Miniguida Account Linking

Gruppo GARR SPID / CIE / EIDAS
Di Andrea Ranaldi - ISPRA

Glossario

Piccolo glossario per definire sinificato ed accezione ai termini di questo documento

- **Utente** – La persona fisica che opera
- **Account** – le credenziali ed in generale il sistema che permette all'utente di essere riconosciuto come tale
- **Identificazione** – Il processo con cui si collega un utente in modo certo alla sua identità.
  Es: un poliziotto ti ferma e verifica i tuoi documenti, sei stato identificato.
- **SPID** - Sistema Pubblico di identità Digitale, un sistema che permette agli utenti di essere identificati digitalmente a livello nazionale
- **CIE –** Carta di identità elettronica, può essere utilizzata per identificarsi digitalmente a livello nazionale
- **EIDAS** - electronic IDentification, Authentication and trust Services, un sistema che permette di essere identificati digitalmente a livello europeo
- **Account interni** – Utenti gestiti ed identificati internamente all'ente
- **Account esterni** – Utenti gestiti dall'ente ma privi di identificazione

Non una sola ricetta:

Non esiste un unico modo per unificare gli account ma varia in base alle esigenze applicative

- Livello di identificazione dell'utente richiesto
- Livello di autenticazione richiesto
- Livello di autorizzazione necessaria
- Dati disponibili a livello applicativo
- Dati ottenibili nella fase di autenticazione

Identificazione

Definiamo come livello di identificazione la certezza con cui possiamo collegare un utente alla sua identità e la regolamentazione che vincola la persona alle proprie credenziali.

In base a questa definizione possiamo creare una semplice scala.

- **Non identificato**
  tutte le forme di registrazione autodichiarate.
- **Bassa**
  identificato de visu o tramite documento ma senza una responsabilità chiara dell'utente verso le credenziali.
- **Alta**
  identificato de visu o tramite documento con una chiara responabilità dell'utente verso le credenziali e l'uso che ne viene fatto.

Esempi di identificazione

Non identificato

- Amazon richiede i dati fiscali, verifica la email, il telefono e la tua carta di credito ma non controlla chi tu sia, soltanto che tu possa pagare e che tu possa recuperare le credenziali di accesso tramite telefono o email. (quando inserisci una carta ti chiede a chi è intestata)
- Google richiede un numero di telefono e controlla che tu possa leggerlo ma non può collegare i tuoi dati anagrafici al telefono.

Bassa

- Gli account di ufficio, le credenziali sono date ai dipendenti ma raramente viene definita la responsabilità e gli obblighi legali verso le stesse, le credenziali sono spesso date e fatte utilizzare a terzi (colleghi).

Alta

- Accesso tramite **SPID** / **EIDAS**: l'utente viene identificato tramite documento, ha l'obbligo legale di non cedere le credenziali a terzi, ha l'obbligo legale di mantenere i dati di registrazione aggiornati.
- Accesso tramite **CIE**: l'utente viene identificato da un pubblico ufficiale al momento del rilascio, l'utente ha l'obbligo legale di conservazione del documento e di denunciare lo smarrimento o furto.

Identificazione – Regole auree

Puoi confrontare soltanto dati certi

- Se identifichi tramite email e la email è la stessa l'identità è la stessa.
- Se identifichi la persona con codice fiscale (SPID) avere la stessa email non è indicativo (più persone potrebbero usarla)
- Se un dato non è univoco non può essere utilizzato per collegare gli account, es: potrebbero esistere migliaia di Andrea Ranaldi

Livello maggiore sovrascrive livello inferiore

- Se colleghi due account vincono i dati presenti nel sistema con maggiore certezza di identificazione.

In caso di pari livello il dato più nuovo sovrascrive il dato più vecchio

- Se un utente accede con diversi mezzi con pari identificazione (es: SPID - CIE) i dati più nuovi sovrascrivono i più vecchi.

Autenticazione

Come autenticazione intendiamo tutto il processo con cui si accede ai sistemi: come vengono gestite le credenziali, le forme di sicurezza previste per l'autenticazione, rotazione e requisiti delle password, secondi fattori e sistemi di autorizzazione.

In base alla tipologia di processo possiamo definire una semplice scale:

- Bassa
  Credenziali gestite autonomamente dall'utente
- Media
  Requisiti password, monitoraggio degli accessi.
- Alta:
  Requisiti password definiti, secondo fattore / one time password / dati biometrici, monitoraggio degli accessi.

Esempi di autenticazione

Bassa

- Accesso di default al proprio computer
- La maggior parte dei siti internet incluso Google ed Amazon se privi di secondo fattore attivato.

Media

- Accesso di default ad Active Directory (Scadenza password a 6 mesi, 5 password memorizzate, password di minimo 8 caratteri)
- SPID level 1

Alta

- SPID level 2 e level 3
- CIE
- Google con second factor attivo
- Microsoft 365 con second factor attivo

Autenticazione – Regole auree

Autenticazione ≠ Identificazione

- Avere una autenticazione solida non garantisce una identificazione certa. (es: Google con one time password)

L'identificazione non varia con l'autenticazione

- Le regole di identificazione non variano in base al processo di autenticazione.

l'autenticazione influisce sull'autorizzazione

- Le possibilità di un utente variano in base al livello di autorizzazione

Account – Identificazione

SPID

- Il codice fiscale identifica univocamente l'utente (persona)
- lo spid-code Identifica l'account ed è univoco per ogni account spid (es: Andrea Ranaldi su poste ha uno spid-code differente da Andrea Ranaldi su Infocert). Indirettamente identifica la persona: so che lo spid-code identifica un Andrea Ranaldi ma senza codice fiscale non so quale Andrea Ranaldi

CIE

- Il codice fiscale identifica univocamente l'utente (persona)
- Il numero di documento identifica univocamente il documento

EIDAS

- il PersonIdentifier identifica univocamente l'utente (persona)
- Identifica l'accoun con lo PersonIdentifier, univoco per ogni account EIDAS (es: Andrea Ranaldi su poste ha uno PersonIdentifier differente da Andrea Ranaldi su Infocert)

Account interni

- Se presente il codice fiscale identifica univocamente la persona
- Il nome utente identifica univocamente l'account sul dominio di riferimento
- Gli utenti vengono solitamente identificati de visu

Account esterni

- I dati identificativi sono autodichiarati
- Nome utente (frequentemente email) identifica univocamente l'account
- Gli utenti non sono identificati

Rif. Attributi https://wiki.idem.garr.it/w/images/b/b7/Confronto_attributi_SPID_CIE_EIDAS.ods

Account linking – Falsi amici!

Non tutti i dati sono idonei ad identificare un utente, spesso accettiamo dati incerti o non univoci come identificativi.

Di seguito riportiamo alcuni esempi di errori classici:

Email

- L'email non è un dato univoco, io e mia moglie potremmo registrare i nostri account SPID con lo stesso indirizzo email, sarebbe lecito.
- L'email definisce un canale per le comunicazioni non identifica la persona, non indica un domicilio digitale.

Nome e cognome

- Chiamarsi allo stesso modo non implica essere la stessa persona.

Somma di dati personali

- Anche sommando i dati personali non univoci (es: nome, cognome, data di nascita, ecc.) non si esclude la possibilità di omonimie, la rende soltanto meno probabile.

Regola aurea contro i falsi amici:

L'account linking va fatto unicamente con dati univoci condivisi!

Account linking – Veri amici!

In Italia è presente un solo ed unico codice che identifica univocamente gli utenti (persone):

CODICE FISCALE

Il codice fiscale è l'unico dato condiviso che ti permette di unire più account con un alto livello di identificazione, tutti gli altri dati sono falsi amici.

Account linking SPID / CIE / EIDAS

SPID / CIE

- Gli account SPID e CIE posso essere ricollegati tramite codice fiscale, questa operazione è sicura e può essere automatica, indipendentemente dal numero di account di cui un utente dispone.

EIDAS

- Purtroppo gli account EIDAS non dispongono di un codice fiscale ne di omologhi europei o nazionali. Gli account EIDAS vengono identificati tramite PersonIdentifier e non possono essere riconciliati ad altri account.

Account interni

- Se presente il codice fiscale gli account interni, identificati de visu, possono essere riconciliati insieme agli account SPID / CIE

Account Esterni

- Gli account non identificati in linea di principio non possono essere riconciliati.
- Gli accessi tramite account esterni sono sconsigliati e limitati ai casi specifici in cui gli utenti non possono ottenere un account SPID.

Account linking – Regole auree

Si esegue

- Soltanto in presenza di dati univoci, sicuri e condivisi

Non si esegue

- In presenza di una qualunque ambiguità
- Se il link diminuisce il livello di identificazione dell'utente