Requisiti per i profili di Identity Assurance della Federazione IDEM

La definizione di profili di identity assurance per la Federazione IDEM si basa sui componenti individuati nel REFEDS Assurance Framework [RAF]:

- **Identifier uniqueness**: esprime la modalità ed i requisiti con cui un'organizzazione fornisce un identificatore stabile che rappresenti una persona fisica.
- **Identity proofing and credential issuance, renewal and replacement**: 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.
- **Attribute quality and freshness**: 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.

La definizione dei livelli di robustezza del processo di autenticazione per la Federazione IDEM si basa sui profili individuati nei REFEDS Authentication Profiles:

- **REFEDS SFA Profile**: profilo di autenticazione a singolo fattore, vedi https://refeds.org/profile/sfa
- **REFEDS MFA Profile**: profilo di autenticazione a più fattori, vedi https://refeds.org/profile/mfa

REFEDS Assurance Framework

Identifier uniqueness

Il componente *Identifier uniqueness*, abbreviato come "ID", descrive la modalità in cui un Identity Provider esprime che un identificatore utente rappresenta una singola persona fisica e se la relazione tra l'identificatore e la persona persiste nel tempo.

Requisiti RAF 1.0

Valore	Descrizione
https://refeds.org/assurance/ID/unique	L'identificatore deve avere le seguenti proprietà: (Unique-1) L'identificatore utente rappresenta una singola persona fisica. (Unique-2) L'organizzazione a cui fa capo l'IdP è in grado di contattare la persona a cui è assegnato l'identificatore.

	(Unique-3) L’identificatore utente non è mai riassegnato. (Unique-4) L’identificatore utente è uno dei seguenti: eduPersonUniqueId [eduPerson], SAML 2.0 persistent name identifier [SAML-Core-2.0-os], SAML 2.0 subject-id or pairwise-id [SAML-SubjectID-v1.0], OIDC sub (type: public o pairwise) [OpenID.Core]

Oltre agli identificatori elencati in Unique-4, è possibile utilizzare eduPersonPrincipalName (ePPN) solo nel caso in cui l’organizzazione si impegni a non riassegnarlo (cosa invece possibile secondo lo schema eduPerson). **NOTA BENE:** Nel caso della Federazione IDEM, ePPN è già definito come non riassegnabile.
Se l’identificatore utente utilizzato è ePPN, l’IdP dovrà specificare la non riassegnabilità utilizzando un valore ulteriore di assurance:

Valore	Descrizione
https://refeds.org/assurance/ID/eppn-unique-no-reassign	Il valore di eduPersonPrincipalName rispetta le proprietà Unique-1, Unique-2 e Unique-3.

Requisiti DRAF 2.0

Valore	Descrizione
https://refeds.org/assurance/ID/unique	Valorizzare questo campo significa che devono essere forniti uno o più identificatori come elencati in (Unique-0). L'identificatore deve avere le seguenti proprietà: (Unique-0) L’identificatore utente è uno dei seguenti: SAML 2.0 persistent name identifier [OASIS SAML], SAML 2.0 subject-id or pairwise-id [OASIS SIA], OIDC sub (type: public o pairwise) [OpenID.Core] o eduPersonUniqueId (eduPerson). (Unique-1) L’identificatore utente rappresenta una singola persona fisica. (Unique-2) L’organizzazione a cui fa capo l’IdP **DEVE** essere in grado di contattare la persona a cui è assegnato l’identificatore.

	(Unique-3) L’identificatore utente non è mai riassegnato.

Casi d’uso

Considerazioni generali:

- Le Norme di Partecipazione alla Federazione IDEM [IDEM-NdP] stabiliscono che gli IdP della Federazione gestiscano una “identità digitale in modo che la persona a cui essa si riferisce sia identificabile”. Ciò non implica automaticamente che la **persona** riferita sia una “singola persona fisica”, né la qualità e le proprietà degli identificatori assegnati.
- Le Specifiche tecniche per la compilazione e l'uso degli attributi [IDEM-STA] dichiarano che il valore assegnato a eduPersonPrincipalName “non può essere assegnato ad altri utenti”.

Account non personali:

- Di gruppo: gli account di gruppo non possono mai rispettare Unique-1 e Unique-3 di ID.
- Di ruolo/di servizio: gli account di ruolo non possono mai rispettare Unique-3 di ID.

Valori proposti per la Federazione IDEM

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	Da definire

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	Da definire

Identity proofing and credential issuance, renewal and replacement

[DA COMPLETARE]

Il componente *Identity proofing and credential issuance, renewal and replacement*, abbreviato come “IAP”, esprime numerose caratteristiche dell’identità per cui viene espresso. A tutti gli effetti è il componente principale del framework di REFEDS.

RAF IAP low

Equivale per molti aspetti al Kantara Assurance Level 1 di cui riprende la maggior parte dei requisiti. E’ inoltre compatibile con i profili di assurance di IGTF DOGWOOD e ASPEN [IGTF-LOA].
Sostanzialmente è utilizzabile per rappresentare identità auto registrate con verifica dell’email o di un numero di telefono del richiedente.

Requisiti RAF 1.0

Regole di veridicità dell’identità [KIAF-1420] 5.1.2.1	1. Le credenziali emesse dal servizio devono essere distinguibili da quelle emesse da altri servizi della stessa organizzazione (se di tipo diverso). 2. Assicurarsi che l’identità del richiedente sia associata in modo univoco con una o più credenziali e che sia univocamente riconoscibile all’interno della comunità di utenti del servizio.
Verifica dell’identità [KIAF-1420] 5.1.2.2	1. Il servizio deve implementare almeno una delle regole di veridicità dell’identità (più altre eventuali sulla base della natura del servizio). 2. Deve implementare uno dei seguenti sistemi di verifica della veridicità dell’identità: a. Verifica di persona. b. Verifica remota.
Verifica di persona [KIAF-1420] 5.1.2.3	Il servizio accetterà una auto-asserzione dell’identità e una auto-certificazione a supporto.
Verifica remota [KIAF-1420] 5.1.2.4	Il richiedente deve fornire un numero di telefono o un indirizzo email, che sarà verificato dal servizio e che sia nella disponibilità del richiedente.
Credenziali derivate [KIAF-1420] 5.1.2.7 Vedi [AARC-G031]	Il servizio può decidere di accettare credenziali di altri servizi per la verifica dell’identità. In tal caso il richiedente dovrà dar prova di essere in possesso e di avere il controllo delle credenziali utilizzate.
Verifica secondaria dell’identità [KIAF-1420] 5.1.2.8	Il servizio deve definire misure addizionali della verifica dell’identità (ad es. basate su documenti d’identità) sia nel caso in cui quelle ordinarie non siano applicabili, sia nel caso in cui voglia implementare processi di verifica alternativi a quelli indicati, ma equivalenti in termini di affidabilità.

Registrazioni della veridicità dell'identità [KIAF-1420] 5.1.2.9	Su richiesta da parte di soggetti qualificati il servizio dovrà essere in grado di fornire registrazioni attestanti l'identità relativa alla credenziale oggetto della richiesta. I soggetti qualificati possono essere: soggetti pubblici autorizzati, soggetti autorizzati dall'interessato, soggetti aventi diritto per regole di federazione. Il servizio deve permettere all'interessato di modificare le informazioni relative alla propria identità con il sufficiente grado di autenticazione (pari a quello in essere).
Rinnovo delle credenziali [KIAF-1420] 5.1.3	Il servizio deve permettere la modifica della password (o del PIN) associato alle credenziali. La procedura di modifica della password deve prevedere la verifica del possesso delle credenziali.

Requisiti DRAF 2.0

GR General Requirements

- [GR1] The CSP takes measures to ensure that the Person accomplishing each step of the identity proofing and credential issuing process is the same Person throughout the process.
- [GR1] Il CSP prende misure per assicurare che la persona che effettua ogni passaggio di verifica dell'identità e rilascio delle credenziali è la stessa persona lungo tutto il processo.
- [GR2] The identity proofing process follows documented procedures, and the documentation addresses how the CSP meets all applicable criteria for each IAP level they support.
- [GR2] Il processo di Identity Proofing segue una procedura documentata e la documentazione indica come il CSP segue tutti i criteri che si applicano ad ogni livello IAP supportato.

IE Identity Evidence

- [IE0] No identity evidence is required.
- [IE0] Non è richiesta nessuna verifica dell'identità.

VA Validation

- [VA0] No identity evidence documents are required.
- [VA0] Non è richiesto nessun documento di identità.
- VF Verification
- [VF0] The Claimant is checked to be a Person.
- [VF0] Si verifica che il richiedente sia una persona.

AB Authenticator Binding

- [AB1] Initial contact information
  The Claimant must provide and demonstrate control of contact information (e.g., email, postal address, telephone number, or similar) during the identity proofing process to be used for notification or initial authenticator issuance purposes.
- [AB1] Initial contact information
  Il richiedente deve fornire e dimostrare il controllo di uno strumento di contatto (p.e.,

mail, indirizzo postale, numero di telefono o simili) usato per la notifica o iniziale autenticazione durante il processo di verifica dell'identità.

- [AB2] Initial authenticator issuance
  If the CSP issues an authenticator to the Claimant during or after the identity proofing process, it must be delivered in a manner that can be assumed to only reach the Claimant.
- [AB2] Rilascio dell'autenticatore iniziale
  Se il CSP rilascia un autenticatore al richiedente durante o dopo il processo di verifica dell'identità, questo deve essere consegnato in modo che possa essere ricevuto solo dal richiedente.
- [AB3] Initial binding of previously issued authenticator
  If the CSP permits the Claimant to register a previously issued authenticator, then the Claimant must demonstrate control of that authenticator to the CSP during the identity proofing process.
  Such an authenticator may either be issued by the CSP in a prior context or one issued by a third party that has been documented as acceptable by the CSP.
- [AB3] Connessione con autenticatori rilasciati in precedenza
  Se il CSP permette al richiedente di utilizzare un autenticatore rilasciato in precedenza, il richiedente deve dimostrare di averne il controllo durante il processo di verifica dell'identità.
  Tale autenticatore potrebbe essere stato emesso del CSP in un contesto differente (precedente) o da terze parti ritenute accettabili dal CSP.
- [AB4] Managing authenticators and contact information
  After initial identity proofing is complete, the processes of
  - renewal or replacement of a vetted Person's existing authenticator, and
  - registering a new authenticator, and
  - updating or adding contact information

  must maintain the binding with their vetted identity either by re-identity proofing at the same or higher level or by authenticating with a valid authenticator previously bound to the vetted identity at the same or higher level. A new authenticator must be of a kind that is documented as acceptable by the CSP.
- [AB4] Gestione degli autenticatori e informazioni di contatto
  Dopo il completamento del processo di verifica dell'identità, i processi di
  - rinnovo o sostituzione dell'autenticatore di una persona verificata
  - registrazione di un nuovo autenticatore
  - aggiornamento ovvero aggiunta di informazioni di contatto

  devono mantenere il collegamento con l'identità verificata sia riverificando l'identità allo stesso livello o livello superiore, che autenticandola con un autenticatore valido rilasciato in precedenza per lo stesso livello o superiore. Un nuovo autenticatore deve essere uno di quelli accettati dal CSP.

PR Process

- [PR0] A method of account recovery is registered that is unique to the Person, such as one of the following used appropriately to deliver account recovery:
  - an alternative third-party credential (e.g. a National Electronic Identifier) which itself is assured at the same or higher level of the RAF level
  - an address of record (e.g., email, phone or physical) to be used to deliver account recovery method
  - a backup authenticator (e.g. recovery codes) issued by the registrar

This recovery information is captured during the issuing process to ensure that it is associated with the same Person whose identity has been proofed. The CSP may support updating and/or changing the means of account recovery by the same Person.

- [PR0] Il recupero delle credenziali avviene tramite uno strumento unico per ogni utente. Ad esempio uno dei seguenti:
    - credenziali di terze parti per le quali l'utente ha lo stesso grado di affidabilità di RAF o maggiore
    - un indirizzo email, numero telefonico o indirizzo fisico
    - un codice di autenticazione emesso dal registrante

  Le informazioni per il recupero delle credenziali sono acquisite durante il processo di emissione delle stesse per assicurare che siano associate allo stesso utente la cui identità viene provata. Il CSP consentire l'aggiornamento e/o il cambio del mezzo per il recupero da parte dell'utente stesso.

RP Remote Process

- [RP0] IdP has confirmed an user's address, and user confirmed receipt of confirmation during the credential issuing process.
  [does this prove the applicant is a Person, or do we allude to other 'are you a robot' checks?]

  Note: This address can be the user's claimed phone number, physical address, or a third-party email address. UserApplicant will confirm receipt of IdP's address confirmation message through a means that proves the user received the message through the selected address.
- [RP0] …. [questo prova che il richiedente è una persona, oppure alludiamo ad altre verifiche "non sono un robot"?]

  Note: Questo indirizzo può essere sia un numero di telefono dichiarato dall'utente, un indirizzo fisico o l'indirizzo email di una terza parte. Il richiedente confermerà la ricevuta del messaggio di conferma dell'indirizzo emesso dall'IdP tramite uno strumento che provi che ha ricevuto il messaggio all'indirizzo selezionato

Casi d'uso

- Copre l'emissione di credenziali per studenti pre-immatricolati (prospect) laddove non sia utilizzato SPID o non sia possibile utilizzarlo.
    - Il motivo per cui è necessario fornite credenziali federate a questi utenti è che devono poter accedere a servizi federati (spesso interni) legati al percorso di perfezionamento dell'immatricolazione.
- (UNIMI) Ospiti:
    - Utenti registrati al di fuori dei DB del personale e degli studenti che sono individuati come ospiti nella directory di ateneo e possono essere forniti di identità federata.
    - Utenti autoregistrati - limitati a DB specifici (no identità federata).
- (CNR) Utenti autoregistrati: eventualmente solo per specifici servizi (no identità federata).

- (eventualmente GARR ed altri) IdP aperti e/o modello eduID - vedi SWITCH eduID.ch e SWAMID eduID.se:
    - Utenti autoregistrati su IdP registrati nelle federazioni di identità nazionali (in alcuni casi esportati su eduGAIN). Possibilita' di elevare il grado di affidabilita' dell'identità tramite account linking (ad es. SPID) o associazione dell'ente di appartenenza.

RAF IAP medium

Equivale per molti aspetti al Kantara Assurance Level 2 (sections 5.2.2-5.2.2.9, section 5.2.2.12 and section 5.2.3) di cui riprende la maggior parte dei requisiti. E' inoltre compatibile con i profili di assurance di IGTF BIRCH e CEDAR [IGTF-LOA] ed è allineato all'eIDAS assurance level low [eIDAS-LOA].
Sostanzialmente è utilizzabile per rappresentare identità verificate tramite un documento di identita', ma senza controlli approfonditi sull'autenticita' dello stesso.

Requisiti RAF 1.0

Regole di veridicità dell'identità [KIAF-1420] 5.2.2.1	(vedi RAF IAP low) Il servizio deve pubblicare le regole di verifica dell'identita' e attenervisi.
Verifica dell'identità [KIAF-1420] 5.2.2.2	3. Il servizio deve implementare almeno una delle regole di veridicità dell'identità (più altre eventuali sulla base della natura del servizio). 4. Deve implementare uno dei seguenti sistemi di verifica della veridicità dell'identità: a. Verifica di persona. b. Verifica remota. c. Verifica basata sulla relazione gia' in essere. d. Verifica basata sull'affiliazione.
Verifica di persona [KIAF-1420] 5.2.2.3	Il servizio verifica l'identita' della persona tramite un documento di identita' riconosciuto e **apparentemente autentico**.
Verifica remota [KIAF-1420] 5.2.2.4	Il servizio verifica l'identita' della persona **in remoto** tramite l'esibizione o l'invio di una copia di un documento di identita' riconosciuto e **apparentemente autentico**, o di un documento che attesti il proprio status di studente o impiegato (tessera aziendale), o ancora un numero di conto corrente, o l'identificativo cliente di una fornitura di servizi pubblici (energia elettrica, acqua, ecc.). Il servizio verifichera' l'attendibilita' e l'autenticita' dei documenti prodotti con le autorita' che li hanno emessi.
Verifica basata su relazione già in essere [KIAF-1420]	La verifica e' positiva se: - esiste una relazione già in essere tra la persona e l'organizzazione e tale relazione ha dato luogo alla fornitura di credenziali con password con livello di entropia compatibile con Kantara AL2 (NIST 800-63 Appendice A)

5.2.2.5	- l'identita' e' stata verificata di persona o in remoto secondo quanto previsto in 5.2.2.3 e 5.2.2.4
Verifica basata su affiliazione [KIAF-1420] 5.2.2.6	La verifica e' positiva se rispetta i requisiti indicati in 5.2.2.5 ed e' possibile verificare l'affiliazione con documenti ufficiali (tesserini e simili).

Requisiti DRAF 2.0 (vedi "Table of Normative IAP Criteria")

GR General Requirements

- [GR1] The CSP takes measures to ensure that the Person accomplishing each step of the identity proofing and credential issuing process is the same Person throughout the process.
- [GR1] Il CSP prende misure per assicurare che la persona che effettua ogni passaggio di verifica dell'identità e rilascio delle credenziali è la stessa persona lungo tutto il processo.
- [GR2] The identity proofing process follows documented procedures, and the documentation addresses how the CSP meets all applicable criteria for each IAP level they support.
- [GR2] Il processo di Identity Proofing segue una procedura documentata e la documentazione indica come il CSP segue tutti i criteri che si applicano ad ogni livello IAP supportato.
- [GR3] Records are kept to record:
    - when the Person was identity-proofed
    - who was proofed
    - to what IAP level

  Each record should be preserved in accordance with local record-retention guidelines.
- [GR3] Viene tenuta traccia di:
    - quando è stata verificata l'identità di una persona
    - chi è stato verificato (?)
    - livello IAP assegnato

  Questi dati devono essere conservati nel rispetto delle locali regole di conservazione dei dati.

IE Identity Evidence

[IE1] Identity evidence is acceptable for use in identity proofing if it is valid at the time of identity proofing and is either issued by a nationally recognised source or is nationally recognised as being valid for identification purposes or is a documented attestation from an authority recognised by the CSP per [VA3.3].

[IE1] Una attestazione di identità è accettabile nel processo di verifica dell'identità se è valida nel momento in cui l'identità è verificata ed è emessa da una fonte nazionale ovvero è nazionalmente riconosciuta come valida ai fini dell'identificazione ovvero è una attestazione riconosciuta dal CSP come valida per [VA3.3].

VA Validation

- [VA1] Identity evidence presented appears to be genuine.
- [VA1] L'attestazione di identità presentata sembra essere autentica.

VF Verification

- [VF0] The Claimant is checked to be a Person.
- [VF0] Si verifica che il richiedente sia una persona.
- [VF1] Presented identity evidence reasonably appears to belong to the Claimant.
- [VF1] L'attestazione di identità presentata ragionevolmente appare come appartenere al richiedente.

AB Authenticator Binding

- [AB1] Initial contact information
  The Claimant must provide and demonstrate control of contact information (e.g., email, postal address, telephone number, or similar) during the identity proofing process to be used for notification or initial authenticator issuance purposes.
- [AB1] Informazioni di contatto iniziali
  Il richiedente deve fornire e dimostrare il controllo di uno strumento di contatto (p.e., mail, indirizzo postale, numero di telefono o simili) usato per la notifica o iniziale autenticazione durante il processo di verifica dell'identità.
- [AB2] Initial authenticator issuance
  If the CSP issues an authenticator to the Claimant during or after the identity proofing process, it must be delivered in a manner that can be assumed to only reach the Claimant.
- [AB2] Rilascio dell'autenticatore iniziale
  Se il CSP rilascia un autenticatore al richiedente durante o dopo il processo di verifica dell'identità, questo deve essere consegnato in modo che possa essere ricevuto solo dal richiedente.
- [AB3] Initial binding of previously issued authenticator
  If the CSP permits the Claimant to register a previously issued authenticator, then the Claimant must demonstrate control of that authenticator to the CSP during the identity proofing process.
  Such an authenticator may either be issued by the CSP in a prior context or one issued by a third party that has been documented as acceptable by the CSP.
- [AB3] Connessione con autenticatori rilasciati in precedenza
  Se il CSP permette al richiedente di utilizzare un autenticatore rilasciato in precedenza, il richiedente deve dimostrare di averne il controllo durante il processo di verifica dell'identità.
  Tale autenticatore potrebbe essere stato emesso del CSP in un contesto differente (precedente) o da terze parti ritenute accettabili dal CSP.
- [AB4] Managing authenticators and contact information
  After initial identity proofing is complete, the processes of
  - renewal or replacement of a vetted Person's existing authenticator, and
  - registering a new authenticator, and
  - updating or adding contact information

must maintain the binding with their vetted identity either by re-identity proofing at the same or higher level or by authenticating with a valid authenticator previously bound to the vetted identity at the same or higher level. A new authenticator must be of a kind that is documented as acceptable by the CSP.

- [AB4] Gestione degli autenticatori e informazioni di contatto
  Dopo il completamento del processo di verifica dell'identità, i processi di
  - rinnovo o sostituzione dell'autenticatore di una persona verificata
  - registrazione di un nuovo autenticatore
  - aggiornamento ovvero aggiunta di informazioni di contatto

  devono mantenere il collegamento con l'identità verificata sia riverificando l'identità allo stesso livello o livello superiore, che autenticandola con un autenticatore valido rilasciato in precedenza per lo stesso livello o superiore. Un nuovo autenticatore deve essere uno di quelli accettati dal CSP.

UR Unsupervised Remote Proofing

- [UR2] [VA3] is an additional validation requirement.
- [UR2] [VA3] E' un requisito di validazione addizionale.

Casi d'uso

(CNR) Utenti con rapporto non strutturato e a tempo:

- Assegnista e/o Dottorando/Studente di Master: registrati localmente (nell'istituto di afferenza tramite delega) e sono sincronizzata nella directory centrale in seguito all'approvazione del direttore. Account utilizzati principalmente per l'accesso a servizi interni, ma comunque disponibili sull'IdP del CNR. NON HANNO affiliazione ed email valorizzati.

(CNR) Registrazione utenti:

- (**da verificare**) verifica della fedina penale.

(UNIMI) Registrazione Studenti:

- Ammissione studenti: estremi del documento.
- Immatricolazione: scansione del documento con verifica dell'autenticita' basata su requisiti fisici e correlazione con gli altri documenti e dati presentati (Codice Fiscale, residenza, ecc.).

(INFN) Registrazione utenti, riconoscimento:

- Esibizione di un documento d'identita'.
- Personalmente riconosciuta.

RAF IAP high

[DA COMPLETARE]

Attribute quality and freshness

Il componente *Attribute quality and freshness*, abbreviato come "ATP", esprime la qualità e la frequenza di aggiornamento di determinati attributi. Al momento gli unici attributi per cui è definito sono **eduPersonAffiliation, eduPersonPrimaryAffiliation** ed

eduPersonScopedAffiliation ed unicamente in relazione alle affiliazioni *student, faculty, member*. I valori previsti indicano la sola frequenza di aggiornamento:

Requisiti RAF 1.0

Valore	Descrizione
https://refeds.org/assurance/ATP/ePA-1m	Aggiornamento dell'attributo entro 31 giorni dalla modifica dello stato.
https://refeds.org/assurance/ATP/ePA-1d	Aggiornamento dell'attributo entro 1 giorno dalla modifica dello stato.

Requisiti DRAF 2.0

Casi d'uso

Bocconi:

- al termine degli studi passano 18 mesi prima che il valore di affiliazione di uno studente diventi *alumn*.

Unimilano (non chiaro come e se quanto sotto si rifletta in ePA/ePPA/ePSA):

- studenti: account valido per sempre, ma con cambio di gruppo (l'informazione sul gruppo di appartenenza non è in LDAP ma su db, comunque reperibile): la velocità con cui il cambio gruppo viene inserita dipende dalle singole segreterie studenti (es: infermieristica, pochi studenti, in settimana, studi umanistici, un mesetto).
- docenti e personale: se accedi almeno una volta l'anno al tuo account di posta l'account viene mantenuto vivo in LDAP, però dall'anagrafica è possibile sapere se un utente è "cessato" e la data di cessazione viene inserita in anticipo.

INFN

- Aggiornamento dello stato degli account in tempo reale, cioe' automaticamente sulla base dei valori contenuti nelle basi di dati amministrative/contabili.

INGV

- Il database viene popolato su richiesta, prevede l'uso solo da dipendenti e assegnisti/borsisti su fondi interni;
- Il controllo viene fatto tre/quattro volte l'anno rispetto alle tabelle dei contratti di lavoro attivi;
- Alcuni account rimangono attivi anche dopo il termine del contratto per venire incontro a necessità di progetto o in attesa di associatura.

ISPRA

- Aggiornamento dello stato degli account __teoricamente__ in tempo reale, di fatto ci possono esserci ritardi dovuti alla traslazione dei valori dalle basi di dati amministrative/contabili alla directory dell'ente.

Valori proposti per la Federazione IDEM

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	Da definire

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, cioe’ che consentano l’accesso a dati particolari (GDPR) e/o risorse particolarmente pregiate.
Profili	Da definire

Valore	Nessun valore
Descrizione e casi d’uso	La frequenza di aggiornamento del valore di affiliazione non è indicata.
Profili	Da definire

REFEDS SFA Profile

REFEDS MFA Profile

Casi d’uso

Modalita’ di attivazione:

CINECA - Abilitazione secondo fattore via primo fattore, ma reset del secondo fattore solo via account esterno (e collegato) SPID con auth L2 oppure con SMS. In dettaglio:
ENROLLMENT
Necessario per attivare la generazione del seed e la configurazione dell'app utente

- E1. L'utente accede ad un servizio web che, previa autenticazione semplice, richiede la generazione di un segreto numerico chiamato seed.
- E2. Il servizio web genera il seed che viene mostrato all'utente in modalità alfanumerica e mediante QR code.
- E3. L'utente configura opportunamente una app sul proprio dispositivo inquadrando il QR code o inserendo il seed.

- E4. L'utente utilizza l'app per visualizzare il passcode corrente e lo inserisce sul servizio web per conferma.
- E5. Il servizio web genera a sua volta il passcode con il seed precedentemente assegnato, lo confronta con quello inserito dall'utente e, se corretto, associa il seed all'utente.
- E6. Il servizio web propone all'utente l'inserimento di un numero di telefono personale su cui ricevere il token per il reset dell'enrollment
- E7. L'utente inserisce il numero ed richiede l'invio di un token via SMS a conferma del numero
- E8. Il servizio web invia un SMS e propone e richiede all'utente l'inserimento del token
- E9. L'utente inserisce il token ricevuto via SMS, conferma e termina il processo

Riferimenti

[RAF] REFEDS Assurance Framework (v1.0)
https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0

[DRAF-20] Draft REFEDS Assurance Framework (v2.0)
https://docs.google.com/document/d/13tfexdOafnSEXidJ6fbcT0a5qo0wrsu_fqLk856AaTA/edit#

[IDEM-NdP] Norme di Partecipazione alla Federazione IDEM (v1.6)
https://wiki.idem.garr.it/wiki/File:Norme_di_partecipazione_alla_Federazione_IDEM_v_1.6.pdf

[IDEM-STA] Specifiche tecniche per la compilazione e l'uso degli attributi (v3.0)
https://wiki.idem.garr.it/wiki/File:SpecificheTecnicheAttributi_v3.0_20161129.pdf

[SAML-Core-2.0-os] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML-SubjectID-v1.0] SAML V2.0 Subject Identifier Attributes Profile Version 1.0
https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html

[OpenID.Core] OpenID Connect Core 1.0
https://openid.net/specs/openid-connect-core-1_0.html

[eduPerson] Internet2/MACE. eduPerson Object Class Specification (202111)
https://wiki.refeds.org/display/STAN/eduPerson+2021-11

[ITU-T-X-1254-09-20]
https://www.itu.int/rec/T-REC-X.1254-202009-I/en

[KIAF-1420]
https://kantarainitiative.org/download/7663

[IGTF-LOA]
https://www.igtf.net/ap/authn-assurance/

[eIDAS-LOA]
IT https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32015R1502
EN https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502

[SPID-LG-RAO-PA]
SPID: emanate le Linee Guida per l'identificazione degli utenti da parte delle PA
https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/193241617130O__OLinee+Guida+RAO+Pubblico+v.1.0.pdf

[SPID-R]
REGOLAMENTO RECANTE LE MODALITÀ ATTUATIVE PER LA REALIZZAZIONE DELLO SPID (articolo 4, comma 2, DPCM 24 ottobre 2014)
https://www.agid.gov.it/sites/default/files/repository_files/circolari/spid-regolamento_modalita_attuative_v1.pdf

[AARC-G031]
Guidelines for the evaluation and combination of the assurance of external identities
https://doi.org/10.5281/zenodo.1308682