Authentication and Authorisation for Research and Collaboration

The future of Federated Access within WLCG

Authentication and Authorisation for Research and Collaboration

Hannah Short

IT-DI-CSO

CERN

GDB, CERN

13 January 2016

Contents

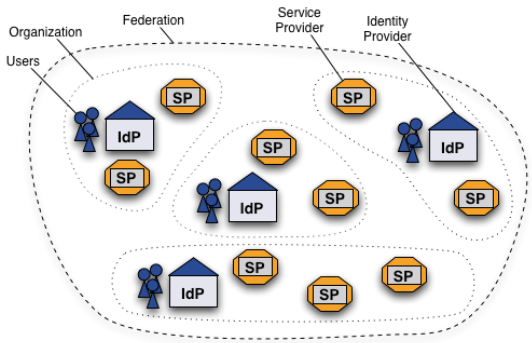
What is AARC?

- 2-year EC-funded project
- Objective is to design an integrated cross-discipline AAI (Authentication and Authorisation Infrastructure) framework
- CERN is leading
  - Security Incident Response Framework
  - Training and outreach for Services within WLCG
- https://aarc-project.eu

The AARC vision is to create a future in which e-Infrastructures and new research collaborations cooperate seamlessly on top of a scalable and interoperable AAI.

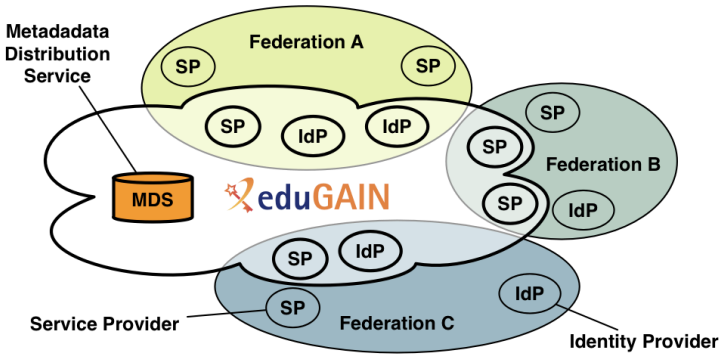
The benefits of federation

- More accurate provisioning for new users
  - The home organisation is responsible for the account and can typically provide the greatest assurance of the identity and quality of personal data
- Reduced account maintenance
  - Decreased liability for weak or re-used passwords
  - Significant streamlining in administrator and help desk effort in managing accuracy of user database
- Minimal bilateral agreements between participants
  - Common, federation-wide policies can be leveraged
- Increased collaboration
  - CERN can both expand the number of services available to its users, and grow its own user base



CERN belongs to the Swiss Federation, SWITCH
https://www.switch.ch/aai/about/federation/

The benefits of inter-federation

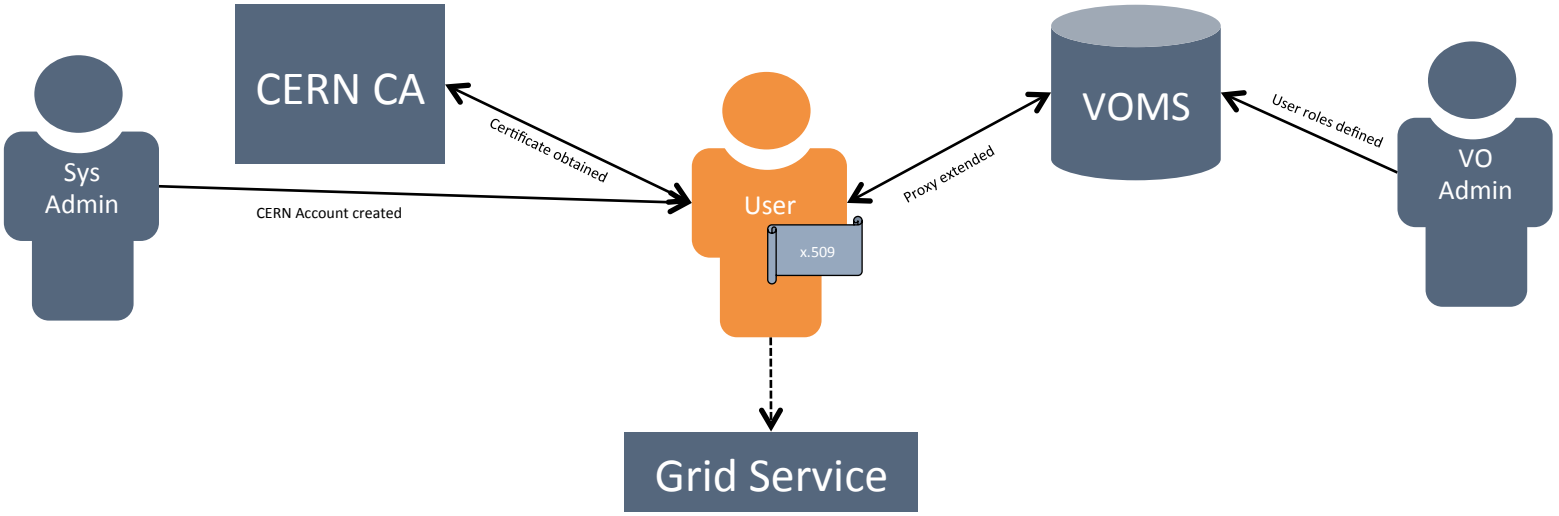


eduGAIN interconnects identity federations around the world

- Unified end-user experience of services
- Access to services and user groups can be expanded world wide… more collaboration!

Content adapted from http://services.geant.net/edugain/About_eduGAIN/Pages/Home.aspx

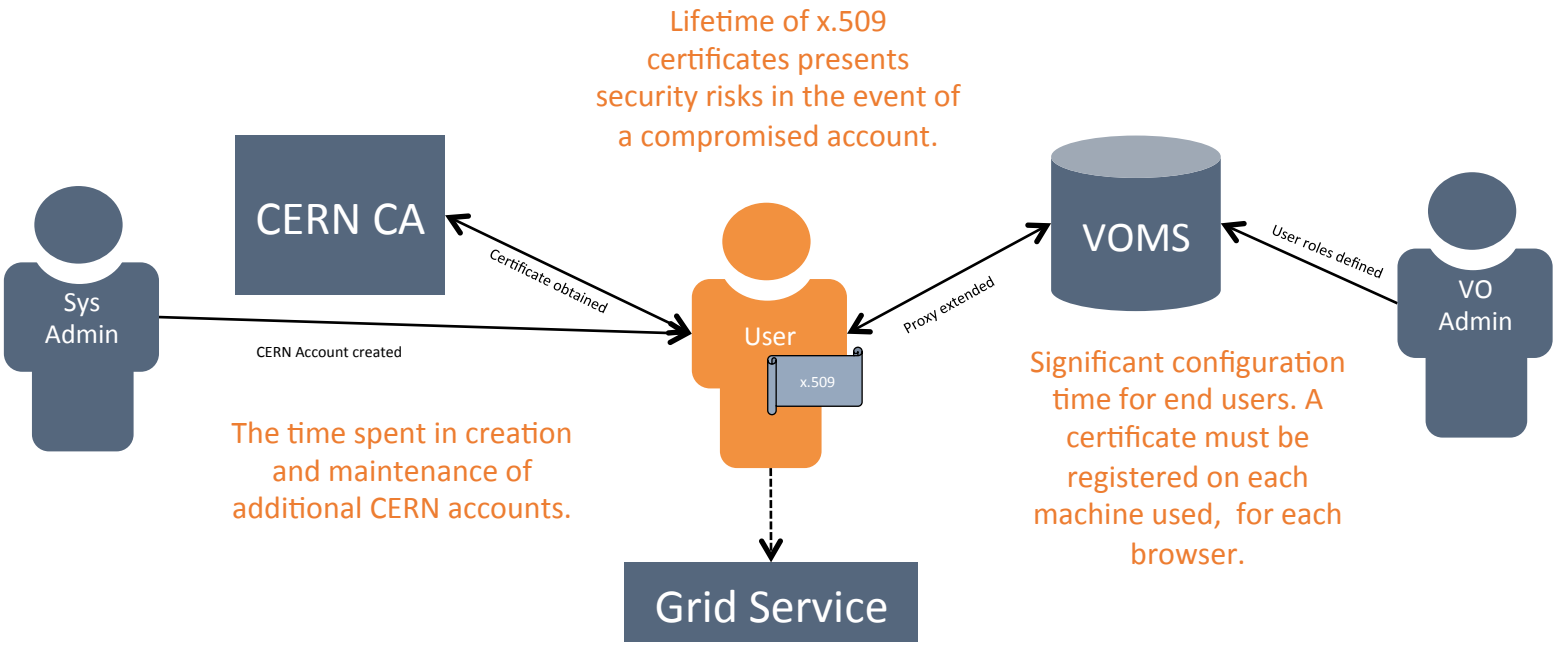
Authorisation and Authentication at WLCG



Example of current process for external users

- Admin creates a CERN Account
- Admin adds user to VOMS
- User downloads X.509 certificate (renewed annually)
- User generates and signs proxy
- Proxy is extended and re-signed by VOMS
- User accesses grid service

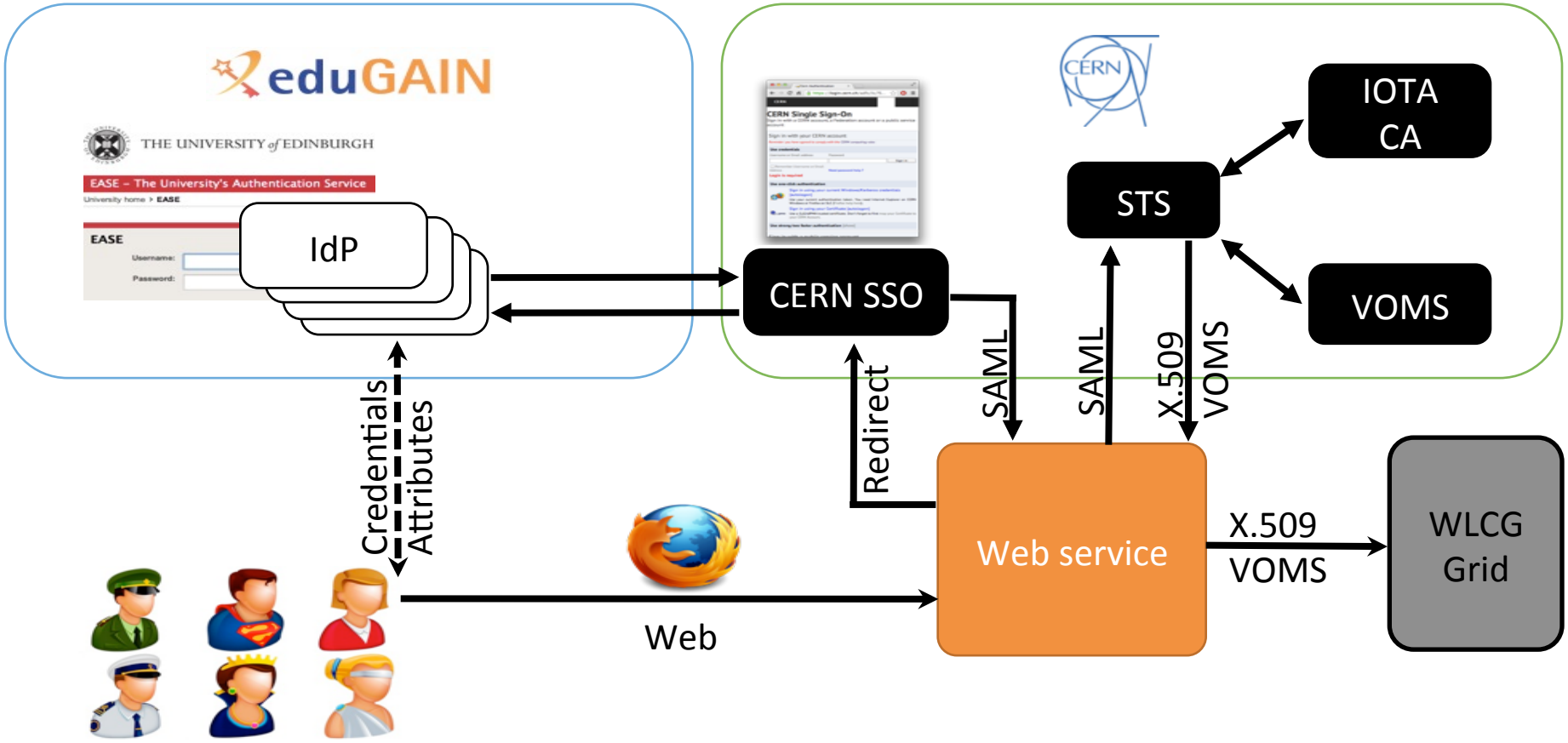
Drawbacks of current state



Risks of not adopting Federated Access

- Increased security overhead
- Loss of recognition as leader in connected computing
- Increased difficulty in securing funding, the European Commission strongly backs the federated model

WLCG Pilot


eduGAIN
THE UNIVERSITY of EDINBURGH
EASE – The University's Authentication Service
EASE
IdP
CERN
CERN Single Sign-On
CERN SSO
IOTA CA
STS
VOMS
Credentials
Attributes
Redirect
SAML
SAML
X.509 VOMS
Web service
X.509 VOMS
WLCG Grid
Web

The pilot explained

1. A user logs into a web based WLCG service
2. They are redirected to CERN SSO and authenticate through eduGAIN
3. The SAML token from eduGAIN is forwarded to the Security Token Service (STS)
4. STS validates the user against VOMS and returns an x.509 certificate and VOMS proxy to the web service
5. The user is granted access to the grid service using these credentials

For more details of the modules used in the pilot
- https://gitlab.cern.ch/sts/kipper
- https://gitlab.cern.ch/sts/sts-server

Deployment

IOTA CA

- Crucial element in reaching a production-ready solution
- Accredited by IGTF
- Only for use at VOs that employ strong identity vetting
  - Currently only valid for WLCG VOs
- Will be deployed WLCG wide following final hardware acquisition

Web portals

- Large proportion of web-based services at WLCG are behind portals
- Streamline deployment to leverage existing portals

Future plans

Key elements required for Federated Access via eduGAIN at WLCG are coming together.

We are starting discussions with VOs and aiming to deploy the solution at some initial production services.

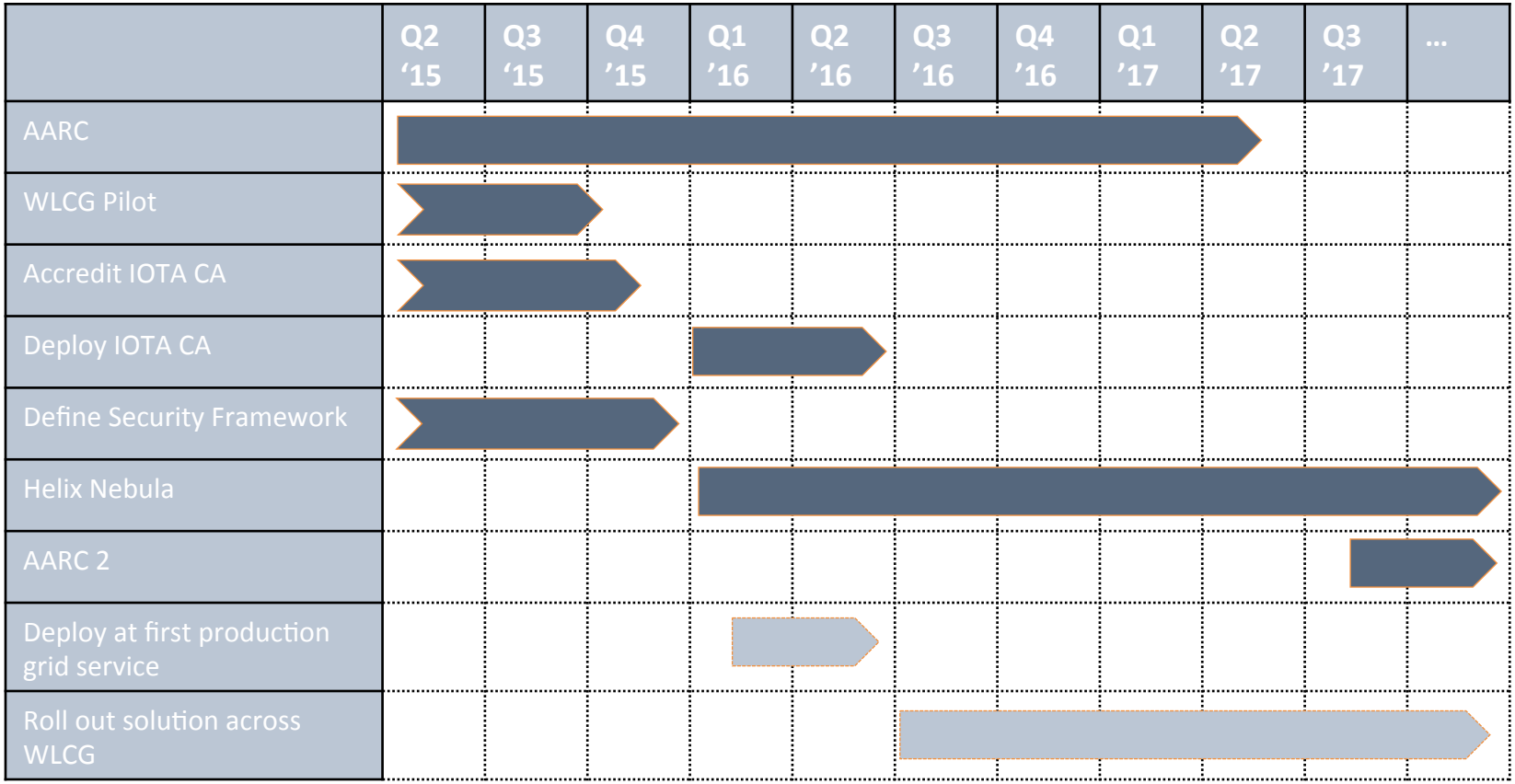
With the expertise gathered from the Pilot, CERN IT can arrange training and support deployment.

This solution is an important step towards x.509 free authorisation!

Federation Checklist

- ✓Policies in place
- ✓Security trust framework
- ✓Working pilot
- ✓Production ready solution
- ✓CERN supports strategy

Timeline


Q2 '15
Q3 '15
Q4 '15
Q1 '16
Q2 '16
Q3 '16
Q4 '16
Q1 '17
Q2 '17
Q3 '17
...
AARC
WLCG Pilot
Accredit IOTA CA
Deploy IOTA CA
Define Security Framework
Helix Nebula
AARC 2
Deploy at first production grid service
Roll out solution across WLCG

Remaining challenges

- Non-web based access still requires local x.509 certificates
- The adoption of a globally unique, non-re-assignable ID for each user would aid success
- Competing with a myriad of other projects for priority at VOs

Summary

- Introduced the AARC project and the benefits it can bring to WLCG
- Discussed the current and future states of AAI at WLCG
- Draft timeline of activities

If you would like more information, please stop by my office or take a look at the Twiki
https://twiki.cern.ch/twiki/bin/viewauth/IT/FederatedAccess

Thank you

Any Questions?

hannah.short@cern.ch

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. 653965 (AARC).