



**NET  
MAKERS**

# Attributi dinamici per l'autorizzazione application-aware

Fabio Farina  
Consortium GARR

# Caso di studio per GARR-T

- Sviluppo attivo
- Goal: Evolvere autorizzazione oltre i limiti attuali
- Come: Know-how autenticazione federata
- Strumenti, implementazione, primi risultati

# L'autenticazione? No problem

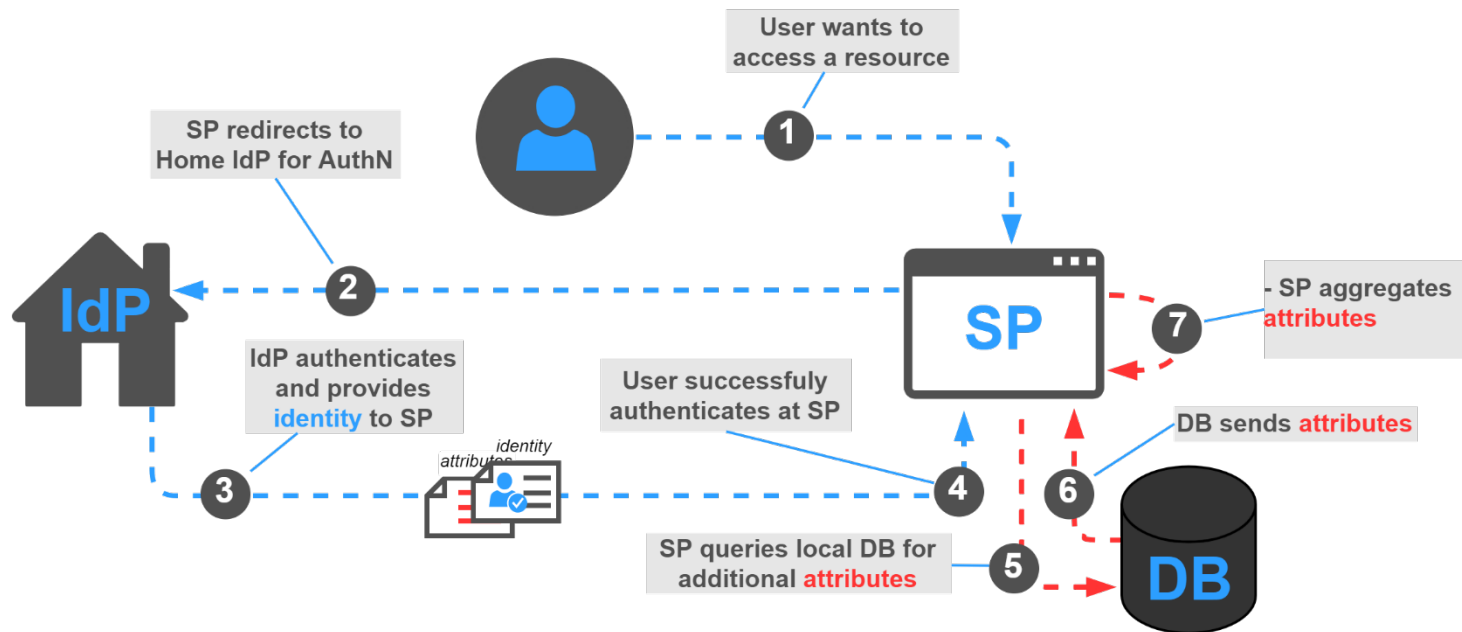


- Esterna alle applicazioni
- Federata e logiche di delega
- Protocolli standard
- Interoperabilità & proxy



# L'Autorizzazione oggi

- Definizione + Valutazione + Enforcement  
→ integrazione molto stretta



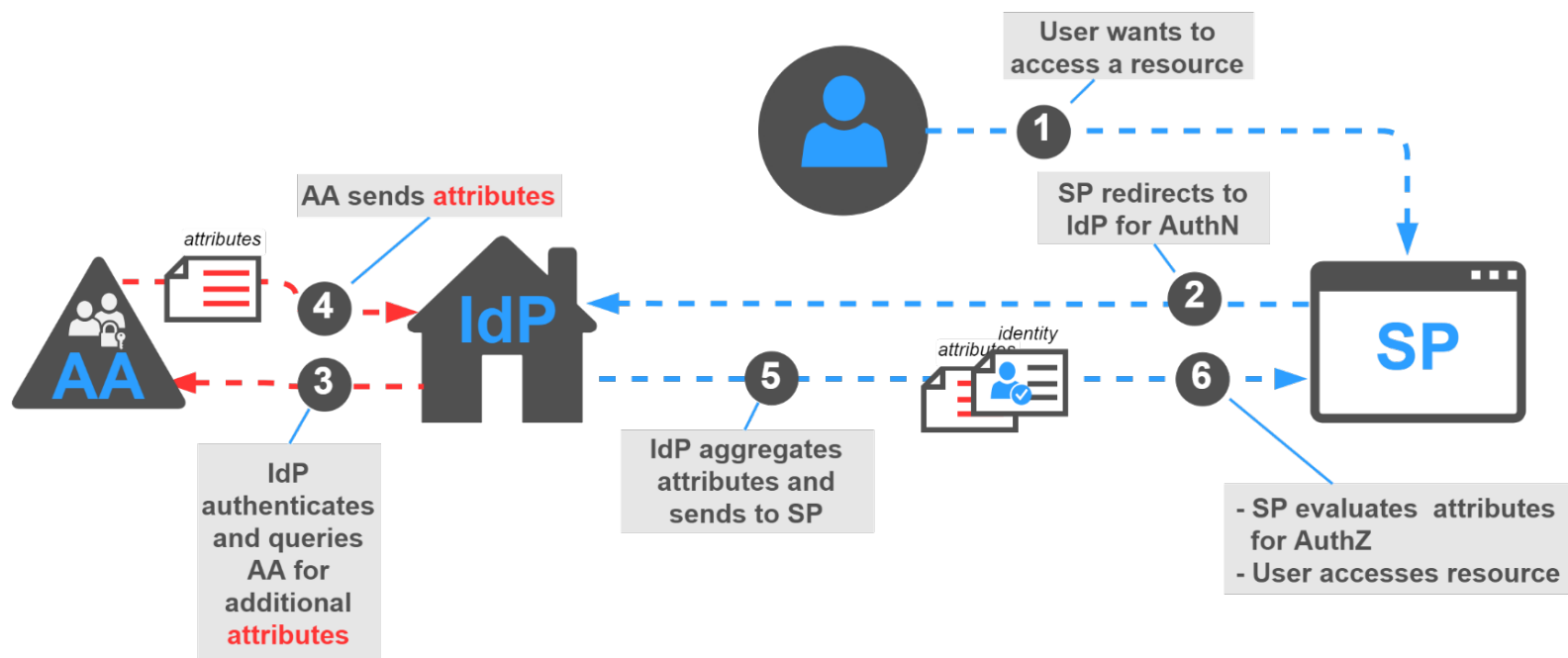
# I limiti dei modelli autoritativi

- Silos monolitici
  - Ogni servizio ha il suo mondo
  - DB locale come fonte autoritativa unica
- Modelli piatti, statici
  - Utente o admin
  - RBAC → ruoli & gruppi
  - ABAC → attributi utente



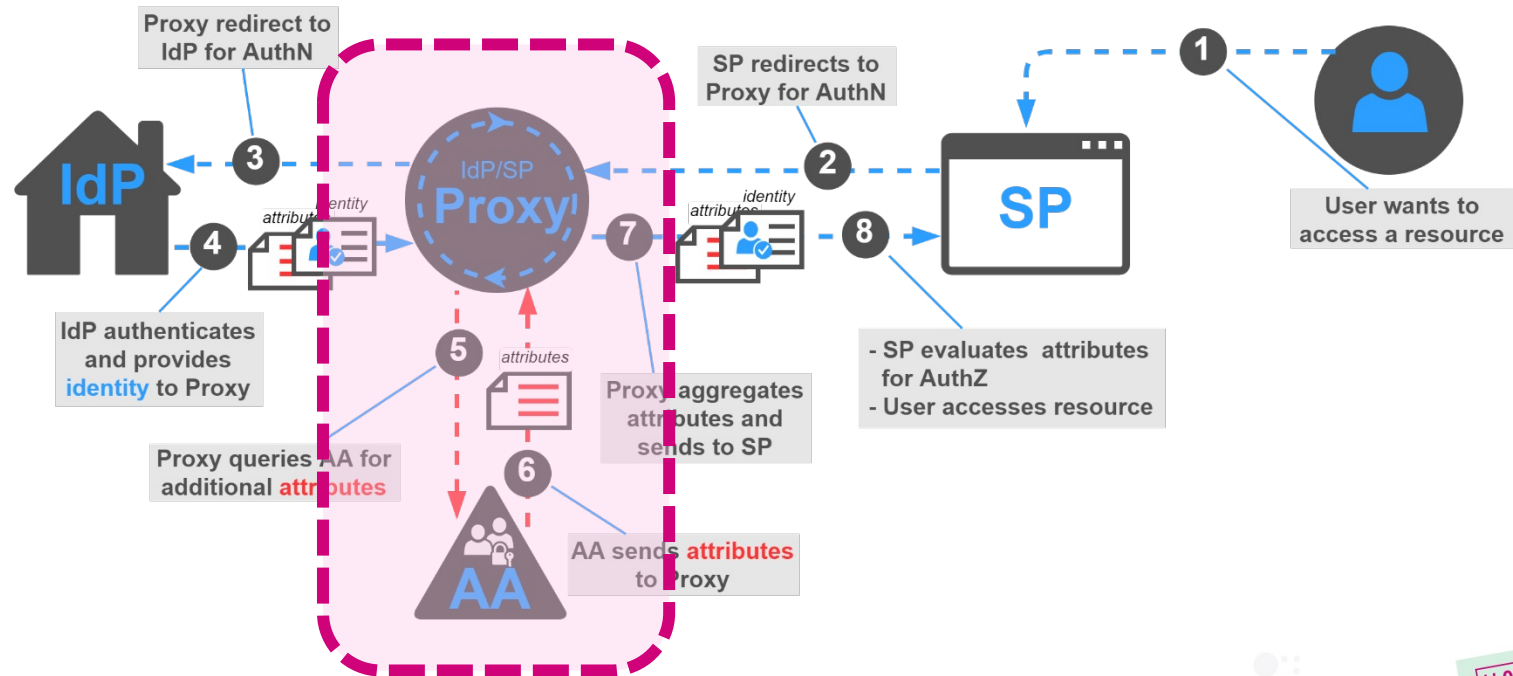
# Modelli distribuiti esistenti

- Gli IdP come fonte d'informazione autoritativa
  - Enforcement esterna
  - Limiti scalabilità e ruolo extra-specifica
  - Focus funzionale

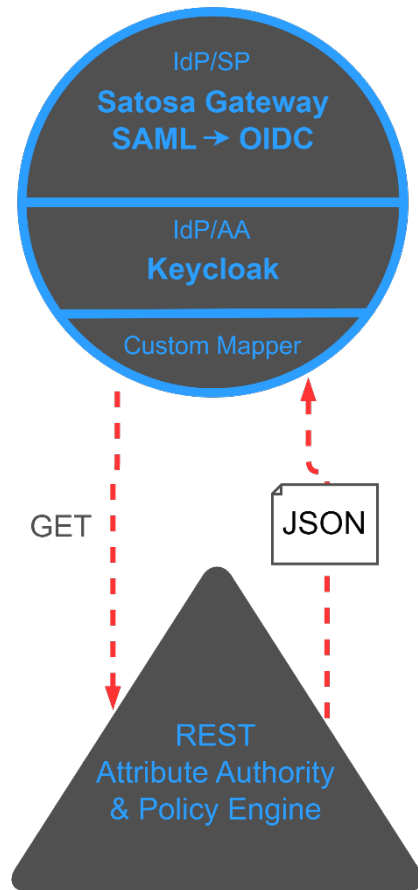


# L'autorizzazione che occorre in GARR-T

- Disaggregata, ruoli SP-IdP preservati
- Delega con gerarchia sub-admin
- Policy funzionali e non funzionali, valutate on-the-fly



# Il prototipo GARR, primi risultati



- **Satosa Gateway**

- Propagazione  
EduPersonPrincipalName  
EduPersonScopedAffiliation

- **Keycloak-Satosa in trust**

- Gruppi, ruoli, attributi per Client/Servizio
- Catene di autenticazione
- Mapper ad hoc per attributi dinamici

- **Verso Attribute Authority generalizzata**

- GET <http://<AA>/?servizio=...&userid=...>



# Lezione appresa e prossimi passi



www.shutterstock.com - 613586348

- Oltre i limiti dell'autorizzazione
  - Obiettivi definiti
  - Interoperabilità SAML e OIDC
  - Docker e Ansible per contenere complessità
- Portale GARR-T e Attribute Authority generalizzata
  - Delega e espressività policy (e sistema inferenza)
  - Semplicità d'uso criterio chiave
  - Modelli per servizi, gruppi, utenti
- Goal, feature disponibile entro WS 2023



# GRAZIE!

ACK a Davide Vagheti per i diagrammi su AAI Federata