IDEM assurance profiles and the international identity assurance landscape

Davide Vaghetti (GARR)
<davide.vaghetti@garr.it>
IDEM GARR AAI Coordinator
eduGAIN Service Owner
GARR Data Protection Officer

Workshop sul Calcolo nell'I.N.F.N.
Palau (Sassari) 20 - 24 maggio 2024

Trust and Identity Assurance in identity federations

TRUST

Trust level of confidence on an entity - standards and policies compliance, reliability.

ASSURANCE

Assurance is the level of confidence on an identity, or an attribute, as asserted by a trusted party - identity proofing quality, authentication reliability, etc.

IDEM, the Italian Research and Education Identity Federation

IDEM lets millions of students and researchers to seamlessly and securely access research services leveraging their institutional credentials.
IDEM participates to eduGAIN, the global inter-federation service that hosts thousands of services world-wide, from academic journals to the services dedicated to large scientific experiments, such as CERN's LHC and European and American Gravitational Observers.

IDEM GARR AAI Service

Federations standards and policies

Metadata management, signing and distribution

Technical Support

Documentation and Training

IDEM Technical Committee

Working Groups and Guide Lines

150
Members

80
Partners

1.800.000
Students and Researchers

100%
State Universities

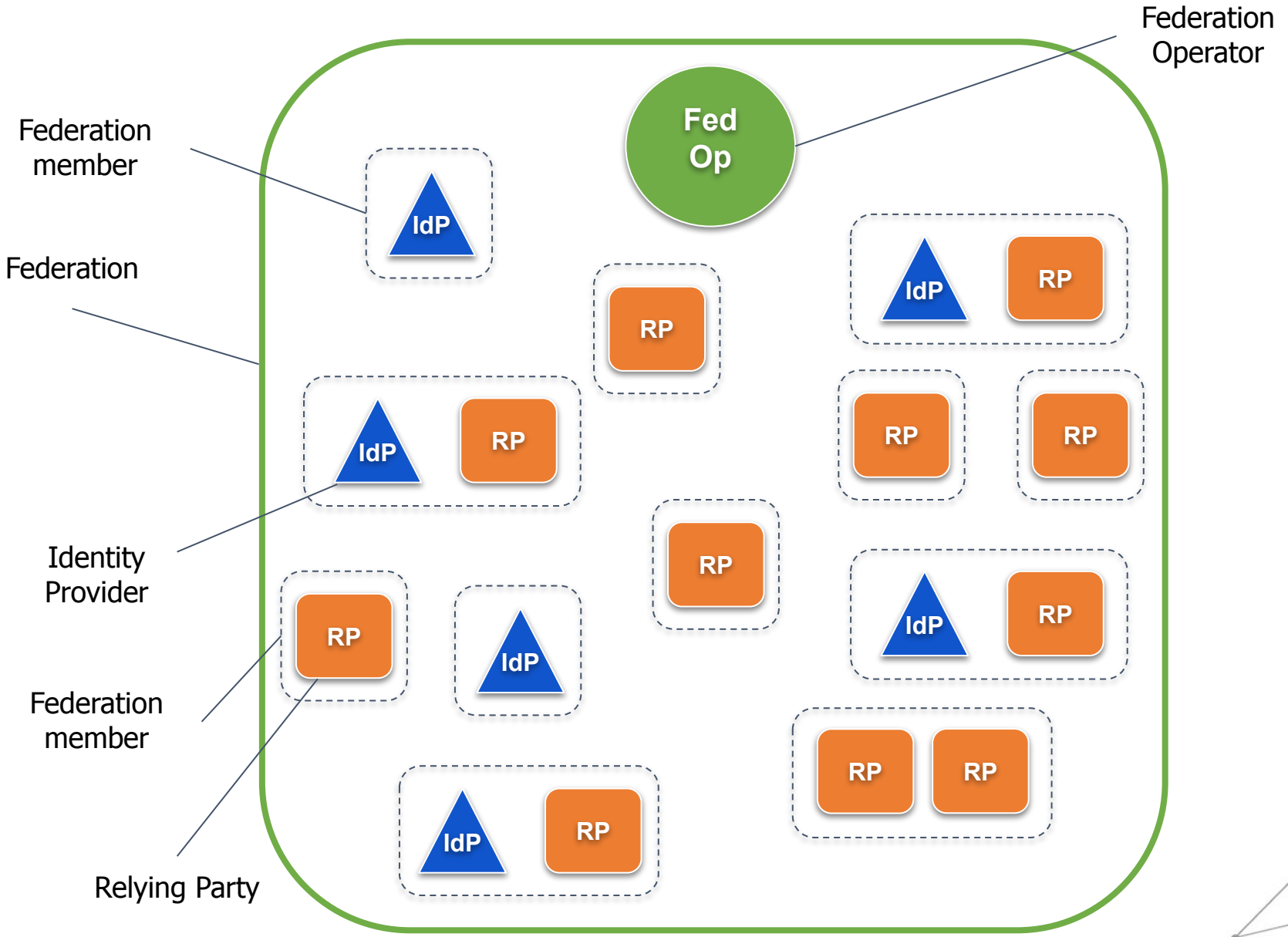
3.663
National and global resources

500.000.000
Annual logins*
**projection based on actual data*

https://www.idem.garr.it

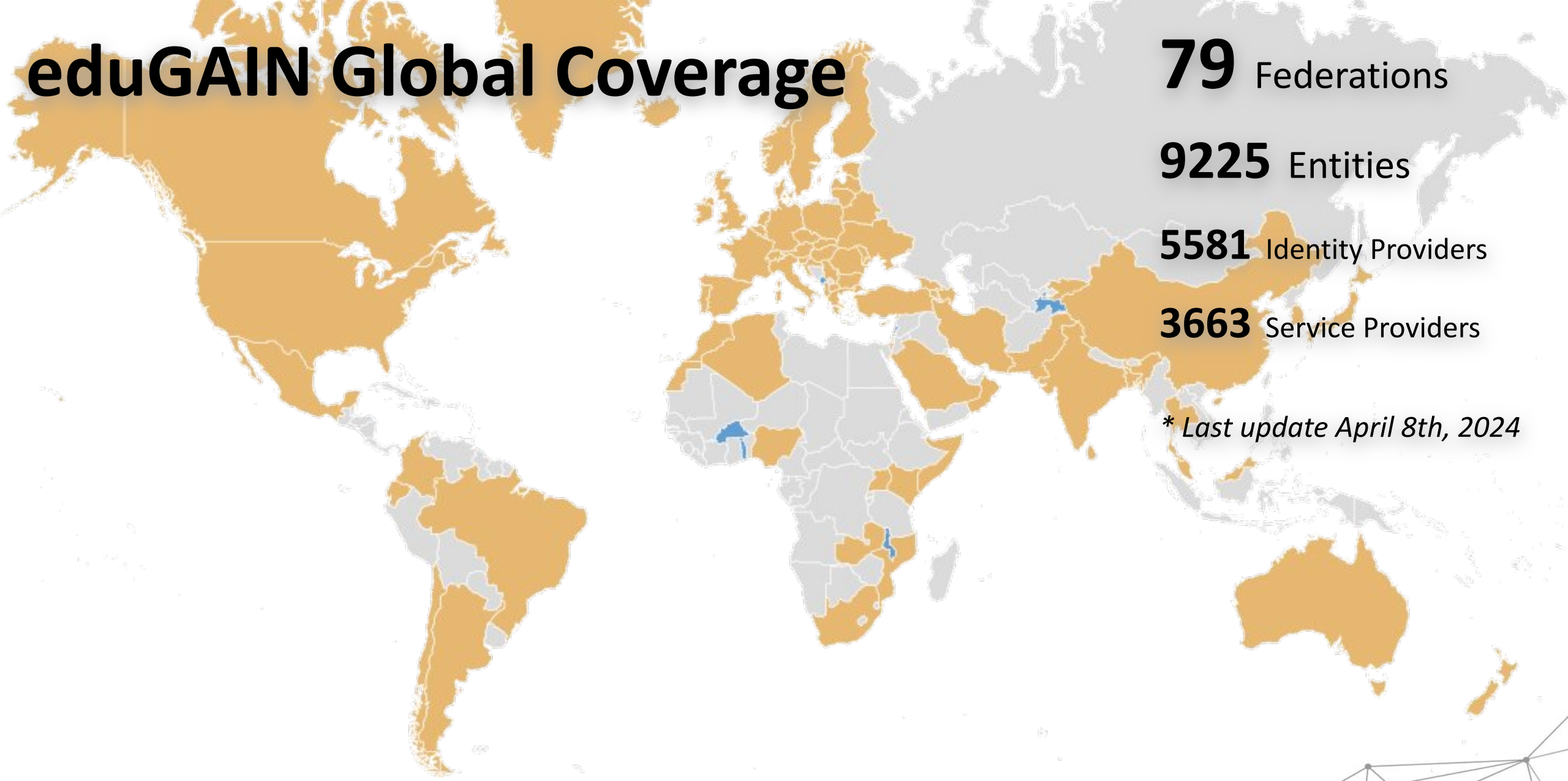
Research and Education Identity Federations

- NREN membership
- community governance
- open standards
- multilateral
- trusted 3d party
- signed metadata
- inter-Federation AKA
- eduGAIN



*"eduGAIN **interfederation service** connects identity federations around the world, simplifying **access** to content, services and resources for the **global** research and education community"*

eduGAIN Global Coverage



79 Federations

9225 Entities

5581 Identity Providers

3663 Service Providers

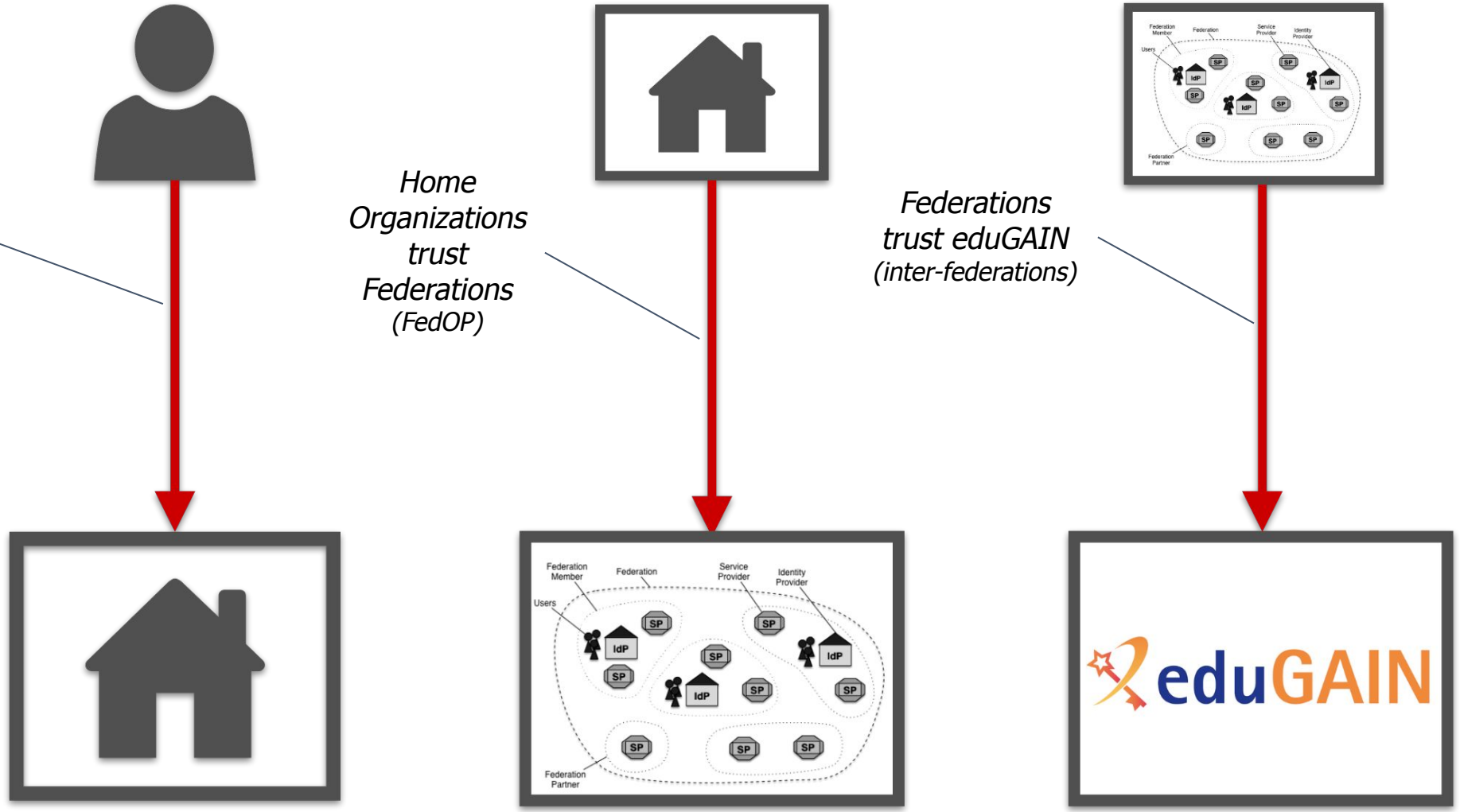
** Last update April 8th, 2024*

Trust flows in R&E Identity Federations

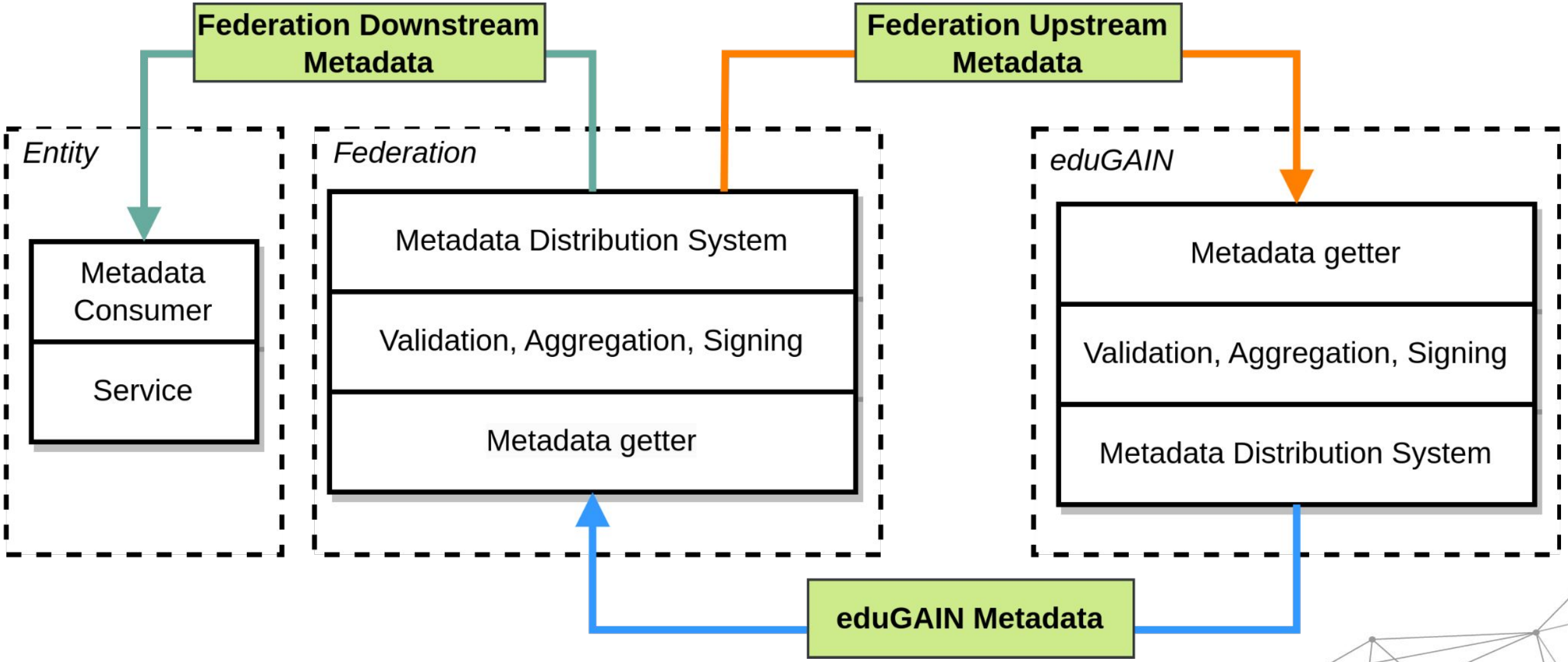
Users trust Home Organizations

Home Organizations trust Federations (FedOP)

Federations trust eduGAIN (inter-federations)



Signed metadata



REFEDS Assurance Framework

To manage risks related to the access control of their services, the Relying Parties of the research and education federations need to make decisions on how much to trust the assertions made by the Identity Providers [..]

https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0

RAF Components

Identifier uniqueness	single natural person the person can be contacted by the CSP the user identifier is never re-assigned the user identifier is one of eduPersonUniqueID, SAML 2.0 subject-id or OIDC sub	**ID/unique** **ID/eppn-unique-no-reassign**
Identity proofing and credential management	Processes by which the CSP captures and verifies sufficient information to identify a user and issue, renew and replace an associated set of credentials. It is expressed as a	**IAP/low** **IAP/medium** **IAP/high**
Attribute Assurance	Quality and freshness of attributes. Currently implemented only for eduPersonAffiliation, it shows the latency in affiliation update.	**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

REFEDS SFA - Single Factor Authentication

Authentication Type	Base	Minimum Length
Memorized secret	>= 52 characters	12 characters
	>= 72 characters	8 characters
OTP (one time **generated** secrets)	10-51 characters	6 characters
	>= 52 characters	4 characters
Single use secret	10-51 characters	10 characters
	>= 52 characters	6 characters
Cryptographic Keys	RSA	2048 bit
	ECDSA	256 bit

REFEDS MFA Profile - Multi Factor Authentication

Authentication MUST use a combination of at least two of the four distinct types of factors:

- something an entity has (e.g., a hardware device containing a credential)
- something an entity knows (e.g., password)
- something an entity is (e.g., biometric)
- something an entity does (e.g., behavioural).

All the authentication types defined in the REFEDS SFA Profile can be used.

IMPORTANT: *Initial enrollment of one or more additional factors MAY take place subject to authentication by only a single factor. Subsequently, the factors used MUST be independent; this includes processes to recover, replace, or add authentication factors.*

Identity Assurance Frameworks and Standards

REFEDS

ITU

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

European Commission

kantara INITIATIVE

INFN Istituto Nazionale di Fisica Nucleare

- REFEDS Assurance Framework 1.0
- ITU-T X.1254 (ISO/IEC 29115:2019)
- Special Publication 800-63-3
- REGOLAMENTO DI ESECUZIONE (UE) 2015/1502 DELLA COMMISSIONE
- Kantara Initiative Identity Assurance Framework: Service Assessment Criteria
- INFN AAI LoA

spid

CARTA DI IDENTITÀ ELETTRONICA

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 Assurance Framework				
IDEM Assurance Profiles				
eIDAS Levels of Assurance				
NIST 800-63-3 IAL and AAL				
Italian eGOV-ID	natural person unique identifier self asserted single factor authN	natural person unique identifier authoritative source OR identity document proof single factor authN	natural person unique identifier identity document verification multi factor authN	natural person unique identifier identity document verification + biometric multi factor authN + strong authN
ITU-T X1254 (09/2012)				
ITU-T X1254 (09/2020)				

REFEDS Assurance Framework - use cases

- ELIXIR
- BBMRI

- LUMI (warning)
- FENIX (in progress)

- Grant Programs
- Datasets
- Research collaborations

IDEM Assurance Profiles

WHO the GARR and IDEM community, Universities, Research Centers, etc.

WHAT an IDEM specification that implements RAF for IDEM members.

WHEN 2021-2023

WHERE in the IDEM CTS Identity Assurance Working Group

WHY to be able to access RAF protected resources, foster the adoption of MFA, and compliance with international assurance standards.

HOW with the support of the IDEM GARR AAI Service as the trusted party that can play the role of auditor and certifier

IDEM Assurance Profiles key components

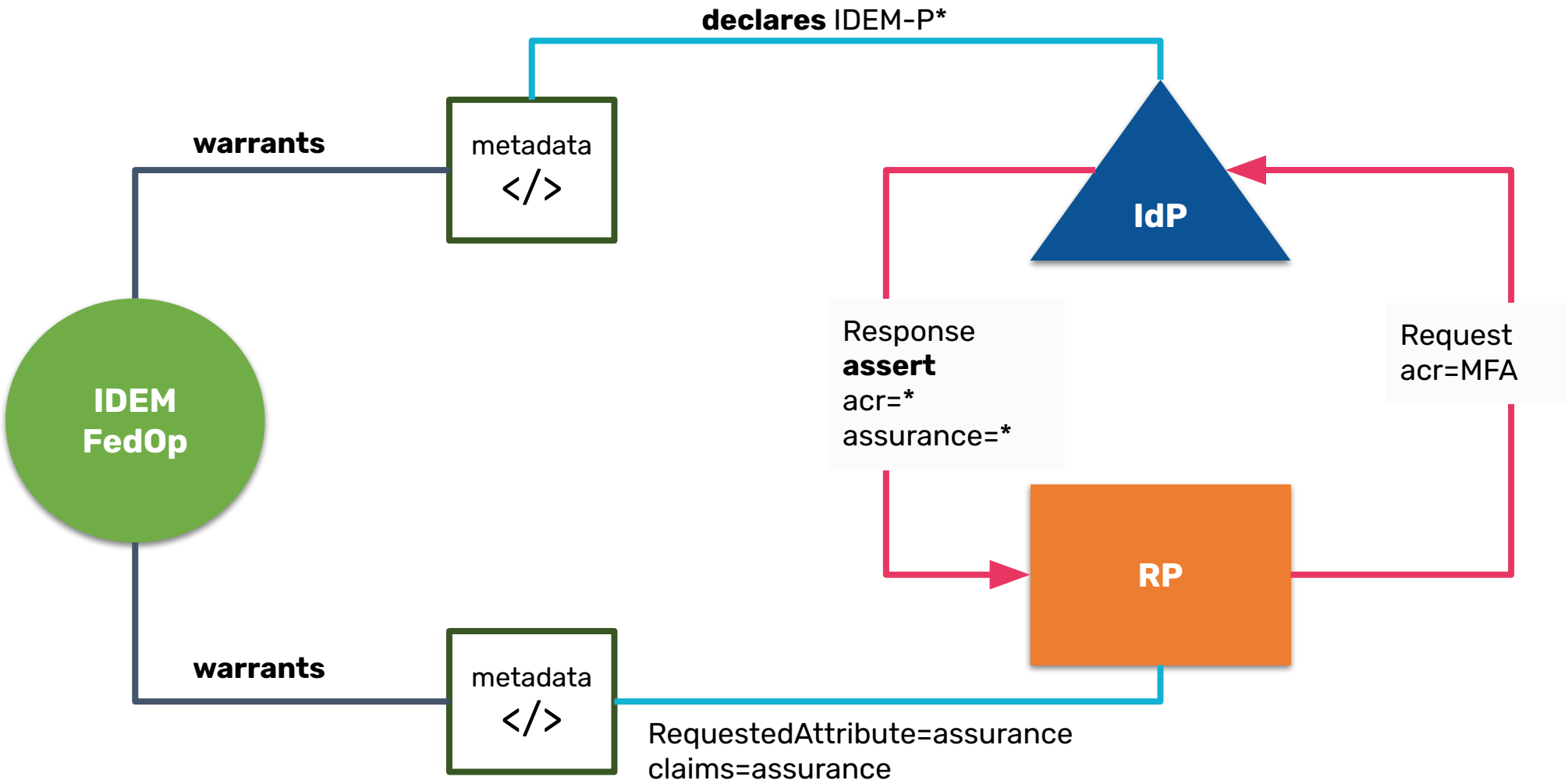
Identifiers	Identity verification and credential management	Attributes Quality
• Protocol identifiers (SAML 2.0/OIDC 1.0) • Natural Person • Contactable • No reassignment	• Registration and accreditation • Identity check and verification • Issuance, delivery and activation • Suspension, revocation and reactivation • Renewal and replacement	• Affiliation: student, staff, member • Update within 1 month • Update within 1 day

The Italian use case: IDEM Assurance Profiles

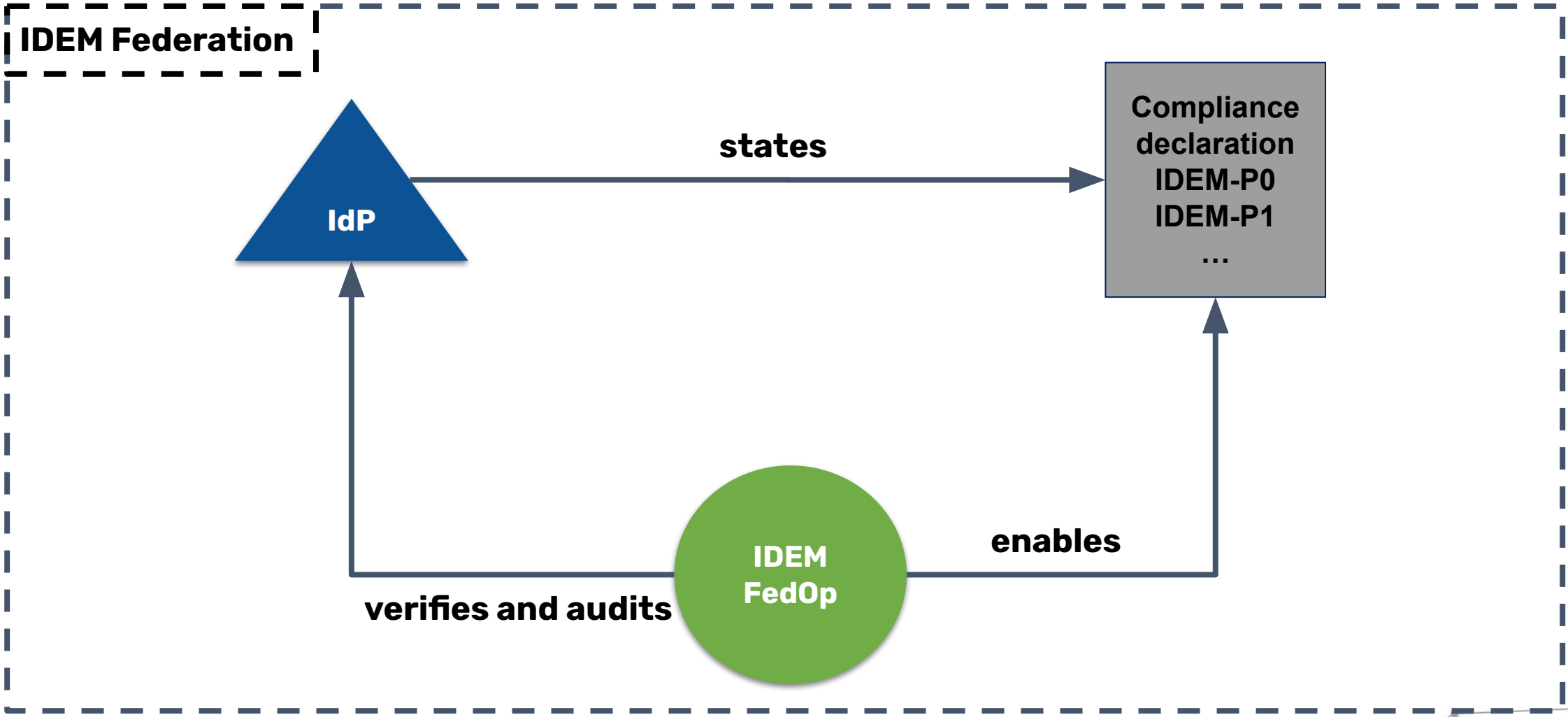
	IDEM-P0	IDEM-P1	IDEM-P2	IDEM-P3
Identifiers	Natural person, unique identifiers	Natural person, unique identifiers	Natural person, unique identifiers	Natural person, unique identifiers
Identity vetting	Contacts	Identity document	Identity document + verification	Electronic Identity Card or Passport
Attributes quality	-	Affiliation updated within one month*	Affiliation updated within one day*	Affiliation updated within one day*
Authentication	REFEDS SFA	REFEDS SFA	REFEDS MFA	REFEDS MFA

** if present*

IDEM Assurance profiles: signal, request, assertion



Context, Compliance and Audit



References

[eIDAS-LoA]
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015R1502
[ITU-T X.1254 09/2012]
https://www.itu.int/rec/T-REC-X.1254
[ITU-T X.1254 09/2020]
https://www.itu.int/rec/T-REC-X.1254
[NIST 800-63B]
https://doi.org/10.6028/NIST.SP.800-63b
[IDEM-Assurance-Profiles]
File:Profili di garanzia delle identità digitali della Federazione IDEM-v1.pdf
[IDEM-Assurance-Process]
https://wiki.idem.garr.it/wiki/AdesioneProfilidiGaranziaIDEM
[RAF-1.0] REFEDS Assurance Framework 1.0
https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0
[RAF-2.0] REFEDS Assurance Framework 2.0
https://refeds.org/wp-content/uploads/2023/12/RAF-2.0-Final-version.pdf
[REFEDS-SFA] REFEDS SFA Profile
https://doi.org/10.5281/zenodo.5113499
[REFEDS-MFA] REFEDS MFA Profile
https://doi.org/10.5281/zenodo.5113296
[SAML-IAP] SAML V2.0 Identity Assurance Profiles Version 1.0
https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html
[OIDC-Assurance] OpenID Connect for Identity Assurance 1.0
https://openid.net/specs/openid-connect-4-identity-assurance-1_0-13.html

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Questions welcomed