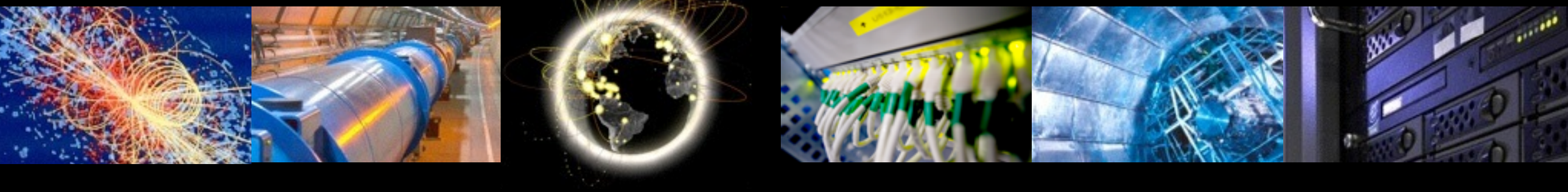
WLCG Group

# Update on Identity Federation in HEP / WLCG

GDB, 9th Septembre 2014

R. Wartel, CERN



WLCG Worldwide LHC Computing Grid

# Goals

- See March 2014 GDB for more background details

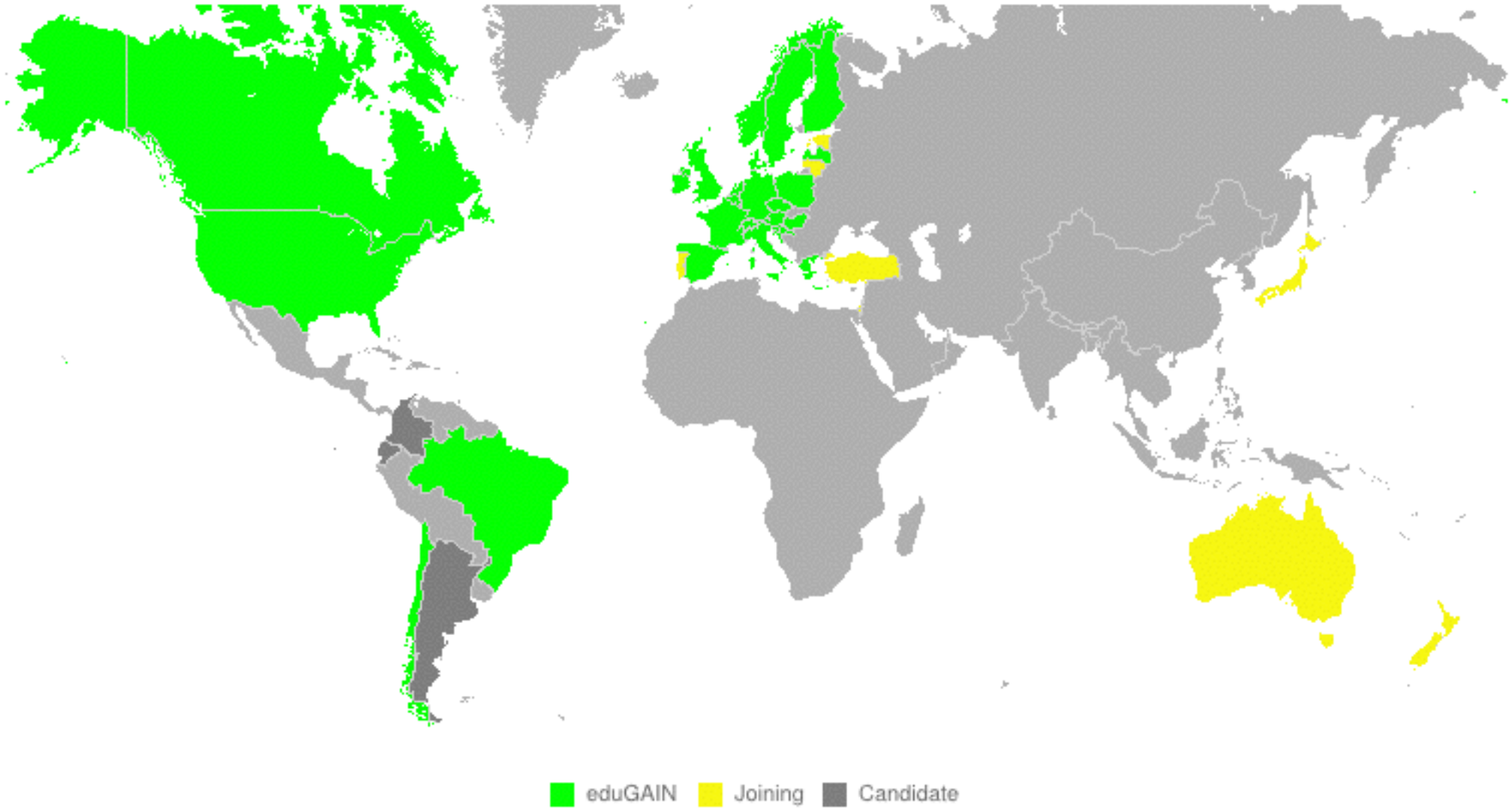
- Enable people to use their home organisation credentials
  - Submit grid jobs without the need of end user certificates
  - Access Web portals (monitoring, etc.)
  - Interact with X509 services

- Aim to make some services available to a wider community
  - Indico, Vidyo, etc.

- Non-Web use case not included for now
  - Lack of ECP availability
  - But current work essential for non-Web use case too

# Federations

- Build on existing federations and infrastructures
  - eduGAIN




- CERN participates in eduGAIN via SWITCHaai
- Many NREN participates in eduGAIN too

# Technical aspects

[DONE] CERN to sign-up to SWITCHaai

[DONE] Implement necessary components for SWITCHaai

[DONE] Incorporate CERN's ADFS SSO into SWITCHaai

[DONE] Enable inter-federation authentication (eduGAIN)

[DONE] Enable eduGAIN on production SSO

[DONE] Discover horrible and incomprehensible bugs

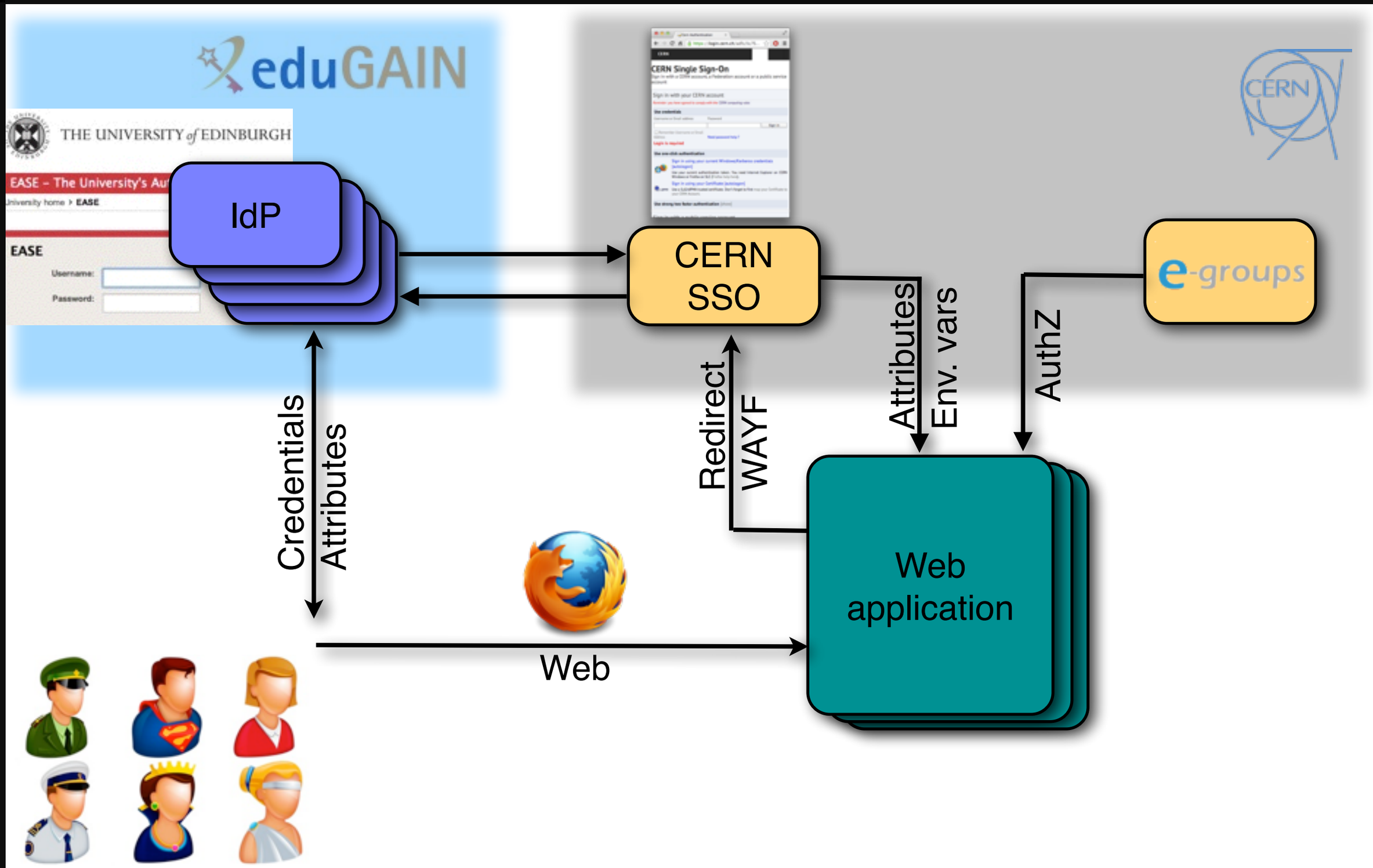
[WIP] Enable eduGAIN on key services (Indico, OpenStack…)

[WIP] Conduct extensive tests with other IdPs

[TBD] Approach experiments and enable federated identity access to several core services

[WIP] Enable access to grid services (STS, WebFTS, etc.)

# A pilot project for WLCG

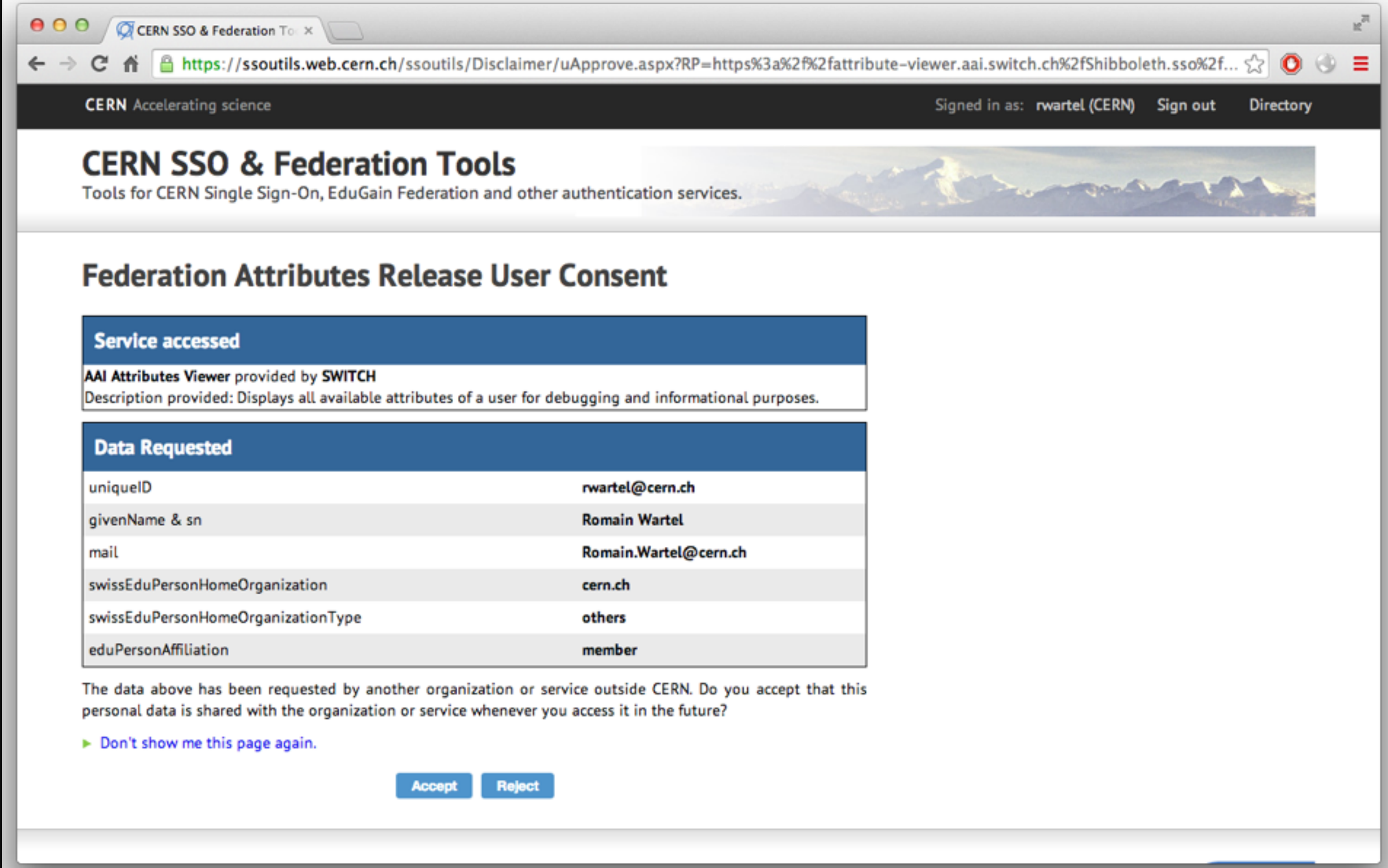



Identity Federation with the CERN SSO

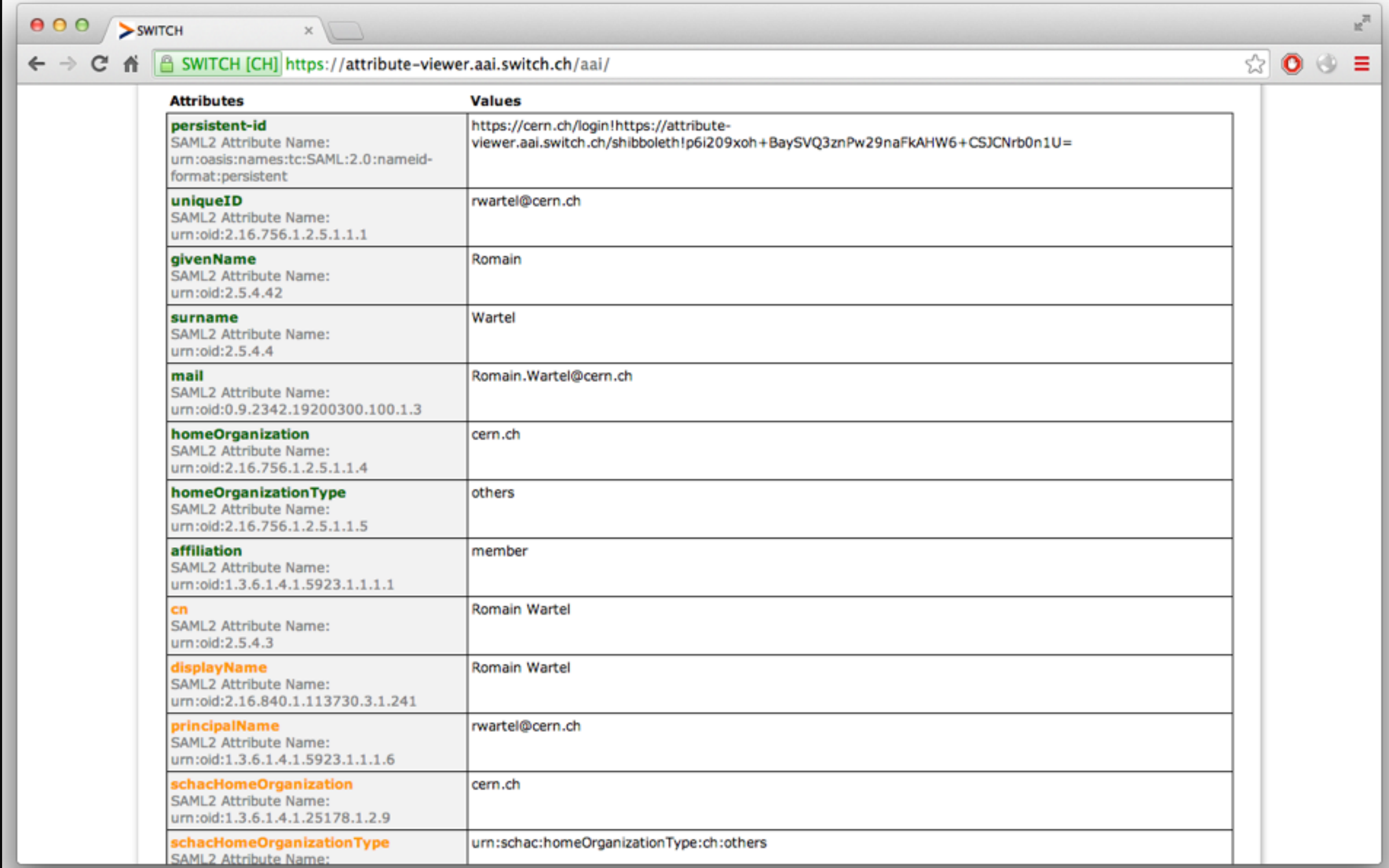
**PHASE 1**

# CERN production SSO

# Hello, World.


CERN SSO & Federation To
https://ssoutils.web.cern.ch/ssoutils/Disclaimer/uApprove.aspx?RP=https%3a%2f%2fattribute-viewer.aai.switch.ch%2fShibboleth.sso%2f...
CERN Accelerating science
Signed in as: rwartel (CERN) Sign out Directory
CERN SSO & Federation Tools
Tools for CERN Single Sign-On, EduGain Federation and other authentication services.
Federation Attributes Release User Consent
Service accessed
AAI Attributes Viewer provided by SWITCH
Description provided: Displays all available attributes of a user for debugging and informational purposes.
Data Requested
uniqueID rwartel@cern.ch
givenName & sn Romain Wartel
mail Romain.Wartel@cern.ch
swissEduPersonHomeOrganization cern.ch
swissEduPersonHomeOrganizationType others
eduPersonAffiliation member
The data above has been requested by another organization or service outside CERN. Do you accept that this personal data is shared with the organization or service whenever you access it in the future?
Don't show me this page again.
Accept
Reject

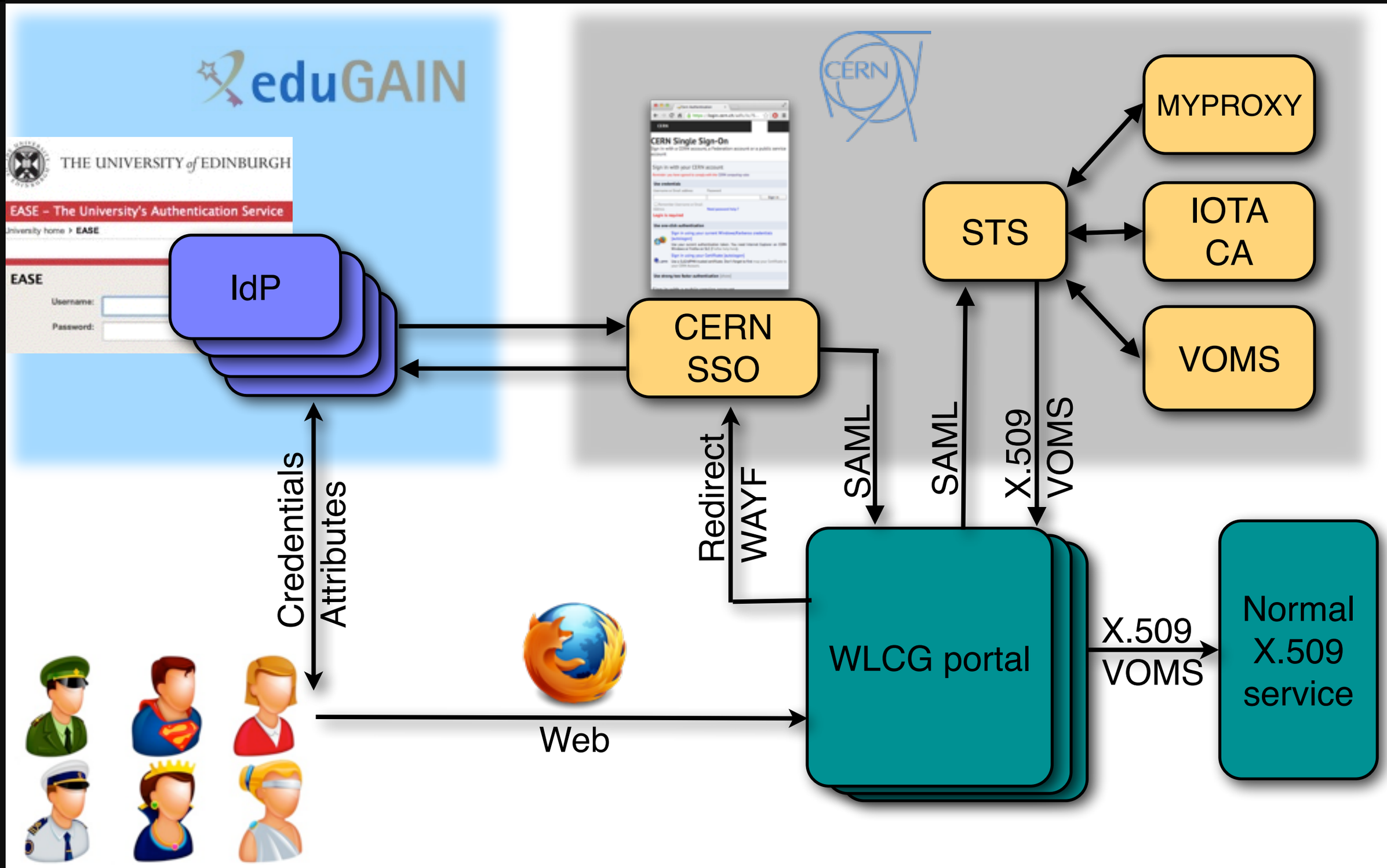
# Hello, World.




| Attributes | Values |
|---|---|
| **persistent-id**<br>SAML2 Attribute Name:<br>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent | https://cern.ch/login!https://attribute-viewer.aai.switch.ch/shibboleth!p6i209xoh+BaySVQ3znPw29naFkAHW6+CSJCNrb0n1U= |
| **uniqueID**<br>SAML2 Attribute Name:<br>urn:oid:2.16.756.1.2.5.1.1.1 | rwartel@cern.ch |
| **givenName**<br>SAML2 Attribute Name:<br>urn:oid:2.5.4.42 | Romain |
| **surname**<br>SAML2 Attribute Name:<br>urn:oid:2.5.4.4 | Wartel |
| **mail**<br>SAML2 Attribute Name:<br>urn:oid:0.9.2342.19200300.100.1.3 | Romain.Wartel@cern.ch |
| **homeOrganization**<br>SAML2 Attribute Name:<br>urn:oid:2.16.756.1.2.5.1.1.4 | cern.ch |
| **homeOrganizationType**<br>SAML2 Attribute Name:<br>urn:oid:2.16.756.1.2.5.1.1.5 | others |
| **affiliation**<br>SAML2 Attribute Name:<br>urn:oid:1.3.6.1.4.1.5923.1.1.1.1 | member |
| **cn**<br>SAML2 Attribute Name:<br>urn:oid:2.5.4.3 | Romain Wartel |
| **displayName**<br>SAML2 Attribute Name:<br>urn:oid:2.16.840.1.113730.3.1.241 | Romain Wartel |
| **principalName**<br>SAML2 Attribute Name:<br>urn:oid:1.3.6.1.4.1.5923.1.1.1.6 | rwartel@cern.ch |
| **schacHomeOrganization**<br>SAML2 Attribute Name:<br>urn:oid:1.3.6.1.4.1.25178.1.2.9 | cern.ch |
| **schacHomeOrganizationType**<br>SAML2 Attribute Name: | urn:schac:homeOrganizationType:ch:others |

WLCG Worldwide LHC Computing Grid

# A pilot project for WLCG




Identity Federation with the CERN SSO

**PHASE 2**

# Policy & Trust issues

- There is no trust / guaranty about the identities used
  - Our security models relies on Authorization
  - How people get registered in the experiments is CRITICAL
- Significant policy and trust issues ahead
  - Probably years of work!
    - Many more participants than just WLCG
    - Legal situation has significantly changed
    - eduGAIN really “opens the gate” to world + dog, this has profound security and operational implications
    - eduGAIN is currently an operational security wild west
  - Transition
    - Operating during this transition also involves work
    - How can we open access to our services without trusting identities and without an operational or trust framework?

# Policy & Trust issues

- Two main categories and policy / trust issues:
  - Operational Security (opsec)
    - Incident handling
    - Exchange of confidential information between eduGAIN identity providers or service providers
    - Coordinated response to security incident
  - Privacy, traceability, and protection of personal data (privacy)
    - EU Directive 95/46/EC on the protection of personal data
    - Current WLCG AUP and data protection policy must be reviewed
    - Incompatible traceability requirements (all vs nothing)
    - Must balance and document legitimate interests to collect data with the rights and interests of the user
      http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
    - “user consent” no longer sufficient
  - “We must record everything running in our data center”
  - “We don’t keep any user logs - it’s too much of a liability”

# Ongoing efforts

- Coordinated efforts to address some of these issues:
  - SCI - Security for Collaboration among Infrastructures
    - http://www.eugridpma.org/sci/
    - Members: WLCG, EGI, OSG, PRACE, EUDAT, CHAIN, XSEDE
  - Sir-T-Fi: Security Incident Response Trust Framework for Federated Identity
    - <sirtfi@terena.org>
    - Largely based on SCI work
    - Members: SCI + Internet2, InCommon, eduGAIN, REFEDS, etc.
  - FIM4R: Federated Identity Management for Research Collaborations
    - https://cdsweb.cern.ch/record/1442597
    - Members: WLCG/HEP, ELIXIR, CLARIN, DARIAH, PanData, CRIPS, earth sciences, etc.
  - AARC: H2020 proposal on AAI
  - Terena, Geant, REFEDS, etc.

# Objectives

- Key objectives for these projects:
  - Operational Security (opsec)
    - Propose an incident response procedure for federations, defining roles and responsibilities
    - Propose a trust framework to enable (inter)federation participants to cooperate and share confidential data
    - Propose a minimal set of requirements on IdPs and SPs …and enforce these requirements via metadata
  - Privacy, traceability, and protection of personal data (privacy)
    - Propose a trust framework and guidelines enabling both legal compliance with (EU/US) legislation and safe operation of our services
    - Ensure convergence or at least compatibility between participants
    - Adapt the set of WLCG policies accordingly
    - Adapt our services accordingly

# EduGAIN- Data protection Code of Conduct

- GÉANT's Data Protection Code of Conduct (CoC)
  - Push eduGAIN SPs to enforce basic data protection practices
  - Goal: encourage IdPs to release attributes (i.e make eduGAIN work)

- CLARIN, DARIAH, DASISH and ELIXIR research infrastructures and projects have endorsed the COC
- https://wiki.edugain.org/CoCoEndorsement

- WLCG should endorse this CoC too!

# Conclusion

- Identity Federation is a very complex problem
  - Not only a technical problem, lots of trust/policy issues
  - Devil is in the details
- Technical work
  - Web use case requires significant work
  - Central infrastructure ready
  - Testing + enabling access to more portals in progress!
  - Grid use case also in progress
- Trust and policy
  - World is changing: we need to adapt our policies and services
  - A number trust/policy issues to address
  - Many partners, cultures, projects and efforts
  - Impact on (security) operations
  - Implications for users and personal data