IdP Account Linking

Francesco Malvezzi

Università di Modena e Reggio nell'Emilia

6 aprile 2017

Introduzione

Dando per scontato che l'autenticazione SPID si integri sul nostro IdP, cosa succede se l'identità proveniente da SPID non si correla con una [1] identità locale?

[1] ed esattamente una sola

Gli scenari dell'orrore sono due:

- nessuna identità locale (si tratta di un cittadino che non ha un account nella nostra organizzazione);
- profili locali multipli (ad esempio docente e direttore di un dipartimento). Questo succede quando ad una sola persona identificata con un codice fiscale possono coincidere più account.

Nessun match

Qui il rischio è che un SP dia per scontato che se un utente è autenticato, allora è anche autorizzato.
In questo caso abbiamo un accesso indebito ai dati.

Nessun match: nessun attributo

Accertarsi che un utente solo SPID manchi di tutti gli attributi normali. Se SPID rilascia nome, cognome e mail, assicurarsi che popolino un attributo diverso dai fidati `givenName`, `sn` e `mail`.
Avremo un errore `500`[2] sullo SP, ma evitiamo un accesso indebito.
In prospettiva l'amministratore dello SP dovrebbe sistemare il suo codice.

[2] internal server error

Nessun match: Profile Intercept

Usare il *Profile Intercept* di Shibboleth-IdP-v3 per impedire l'autenticazione degli utenti SPID se la controparte[3] non è pronta.
Si tratta in effetti di un'autorizzazione effettuata dall'IdP, cioé una delle radici del male cosmico.

[3] cioè lo SP identificato con il suo entityID

Troppi match: c14n

La soluzione è nel meccanismo della canonicalizzazione (c14n) che lo IdP-v3 inserisce dopo l'autenticazione e prima della risoluzione degli attrbuti.
In pratica è un Spring WebFlow identico a quelli di autenticazione.

Troppi match: attribute-sourced-subject

Grazie al flow c14n incluso nella distribuzione *attribute-sourced-subject* è possibile introdurre un filtro che riduce le correlazioni sperabilmente al match singolo.
Si tratta di un meccanismo rigido che impone una scelta organizzativa meditata.

Troppi match: form di scelta utente

Tuttavia bisogna scrivere codice: `https://github.com/francescm/idp3-accountlinking`