UNIVERSITÀ
DEGLI STUDI
DI PADOVA

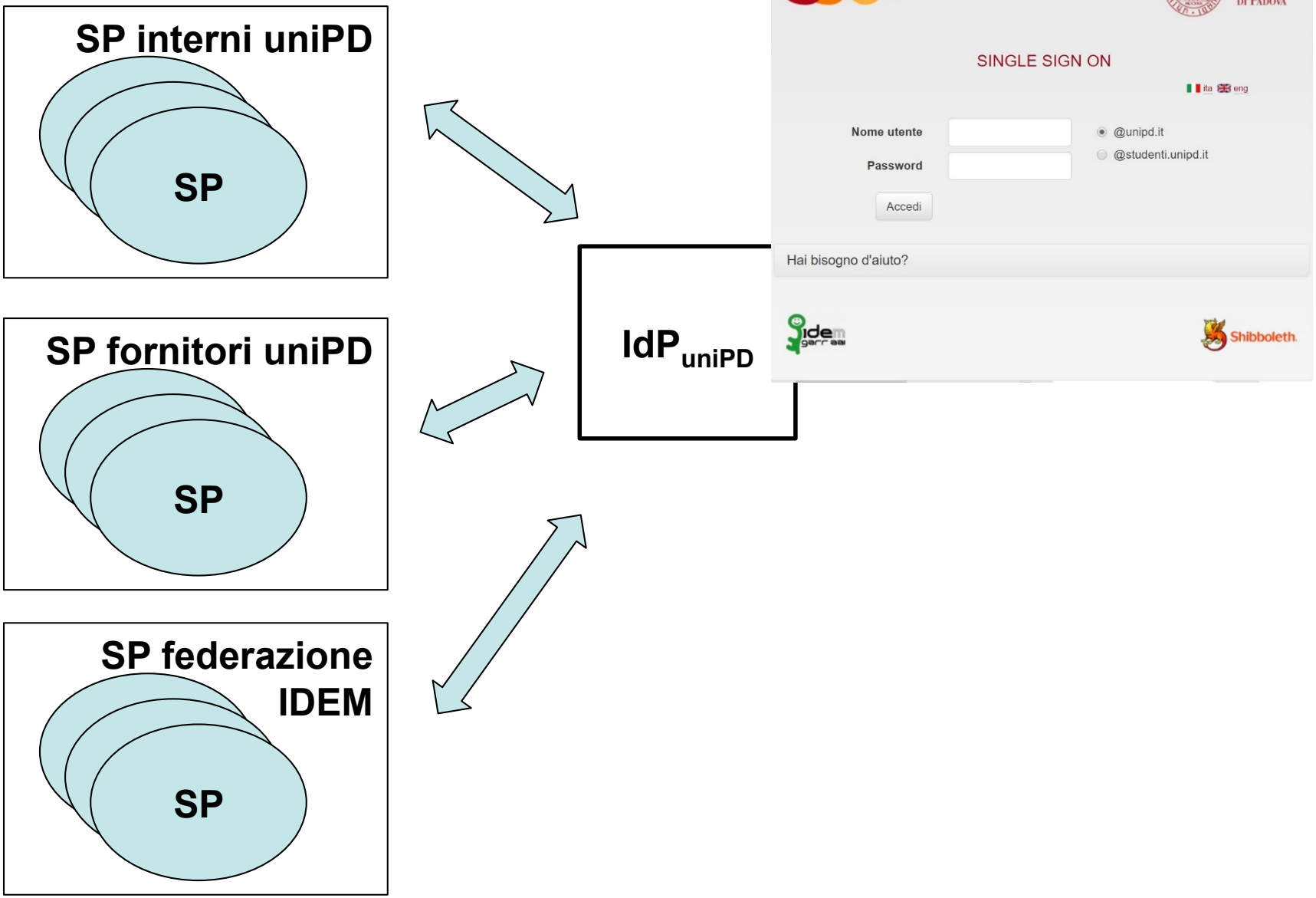
Integrazione di SPID con il SSO di Ateneo

Workshop Garr 2017, Roma 6/4/2017

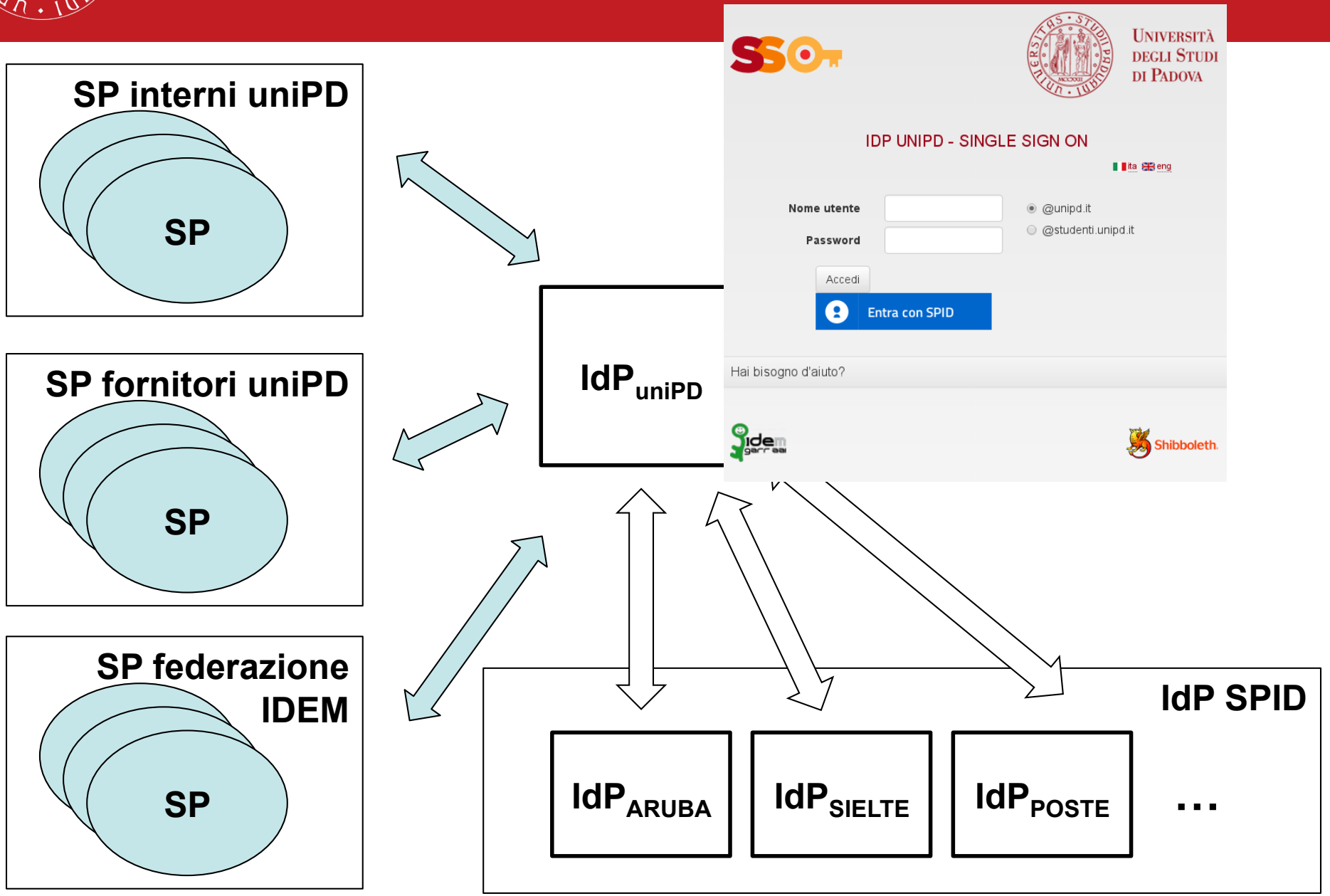
Marco Naimoli
Marco.naimoli@unipd.it

Stefano Zanmarchi
stefano.zanmarchi@unipd.it

Architettura SSO esistente



Architettura SSO con SPID



UNIVERSITÀ DEGLI STUDI DI PADOVA

Obiettivi

- L'IdP$_{\textbf{uniPD}}$ deve autenticare l'utente:
  - localmente (LDAP di ateneo)
  - tramite altro IdP (Sielte, Aruba, Poste,…)
- L'IdP$_{\textbf{uniPD}}$ deve passare agli SP gli attributi:
  - ricavati localmente (LDAP, DB)
  - ricevuti da altro IdP (Sielte, Aruba, Poste,…)
- Non sviluppare codice:
  - facilità di manutenzione
  - resilienza agli upgrade
- Soluzione «shibboleth only»

UNIVERSITÀ DEGLI STUDI DI PADOVA

La nostra idea

- Installato sul server IdP_{uniPD} anche il sw SP:
  - IdP_{uniPD} resta un IdP
  - IdP_{uniPD} diventa anche un SP per gli IdP_{SPID}
- Ovviamente questo SP è registrato in SPID
- Cliccando su «entra con SPID» il controllo passa al sw SP (che ridirige l'utente a un IdP_{SPID})
- Superata l'autenticazione SPID l'utente torna a IdP_{uniPD} e il controllo torna al sw IdP

UNIVERSITÀ DEGLI STUDI DI PADOVA

Semplice ma…

I sw SP e IdP non nascono per scambiarsi il controllo del flusso di autenticazione come vogliamo noi. Tre problemi:

1. «L'andata verso SPID»: passaggio del flusso dal sw IdP al sw SP solo per chi vuole accedere con SPID.

2. «Il ritorno da SPID»:
   - passaggio del flusso dal sw SP al sw IdP
   - accettazione dell'autenticazione SPID
   - passaggio dell'identità utente e degli attributi SPID

3. Il mantenimento dell'autenticazione locale (per chi non vuole accedere con SPID.

UNIVERSITÀ DEGLI STUDI DI PADOVA

Soluzioni ai 3 problemi

Tre soluzioni per tre problemi:

1.«L'andata». Il sw IdP inizia un autenticazione RemoteUser, con la location `/idp/Authn/RemoteUser` protetta dal sw SP (che quindi ridirige l'utente a SPID).

2. «Il ritorno». Il mod_headers di Apache passa il REMOTE_USER e gli attributi SPID al sw IdP.

3. Il meccanismo MFA del sw IdP gestisce il controllo dei flussi di autenicazione

UNIVERSITÀ DEGLI STUDI DI PADOVA

Conclusioni

- Condividiamo la nostra soluzione su GitHub: http://goo.gl/B1wqde
- Da fare/migliorare:
  - LoA impostabili dai SP di backend
  - Logout
  - Flow aggiuntivo nel caso l'utente avesse più identità locali (con stesso CF) tra le quali scegliere.
    Ad oggi abbiamo implementato la gestione tramite una regola statica (canonicalizzazione c14n): scegliamo noi la priorità delle identità.