THE ITALIAN RESEARCH & EDUCATION NETWORK | Consortium GARR

Una nuova infrastruttura di AA multiprotocollo (SAML e OIDC) per accedere ai servizi GARR Cloud… e non solo

Davide Vaghetti <davide.vaghetti@garr.it>

WORKSHOP GARR 2017 | Roma, 06/04/2017

Agenda

- Perché una nuova infrastruttura
- AARC Blueprint Architecture
- Workflow IdP, SP e IdP/SP Proxy con Attribute Authority
- Il caso d’uso della GARR Cloud
- Quali vantaggi?

Perché una nuova infrastruttura

Accesso a risorse federate tramite IdP esterni alla federazione e/o protocolli non SAML

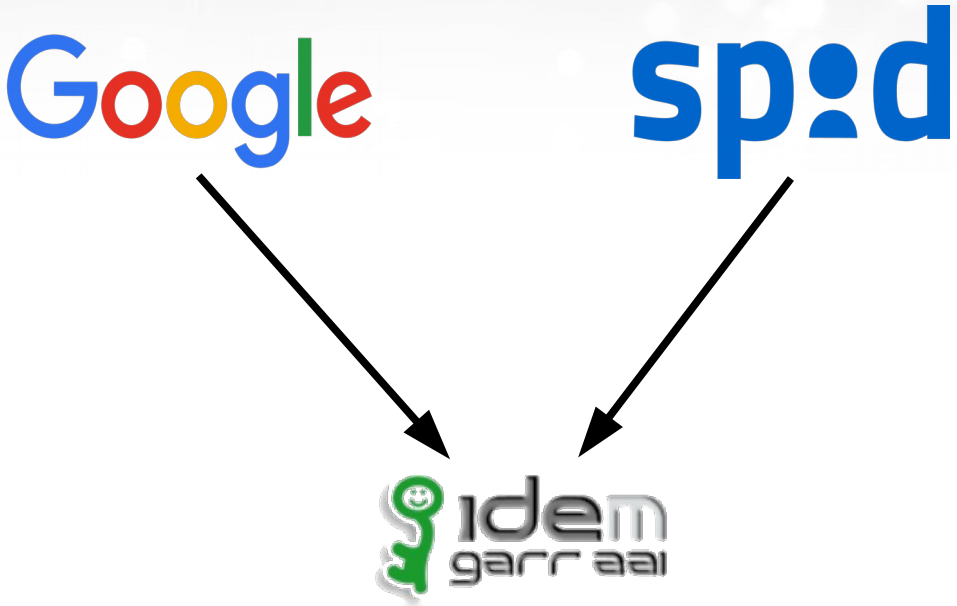
Supporto per Virtual Organization con utenti *misti*

Perché una nuova infrastruttura

Account Linking

mobilità utenti

upgrade relazione con ente

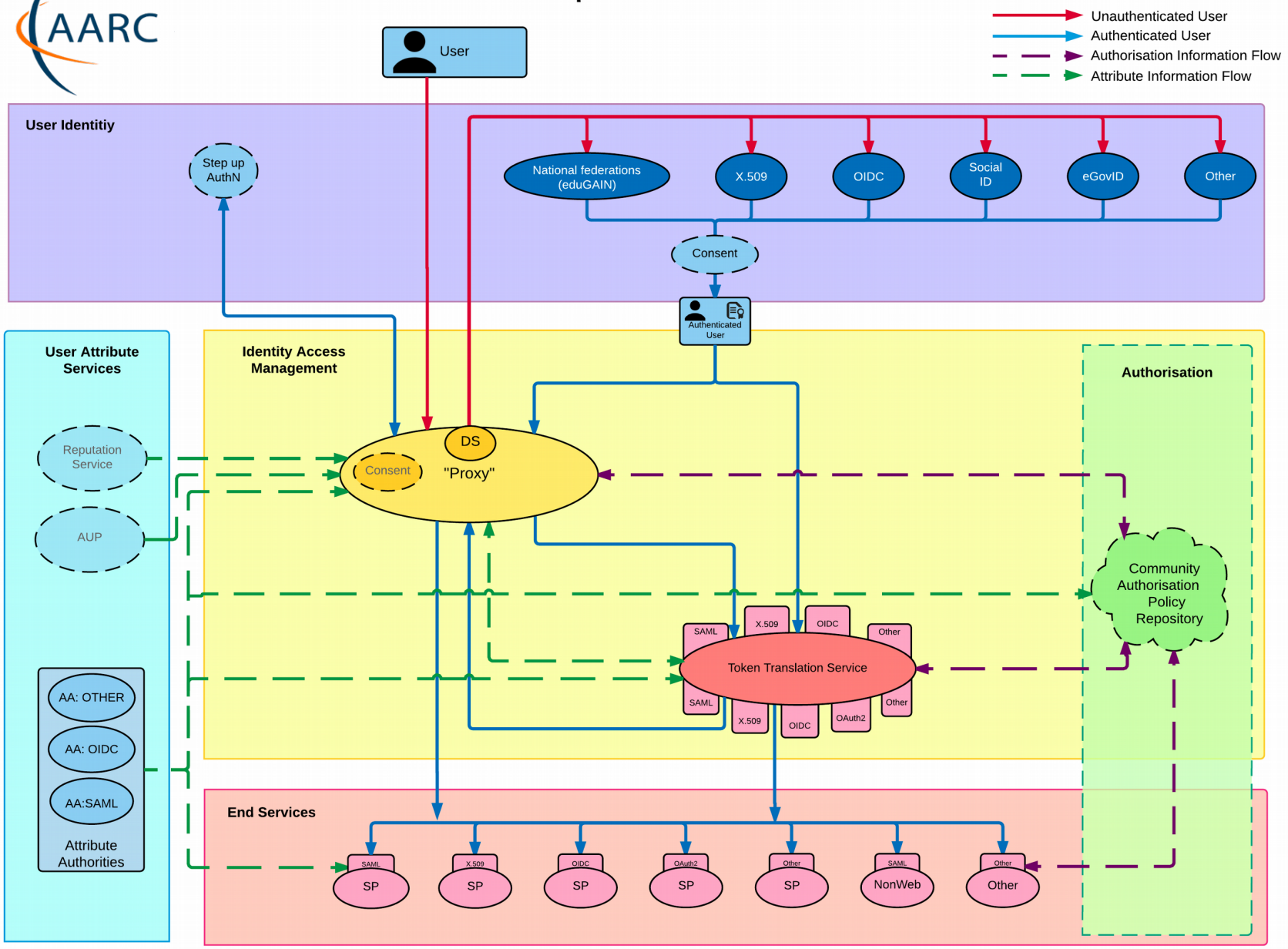


AuthZ Federata

Delega gestione autorizzazione

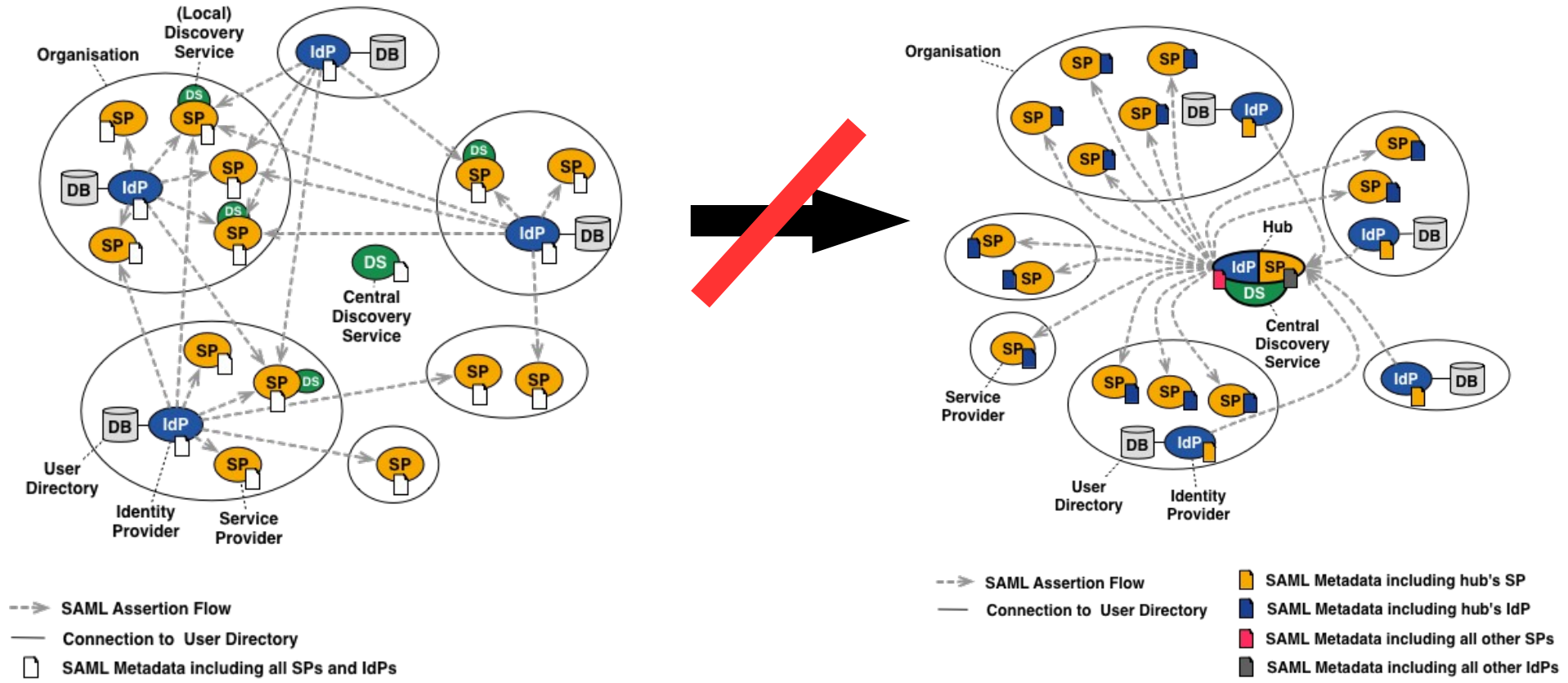
Riutilizzo gruppi e ruoli

AARC Blueprint Architecture

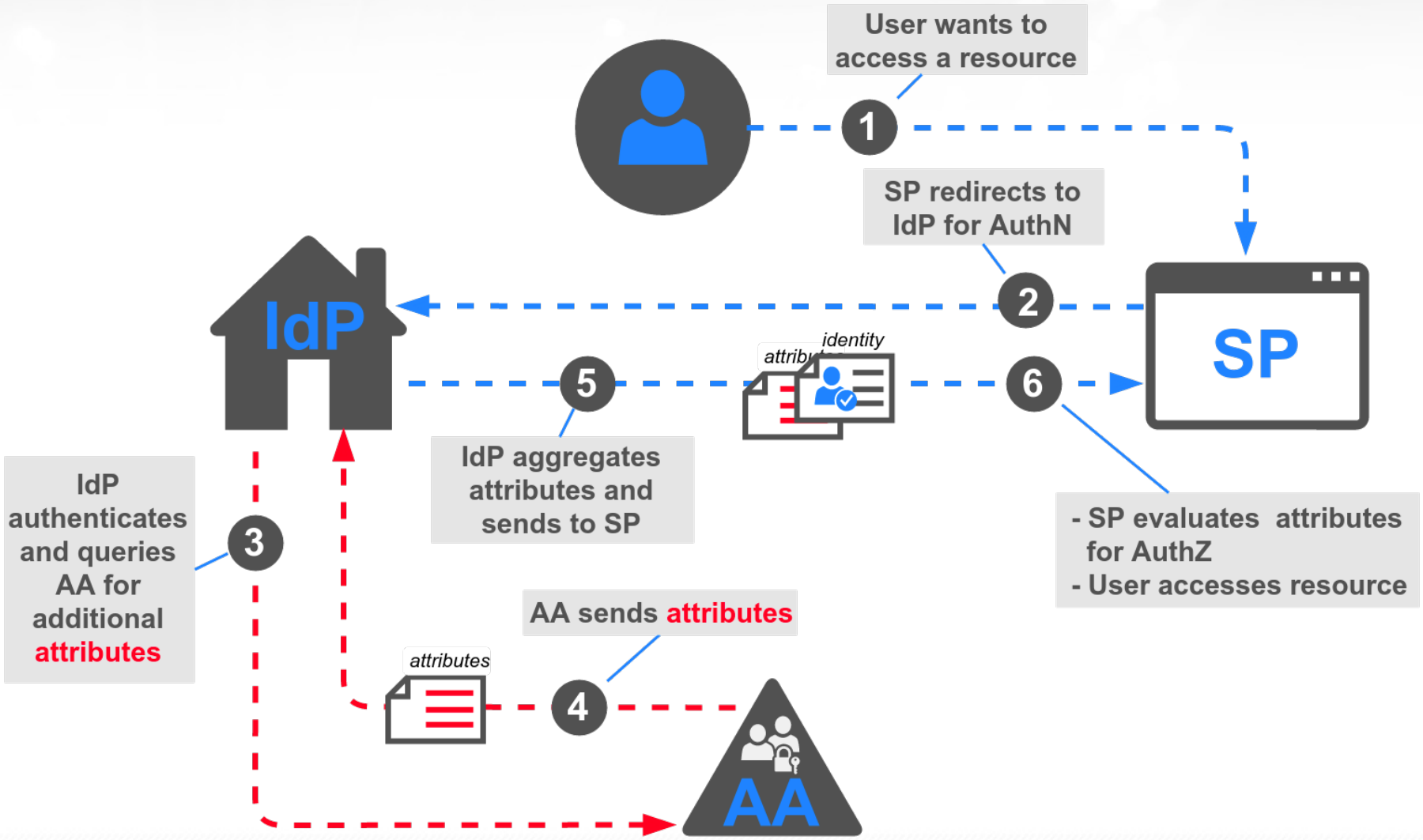


https://aarc-project.eu/

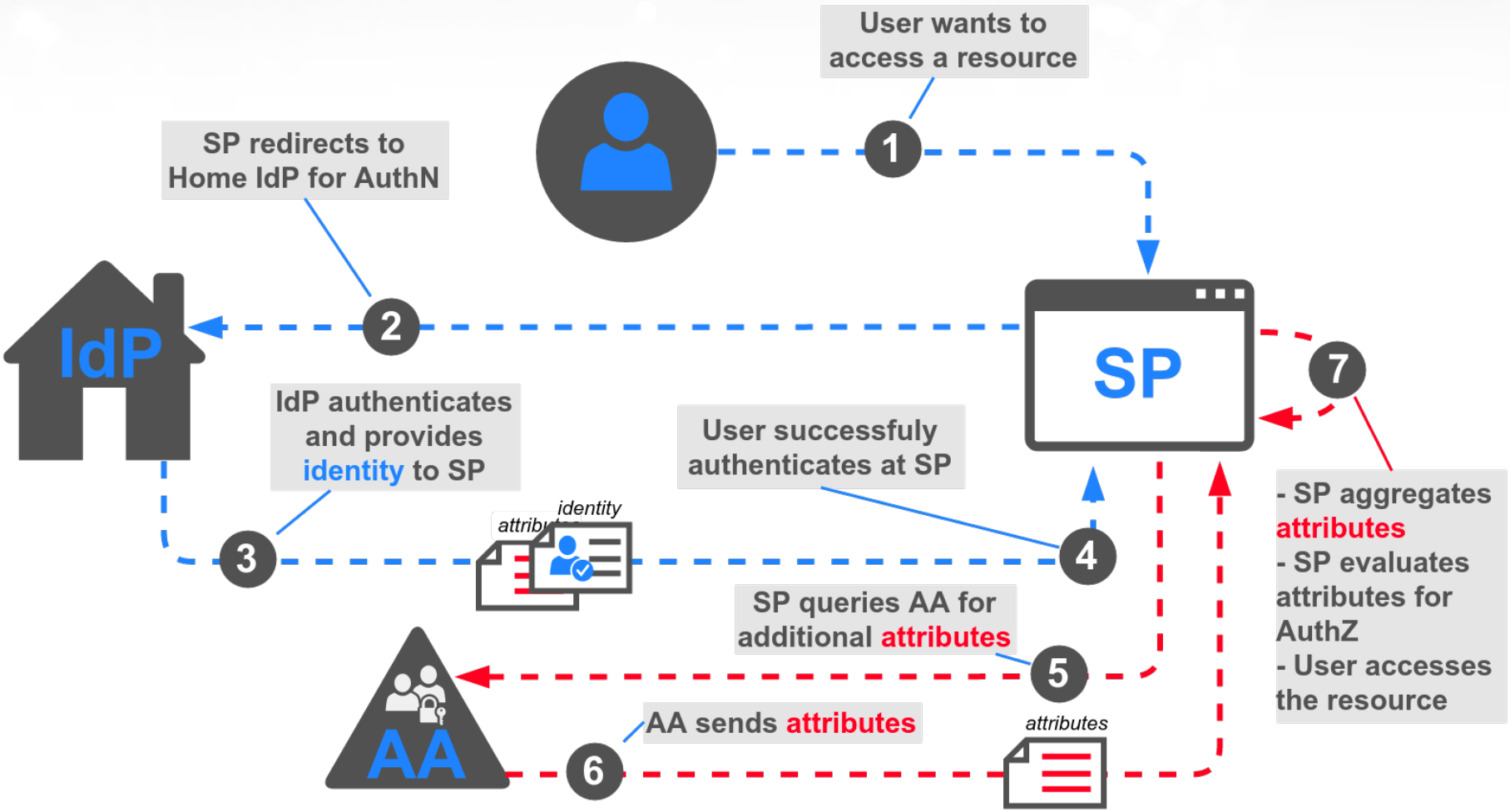
IDEM rimane una federazione Full Mesh!



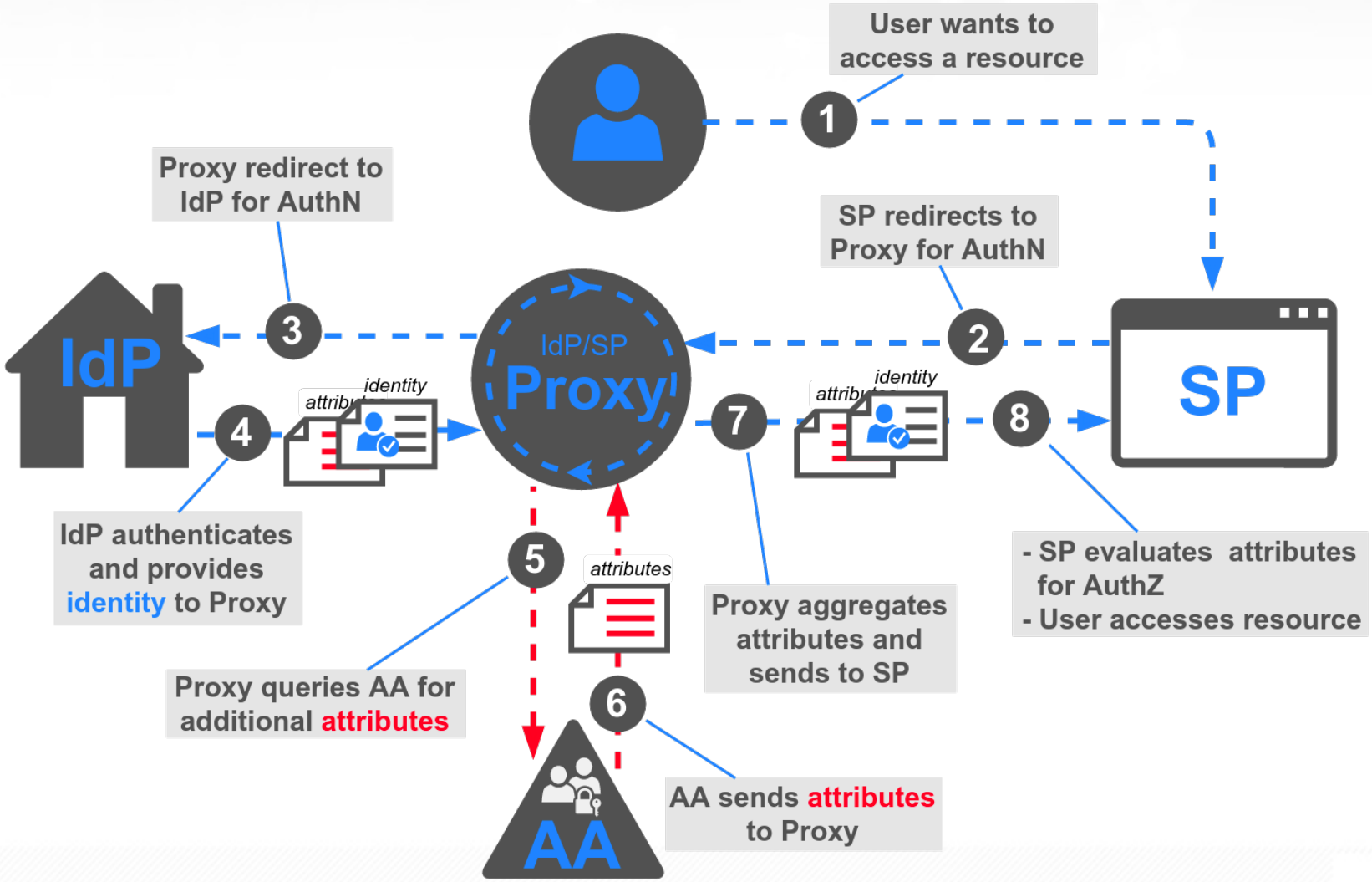
Accesso federato e Attribute Authority



Accesso federato e Attribute Authority

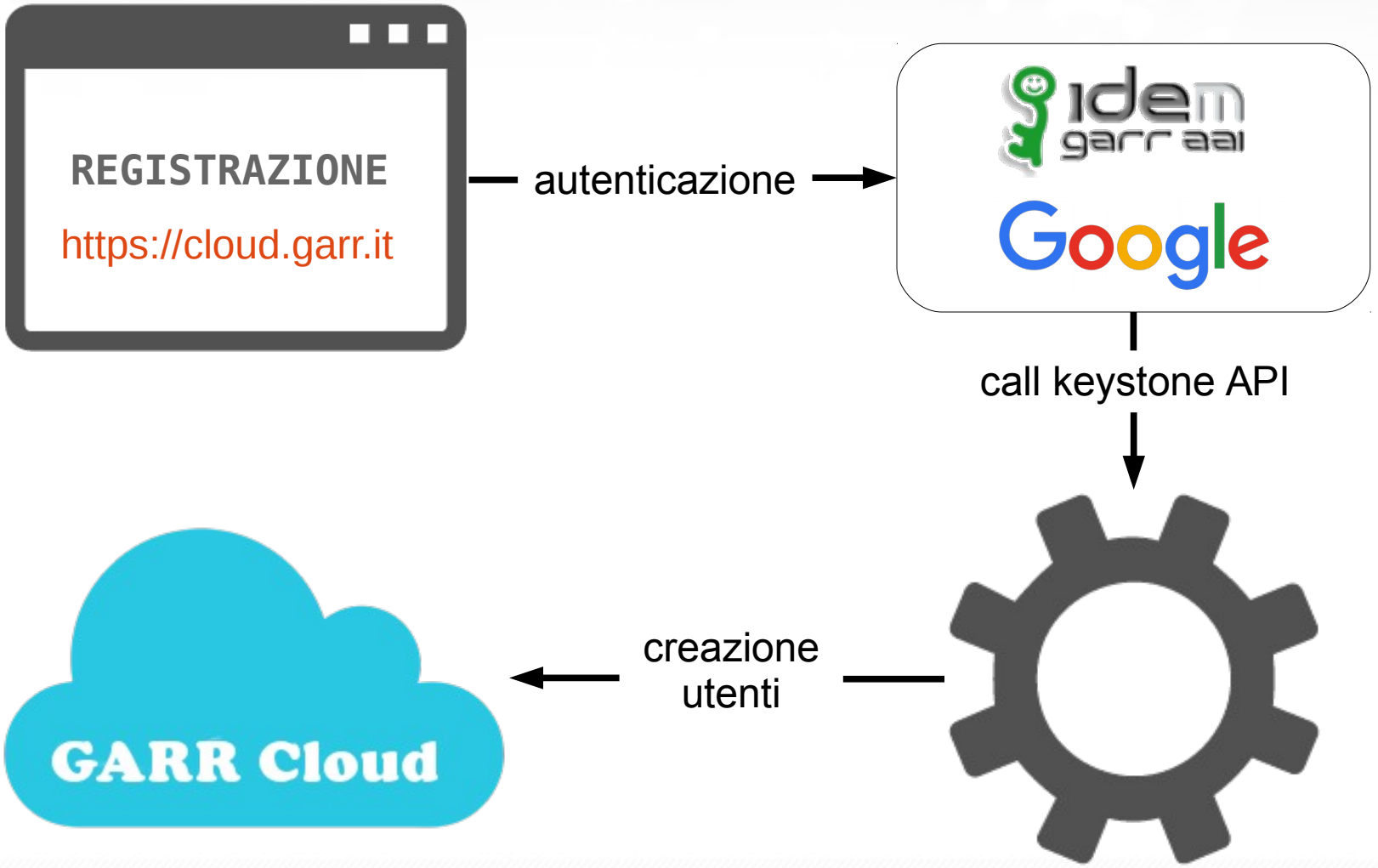


Accesso federato con IdP/SP Proxy e Attribute Authority

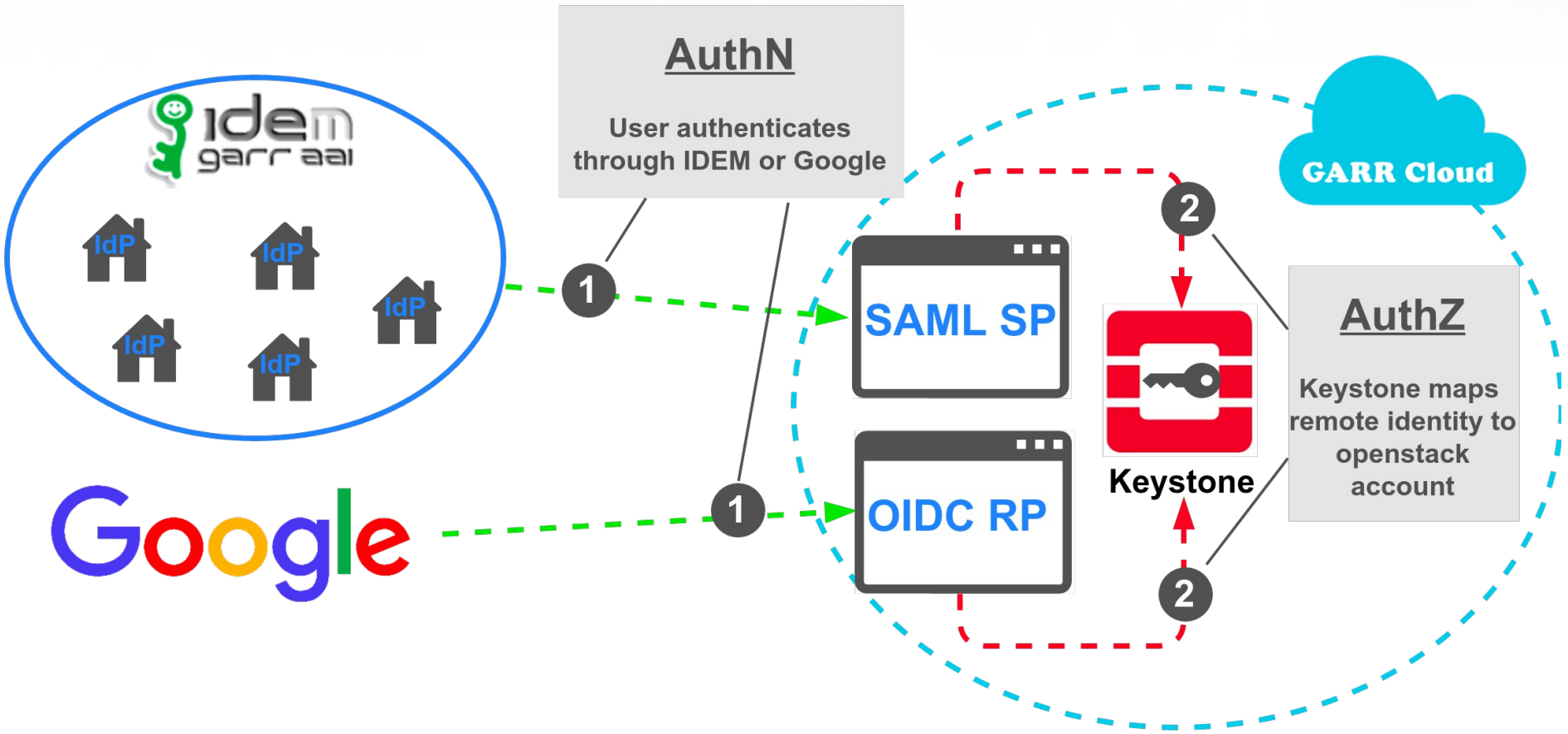


Un caso d’uso specifico

Provisioning utenti @GARR Cloud



AuthN e AuthZ @GARR Cloud



AuthN e AuthZ @GARR Cloud

PRO

- Veloce da implementare e Funziona!
- Architettura e Workflow semplici
- No single point of failure
- Coerenza: autorizzazione gestita via dashboard
- *Applicazione ad hoc per registrazione e provisioning utenti*

CONTRO

- Non espandibile verso altri protocolli e framework
- Non supporta ABAC/RBAC
- Non supporta delega AuthZ (no Policy Decision Point esterni)
- Applicazione ad hoc per registrazione e provisioning utenti, non riutilizzabile per altri servizi GARR

Riassumendo, quali vantaggi?

Per i servizi GARR

- Utilizzo di entitlements, ruoli e gruppi per AuthZ federata
- Delega della AuthZ ad admin dei servizi lato Home Organization

Per gli enti e le collaborazioni di ricerca

- Virtual Organization con utenti federati e non
- Level of Assurance basato su admin di gruppi
- Un’unica soluzione per tutti i servizi utilizzati dal gruppo di ricerca

Per le Home Organization:

- Account linking su IdP esterni semplifica mobilita e trasformazione delle relazioni tra utente ed ente

Grazie