Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Matching federation identities, the eduGAIN and STORK approach

Elena Torroglosa *, Jordi Ortiz, Antonio Skarmeta

University of Murcia, Campus de Espinardo, Spain

HIGHLIGHTS

- Review of the most relevant identity federations.
- Detailed analysis of eduGAIN and STORK2.0 federations.
- Proposal of interoperability mechanisms needed to interconnect eduGAIN and STORK focused on identity matching and attribute exchange.
- Evaluation study through the implementation and deployment of the proposed solution with the successful translation and matching of identities and attributes between both federations.

ARTICLE INFO

Article history:
Received 12 January 2017
Received in revised form 12 June 2017
Accepted 30 September 2017
Available online xxxx

Keywords:
Identity management
Federation
Interoperability
STORK
eduGAIN
Authentication
AAI
eID

ABSTRACT

Several identity federations with different authentication mechanisms exist in the area of governments and educational institutions. STORK from the European administration side and eduGAIN from research and educational institutions side are the main exponents in their areas. Both federations are investing on harmonizing and integrating their federations with other Authentications and Authorization Infrastructures (AAI) to improve and gain users and services. This paper analyses each federation and different integration scenarios proposing an interfederation solution that interconnects both federations through ad-hoc interoperability mechanisms, focusing on identity matching. In addition, an international testbed has been deployed to probe the viability and quality of the solution, with the focus on the user experience. The proposed integration allows an explosion of users and services both federations, allowing also the conversion of some face to face procedures to online transactions thanks to the use of strong authentication mechanisms.

1. Introduction

Governments and institutions are working hard on doing the best use of their networks and services, always studying new ways to improve the existing resources and creating new ones. Due to the several federations options with different authentication mechanisms appearance, bigger effort on homogenize and integrate existing Authentication and Authorization Infrastructures (AAI) [1] have also risen.

In general, once a new federation is established and deployed it raises the problem of being isolated from other federations and systems. Each federation has its own users and services and focuses on its specific environment, but the users from one federation cannot interact with users from other federations, and the services cannot be offered outside borders due to different internal technologies and infrastructures.

The existence of multiple federations creates the problem of lack of interoperability and a drawback for global solutions. The creation of integration mechanisms between identity federations allows at the same time to join user bases and potential services between them.

In the area of educational institutions there is a federation that stands out above the others, eduGAIN (EDUcation Global Authentication INfrastructure). This initiative started as a research activity in the project GÉANT2 (2004–2009), co-funded by the Europe's NRENs and the European Union and more recently it is part of the GÉANT 2020 Framework Partnership Agreement. This successful world wide federation is operating with impressive numbers: such as 2262 IdPs and 1413 SPs. Its higher impact rates are located at south and north America, Europe, Japan and Australia. eduGAIN interconnects research and education identity federations, enabling the secure exchange of information related to identity, authentication and authorization between participating federations.

* Corresponding author.
E-mail addresses: emtg@um.es (E. Torroglosa), jordi.ortiz@um.es (J. Ortiz), skarmeta@um.es (A. Skarmeta).

https://doi.org/10.1016/j.future.2017.09.076
0167-739X/

By contrast, the European governments have done a big effort to interconnect national services establishing inter-state interoperability mechanisms based on the STORK European eID Interoperability Platform that allows citizens to establish new e-relations across borders, just by presenting their national eID. The project has been deployed on a large scale that involves 19 Members States and implies the availability to all of their population with the biggest impact in the international electronic transaction between governments and citizens. STORK2 project has been focus on expand the interoperability to new strategic areas as eLearning and Academic Qualifications, eBanking, Public Services for Business and eHealth. STORK project has its continuation with the eIDAS Regulation [2], which is based on STORK results to define electronic identification and trust services for electronic transactions in the European internal market.

Both federations are in production state and are used in a daily basis by their users. Because of its nature, STORK is limited to an European Union scope mostly because obtaining an eID is restrained to EU member state citizenship, however the services already deployed are of big impact and business oriented. On the contrary, eduGAIN is not limited by any political state border and in consequence, it is already extended to multiple continents, nevertheless the services provided are of relative importance and focused on the research and educational business thus limited in terms of daily life impact. Therefore the union of both will provide with a wider user base to STORK and wider service offer to eduGAIN. Expanding own influence is hard and expensive to achieve individually. For all these reasons, both projects dedicate specific resources and efforts to interconnect and harmonize with other federations which allow to get at the same time new users and services. Integrating this type of federations allows levering their deployed large scale infrastructures and identity management tools to integrate users and services, offering better services to a greater number of users.

University of Murcia has a long research career in the field of identity management and federated systems with more than ten years collaborating with GÉANT and other international projects to innovate and improve the use of digital identities. Some of the projects focus on the integration of different authentication mechanisms in which the University of Murcia has been involved are SWIFT [3], GEMBUS [4], SEMIRAMIS [5], STORK 2.0 [6] among others. Currently, our University is involved too in solving similar problems found in the integration between eduGAIN and eIDAS, since eIDAS inherits its operations and elements from STORK 1 project.

There exists different big proposals to integrate authentication mechanisms [7] and identity federations [8] but in general they imply the migration to new common protocols (such as OpenID [9], OAuth [10] or OpenID Connect [11]) and the modification of all the entities involved (Service Providers, Identity Providers, Attribute Providers, etc.). They even can affect end users since the integration process may not be transparent. In addition, the use of general superfederation solutions usually implies new legal and political issues for the existing federations.

Based on our collaboration experience in eduGAIN and STORK projects, we will work to define an specific and ad-hoc solution for the interoperability problem of integrating both federations. The proposal is focused on the establishment of interoperability mechanisms that allow transparent interaction for services and users from both federations thanks to identity management mechanisms and trust control. Therefore, users maintain their identities between federations and at the same time, they can access to services of the other federation.

The ideal objective is to achieve bidirectional matching between eduGAIN and STORK identities with the specific properties of transparent, fluid and "on the fly" integration between users and services of both federations, not only allowing basic authentication but also complex scenarios like linking existing accounts and requesting additional attributes. To reach total integration for all the use cases is a very ambitious objective, so we will follow a step by step approach firstly studying different integration possibilities depending of the preconditions and the scenarios proposed.

Our proposed solution is to incorporate a new entity situated between the STORK and eduGAIN federations. This intermediate entity would be in charge of the SAML translation (between $SAML_{stork}$ and $SAML_{int}$) as well as of the translation of identifier and attributes. This entity has to act as a trusted entity for both federations, playing the role of DS and MDS of any other eduGAIN federation for the eduGAIN side, and acting as a PEPS (S-PEPS or C-CPEPS depending on the scenario) of another country for the STORK side.

The remainder of this paper is organized as follows. State of the Art Section (Section 2) introduces main characteristics of STORK and eduGAIN federations in the context of the AAI, putting the focus on the entities involved, the operation flows and describing their particularities. Interoperability Mechanisms Proposal Section (Section 3) exposes the interoperability problem between the aforementioned federations and offers two different points of view for integration scenarios together with several use cases and the interoperability mechanisms required to interoperate them. Validation Section (Section 4) explains the context of the prototype implemented and describes the validation of proposed integration solution through the analysis of two pure scenarios (STORK and eduGAIN) and two integrated scenarios. Conclusions Section (Section 5) summarize paper proposal and results and gives some indications of the future work.

2. State of the art

Nowadays there are several projects working on different AAI solutions and identity federation technologies. In the area of science there are several options. EGI [12] is a highly distributed, multi-disciplinary resource infrastructure, integrating more than 300 resource centres (service providers) and almost 20 000 users. EUDAT [13] offers common data services, supporting multiple research communities as well as individuals in a resilient network of 33 European organizations based on B2ACCESS [14] and Unity [15], ELIXIR [16] builds its own infrastructure for biological information, while Umbrella [17] is the pan-European federated identity system for the 30 000 users of the European large photon/neutron facilities. All are good AAI examples but as we will see below, their numbers in terms of users and services are not comparable with STORK [18] and eduGAIN [19].

The interconnection of identity federation is a relevant work area with several project and researchers working in parallel. A very important work is being done in papers like [20,21] and [22] to analyse the requirements of federation and interfederation initiatives and propose alternative solutions to solve the problem like the GÉANT Trust Broker [23]. Kantara initiative [24], which is based on Liberty Alliance Identity Assurance Expert Group [25], works on create a common framework to harmonize baseline policies, business rules, and commercial terms against which identity trust services can be assessed and evaluated. Other projects, like InCommons [26] in the United States and AARC [27] in Europe, dedicate part of their efforts to expand their base federations to interconnect with others.

There is previous projects, that like us, have been working on achieving the interoperability between IdM Systems based on the use of adapters, bridges and proxies but always limited by the specific protocols and technologies required in each case and implying the modification of the entities involved as in the case of The IntCloudWare project [28] that proposes the use of an ESB

Please cite this article in press as: E. Torroglosa, et al., Matching federation identities, the eduGAIN and STORK approach, Future Generation Computer Systems (2017), https://doi.org/10.1016/j.future.2017.09.076.