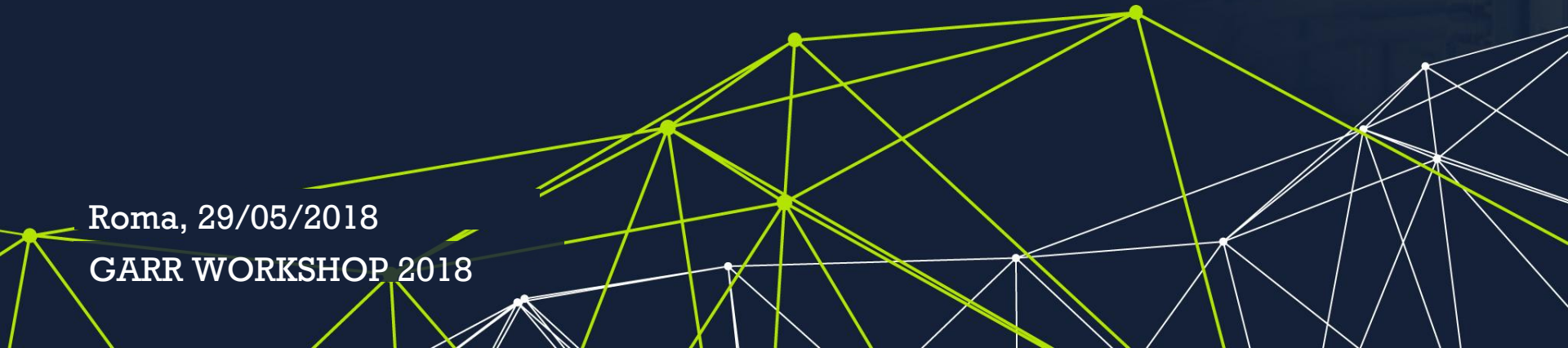
Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Casi d'uso: web access, SSO, autenticazione federata

idem garr aai

Davide Vaghetti (GARR) – davide.vaghetti@garr.it



Roma, 29/05/2018

GARR WORKSHOP 2018

Agenda

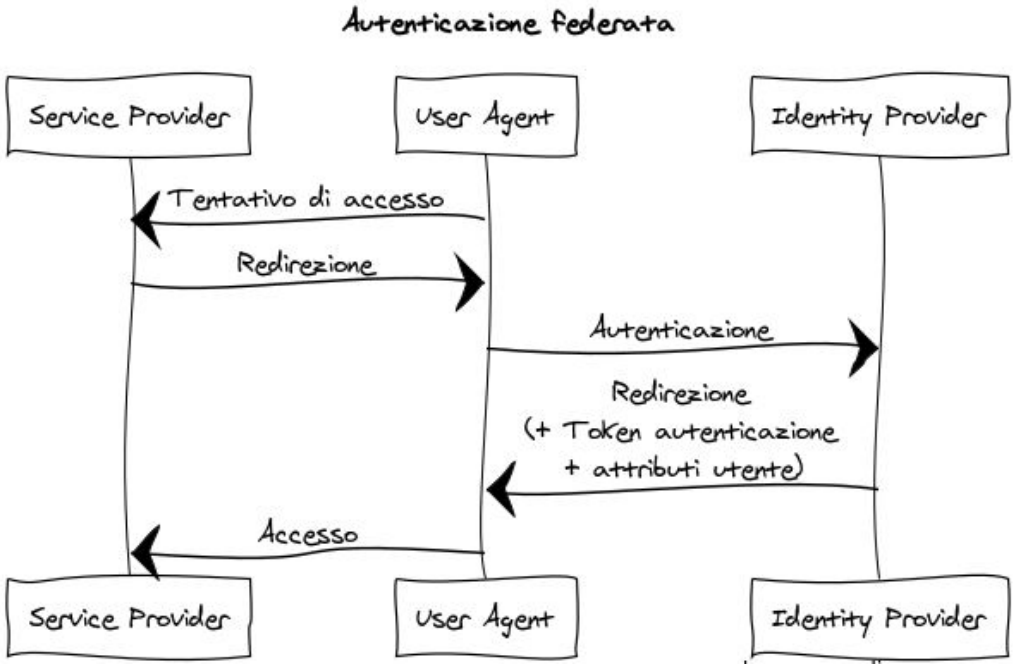
- Autenticazione web e Federata
- Servizi federati
- Federazione IDEM e eduGAIN
- Entità affidabili
- Basi legali per il rilascio degli attributi

Autenticazione web locale

- Gestore dell'identità == Gestore del servizio
- Registrazione e profilazione locali
  - Nome
  - Cognome
  - Email
  - ecc.
- Accesso tramite credenziali locali

Titolare del trattamento (data controller) == **Responsabile del trattamento (data processor)**

Autenticazione Federata



1. L'utente tenta di accedere ad una applicazione protetta da un Service Provider.
2. Il Service Provider richiede l'autenticazione federata (discovery) e redirige l'utente ad un Identity Provider.
3. L'utente si autentica.
4. Il Identity Provider redirige l'utente al servizio con un token di autenticazione (ed eventualmente un insieme di attributi).
5. L'utente accede al servizio.

Autenticazione Federata

- Registrazione e profilazione su IDMS dell'organizzazione
- Autenticazione in carico al Identity Provider dell'organizzazione
- Service Provider che insistono su Identity Provider per l'autenticazione degli utenti
- (eventuale ulteriore profilazione lato Service Provider)

Titolare del trattamento (data controller) **!=** **Responsabile del trattamento (data processor)**

Servizi federati

Quattro casi semplici:

1. Mera autenticazione e passaggio di attributi NON personali (*entitlements*).
    a. Riviste elettroniche.
2. Identificatore *targeted* e affiliazione.
    a. Wiki, CMS, ecc.
3. Identificatore *targeted* e attributi personali.
    a. Servizi di videoconferenza, Filesender, ecc.
4. Identificatore univoco, globale e persistente (ePPN) + attributi personali.
    a. GARR Cloud, File Sharing & data cloud, PaaS (Office365).

Servizi federati: mera autenticazione e *entitlements*

ATTENZIONE

- *eduPersonEntitlement* potrebbe contenere valori ulteriori **da non condividere**.
- Filtrare i valori con una regola per ogni Service Provider, rilasciando a ciascuno solo i valori destinati al servizio.

<xml />

```
[...]
<saml2p:Status>
   <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</saml2p:Status>
[...]
<saml:Attribute [...] FirendlyName=”eduPersonEntitlement”>
   <saml:AttributeValue>urn:mace:dir:entitlement:common-lib-terms</saml:AttributeValue>
[...]
```

Servizi federati: Identificatore *targeted* e affiliazione.

Identificatore *targeted*

- Identity Provider entityID

  https://orgdomain/idp

- Service Provider entityID

  https://spdomain/sp

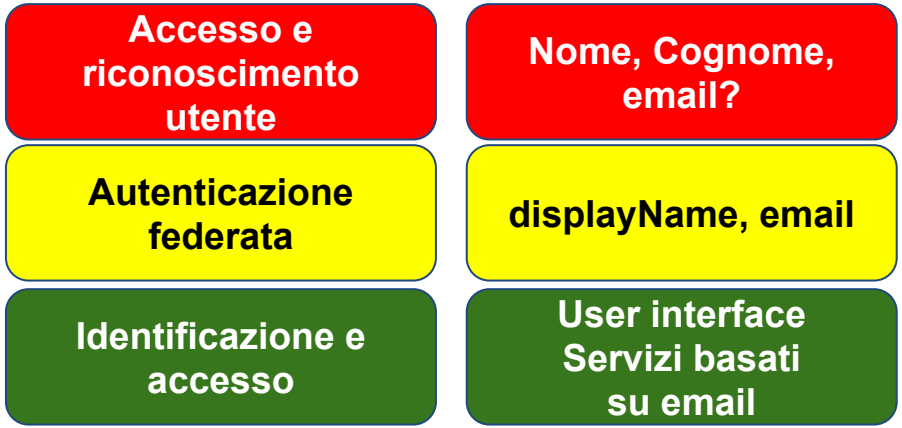
- Opaque User identifier

  Ad es. (random)uuid

<xml />

```
[...]
<saml2p:Status>
   <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</saml2p:Status>
[...]
<saml:Attribute [...] FirendlyName=”eduPersonScopedAffiliation”>
   <saml:AttributeValue>student@orgdomain</saml:AttributeValue>
[...]
```

Servizi federati: Identificatore *targeted* e attributi personali



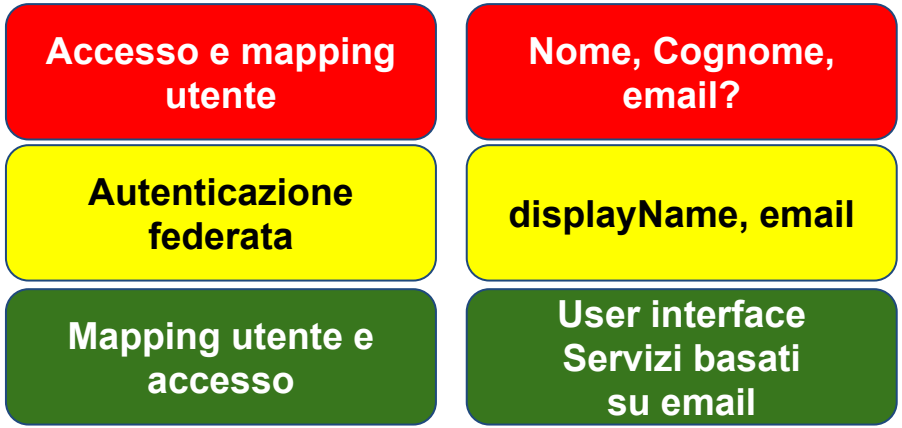
<xml />

```
[...]
   <saml:NameID
     Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
[...]
<saml:Attribute [...] FirendlyName=”email”>
   <saml:AttributeValue>student@orgdomain</saml:AttributeValue>
[...]
```

Funzionalità legate agli attributi personali:

- Videoconferenza:
  - Nome partecipante
  - Notifiche via mail
- Filesender:
  - Invio di messaggi con il mittente dell’utente
- Blog, CMS:
  - Nome autore articoli
  - Notifiche via mail

Identificatore univoco, globale e persistente (ePPN) + attributi personali



<xml />

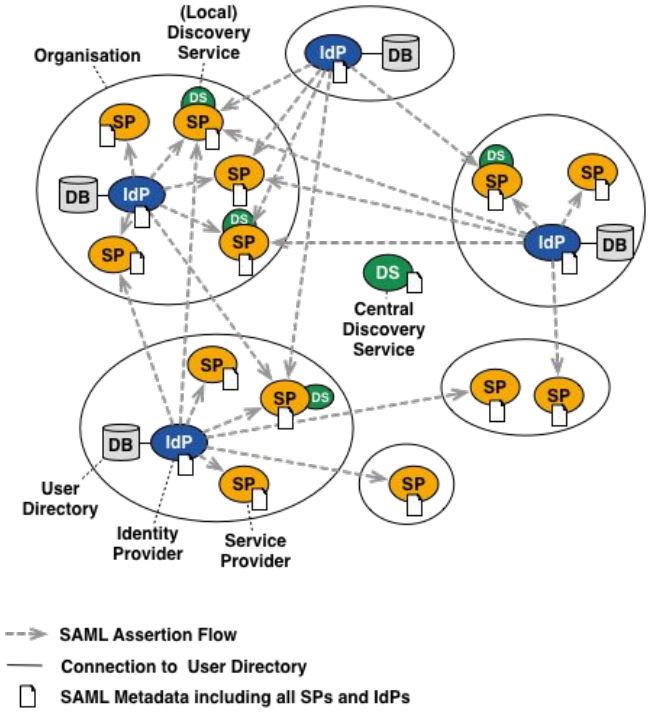
```
[...]
<saml2p:Status>
   <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</saml2p:Status>
[...]
<saml:Attribute [...] FirendlyName=”eduPersonPrincipalName”>
   <saml:AttributeValue>(opaque)uid@orgdomain</saml:AttributeValue>
[...]
```

Perché un identificatore globale?

Per condividerlo con altri servizi:

- Servizi accessori: mapping su utente locale potenzialmente oggetto di servizi federati accessori (spesso della stessa organizzazione).
- Servizi collegati: lo stesso utente può collegare altri servizi federati (**spesso di organizzazioni diverse**).

La Federazione IDEM

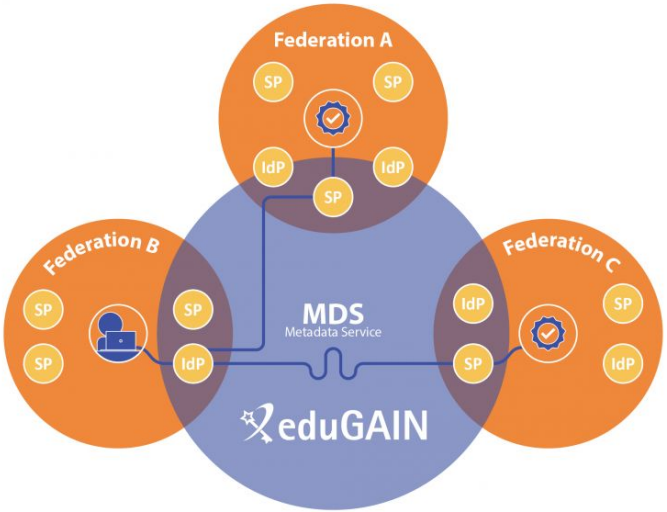


- **Full mesh**: IdP e SP si parlano direttamente (no HUB centralizzato).
- **Membri**: Enti GARR con almeno un IdP o un SP registrato in federazione.
- **Partner**: fornitori di servizi con almeno un SP registrato in federazione.
- **Servizi nazionali:** comunià della ricerca, GARR, commerciali
- **Servizi internazionali:** comunita' della ricerca, e/r-infrastructures, GEANT, NREN, commerciali

La Federazione IDEM: requisiti per i Service Provider

- conformi specifiche tecniche
- responsabilità legale
- metadata aggiornati
- contatti tecnici
- certificati digitali
- auditing servizio IDEM GARR AAI
- log
- limitare richiesta dati
- indicare scopo richiesta dati
- condivisione con terzi
- non aggregare

La Federazione IDEM + eduGAIN



- **Interconnessione** Federazioni di identità nazionali tramite aggregazione dei metadata.
- **Politiche comuni** di federazione.
- **Comunità omogenee**, almeno in buona parte.
- **Regole diverse** di partecipazione.
- **Affidabilità esplicita** di Service Provider e Identity Provider tramite *tagging* dei metadata.

Entità affidabili

REFEDS Research and Scholarship Entity Category

- https://refeds.org/research-and-scholarship
- Bundle di attributi (Identificatore persistente, Nome, Cognome, Email, Affiliazione)
- Servizi *della* e *per la* comunità della ricerca

REFEDS Sirtfi - (Security Incident Response Trust Framework for Federated Identity)

- https://refeds.org/sirtfi
- sicurezza operativa e incident response

GÉANT Data Protection Code of Conduct

- https://wiki.refeds.org/x/MIAY
- privacy policy (assolve anche a informativa sullo scopo del trattamento)
- attributi richiesti

Basi legali per il rilascio degli attributi

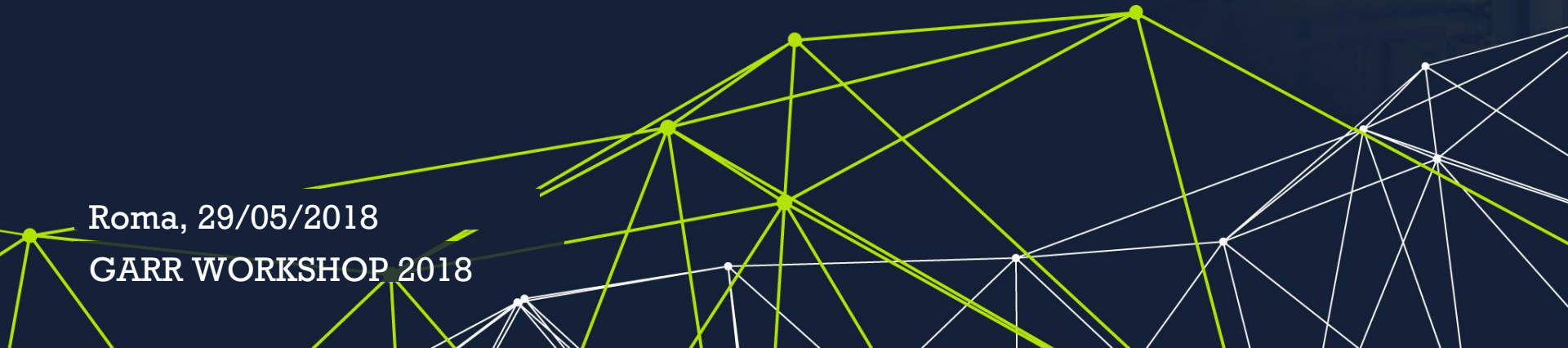
Contratto	• **Accesso a rivista elettronica X tramite IdP https://orgdomain/idp** • **Autorizzazione utenti con ePE =** urn:mace:dir:entitlement:common-lib-terms
Legittimo interesse	• ***potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento*** • ***Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali***
Consenso	• **Il consenso prestato da un dipendente o uno studente e' libero? (*l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile…*)**

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

GRAZIE

domande?

Davide Vaghetti (GARR) - davide.vaghetti@garr.it



Roma, 29/05/2018

GARR WORKSHOP 2018