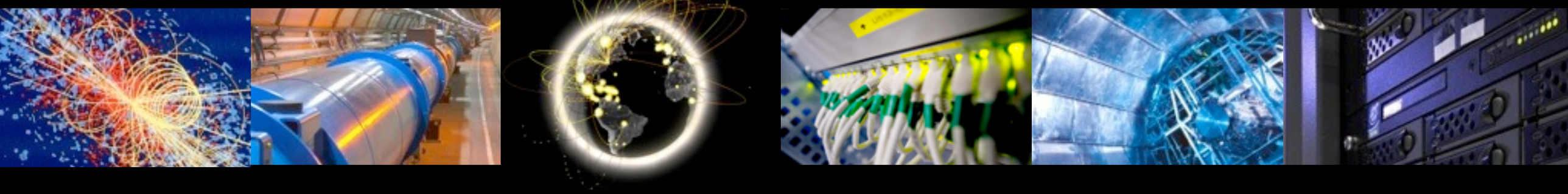
WLCG Group

Identity Federation in HEP / WLCG

GDB, 9th 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

Background

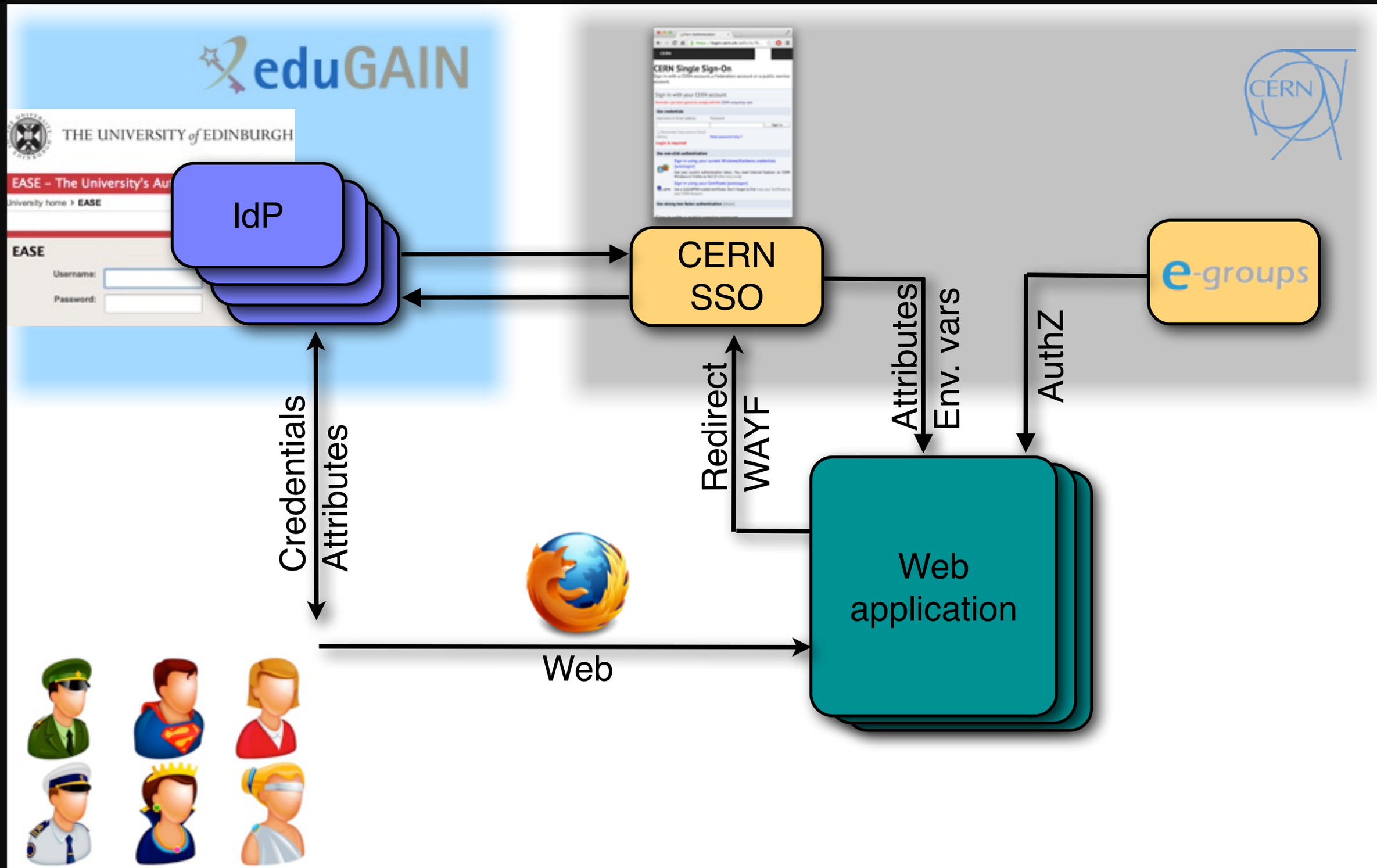
- Identity Federation is a very complex problem
  - Not only a technical problem, lots of trust/policy issues
  - Devil is in the details

- Discussed a number of issues
  - What problem are we trying to solve, CLI vs Web use cases
  - What federation(s) to join and how?
  - WLCG infrastructure and service design in a federated world
  - Trust/policy issues
  - Impact on (security) operations
  - Implications for users and personal data

Concensus in WLCG

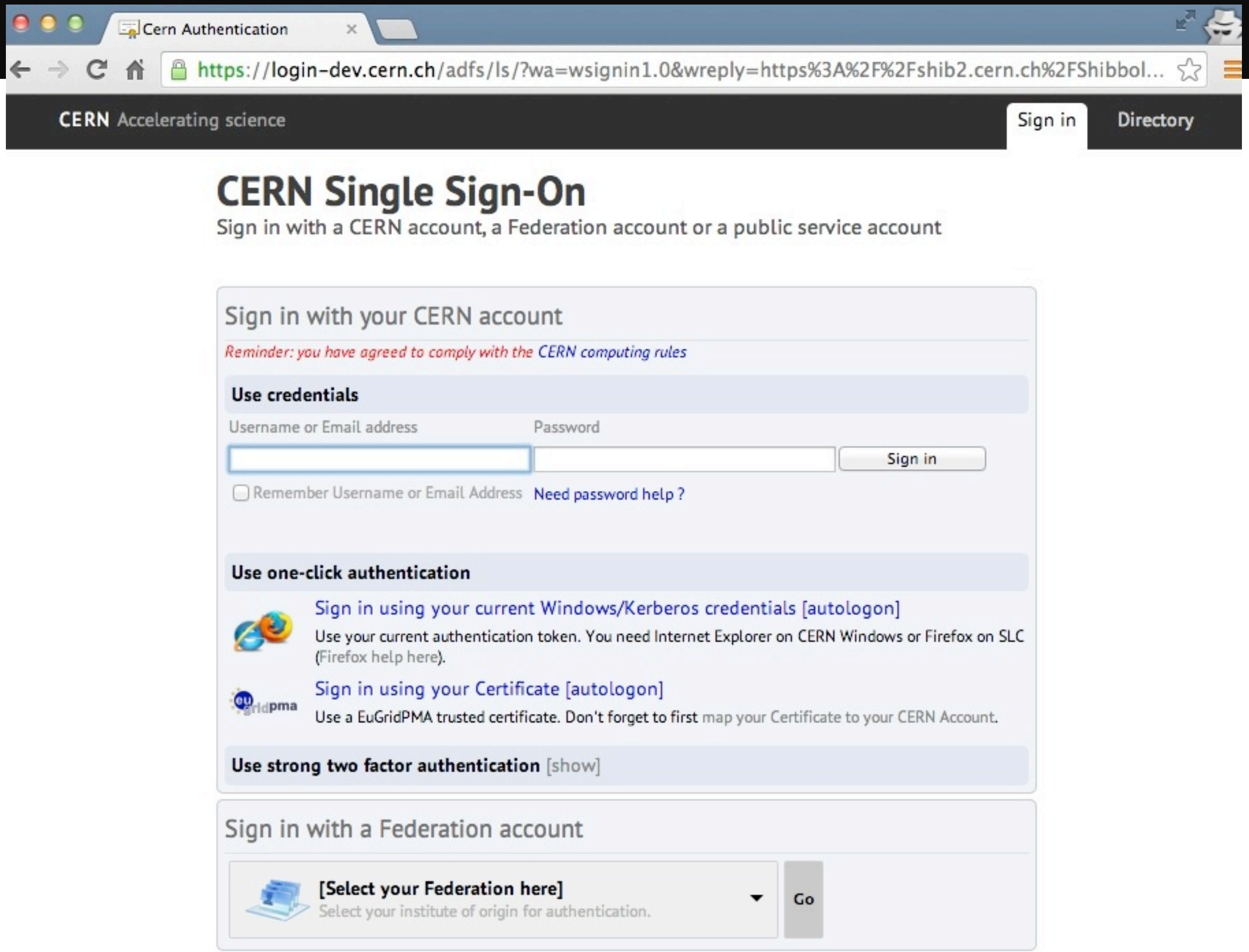
- WLCG should build on existing federations and infrastructures (NRENs, etc.)
  - Perhaps a catch-all solution would be needed
- Priority is to focus on the Web use cases
  - CLI pilot worked very well technically!
  - CLI work halted at this stage due to lack of ECP availability
- Building blocks identified and exist: *STS, CiLogon, TCS, VOMS, SAML, ECP, IOTA, EduGAIN, IGTF, etc.*
- EduGAIN identified as the appropriate forum for WLCG to reach out to its users and IdPs
- Another pilot, including realistic workflow:
  - Web based, but involving traditional grid services
  - E.g. Download a “grid” file from a Web browser?

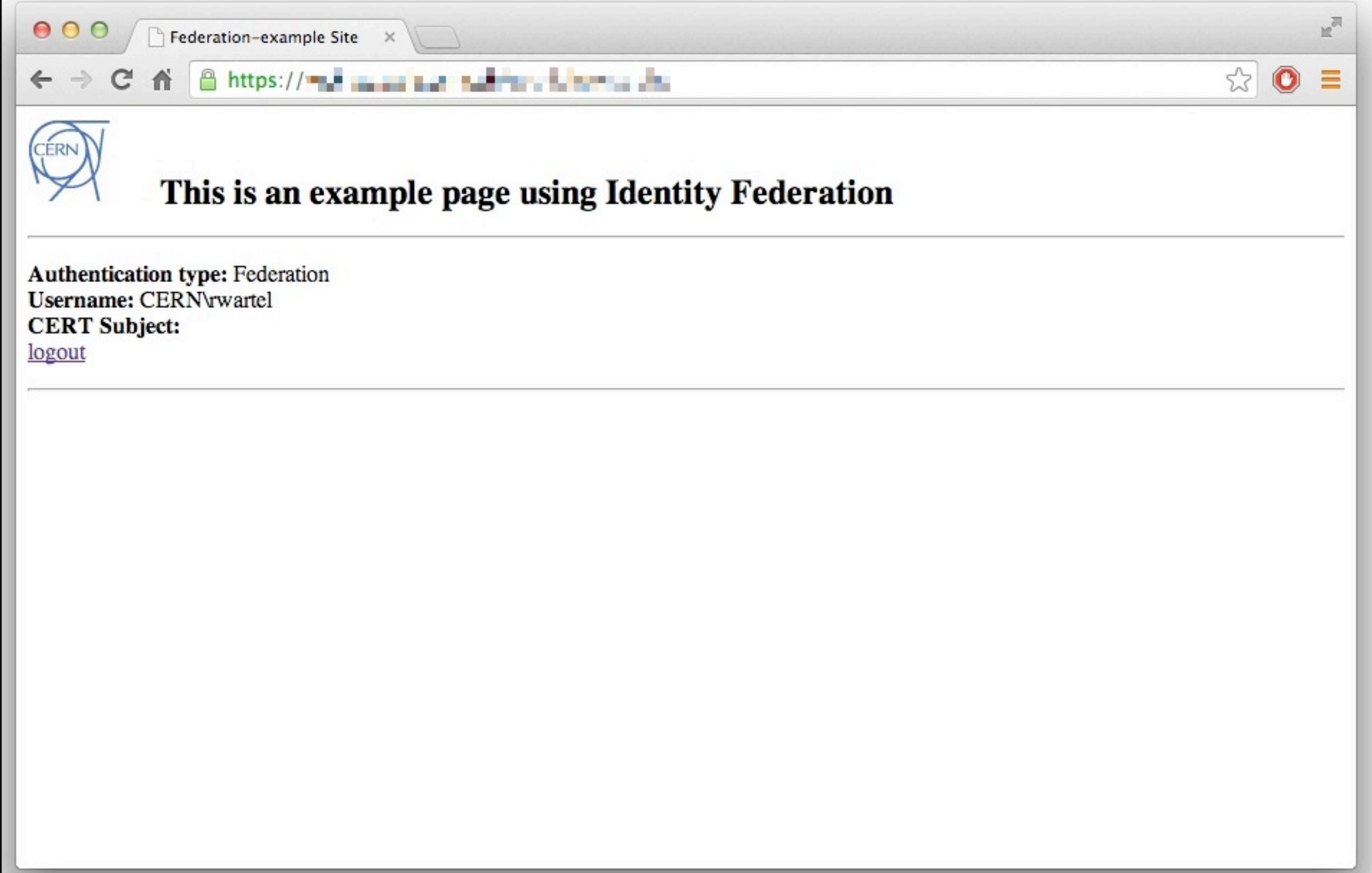
A pilot project for WLCG



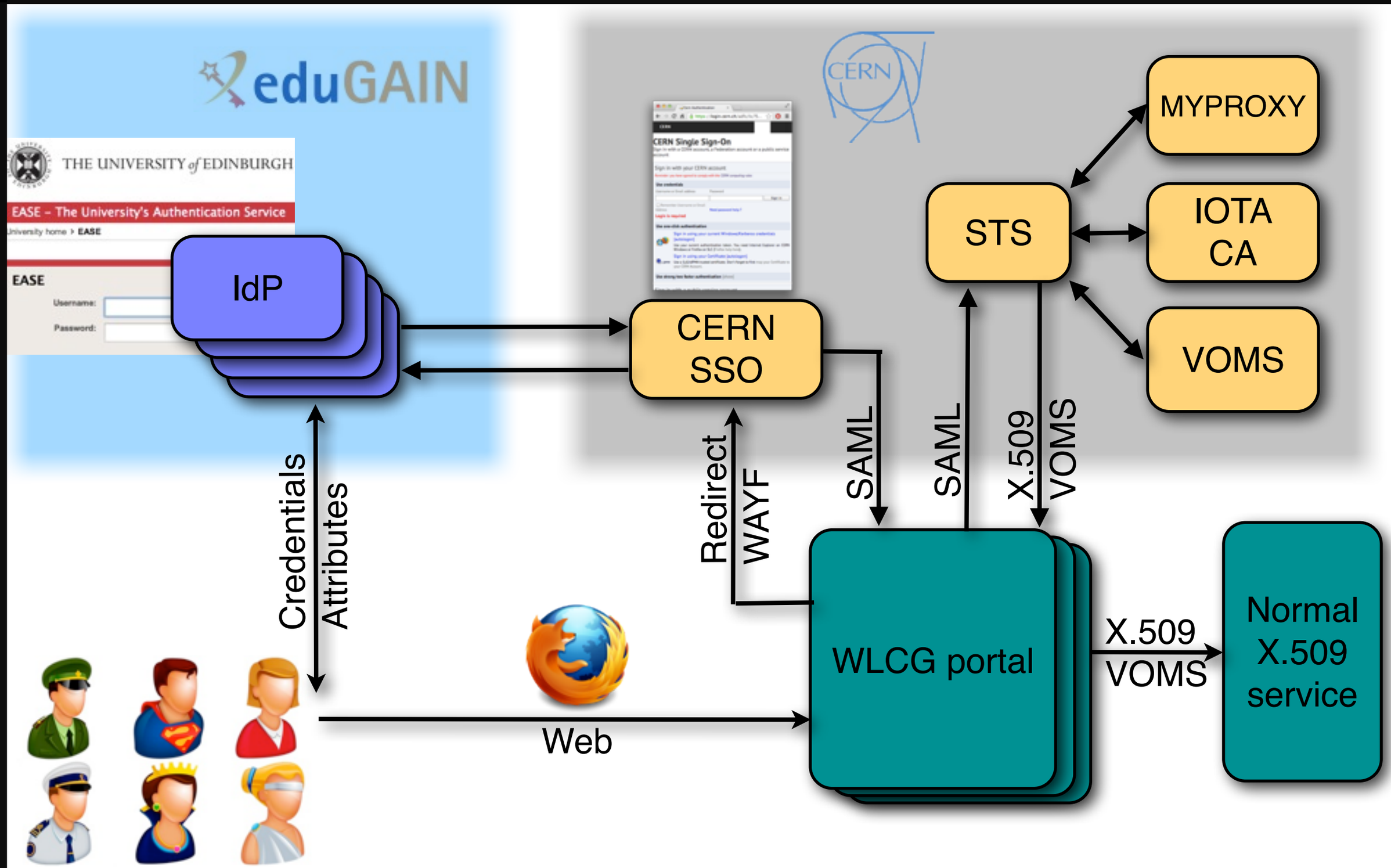
Identity Federation with the CERN SSO

PHASE 1


Cern Authentication
https://login-dev.cern.ch/adfs/ls/?wa=wsignin1.0&wreply=https%3A%2F%2Fshib2.cern.ch%2FShibbol...
CERN Accelerating science
Sign in
Directory
CERN Single Sign-On
Sign in with a CERN account, a Federation account or a public service account
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 Federation account
[Select your Federation here]
Select your institute of origin for authentication.
Go


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

MANY open questions

- Can this work, in particular “phase 2”?
- How to map attributes from other federations in ADFS?
- Is it possible to get the original SAML assertion via ADFS?
- Can the STS interact with an online CA at CERN?
- How to choose the appropriate VOMS instance?
- How to manage the “new” DN of the users and VOMS?
  - Preregistration in VOMS by the users?
  - Preregistration in VOMS by STS?
- 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.?

Policies and Trust

- IGTF: IOTA Profile (http://www.igtf.net/ap/iota)
  - Lower assurance on ID vetting by CA
  - Key element for identity federation!

- A common policy framework is necessary
  - **EduGAIN security policies insufficient for "real" operations**
  - Alternative: 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?

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
  - Can it work?
  - Devil in the details, but they are also many identified challenges
  - Lack of common security policies/practices is a serious issue
- Many different areas to discuss
  - Technical work
  - Attributes
  - Trust issues
  - Roles and responsibility
  - Transition
- All an open discussion, feel free to contribute!