Trust and Identity Assurance in Research and Education Identity Federations

Davide Vaghetti[1]

[1]Consortium GARR, Via dei Tizii 6, 00185, Rome, Italy

Abstract

This paper explores the current landscape of identity federations within research and education networks, concentrating on the trust flow and identity assurance, with a specific focus on the international and the Italian case. It delves into the role of National Research and Education Networks (NRENs), Identity Federations, and the eduGAIN global trust infrastructure. It will also provide a quick overview of the REFEDS Assurance Framework and some details of its implementation in the Italian research and education identity federation IDEM GARR AAI.

Keywords

Federation, identity assurance, research and education, trust, eduGAIN

1. Introduction

In the modern digital landscape of research and education, secure and seamless access to online resources is crucial for collaboration and innovation. Identity federations have emerged as a solution to provide access to services and resources for students and researchers across institutions globally. Research and Education (R&E) federations rely on a network of trust between Home Organizations, Service Providers and Federation Operators, with National Research and Education Networks (NRENs) providing the necessary infrastructure and governance.

This paper examines the trust flow within these federations and the inter-federation service eduGAIN [1], highlighting key standards and frameworks elaborated by REFEDS, the Research and Education FEDerations group. It will also give a concrete example of implementation of the REFEDS Assurance Framework [2] in the Italian research and education Identity Federation, IDEM GARR AAI [3].

2. NRENs and R&E Identity Federations

NRENs, such as SURF in the Netherlands, DFN in Germany, Renater in France, Internet2 in the United States, or GARR in Italy, are pivotal in establishing and maintaining national identity federations for research and education. These federations connect universities, research institutions, and other academic entities to Service Providers in order to facilitate access to digital resources such as academic journals, online office suites, sync and share services, cloud

TDI 2024: 2nd International Workshop on Trends in Digital Identity, April 9, 2024, Rome, Italy

davide.vaghetti@garr.it (D. Vaghetti)

© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR-WS.org/Vol-3863/short1.pdf

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

computing instances, student mobility resources, etc. The governance model of these federations is typically community-driven, with an emphasis on open standards and interoperability. Key characteristics of these federations include multilateralism, trusted third-party validation, signed metadata, and the participation in the global inter-federation service eduGAIN. Identity federations operate on the principles outlined by the Secure Assertion Markup Language (SAML). SAML 2.0 core specification [4] defines protocols for authentication and attribute sharing between users' Home Organizations and providers of services, or Identity Providers and relying parties. SAML 2.0 metadata specification [5] also plays a critical role by providing a standardized format, called *metadata*, for sharing information about federation members, such as their endpoints, supported attributes, and cryptographic keys.

3. Trust Flow in Identity Federations

Trust within R&E identity federations is a hierarchical and multi-faceted concept. At the foundational level, users trust their Home Organizations, which are typically universities or research institutions. These Home Organizations, technically acting as Identity Providers, are responsible for authenticating their users and asserting their identities and affiliation attributes toward services within the federation. Services and resources are published in the federation by Service Providers, either commercial, such as academic journals publishers, or public funded, such as research projects resources. Federations act as trusted third parties between Home Organizations and Service Providers, publishing cryptographically signed metadata that provides both an effective way to exchange technical configuration details among the federation participants, as well as a mean to prove the authenticity and the validity of those information. Signed metadata are the fundamental building block of trust in identity federations.

4. eduGAIN: Enabling Global Interfederation

The trust extends beyond national borders through eduGAIN, the inter-federation service that connects research and education identity federations globally. eduGAIN can be considered a federation of federations, operating on the same technical specifications employed by national federations with the role to simplify access to resources and services at the international level, avoiding the registration of services in multiple federations.

eduGAIN collects and validates metadata about the entities of each participating identity federation. Collected metadata are then aggregated, cryptographically signed to prove the authenticity and the validity, and finally published so that participating federations can import and redistribute them to their constituency.

eduGAIN enhances the global interoperability of identity federations by connecting 80 federations and over 9,000 entities among Identity and Service Providers. The eduGAIN SAML Profile [6] establishes requirements for metadata management, registration authority, validity period, cryptographic signature, and publication rules, ensuring that federations worldwide can communicate securely and efficiently. The success of eduGAIN lies in its ability to enforce a

consistent standard across diverse federations, allowing users to access resources internationally without compromising on security or trust.

5. REFEDS Assurance Framework

To mitigate the risks associated with federated identity management, R&E federations implement assurance frameworks that provide clarity on the reliability of identity assertions. The REFEDS Assurance Framework is an identity assurance framework that has been developed by the federation operators community, providing a global standard for the research and education environment. It specifies how Identity Providers should communicate assurance information to Service Providers, including the uniqueness of identifiers, the identity proofing level, and the quality of attributes provided.

5.1. Identifier Uniqueness

Within the REFEDS Assurance Framework, the uniqueness of a user's identifier is paramount. Unique identifiers must represent one natural person within the Home Organization, must not be reassigned to other person at any time, and must be asserted using one of the provided SAML or OpenID Connect protocol identifiers provided in the specification.

5.2. Identity Proofing Levels

The framework defines different levels of identity proofing and authenticator issuance, renewal and replacement processes (IAP), ranging from low to high, which reflect the confidence in the identity vetting process conducted by the Identity Provider. These levels guide Service Providers in assessing the reliability of the identity assertions they receive, allowing them to make informed decisions about granting access to sensitive resources. The framework defines three levels:

- IAP/low means that asserted identity corresponds to a person with a self-asserted identity.
- IAP/medium can be used for reasonably validated and verified identities.
- IAP/high is reserved for well validated and verified identity.

Each level also defines strict rules for the credentials issuance, renewal and replacement.

5.3. Attribute Quality and Freshness

Attribute assurance deals with the quality and timeliness of user attributes beyond the unique identifier. Currently, it is limited to the freshness of the affiliation attributes and defines two values:

- ATP/ePA-1m, affiliation updated within one month since the change.
- ATP/ePA-1d, affiliation updated within one day since the change.

6. The Italian Case: IDEM Assurance Profiles

IDEM is the Italian Research and Education identity federation that has been set up by GARR to provide a trust infrastructure for the Italian researches and students. Currently, IDEM serves over 2 million students, researchers, and staff across Italian universities and research centers. In order to provide support for national and international use cases with assurance requirements, IDEM elaborated a set of assurance profiles (IDEM-P0 to IDEM-P3) that define specific criteria for identifier uniqueness, identity vetting, attribute quality, and authentication methods [7].

IDEM assurance profiles are an implementation of the REFEDS Assurance Framework at a national level, also providing references to the eIDAS level of assurance [8] and the Italian eGOV-ID system SPID [9].

6.1. IDEM Assurance Profiles

- IDEM-P0: The basic level with minimal identity vetting, suitable for low-risk applications.
- IDEM-P1: Requires identity proofing based on identity documents, with updated affiliations checked within one month.
- IDEM-P2: Involves the verification of identity documents, along with Multi-Factor Authentication (MFA) as defined by the REFEDS MFA Profile [10], ensuring a higher level of identity assurance.
- IDEM-P3: The highest level, requiring an electronic identity card or passport for verification, as well as Multi-Factor Authentication.

These profiles ensure that the federation meets diverse assurance needs, from basic access to high-security applications, and align with the broader European and global standards based on the REFEDS Assurance Framework.

6.2. Signal, Request, Assertion

In addition to the identity assurance assertions based on the REFEDS Assurance Framework, the IDEM assurance profiles provide methods to signal support and adherence to specific assurance profiles directly in the metadata of the Identity Provider, implementing the SAML identity assurance profile specification [11].

Home Organizations that want to assert support for an assurance profile, must submit a compliance declaration targeting a specific assurance profile (i.e. IDEM-P2) to the IDEM federation operator. After the due verification process, the IDEM federation operator will add the IDEM profile support information in the entity metadata, resigning it to provide authenticity and validity. Moreover, the IDEM assurance profiles explicitly define how to request and process assurance information in a federated authentication flow.

7. Conclusion

The trust and identity assurance mechanisms in research and education identity federations are fundamental to the secure and efficient operation of digital resources for the global scientific

community. As the eduGAIN inter-federation service and national federations continue to expand and integrate more diverse entities, the adoption of specifications like REFEDS Assurance Framework will be critical. These frameworks enhance security and trust in identity federations, enabling the support of advanced use cases, such as e-health and life sciences, high performance computing, and the like.

The ongoing efforts to refine and expand these standards reflect the dynamic nature of digital identity management in research and education, as well as the continually evolving technological landscape. By adhering to robust specifications and fostering trust at all levels, research and education federations will be able to support both current advanced use cases and new identity paradigms, like verifiable credentials and distributed identities.

References

[1] eduGAIN, 2024. URL: https://edugain.org.

[2] REFEDS, REFEDS Assurance Framework, 2023. URL: https://refeds.org/assurance.

[3] Consortium GARR, IDEM GARR AAI, 2024. URL: https://www.idem.garr.it/.

[4] OASIS Open, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 2005. URL: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[5] OASIS Open, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 2005. URL: https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

[6] eduGAIN, eduGAIN SAML Profile, 2018. URL: https://wiki.geant.org/display/eduGAIN/eduGAIN+SAML+Profile.

[7] IDEM, Profili di garanzia delle identità digitali della Federazione IDEM, 2023. URL: https://wiki.idem.garr.it/wiki/File:Profili_di_garanzia_delle_identit%C3%A0_digitali_della_Federazione_IDEM-v1.pdf.

[8] European Union, Implementing Regulation (EU) 2015/1502, in: Official Journal of the European Union, volume OJ L 235/7, 2015. URL: https://data.europa.eu/eli/reg_impl/2015/1502/oj.

[9] AGID, Sistema Pubblico di Identità Digitale (SPID), 2024. URL: https://www.spid.gov.it/.

[10] REFEDS, REFEDS MFA Profile – Version 1.2, 2023. doi:10.5281/zenodo.10135577.

[11] OASIS Open, SAML V2.0 Identity Assurance Profiles Version 1.0, Committee Specification, 2010. URL: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cs-01.pdf.