WORKSHOP GARR 2023

NET MAKERS

Profili di garanzia delle identità digitali della Federazione IDEM

Arianna Arona - UNIMI

Davide Vaghetti - GARR

Agenda

- Identity Assurance Frameworks
- Profili di garanzia IDEM
- Autenticazione
- Procedure di accreditamento e casi d’uso
- Segnalazione, richiesta, asserzione
- Ambito, Conformità e Verifica

Solo Identity Assurance?

Assurance component	Descriptions	Activities

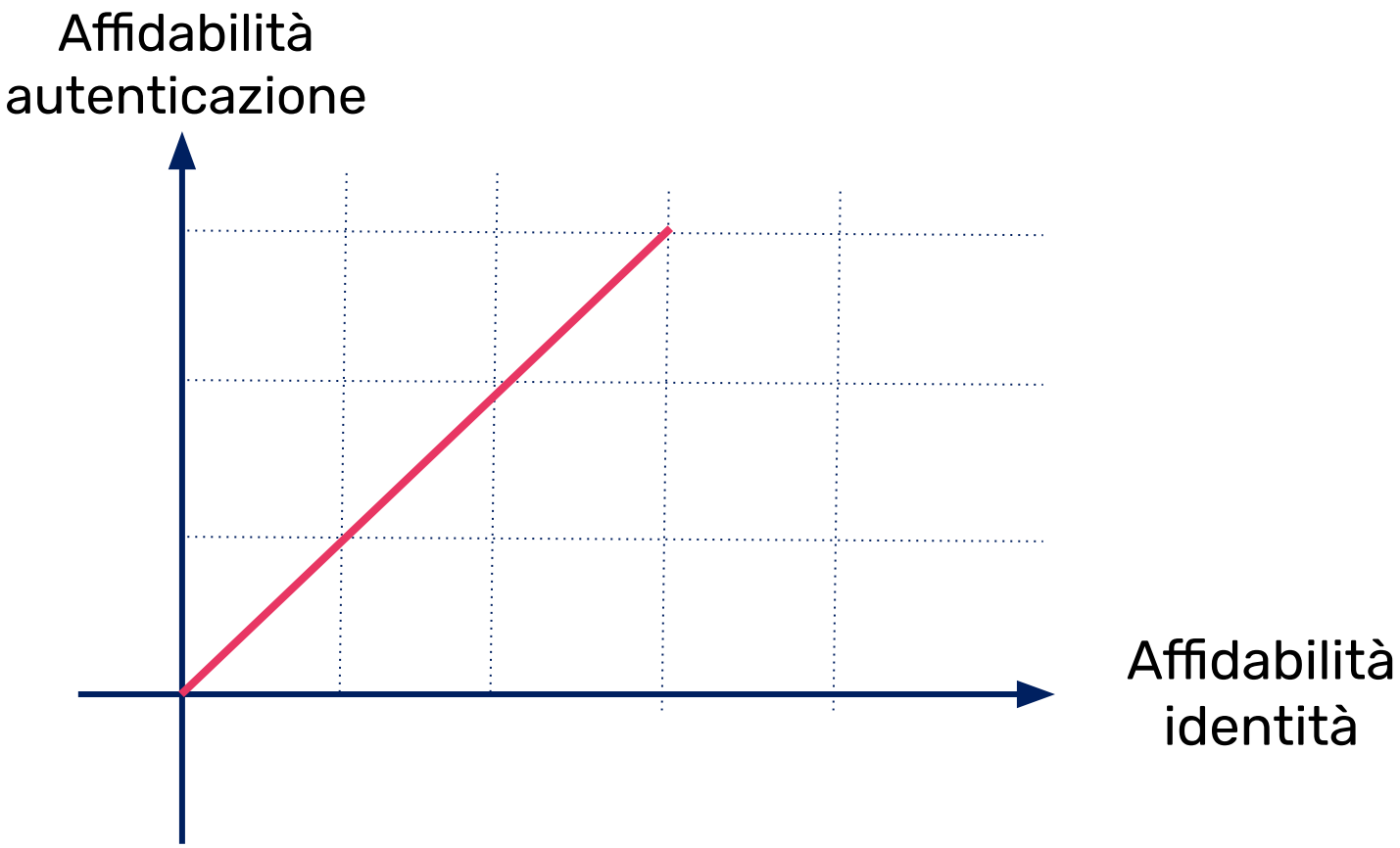
IA *Identity assurance*	Robustness of the identity proofing process and the binding between the authenticator and the identity-proofed individual.	• Identity proofing
		  • Resolution
		  • Validation
		  • Verification
		• Enrollment
		• Binding

AA *Authentication assurance*	Confidence that a given claimant is the same as the previously authenticated subscriber.	• Authentication
		• Credential management
		  • Credential issuance
		  • Credential suspension, revocation, and/or destruction
		  • Credential renewal and/or replacement

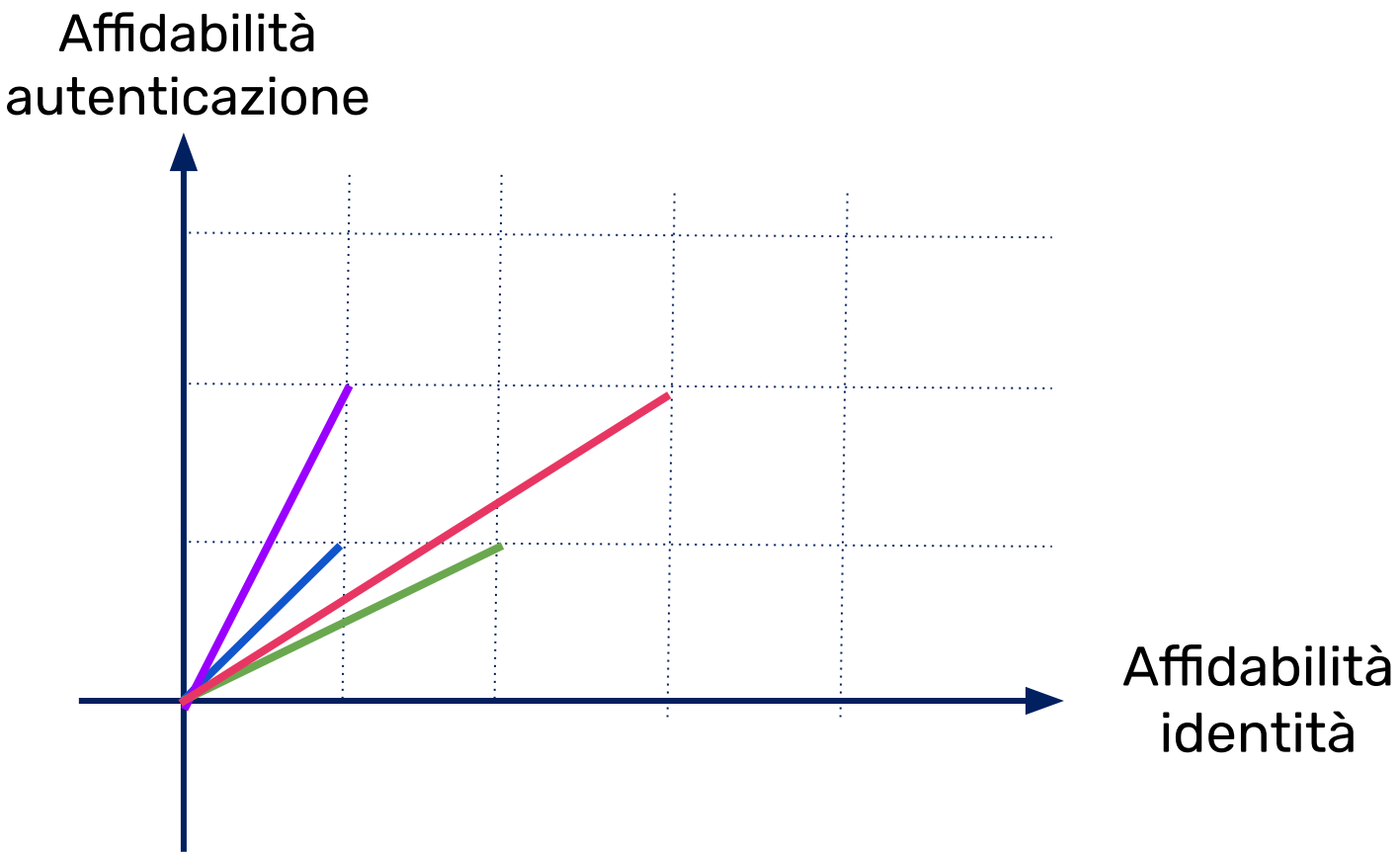
FA *Federation Assurance*	Combines aspects of the federation model, assertion protection strength, and assertion presentation	• Key management • Runtime decisions • Attribute management

Fonte: Recommendation ITU-T X.1254 (09/20) - Entity authentication assurance framework

Identity Assurance



Identity Assurance



REFEDS Assurance Framework
Casi d'uso

LIFE SCIENCE RI

- Risorse ELIXIR
- Risorse BBMRI

neic PUHURI

- LUMI
- FENIX

NIH National Institutes of Health
Turning Discovery Into Health

- Grant Programs
- Datasets
- Research collaborations

Identity Assurance Framework

REFEDS

REFEDS Assurance Framework 1.0

ITU

ITU-T X.1254 (ISO/IEC 29115:2019)

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

Special Publication 800-63-3

European Commission

REGOLAMENTO DI ESECUZIONE (UE) 2015/1502 DELLA COMMISSIONE

spid

CARTA DI IDENTITÀ ELETTRONICA

kantara INITIATIVE

Kantara Initiative Identity Assurance Framework: Service Assessment Criteria

Profili di garanzia IDEM

1. Accesso ai servizi REFEDS Assurance Framework
2. Rispetto norme europee e standard internazionali
3. Diffusione standard di sicurezza e autenticazione a più fattori (MFA)

Requisiti: Identificatori

- Identificatori di protocollo (SAML 2.0/OIDC 1.0)
- Persona fisica
- Contattabile
- No riassegnazione

Verifica dell’identità e gestione delle credenziali

- Registrazione e accreditamento
- Controllo e verifica dell’identità
- Emissione, consegna e attivazione
- Sospensione, revoca e riattivazione
- Rinnovo e sostituzione

Qualità degli attributi

- Affiliazione: student, staff, member
- Aggiornamento entro 1 mese
- Aggiornamento entro 1 giorno

Autenticazione a singolo fattore

Tipo di autenticazione	Specifiche base	Lunghezza minima
Segreto memorizzato	>= 52 caratteri	12 caratteri
	>= 72 caratteri	8 caratteri
OTP (segreti generati e usati una sola volta)	10-51 caratteri	6 caratteri
	>= 52 caratteri	4 caratteri
Segreto ad uso singolo	10-51 caratteri	10 caratteri
	>= 52 caratteri	6 caratteri
Chiavi crittografiche	RSA	2048 bit
	ECDSA	256 bit

Autenticazione a più fattori

- Combinazione più fattori o dispositivi multifattore
- Fattori di tipo diverso
- Fattori indipendenti
- **Eccezione**, attivazione ulteriore fattore:
  - misure ulteriori, ad es. processo supervisionato
  - **sempre** notifica utente

Procedure di accreditamento

- Studenti
  - verifica documento in sede di tolc (se in sede)
  - caricamento documento in fase di immatricolazione
  - nessuna ulteriore verifica diretta
- Personale TAB
  - nuovi assunti: https://portale.inpa.gov.it/ spid
  - mobilità, assunti prima di settembre: autoregistrazione + esibizione documento alla presa di servizio
- Personale docente
  - esibizione documento in fase di colloquio
  - eventuale firma digitale del contratto

Strategie di assegnazione dell'assurance

- Statica (se popolazione utente uniforme)
  - assegno a tutti gli utenti gli stessi valori

- Mapping sul ruolo in presenza di procedure di accreditamento differenziate
  - studenti/dipendenti
  - guest

- Condizionale, basata su più fattori
  - se dipendente e identificazione via SPID
  - gli altri dipendenti

Aumento dell'affidabilità delle identità

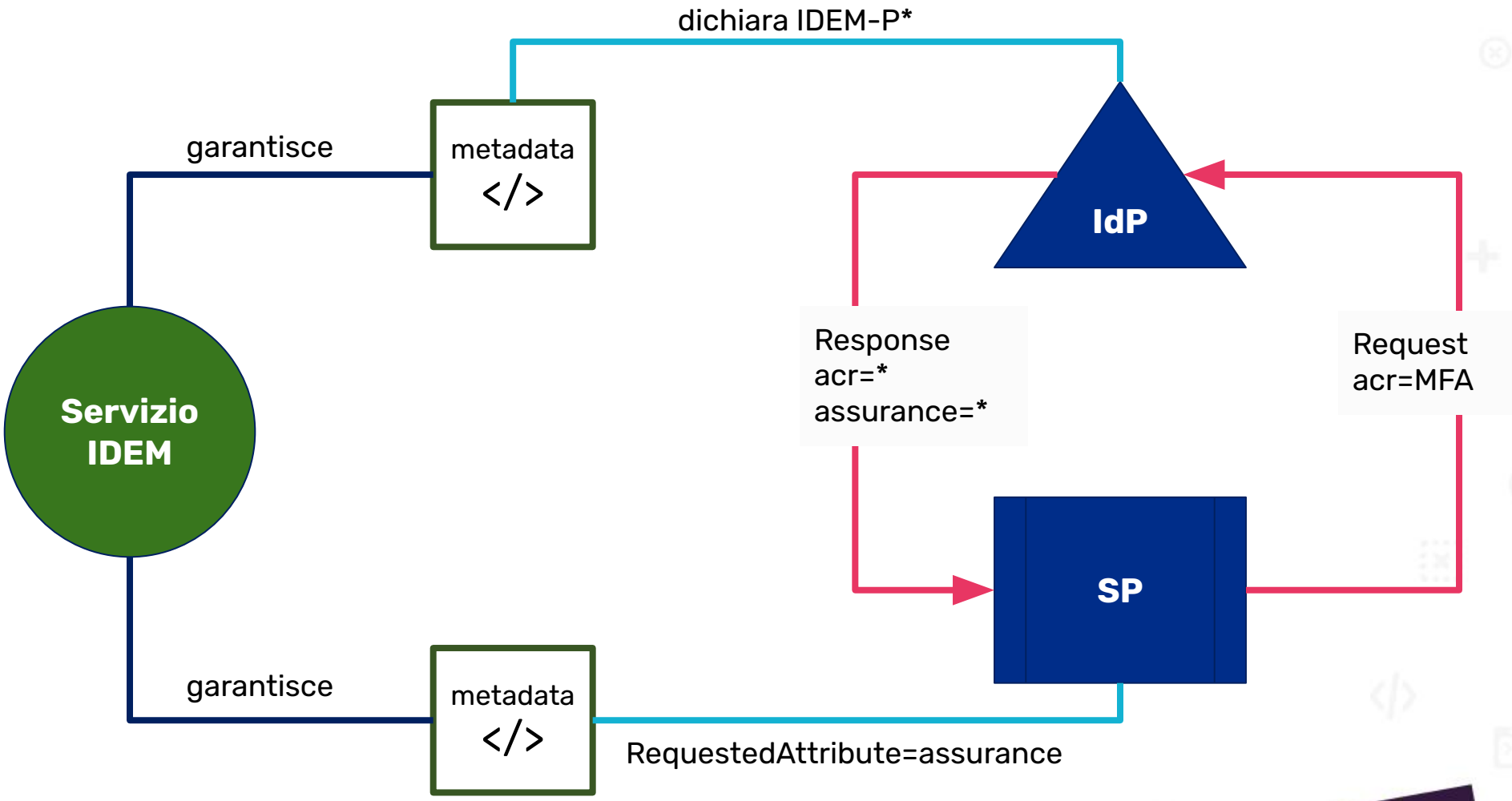
- Adozione di ulteriori procedure di riconoscimento interno
  - Registration Authority per il rilascio dei certificati
  - Possibilità di attuare il processo tramite SPID o CIE

- Verifica di ulteriori mezzi di autenticazione o identificazione
  - firma digitale, per cui siano state **già attuate** procedure di accreditamento con affidabilità superiore

Profili di garanzia IDEM e casi d'uso

	IDEM-P0	IDEM-P1	IDEM-P2	IDEM-P3
Identificatori	Persona fisica, identificatori univoci	Persona fisica, identificatori univoci	Persona fisica, identificatori univoci	Persona fisica, identificatori univoci
Verifica dell'identità	verifica del contatto	verifica del documento d'identità	verifica del documento d'identità e altre fonti	verifica con CIE o simili/superiori
Qualità degli attributi	-	affiliazione aggiornata entro un mese	affiliazione aggiornata entro un giorno	affiliazione aggiornata entro un giorno
Autenticazione	Singolo fattore	Singolo fattore	Più fattori	Più fattori

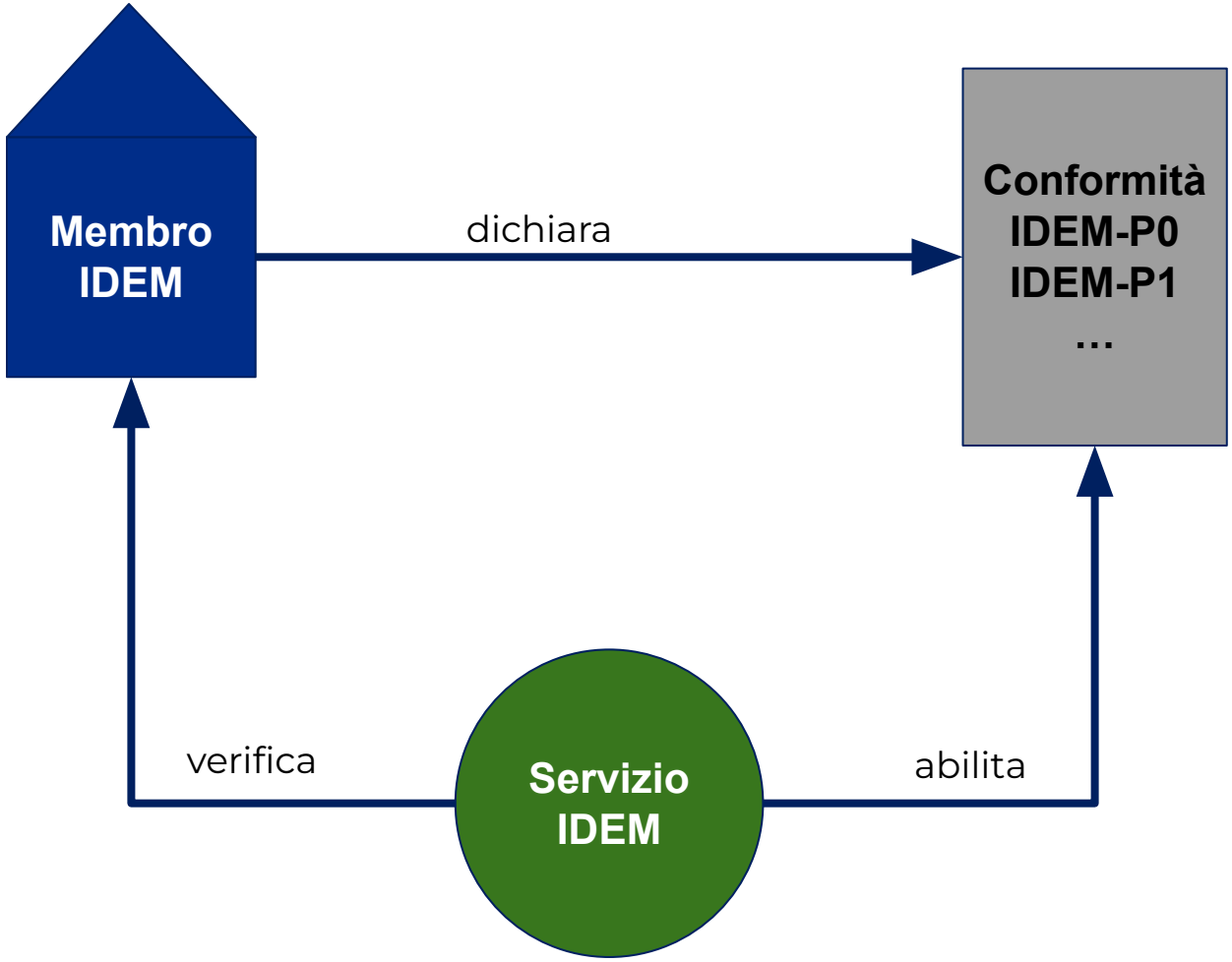
Segnalazione, richiesta, asserzione



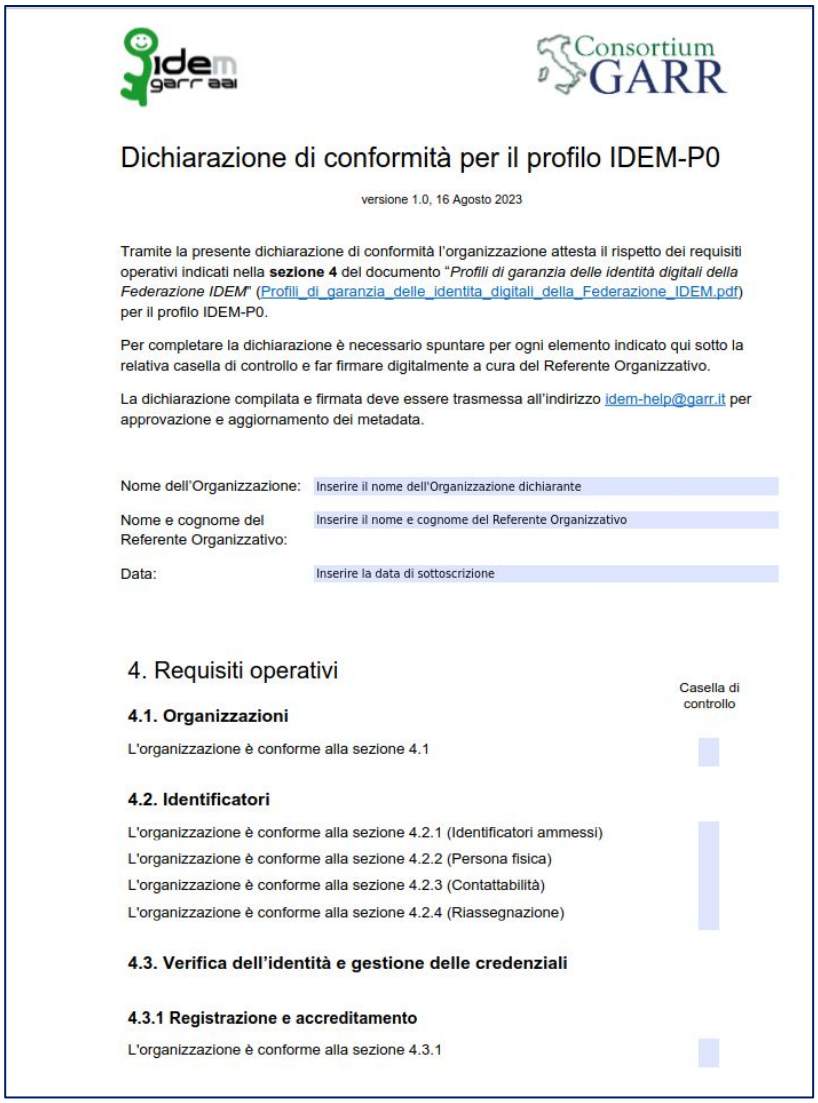
Segnalazione, richiesta, asserzione

	Identity Provider	Service Provider	Servizio IDEM
metadata	Profili supportati: IDEM-P0 IDEM-P1 …	RequestedAttribute *assurance*	Verifica requisiti
flusso attributi	Trasmette sempre le informazioni di *assurance*	Verifica *assurance*	Verifica rispetto specifiche
autenticazione	Supporta e implementa SFA e MFA	Richiede SFA o MFA Verifica ACR	Vigila sul rispetto delle specifiche per SFA e MFA

Ambito, Conformità e Verifica



Autodichiarazione di conformità



Dichiarazione di conformità per il profilo IDEM-P0

versione 1.0, 16 Agosto 2023

Tramite la presente dichiarazione di conformità l'organizzazione attesta il rispetto dei requisiti operativi indicati nella **sezione 4** del documento "*Profili di garanzia delle identità digitali della Federazione IDEM*" (Profili_di_garanzia_delle_identita_digitali_della_Federazione_IDEM.pdf) per il profilo IDEM-P0.

Per completare la dichiarazione è necessario spuntare per ogni elemento indicato qui sotto la relativa casella di controllo e far firmare digitalmente a cura del Referente Organizzativo.

La dichiarazione compilata e firmata deve essere trasmessa all'indirizzo idem-help@garr.it per approvazione e aggiornamento dei metadata.

Nome dell'Organizzazione:	Inserire il nome dell'Organizzazione dichiarante
Nome e cognome del Referente Organizzativo:	Inserire il nome e cognome del Referente Organizzativo
Data:	Inserire la data di sottoscrizione

4. Requisiti operativi

	Casella di controllo
4.1. Organizzazioni	
L'organizzazione è conforme alla sezione 4.1	
4.2. Identificatori	
L'organizzazione è conforme alla sezione 4.2.1 (Identificatori ammessi)	
L'organizzazione è conforme alla sezione 4.2.2 (Persona fisica)	
L'organizzazione è conforme alla sezione 4.2.3 (Contattabilità)	
L'organizzazione è conforme alla sezione 4.2.4 (Riassegnazione)	
4.3. Verifica dell'identità e gestione delle credenziali	
4.3.1 Registrazione e accreditamento	
L'organizzazione è conforme alla sezione 4.3.1	

1. **[Membri IDEM]** dichiarazione di conformità
2. **[Servizio IDEM]** verifica correttezza formale e tecnica
3. **[CTS IDEM]** Può richiedere ulteriori controlli
4. **[Servizio IDEM]** Pubblica il supporto del profilo nei metadata dell'IdP
5. **[Membro IDEM]** Ogni anno rinnova la dichiarazione di conformità

Grazie al gruppo di lavoro Identity Assurance!

Arianna Arona (UNIMI), Francesco Zanolin (INGV), Stefano Colagreco (CNR), Simone Lanzarini (CINECA), Silvio Scipioni (CNR), Andrea Ranaldi (ISPRA), Enrico Maria Vincenzo Fasanelli (INFN), Antonella Monducci (INFN), Loredana Martuscello (CNR), Davide Vaghetti (GARR)

Grazie per l'attenzione

https://u.garr.it/idemassurance