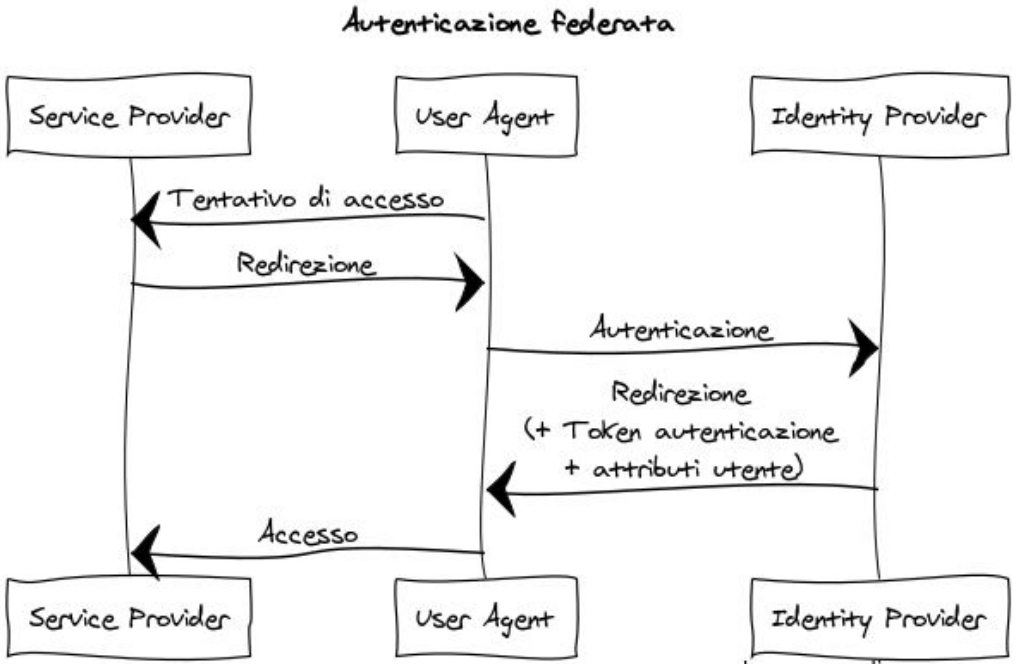
GARR Virtual Organization Platform

IDEM DAY 2018
Roma 7-9 Giugno 2018
Davide Vaghetti - IDEM GARR AAI
davide.vaghetti@garr.it

Agenda

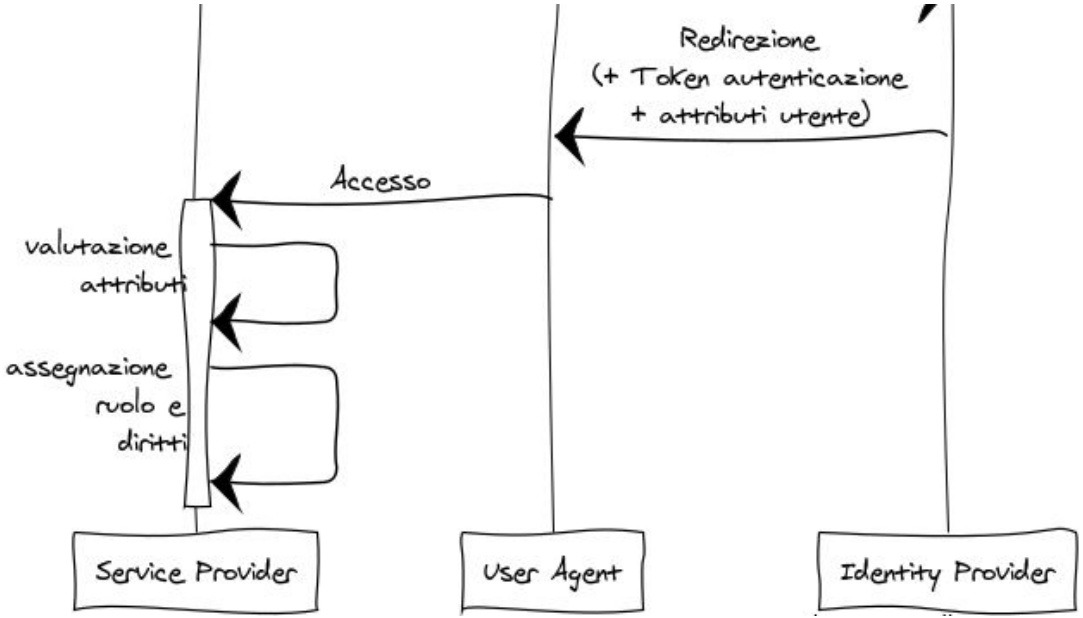
- Autenticazione federata (in pillole)
- Autorizzazione federata: modelli, problemi e soluzioni
- Virtual Organisation
- GARR VO Platform(s)
- Casi d’uso della comunità IDEM GARR

Autenticazione federata



1. L'utente tenta di accedere ad un applicazione protetta da un Service Provider.
2. Il Service Provider richiede l'autenticazione federata.
3. L'utente sceglie la propria organizzazione e viene rediretto al Identity Provider.
4. L'utente si autentica.
5. Il Identity Provider redirige l'utente al servizio con un token di autenticazione ed una serie di attributi.
6. L'utente accede al servizio.

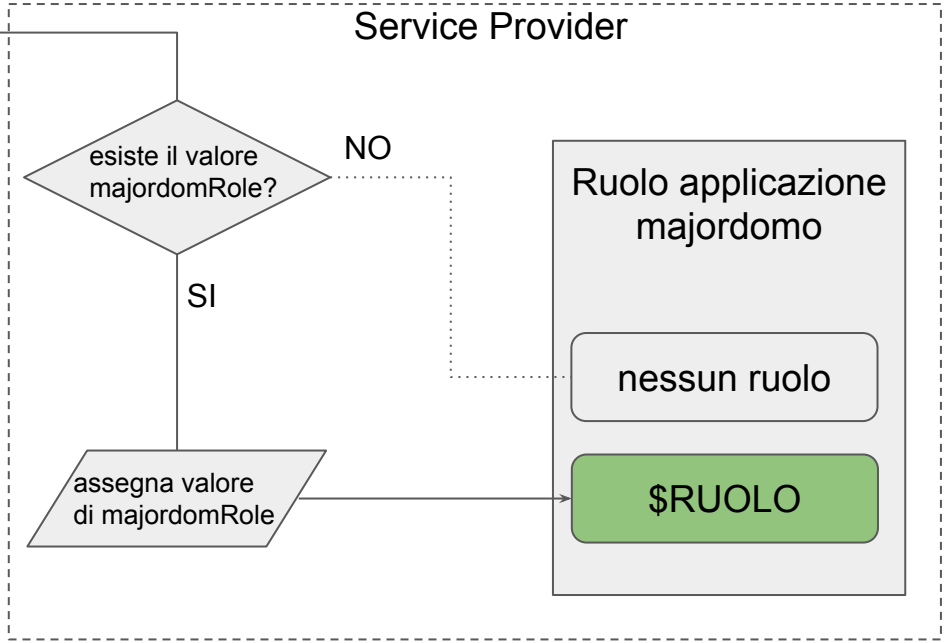
Autorizzazione federata



1. L'utente si ripresenta al servizio con token di autenticazione (asserzione SAML) e un insieme di attributi.
2. L'utente accede al servizio:
   a. Il servizio valuta gli attributi.
   b. Il servizio assegna un ruolo locale e un insieme di diritti all'utente.

Autorizzazione diretta

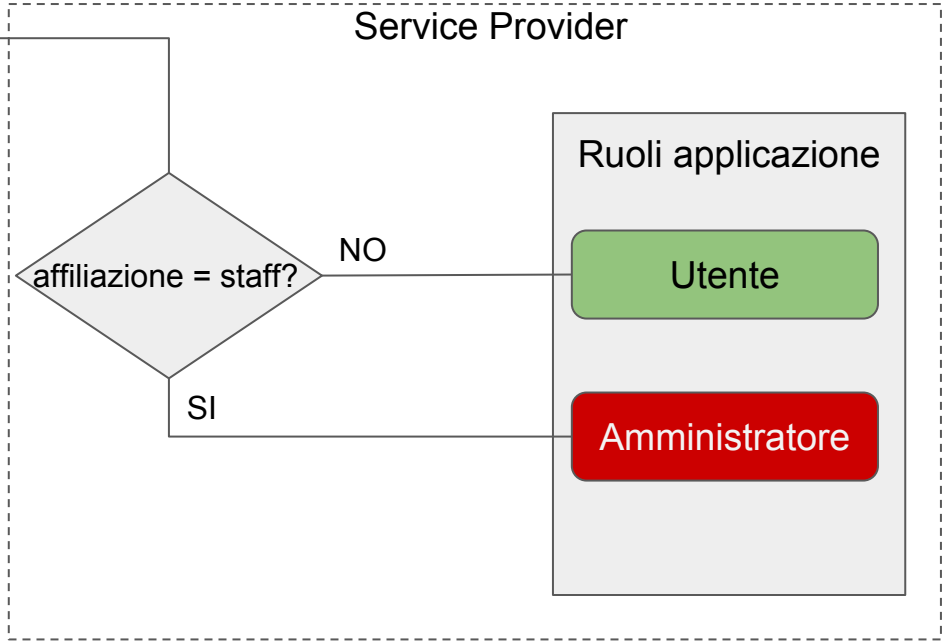
Attributi forniti dal Identity Provider	
E-mail	davide.vaghetti@garr.it
UserID	vaghetti
x-garr-ApplicationUserAccess	redmine.dir.garr.it nfcert.dir.garr.it nagios-web.irccs.garr.it puppetmaster.irccs.garr.it StartWeb nf.rm1.garr.net gitlab.dir.garr.it wiki.garr.it nf4.rm2.garr.net majordomRole::user grouper.idem.garr.it
x-garr-WikiName	DavideVaghetti



Autorizzazione indiretta o derivata

Attributi forniti dal Identity Provider

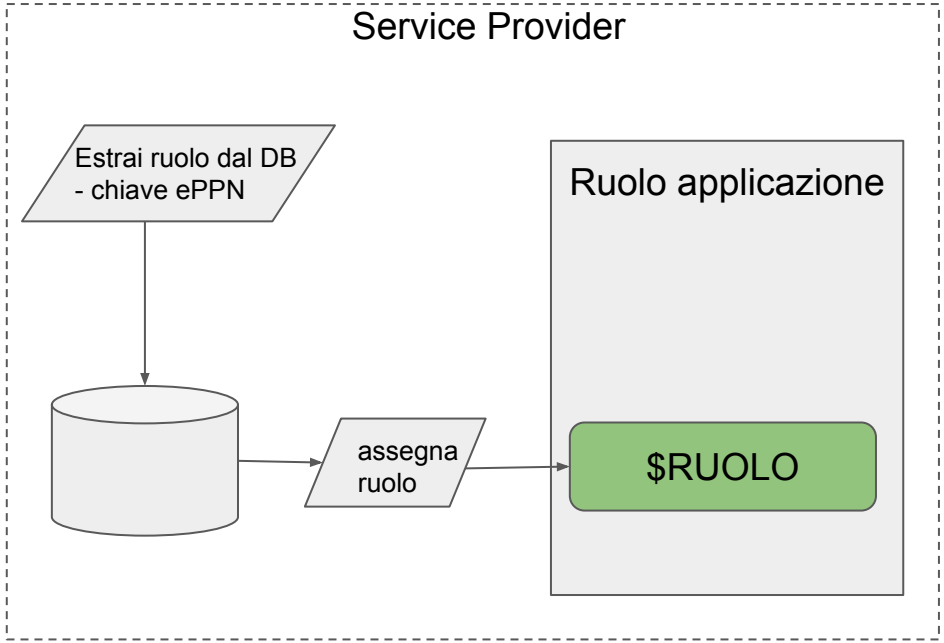
Information to be Provided to Service	
Display name	Davide Vaghetti
eduPersonPrincipalName	vaghetti@garr.it
Scoped Affiliation	staff@garr.it member@garr.it
E-mail	davide.vaghetti@garr.it
Name	Davide
Surname	Vaghetti



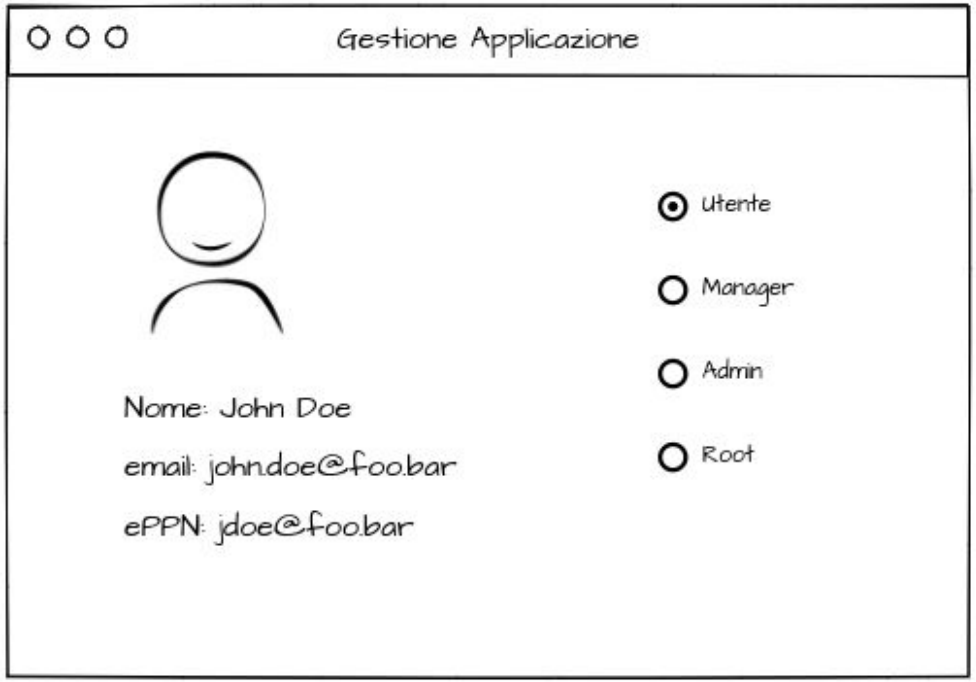
Autorizzazione locale

Attributi forniti dal Identity Provider

Information to be Provided to Service	
Display name	Davide Vaghetti
eduPersonPrincipalName	vaghetti@garr.it



Autorizzazione locale



L’applicazione protetta dal Service Provider ha un modulo di gestione per assegnare i ruoli agli utenti.

Autorizzazione: modelli e problemi

Autorizzazione diretta

Organizzazioni (Identity Provider)

- 1000 utenti * 100 applicazioni = 100000 elementi di configurazione.
- l'autorità sui servizi è naturalmente distribuita.
- L'organizzazione deve adeguarsi ai parametri di autorizzazione del Service Provider.

Applicazioni (Service Provider)

- Il Service Provider, di fatto, non è più autoritativo.
- L'assegnazione diretta di ruoli e diritti espone ad attacchi, per mitigare il rischio:
  - Filtri sui valori trasmessi dagli Identity Provider (eduGAIN 2500 Identity Provider).
  - Accordi per stabilire un canale fiduciario con ogni Identity Provider (eduGAIN…).

Autorizzazione: modelli e problemi

Autorizzazione indiretta o derivata

Organizzazioni (Identity Provider)

- Gli utenti devono essere raggruppati in categorie corrispondenti a diverse classi di servizi.

Applicazioni (Service Provider)

- Ogni Identity Provider ha il suo sistema di classificazione
  - Ad esempio, a valori equivalenti di affiliazione (student, staff, faculty, member) non corrispondono le stesse categorie di utenti, i valori vanno interpretati, nel migliore dei casi, stato per stato.

Autorizzazione: modelli e problemi

Autorizzazione locale

NOTA BENE: Di fatto l'autorizzazione federata non avviene o è limitata al mero accesso.

Organizzazioni (Identity Provider)

- I problemi di accesso degli utenti non sono risolvibili con azioni lato Identity Provider.

Applicazioni (Service Provider)

- Procedure complesse per la *cattura* dell'identificatore per la creazione utente.
- Notevole sovraccarico amministrativo per l'assegnazione dei ruoli e dei diritti agli utenti.

Autorizzazione: problemi e soluzioni

Possibili soluzioni ai problemi dei diversi modelli di autorizzazione federata:

- Gruppi indipendenti dalla classificazione interna dell'organizzazione.
- Gestione delegata dell'appartenenza ai gruppi.
- Piattaforma esterna per la gestione dei gruppi con rapporti fiduciari verso i Service Provider.

Benefici aggiuntivi:

- Una sola piattaforma per più organizzazioni.
- Gruppi trasversali tra diverse organizzazioni (leggi gruppi di ricerca, gruppi di lavoro, commissioni, ecc.)

Virtual Organisation (VO)

Cosa sono?

Entità, di solito di durata limitata, che raggruppano persone che hanno qualcosa in comune, come un progetto di ricerca, un gruppo di lavoro, o un incarico specifico.

A che servono?

Ad individuare i membri di uno specifico gruppo. Opzionalmente possono ospitare attributi personali assegnati ai membri.

Come si gestisce l'afferenza?

Tramite la delega ad un responsabile.

GARR VO Platform

https://grouper.idem.garr.it

- in produzione
- accesso federato
- Attribute authority indipendente interrogata dai Service Provider (chiave = ePPN)
- attualmente utilizzata per il wiki di IDEM
- flusso di accreditamento poco flessibile

GARR VO Platform

`https://comanage.idem.garr.it`

- in test
- attualmente utilizzata per il progetto CTA (INAF)
- accesso federato
- Attribute authority indipendente interrogata dai Service Provider (chiave = ePPN)
- Molteplici flussi di accreditamento (invito, autoregistrazione, approvazione admin, ecc.)
- Supporta account linking
- Supporta definizione e provisioning di attributi secondari
- Supporta chiavi SSH

Casi d’uso comunità GARR IDEM

Avete dei casi d’uso?

Scrivete a:

idem-help@garr.it

Domande?

GRAZIE

IDEM DAY 2018
Roma 7-9 Giugno 2018
Davide Vaghetti - IDEM GARR AAI
davide.vaghetti@garr.it