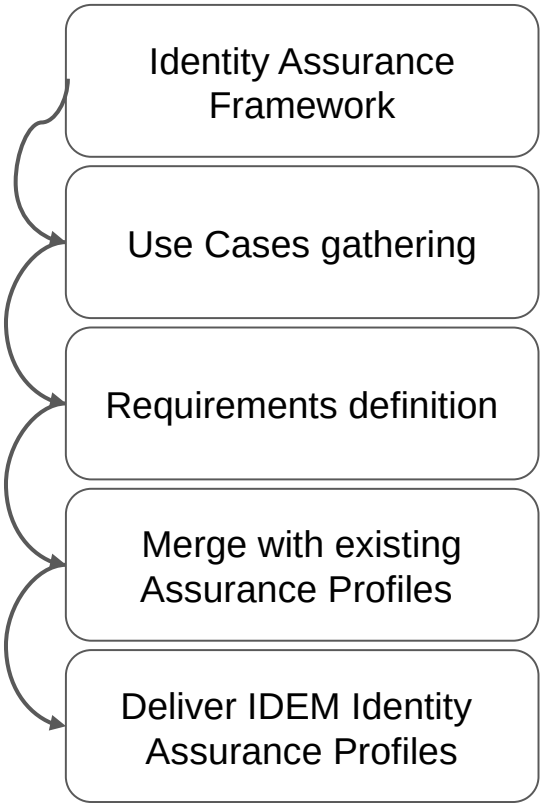
IDEM CTS- Gruppo di lavoro Identity Assurance

Riferimenti

	REFEDS Assurance Framework
	NIST Special Publication 800-63-3
	Kantara Initiative Identity Assurance Framework: Service Assessment Criteria
	ITU-T X.1254 (corrispondente a ISO/IEC 29115:2013)
	SPID
	eIDAS INFN

Gruppo di lavoro Identity Assurance



kantara
REFEDS
NIST
AGID

Accesso a servizi con conseguenze verso terzi minime o trascurabili
Accesso a servizi con potenziali conseguenze verso terzi
Accesso ad infrastrutture dedicate e/o dati riservati
Accesso ad infrastrutture dedicate e/o dati riservati

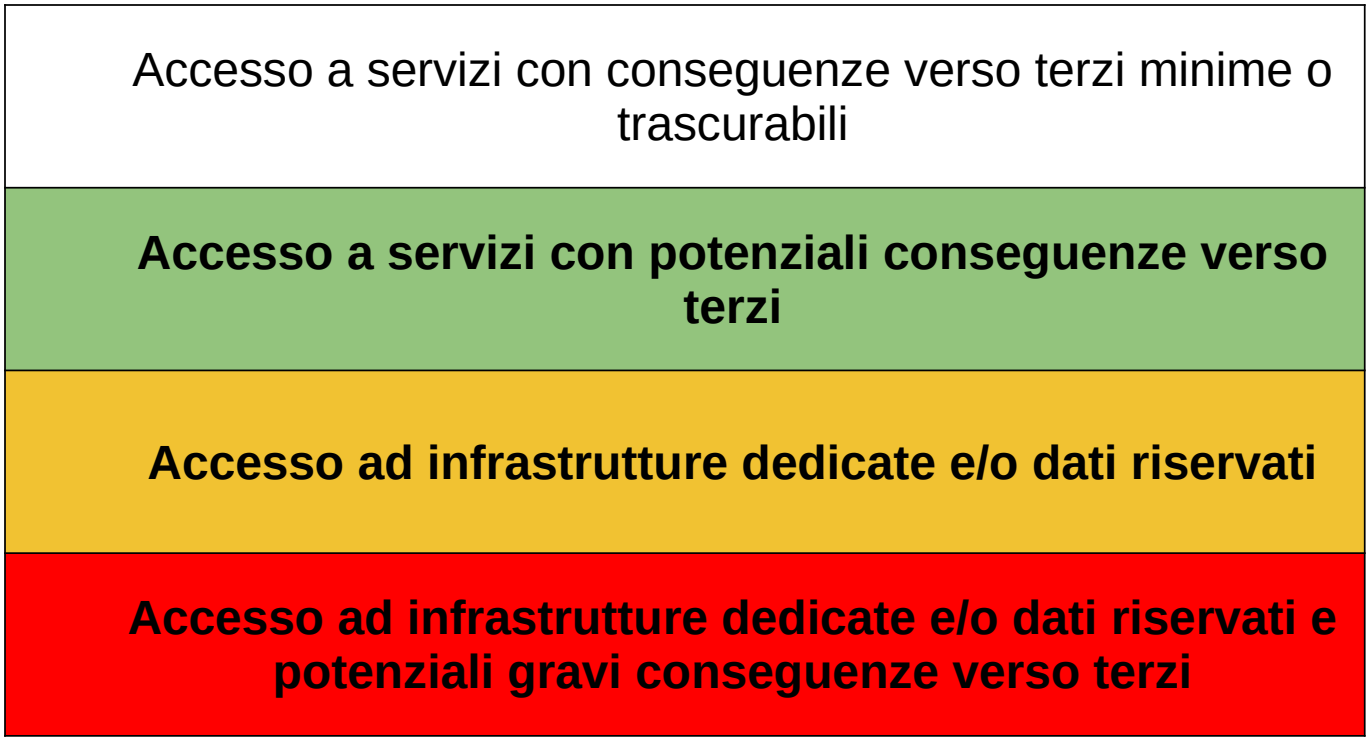
INFN
Istituto Nazionale di Fisica Nucleare

spid
AGID

Scopo

Creare profili di Identity Assurance per ***stabilire il grado di affidabilità delle identità digitali*** *per la rete della ricerca italiana.*

Casi d’uso


Accesso a servizi con conseguenze verso terzi minime o trascurabili
Accesso a servizi con potenziali conseguenze verso terzi
Accesso ad infrastrutture dedicate e/o dati riservati
Accesso ad infrastrutture dedicate e/o dati riservati e potenziali gravi conseguenze verso terzi

Norme di Partecipazione alla Federazione IDEM

impiegare per tutti gli utenti **procedure di accreditamento** ben definite e documentate
accreditare gli utenti previo **riconoscimento**
gestire ogni identità digitale in modo che la persona a cui essa si riferisce sia **identificabile**
impiegare metodi di autenticazione basati su **almeno un fattore** (password, certificato, ecc.)
adottare **misure di sicurezza per la consegna o la creazione del fattore di autenticazione** tali da evitare eventuali furti o compromissioni
fornire agli utenti informazioni relativamente alle loro responsabilità nella custodia e nel mantenimento della sicurezza dei propri account
definire delle **politiche di disabilitazione degli account** e/o delle autorizzazioni ad essi associati e darne comunicazione agli utenti
mantenere sui propri sistemi dei registri d'uso (*log*) che consentano di risalire agli utenti delle **sessioni di autenticazione**

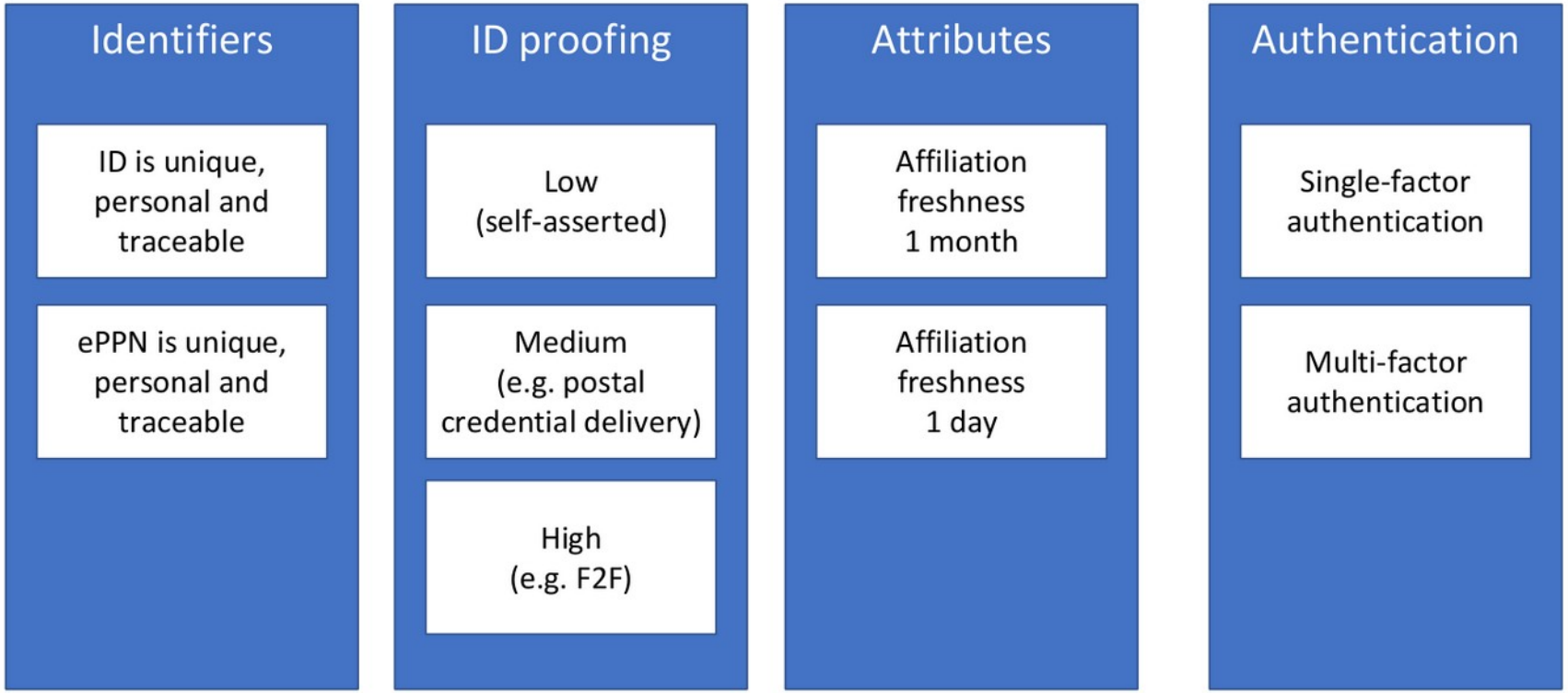
REFEDS Assurance Framework 1.0

- **Multidimensionale**
  - Opposto ai framework monolitici basati su LoA
  - Assurance suddivisa in 3 dimensioni + autenticazione
  - Proposti due assurance profile
- **Semplice**
  - Lo scopo è l'adozione: più complicate sono le specifiche, minore sarà l'adozione
- **Non reinventa la ruota**
  - Specifiche e framework già esistenti: ITU X.1254, eIDAS LoA, NIST SP 800-63-3, Kantara Identity Assurance Framework, IGTF Levels of Authentication Assurance
- **Trasversale**
  - Pensato sia per le federazioni di identità della ricerca e dell'educazione, sia per le comunità della ricerca.

Profili di Assurance IDEM

- Basati sul REFEDS Assurance Framework
- Riferiti alle procedure di accreditamento degli enti GARR
- Almeno 3 livelli (da auto accreditamento a riconoscimento forte)
- Corrispondenza con i livelli SPID ed i principali framework di riferimento

The big picture of assurance



RAF Identity uniqueness

Value	Description
`https://refeds.org/assurance/ID/unique`	- User account belongs to a single natural person - CSP can contact the person to whom the account is issued - The user identifier will not be re-assigned - The user identifier is eduPersonUniqueID, OpenID Connect sub (type: public) or one of the pairwise identifiers recommended by REFEDS

RAF ID Proofing

Value	Description
`https://refeds.org/assurance/IAP/low`	Identity proofing and credential issuance, renewal, and replacement qualify to any of - sections 5.1.2-5.1.2.9 and section 5.1.3 of Kantara assurance level 1 [Kantara SAC] - IGTF level DOGWOOD [IGTF] - IGTF level ASPEN [IGTF]
`https://refeds.org/assurance/IAP/medium`	Identity proofing and credential issuance, renewal, and replacement qualify to any of - sections 5.2.2-5.2.2.9, section 5.2.2.12 and section 5.2.3 of Kantara assurance level 2 [Kantara SAC] - IGTF level BIRCH [IGTF] - IGTF level CEDAR [IGTF] - section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level low [eIDAS LoA]
`https://refeds.org/assurance/IAP/high`	Identity proofing and credential issuance, renewal, and replacement qualifies to any of - section 5.3.2-5.3.2.9, section 5.3.2.12 and 5.3.3 of Kantara assurance level 3 [Kantara SAC] - section 2.1.2, section 2.2.2 and section 2.2.4 of eIDAS assurance level substantial [eIDAS LoA]

RAF Attribute quality and freshness

Value	Description
`https://refeds.org/assurance/ATP/ePA-1m`	eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within 30 days time
`https://refeds.org/assurance/ATP/ePA-1d`	eduPersonAffiliation, and eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within one days time