Status and plans of AARC SA1 Libraries pilots

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

SA1 TSA1.1 Pilots on Guest Identities

Subtask TSA1.1.3 Libraries

Content

- **Goals** for subtask TSA1.1.3 (Libraries)
  - Key aspects for defining solutions and planning pilots
- Requirements and Pilots
  - Pilot #1 : Libraries Extended Multi-Scenario pilot
  - Pilot #2: Proxy Model for Library Consortia
- **Pilot #1:** Libraries Extended Pilot on Hybrid Access:
  - Scenario 1 - EZ proxy access mode switch
  - Scenario 2 - Walk in user portal including IP based AuthN
  - Scenario 3 - Super Walk In portal dealing with multiple libraries
- **Pilot #2**: Showcasing benefits for Library Consortia to join a federation as an IDP/SP proxy

- Next Steps

Goals for subtask TSA1.1.3 (Libraries)

- Pilot solutions (from JRA1) for **supporting Libraries in adopting Federated AAI**
  - taking into account the requirements from users' communities

- Library pilots have to take into account:
  - Solutions allowing **Hybrid Authentication**
    - IP-based AuthN and Identity Federations
  - **Walk-In Users:**
    - Library Users might not be registered in any IDP
  - **Library Consortia / Branding:**
    - In many cases one or few organizations manage contracts with publishers at the national level

Identity Federation vs Libraries Consortia

National bodies dealing with purchasing electronic resources are the Identity Federations only in few cases in Europe

We Need a link between Nat Id Federations and National Bodies for the Negotiation of electronic resources

Examples:

- UK(JISC), NL,
  - contract signer = National Identity Federation
- FR, SP, IT:
  - IT ,FR ,SP: Nat Id Fed does not manage contracts + National Body to issue contracts (not managing any Federation)
- GR : 2 Federations : HEAL-Link and GRnet

Goals for pilot #1

Scenario 1:

- Demonstrate usage of EZproxy as Access Mode Switch (AMS)
- Gain hands-on experience on the tool
- Write a comprehensive guide supporting libraries in the configuration of EZ proxy as AMS
  - enabling SAML IDP based AuthN wherever possible

Scenario 2

- Extend Authentication mechanisms for one library to
  - set Attributes in assertions based on IP information
  - providing a portal dealing with walk-in users as bulk users

Scenario 3

- Extend Scenario 2 to the case of multiple libraries

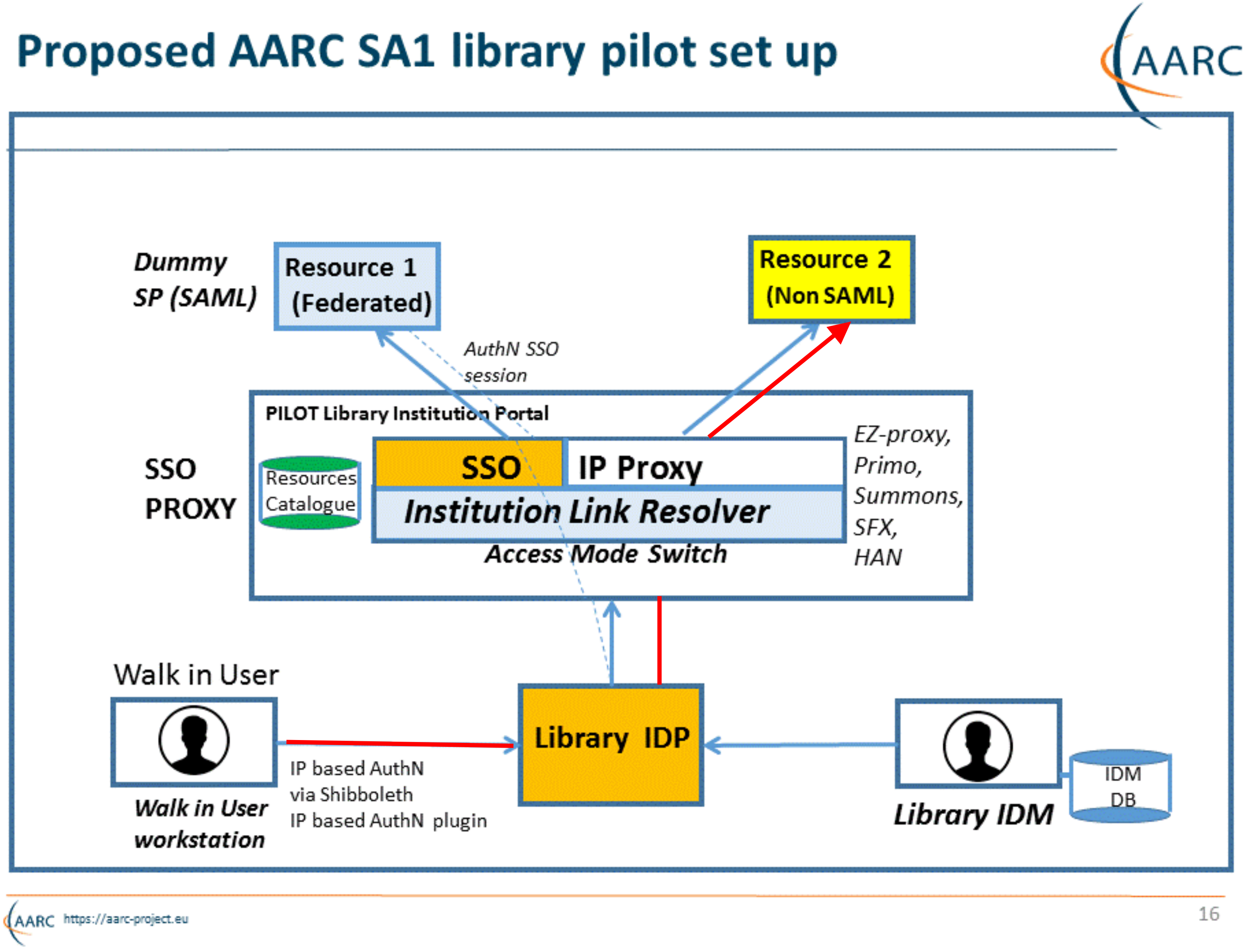
Goals for pilot #2

- Showcase benefit for a Library Consortium to join a federation as and IDP/SP proxy

[see later slides from Nicolas here]

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

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



Proposed AARC SA1 library pilot set up

Dummy SP (SAML)

Resource 1 (Federated)

Resource 2 (Non SAML)

AuthN SSO session

PILOT Library Institution Portal

SSO PROXY

Resources Catalogue

SSO

IP Proxy

Institution Link Resolver

Access Mode Switch

EZ-proxy, Primo, Summons, SFX, HAN

Walk in User

Walk in User workstation

IP based AuthN
via Shibboleth
IP based AuthN plugin

Library IDP

Library IDM

IDM DB

https://aarc-project.eu

Wrap up of Work Done on OCLC EZproxy (Scenario 1) 1/4

1. Installed EZpx working as a **standard IP proxy** @ GARR Firenze
   a. working with actual publishers
   b. local DB to store credentials (username and password of users)
2. Shibboleth: Made EZproxy become an SP in the test federation
   a. required wildcard * certificates - used TCS digicert - easy to obtain - wild card for port 443
   b. self-signed certificate for metadata
3. Configured a trusted connection to a single IDP
4. Release of attributes to EZproxy:
   a. entitlement of the user (not only affiliation, but if a user belongs to a specific department...and so on) - Shibboleth set up, you can specify specific roles - I followed the suggestion on the guide
   b. Many options are available
5. Configured **federated login** on EZproxy
   a. Users logged in on EZproxy using their HO credentials

Wrap up of Work Done on OCLC EZproxy (Scenario 1) 2/4

6. ~~After login, the PX mechanism would be in place also publishers~~ support federated ID
7. Configured the Access Mode Switch:
   a. Each resource/publisher has been configured in EZproxy standard way (database stanzas)
   b. For those publisher who provides "Institutional Login" a special directive (SPUEdit) has been configured
   c. Any user request is served redirecting the user session to the SP login initiator if available or simply proxying contents otherwise
8. Advantages: in case of IP proxing, the network traffic mostly depends on the proxy activity - in the other case the user is redirected to the publisher reducing the network connections

Wrap up of Work Done on OCLC EZproxy (Scenario 1) 3/4

Compared to the standard proxy mechanism (based on IP) the advantage of SSO is to maintain user profiling feature (if available by the provider)

EZpx acts like a service provider accepting federated login and thus avoiding the need of having a local user DB

EZpx is already in place in many location of our community and is known to work well with many discovery service tools and library delivery systems

So: if resources are not federated → Simple IP Px

If resources are federated, use the redirect SSO, BYPASSING the IP proxying mechanisms

A guide has been written based on the experience of this pilot

IP based authn and walk ins in Scenario 1

- Implemented mechanisms for Guest Users a smart way to manage users not yet in IDP
- Libraries accepting walk in users - not registered in the IDP - on a public terminal

Shibboleth in the IDP instance can support not only username and password but also IP
IP-based access from the IDP side (>>>> only towards IP endpoints) [few IP address to be Auth]

>> Not prompted for username and password

Outcome Pilot Scenario 1: full exploitment of EZproxy

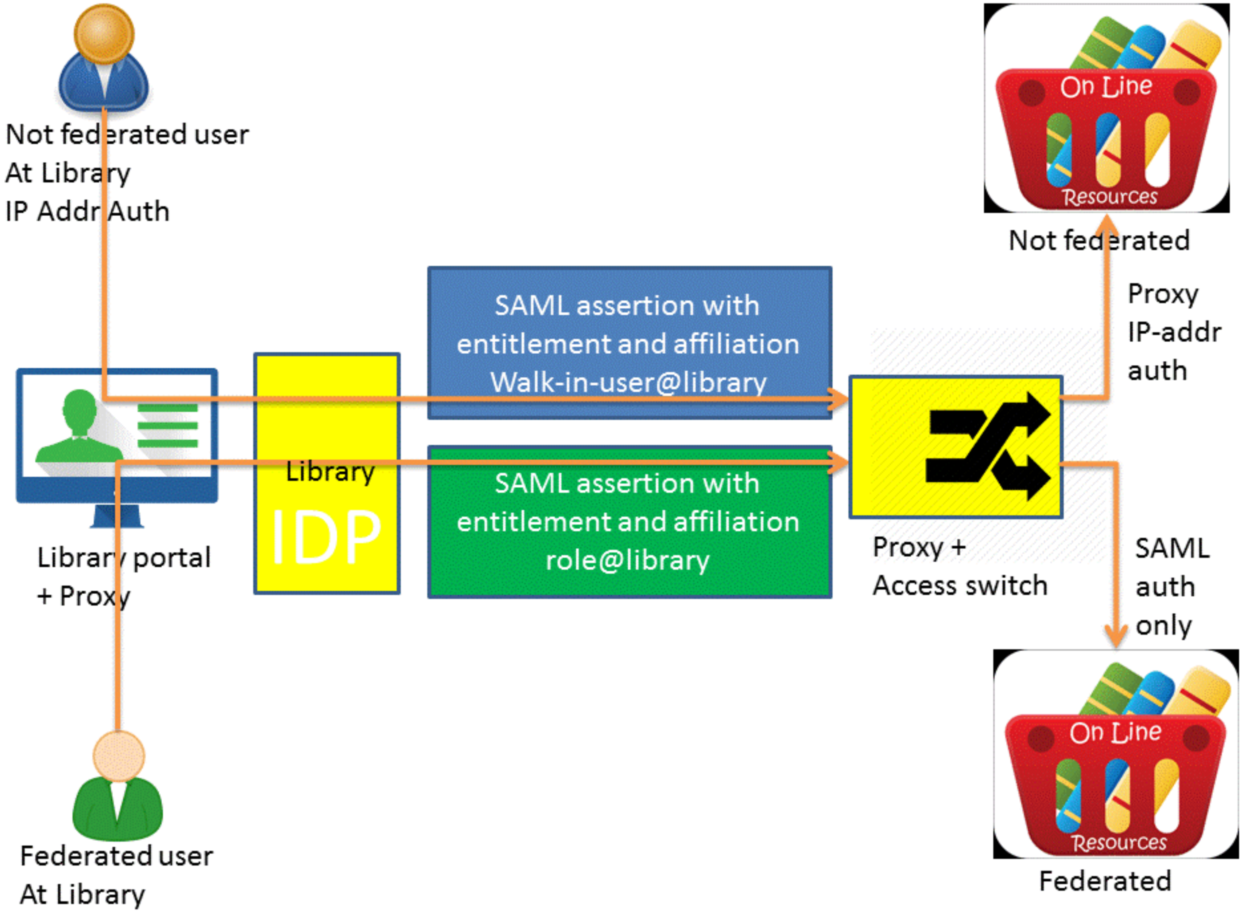
- Full validation of EZ proxy as Access Mode Switch
- Produced Install and Config guide to support Librarians in configuriong EZ-proxy:
- https://wiki.geant.org/download/attachments/58131750/guidaEzproxyShibboleth-en-2.pdf?version=1&modificationDate=1463672915747&api=v2
- Guide will be initial input for a dedicated training program for Librarians (---> NA2)

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

Portal allowing both IP and federated AuthN

Dealing with 1 Library (1 IDP)

Setting attributes based on IP info



Scenario 2

- Currently being implemented by Pete - Martin on OKEANOS resources
- Based on IP-based Authentication extension for Shibboleth IDP version 3
- DAASI has gained experience on IP based Shib IDP extension from past projects

Scenario 3:
“Super Walk-in” portal dealing with multiple libraries

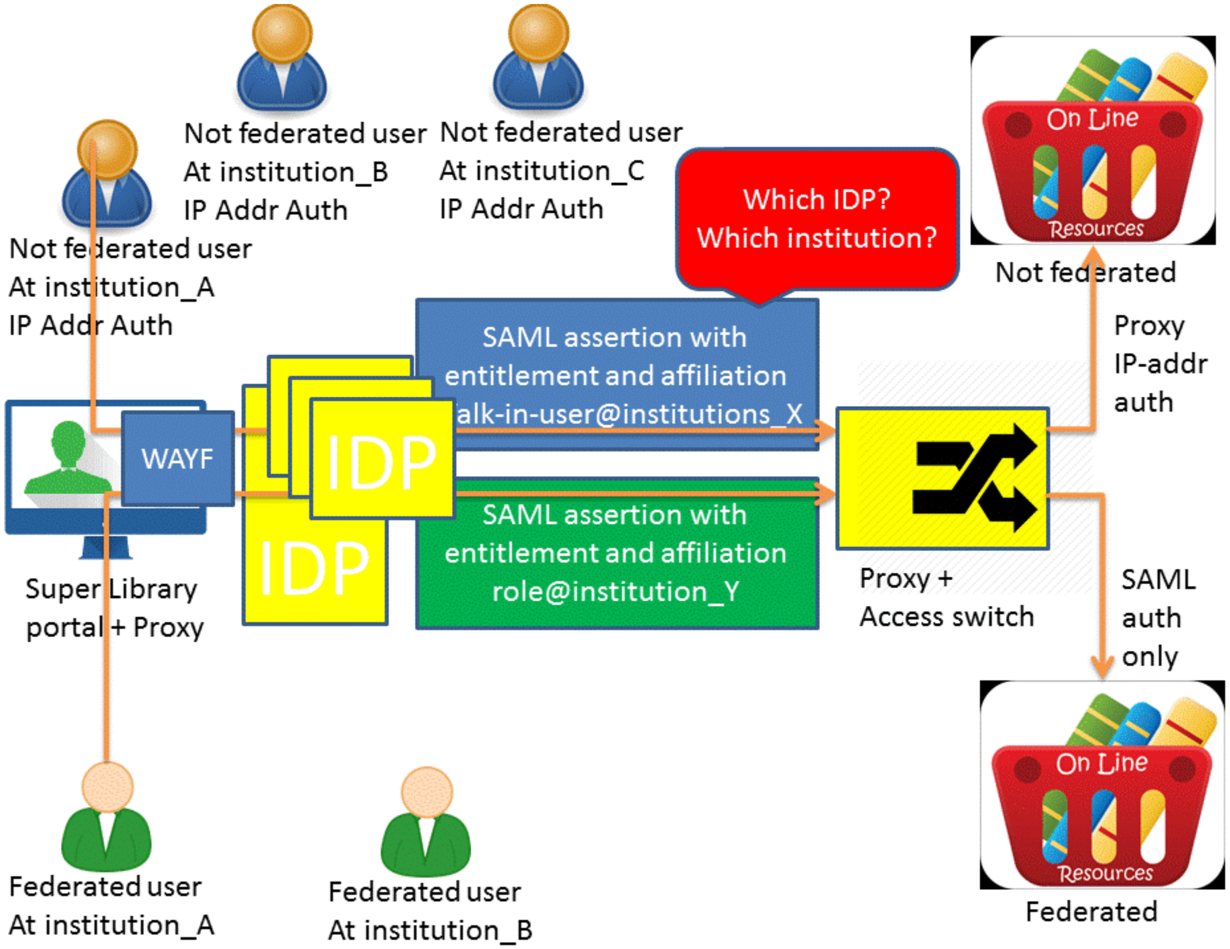
Portal dealing with many Libraries

Acting as User Interface

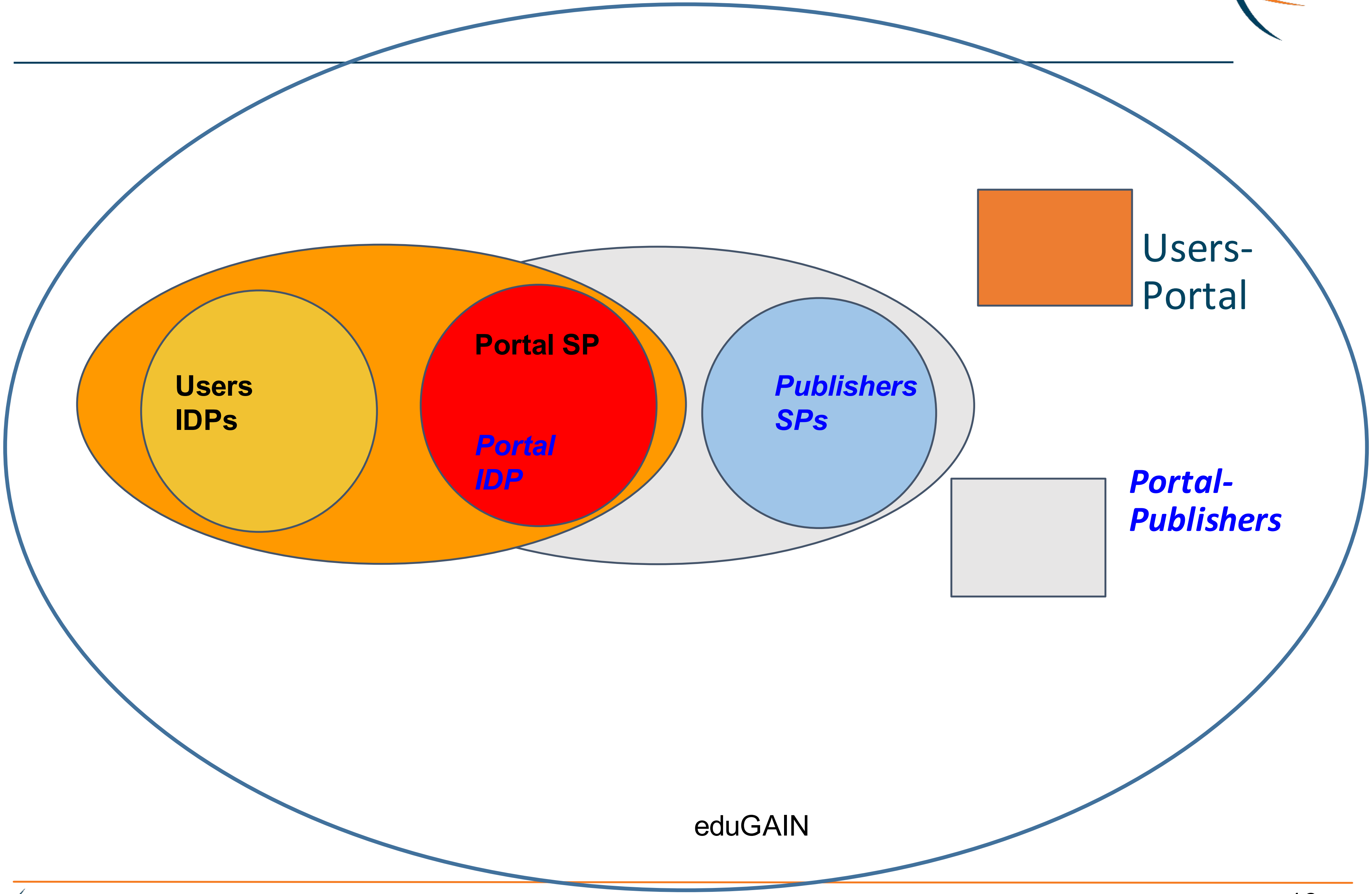
Publishers see IDPs selected by user

Portal is a Federation SP

Manages IP based info



Simplified Trust Model



Scenario 3 : Super Walk-In portal for many libraries

Additional features w.r.t. Scenario 1 and 2:

- Deals with multiple libraries
- Manages contracts centrally → Sets IP ranges for Libraries
- Enables both Authentication methods:
  - IP-based
  - Federated IDP
- Sets appropriate SAML Attribute based on IP-based info
  - ePSA = library-walkin@scope
  - ePE = staff, student, ….

Scenario 3: User Workflow

Users can own Federated IDs in a Library IDP or be walk-ins:

- Portal UI has a Federation SP component:
  - if in IDP , they log in on the portal selecting their IDP
  - if not, they are identified as Walk-in users @ library

- Once logged in, the portal act as a multiple connector:
  - a SSO proxy redirecting to publisher SP if users are federated towards federated SP presenting IDP released attributes
  - an IDP to SP releasing walk-in@scope (ePSA) to federated SPs for walk-in users (IP-based AuthN)
  - an IP proxy for all AuthN'ed users towards non-federated SPs

Scenario 3: Management Workflow

Libraries managers:

- log in to the portal
- set IP ranges (net/subnets) for IP based AuthN
- select which attributes they want the portal to release
  - matching IP based information
  - Eg. ePSA ePE
  - Attribute release can be SP-specific

AARC SA1
Pilots

Subtask SA1.1.3
Pilot #2 - Proxy Model for Library Consortia

Nicolas Liampotis
GRNET

3rd AARC General Meeting
24 May 2016, Utrecht

Pilot goals (I)

The main goal of this pilot is to showcase the benefits for a library consortium, namely HEAL-Link, joining a federation as an IdP/SP proxy. These benefits include:

allowing publisher contracts to be managed centrally by the consortium

easier to implement and manage than establishing trust relationships among IdPs and SPs (either bilateral or through a federation)

the consortium will retain control on the branding and policies

disconnecting the establishment of technical trust between the IdP and SP entities from the application of policies relating to contracts (publisher subscriptions etc.)

more precise and easier to produce statistics

Pilot goals (II)

Integrate with the other library pilot activities in order to investigate the possibilities in the proxy model to address library requirements relating to the use of:

- guest identities
- mixed federated and IP-based access

Pilot milestones

Deploy IdP/SP proxy and publish metadata to REEP ✔

Test login workflow using AARC DIY IdP and pilot SP entities ✔

The IdP/SP proxy has joined GRNET federation ✔

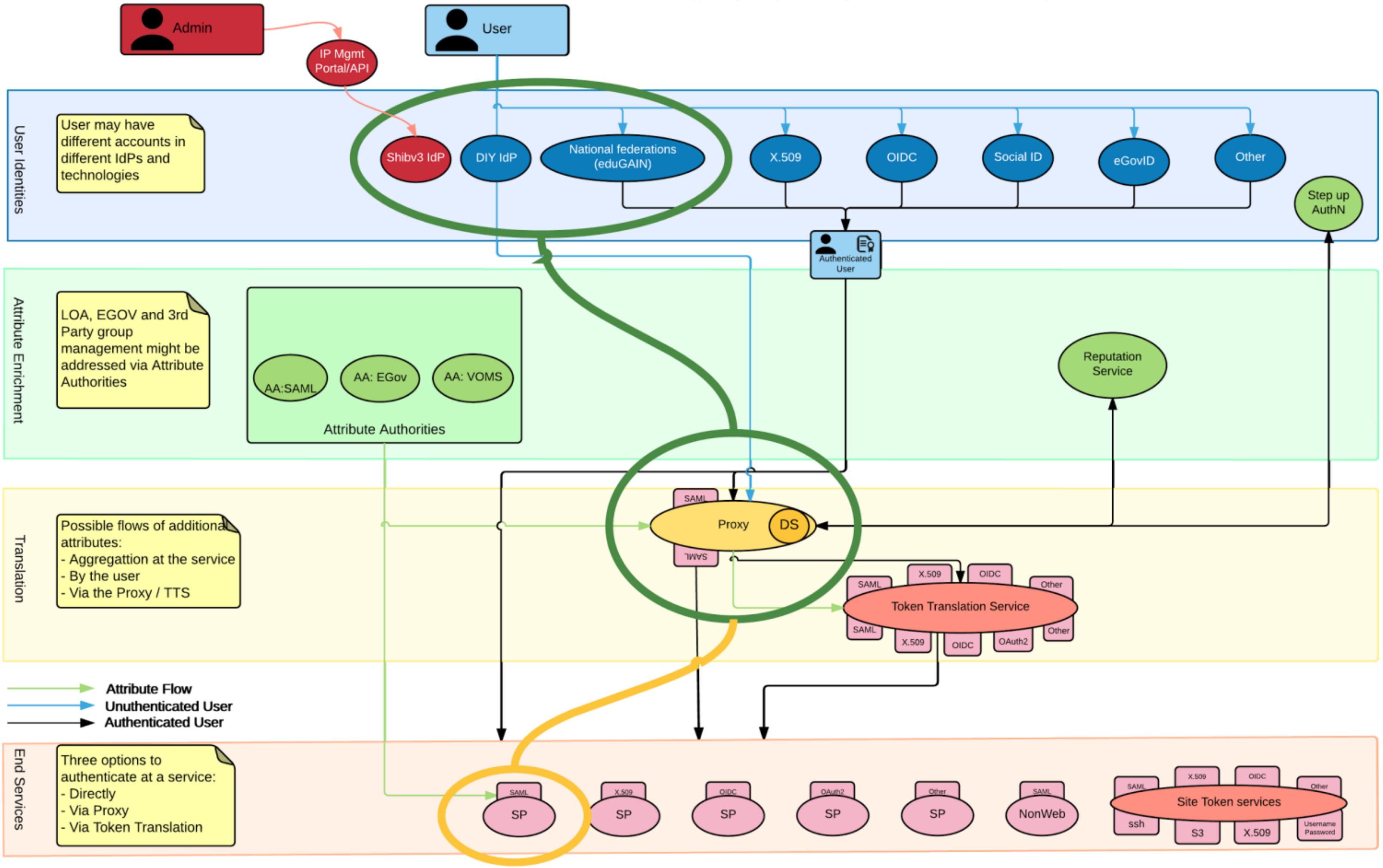
Test login workflow using production IdPs in Greece [WIP]

Federate IdP/SP proxy with at least one SP of a publisher (even demo/testing), who partners with HEAL-Link [WIP]

Test login workflow and access to content has been tested successfully.

AAI: The e-Infrastructure view

What is happening on top of existing Federation infrastructures today



Admin

IP Mgmt Portal/API

User

User Identities

User may have different accounts in different IdPs and technologies

Shibv3 IdP

DIY IdP

National federations (eduGAIN)

X.509

OIDC

Social ID

eGovID

Other

Step up AuthN

Authenticated User

Attribute Enrichment

LOA, EGOV and 3rd Party group management might be addressed via Attribute Authorities

AA:SAML

AA: EGov

AA: VOMS

Attribute Authorities

Reputation Service

Translation

Possible flows of additional attributes:
- Aggregattion at the service
- By the user
- Via the Proxy / TTS

SAML

Proxy

DS

SAML

SAML

X.509

OIDC

Other

Token Translation Service

SAML

X.509

OIDC

OAuth2

Other

Attribute Flow

Unuthenticated User

Authenticated User

End Services

Three options to authenticate at a service:
- Directly
- Via Proxy
- Via Token Translation

SAML

SP

X.509

SP

OIDC

SP

OAuth2

SP

Other

SP

SAML

NonWeb

SAML

X.509

OIDC

Other

Site Token services

ssh

S3

X.509

Username Password

Pilot extension: Mixed federated and IP-based access

Adding support for Library (Walk-In) users based on IP address would require:

- Interconnecting proxy to Shibv3IdP with IP-based AuthN plugin
- Allowing admin staff of consortium and member libraries to manage IP address ranges / eduPersonEntitlements via:
  - Web portal
  - REST API

Next Steps

- Proceed with implementation of Scenario 2- 3 for Pilot#1
  - Finalize/Test scenario 2
  - Enlarge discussion to Libraries and publishers about Scenario 3
  - Expand carefully the design into further detail for Scenario 3
    - Splitting admin and user profiles/roles
      - requires assessment of possible options/solutions
  - Test in multiple federation scenarios

- Proceed with workplan for Pilot#2
  - test in production
  - add support for walk-in users