Authentication and Authorisation for Research and Collaboration

CTA Pilot Report

Authentication and Authorisation for Research and Collaboration

Fabio Vitello, Alessandro Costa, Eva Sciacca (INAF)

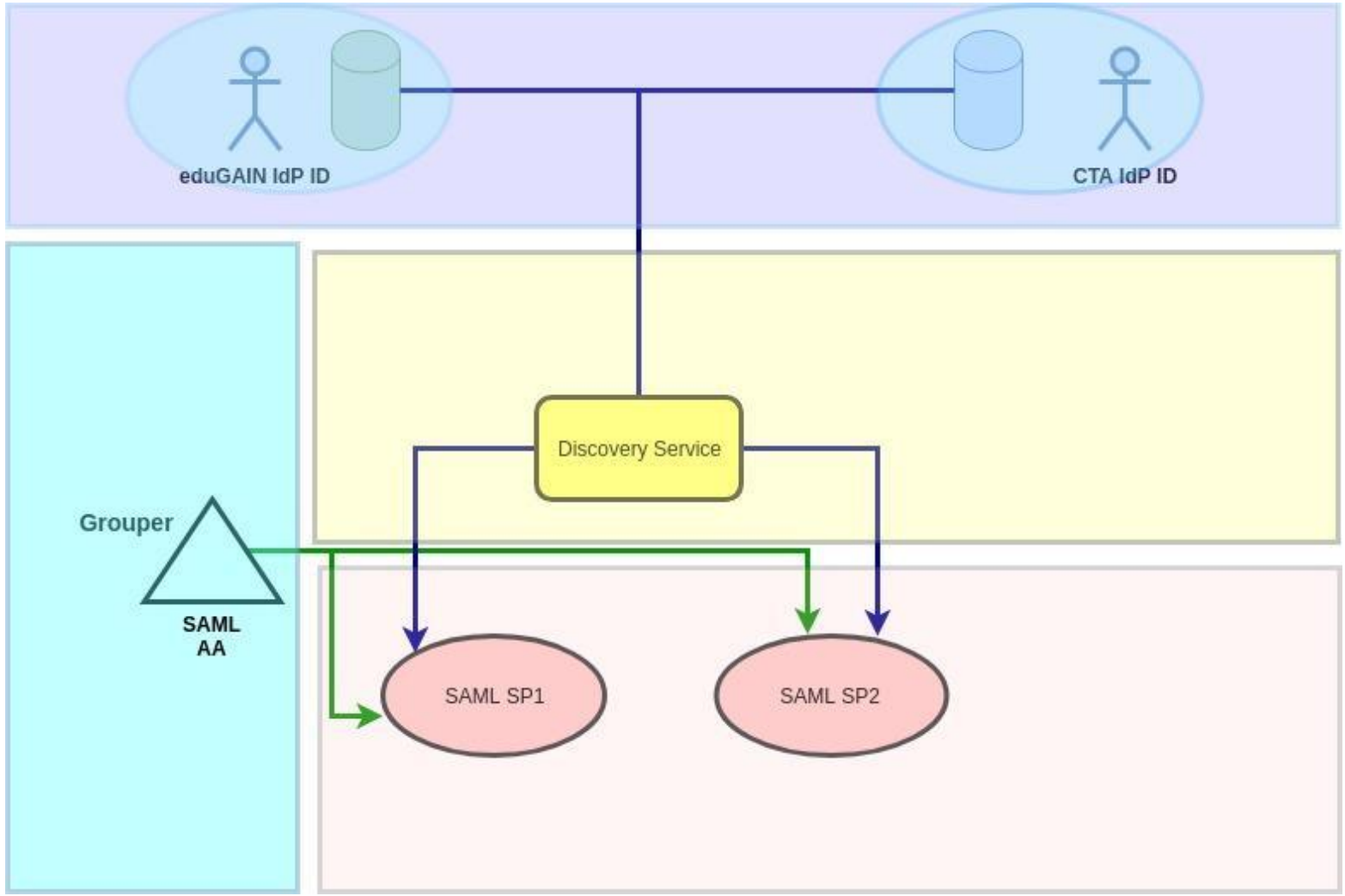
With input from Barbara Monticini, Mario Reale, Davide Vaghetti and Jouke Roorda

AARC2 All Hands Meeting Athens
April 12th 2018

Outline

- INAF-CTA AAI
- Requirements
- AARC All Hands Meeting, November 2017
- CTA Pilot Use Cases

Before AARC2: INAF-CTA AAI



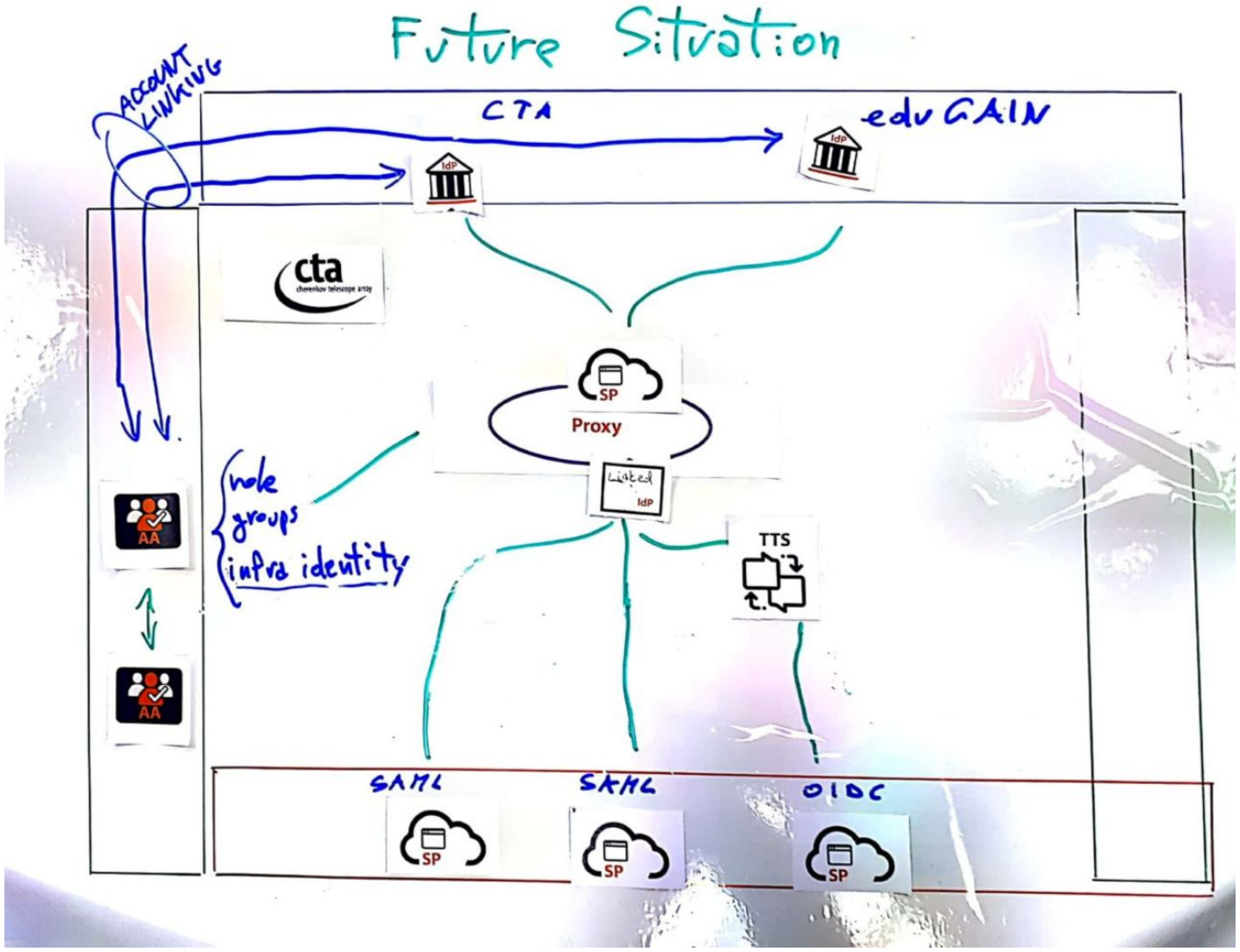
- **Authentication**
  - based on eduGAIN inter-federation and on a centralized CTA IdP.
- **Attribute authority**
  - Using Grouper.

CTA Requirements

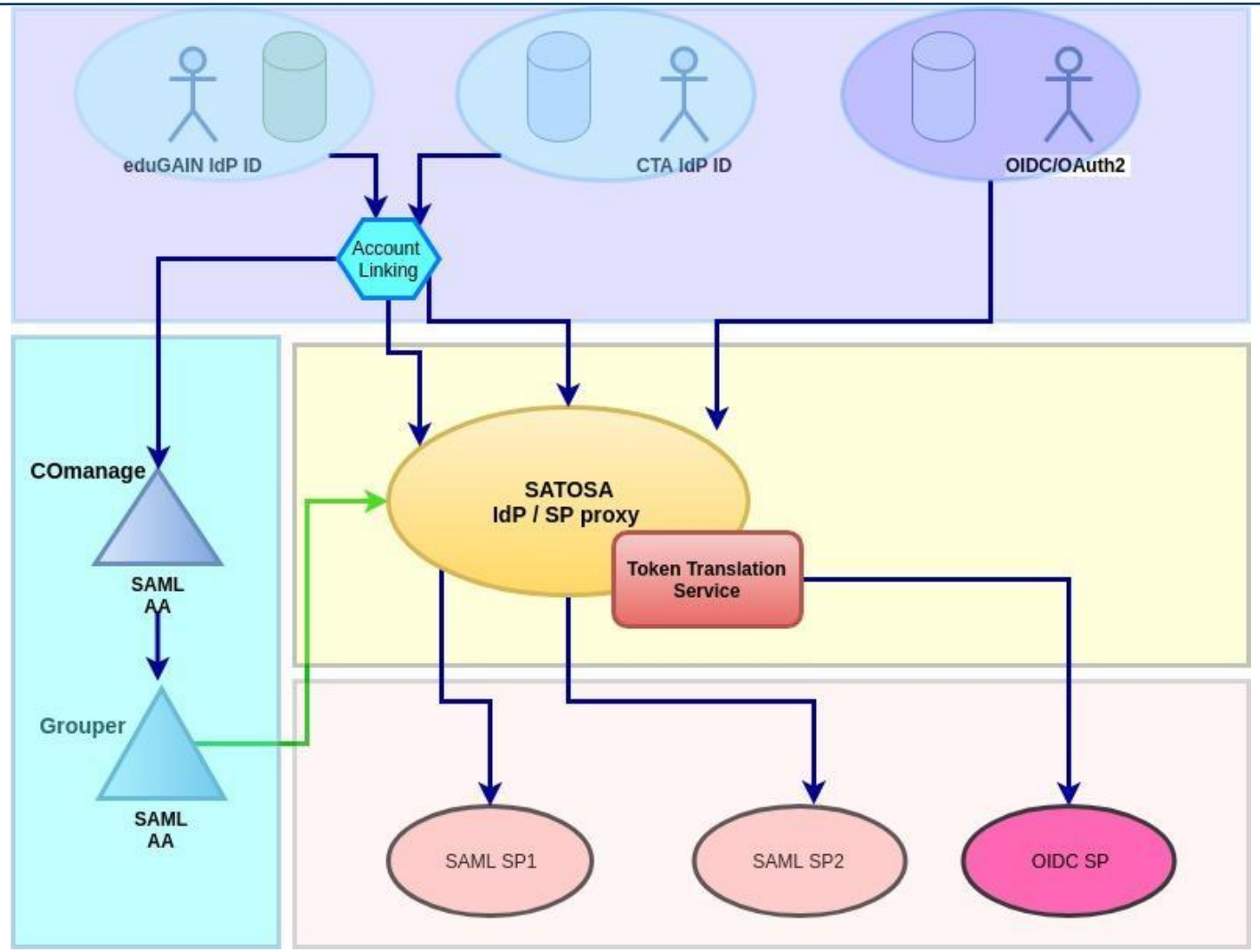
The goal of this pilot is to provide a non-invasive solution to simplify access to CTA services from eduGAIN and the CTA idp. The Pilot meets the requirements

- Implement a user-friendly user enrollment flow;
- Manage both CTA and eduGAIN identities for users;
- Link identities under administrator approval;
- Include guest identities (Social IDs) - [light requirement]
- Support OIDC RP - [light requirement]

AARC All Hands Meeting November 2017



AARC All Hands Meeting November 2017



AARC2 CTA Pilot Use Cases

A CTA user willing to reach a CTA service provider can:

1. Be an existing user on the CTA catch-all IdP
   - existing both in COmanage and Grouper
2. Be a brand new user for CTA existing in eduGAIN not in CTA catch-all IdP
   - Not existing in Grouper and in COmanage
3. Be an existing user on the CTA catch-all IdP with also an eduGAIN identity
   - Wants to link identities

UC1: Existing user on the CTA catch-all IdP

1. A user wants to login to a CTA SP.
2. He/She gets redirected to the CTA IdP/SP PX.
3. He/she authenticates on the CTA IdP - IdP asserts successful AuthN to the PX and ships along basic set of attributes.
4. Check the ID in AA
5. If these are enough to AuthN on the SP, the PX forwards to SP successful AuthN response
6. User manages to login onto the CTA SP.

Before AARC2:

- Users were provisioned directly from CTA LDAP into Grouper

Within AARC2:

- Users are provisioned from CTA LDAP to COmanage provisioning Grouper
- Proxy

UC2: New user for CTA existing in eduGAIN

1. An eduGAIN user wants to login to a CTA SP;
2. If is the first access (=totally unknown to the system):
    i. He/She is invited to enroll into COmanage;
    ii. User information are provisioned from COmanage to Grouper;
3. He/She gets redirected to the CTA IdP/SP PX.
4. He/she chooses his/her IdP while being presented to a list of eduGAIN IdPs by the Discovery Service on the PX.
5. He/she authenticates on the Home Org IdP - IdP asserts succesful AuthN to the PX and ships along basic set of attributes.
6. Check the ID in AA or not
7. If these are enough to AuthN on the SP, the PX forwards to SP successful AuthN response
8. User manages to login onto the CTA SP.

UC3: Existing user on the CTA catch-all IdP with also an eduGAIN identity

1. A CTA Idp user with already enrolled eduGAIN identity (see UC2) wants to link his/her identities;
2. He/She requests to the administrator to link his/her identities;
   a. The administrator manually links both Org identities for the user in a single COPerson;
3. The User wants to login to a CTA SP;
4. He/she chooses his/her IdP while being presented to a list of eduGAIN IdPs or CTA IdP by the Discovery Service on the PX.
5. **SATOSA microservice queries COmanage (using API) in order to discover if the user have multiple identities**
   a. **If yes "translate" the eduGAIN eppn into the CTA eppn**
6. He/she authenticates on the IdP - IdP asserts succesful AuthN to the PX and ships along basic set of attributes.
7. If these attributes are enough to AuthN on the SP, the PX forwards to SP successful AuthN response
8. User manages to login onto the CTA SP.

TODO

- Solve SATOSA <-> CTA IdP issue: *InvalidSecurityConfiguration*;
- Write SATOSA “translator” Microservice (UC3);
- Can we dismiss Grouper and use only COmanage as AA?

Thank you

Any Questions?

fabio.vitello@inaf.it

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).