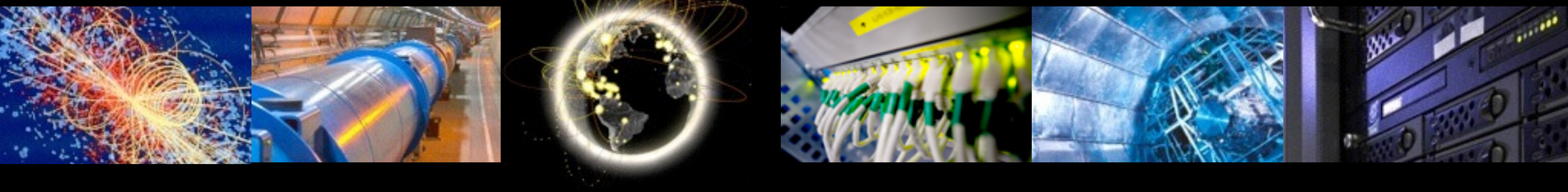
WLCG Group

Identity Federation in HEP / WLCG

FIM4R, Frascati, 23-24 April 2014

R. Wartel, CERN



WLCG Worldwide LHC Computing Grid

Background

- We have been working with identity federation for 10+ years
- X.509-based infrastructure, policy and accreditations of IdPs
- Very successful!
- But has some limitations from the users
  - Users repeatedly reported X.509 is not easy to manage
  - X.509 for end-users not widely adopted in the industry
  - Multiple accounts to manage for all users (CERN account, home account, X.509 certificate)
- Aim to make some services available to a wider community
  - Including non-X.509 users, services, organisations
- EduGAIN identified as the appropriate forum for CERN and WLCG to reach out to its users and IdPs

CERN - SWITCHaai

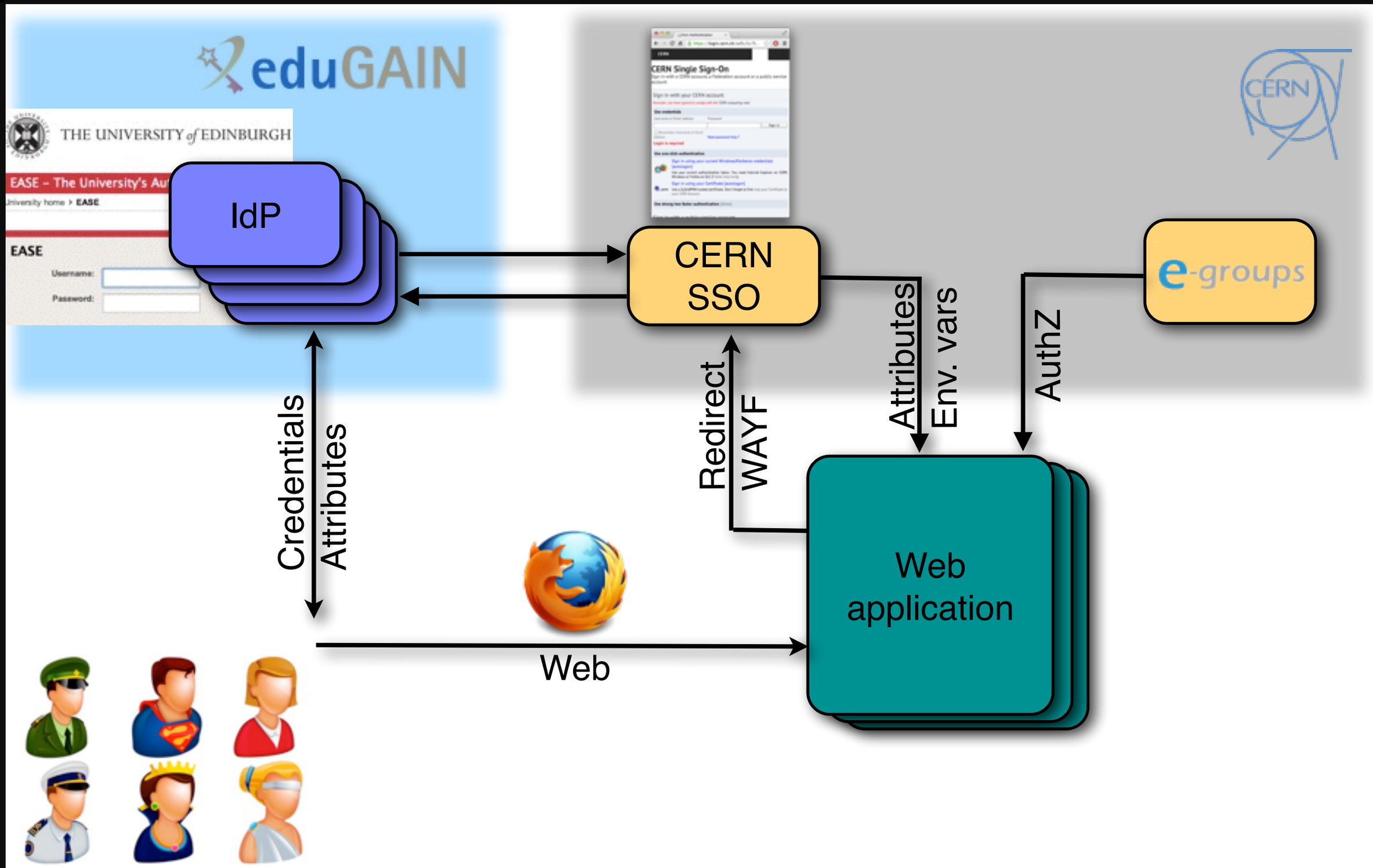
- CERN and WLCG wish to reach out to their users as well as the wider research community, via eduGAIN
- SWITCH is the Federation Operator of SWITCHaai
  - Higher education Fed for Switzerland - one of the first SAML Fed
  - Plays an leading role in enabling new user communities for the eduGAIN interfederation service.
- CERN now participating in SWITCHaai
  - Most documents signed
  - Official announcement expected in the coming weeks
- Technical work has started at CERN with help from SWITCH
  - Goal: open some services to eduGAIN IdPs under 2 conditions:
    - Signed/opt-in inter-federation access
    - CERN is assured that basic security practices are in effect
      - Discussions with Geant, eduGAIN, and other communities started

Next steps for WLCG

- Another pilot, including realistic workflow:
  - Web based, but involving traditional grid services
  - E.g. Download a “grid” file from a Web browser?

- Aims:
  - Learn what the issues are
  - Straw-man architecture

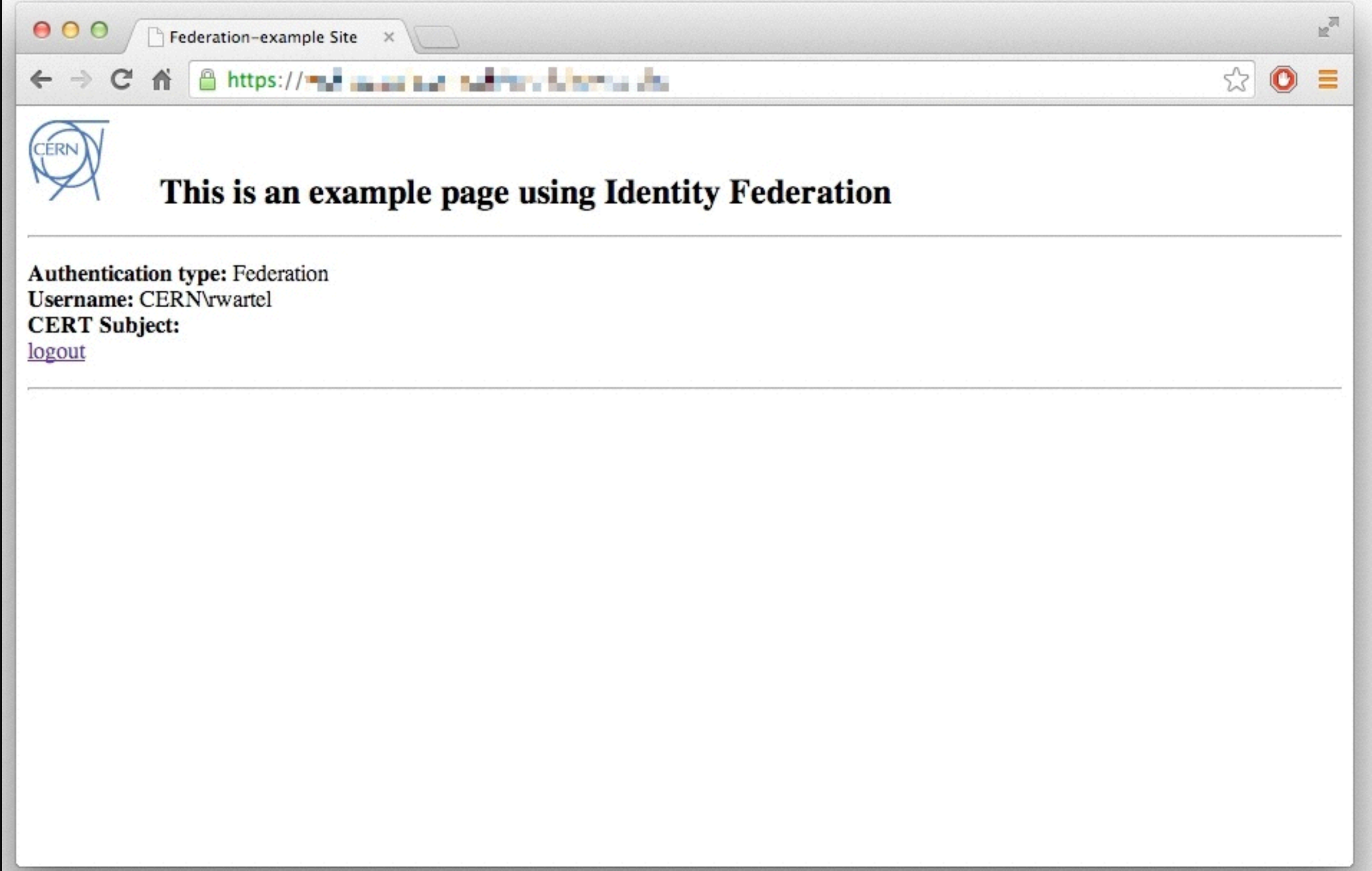
A pilot project for WLCG



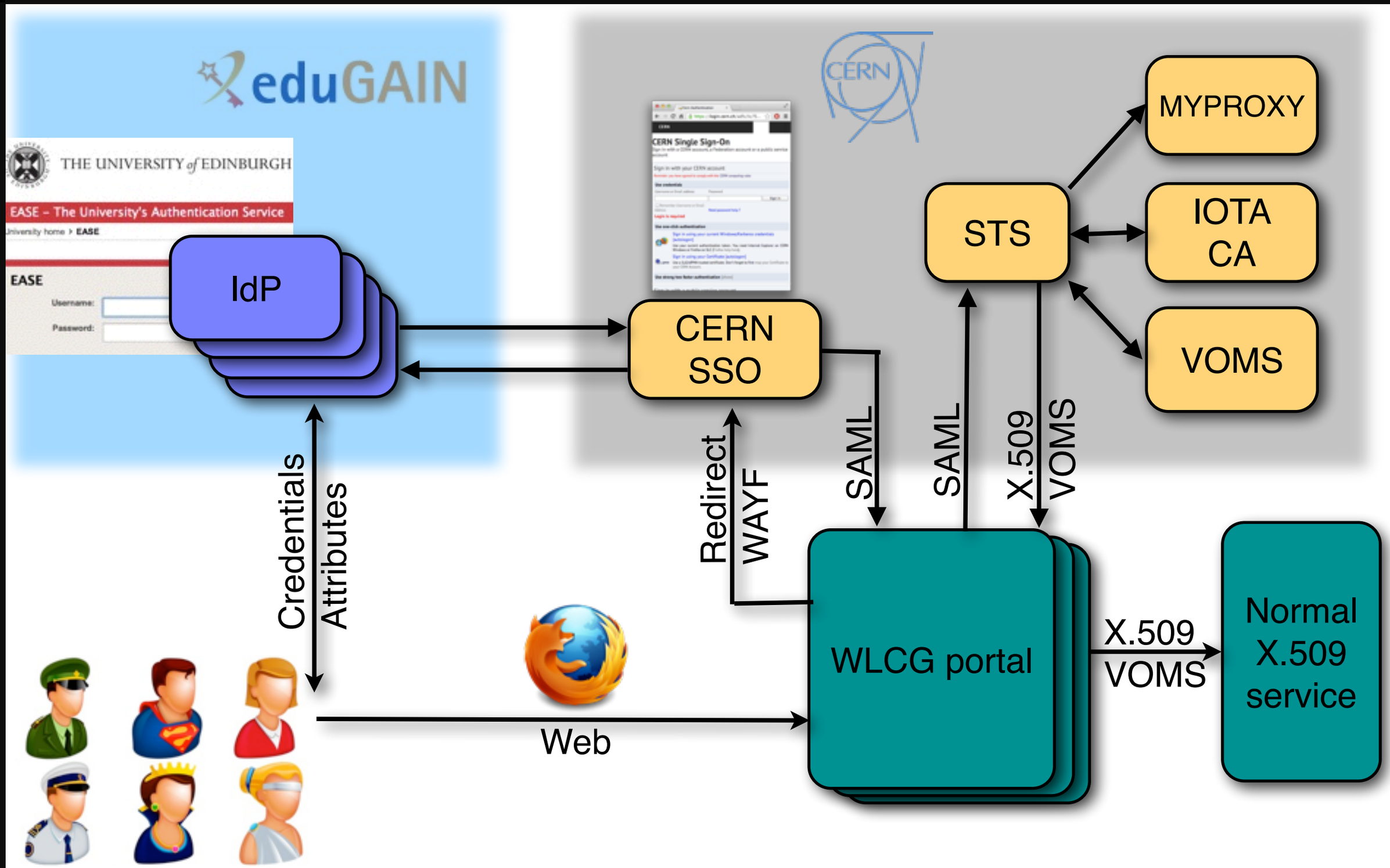
Identity Federation with the CERN SSO

PHASE 1


Cern Authentication
https://login-dev.cern.ch/adfs/ls/?wa=wsignin1.0&wreply=https%3A%2F%2Fshib2.cern.ch%2FShibboleth.sso%2FADFS&wct=2...
CERN Single Sign-On
Sign in with a CERN account, a Federation account or a public service account
ACT NOW! Please change your CERN passwords before 13 May 2014
Due to a serious vulnerability named "Heartbleed" affecting many different Internet services, we are taking now more proactive measures and ask you to CHANGE your CERN passwords
[Click to expand]
Sign in with your CERN account
Reminder: you have agreed to comply with the CERN computing rules
Use credentials
Username or Email address
Password
Sign in
Remember Username or Email Address
Need password help ?
Use one-click authentication
Sign in using your current Windows/Kerberos credentials [autologon]
Use your current authentication token. You need Internet Explorer on CERN Windows or Firefox on SLC (Firefox help here).
Sign in using your Certificate [autologon]
Use a EuGridPMA trusted certificate. Don't forget to first map your Certificate to your CERN Account.
Use strong two factor authentication [show]
Sign in with a public service account
Facebook, Google, Live, etc. (DEV)
Authenticate using an external account provider such as Facebook, Google, Live, Yahoo, Orange.
Sign in with a Federation account
Go
INFN
SWITCH AAI
Switch AAI Guest Login


Federation-example Site
https://
CERN
This is an example page using Identity Federation
Authentication type: Federation
Username: CERN\rwartel
CERT Subject:
logout

A pilot project for WLCG



Identity Federation with the CERN SSO

PHASE 2

Benefits

- **Users can access WLCG services without asking for a certificate**
  - Major step forward!
- Possible to reach out and interconnect easily with other research communities
- Many workflow and usability advantage
- However, many open questions!
  - How to choose the appropriate VOMS instance?
  - How to manage the “new” DN of the users and VOMS?
  - Who gets to use identity federation?
  - How to manage the “transition” for all users and avoid multiple DNs?
  - How will we manage traceability, incident handling, etc.?

Attributes requirements and regulation

- A policy on “Attributes for WLCG”
  - Define what attributes should be required from users, and the conditions to release them (or not)
    - Persistent user id (random string)
    - Back channel to get back in touch with the user (email address)
    - VO membership and role
    - Real name (not released unless conditions in a security policy are matched)
  - Lose real name in credential string (gridmap file, DN)
  - Transfer the Level of Assurance requirements, under some circumstances, to the attribute providers (VOMS)
    - Make it easier to user our services (InCommon Basic, etc.)
    - Focus our attention and requirements on Authorization/Attributes
- HEP/WLCG needs few and simple attributes
  - But they need to be fully harmonised across administrative domains

Policies and Trust

- A common policy framework is necessary
  - Especially for inter-federation work
  - EduGAIN security policies insufficient for “real” operations
  - Avoid many bilateral agreements with the IdPs
  - All these agreements will have to be repeated for each community
- A lot of work has been done already
  - SCI: Security for Collaborating Infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, and XSEDE
  - http://www.eugridpma.org/sci/
  - Can we expand this work to federation and have more communities to join?
- IGTF: IOTA Profile (http://www.igtf.net/ap/iota)
  - Lower assurance on ID vetting by CA
  - Key element for identity federation!

Operational considerations

- Identity federation brings more than implementation issues
  - Affects security incident handling and security operations
- In the current model
  - Service providers implement user banning & conduct forensics
  - IdPs (e.g. certificate authority) perform (almost) no operational role
- In a federated realm
  - IdPs implement emergency suspension and also collect essential traceability information
  - IdPs will therefore have to provide operational capabilities and actively participate in incident response
- Providing operational capability is a significant change
  - Requires careful planning to ensure sufficient logging, expertise, communication channels, etc. are in place

Conclusion

- Pretty exciting time!
  - Interesting window of opportunity
- Feasibility and architecture still being discussed
  - Devil in the details, but they are also many identified challenges
- Appropriate operational security essential
  - Discussion started, everyone welcome!
- Many different areas to discuss
  - Technical work
  - Attributes
  - Trust issues
  - Roles and responsibility
  - Transition