SPiD e CIE in AAI

Workshop di CCR

Zoom 24-28 maggio 2021

Ringraziamenti

- Marco Esposito Micenin e Michele Antonio Tota per l'analisi, lo sviluppo del codice, i test ed il supporto nella compilazione degli atti amministrativi
- Roberto Gomezel per la gestione dei flussi amministrativi per le convenzioni
- Il gruppo AAI per aver preso in carico e condotto l'attività con utili contributi per l'analisi.

Perchè SPiD e CIE

- Il “Decreto Semplificazione e Innovazione Digitale” (DL n. 76/2020 convertito in Legge n. 120/2020) stabilisce che
  - Entro il 28 febbraio 2021, tutte le amministrazioni sono tenute ad avviare il passaggio dalle diverse modalità di autenticazione online al Sistema Pubblico di Identità Digitale – SPID e alla Carta d'Identità Elettronica.
  - Da tale data le amministrazioni non potranno più rilasciare o rinnovare le vecchie credenziali. Potranno essere utilizzate le credenziali rilasciate in precedenza fino alla loro naturale scadenza e non oltre il 30 settembre 2021.

Fonte AGiD

Chiarimenti

- Il CTS di IDEM ha sottoposto al Dipartimento per la Trasformazione Digitale alcune domande relative all'obbligo di attivare SPiD e CIE per i propri utenti e le risposte dicono che
  - **Per i servizi rivolti ai dipendenti non sussiste alcun obbligo relativamente a SPiD a CIE**
  - Non sussiste alcun obbligo di utilizzo di SPiD e CIE per tutti i casi in cui non sia tecnicamente possibile utilizzare SPiD e CIE, ne consegue che le credenziali gestite internamente alle organizzazioni dovranno essere mantenute.
  - **In generale i servizi online aperti ai cittadini (come ad esempio i concorsi pubblici e le immatricolazioni di studenti) devono prevedere l'accesso tramite SPiD e CIE** .
  - Per gli studenti sussiste l'obbligo di accedere tramite SPiD e CIE per tutti i servizi online relativi ad attività amministrative. Anche nei casi in cui sussista l'obbligo, vanno però previste credenziali alternative a SPiD per tutti quegli studenti che non possono averle, come minorenni, stranieri, ecc.
  - Sarà quindi opportuno, per tutte le università e gli enti di ricerca, definire in modo specifico i casi d'uso relativi alle attività amministrative.

SPiD e CIE: obbligo o opportunità?

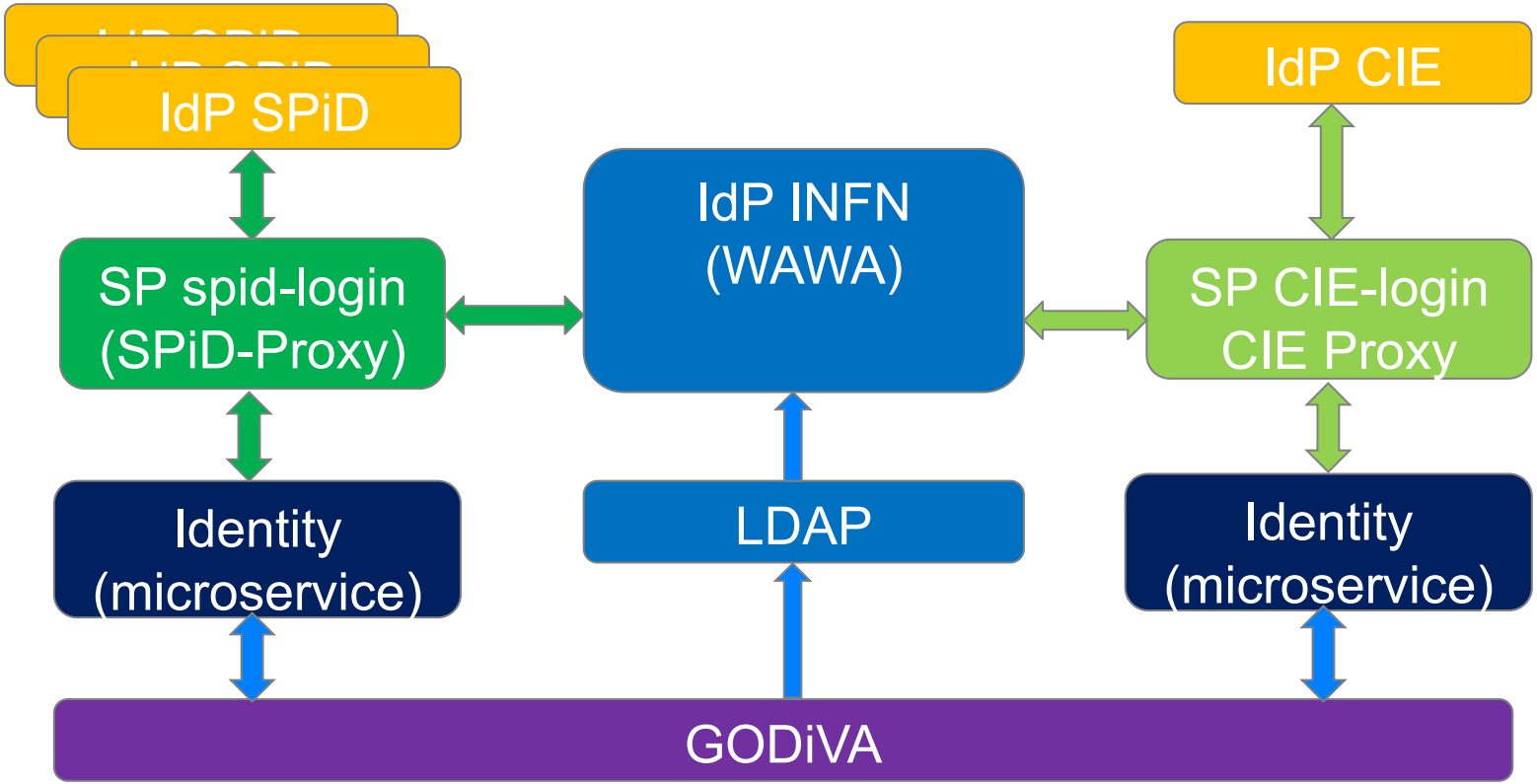
- Obbligo
  - Accesso al servizio web di gestione concorsi pubblici
- Opportunità
  - **Acquisizione Identità Digitali già certificate (LoA2)**
  - Utilizzo di SPID e CIE per la certificazione nei flussi autorizzativi di userPortal
  - Secondo fattore di autenticazione per esecuzione di alcune azioni in autonomia (e.g: reset password)

Workflow tecnico/amministrativo

done – in progress – to do

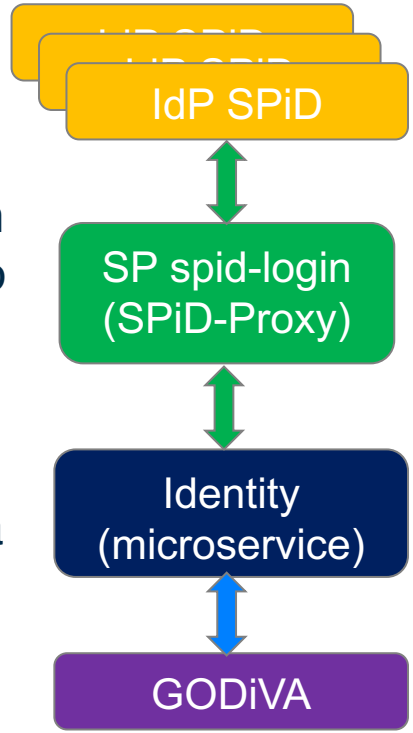
- SPiD
  - Implementazione tecnica
  - Verifica tecnica
  - Collaudo
  - Firma convenzione
  - Messa in produzione
- CIE
  - Firma convenzione
  - Implementazione ambiente di test
  - Verifiche
  - Implementazione ambiente di produzione

Architettura



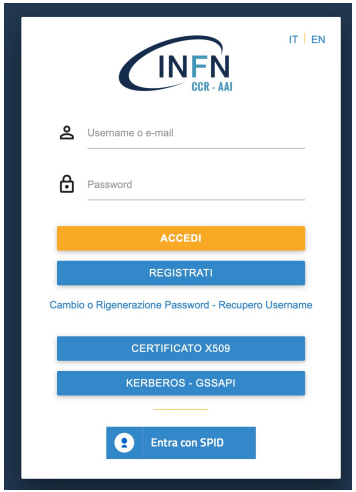
SP spid-login (spid-proxy)

- SP SPiD con backend Identity (il DB “staging” di GODiVA per i microservizi)
- Basato su spid-php di Michele D’Amico (@damikael) del team developersitalia, aggiornato a SimpleSAMLphp 1.19 da Marco Esposito Micenin (@voidloop) ora uno dei top-contributors del progetto su github
  - https://github.com/italia/spid-php
- Modulo di gestione/linking delle identità sviluppato ex-novo da Marco e Michele



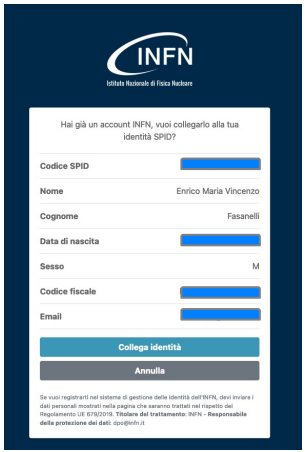
SP spid-login (spid-proxy) workflow

- Il pulsante “Accedi con SPiD” in WAWA redirige al nostro spid-proxy che a sua volta invia l’asserzione SAML all’IdP selezionato
- Al login andato a buon fine il proxy
  - Confronto tra
    - SPiD-code
    - Codice Fiscale
    - E-mail (+ luogo e data di nascita)
  - Se l’identità SPiD non corrisponde a nessuna identità in GODiVA, la crea LoA2 e ritorna a WAWA l’infnUUID appena creato
  - Se trova una corrispondenza → next slide



SP spid-login (spid-proxy) identity linking

- Se la corrispondenza è con uno SPiD-code già registrato → OK ritorna l'infnUUID a WAWA
- Se match con CF su identità LoA2
  - Richiesta di identity-linking → aggiuge lo SPiD-code all'identità digitale INFN in GODiVA → ritorna l'infnUUID a WAWA
- Se match con e-mail .AND. luogo-e-data-di-nascita
  - Richiesta di identity-linking → aggiuge lo SPiD-code all'identità digitale INFN in GODiVA → ritorna l'infnUUID a WAWA
- In tutti gli altri casi, ritorna un errore con indicazione di rivolgersi ad aai-support



SPiD & IDEM

- Anche se il processo di autorizzazione all'utilizzo di una risorsa dovrebbe essere sempre a carico della risorsa, le regole di partecipazione ad IDEM ci impongono di impedire l'accesso a risorse IDEM ed eduGAIN a persone che non siano almeno "affiliate"
  - Staff del dipartimento ospitante le sezioni
  - Ospiti/Visitatori
- Aggiunto un controllo che impedisce agli utenti che non hanno alcun ruolo nell'INFN di accedere via autenticazione INFN ad SP IDEM ed eduGAIN

Work-in-progress & to do

- Implementazione delle specifiche CIE nel CIE-SP
- CIE identity linking con i soli attributi trasmessi da CIE
  - Nome, Cognome, data di nascita, codice fiscale
- Messa in produzione di CIE
- Inserimento dell'identificazione con SPiD/CIE nel flusso di richiesta abilitazione di userPortal

The End

Grazie

Domande?