Risultati del pilot su EZproxy ed accesso federato

MARIO REALE

GARR

Roma, 8 Maggio 2018

IDEM DAY 2018

Agenda

- Contesto e scopo del pilot su EZproxy
  - I requisiti degli utenti
- Il progetto AARC
- Il lavoro di installazione e configurazione di EZproxy
- Risultati
- Conclusioni

Contesto del pilot su EZproxy

Il contesto in cui si e' svolto il pilot su EZproxy e' quello che **progetto AARC** (https://aarc-project.eu/) che

- mira a **promuovere l'adozione di tecnologie di AAI federate** presso le comunitá utente
- a **supportarle nella definizione** della loro infrastruttura di autenticazione ed autorizzazione e **nell'uso delle eInfrastructure esistenti**
- GARR ha coordinato il **task SA1.1** della fase 1 (05/15-04/17) del progetto:
  - SA1 Task1: Pilots on Guest Identities
    - Subtask 3 : Libraries

I requisiti utente delle biblioteche

- beneficiare dei **vantaggi dell'autenticazione federata** per i propri utenti rispetto a quella IP-based:
  - eliminazione del problema utenti in "roaming" / necessità' di VPN
  - maggiore possibilita' di profilazione / accesso basato sul ruolo
  - maggiore tracciabilità degli utenti e possibilità
- gestire per alcuni anni un **modello di AAI ibrido**, in cui alcuni publishers presentano endpoint federati, altri IP-based, o entrambi
- interfacciarsi (in alcuni casi) con **body di coordinamento a livello nazionale** per i contratti quadro con gli editori online (*national bodies for the negotiation of electronic resources* (https://goo.gl/dH1otb))
- Gestire i **walk-in users**: utenti che hanno accesso alle risorse in virtù del loro essere in sede, in biblioteca

Mandato del subtask TSA1.1.3 di AARC

- Il mandato del task è stato quello di implementare progetti pilota sulle soluzioni (Pilot, definite anche con JRA1) per **supportare le biblioteche nell'adozione dell' AAI federata**
  - tenendo in considerazione i requirement della comunità' utenti
- I pilot per le biblioteche devono tenere in considerazione:
  - Soluzioni che permettano la **Hybrid Authentication**
    - IP-based AuthN e SAML/Identity Federations
  - **Walk-In Users:**
    - Utenti delle biblioteche che non siano registrati in nessun IDP – ma sono "on premises' connessi ad un terminale
  - **Library Consortia / Branding:**
    - In molti casi una o più organizzazioni gestiscono i contratti con gli editori, negoziano l'accesso alle risorse elettroniche a livello nazionale

Il progetto AARC

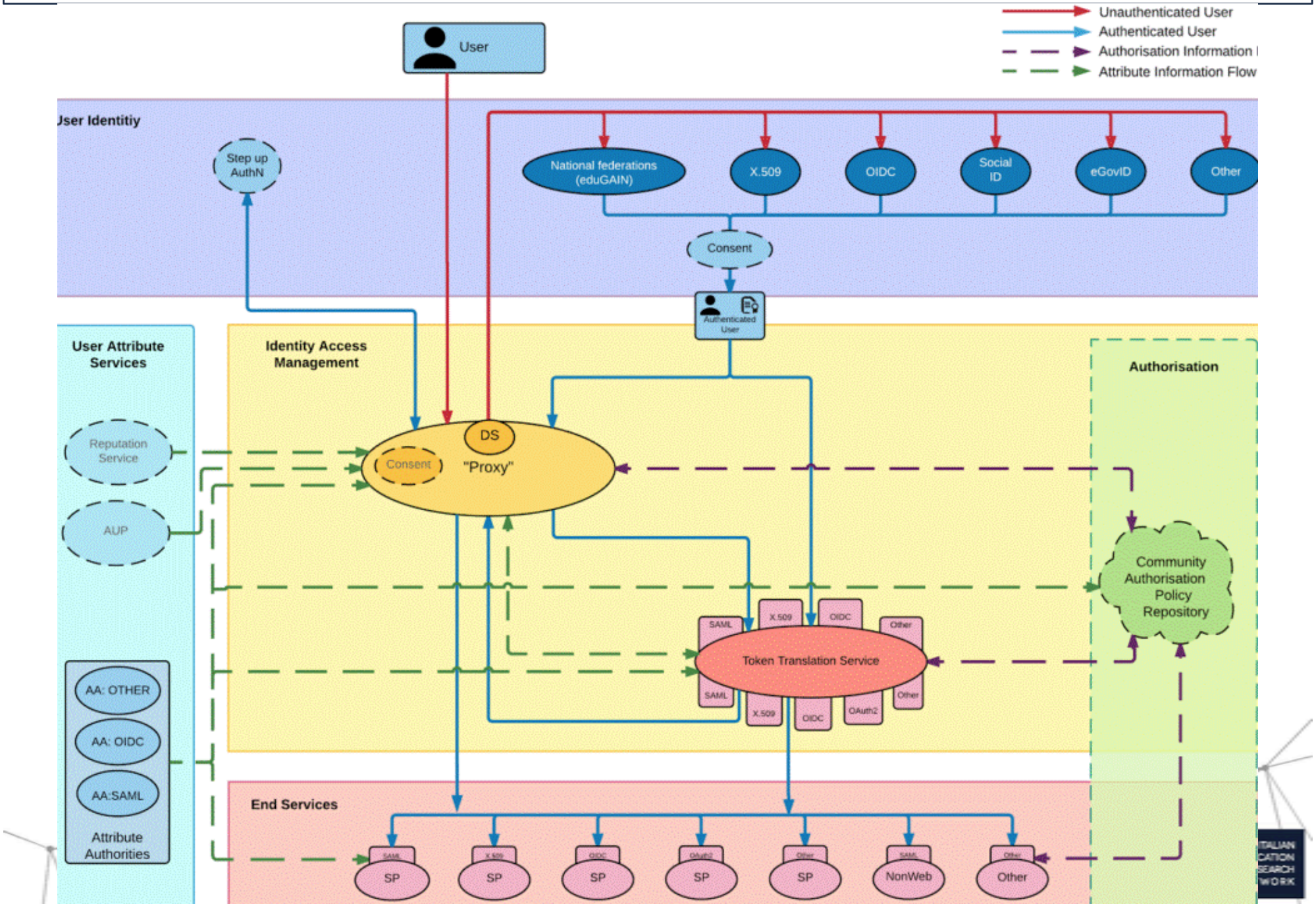
AARC (Authentication and Authorization for Research and Collaboration) e' un progetto EU in ambito H2020 - **https://aarc-project.eu**

- Iniziato Maggio 2015 :
  - Fase 1 (05/2015 - 04/2017)
  - Fase 2 (05/2017 - 04/2019)
- Obbiettivi:
  - Incentivare e supportare **l'adozione dell' AAI Federata** nell' eScience
  - Definire un'architettura di riferimento (**Blueprint Architecture**), compatibile con **eduGAIN**, per l' Autenticazione e l' Autorizzazione, Step-Up Auth
  - Riferirsi a **Policy Framework** noti e condivisi
  - Definire ed incentivare l' adozione di **Best Practices** in ambito AAI
  - Supportare l'evoluzione della Blueprint Architecture (BPA) stessa
  - **Rendere i risultati sostenibili** attraverso dei pilot da implementare poi in produzione
  - Evangelizzare e formare la comunita' utenti attraverso **training dedicato e generale**
  - https://aarc-project.eu/wp-content/uploads/2016/12/AARCStrategy.pdf

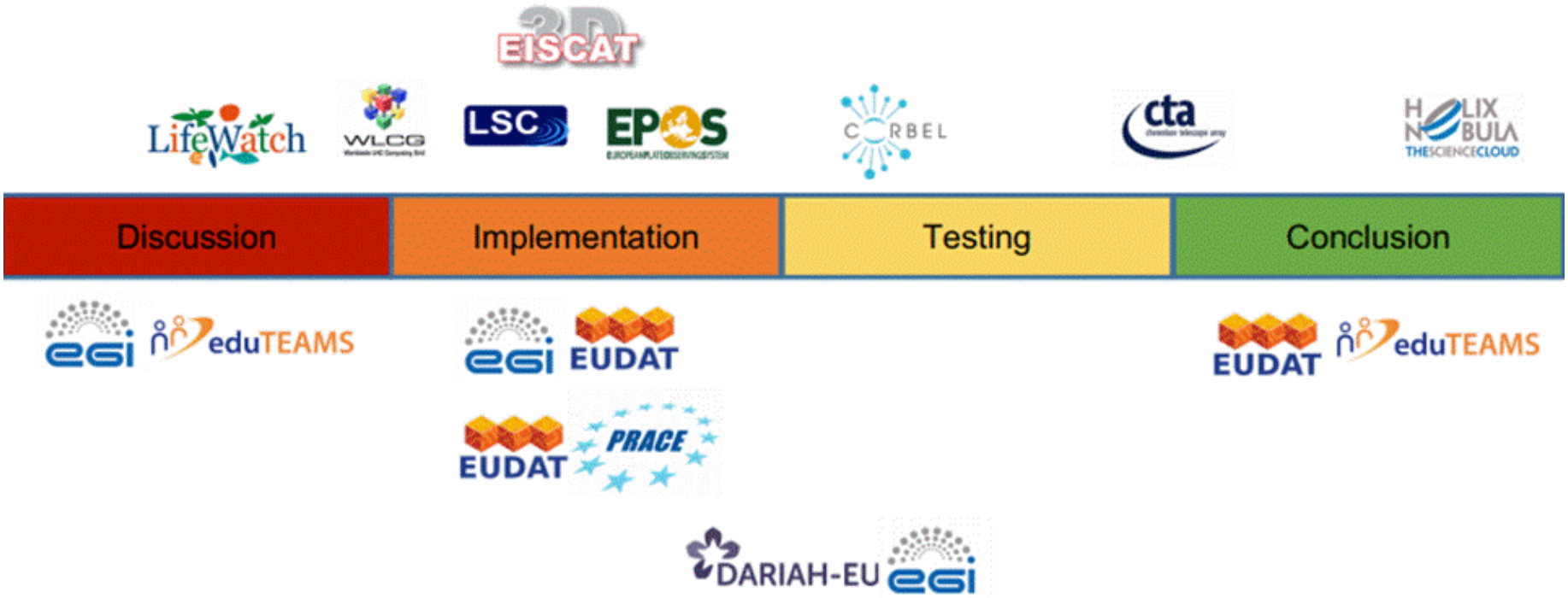
Il progetto AARC (fase 2) 2017-2019

- Budget Indicativo: 3 MEuro
- Manpower: 325 PM
- Attivita':
  - NA1 Management
  - NA2 Dissemination and Training
  - NA3 Policies and Best Practices
  - JRA1 Architecture
  - SA1 Pilots with User Communities

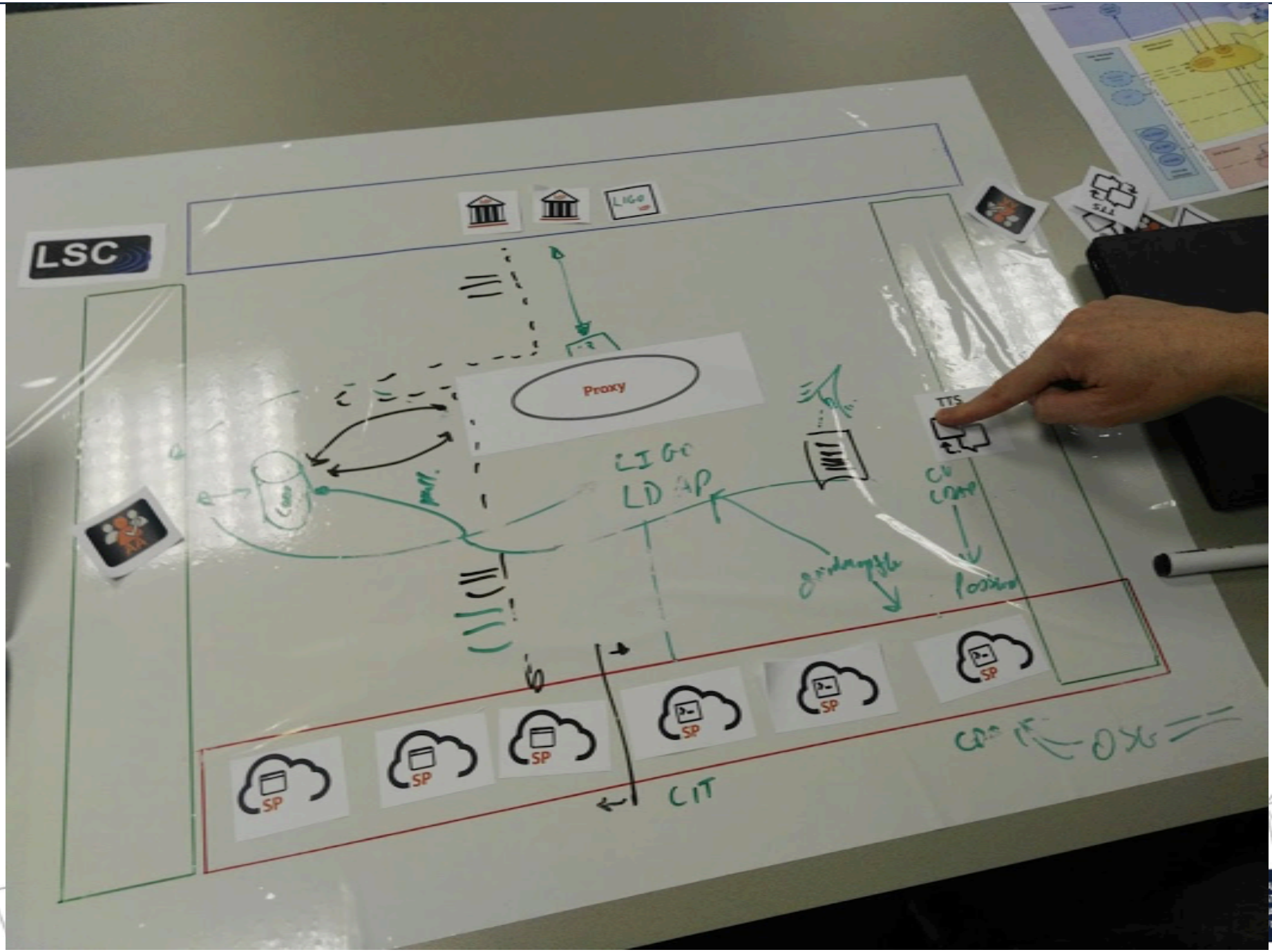
La AARC Blueprint Architecture

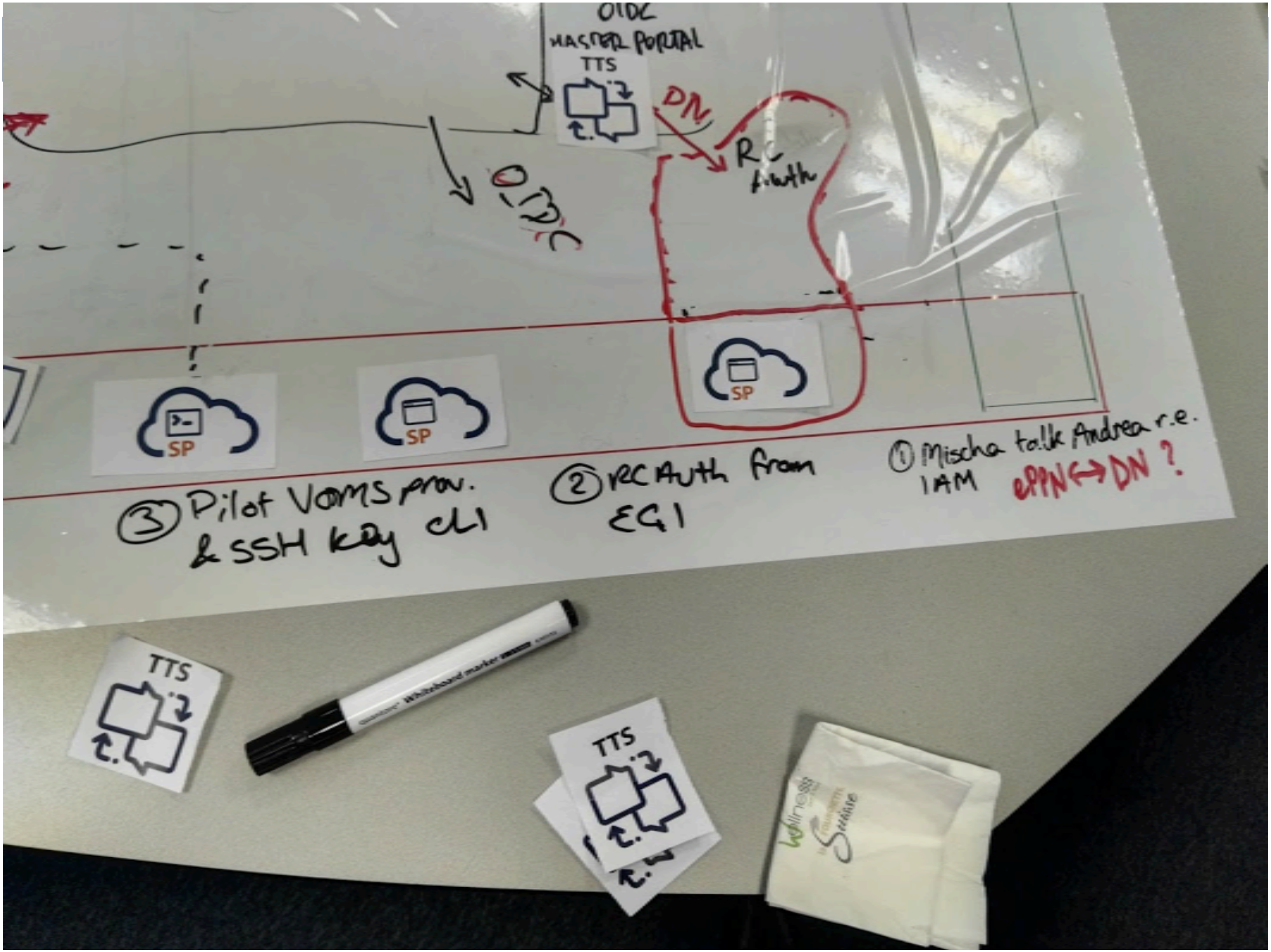


AARC SA1: Pilot con le comunita' utente e le eInfrastructure



Come lavoriamo in AARC SA1 in pratica..

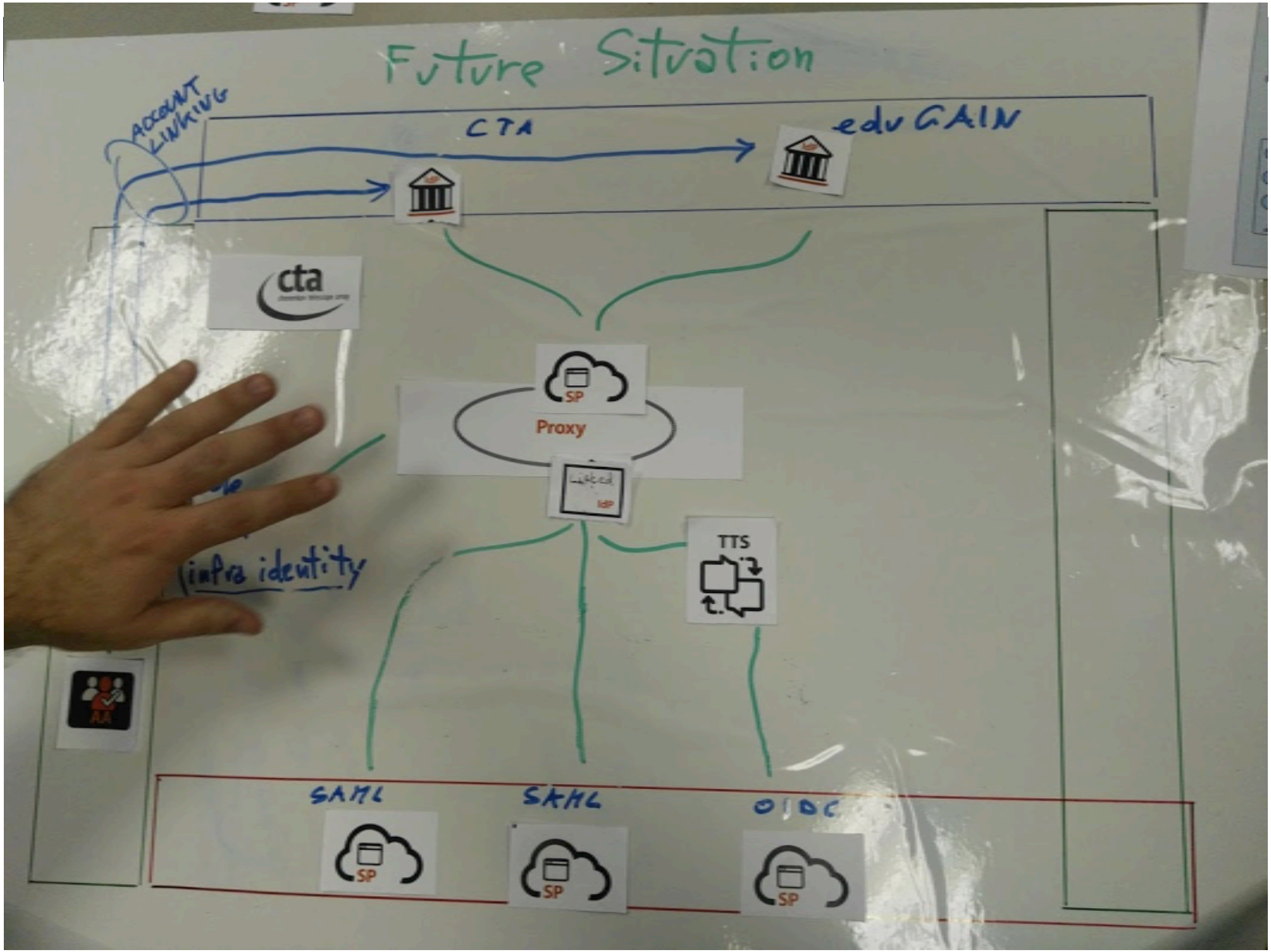




③ Pilot VOMS prov. & SSH key cli

② RC Auth from EGI

① Mischa talk Andrea r.e. IAM eppn↔DN ?


Future Situation
ACCOUNT LINKING
CTA
eduGAIN
cta
SP
Proxy
IdP
TTS
infra identity
SAML
SAML
OIDC
SP
SP
SP

Scopo del pilot su EZproxy

Il pilot su EZproxy ha implicato l'implementazione di 3 scenari operativi che riflettono i requisiti utente:

Scenario 1:

- Dimostrare l'utilizzo di EZproxy come ***Access Mode Switch (AMS)***
- Fare esperienza sul tool EZproxy
- Configurare la **plugin Shib IdP per la IP-based Authentication**
- Scrivere una **guida dettagliata** su come supportare le biblioteche nella configurazione di EZproxy come AMS
  - abilitando l' autenticazione con SAML IDP ogni volta possibile

Scenario 1 EZpx=AMS

Scenario 2:

- Estendere il meccanismo di autenticazione per una biblioteca in modo da
  - definire gli Attributi nelle asserzioni SAML basandosi su informazione IP-based
  - Fornire un portale che gestisca i walk-in users come gli utenti principali, maggioritari

Scenario 2 Walk In portal

Scenario 3:

- Estendere lo scenario 2 al caso di molte biblioteche

Scenario 3 Multilibrary Walk in portal

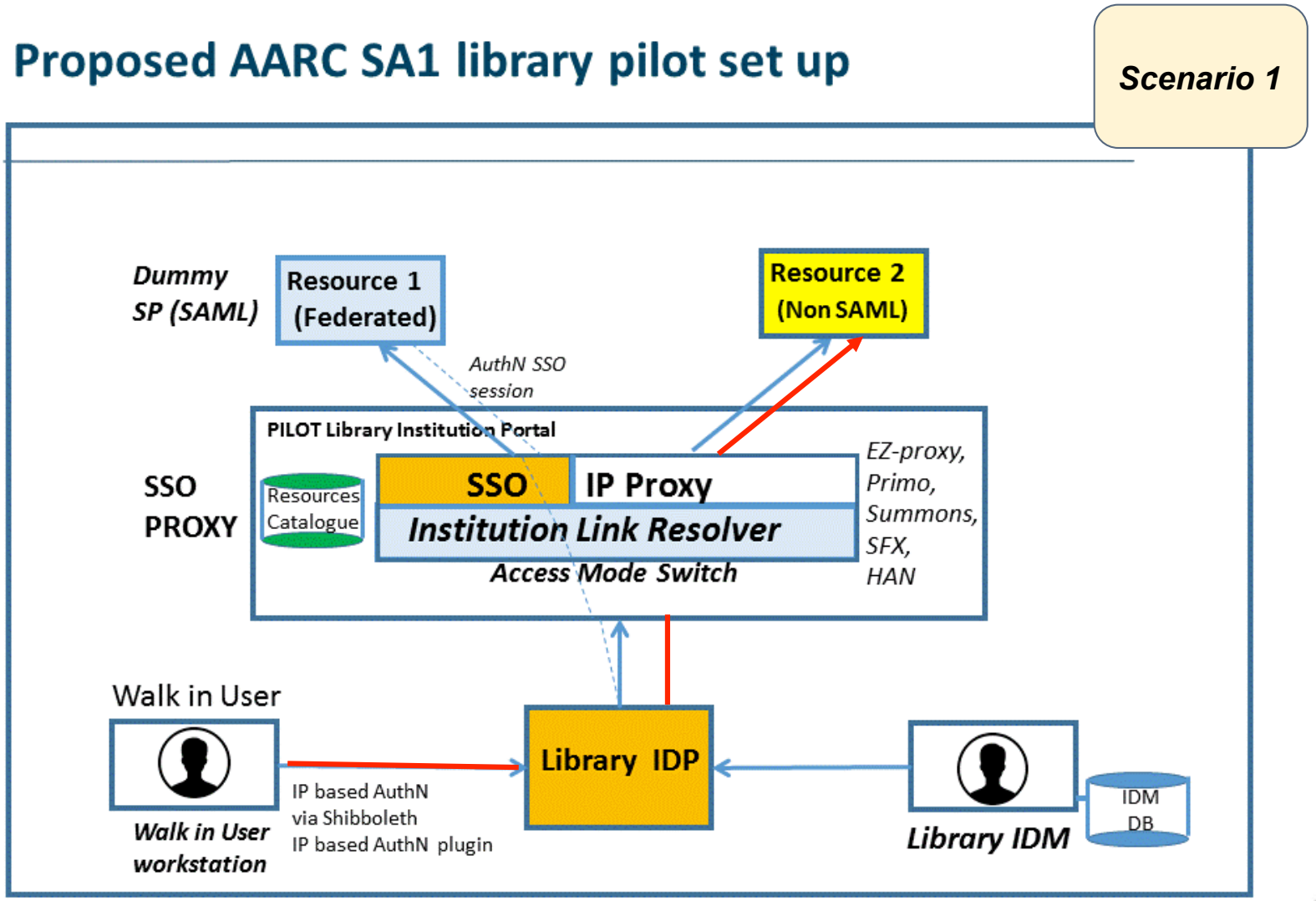
Scenario 1

EZproxy come Access Mode Switch e plugin Shibboleth IdP per la IP based AuthN (walk-in-users)

Scenario 1
EZpx=AMS

Scenario 1: Hybrid access (EZproxy as access mode switch)

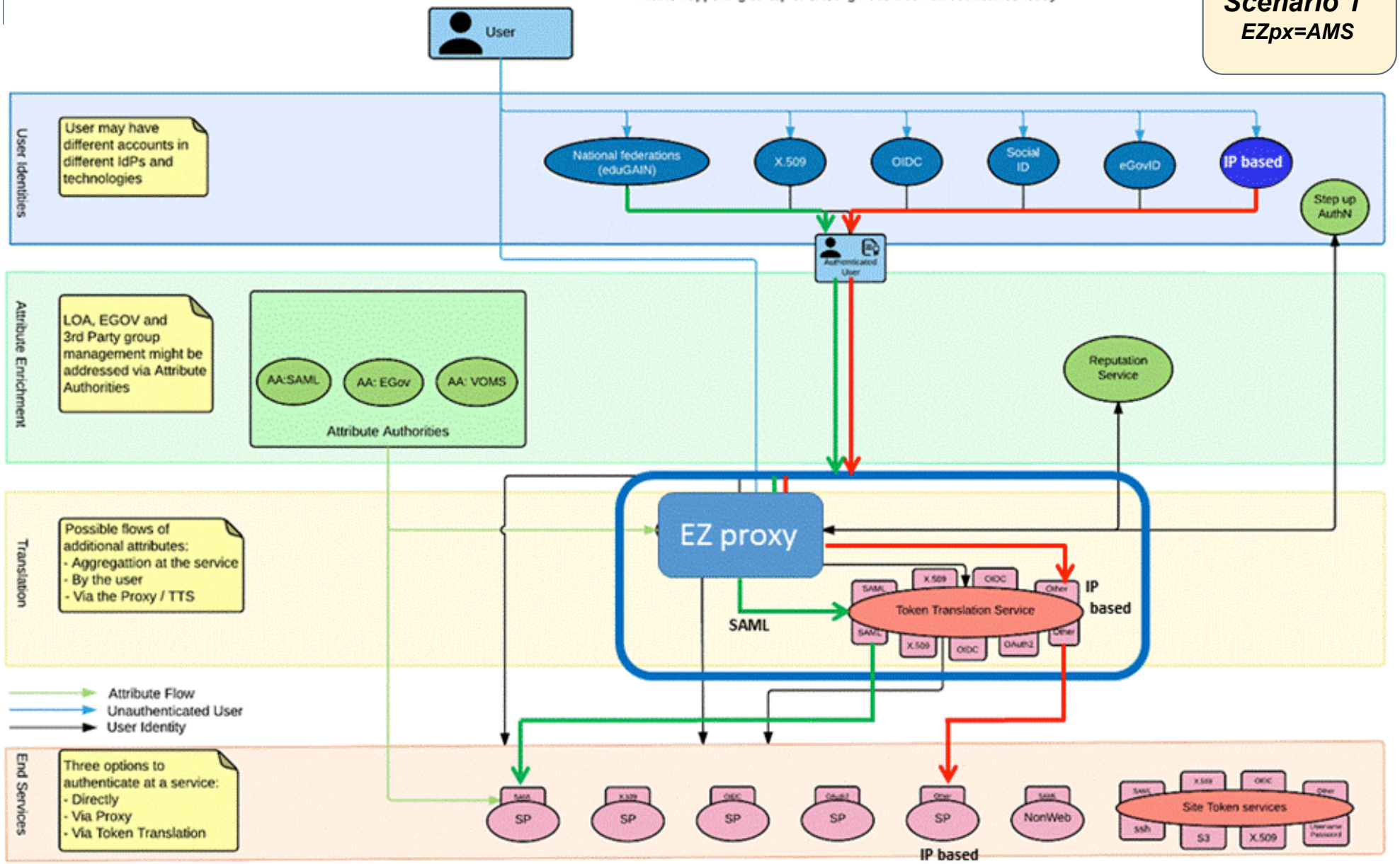
OCLC EZproxy acting as access mode switch + IP based IDP ext for Walk-in users



AAI: The e-Infrastructure view

What is happening on top of existing Federation infrastructures today

Scenario 1
EZpx=AMS



Riassunto del lavoro di configurazione di EZpx

1. EZproxy installato e configurato come **standard IP proxy** @ GARR Firenze
   a. configurato per lavorare con vere risorse di editori online
   b. local DB per le credenziali utente (username e password degli utenti)
2. Shibboleth: Registrato EZproxy come **SP nella IDEM test federation**
   a. uso di wildcard * certificates - used TCS digicert - facile da ottenee - wild card per port 443
   b. self-signed certificate per i metadati
3. Configurata una trusted connection verso un **singolo IdP**
4. Release degli attributi verso EZproxy:
   a. entitlement
   b. affiliation
   c. Shibboleth set up,si possono specificare ruoli specifici – vedi guida
   d. Many options are available
5. Configurata la login **login** federata su EZproxy
   a. Gli utenti possono loggarsi su EZproxy utilizzando le loro credenziali domestiche (della loro Home Organization)

Scenario 1
EZpx=AMS

Riassunto sulla configurazione di EZpx

Scenario 1
EZpx=AMS

6. Dopo la login utente, il meccanismo di proxy e' disponibile
7. Configurazione dell'**Access Mode Switch**:
   a. Ogni risorsa/publisher e' stata configurata in EZproxy in maniera standard (utilizzando quelle che lui chiama *database stanzas*)
   b. Per quei publishers che forniscono una "Institutional Login" e' stata configurata una direttiva specifica (SPUEdit)
   c. Ogni richiesta utente e' servita con il redirecting della sessione utente verso SP login initiator se disponibile oppure semplicemente proxando i contenuti
8. Vantaggi :
   a. nel caso di IP proxying, il traffico di rete dipende strettamente dal traffico del proxy
   b. Negli altri casi l'utente e' **re-diretto verso l' endpoint del publishers**, riducendo il traffico di rete del proxy stesso

Una trascrizione del flusso operativo, descritto anche in un video dimostrativo, e' disponibile su https://goo.gl/Fhqtp6

I vantaggi dell' utilizzo di EZproxy

Scenario 1
EZpx=AMS

- Tutti i **vantaggi della Autenticazione Federata rispetto a quella IP based** – ogni qual volta essa e' disponibile (no IP proxying, no VPN..)
- In confronto ai meccanismi di proxy standard basati su IP il vantaggio dell' SSO e' di **permettere l' user profiling** (se supportato dal provider) EZpx agisce come SP di Federazione accettando login federate, e permettendo anche di non utilizzare il DB utenti locale in questo caso
- EZpx e' un tool abbastanza diffuso, disponibile presso varie istituzioni della comunità' delle biblioteche **e lavora molto bene con molti tools di discovery a disposizione** delle biblioteche stesse, e con sistemi di delivery delle biblioteche
- Per questo motivo se le risorse non sono federate si utilizza la sua funzionalita' di proxying IP

Abbiamo scritto una **guida dettagliata** sull' utilizzo di EZproxy come AMS – disponibile su https://goo.gl/GcJ2Sv

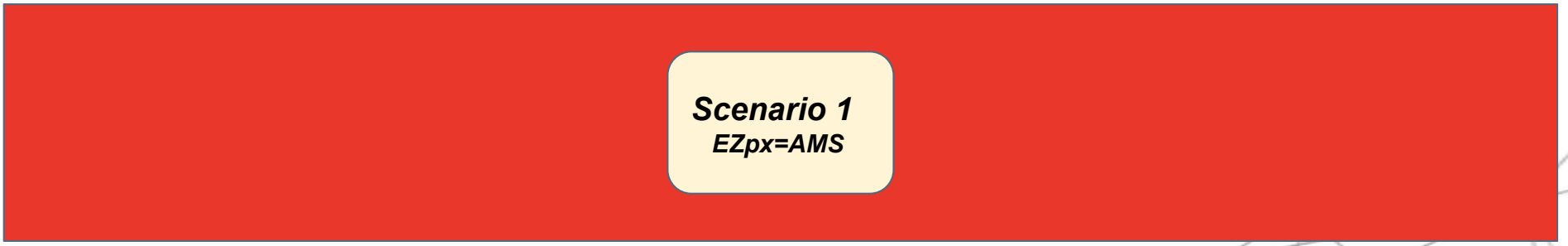
Plugin IP-based AuthN per Shib IdP per i Walk In users

Scenario 1
EZpx=AMS

- E' stato anche implementato un meccanismo per i **Guest Users**, un modo di gestire gli utenti che non sono dentro all'Identity Provider
- O per le biblioteche, che accettano Walk In users: utenti non registrati nell IDP ma connessi su un terminale pubblico dentro la biblioteca
- Infatti Shibboleth sull' istanza dell' IdP non supporta solo Username e Password come meccanismo di autenticazione, ma anche **IP-based information**
- Accesso basato sull' IDP dal lato dell' Identity Provider (solo verso endpoint IP)
- >> **Per un certo numero di IP configurati, quindi, non vengono richiesti username e password**

Conclusioni sullo Scenario 1

- E’ stata effettuata una validazione completa, sul campo, di EZproxy come Access Mode Switch
- E’ stata anche collaudata la plugin IP-based AuthN per lo Shibboleth IdP per permettere una soluzione per i Walk in users
- E’ stata prodotta una guida completa di Installazione e Configurazione ad uso delle biblioteche e del loro personale IT per la configurazione di EZproxy in questa modalità’
  - https://goo.gl/GcJ2Sv
- Un video dimostrativo sul pilot EXproxy di AARC e’ su
  - https://goo.gl/oEyCWQ



Scenario 2

Walk in user Portal

Set di Attributi SAML sulla base di informazioni IP-based

Scenario 2 Walk In portal

Scenario 2: Walk In user portal

Scenario 2 Walk In portal

Scopo:

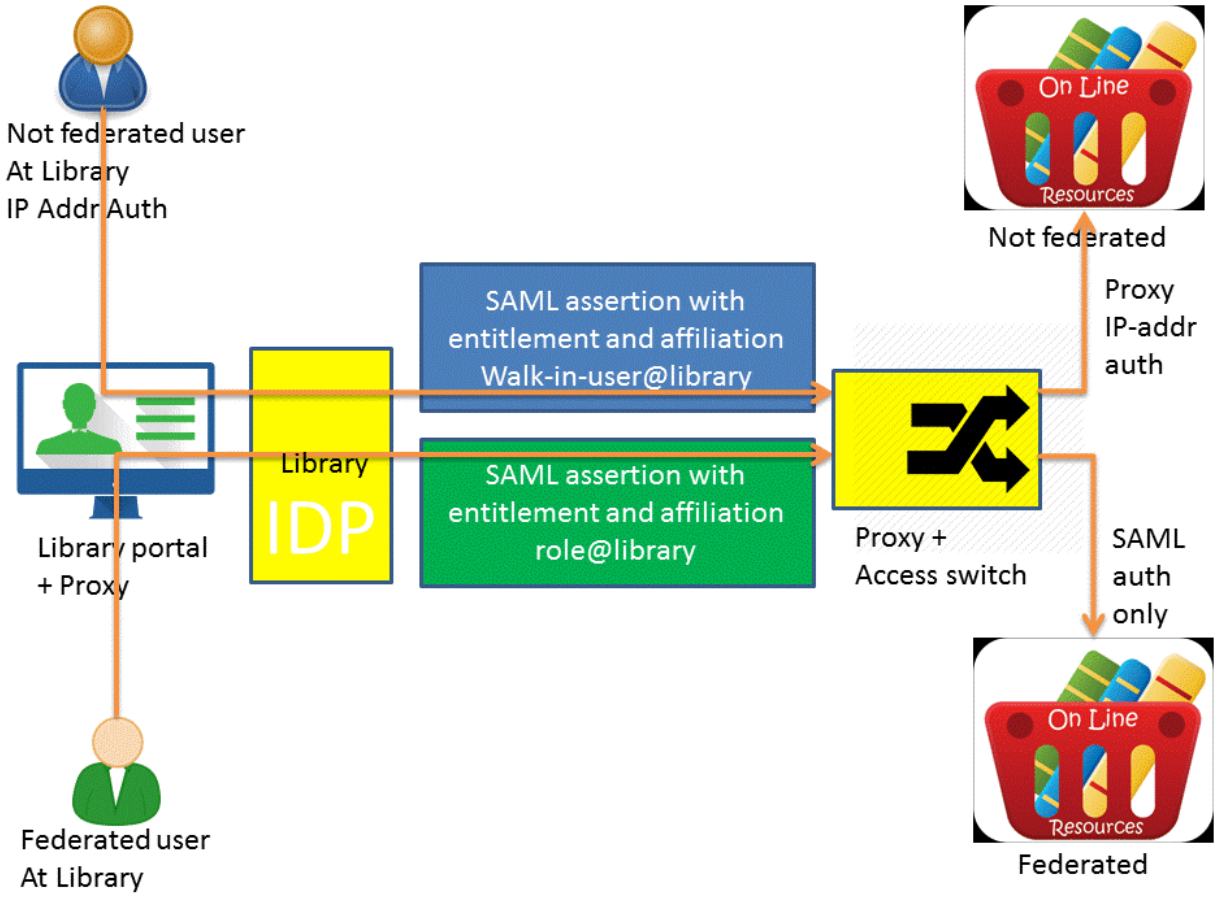
Dimostrare la realizzabilità' di un portale per i Walk-In users nel caso in cui essi siano i bulk users

Caso di 1 biblioteca

Scenario 2
Walk-In user portal including IP-based AuthN

Scenario 2 Walk In portal

- Portal allowing both IP and federated AuthN
- Dealing with 1 Library (1 IDP)
- Setting attributes based on IP info



Scenario 3: Super Walk In user portal

Scenario 3 Multilibrary Walk in portal

Scopo:

- Dimostrare la **realizzabilità di un portale per i Walk-In users** nel caso in cui essi siano i bulk users

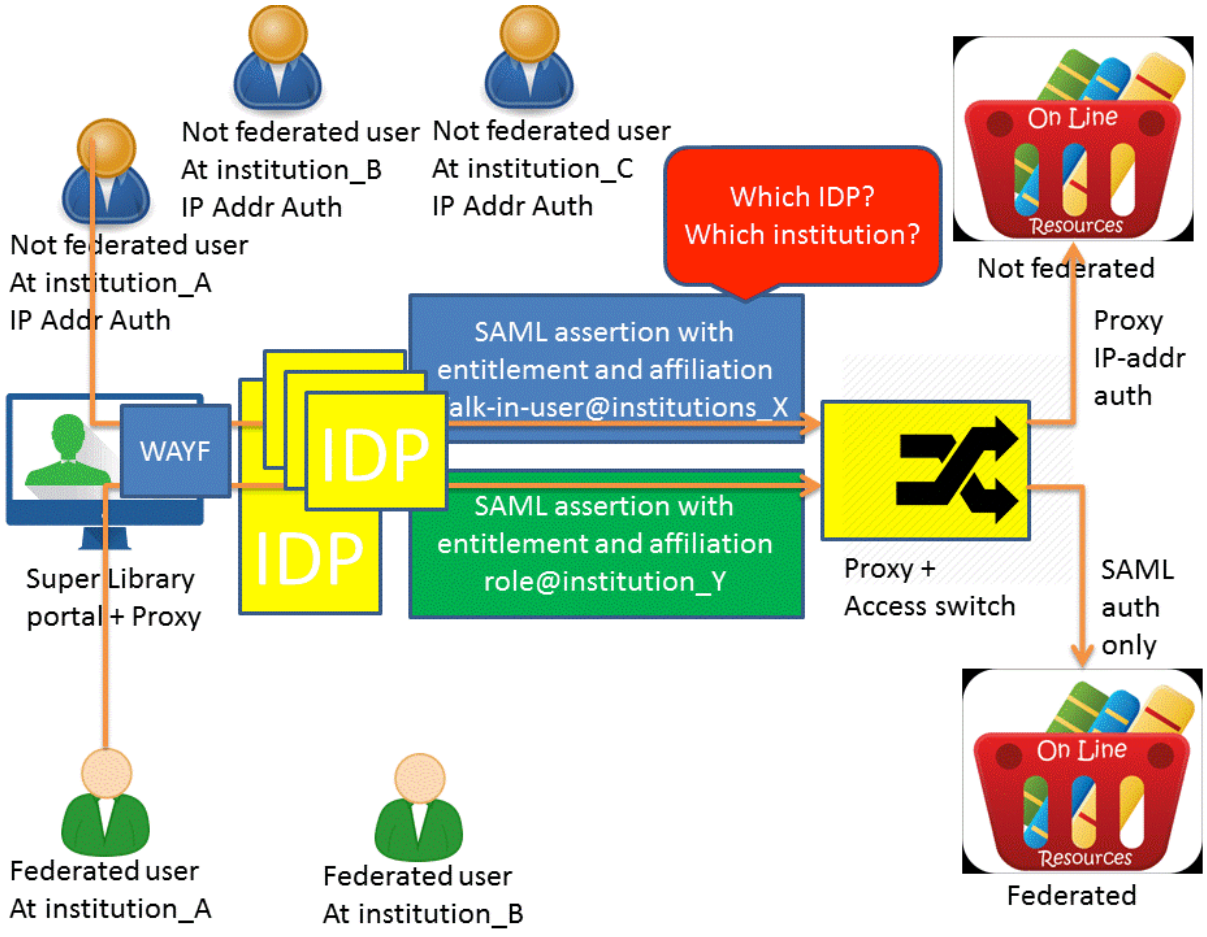
- Settando attributi in **asserzioni SAML sulla base di informazioni IP-based**

- Estendendo il caso dello Scenario 3 ad una situazione con molte biblioteche da gestire attraverso il portale

“Super Walk-in” portal dealing with multiple libraries

- Portal dealing with many Libraries
- Acting as User Interface
- Publishers see IDPs selected by user
- Portal is a Federation SP
- Manages IP based information

Scenario 3 Multilibrary Walk in portal



Conclusioni

- Vantaggi per la Comunita’ IDEM:
- EZproxy e’ un prodotto **affidabile**, diffuso e spesso già in dotazione di molte biblioteche che a volte semplicemente non sanno della possibilità di configurarlo come **Access Mode Switch.**
- Può comportarsi come un proxy IP quando necessario e come SAML proxy che permette accesso tramite
  - E’ quindi ideale per gestire una fase di **Autenticazione Ibrida**
    - **Ogni volte possibile, offre quindi tutti I vantaggi dell’Autenticazione Federata (rispetto a quella IP based)**
- Utilizzando tecnologie standard si sono dimostrate la **realizzabilità di portali dedicati alla comunità dei Walk In users** come bulk users del sistema

Contributi ai pilots

Pete Birkinshaw, Martin Haase, Peter Gietz / DAASI
Lalla Mantovani, **Barbara Monticini,** Mario Reale / GARR
Niels van Dijk / SURFnet
Jens Jensen / STFC
Nicolas Liampotis, Christos Kanellopoulos, Zenon Mousmulas / GRNET
Jiri Pavlik, Petr Zabicka / MZK

Riferimenti

Scenario 1

- https://wiki.geant.org/display/AARC/Libraries+EZproxy+access+mode+switch+pilot
- https://wiki.geant.org/display/AARC/EZ+proxy+pilot+description

Video sullo Scenario 1:
https://drive.google.com/file/d/0B6nLU4k7ZZvfaUM4OTJtTmlFN28/view

Guida alla configurazione di EZproxy come Access Mode Switch:
https://www.oclc.org/content/dam/support/ezproxy/documentation/pdf/ezproxy_referencemanual.pdf

Scenari 2 e 3

- https://wiki.geant.org/display/AARC/Libraries+walk-in-user+pilot

Shibboleth IP-based Authentication plugin

- https://wiki.shibboleth.net/confluence/display/SHIB2/IdPAuthIP