Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

terabit

Research and Education Assurance Standards and Policies for the federation of ICSC and TeraBit HPC resources

Davide Vaghetti (GARR) davide.vaghetti@garr.it

Work-Package Leaders Meeting | 15 - 16 ottobre 2024

ICSC AAI Trust and Assurance Objectives

- Support for project **participants' identity providers** and **Research and Education Identity Federations' Users**.
- Users' **level of assurance 2** (ref. ITU-T X1254 09/2020).
- External R&E Identity Providers will be connected through **eduGAIN** if they will meet infrastructure requirements.

Infrastructures and bodies for R&E AAI Interoperability

A common trust infrastructure eduGAIN

A collaborative specifications bodies REFEDS

An forum for the advancement of AAI for Research AARC

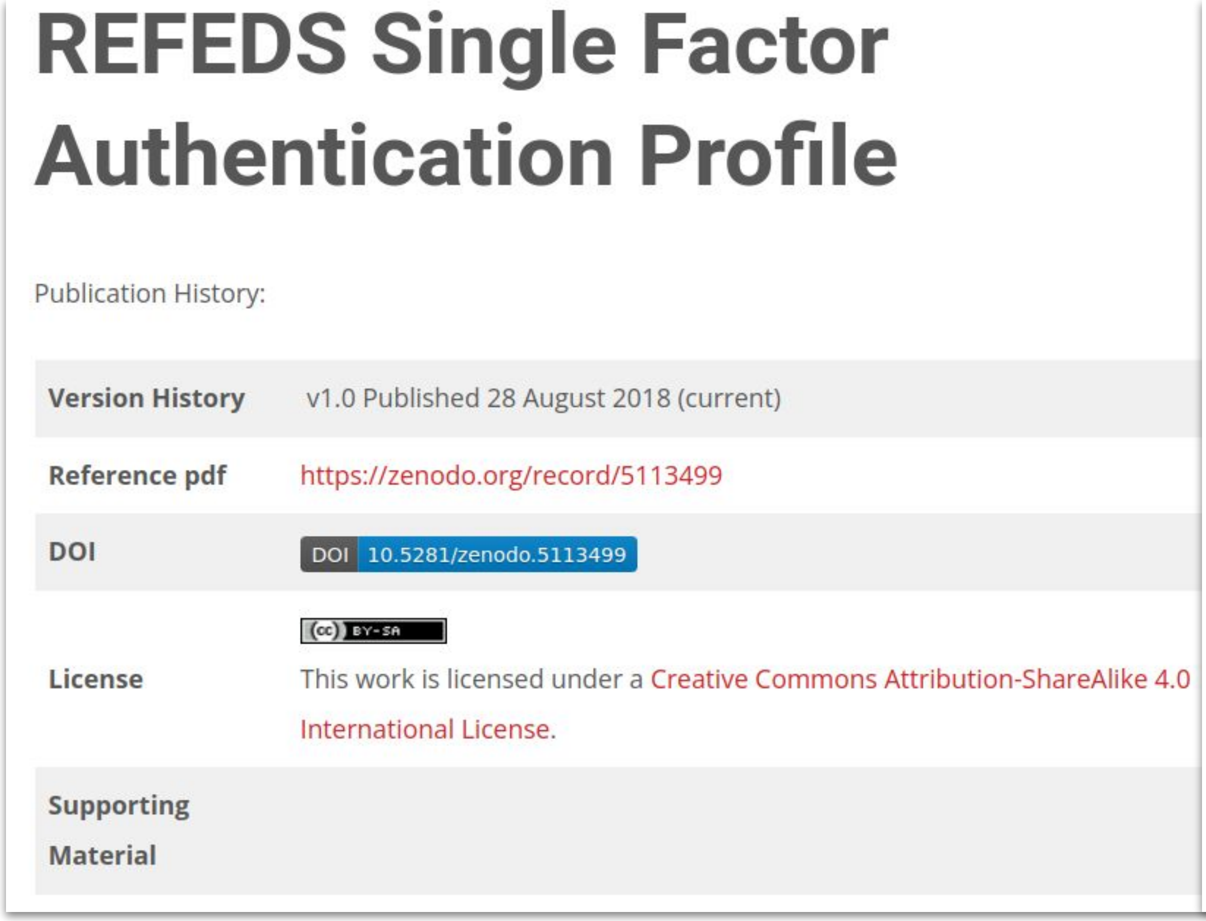
Refeds Assurance Framework componentes

Identifier Uniqueness	A method to communicate to the RP that the user's identifier (such as a login name) is unique, and is only bound to one identity in the CSP's context.	`ID/unique` `ID/eppn-unique-no-reassign`

Identity Assurance	A method to communicate to the RP how certain the CSP was at enrollment time of the real-world identity of the Person to whom the account was issued.	`IAP/low`
		`IAP/medium`
		`IAP/high`

Attribute Assurance	A method to communicate to the RP regarding the quality and freshness of attributes (other than the unique identifier) passed in the login assertion.	`ATP/ePA-1m` `ATP/ePA-1d`

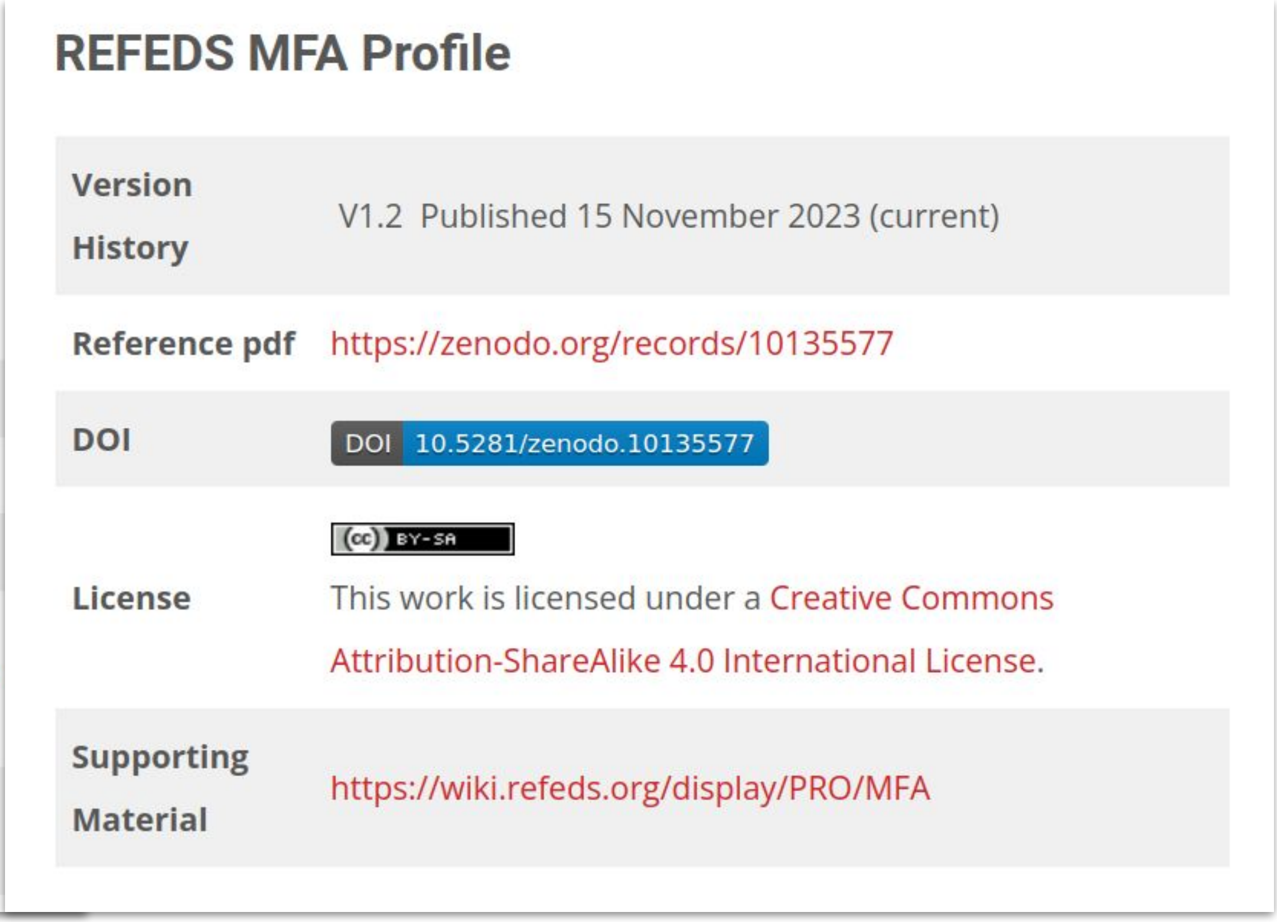
REFEDS Authentication Profiles: SFA and MFA



REFEDS Single Factor Authentication Profile

Publication History:

Version History	v1.0 Published 28 August 2018 (current)
Reference pdf	https://zenodo.org/record/5113499
DOI	DOI 10.5281/zenodo.5113499
License	(cc) BY-SA This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Supporting Material	



REFEDS MFA Profile

Version History	V1.2 Published 15 November 2023 (current)
Reference pdf	https://zenodo.org/records/10135577
DOI	DOI 10.5281/zenodo.10135577
License	(cc) BY-SA This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Supporting Material	https://wiki.refeds.org/display/PRO/MFA

Assurance Framework Mapping

REFEDS Assurance Framework	RAF IAP low	RAF IAP medium	RAF IAP high	
IDEM Assurance Profiles	IDEM-P0	IDEM-P1	IDEM-P2	IDEM-P3
INFN AAI LoA	INFN AAI LoA1	INFN AAI LoA2		
eIDAS Levels of Assurance	eIDAS LoA Low		eIDAS LoA Substantial	eIDAS LoA High
NIST 800-63-3 IAL and AAL	NIST 800-63-3 IAL1/AAL1		NIST 800-63-3 IAL2/AAL2	NIST 800-63-3 IAL3/AAL3
Italian eGOV-ID	/	/	SPID-L1, SPID-L2, SPID-L3	CIE
ITU-T X1254 (09/2012)	LoA1	LoA2	LoA3	LoA4
ITU-T X1254 (09/2020)	/	AAL1	AAL2	AAL3

REFEDS Sirtfi

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations

Operational Security

information resources … availability and integrity ... confidentiality of sensitive information

Traceability

be able to answer the basic questions "who, what, where, and when" concerning a security incident

Incident Response

a security incident response capability exists within the organisation

Participant Responsibilities

All participants (IdPs and SPs) in the federations need to rely on appropriate behavior.

A roadmap for the ICSC AAI: from POC to PROD

- Step 0: define requirements.
- Step 1: define an incremental roadmap based on milestones.
- Step 2 to N-1: Implement milestones.
- Step N: Review and prepare for production.

Requirements

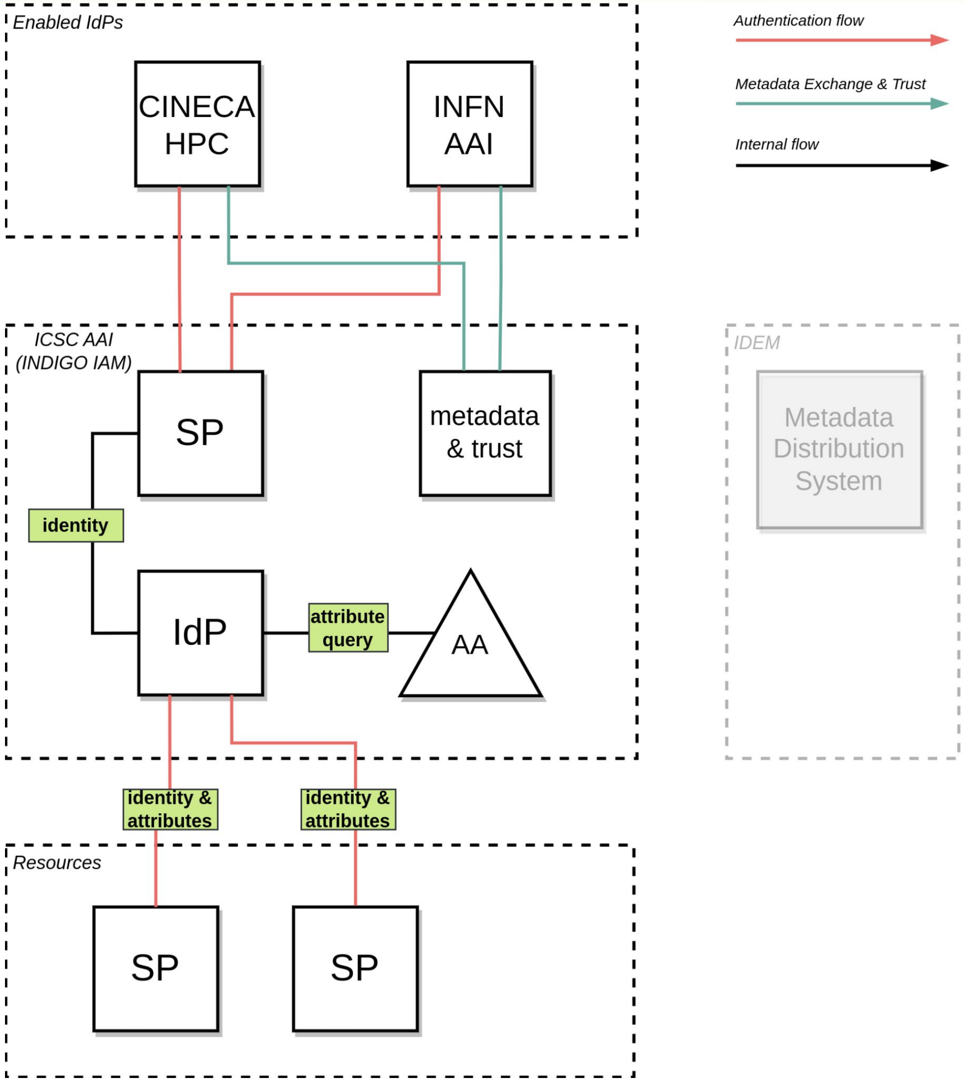
IDP-R01	The IdP is registered in IDEM or in a Research and Education Federation that participates to eduGAIN.
IDP-R02	The IdP respects the IDEM Technical Profile requirements [IDEM-TP].
IDP-R03	The IdP respects the eduGAIN SAML Profile requirements [eduGAIN-SAML-Profile].
IDP-R04	The IdP supports the REFEDS Security Incident Response Trust Framework for Federated Identity version 2.0 [REFEDS-SIRTFI-v2].
IDP-R05	The IdP supports IDEM GARR AAI Identity Assurance Profiles [IDEM-IA-v1], or the REFEDS Assurance Framework version 2.0 [REFEDS-RAF-v2].
IDP-R06	The IdP supports unique identifiers as defined in [IDEM-IAP-v1] or [REFEDS-RAF-v2].
IDP-R07	The IdP supports a level of assurance up to IDEM-P2, RAF High, eIDAS substantial (all equivalent to the Level of Assurance 2 as defined in ITU-T X1254 09/2020).
IDP-R08	The IdP supports multi factor authentication as defined in the REFEDS Multi Factor Authentication Profile version 1.2.
IDP-R09	The IdP releases the attribute set defined by the ICSC AAI.

A 3 milestones roadmap proposal

- Milestone 1
  - The ICSC AAI PoC will initially connect the INFN and CINECA IdPs by direct metadata exchange and it will not enforce identity assurance checks.
- Milestone 2:
  - The ICSC AAI PoC will join the IDEM Federation and verify assurance information for the INFN IdP, but it will not enable external IdPs.
- Milestone 3:
  - Along with the CINECA and the INFN IdPs, the ICSC AAI PoC will enable selected external IdPs published by the IDEM Federation and compliant with the defined requirements.

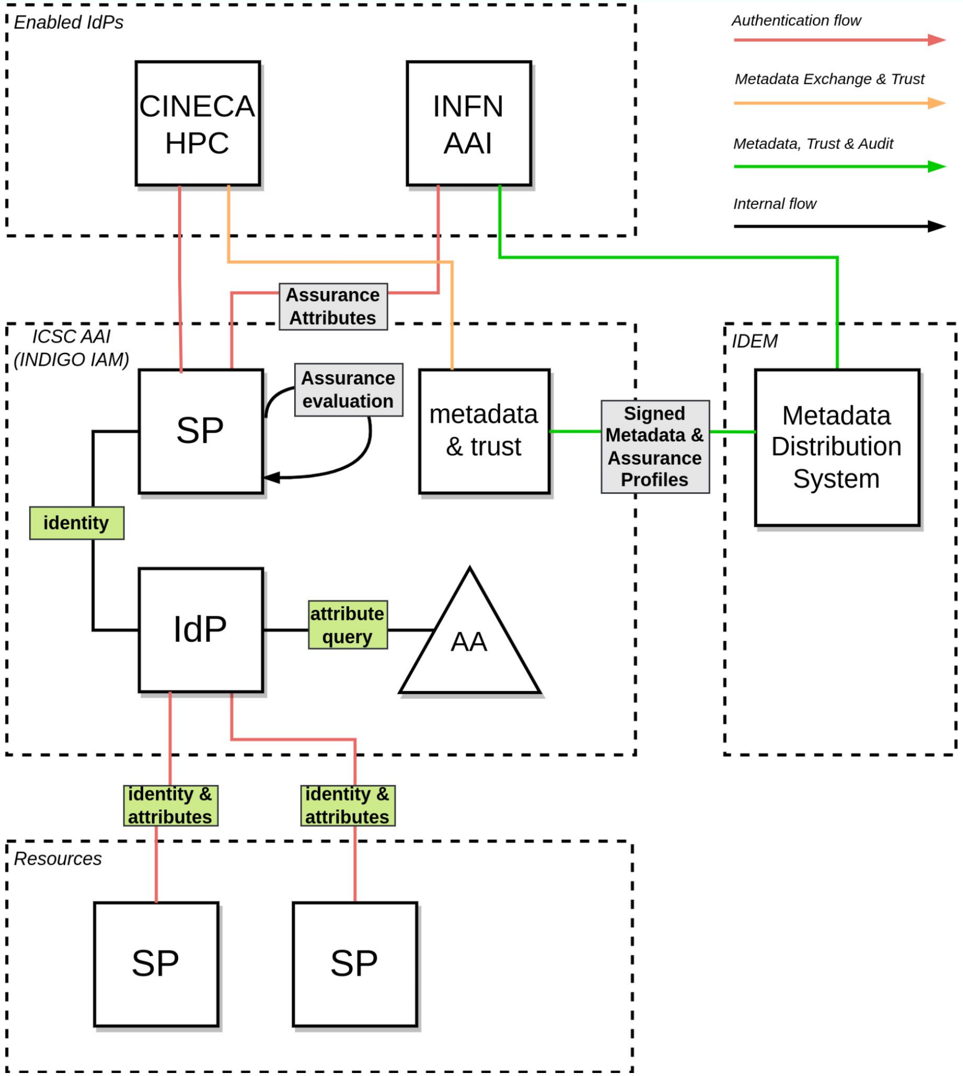
Milestone 1

The ICSC AAI PoC will initially connect the INFN and CINECA IdPs by direct metadata exchange and it will not enforce identity assurance checks.



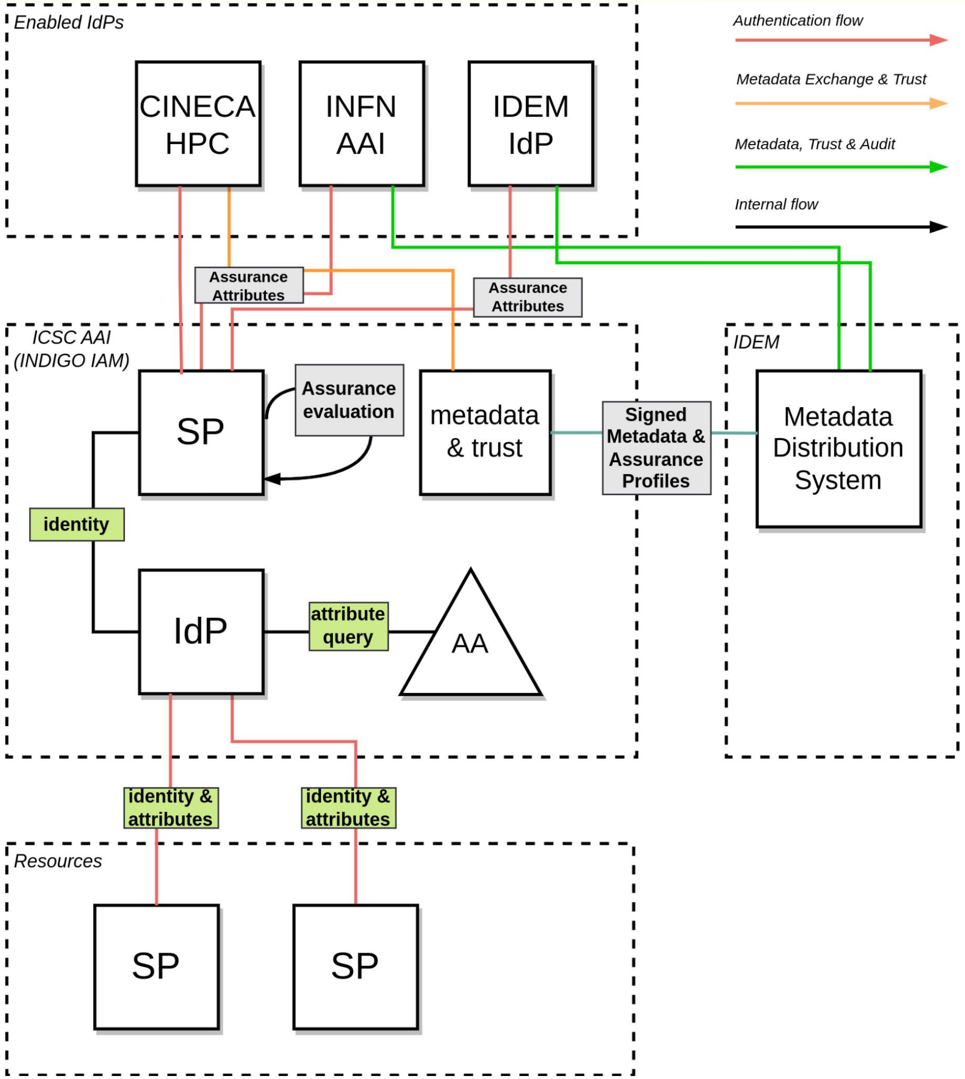
Milestone 2

The **ICSC AAI PoC will join the IDEM** Federation, but **it will not enable external IdPs**. However, the INFN metadata will be imported through the IDEM Federation Metadata Distribution System. Moreover, the ICSC AAI will begin to **verify identity assurance information** about the authenticated users of both the CINECA and the INFN IdPs, and it will issue warnings about the users that will not comply with the requirements IDP-R06, IDP-R07, IDP-R08, IDP-R09.



Milestone 3

Along with the CINECA and the INFN IdPs, the ICSC AAI PoC will enable selected external IdPs published by the IDEM Federation and compliant with the above defined requirements (from IDP-R01 to IDP-R09). The IdPs will be selected on the base of the participation of their users to actual ICSC research projects and resource needs.



Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

terabit

Thanks!