Trust and Assurance in R&E Identity Federations

Davide Vaghetti <davide.vaghetti@garr.it>

Trends in Digital Identity Workshop
Rome 2024

Agenda

NRENs and R&E Identity Federations

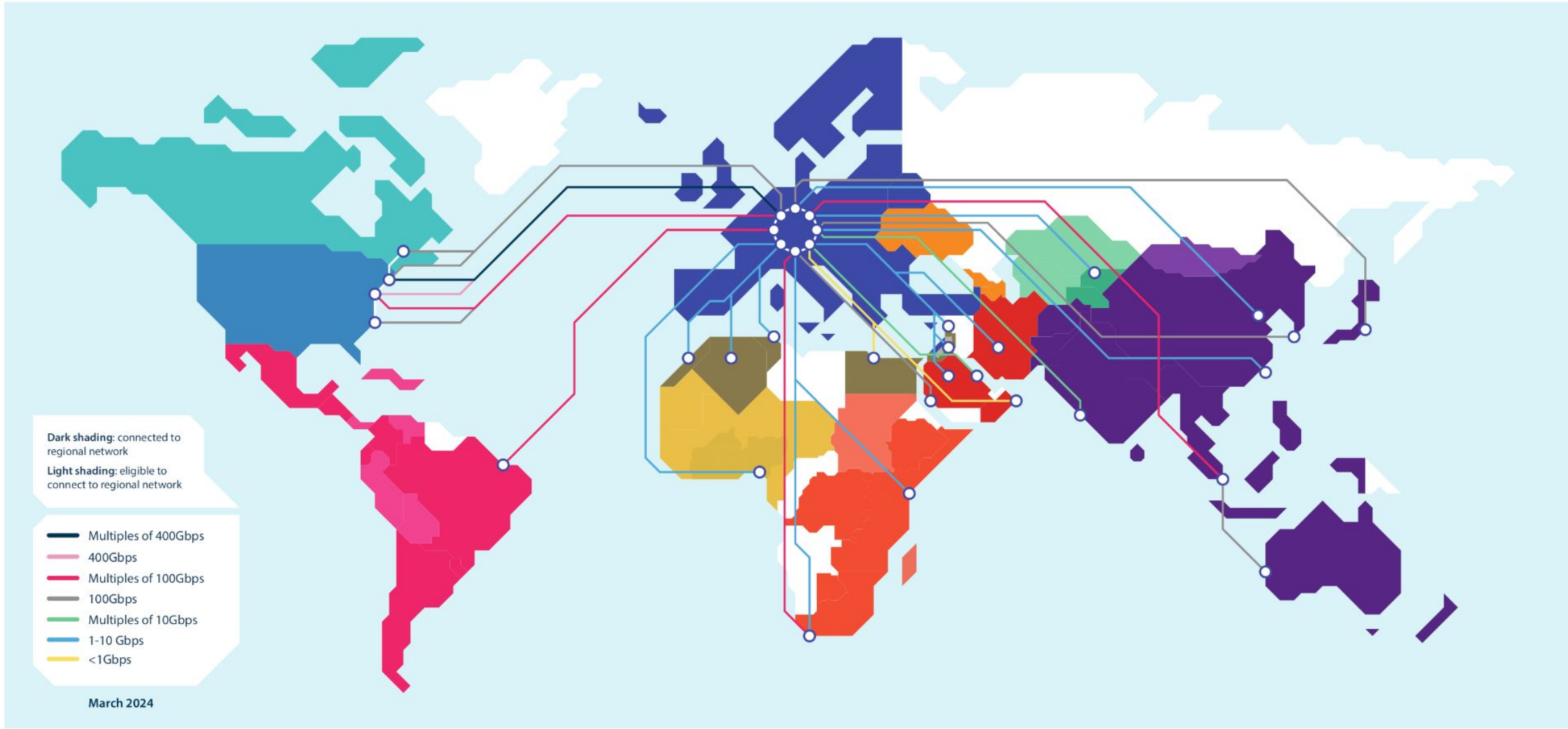
Trust flow

REFEDS Assurance Framework

IDEM Assurance Profiles

AT THE HEART OF GLOBAL RESEARCH AND EDUCATION NETWORKING

GÉANT



Canada & USA

canarie

ESnet

Latin America

Red CLARA

Europe

GÉANT

EU4Digital

EaPConnect

North Africa & Eastern Mediterranean

ASREN

West & Central Africa

Eastern & Southern Africa

UbuntuNet Alliance

Central Asia

CAREN

Asia-Pacific

TEIN

Other R&E Networks

ULTRA- HIGH CAPACITY INFRASTRUCTURE

20.000 Km

OPTICAL FIBRE

782 PB

ANNUAL DATA TRAFFIC

22 Tbps

BACKBONE CAPACITY

600 Gbps

INTERCONNECTION TO THE EUROPEAN GÉANT NETWORK

EXPLORE THE NETWORK

REAL TIME STATISTICS

GARR

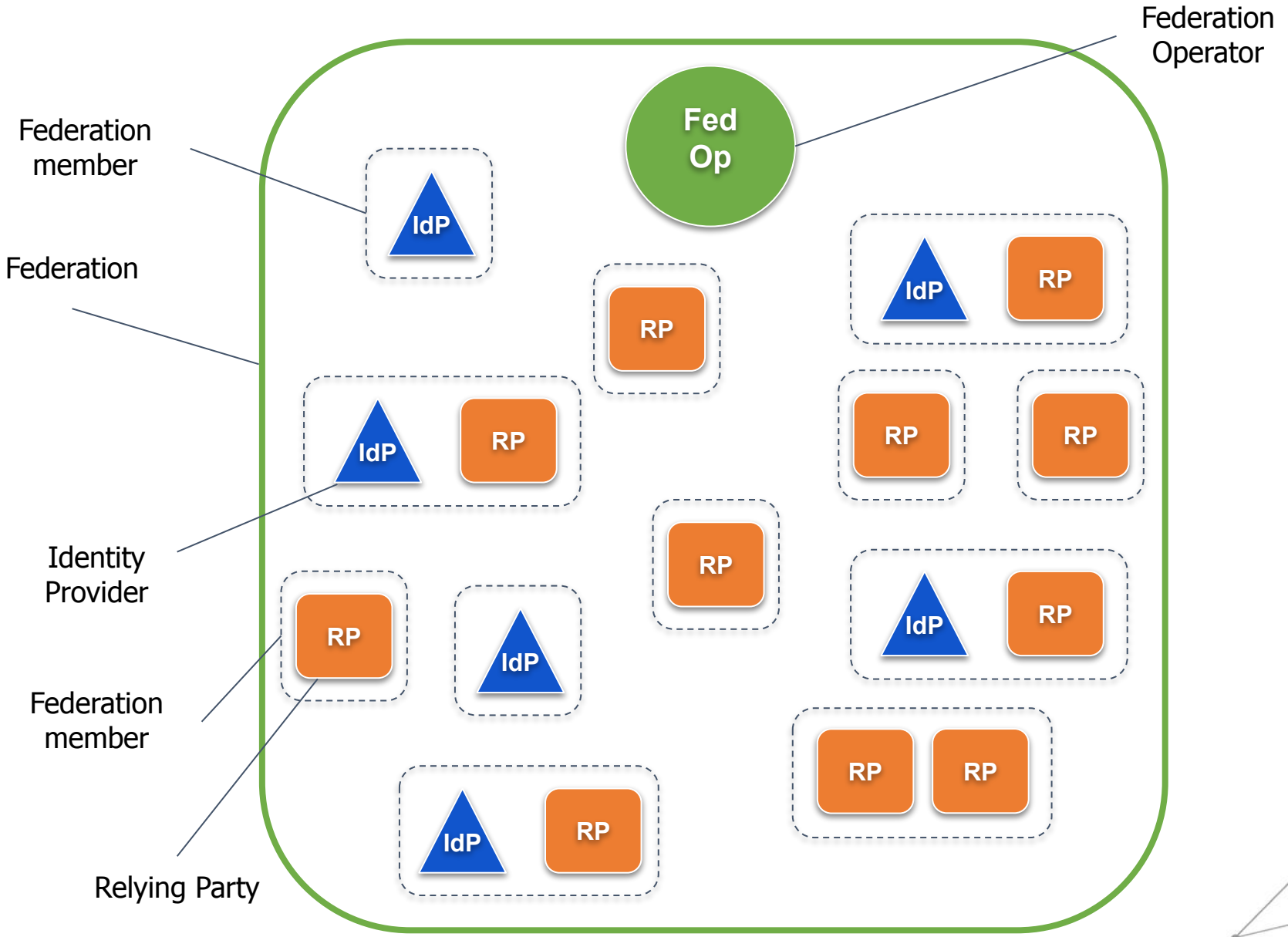
THE ITALIAN NATIONAL RESEARCH AND EDUCATION NETWORK

idem garr aai

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Research and Education Identity Federations

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



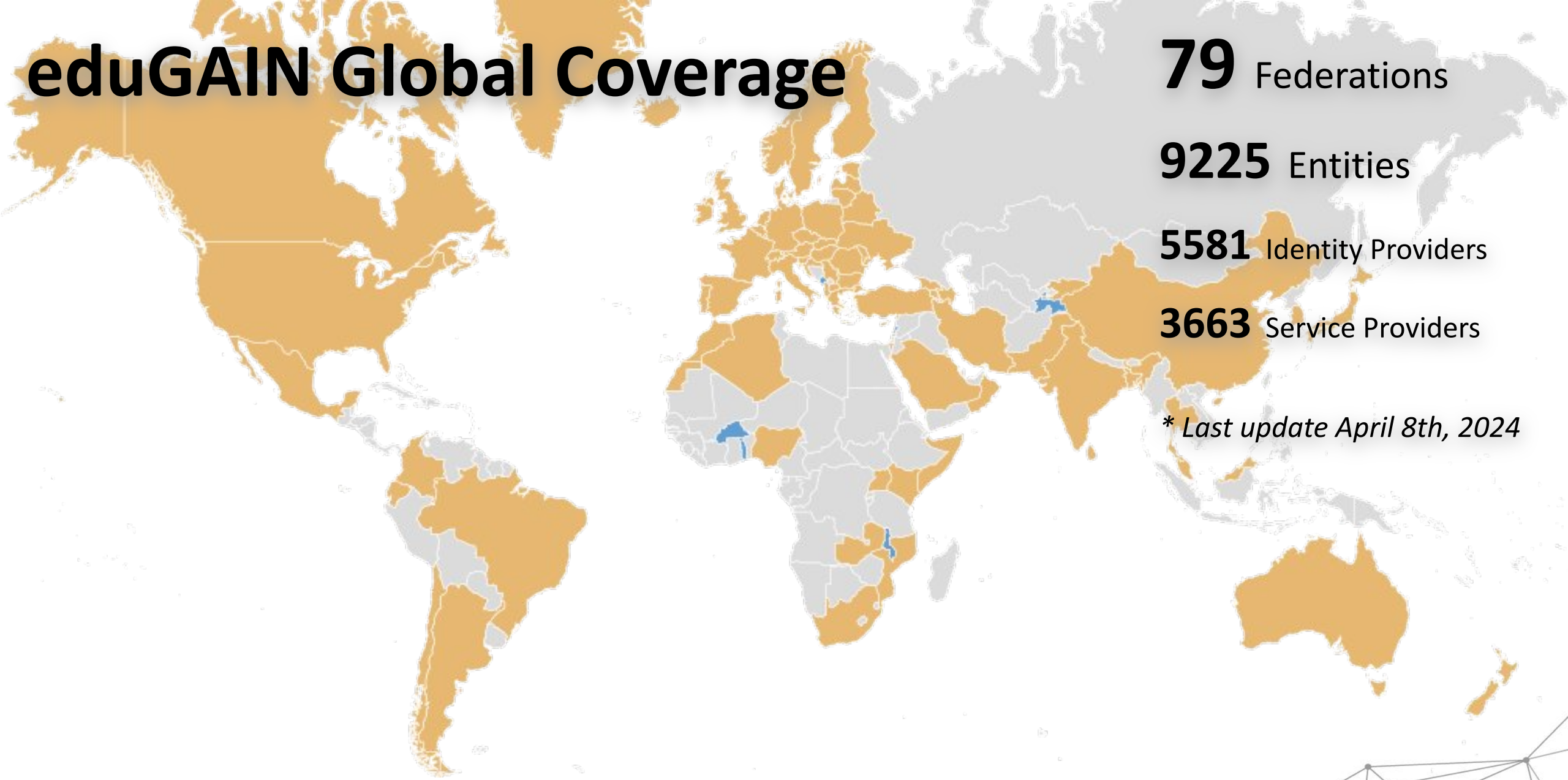
IDEM, the Italian R&E Identity Federation

150 Members and 152 Identity Providers
80 Partners and 132 Services
Cover 100% of the Italian State Universities
Serves around 2.000.000 Students, Researchers and Staff
eduGAIN Participants
REFEDS Participant

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

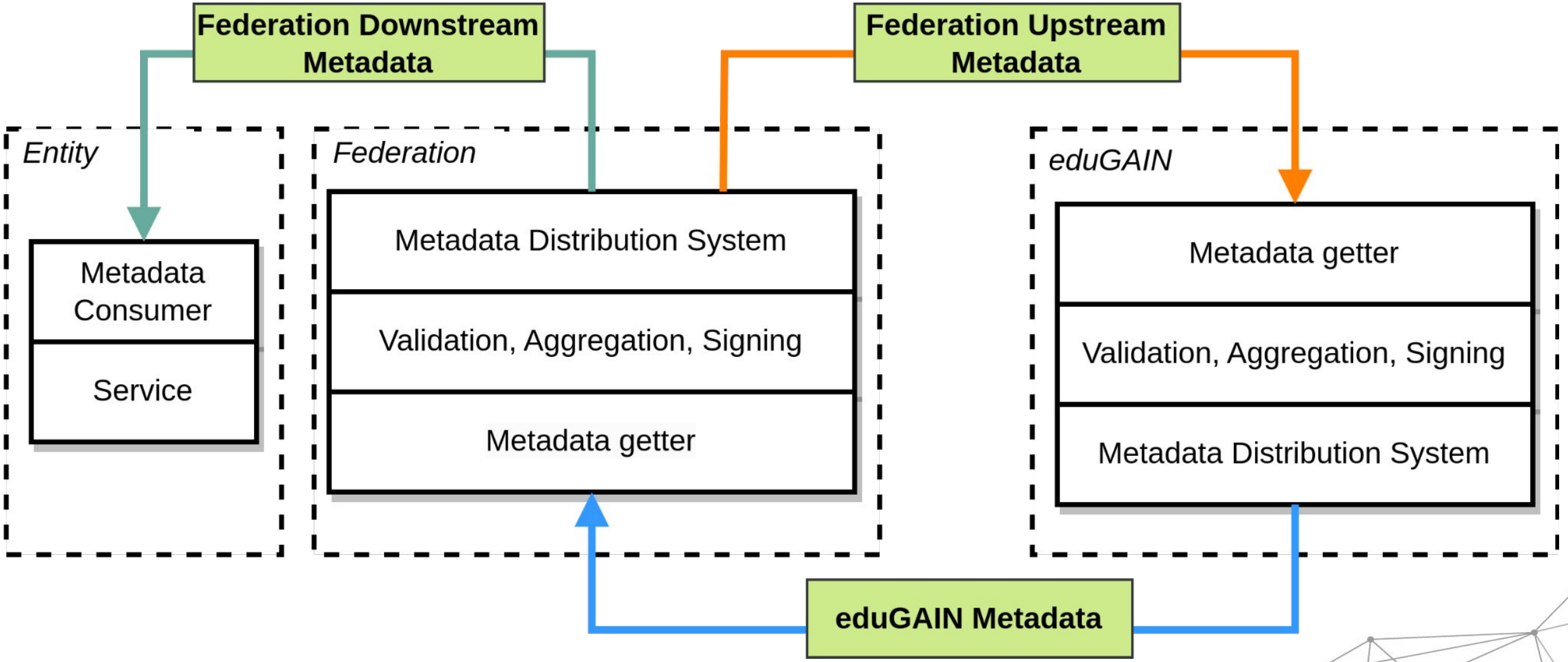
9225 Entities

5581 Identity Providers

3663 Service Providers

** Last update April 8th, 2024*

Signed metadata

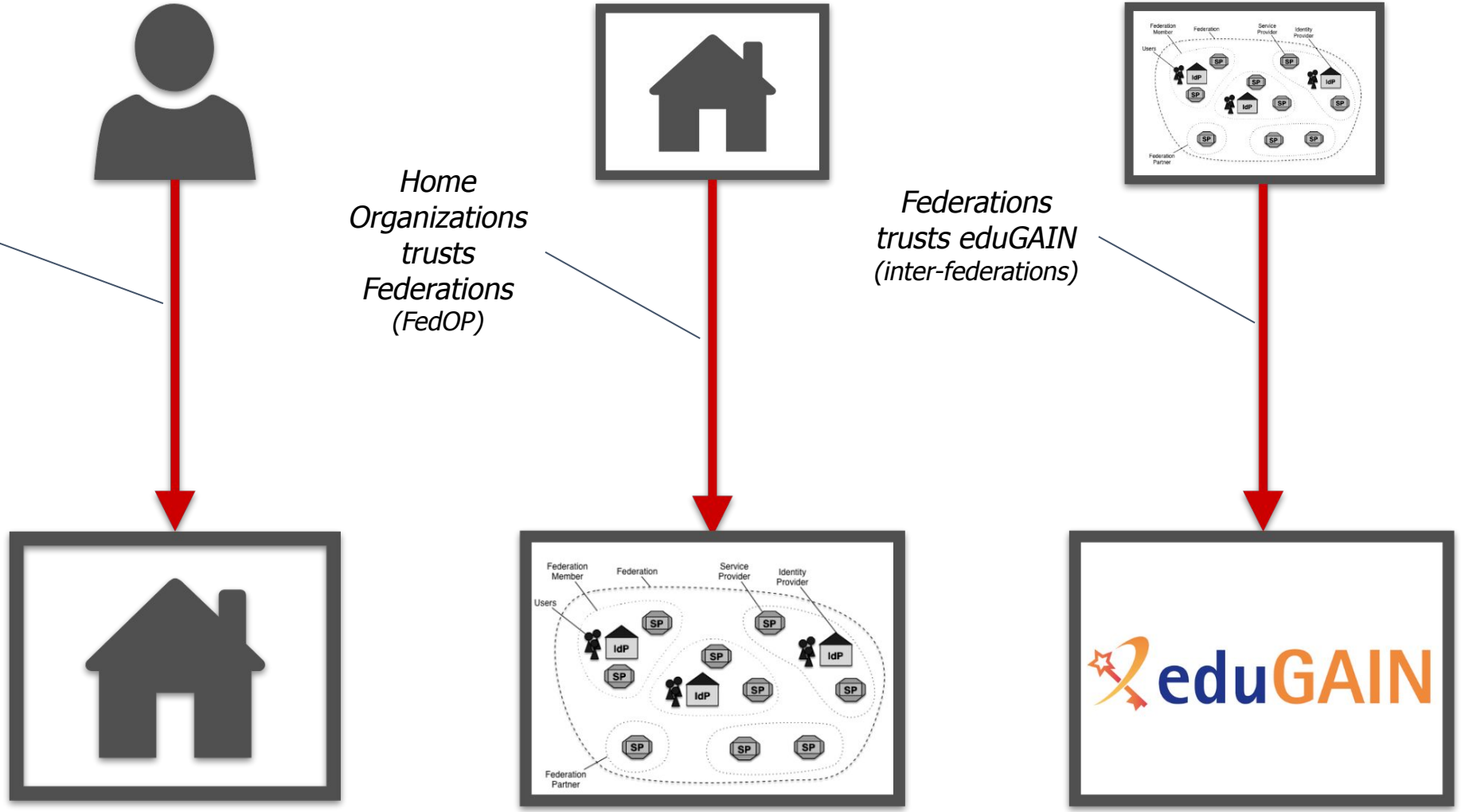


Trust flows in R&E Identity Federations

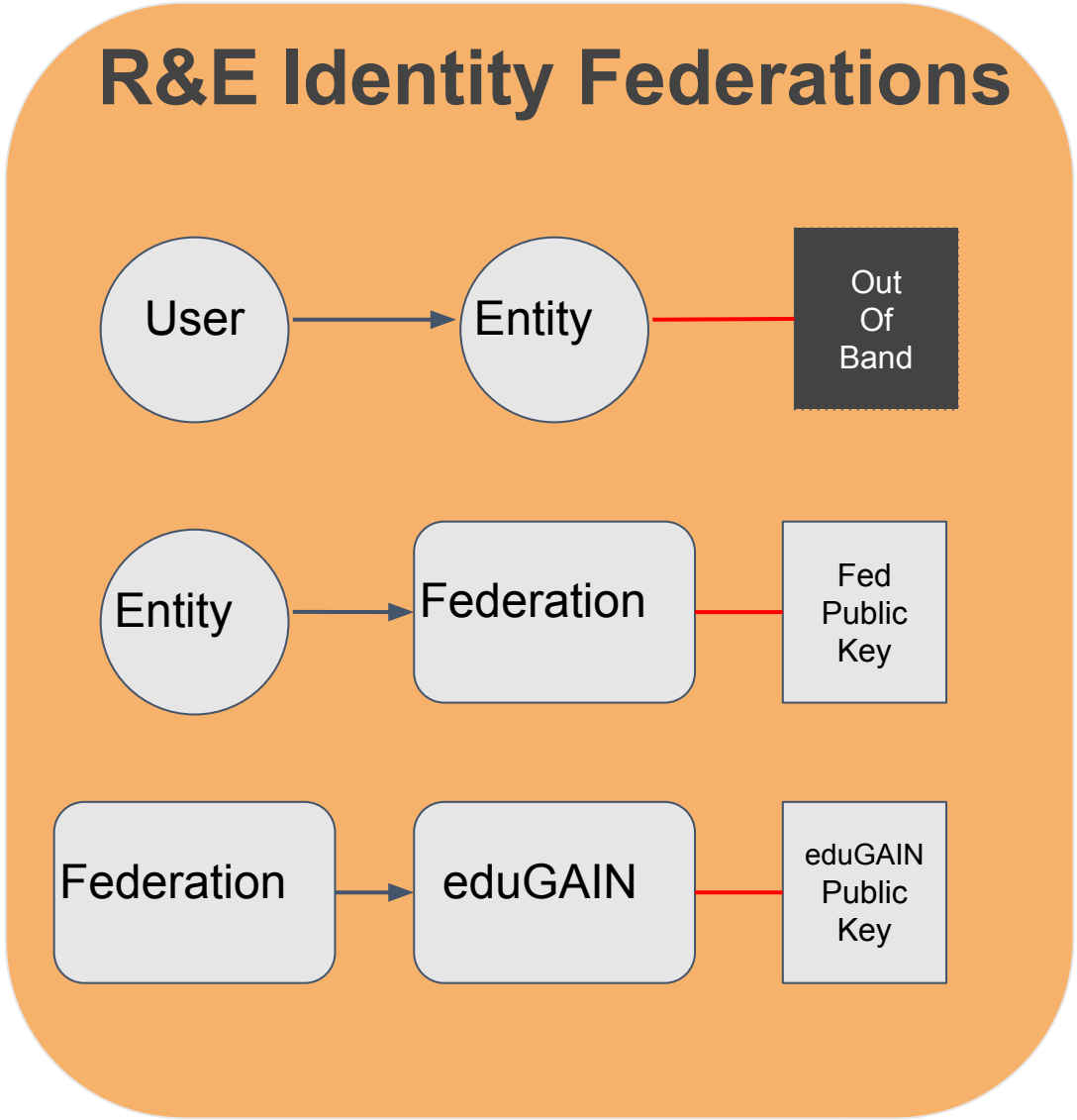
Users trusts Home Organizations

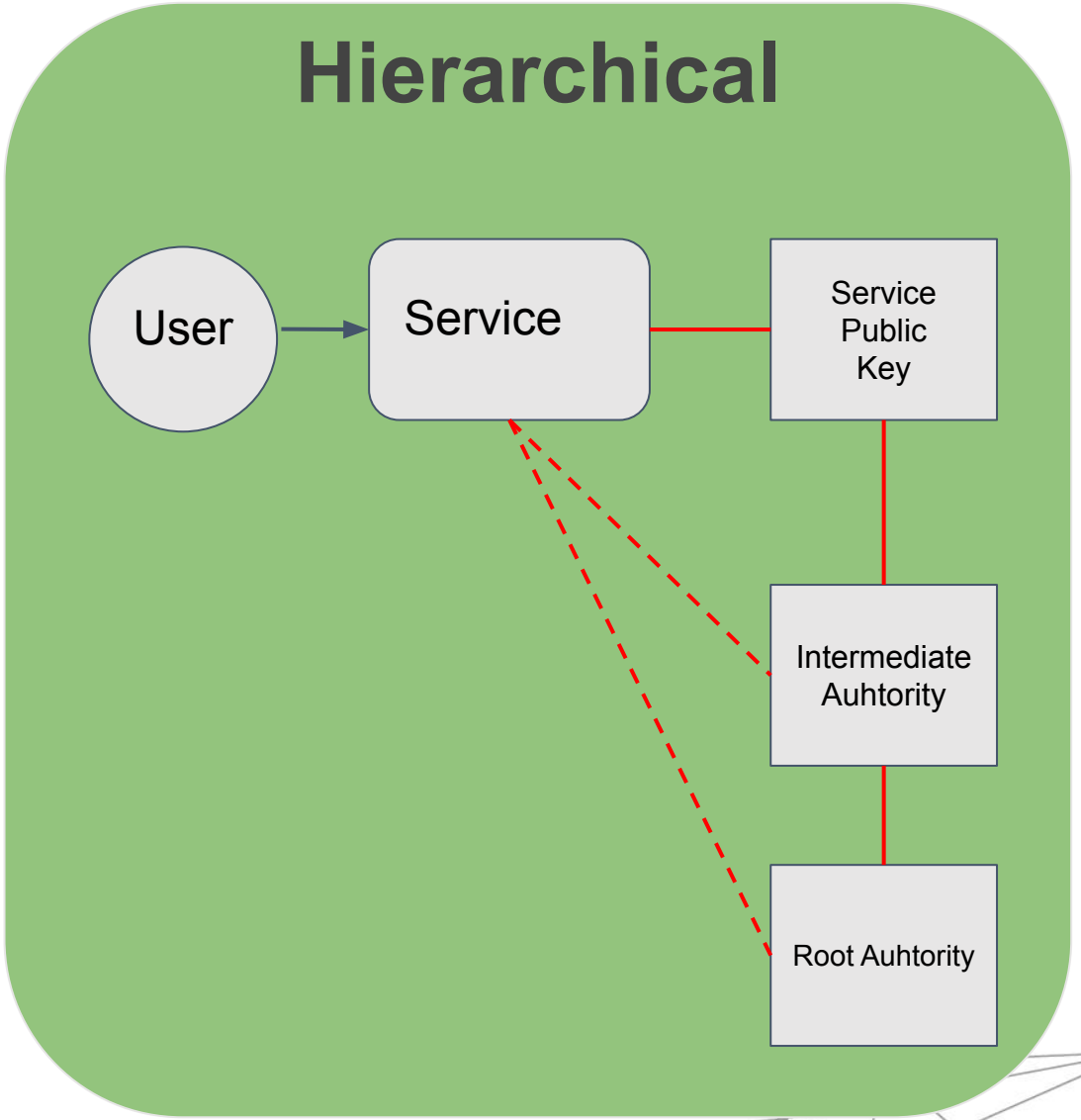
Home Organizations trusts Federations (FedOP)

Federations trusts eduGAIN (inter-federations)



Trust


R&E Identity Federations
User
Entity
Out Of Band
Entity
Federation
Fed Public Key
Federation
eduGAIN
eduGAIN Public Key


Hierarchical
User
Service
Service Public Key
Intermediate Auhtority
Root Auhtority

REFEDS Assurance Framework

"To manage risks related to federated access to their services, some Relying Parties in research and education federations must decide how much confidence they need in the assertions made by the Identity Providers [..]

RAF Components

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	

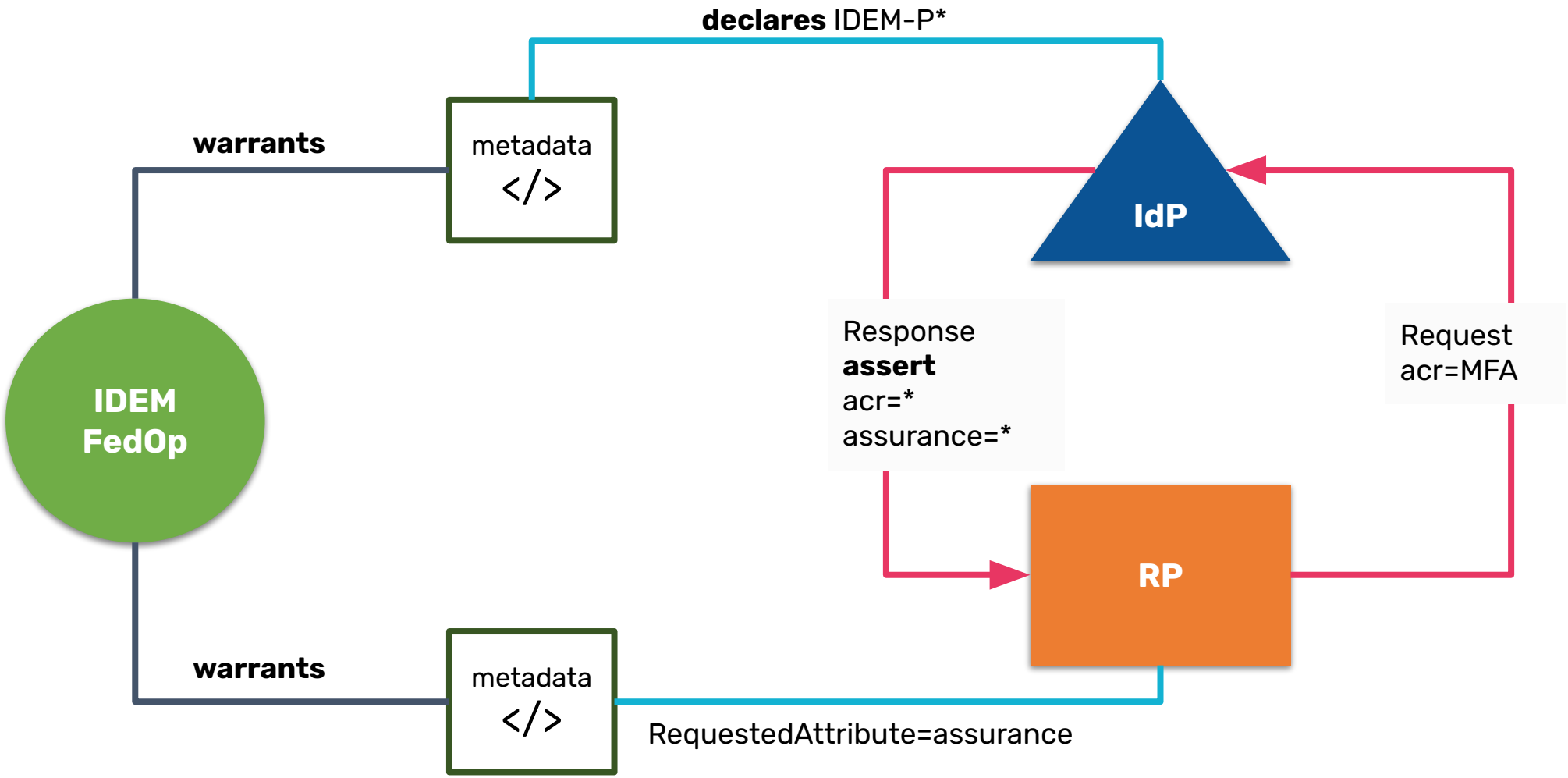
REFEDS MFA Profile

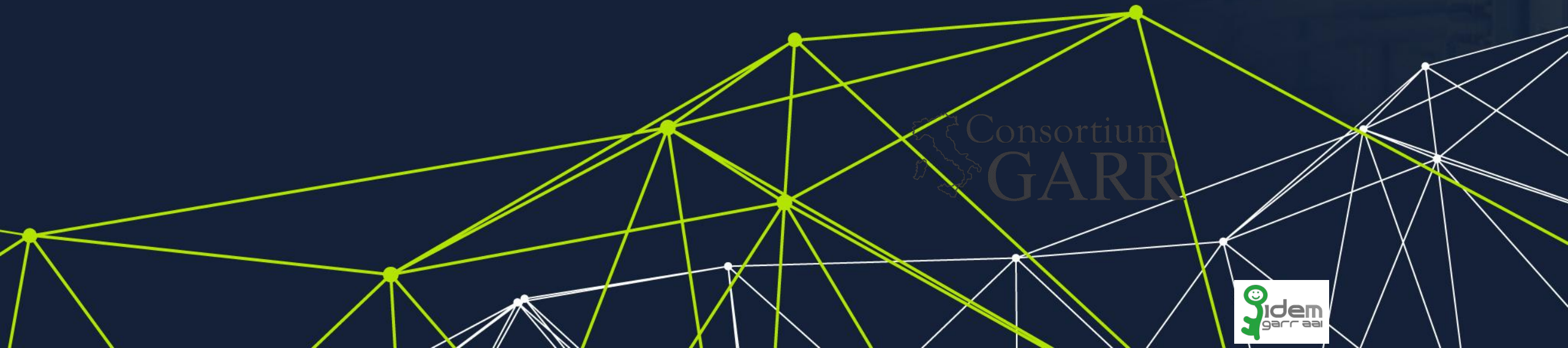
Version History	V1.2 Published 15 November 2023 (current)
Reference pdf	https://zenodo.org/records/10135577
DOI	DOI 10.5281/zenodo.10135577
License	(cc) BY-SA This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Supporting Material	https://wiki.refeds.org/display/PRO/MFA

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 + evidences	Electronic Identity Card or Passport
Attributes quality	-	Affiliation updated within one month	Affiliation updated within one day	Affiliation updated within one day
Authentication	SFA	SFA	MFA	MFA

IDEM Assurance profiles: signal, request, assertion





Thanks!