
CERN

WLCG – FIM4R Update

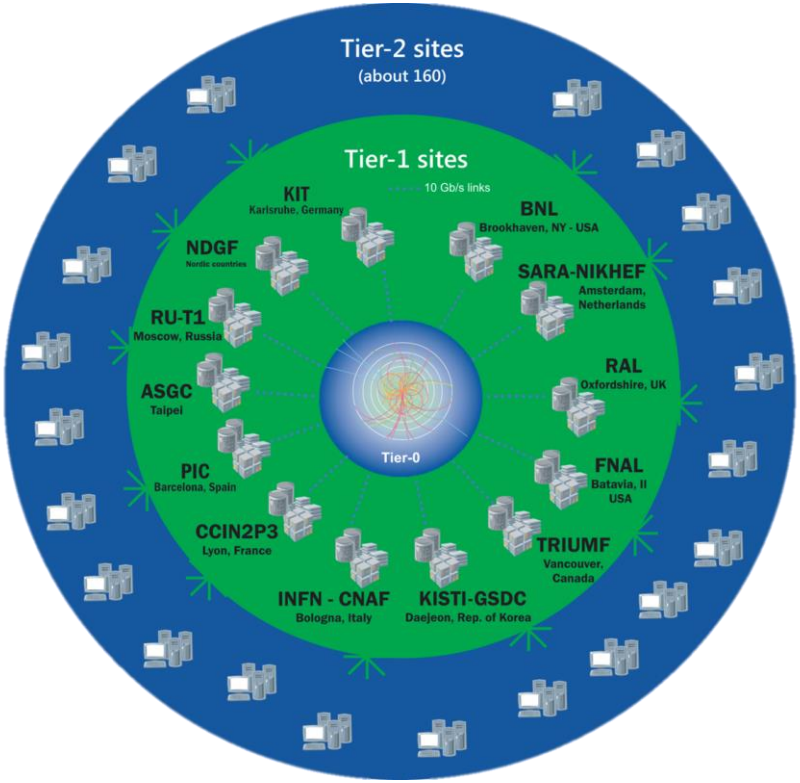
Hannah Short, CERN Computer Security

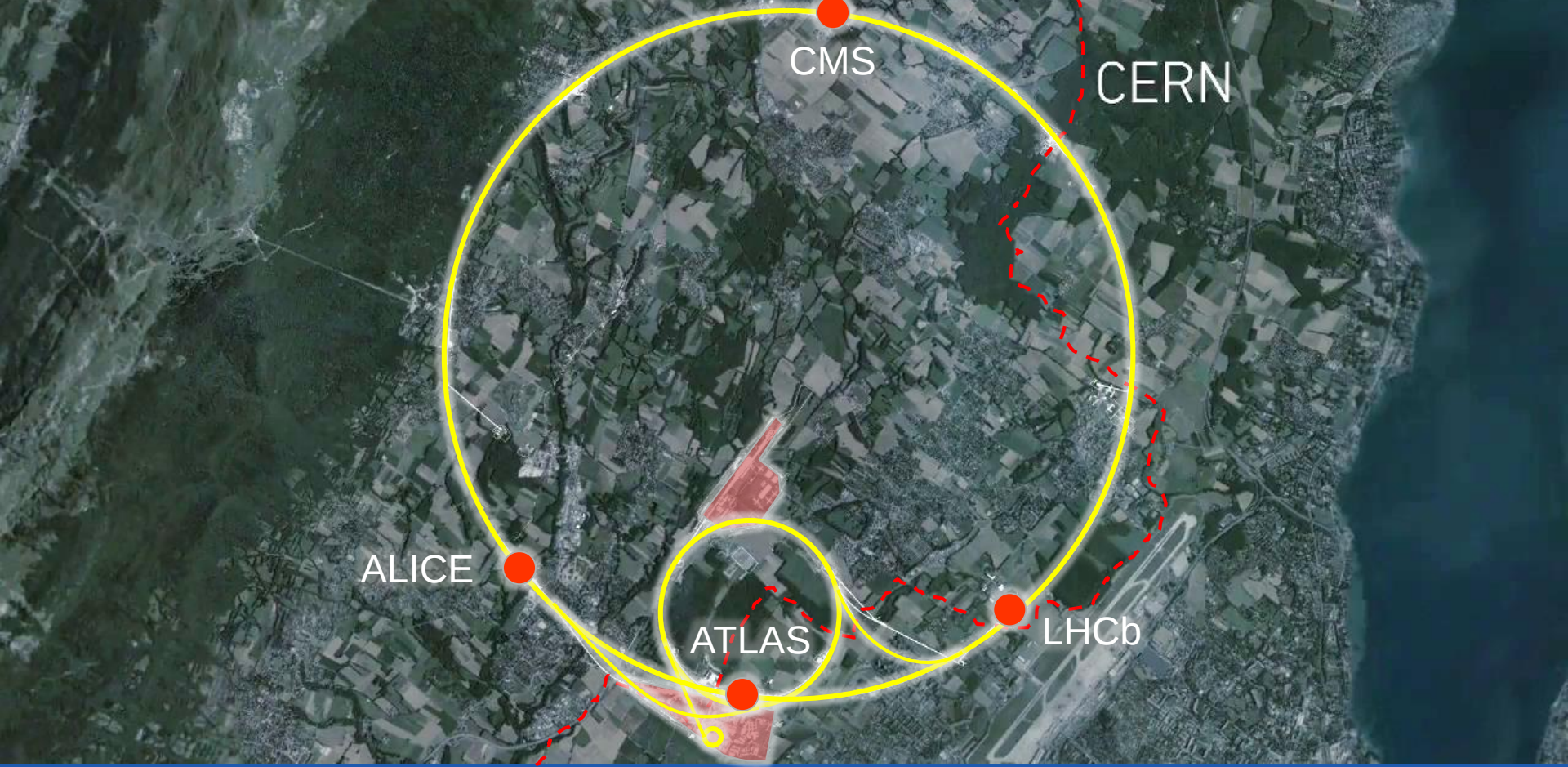
Agenda

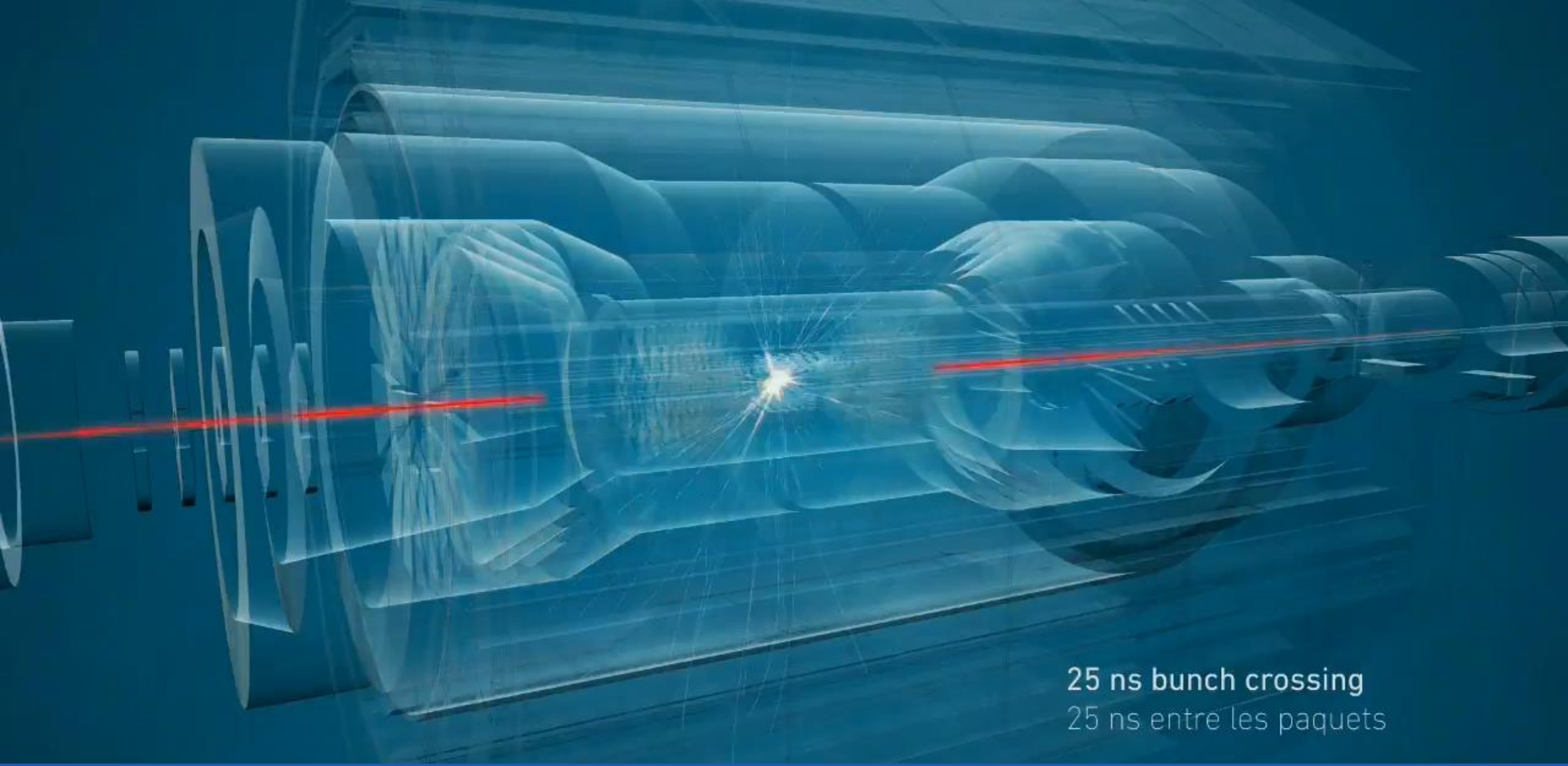
- WLCG Status
- Big challenges
- Current activities

WLCG

- High Energy Physics Computing Infrastructure
- Grid, used by > 15000 scientists for > 10 years

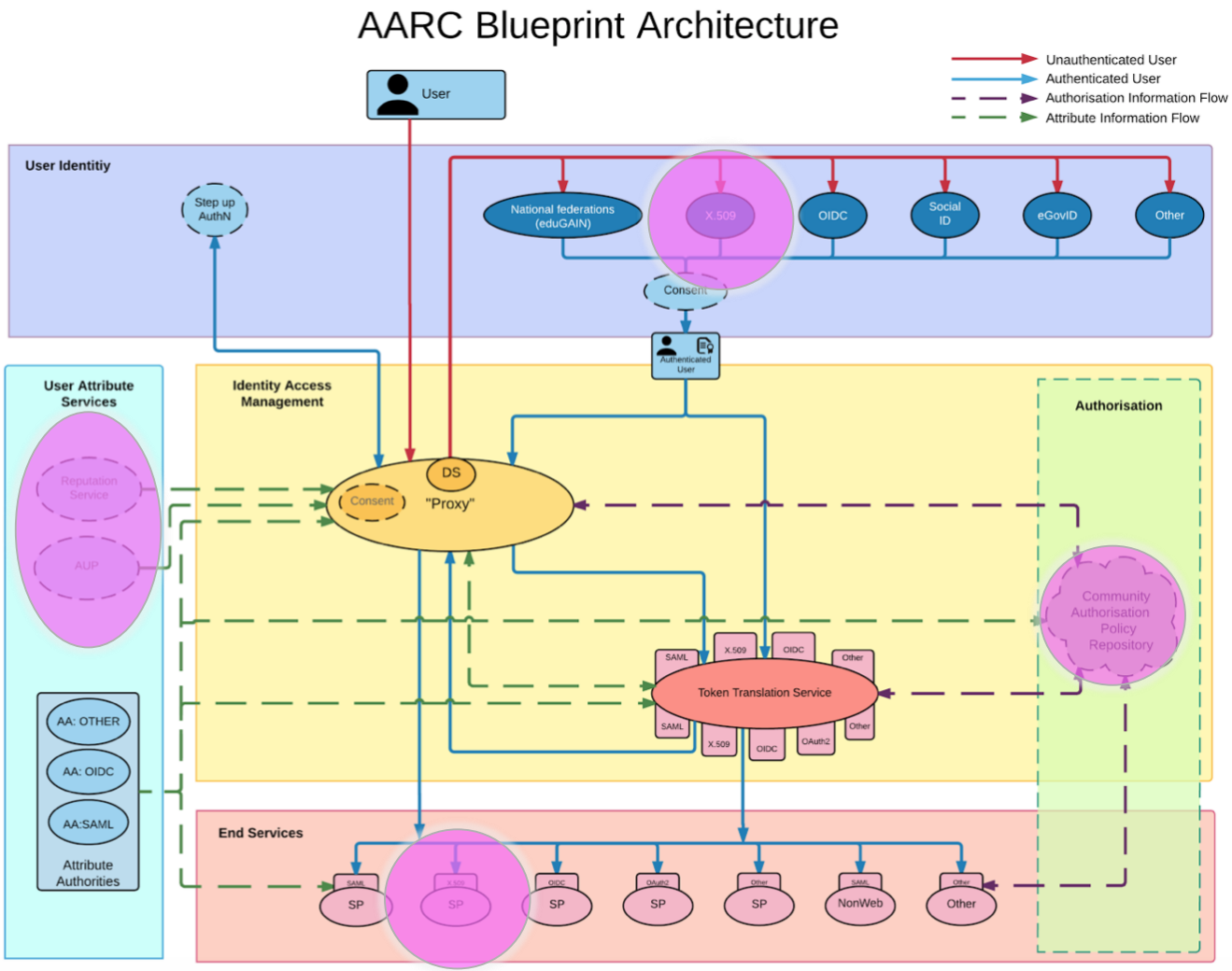



CMS
CERN
ALICE
ATLAS
LHCb


25 ns bunch crossing
25 ns entre les paquets

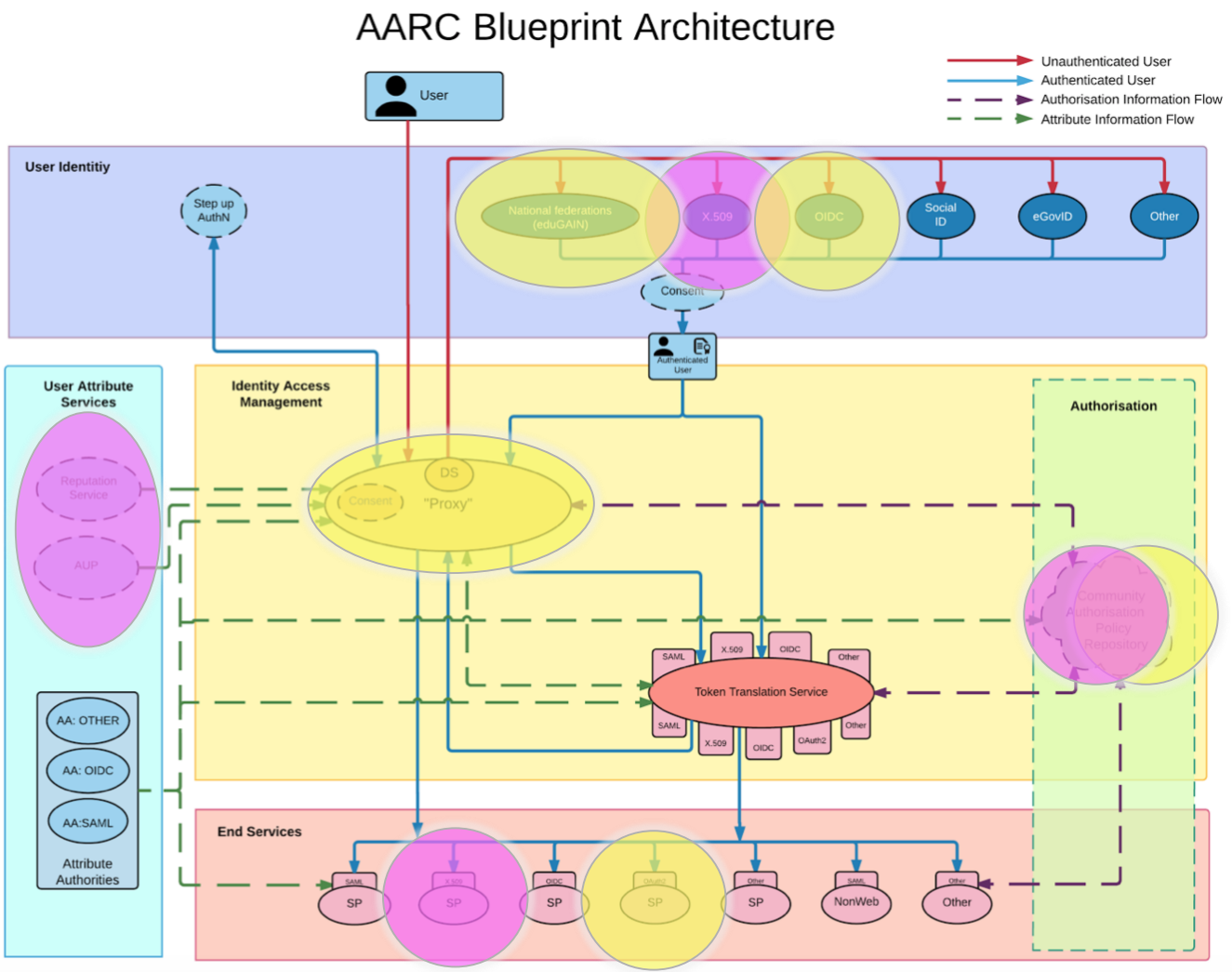
Before

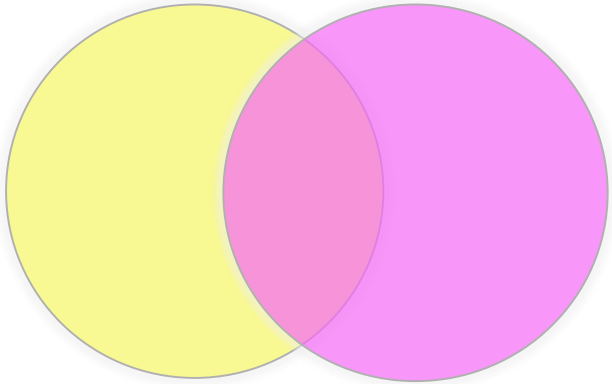
- X509 certificates
- Production > 10yrs
- Authorisation managed by VOMS
- Identities vetted by CERN



Now

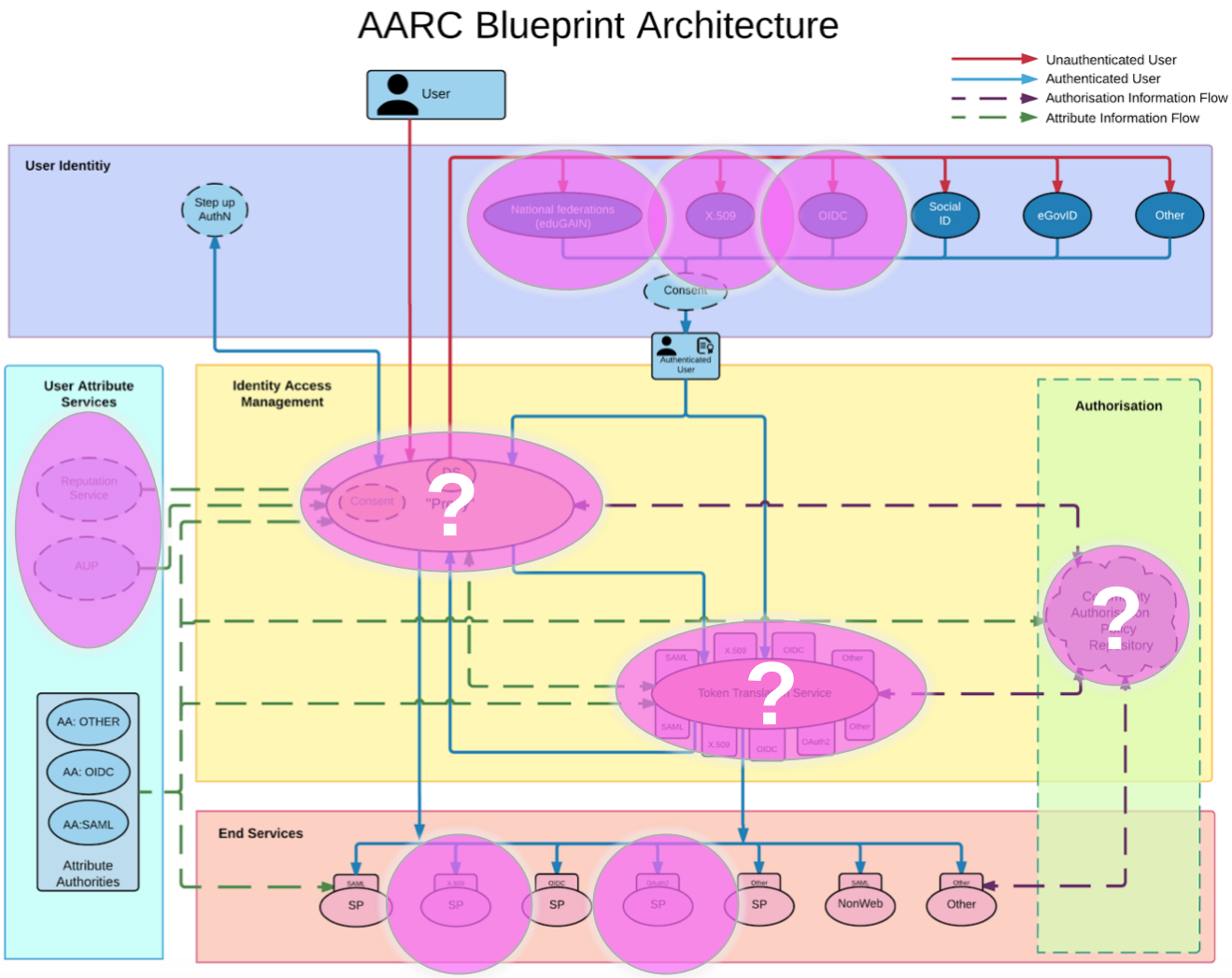
- WLCG
  - X509 certificates
  - Authorisation managed by VOMS
  - Identities vetted by CERN
- CERN
  - SAML + OIDC
  - Authorisation managed by e-groups (email)
  - No Identity Vetting process





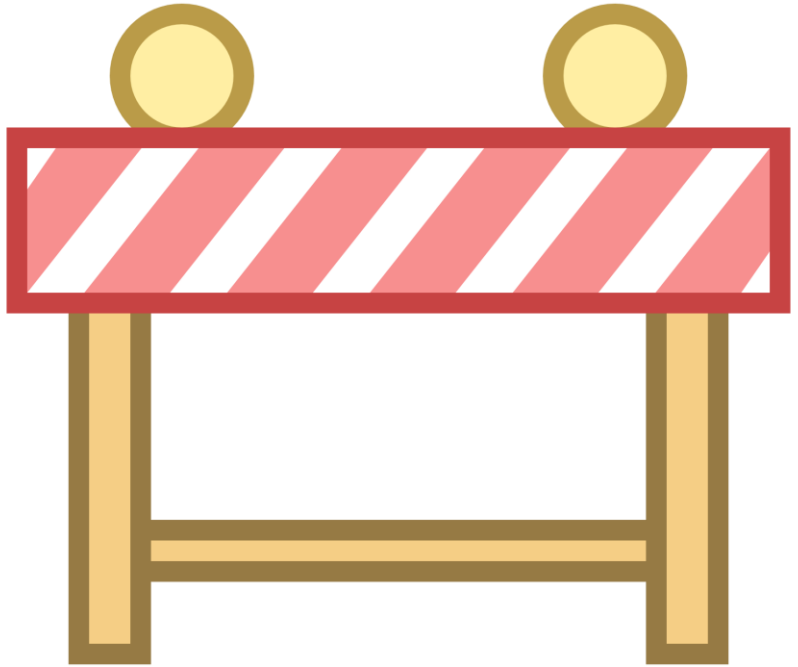
After

- X509 + SAML + OIDC
- Identities vetted by CERN
- Authorisation managed by??
- Token translation managed by??



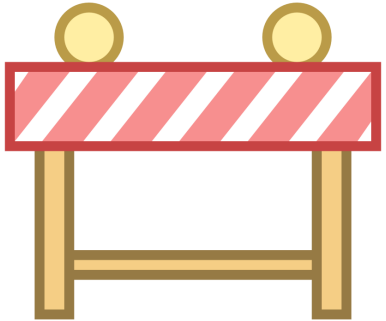
Road blocks

- Proxy
- Authorisation
- Token Translation
- Real command line



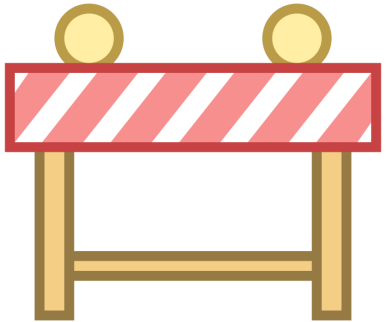
Proxy

- ADFS is unable to fill our requirements (surprise!)
- A replacement MUST cover
  - Kerberos
  - Certificates
  - SAML
  - OIDC
  - Username/Password
  - > 2,000 IdPs
  - > 15,000 SPs
  - Arbitrary AuthZ integration
- Any suggestions??? ☺



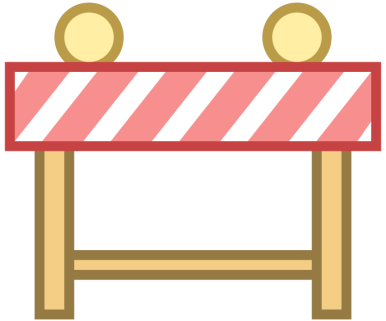
Authorisation

- VOMS
  - Registration only possible with x509
  - Links by email to CERN's identity vetting process, may need to be tweaked
- Alternatives?



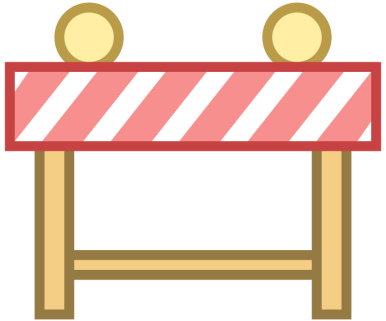
Token Translation

- Currently have a pilot with STS
  - Unmaintained
  - Unused
  - Depends on VOMS
- Other options exist, e.g. WATTS



Real Command Line

- No, not generating a short term certificate for the user and making them handle it
  - (Although this is a nice workaround!)
- Either
  - Move services behind web portals
  - Be clever and find a native approach



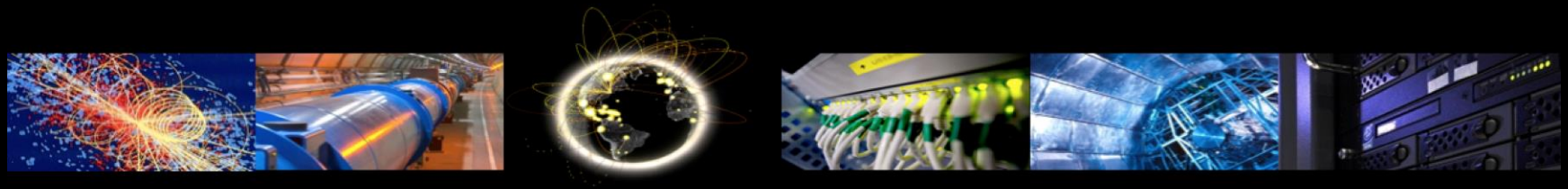
What are we doing about it?

- WLCG AuthZ WG
  - Particularly important given Globus Toolkit end-of-life
- AARC2 Pilot

WLCG Auth WG Overview

Valsan*, Short, Wartel

July 12th 2017



Motivation

- Evolving Identity Landscape
  - User-owned x509 certificates -> Federated Identities
  - Federated Identities linkage with existing VOMS authorizations not supported
  - Maintaining assurance and identity vetting for federated users not supported
- Central User Blocking
  - Retirement of glexec removes blocking capability (& traceability)
  - VO-level blocking not a realistic sanction
- Data Protection
  - Tightening of data protection (GDPR) requires fine-grained user level access control

Plan

1. Identify limitations of current system
2. Understand current system usage
3. Identify solution
   - Enhance current system, or,
   - Implement new system

AARC2 Pilot

- TBD

www.cern.ch