanish academic community); also, the ICGPoAs will be merged in one and will be available as a new connector in the SIR production service (see Figure 1).

5. CONCLUSIONS

The main conclusion we can take out at this moment is that the pilot is up and running. We have made tests of accessing services at Universitat Jaume I authenticating with Spanish and Portuguese eIDs, with good results. The interconnection infrastructure has proven to be stable, easy to maintain and providing a good user experience.

One of the main goals behind this work was to provide the university administrators with a simple way to integrate their services with STORK. We think that this has been achieved, as the administrators will continue to work in the way they know (in this case, by connecting their applications to the SIR service) and moving the complexity of the interconnection to a central point. For instance, any improvement in the STORK specifications will be applied in the component called STORK Engine, and will automatically be available for all the services in the pilot without a single line of code or change of configuration at the universities.

The next step is to test services in the other Spanish universities that joined the STORK pilot, a work that will help us to improve the infrastructure, documentation and experience. If a university wants to offer a service through STORK, the only thing they need to do is install a PoA that protects the service. As of today, all the universities in the pilot are already in SIR, therefore making unnecessary any other deployments or bureaucratic processes. They know the technology, and are familiar with it and with SIR.

6. REFERENCES

STORK website (2010). The Stork project. Retrieved February 10, 2010, from: https://www.eid-stork.eu/.

STORK website (2009). STORK brochure. Retrieved April 29, 2010, from: https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1003

SIR website (2010). Servicio de Identidad de RedIRIS. Retrieved February 10, 2010, from: http://www.rediris.es/sir

RedIRIS website (2010), Directory Schemas. Retrieved April 29, 2010, from: http://www.rediris.es/ldap/esquemas/

RedIRIS website (2010), PAPI web site. Retrieved April 29, 2010, from: http://papi.rediris.es