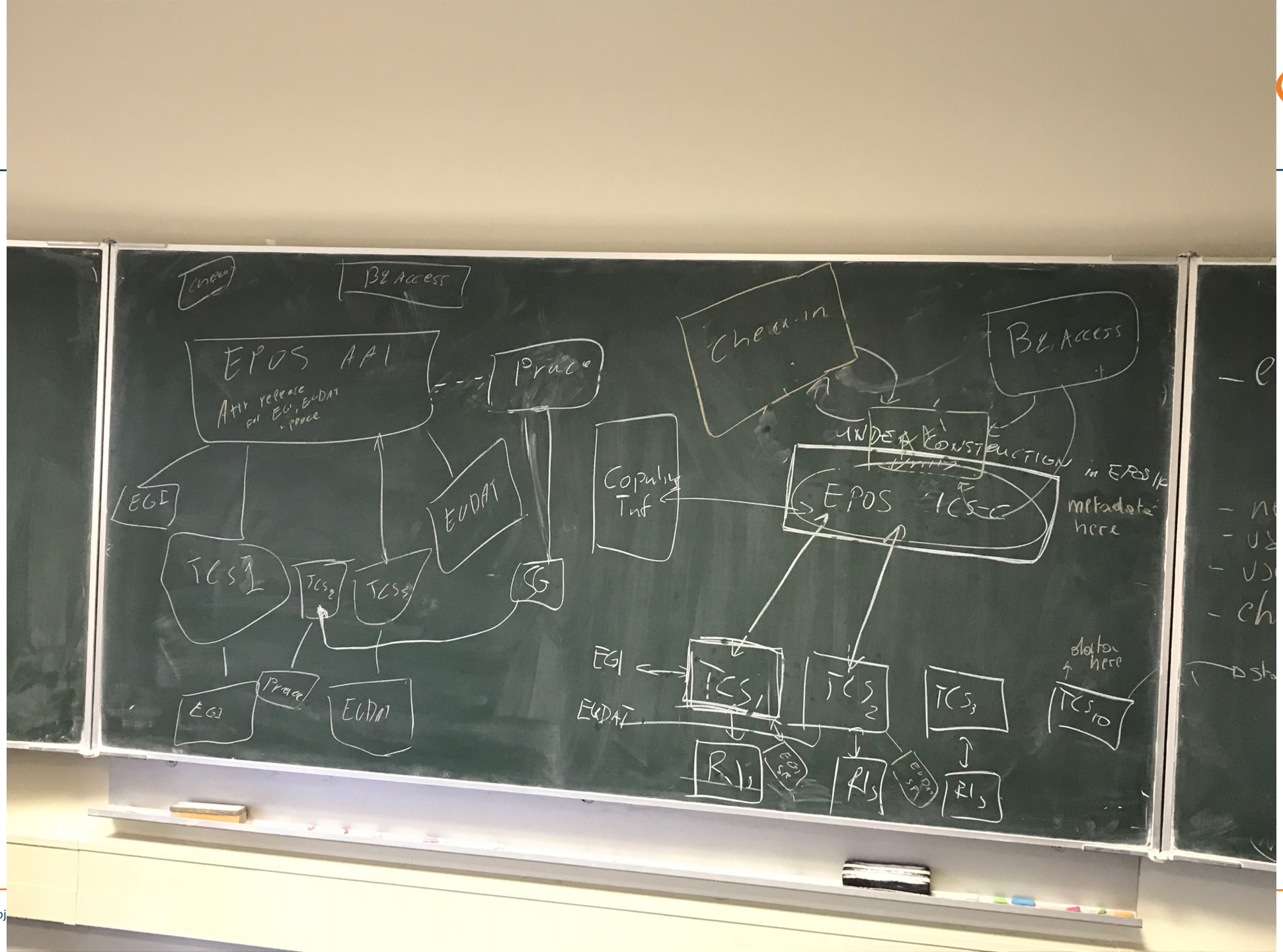
Authentication and Authorisation for Research and Collaboration

SA1 EPOS

Authentication and Authorisation for Research and Collaboration

Name
Mariusz Sterzel
ACC Cyfronet AGH

AARC2 meeting, Athens
10-13.04.2018


Check-in
B2Access
EPOS AAI
Attr. release for EGI, EUDAT, Prace
Prace
EGI
EUDAT
TCS1
TCS2
TCS3
G
Coupling Inf
Check-in
B2Access
UNDER CONSTRUCTION
EPOS TCS-C
in EPOS IP
metadata here
EGI
EUDAT
TCS1
TCS2
TCS3
TCS10
slot for here
RI1
RI2
RI3

EPOS Pilot

Actions for next 6 months:

Obstacle – EPOS ICS-C „under construction”

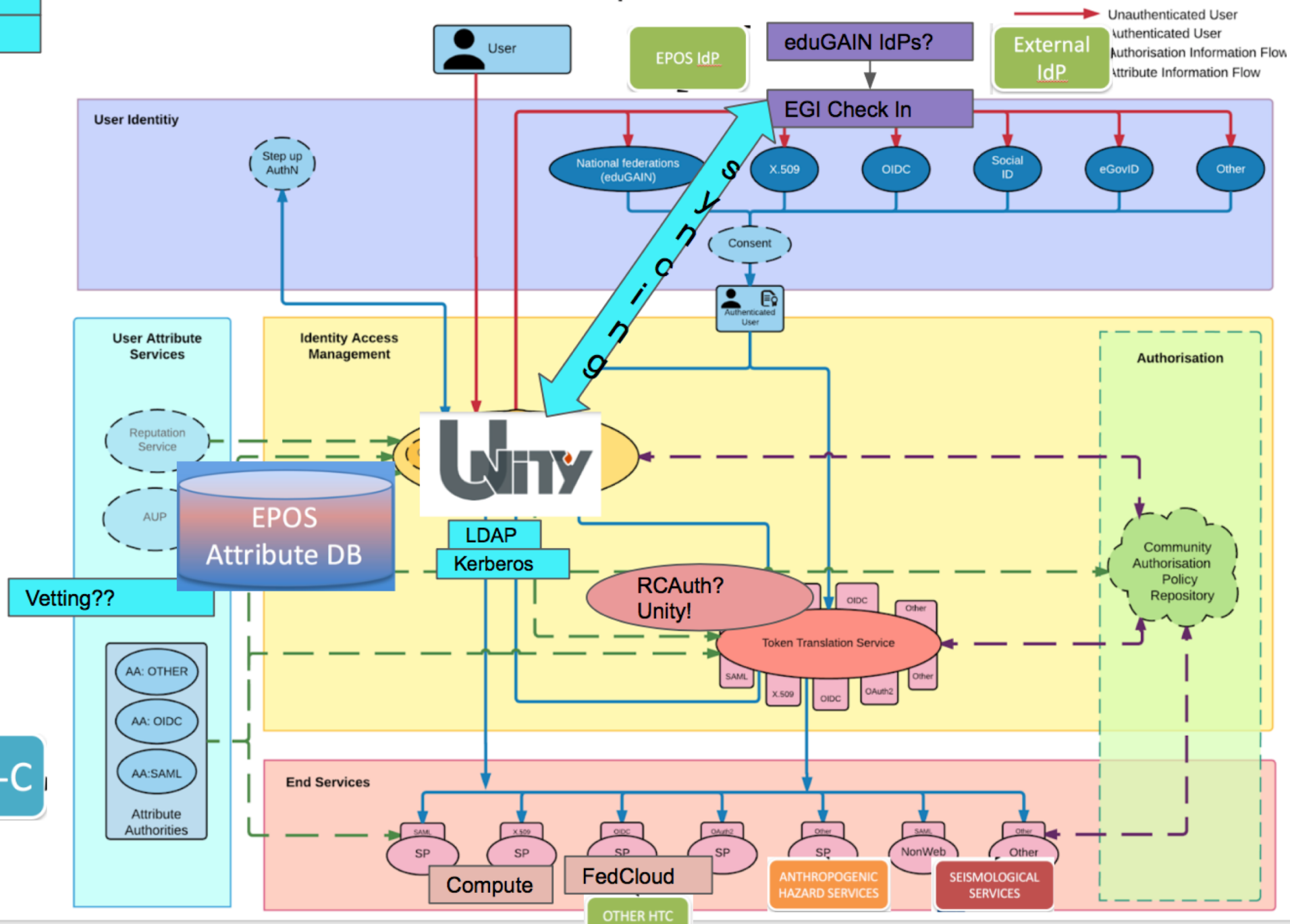
- Set up local EPOS IdP service
- Bind it with the pilot
- Start integrating TCSs (the two with binds to EGI and EUDAT) with the pilot

Training

- Done ;)
  - During EPOS All Hands Meeting
  - 30+ participants
  - Various audience
  - Andrea will provide more details tomorrow

AARC Blueprint Architecture

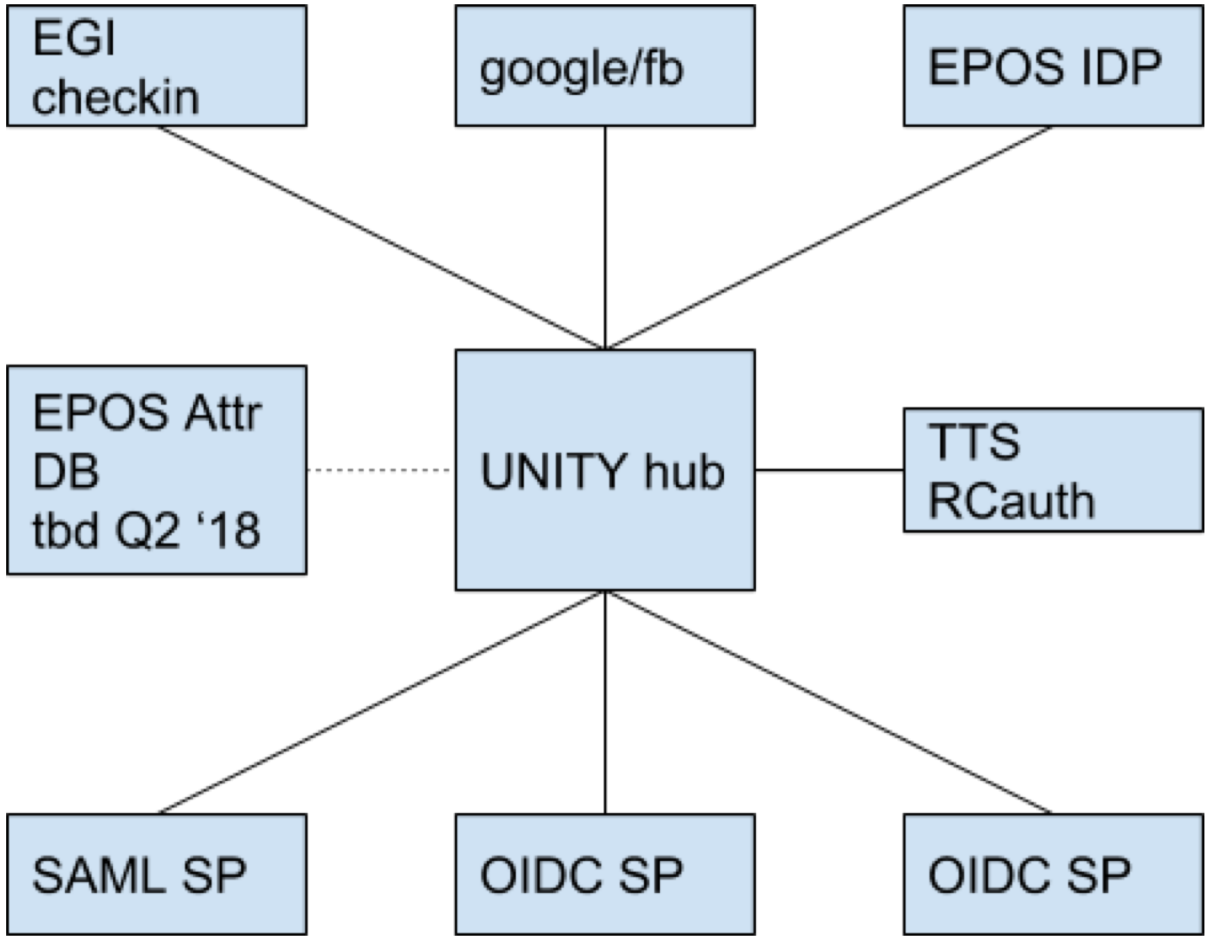
COmanage
PERUN



Utrecht meeting

- General discussion concerning the pilot
  - Minutes: https://docs.google.com/document/d/1_y0LyWNxw4batEDU-3Y9Bmk5oldwDyrjkACwRsWwu28
  - Architecture details
  - Attribute DB
  - Data Access
- Goals / KPIs for the pilot:
  - USers from two TSCs: Seismological and Antropogenic Hazards
  - Authenticate only once
  - And use the services (in a simple scenario pull data from one TCS and store it in the second one)
- PR stuff has to go first (done), followed by actual pilot implementation (in development)
- EPOS AAAI Sustainability

Paul's summary ;)



AAAI for TCS web-services: Why?

- Security: open WS are vulnerable of any attacks from any server on the Planet
  - How many request per minute your service can stay?
  - ICS-C is client (browser) application – not possible to restrict access by IP
- Accounting, Virtual Access: collect data who is using services
  - Currently ICS-C is not able (by architecture) to collect such data
  - E.g. Counting (unique) users require identification
- Access Policy: any formulation of data access policy require a tool to execute it
  - E.g. limitation to universities, EPOS users

AAI for TCSs: What kind of solutions?

- TCS services are implemented in various framework, some operated as legacy implementations

  (ICS team cannot provide support for all)

  → AAAI need to be language/framework agnostic

- ICS should act on services in the same way

  → Adding AAAI to request should be possible to consider as option

Solution: Assumptions

- All request from ICS will have HTTP header with valid oAuth2 *token* that can be (optionally) validated in AAAI service

```
Authorization: Bearer Vd5MDzhpn9-xCeDWnjqWeEJI9baIS8bRvWsA7RRrjtM
```

- Web-services proxy: extra module that can be installed and configured for any legacy service, that
  - Validate token
    - PASS if token is valid
    - FORBIDEN (HTTP 403) when token is not valid
  - Provide additional user attribute set as HTTP header

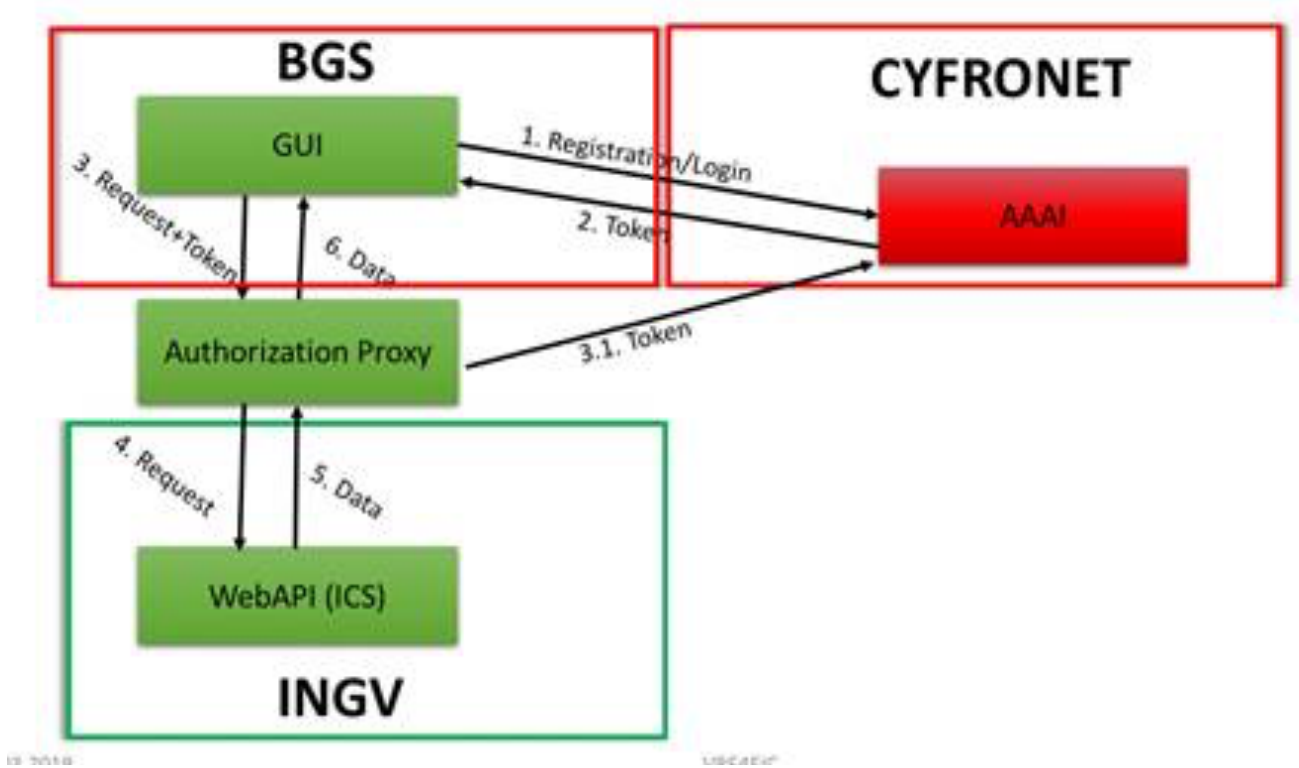
Solution: Implementation

- NGINX module to enable proxy functionality
  - LUA script (LUA script support required)
  - Addition headers:
    - `X-Auth-UserId` – persistence identifier
    - `X-Auth-Scope` – user attributes (JSON format)
  - Hide service from public network
- How to:
  - https://gist.github.com/mkasztelnik/58bd89d348a8a28d7802d3eed4137768#file-compile_openresty
- Testing:
  - Login to ICS-C
  - Copy token (visible in “profile”)

```
export TOKEN=token_payload
curl -v --header "Authorization: Bearer $TOKEN"  http://my.proxy.url
```

Solution: Validation

- Secured WEBAPI by EPOS AAAI and NGIX proxy



Where we are with AAAI?

- Technology for A&A
  - Standards: fixed
  - Tools: implemented, documentation needed
  - Instalation ready
  - Solution for TCSes webservices – ready and tested
- Policies:
  - Authentication: TODO
  - Authorization: TODO
- Accounting:
  - Collection of data technically possible when webservice uses proxy
  - Rest: TODO

AAAI Plans – March 2018

- Create proposal for authorization attributes profiles
- Enable mechanism to collect all required attributes
- Support TCS WS integration with “AAAI Proxy” (or other type of integration)
- Integrate authentication methods with TCSes (to enable existing users to utilise EPOS)
- Prepare proposal to manage GDPR related issues on AAAI level