THE ITALIAN RESEARCH & EDUCATION NETWORK | Consortium GARR

Nuove architetture per le Federazioni di Identità

Davide Vaghetti – GARR - <davide.vaghetti@garr.it>

WS GARR 2017 | Roma 05/04/2017

Agenda

Account Linking

Attribute Authority

Attribute Aggregation

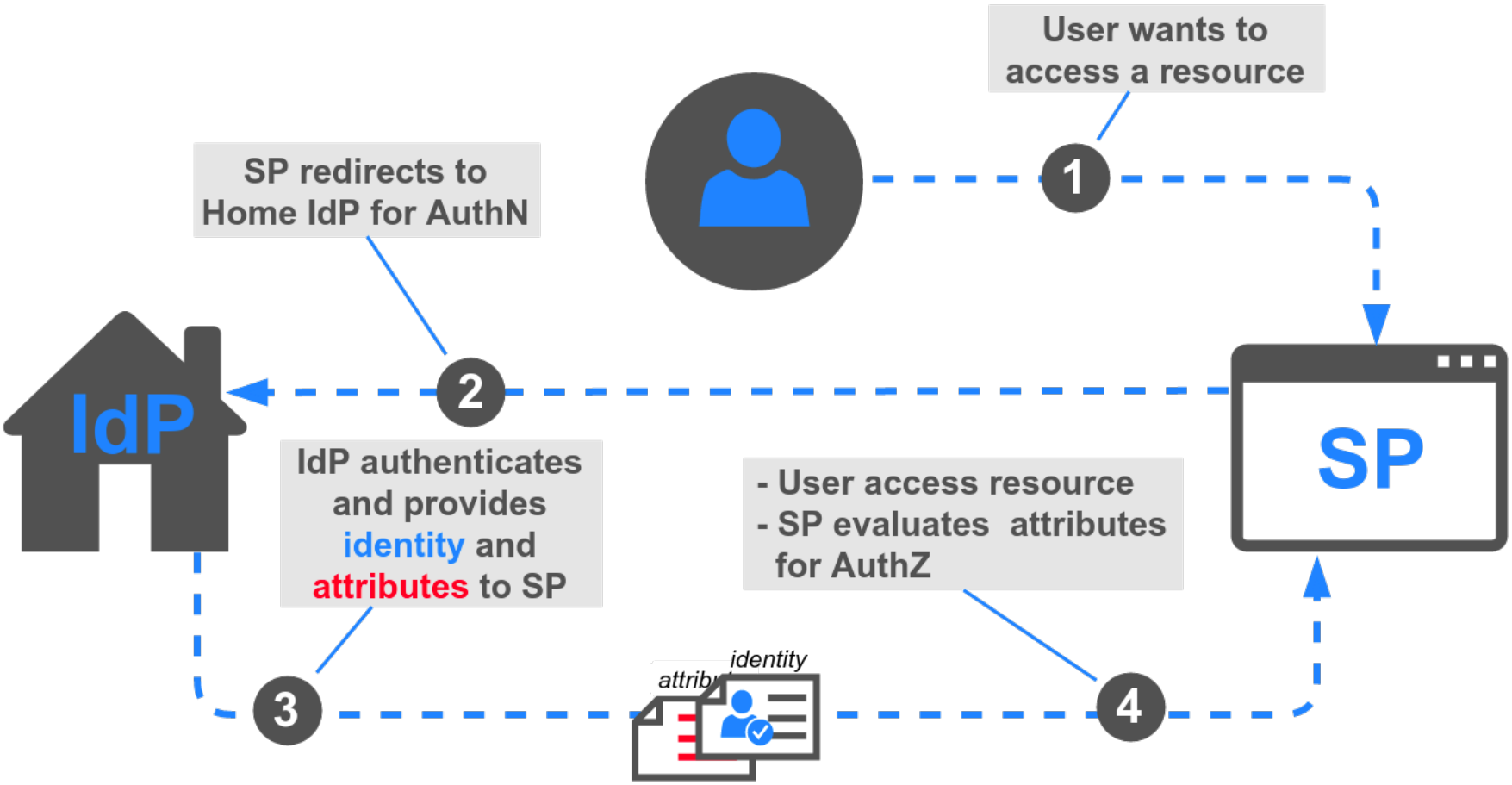
Token Translation

IdP/SP Proxy

Account Linking

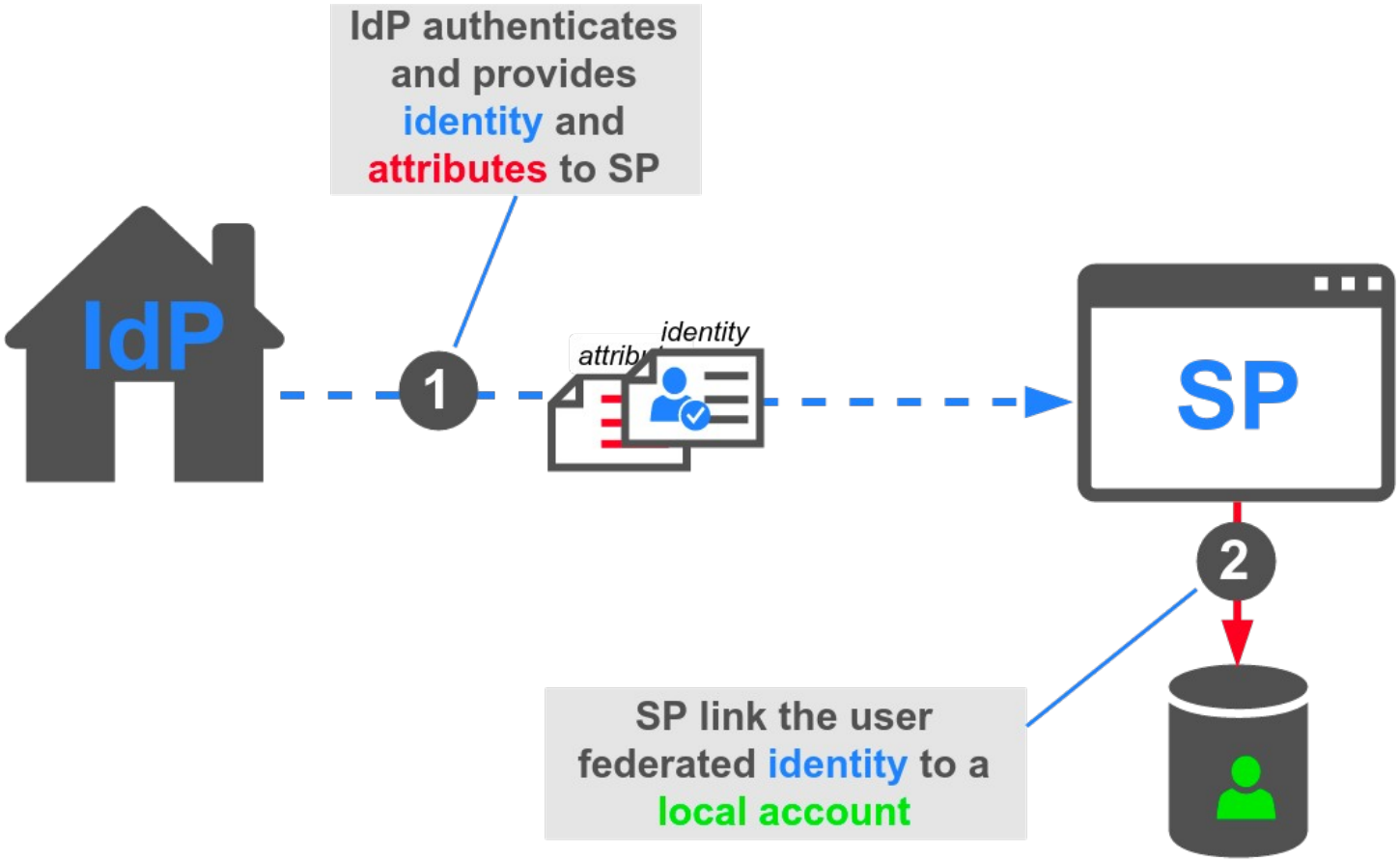
Account Linking

Accesso federato alle risorse



Account Linking

Associare due account provenienti da differenti sistemi



Account Linking

Come avviene l'associazione tra identita' federata e account locale

saml-core-2.0-os

[…] persistent identifiers are typically used to reflect an account linking relationship between a pair of providers […]

Account Linking

Identificatori e Attributi

Identifier / Attribute	Persistent	Revocable	Reassignable	Opaque	Targeted	Portable	Global	Qualifier
SAML2 Transient NameID	No	N/A	N/A	Yes	N/A	N/A	Yes	N/A
SAML2 Persistent NameID	Yes	Yes	No	Yes	Yes	Yes	No	Issuer ID
eduPersonTargetedID	Yes	Yes	No	Yes	Yes	Yes	No	Issuer ID
eduPersonPrincipalName	Yes	Yes	Yes	No	No	No	Yes	Scoped
eduPersonUniqueId	Yes	Yes	No	Yes	No	No	Yes	Scoped
Social Security Number	Yes	No	N/A	No	No	Yes	No	US Citizens
Phone Number	Yes	Yes	Yes	No	No	No	Yes	N/A
OIDC public sub claim	Yes	Yes	No	Yes	No	No	No	Issuer ID
OIDC pairwise sub claim	Yes	Yes	No	Yes	Yes	No	No	Issuer ID
ORCID	Yes	Yes	No	Yes	No	Yes	Yes	N/A

https://wiki.shibboleth.net/confluence/display/CONCEPT/NameIdentifiers

Account Linking

Identificatori e Attributi persistenti

SAML Persistent NameID

formato: vedi eduPersonTargetedID

eduPersonTargetedID

formato: <issuer> | <opaque-local-unique-id> | <target>

eduPersonPrincipalName

formato: <principal>@<scope>

eduPersonUniqueID

formato: <UUID>@<scope>

Account Linking

Identificatori e Attributi persistenti

...e globali (non targeted)

~~**SAML Persistent NameID**~~

~~formato: vedi eduPersonTargetedID~~

~~**eduPersonTargetedID**~~

~~formato: <issuer> | <opaque-local-unique-id> | <target>~~

eduPersonPrincipalName

formato: <principal>@<scope>

eduPersonUniqueID

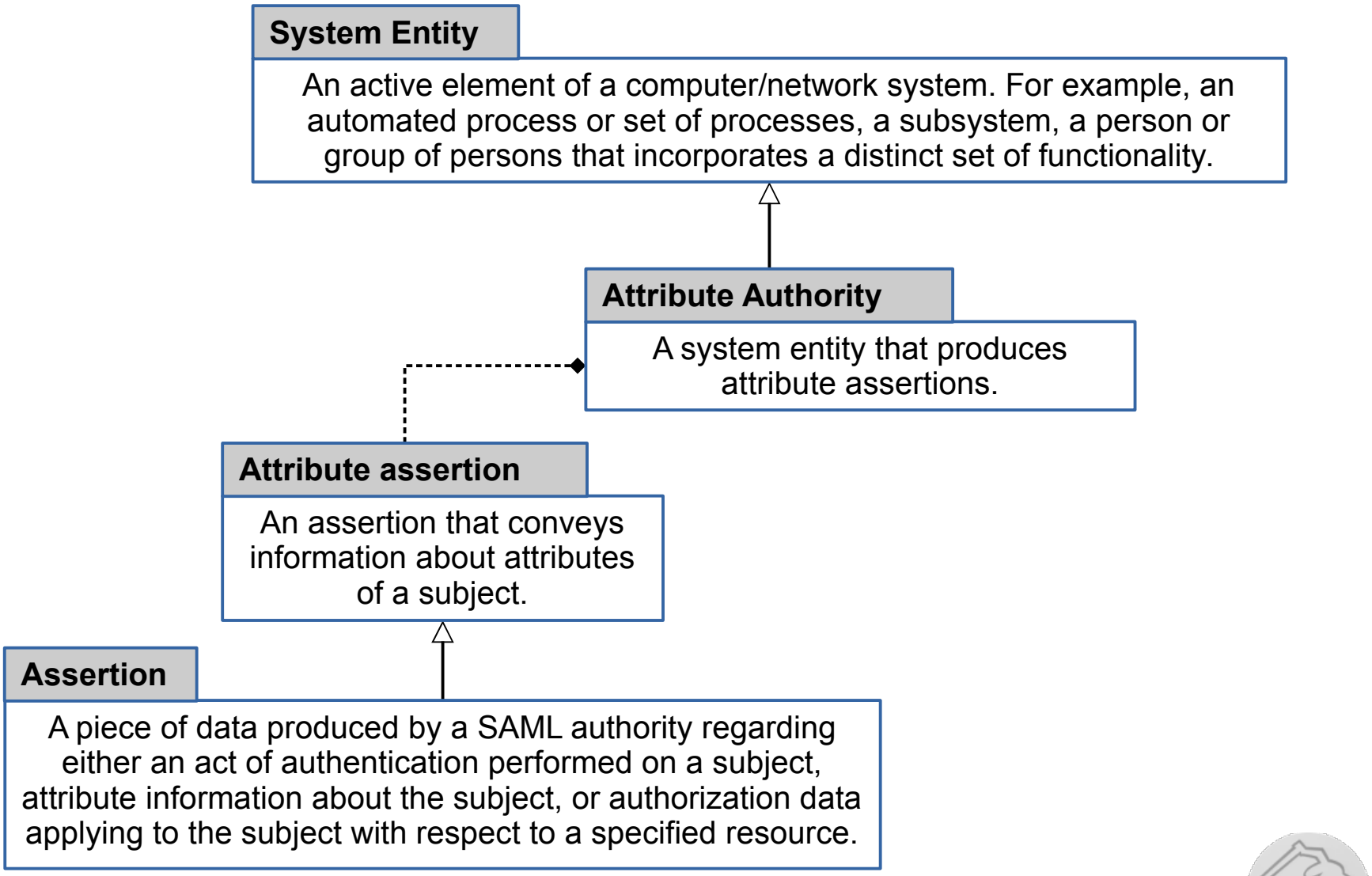
formato: <UUID>@<scope>

Account Linking

IdP esterni

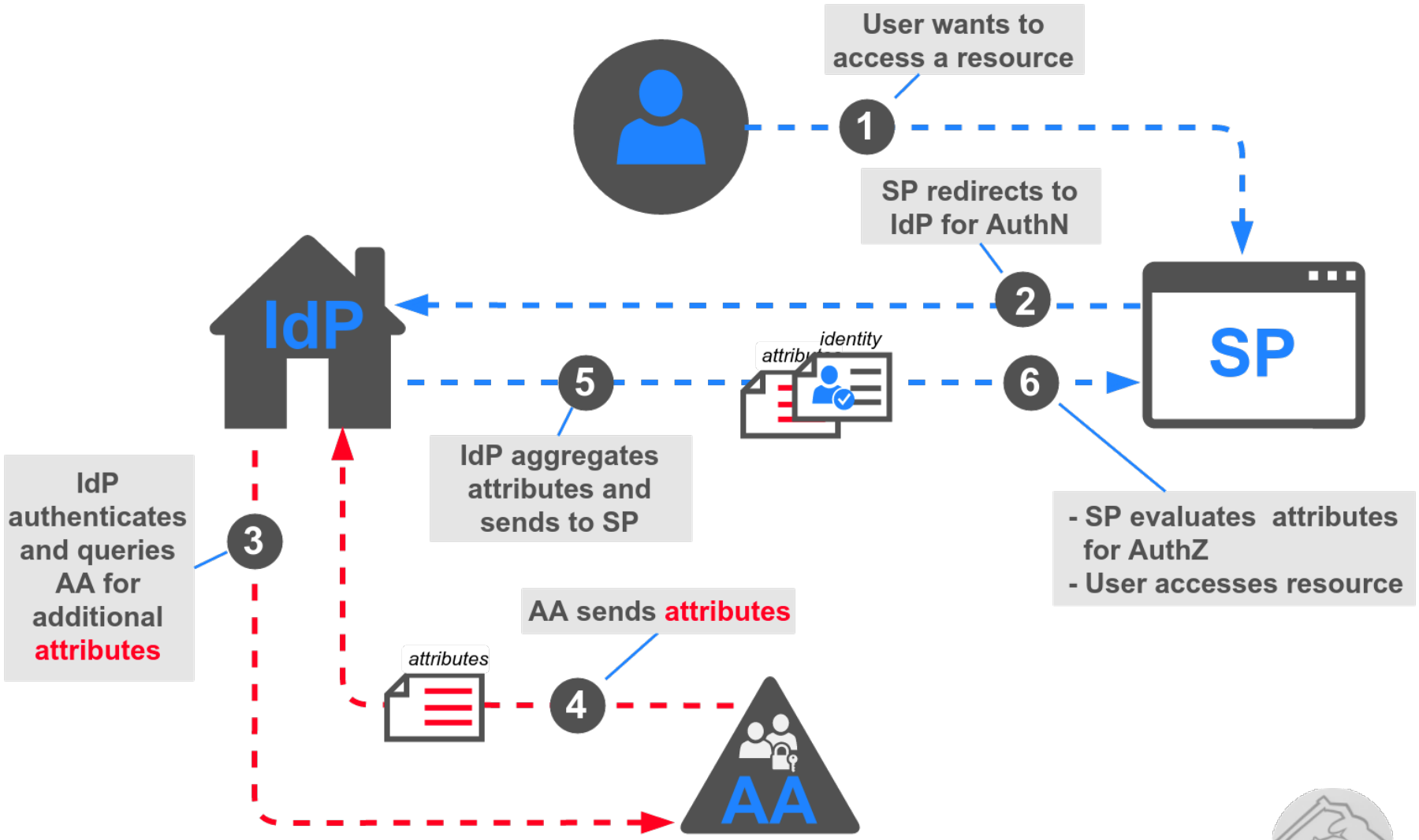
Attribute Authority

Attribute Authority



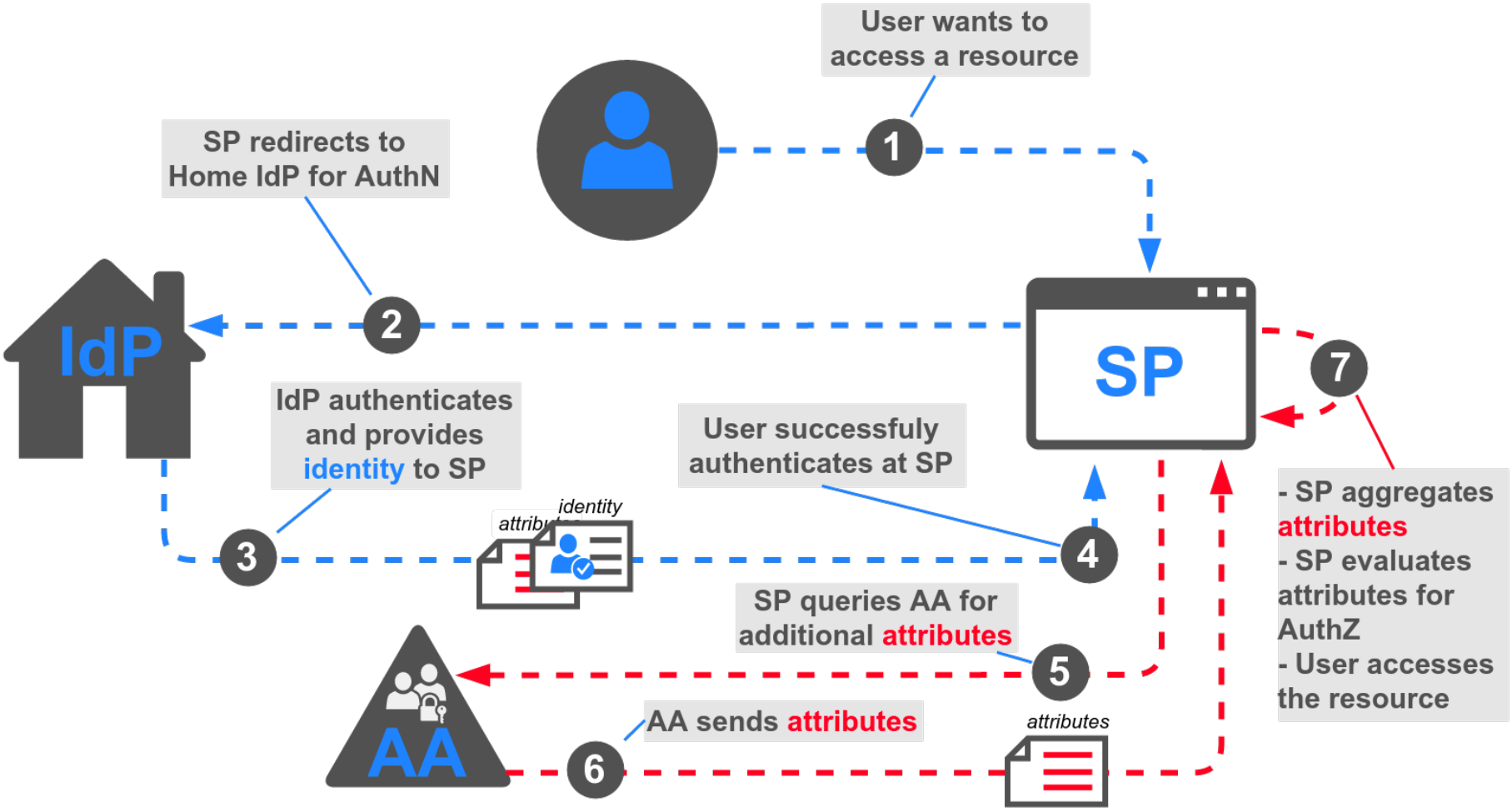
Attribute Authority

Un IdP chiede attributi addizionali ad un Attribute Authority



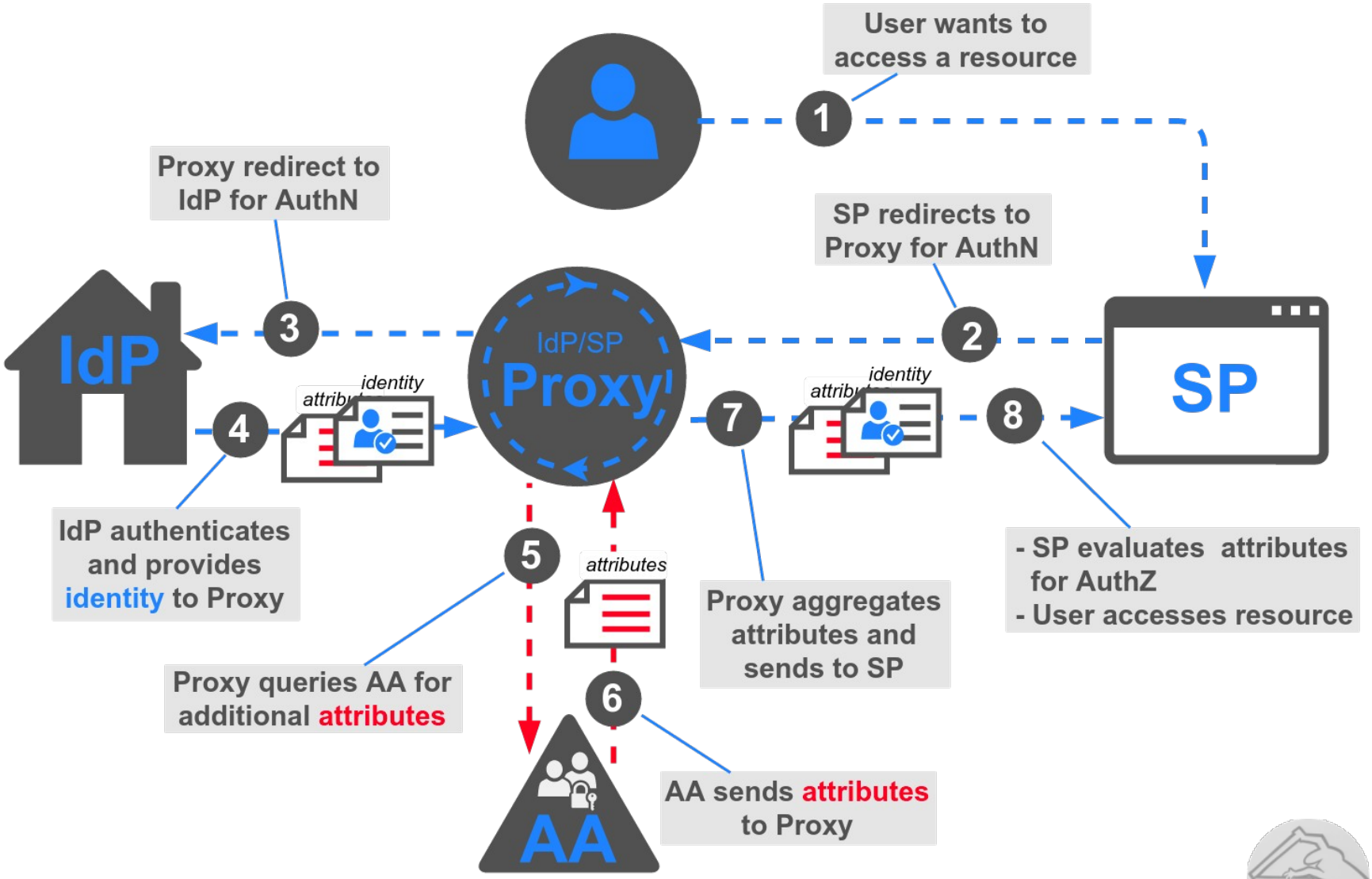
Attribute Authority

Un SP chiede attributi addizionali all'Attribute Authority



Attribute Authority

Un IdP/SP Proxy richiede attributi addizionali ad una Attribute Authority



©CAVA/QUIPOS

Attribute Aggregation

Attribute Aggregation

SimpleAggregation in Shibboleth Service Provider

```
<!-- Uses eduPersonPrincipalName from IdP to query, and asks for
eduPersonEntitlement. -->
<AttributeResolver type="SimpleAggregation" attributeId="eppn"
format="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">
    <Entity>https://ieee.org/idp/shibboleth</Entity>
    <EntityReference>External-Links</EntityReference>
    <saml2:Attribute
        xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        FriendlyName="eduPersonEntitlement"/>
</AttributeResolver>
```

Attribute Aggregation

Alcuni problemi aperti

Attribute scoped

chi è autoritativo?

Logica di aggregazione

default concatenzazione con “,”

Mantenimento del referral

uno standard condiviso è mancante

Una soluzione per tutte: spostare la logica di aggregazione dal Service Provider (o Identity Provider) ad uno strato applicativo

Token Translation

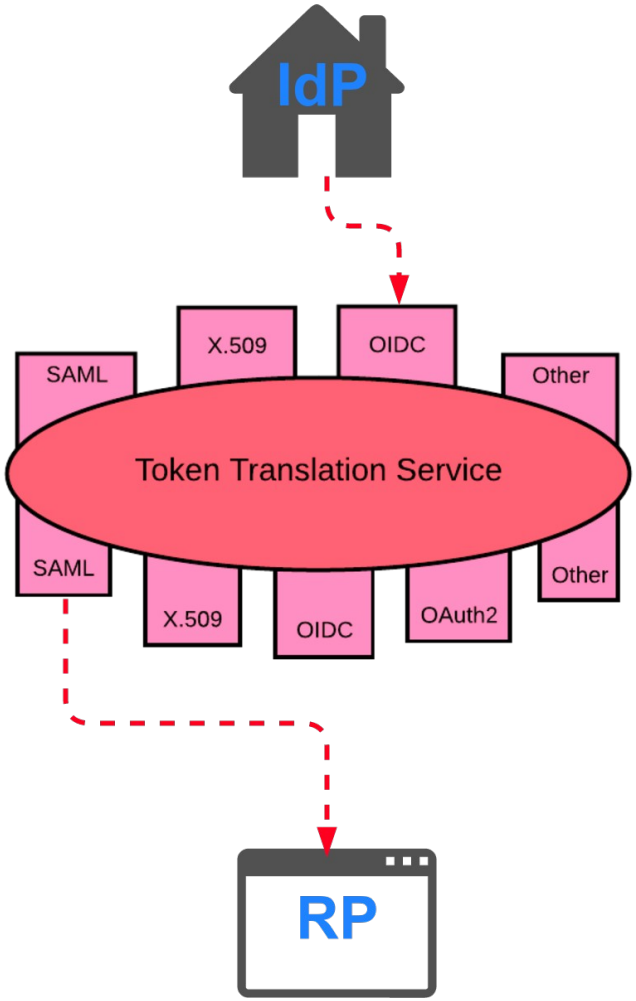
Token Translation

Perché è necessario un servizio di token translation

Ambiente	Autenticazione	Standard
Federazioni di Identità	SAML	SAML2Int
GRID – Comunità della ricerca	X509	IGTF/IETF
eGOV	SAML, OIDC	Custom
Provider Commerciali	OAuth2, OIDC, SAML	Custom

Token Translation

Da OIDC Provider a SAML Service Provider (o Resource Provider)



Token Translation

Traduzione degli attributi

SAML	Google / OIDC	Facebook	LinkedIn
ePUID	sub + issuer	n/a	n/a
ePPN	n/a	third_party_id	n/a
SAML2 Persistent Name ID/ePTID	n/a	id	id
displayName	name	name	formatted-name
givenName	given_name	fist_name	first-name
sn	family_name	last_name	last-name
mail	email	email	email-address

IdP/SP Proxy

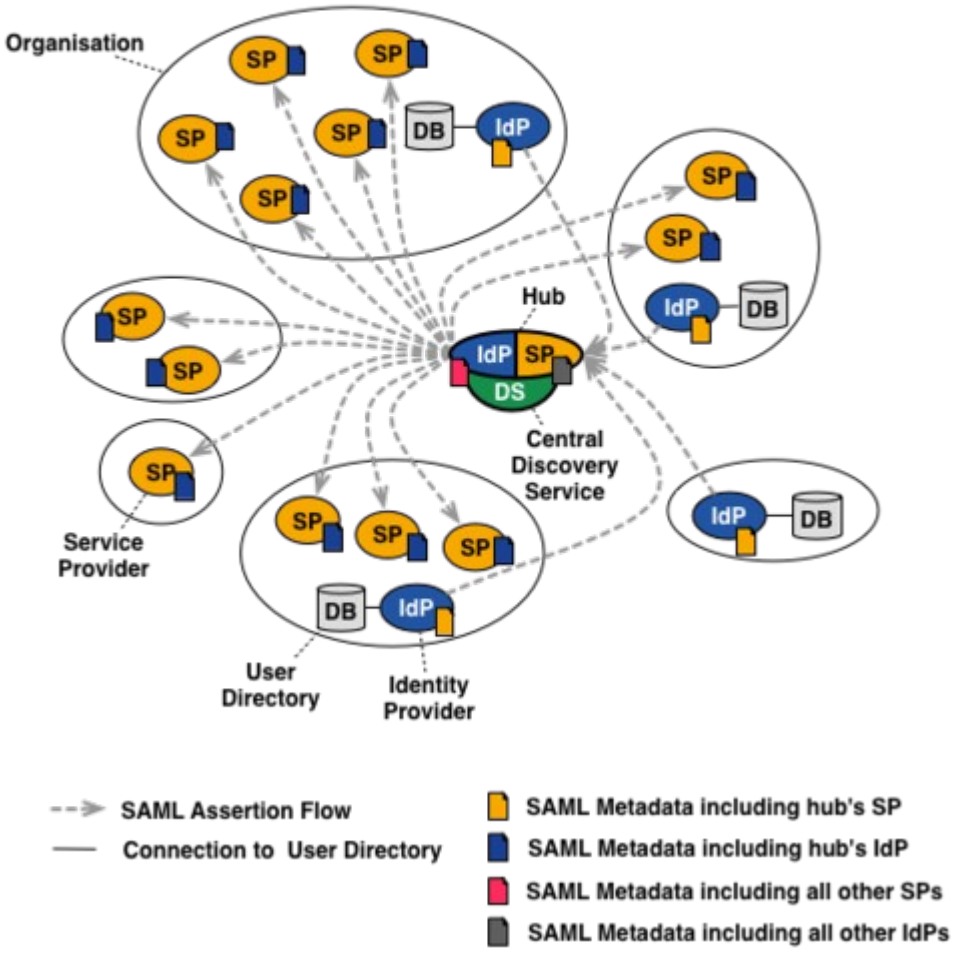
IdP/SP Proxy

Caratteristiche:

- Per gli utenti è un Service Provider
- Utilizza i normali meccanismi di discovery per la scelta del Identity Provider
- È un Identity Provider che utilizza il Service Provider interno come fonte di autenticazione

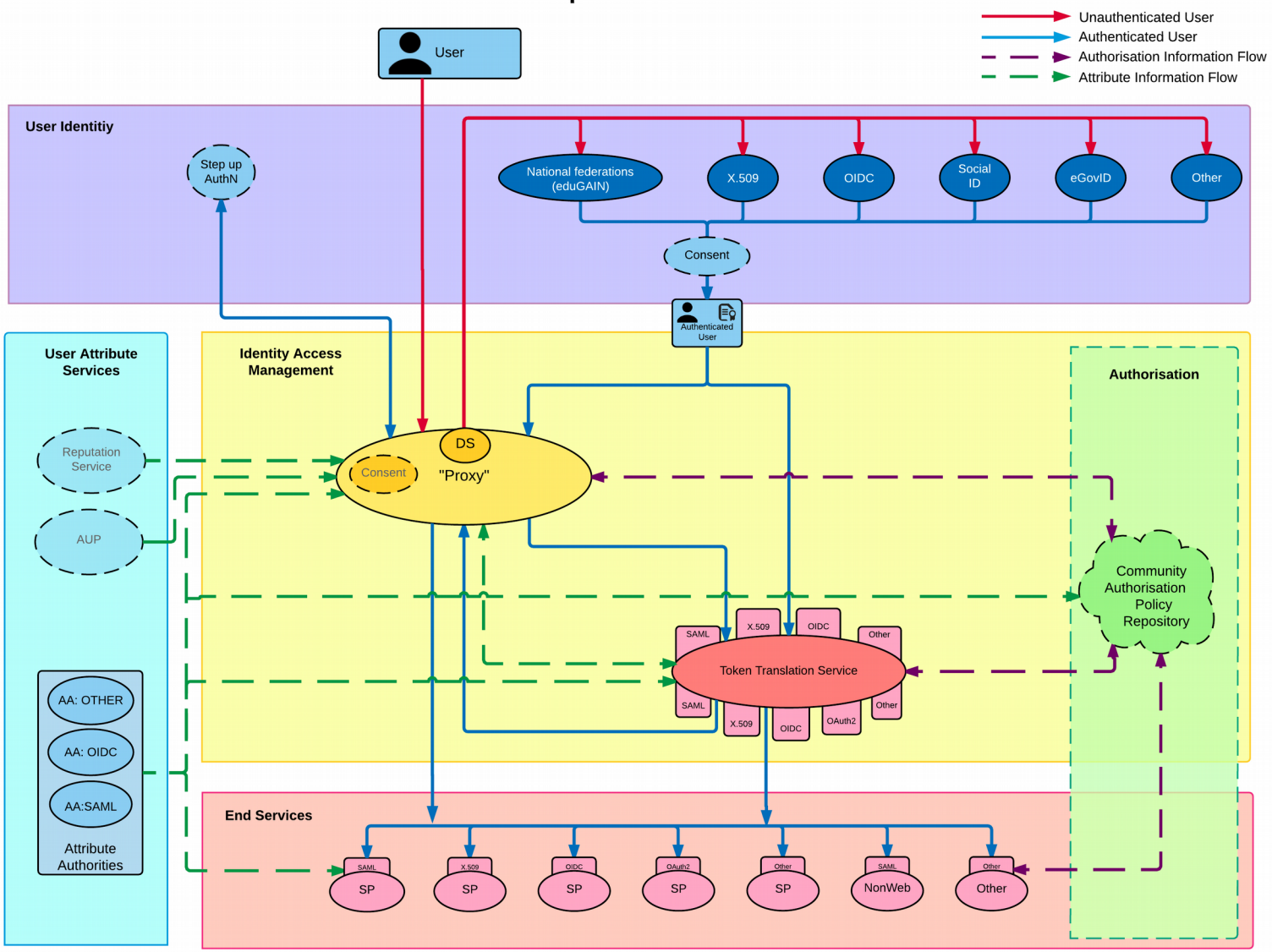
IdP/SP Proxy

IdP/SP Proxy nelle federazioni Hub and Spoke



AARC Authentication and Authorisation for Research and Collaboration

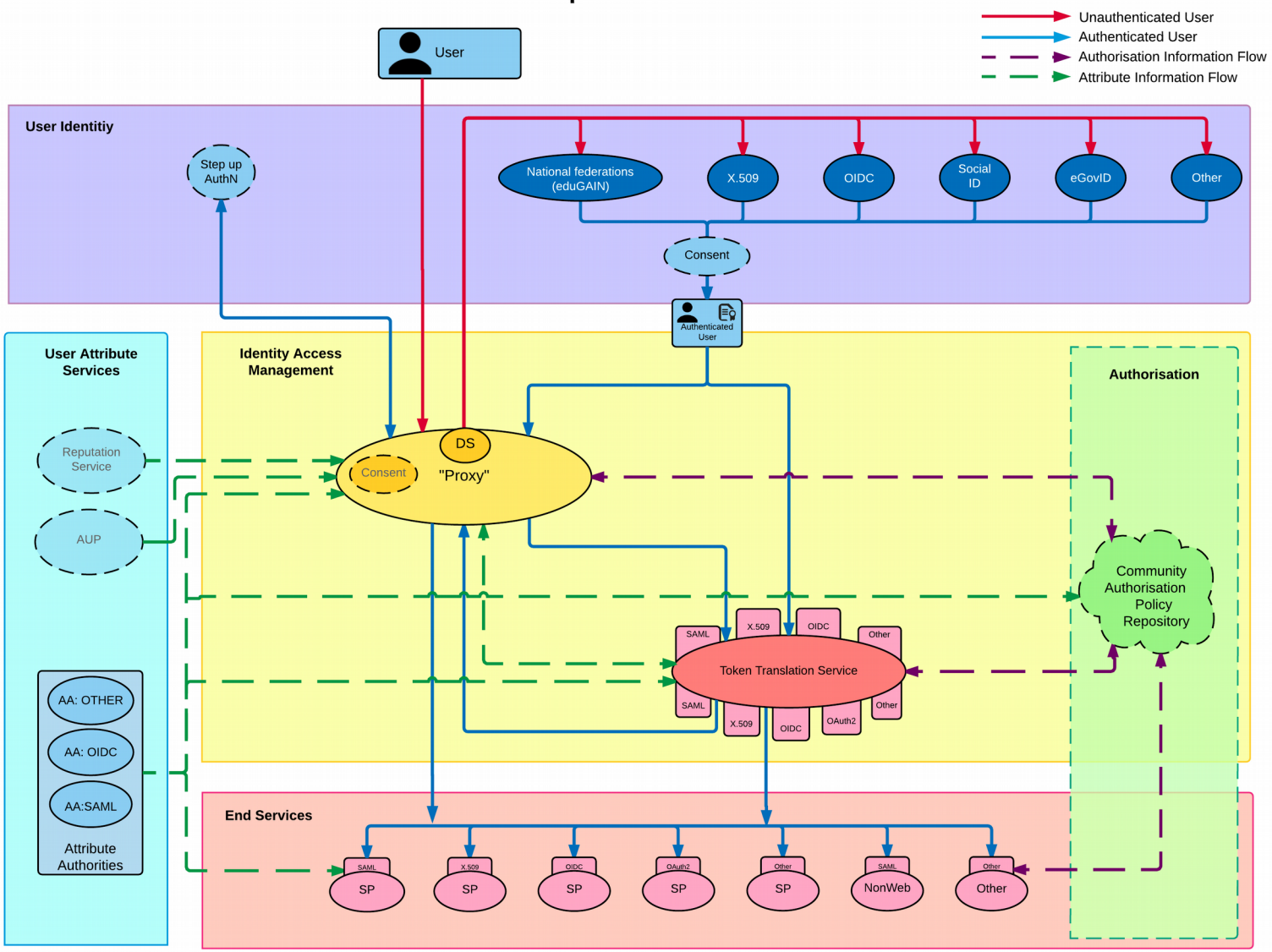
AARC Blueprint Architecture



https://aarc-project.eu/

AARC Authentication and Authorisation for Research and Collaboration

AARC Blueprint Architecture



https://aarc-project.eu/