IDEM e le AAI per le infrastrutture di ricerca

Davide Vaghetti – davide.vaghetti@garr.it
Coordinatore Comitato Tecnico Scientifico Federazione IDEM - GARR

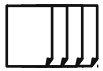
AAI: IDEM e eduGAIN

Infrastrutture di Autenticazione e Autorizzazione basate su SAML

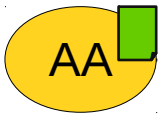
Identità delle organizzazioni di appartenenza

Web-SSO

Nuovi servizi = Nuovi Service Provider



Rilascio attributi basato su accordi e/o EC



Attribute Authority direttamente collegate a SP

Davide Vaghetti – davide.vaghetti@garr.it

Infrastrutture di ricerca

EUDAT 3rd Conference: What's on the Horizon?, 24-25 September 2014
Kimmo Koski, Managing Director CSC - IT Center for Science, Finland & EUDAT Co-ordinator

Davide Vaghetti – davide.vaghetti@garr.it

IDEM AAI e ricerca

La Federazione IDEM supporta pienamente tutti i casi d'uso della comunità della ricerca?

Zak McKracken and the Alien Mindbenders, Lucasfilm Games, 1988

Davide Vaghetti – davide.vaghetti@garr.it

Requisiti delle comunità della ricerca

Deliverable DJRA1.1:
Analysis of user community and service provider requirements
https://aarc-project.eu/wp-content/uploads/2015/10/AARC-DJRA1.1.pdf

Analisi basata su interviste a comunità della ricerca

Risultati:

- Guest Identities / Levels of Assurance
- User Identification
- Attributes: Groups and Authorisation
- Attributes: Release
- Technology requirements
- Privacy, legal issues, and policies
- Training

Davide Vaghetti – davide.vaghetti@garr.it

Requisiti: analisi comparativa

Guest Identities / Levels of Assurance		
Requisito	**IDEM**	**eduGAIN**
“Homeless” Users	NO	SI
Social media identities	NO	NO
Different Levels of Assurance	NO	DIPENDE DALLE FEDERAZIONI
Step up authentication	SI	SI
Integration with e-Government infrastructures	...ci stiamo lavorando!	...work in progress

Davide Vaghetti – davide.vaghetti@garr.it

Requisiti: analisi comparativa

User Identities		
Requisito	**IDEM**	**eduGAIN**
Unique user identities	SI	SI
Persistent User Identifiers	SI (quasi...)	IN PARTE
User-managed identity information	NO (dipendente da IdP)	NO (vedi IDEM)

Davide Vaghetti – davide.vaghetti@garr.it

Requisiti: analisi comparativa

Attributes: Groups and Authorisation		
Requisito	**IDEM**	**eduGAIN**
User groups and roles	SI	NO
Flexible and scalable attribute release policies	IN PARTE con Entity Categories	IN PARTE con Entity Categories
Community based authorisation	SI (ad es. grouper GARR IDEM)	DIPENDE DALLE FEDERAZIONI
Semantically harmonized identity attributes	SI	SOLO IN PARTE

Davide Vaghetti – davide.vaghetti@garr.it

Requisiti: analisi comparativa

Attributes: Release		
Requisito	**IDEM**	**eduGAIN**
Sufficient Attribute release	SI con Entity Categories	SI con Entity Categories
Attribute Aggregation / Account Linking	NO (proxy/AP di federazione)	NO

Davide Vaghetti – davide.vaghetti@garr.it

Requisiti: analisi comparativa

Technology requirements		
Requisito	**IDEM**	**eduGAIN**
Federation solutions based on open and standards based technologies	SI	SI
Browser and non-browser based federated access	NO	NO
Delegation	NO	NO

Davide Vaghetti – davide.vaghetti@garr.it

Requisiti: analisi comparativa

Privacy, legal issues, and policies		
Requisito	**IDEM**	**eduGAIN**
Federated Incident report Handling	SI	https://refeds.org/SIRTFI (Security Incident Response Trust Framework for Federated Identity)
Effective Accounting	SI	Dipendente da Federazioni
Up to date identity information	SI	Dipendente da Federazioni
Policy Harmonization	SI	SI (REFEDS, MACE-DIR, SCHAC)
Best practices for terms and conditions (Service Providers)	SI	SI (REFEDS)

Davide Vaghetti – davide.vaghetti@garr.it

Requisiti: analisi comparativa

Training		
Requisito	**IDEM**	**eduGAIN**
Awareness about R&E Federations	SI	SI
Simplified process for joining identity federation	NO	NO
User and Service Provider friendliness	NO	NO

Davide Vaghetti – davide.vaghetti@garr.it

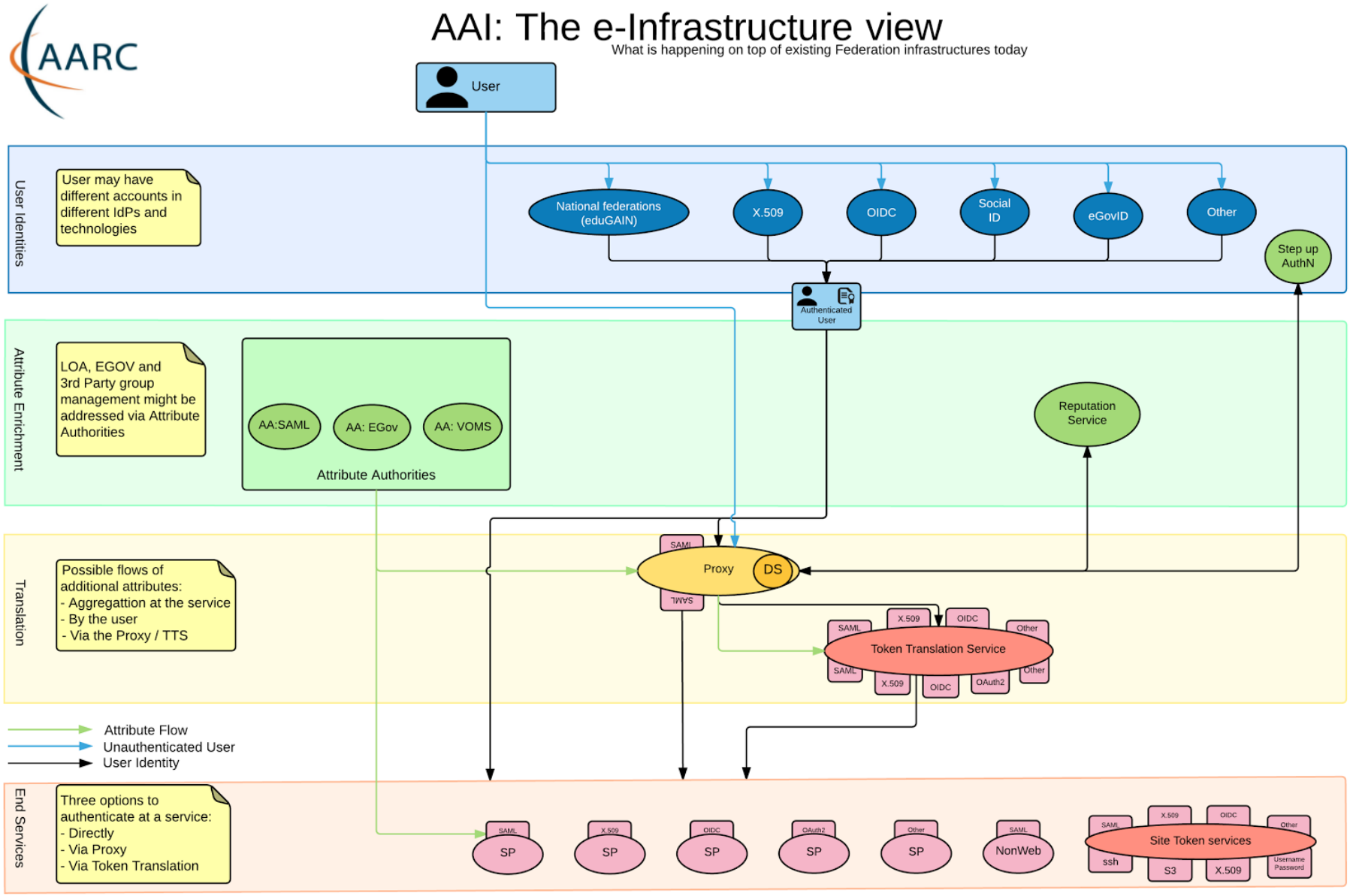
AARC Blueprint Architecture

Milestone MJRA1.4
First draft of the Blueprint Architecture
(in review, non ancora pubblicata)

“The goal of this document is to provide a general AAI architecture that can be used as a blueprint for the design and implementation of integrated and interoperable AAI solutions in the R&E sector.”

Davide Vaghetti – davide.vaghetti@garr.it

AARC: Blueprint (AAI) Architecture

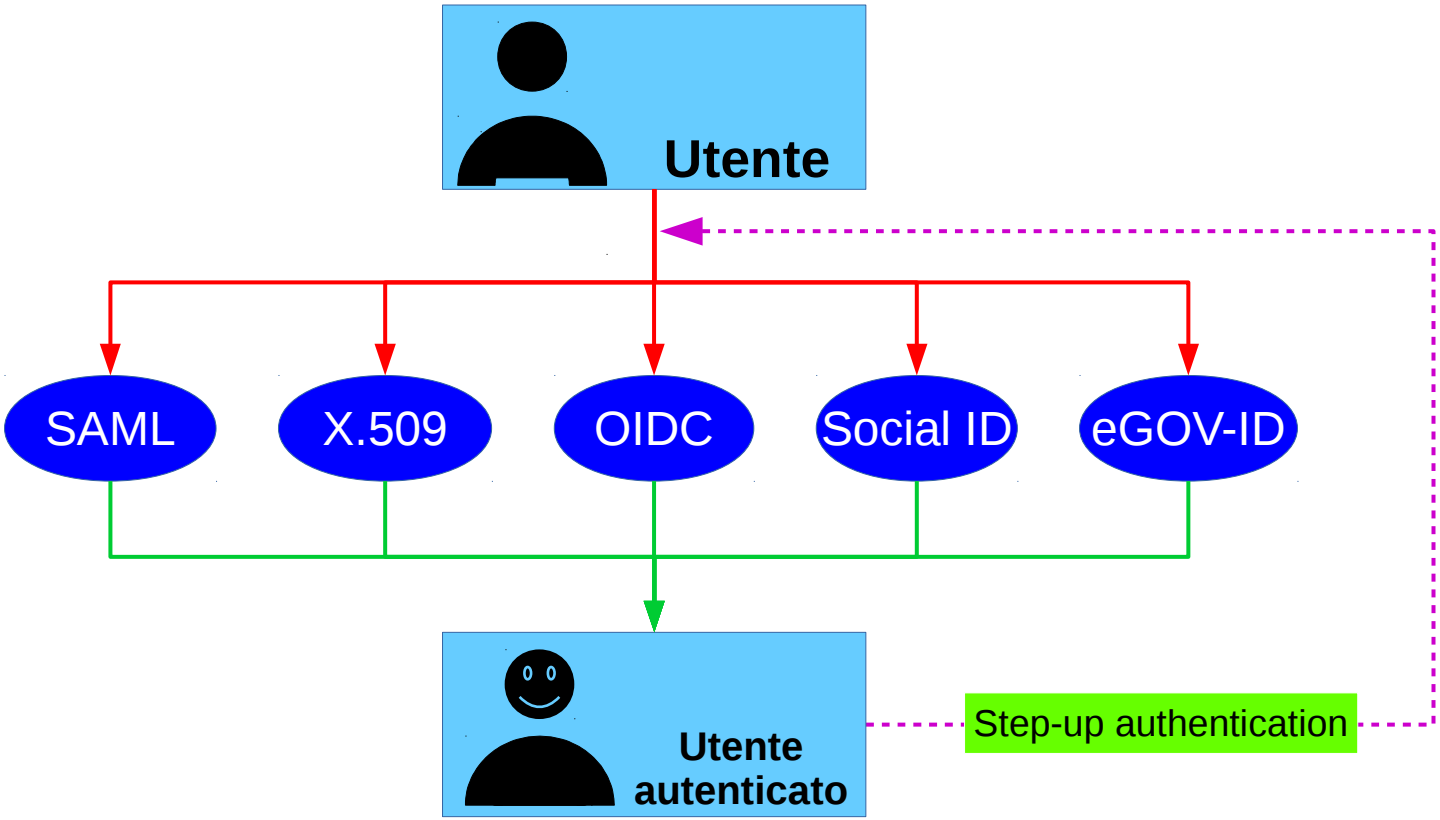


Milestone MJRA1.4, First draft of the Blueprint Architecture

Davide Vaghetti – davide.vaghetti@garr.it

AAI Architecture: User Identities Layer

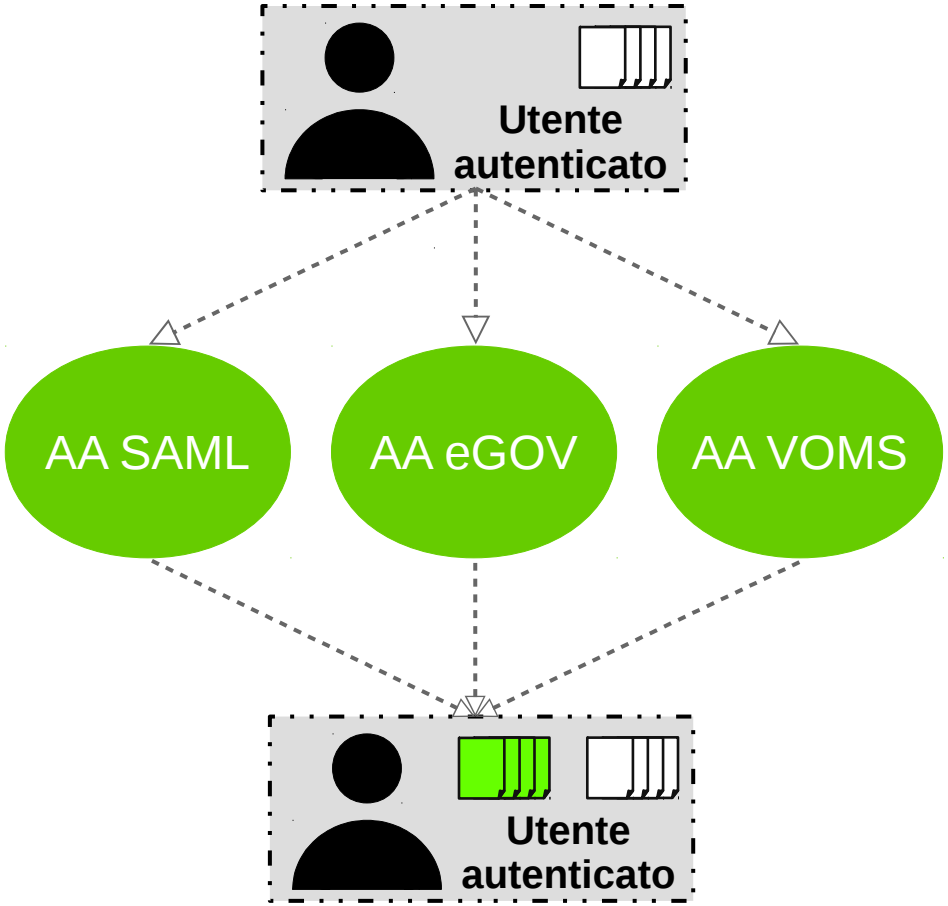
Gli utenti possono avere piu' identita' su diversi IdP che a loro volta implementano differenti tecnologie di autenticazione



Davide Vaghetti – davide.vaghetti@garr.it

AAI Architecture: Attribute Enrichment

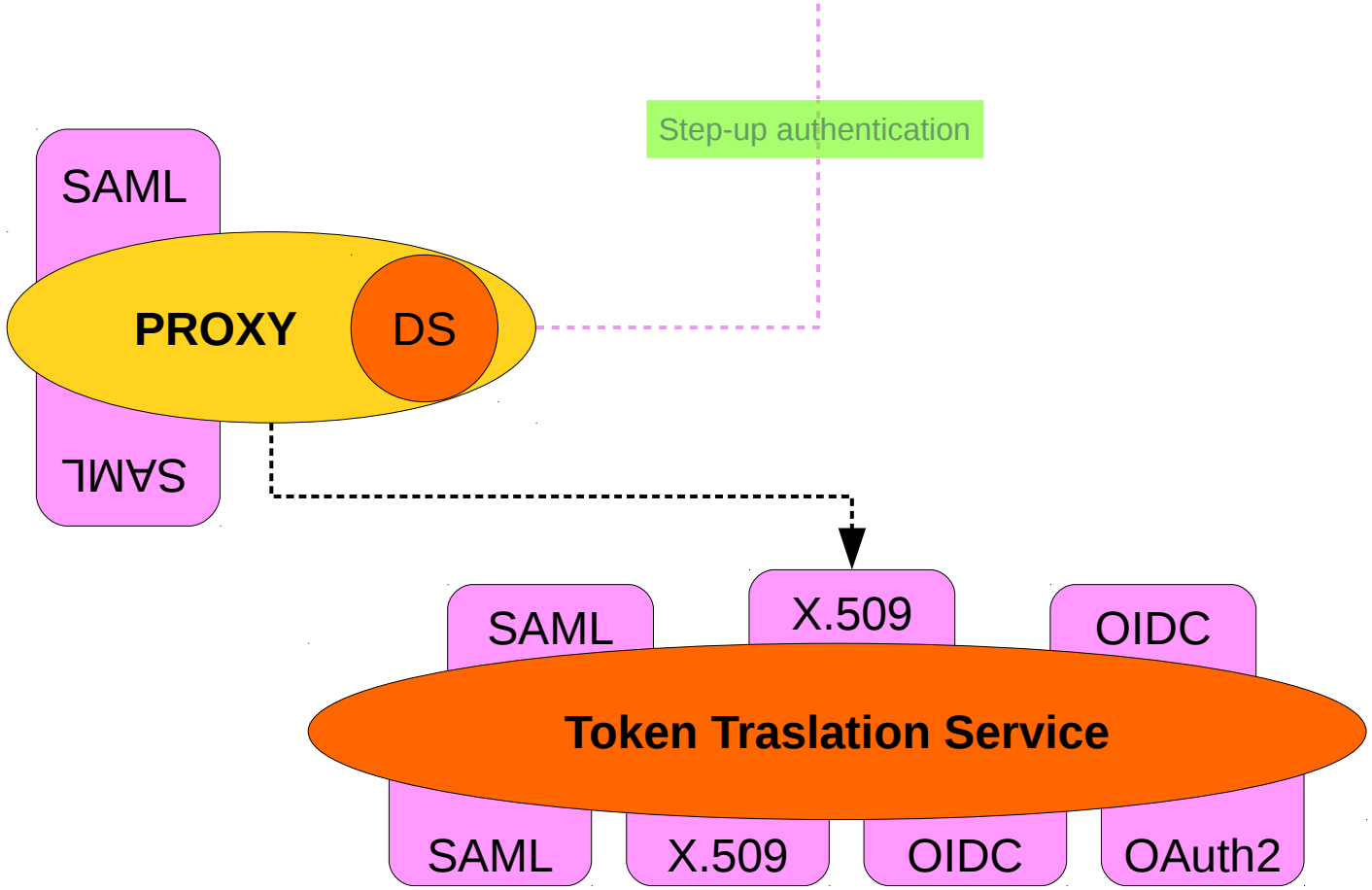
Tramite Attribue Authorities e' possibile arrichire il set di attributi degli utenti con informazioni su gruppi, ruoli, account linking, ecc.



Davide Vaghetti – davide.vaghetti@garr.it

AAI Architecture: Proxy/TTS

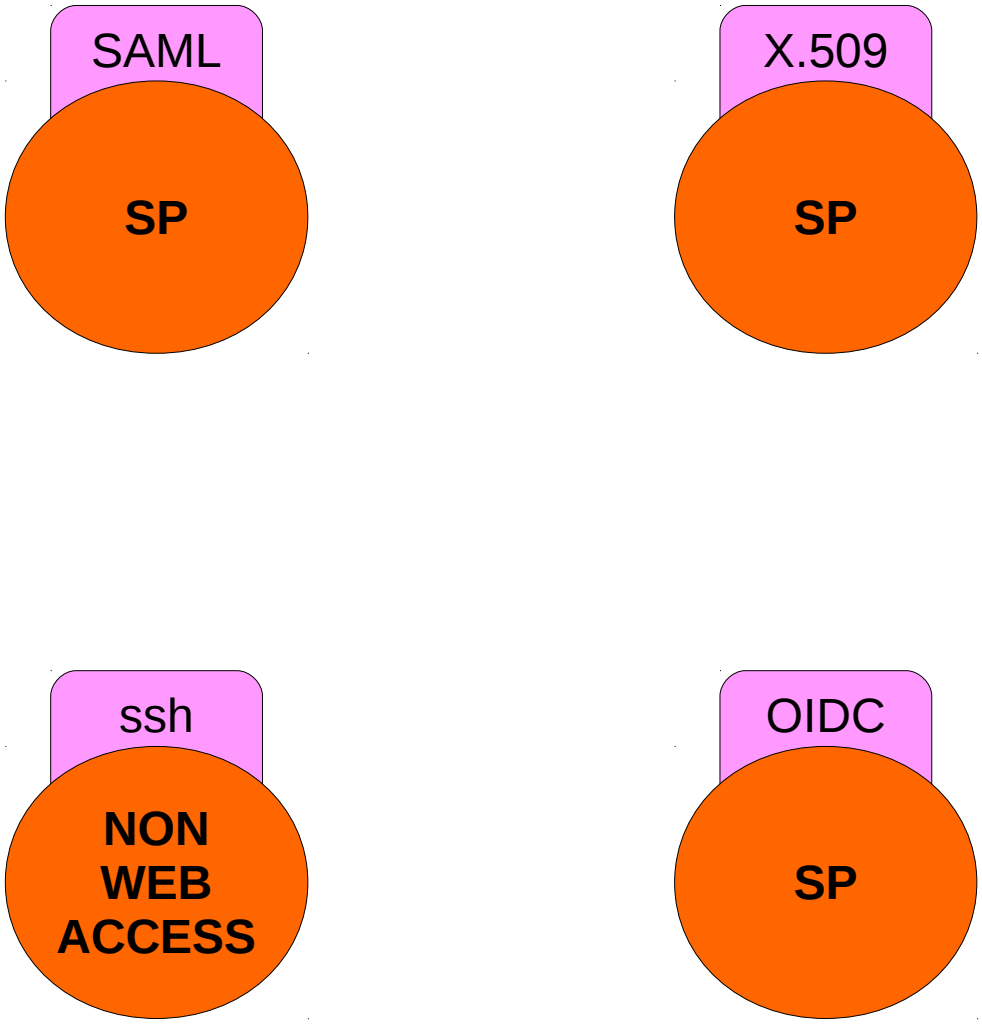
Proxy e TTS mettono a disposizione:
- ulteriore arricchimento attributi tramite aggregazione, inserimento utente, ecc.
- hook per step up authentication
- protocollo di autenticazione di arrivo diverso da quello di partenza (token translation)



Davide Vaghetti – davide.vaghetti@garr.it

AAI Architecture: End Services

I servizi finali vengono acceduti direttamente, o tramite proxy, o tramite TTS.
A loro volta sui Service Provider possono essere integrati servizi trasparenti di TTS, o tecnologie che permettano di utilizzare l'autenticazione federata con servizi NON-WEB (ssh).



Davide Vaghetti – davide.vaghetti@garr.it

AARC: Per saperne di più

IDEM e GARR partecipano alle attività di AARC in tutte e tre le sue declinazioni:

- Architettura e Design (JRA)
- Pilot (SA)
- Disseminazione e Training (NA)

https://wiki.geant.org/display/AARC/AARC+Home

Davide Vaghetti – davide.vaghetti@garr.it

Grazie

Davide Vaghetti – davide.vaghetti@garr.it