Towards User-Centric Identity Federations

Authors
Maarten Kremers, SURFnet  maarten.kremers@surfnet.nl  (+31 88 78 73 000)
Bas Zoetekouw, SURFnet  bas.zoetekouw@surfnet.nl
Andrea Biancini, Consortium GARR  andrea.biancini@garr.it
Marco Malavolti, Consortium GARR  marco.malavolti@garr.it
Rolf Brugger, SWITCH  rolf.brugger@switch.ch
Christoph Graph, SWITCH  christoph.graf@switch.ch
Hans Nordlöf, SWAMID  hanor@sunet.se

Keywords
Identity management, Identity federation, User centric, Long-lived Identity, user mobility.

Abstract
Identity Federations are undergoing important internal transformation to reach new levels of functionality and to provide benefits in a continuously changing environment. On one side, in fact, we have the strive to provide better services to end users. In this respect identity federations are focusing on providing services from a more user-centric perspective, thereby giving more power to the end users to manage their own digital identities. On the other side, identity federations are undergoing strong modification due to external factors. In many countries and communities a profound reorganisation of the federation basis is underway: some are providing more centralized structures to offer more advanced services, others are experiencing strong governmental and banking initiatives in the field of digital identities.

Both of these trends lead to the further decoupling of authentication and authorization functionality in the federations. Where the authentication can be handled by a central function in the federation (EduID) or might even be externalised (BankID, Government ID), the role of the institutions in those situations will move from identity provider (authentication) to attribute provider. Attributes are used to add the relevant Research & Education context to identities that are needed for authorization decisions by Service Providers, or to provide academic information about users. This trend offers new attribute providers like ORCID an opportunity to hook into the whole federation.

Within GN4 phase 1, an activity called EduKEEP was started to model and discuss this new architecture for identity federations, in order to overcome the challenges faced and to provide the basis for the evolution of identity federations. The shift towards a more user-centric model and the decoupling of authentication, attributes and authorization will be described and explained in the introduction of the session. Then the session will continue providing real case scenarios where this architecture is already being applied by NRENs and identity federations: the case of the Swiss eduID and the Swedish eduID will be presented. GARR will provide an overview of the transformation of the Italian federation due to a new
governmental initiative aimed at providing every Italian citizen with a digital identity. Finally
SURFnet will explain how in the light of these developments a centralized federation
infrastructure is an important advantage, offering a central hub in which attributes can be
aggregated and authorization decisions can be made (SURFconext).

Session format

The proposed format for this session is as follows:

- Decoupling Authentication, Attributes and Authorization (by Maarten Kremers, SURFnet) 15 min
  This talk will introduce the challenges experienced by identity federations nowadays and will describe the architecture designed and proposed within the GN4-1 JRA3 activity.
- The case for SWITCH EduID (Christoph Graf, SWITCH) 20 min
  This talk will briefly describe how the EduKEEP architecture is currently being applied to the case in Switzerland. It will focus on the first version of the Swiss edu-ID, which is in operation since spring 2015, and then show some of its first applications in real-world services. The talk will conclude with an outlook of the next evolutionary step of the Swiss edu-ID which is planned for the end of 2016.
- IDEM and the governmental digital identities (Andrea Biancini, GARR) 15 min
  This talk will describe the situation of Italy where the government is proposing a strong initiative to provide every Italian citizen with a personal digital identity. In this presentation the possible implications for the Italian federation will be described and some possible evolution of the federation model will be proposed for discussion.
- EduID in Sweden (Hans Nordlöf, SUNET) 20 min
  This talk will present the EduID project within Sweden. The presentation will describe the benefits of the model and will provide an example of application of an architectural model for identity federations in line with the EduKEEP architecture.
- Central authorization and Attribute Aggregation (Bas Zoetekouw, SURFnet) 15 min
  SURFconext is a hub-and-spoke federation. As such, it is perfectly positioned to offer solutions to our users and institutions for the problems that come with decoupling identity management from the institutions. In this talk, we will shortly visit the new SURFconext functionalities for central (SAML-AA based) attribute aggregation and for central (XACML-based) authorization management.

Acknowledgements

The work with regards to EduKEEP has received funding from the European Union’s Horizon 2020 research and innovation program under Grant Agreement No. 691567 (GN4-1).

Target Audience

This session will be non technical. The intended audience for this session is all federation operators and managers interested in keeping updated on the ongoing transformations. User communities representatives could also be interested to participate to learn user centric concepts and to appreciate the potential benefits for their users.
References

EduKEEP: https://wiki.geant.org/x/XgL3Ag
Swiss eduID: https://eduid.ch
Swedish eduID: https://eduid.se
SURFconext https://www.surfconext.nl

Proposed Speakers

Maarten Kremers, SURFnet maarten.kremers@surfnet.nl
Christoph Graf, SWITCH christoph.graf@switch.ch
Andrea Biancini, Consortium GARR andrea.biancini@garr.it
Hans Nordlöf, SUNET hanor@sunet.se
Bas Zoetekouw, SURFnet bas.zoetekouw@surfnet.nl

Biographies

Maarten Kremers joined SURFnet in 2007 and is currently technical product manager Trust and Identity. He is involved as project member and project manager in the innovation and development of collaboration and identity management infrastructure SURFconext, with focus on group management and authorization. Furthermore he is currently leading the GN4 research task on authorization and attribute management in the federated identity area as well as leadings its predecessor in GN3plus. He holds a MSc degree in Information Management from Tilburg University.

Bas Zoetekouw obtained his PhD in physics from Utrecht University in 2006. After working in industrial research for a few years, he joined SURFnet in 2010 as a technical product manager in the Trust and Security group. He has been a member of the SURFconext operations team for a number of years, but his main focus is adding new functionality to SURFconext. Recently, he has been working on adding better support for authorization and access control to SURFconext, developing a statistics module for SURFconext and on developing tools to automate the process of adding new service providers to the federation.

Andrea Biancini has developed his career working for companies in the Finance and Information Technology fields and I dealt with: IT project management, planning and governance on themes of management and control (budget/costs), project portfolio management. He is particularly oriented in favoring the adoption of structured and effective working methodologies. He is also naturally oriented at developing an organic and systemic vision upon processes, resource management and governance activities. In the last 4 years, Andrea worked for the Italian NREN on different European projects in the field of AAI. Andrea participated to Géant projects starting from GN3+ and has also took part to the AARC project acting for the first 8 months of the project as task leader of the JRA1.4 activity.
Marco Malavolti graduated in computer science with a thesis on a Comparative study on different Metadata Registries. Thanks to the thesis, he learned to use the frameworks Shibboleth and SimpleSAMLphp to implement a simple identity federation. He started his work for IDEM GARR AAI, in 2013 and he had the opportunity to learn and write management guides for Shibboleth IdP, SP and Discovery Service and to deal with an Entity Registry and a Metadata Aggregator to manage federation’s metadata. On behalf of the Italian NREN, he worked on different European projects about Authentication and Authorization Infrastructure and he participated to Géant projects starting from GN3+. He is also involved in the AARC project where, principally, he will support the training task for different communities.

Christoph Graf is head of the “Supporting Operations” department of SWITCH and leads the project Swiss edu-ID. He completed his education with a masters' degree “Dipl. Elektroingenieur ETH” at the Swiss Federal Institute of Technology, Zürich, in 1986 and worked for four years as a designer of integrated circuits with Philips. Christoph joined SWITCH in 1991 as an application engineer and later rejoined SWITCH in 1998 as head of security and system administration.

Rolf Brugger has studied computer science and psychology at the University of Fribourg, Switzerland. He worked as an advisor and product manager at the Swiss Virtual Campus. He joined SWITCH in 2007, worked in various e-learning related projects and is now a member of the Swiss edu-ID project team.

Hans Nordlöf has a background as Systems Architect at Karolinska Institutet and has worked for SWAMID Operations since 2005. He has been working with identity management for many years and was engaged in the Swedish eduID project as project manager in September 2014. Today he is sharing his NREN practices between federation policy making and the eduID project.