Profili di garanzia delle identità digitali della Federazione IDEM

Revisioni

Versione	Data	Descrizione	Autori
1.0	16/05/2023	Prima versione	GARR, CTS IDEM

Indice

1. Introduzione

Questo documento definisce un sistema di regole per la verifica e l'asserzione della qualità delle identità digitali all'interno della Federazione IDEM sulla base delle quali sono costruiti dei profili di garanzia.

I profili di garanzia dell'identità digitale, qui definiti per la Federazione IDEM ed i suoi partecipanti, rispondono alle esigenze dei fornitori di servizi (Service Provider), che devono essere in grado di valutare il grado di affidabilità delle identità ricevute, e dei gestori di sistemi di autenticazione (Identity Provider), che devono poter fare riferimento a regole chiare e condivise per implementare i processi ed i metodi di gestione delle identità a seconda del grado di affidabilità richiesto o atteso.

Le regole di verifica e asserzione della qualità delle identità digitali si basano su componenti di affidabilità indipendenti, poi ricomposte per specificare profili di garanzia con requisiti crescenti: IDEM-P0, IDEM-P1, IDEM-P2, IDEM-P3.

Le componenti che definiscono la garanzia delle identità digitali in termini di processi di accreditamento, verifica dell'identità, gestione delle credenziali e qualità degli attributi sono basate sul REFEDS Assurance Framework [RAF], sui livelli di garanzia definiti dal REGOLAMENTO DI ESECUZIONE (UE) 2015/1502 [eIDAS-LoA] e dall'Entity authentication assurance framework dell'ITU-T [ITU-T X.1254 09/2020]. Le componenti sono così suddivise:

- **Identificatori**: esprime la modalità ed i requisiti con cui un'organizzazione fornisce un identificatore unico e stabile che rappresenti una persona fisica.
- **Verifica dell'identità e gestione delle credenziali**: esprime la modalità ed i requisiti con cui un'organizzazione esegue le procedure di identificazione e accreditamento degli utenti, l'erogazione delle credenziali, il loro rinnovo e la loro sostituzione.
- **Qualità degli attributi**: esprime la modalità ed i requisiti tramite i quali un'organizzazione è in grado di assegnare determinati livelli di qualità ed aggiornamento degli attributi trasmessi.

Le componenti che definiscono la robustezza del processo di autenticazione sono basate sul REFEDS Single Factor Authentication Profile [REFEDS-SFA], sul REFEDS Multi-Factor Authentication Profile [REFEDS-MFA] e sul documento Digital Identity Guidelines: Authentication and Lifecycle Management del NIST [NIST 800-63B].

2. Termini e definizioni

Le parole chiave utilizzate in questo documento, sempre scritte in maiuscolo ed indicate nell'elenco che segue con a fianco la loro versione originale in lingua inglese, devono essere interpretate secondo quanto indicato nella [RFC 2119]:

DEVE/OBBLIGATORIO: MUST/SHALL/REQUIRED
NON DEVE: MUST NOT/SHALL NOT
DOVREBBE/RACCOMANDATO: SHOULD

NON DOVREBBE: SHOULD NOT
PUÒ/FACOLTATIVO: MAY/OPTIONAL

2.1. Definizioni

Fattore di autenticazione: Un mezzo utilizzato per eseguire l'autenticazione digitale. Una persona si autentica in un sistema dimostrando il possesso e il controllo di un fattore di autenticazione.
Interessato o Utente: Una persona fisica affiliata ad un Membro della Federazione IDEM.
Credenziali: Un insieme di dati presentato come prova dell'identità e/o dei titoli dichiarati, ad esempio la combinazione di un nome utente ed una password.
Federazione di identità: Insieme di organizzazioni che decidono di scambiarsi informazioni di identità per l'accesso fidato ai servizi utilizzando regole e specifiche tecniche condivise. Le federazioni di identità agiscono da terza parte fidata tra i servizi di autenticazione, o Identity Provider, ed i servizi di accesso, o Service Provider.
Operatore di federazione: Gestore tecnico di una federazione di identità.
Partecipante (Federazione IDEM): Un Membro od un Partner della Federazione IDEM.
Membro o Organizzazione (della Federazione IDEM): Partecipante alla Federazione IDEM collegato alla rete GARR e che gestisce un Identity Provider.
Partner (della Federazione IDEM): Partecipante alla Federazione IDEM che gestisce un Service Provider.
Identity Provider: Un attore fidato che rilascia e/o gestisce le credenziali. Nell'ambito di questo documento, con Identity Provider ci si riferisce anche al sistema di Identity Management associato che gestisce le identità e gli attributi degli utenti.
Service Provider o Relying Party: Entità che fornisce accesso a risorse o servizi basandosi su un'asserzione o un'affermazione di identità.

3. Ambito, Conformità e Verifica

3.1. Ambito

1. Questo documento definisce i profili di garanzia dell'identità definiti e riconosciuti dalla Federazione IDEM GARR AAI e da tutte le organizzazioni che vi partecipano.
2. Le organizzazioni della Federazione IDEM che dichiarano di essere conformi ad uno o più profili di queste specifiche DEVONO rispettarle per la parte della propria popolazione utente a cui sono riferite.
3. I valori di garanzia trasmessi dall'Identity Provider si riferiscono esclusivamente alle singole identità per cui sono espressi.
4. L'organizzazione aderente DEVE essere in grado di esprimere i profili di garanzia dichiarati per i servizi che ne manifestino la necessità.

3.2. Conformità

1. L'organizzazione che si intende avvalere di uno dei profili di garanzia qui definiti, DEVE presentare una dichiarazione di conformità secondo le modalità indicate dall'operatore di federazione per il profilo desiderato.
2. Tramite la dichiarazione di conformità l'organizzazione attesta il rispetto dei requisiti

operativi indicati nella sezione 4 del presente documento per il profilo di garanzia indicato.
3. I profili per i quali è possibile sottomettere la dichiarazione di conformità sono tutti quelli definiti dal presente documento. I profili con requisiti più elevati includono i profili con requisiti minori, ad esempio la dichiarazione di conformità per il profilo IDEM-P2 include automaticamente i profili IDEM-P1 e IDEM-P0.
4. La dichiarazione di conformità DEVE essere rinnovata annualmente secondo le modalità indicate dall'operatore di federazione.

3.3. Procedure di verifica

1. L'operatore di federazione, in collaborazione con il Comitato Tecnico Scientifico della Federazione, fornisce una lista di controlli per permettere alle organizzazioni di autovalutare il proprio grado di conformità rispetto ai requisiti dei profili di garanzia.
2. L'operatore di federazione esegue controlli periodici volti a verificare il rispetto dei requisiti dei profili di garanzia indicati dall'organizzazione nella dichiarazione di conformità.
3. Le organizzazioni che hanno sottoscritto la dichiarazione di conformità per uno o più profili DEVONO collaborare con l'operatore di federazione per l'attuazione dei controlli periodici sul rispetto dei requisiti.
4. Il Comitato Tecnico Scientifico della Federazione IDEM PUÒ richiedere all'operatore di federazione di eseguire ulteriori verifiche.

4. Requisiti operativi

4.1. Organizzazioni

Tutte le organizzazioni che fanno parte della Federazione IDEM e che assegnano e gestiscono credenziali, rispettano i seguenti requisiti validi per i profili IDEM-P0, IDEM-P1, IDEM-P2 e IDEM-P3. Nello specifico DEVONO:

1. Registrare tutte le informazioni pertinenti al processo di erogazione, gestione delle credenziali e dei fattori di autenticazione, conservarle nella misura consentita dalla legislazione nazionale e renderle disponibili in caso di indagini e verifiche sulla sicurezza delle credenziali e dei dati degli interessati.
2. Attuare controlli tecnici commisurati al rischio per la sicurezza delle credenziali al fine di garantirne la riservatezza, l'integrità e la disponibilità.
3. Consentire l'accesso ai sistemi di gestione delle credenziali e del materiale crittografico ad esse associato solo al personale esplicitamente autorizzato ed adeguatamente formato.
4. Garantire che nessun tipo di segreto (memorizzato o generato) sia conservato in chiaro sui propri sistemi.

4.2. Identificatori

Ad ogni identità digitale è assegnato un identificatore che DEVE rispettare i requisiti qui definiti e validi per i profili IDEM-P0, IDEM-P1, IDEM-P2, IDEM-P3.

4.2.1. Identificatori ammessi

L’identificatore trasmesso dall’Identity Provider DEVE essere almeno uno dei seguenti:

- SAML 2.0 persistent name identifier [OASIS SAML].
- SAML 2.0 subject-id or pairwise-id [OASIS SIA].
- OIDC sub con type public o pairwise [OpenID.Core].
- eduPersonUniqueId [eduPerson].
- eduPersonPrincipalName [eduPerson].

4.2.2. Persona fisica

L’identificatore DEVE essere assegnato ad una singola persona fisica.

4.2.3. Contattabilità

L’organizzazione a cui è associato l’Identity Provider DEVE essere in grado di contattare la persona a cui è assegnato l’identificatore.

4.2.4. Riassegnazione

Gli identificatori assegnati agli utenti NON DEVONO essere mai riassegnati.

4.3. Verifica dell’identità e gestione delle credenziali

In questa sezione sono definiti i requisiti relativi alle procedure di registrazione degli utenti e di gestione dell’identità digitale che le organizzazioni devono rispettare.

4.3.1. Registrazione e accreditamento

I requisiti che seguono sono validi per tutti i profili (IDEM-P0, IDEM-P1, IDEM-P2, IDEM-P3):

1. L’organizzazione DEVE rendere pubbliche e conoscibili agli interessati le proprie procedure di registrazione e accreditamento per l’erogazione dell’identità elettronica.
2. L’organizzazione DEVE accertarsi che l’interessato conosca i termini e le condizioni d’uso dell’identità elettronica fornita.

4.3.2. Controllo e verifica dell’identità

4.3.2.1. Profilo IDEM-P0

L’organizzazione DEVE implementare almeno uno dei seguenti sistemi di verifica dell’identità:

1. Verifica di persona: l’organizzazione DEVE richiedere almeno una auto-asserzione dell’identità e PUÒ decidere di richiedere anche una auto-certificazione a supporto.
2. Verifica remota: l’interessato DEVE fornire un contatto nella propria disponibilità come un numero di telefono o un indirizzo email, che DEVE essere verificato dall’organizzazione.
3. Verifica basata su altre credenziali: l’organizzazione PUÒ decidere di accettare credenziali di altri servizi per la verifica dell’identità. In tal caso, le credenziali DEVONO essere state erogate con regole compatibili o superiori a quelle del livello IDEM-P0 e l’interessato DEVE dar prova di avere il controllo delle credenziali

utilizzate.

4.3.2.2. Profilo IDEM-P1

L'organizzazione DEVE implementare uno dei seguenti sistemi di verifica dell'identità:

1. Verifica di persona: l'organizzazione DEVE verificare l'identità della persona tramite un documento di identità riconosciuto dallo Stato italiano e **apparentemente autentico**.
2. Verifica remota: l'organizzazione DEVE verificare l'identità della persona **in remoto** tramite l'esibizione o l'invio di una copia di un documento di identità riconosciuto dallo Stato italiano e **apparentemente autentico**.
3. Verifica basata su altre credenziali: l'organizzazione PUÒ accettare credenziali di altri servizi per la verifica dell'identità. In tal caso, le credenziali DEVONO essere state erogate con regole compatibili o superiori a quelle del profilo IDEM-P1 e l'interessato DEVE provare di avere il controllo delle credenziali presentate.

4.3.2.3. Profilo IDEM-P2

L'organizzazione DEVE implementare uno dei seguenti sistemi di verifica dell'identità:

1. Verifica di persona: l'organizzazione DEVE verificare l'identità della persona tramite un documento di identità riconosciuto dallo Stato italiano **e che sia stato verificato per stabilirne l'autenticità oppure, secondo una fonte autorevole, esiste ed è collegato a una persona reale**.
2. Verifica remota: l'organizzazione DEVE verificare l'identità della persona **in remoto** tramite l'esibizione o l'invio di una copia di un documento di identità riconosciuto dallo Stato italiano **e che sia stato verificato per stabilirne l'autenticità oppure, secondo una fonte autorevole, esiste ed è collegato a una persona reale**.
3. Verifica basata su altre credenziali: l'organizzazione PUÒ accettare credenziali di altri servizi per la verifica dell'identità. In tal caso, le credenziali DEVONO essere state erogate con regole compatibili o superiori a quelle del profilo IDEM-P2 e l'interessato DEVE provare di avere il controllo delle credenziali presentate.

4.3.2.4. Profilo IDEM-P3

L'organizzazione DEVE implementare un sistema di verifica dell'identità secondo quanto indicato dal Regolamento eIDAS [eIDAS] per il livello di garanzia Elevato.

4.3.3. Emissione, consegna e attivazione

4.3.3.1 Profili IDEM-P0 e IDEM-P1

1. Una volta emesse, le credenziali DEVONO essere consegnate tramite un meccanismo che consenta di presumere che siano ricevute unicamente dall'assegnatario previsto.
2. Le credenziali POSSONO essere consegnate tramite posta tradizionale, così come tramite l'invio di collegamenti per scaricarle (o impostarle) via posta elettronica o SMS, in tal caso DEVONO rispettare i requisiti indicati più avanti nella sezione 4.5.1 *Autenticazione a singolo fattore* punto 2.

4.3.3.2 Profili IDEM-P2 e IDEM-P3

1. Una volta emesse (o rilasciate), le credenziali DEVONO essere consegnate tramite un meccanismo che consenta di assicurare che siano ricevute unicamente dall'assegnatario a cui appartengono.
2. Le credenziali POSSONO essere attivate tramite l'invio di collegamenti via posta elettronica o SMS, in tal caso DEVONO rispettare i requisiti indicati più avanti nella sezione 4.5.1 *Autenticazione a singolo fattore* punto 2.

4.3.4. Sospensione, revoca e riattivazione

I seguenti requisiti sono validi per tutti i profili IDEM-P0, IDEM-P1, IDEM-P2, IDEM-P3.

1. L'organizzazione DEVE essere in grado di sospendere o revocare delle credenziali in modo tempestivo ed efficace.
2. La riattivazione è eseguita solo se sono ripristinati i requisiti di garanzia stabiliti prima della sospensione o della revoca.

4.3.5. Rinnovo e sostituzione

4.3.5.1 Profili IDEM-P0, IDEM-P1 e IDEM-P2

Il processo di rinnovo o sostituzione DEVE soddisfare gli stessi requisiti di verifica dell'identità utilizzati per l'emissione delle credenziali, oppure si DEVE basare su un mezzo di identificazione elettronica valido con livelli di garanzia equivalenti o superiori a quelli dell'identità in questione.

4.3.5.2 Profilo IDEM-P3

Come per i profili IDEM-P0, IDEM-P1 e IDEM-P2 più verifica presso una fonte autorevole del mezzo di identificazione elettronica eventualmente utilizzato.

4.4. Qualità degli attributi

1. I requisiti qui indicati determinano la qualità dell'attributo di affiliazione che PUÒ essere trasmesso insieme all'identità digitale. Questi requisiti sono validi e comuni per i profili IDEM-P0, IDEM-P1, IDEM-P2, IDEM-P3.
2. Gli attributi di affiliazione oggetto di queste specifiche sono esclusivamente eduPersonAffiliation, eduPersonPrimaryAffiliation ed eduPersonScopedAffiliation ed unicamente in relazione alle affiliazioni student, faculty, member.
3. Gli Identity Provider che trasmettono il valore di affiliazione delle identità digitali tramite uno o più degli attributi sopra menzionati DEVONO anche indicarne la qualità intesa come frequenza di aggiornamento.
4. Il valore di affiliazione DEVE essere aggiornato in seguito alla modifica del ruolo o al termine del rapporto con l'organizzazione.
5. Le organizzazioni DEVONO indicare se sono in grado di garantire un tempo di aggiornamento del valore di affiliazione entro 1 mese o un 1 giorno dall'evento che ha determinato la modifica.

4.5. Autenticazione

4.5.1. Ambito di applicazione

1. Tutti i profili di garanzia della Federazione IDEM DEVONO implementare l'autenticazione a singolo fattore.
2. I profili di garanzia IDEM-P2 e IDEM-P3 DEVONO implementare l'autenticazione a singolo fattore e l'autenticazione a più fattori.
3. Quando sono richiesti o impiegati i profili di garanzia IDEM-P0 e IDEM-P1, gli utenti DEVONO autenticarsi con autenticazione a singolo fattore e POSSONO anche avvalersi dell'autenticazione a più fattori.
4. Quando sono richiesti o impiegati i profili di garanzia IDEM-P2 e IDEM-P3, gli utenti DEVONO autenticarsi con autenticazione a più fattori.

4.5.2. Autenticazione a singolo fattore

1. L'autenticazione a singolo fattore DEVE essere effettuata con uno dei seguenti mezzi:
    - un segreto memorizzato, come ad esempio una password o un PIN, che DEVE avere una lunghezza minima di 8 caratteri se scelti da una base di almeno 72 caratteri diversi, oppure DEVE avere una lunghezza minima di 12 caratteri se scelti da una base compresa tra 52 e 72 caratteri (in ogni caso la base NON DEVE essere inferiore a 52 caratteri).
    - un segreto generato e utilizzabile una sola volta (OTP, one time password), che DEVE avere una lunghezza minima di 4 caratteri se scelti da una base di almeno 52 caratteri diversi, oppure DEVE avere una lunghezza minima di 6 caratteri se scelti da una base compresa tra 10 e 51 caratteri (come ad esempio un segreto contenente solo cifre).
    - un segreto ad uso singolo (ad esempio Recovery Key, Sequence Based OTP) che DEVE avere una lunghezza minima di 6 caratteri se scelti da una base di almeno 52 caratteri diversi, oppure DEVE avere una lunghezza minima di 10 caratteri se scelti da una base compresa tra 10 e 51 caratteri.
    - una chiave crittografica RSA che DEVE avere una lunghezza minima di 2048 bit.
    - una chiave crittografica ECDSA che DEVE avere una lunghezza minima di 256 bit.
    - una chiave o dispositivo software crittografico a singolo fattore che DEVE essere conforme alle specifiche NIST 800-63B.
2. I segreti trasmessi DEVONO rispettare i seguenti tempi massimi di validità:
    - i segreti generati tramite un dispositivo TOTP DEVONO essere validi per un tempo massimo di 5 minuti.
    - i segreti comunicati tramite telefono o SMS DEVONO essere validi per un tempo massimo di 10 minuti.
    - i segreti comunicati tramite e-mail (ad esempio messaggio con link per il reset del proprio account) DEVONO essere validi per un tempo massimo di 24 ore.
    - i segreti comunicati tramite posta ordinaria DEVONO essere validi per un tempo massimo di 1 mese.
3. Le specifiche di autenticazione del REFEDS SFA Profile [REFEDS-SFA] sono pienamente compatibili con le specifiche qui indicate.

4.5.3. Autenticazione a più fattori

1. L’autenticazione a più fattori DEVE essere effettuata con uno dei seguenti mezzi:
    - una combinazione di due o più fattori che rispondano agli stessi requisiti indicati per l’autenticazione a singolo fattore (vedi 4.5.1).
    - un dispositivo “Multi-Factor” hardware o software così come definito in [NIST 800-63B].
2. I fattori di autenticazione utilizzati per l’autenticazione combinata DEVONO essere di tipo diverso.
3. I fattori di autenticazione utilizzati per l’autenticazione combinata DEVONO essere indipendenti.
4. Un ulteriore fattore di autenticazione PUÒ essere attivato tramite un fattore esistente, in tal caso DEVE essere sempre prevista la notifica dell’attivazione sui canali di contatto dell’utente, inoltre DEVONO essere adottate misure per limitare il rischio di compromissione, quali l’invio di un messaggio di attivazione secondo le specifiche indicate al punto 2 del paragrafo 4.5.1 o tramite un processo supervisionato. In ogni caso, l’ulteriore fattore NON DEVE essere accessibile utilizzando l'esistente e DEVE mantenere l’indipendenza di tutte le altre operazioni di gestione come l’eliminazione, la modifica, il reset.
5. Le specifiche di autenticazione del REFEDS MFA Profile [REFEDS-MFA] sono pienamente compatibili con le specifiche qui indicate.

Riferimenti

[eIDAS-LoA]
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015R1502
[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
[RAF] REFEDS Assurance Framework
https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0
[REFEDS-SFA] REFEDS SFA Profile
https://doi.org/10.5281/zenodo.5113499
[REFEDS-MFA] REFEDS MFA Profile
https://doi.org/10.5281/zenodo.5113296

Allegato A - Rappresentazione dei valori di garanzia dell’identità digitale per la Federazione IDEM

Tutti i profili di garanzia dell’identità digitale per la Federazione IDEM, ed i valori dei componenti di garanzia ad essi associati, sono espressi tramite l’attributo SAML 2.0 eduPersonAssurance o tramite il claim OpenID Connect edu_person_assurance.
Nelle tabelle che seguono sono indicati i valori da assegnare all’attributo per i profili e per i componenti, una breve descrizione ed un esempio di caso d’uso.

Profili

Valori	https://idem.garr.it/af/IDEM-P0
Descrizione e casi d’uso	L’identità digitale rispetta tutti i requisiti per il profilo IDEM-P0, ad esempio un account autoregistrato con conferma via mail e autenticazione ad un fattore.

Valori	https://idem.garr.it/af/IDEM-P0 https://idem.garr.it/af/IDEM-P1
Descrizione e casi d’uso	L’identità digitale rispetta tutti i requisiti per il profilo IDEM-P1, ad esempio un account verificato tramite documento d’identità e autenticazione ad un fattore.

Valori	https://idem.garr.it/af/IDEM-P0 https://idem.garr.it/af/IDEM-P1 https://idem.garr.it/af/IDEM-P2
Descrizione e casi d’uso	L’identità digitale rispetta tutti i requisiti per il profilo IDEM-P2, ad esempio un account verificato tramite documento d’identità confermato e autenticazione a più fattori.

Valori	https://idem.garr.it/af/IDEM-P0 https://idem.garr.it/af/IDEM-P1 https://idem.garr.it/af/IDEM-P2 https://idem.garr.it/af/IDEM-P3
Descrizione e casi d’uso	L’identità digitale rispetta tutti i requisiti per il profilo IDEM-P3, ad esempio un account verificato tramite documento d’identità confermato dall’autorità emittente e autenticazione a più fattori.

Identificatori

Valori	https://refeds.org/assurance/ID/unique
Descrizione e casi d’uso	L’identificatore utente rispetta tutte le proprietà stabilite da [RAF] e non è eduPersonPrincipalName.
Profili	RAF Espresso, RAF Cappuccino, IDEM-P0, IDEM-P1, IDEM-P2, IDEM-P3

Valori	https://refeds.org/assurance/ID/unique https://refeds.org/assurance/ID/eppn-unique-no-reassign
Descrizione e casi d’uso	L’identificatore utente utilizzato è eduPersonPrincipalName e rispetta tutte le proprietà stabilite da [RAF].
Profili	RAF Espresso, RAF Cappuccino, IDEM-P0, IDEM-P1, IDEM-P2, IDEM-P3

Verifica dell’identità e gestione delle credenziali

Valori	https://refeds.org/assurance/IAP/low
Descrizione e casi d’uso	Identità auto-registrata e verificata unicamente tramite la conferma del possesso di un mezzo di contatto (e-mail, numero di telefono, ecc.).
Profili	IDEM-P0

Valori	https://refeds.org/assurance/IAP/low https://refeds.org/assurance/IAP/medium
Descrizione e casi d’uso	Identità verificata tramite un documento apparentemente autentico.
Profili	RAF Cappuccino, IDEM-P0, IDEM-P1

Valori	https://refeds.org/assurance/IAP/low https://refeds.org/assurance/IAP/medium https://refeds.org/assurance/IAP/high
Descrizione e casi d’uso	Identità verificata tramite un documento apparentemente autentico e confermato tramite una fonte autorevole.
Profili	RAF Cappuccino, RAF Espresso, IDEM-P0, IDEM-P1, IDEM-P2

Valori	https://refeds.org/assurance/IAP/low https://refeds.org/assurance/IAP/medium https://refeds.org/assurance/IAP/high
Descrizione	Identità verificata tramite un documento autentico confermato dall’emittente.

Valori	https://refeds.org/assurance/IAP/low https://refeds.org/assurance/IAP/medium https://refeds.org/assurance/IAP/high
e casi d’uso	
Profili	RAF Cappuccino, RAF Espresso, IDEM-P0, IDEM-P1, IDEM-P2, IDEM-P3

Qualità degli attributi

Valori	https://refeds.org/assurance/ATP/ePA-1m
Descrizione e casi d’uso	Il valore di affiliazione viene aggiornato almeno mensilmente. Valore ottimale per tutti servizi federati non critici.
Profili	IDEM-P0, IDEM-P1, IDEM-P2, IDEM-P3, RAF Cappuccino, RAF Espresso

Valori	https://refeds.org/assurance/ATP/ePA-1m https://refeds.org/assurance/ATP/ePA-1d
Descrizione e casi d’uso	Il valore di affiliazione viene aggiornato almeno giornalmente. Valore ottimale per tutti servizi federati critici, ovvero che consentano l’accesso a dati particolari (GDPR) e/o risorse particolarmente pregiate.
Profili	IDEM-P0, IDEM-P1, IDEM-P2, IDEM-P3, RAF Cappuccino, RAF Espresso

Allegato B - Sintesi dei profili di garanzia dell’identità digitale della Federazione IDEM

	Autoregistrazione	Documento apparentemente autentico	Documento apparentemente autentico e confermato	Documento verificato dall'emittente
SFA	IDEM-P0	IDEM-P1	IDEM-P1	IDEM-P1
MFA	IDEM-P0	IDEM-P1	IDEM-P2	IDEM-P3

IDEM-P0

Esempio di caso d’uso:

- Test di ingresso / autovalutazione per l’iscrizione all’università, iscrizione a portali web tramite auto-registrazione.
- Identificazione tramite verifica del contatto (email, numero di telefono).
- Autenticazione a singolo fattore.

Rappresentazione nei metadata

- SAML 2.0: eduPersonAssurance RequestedAttribute

```
<RequestedAttribute FriendlyName="eduPersonAssurance"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired="true"/>
```

Richiesta di Autenticazione (Service Provider)

AuthnContextClassRef (SAML 2.0) o acr (OIDC) DEVE contenere una delle classi seguenti:

- REFEDS SFA: https://refeds.org/profile/sfa
- REFEDS MFA: https://refeds.org/profile/mfa

Risposta (Identity Provider)

- SAML 2.0: AuthnContextClassRef DEVE contenere la classe richiesta https://refeds.org/profile/sfa o https://refeds.org/profile/mfa
- OIDC: acr DEVE contenere la classe richiesta https://refeds.org/profile/sfa o https://refeds.org/profile/mfa

L’attributo eduPersonAssurance (SAML 2.0) o il claim edu_person_assurance (OIDC) (eduPersonAssurance requested attribute) DEVE contenere i seguenti valori:

https://refeds.org/assurance
https://refeds.org/assurance/ID/unique
https://refeds.org/assurance/ID/eppn-unique-no-reassign
https://refeds.org/assurance/IAP/low
https://idem.garr.it/af/IDEM-P0

IDEM-P1

Esempio di caso d’uso:

- Immatricolazione di uno studente.
- Identificazione tramite esibizione di un documento di identità apparentemente autentico o identificazione tramite altre credenziali, ad esempio SPID-L1.
- Affiliazione aggiornata almeno entro un mese e opzionalmente entro un giorno.
- Autenticazione ad un fattore.

Rappresentazione nei metadata

```
<RequestedAttribute FriendlyName="eduPersonAssurance"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired="true"/>
```

Richiesta di Autenticazione (Service Provider)

AuthnContextClassRef (SAML 2.0) o acr (OIDC) DEVE contenere una delle classi seguenti:

- REFEDS SFA: https://refeds.org/profile/sfa
- REFEDS MFA: https://refeds.org/profile/mfa

Risposta (Identity Provider)

- SAML 2.0: AuthnContextClassRef DEVE contenere la classe richiesta https://refeds.org/profile/sfa o https://refeds.org/profile/mfa
- OIDC: acr DEVE contenere la classe richiesta https://refeds.org/profile/sfa o https://refeds.org/profile/mfa

L’attributo eduPersonAssurance (SAML 2.0) o il claim edu_person_assurance (OIDC) (eduPersonAssurance requested attribute) DEVE contenere i seguenti valori:

https://refeds.org/assurance
https://refeds.org/assurance/ID/unique
https://refeds.org/assurance/ID/eppn-unique-no-reassign
https://refeds.org/assurance/IAP/low

https://refeds.org/assurance/IAP/medium
https://refeds.org/assurance/ATP/ePA-1m
https://refeds.org/assurance/ATP/ePA-1d*
https://idem.garr.it/af/IDEM-P0
https://idem.garr.it/af/IDEM-P1
https://refeds.org/profile/cappuccino

* Opzionale

IDEM-P2

Esempio di caso d’uso:

- Registrazione di un dipendente.
- Identificazione tramite esibizione di un documento di identità e ulteriori verifiche tramite codice fiscale e altri documenti, o identificazione tramite altre credenziali, ad esempio SPID-L2.
- Affiliazione aggiornata entro un giorno.
- Autenticazione a due fattori.

Rappresentazione nei metadata

- SAML 2.0: eduPersonAssurance RequestedAttribute

```
<RequestedAttribute FriendlyName="eduPersonAssurance"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired="true"/>
```

Richiesta di Autenticazione (Service Provider)

AuthnContextClassRef (SAML 2.0) o acr (OIDC) DEVE contenere la classe seguente:

- REFEDS MFA: https://refeds.org/profile/mfa

Risposta (Identity Provider)

- SAML 2.0: AuthnContextClassRef DEVE contenere la classe richiesta https://refeds.org/profile/mfa
- OIDC: acr DEVE contenere la classe richiesta https://refeds.org/profile/mfa

L’attributo eduPersonAssurance (SAML 2.0) o il claim edu_person_assurance (OIDC) (eduPersonAssurance requested attribute) DEVE contenere i seguenti valori:

https://refeds.org/assurance

https://refeds.org/assurance/ID/unique
https://refeds.org/assurance/ID/eppn-unique-no-reassign
https://refeds.org/assurance/IAP/low
https://refeds.org/assurance/IAP/medium
https://refeds.org/assurance/IAP/high
https://refeds.org/assurance/ATP/ePA-1m
https://refeds.org/assurance/ATP/ePA-1d*
https://idem.garr.it/af/IDEM-P0
https://idem.garr.it/af/IDEM-P1
https://idem.garr.it/af/IDEM-P2
https://refeds.org/profile/cappuccino
https://refeds.org/profile/espresso

* Opzionale

IDEM-P3

Esempio di caso d’uso:

- Accesso a servizi critici o altamente confidenziali in cui è essenziale accertare l’identità degli accessi.
- Identificazione tramite altre credenziali come CIE o superiori.
- Identificazione tramite esibizione di un documento d’identità verificato dall’ente emittente.

Rappresentazione nei metadata

- SAML 2.0: eduPersonAssurance RequestedAttribute

```
<RequestedAttribute FriendlyName="eduPersonAssurance"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
isRequired="true"/>
```

Richiesta di Autenticazione (Service Provider)

AuthnContextClassRef (SAML 2.0) o acr (OIDC) DEVE contenere la classe seguente:

- REFEDS MFA: https://refeds.org/profile/mfa

Risposta (Identity Provider)

- SAML 2.0: AuthnContextClassRef DEVE contenere la classe richiesta https://refeds.org/profile/mfa
- OIDC: acr DEVE contenere la classe richiesta https://refeds.org/profile/mfa

L'attributo eduPersonAssurance (SAML 2.0) o il claim edu_person_assurance (OIDC) (eduPersonAssurance requested attribute) DEVE contenere i seguenti valori:

https://refeds.org/assurance
https://refeds.org/assurance/ID/unique
https://refeds.org/assurance/ID/eppn-unique-no-reassign
https://refeds.org/assurance/IAP/low
https://refeds.org/assurance/IAP/medium
https://refeds.org/assurance/IAP/high
https://idem.garr.it/af/IDEM-P0
https://idem.garr.it/af/IDEM-P1
https://idem.garr.it/af/IDEM-P2
https://idem.garr.it/af/IDEM-P3
https://refeds.org/profile/cappuccino
https://refeds.org/profile/espresso