



# Access to WLCG resources: The X509-free pilot

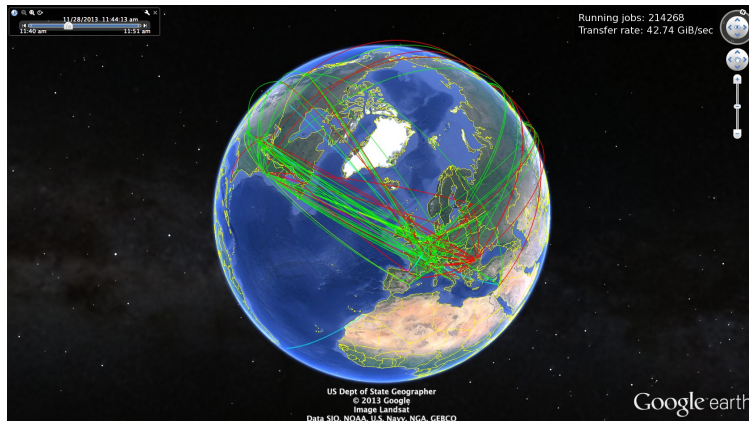
**H. Short** ( presenter), A. Manzi, P. Tedesco, V. De Notaris, A. Kirianov, O. Keeble, H. Mikkonen, R. Wartel

# Authentication and Authorisation at WLCG

- “To use WLCG you must possess a personal digital certificate from a Certification Authority (CA) recognised by WLCG” [1]



- These CAs are accredited by the IGTF
- End users own and manage these certificates
  - Certificate renewal
  - Grid Proxy Certificate generation
- VOMS defines roles and groups for additional authorisation



Maybe it's time for a different approach?

# What is Federated Access?

- The ability to log in to a service using an identity managed by a separate organisation
- eduGAIN is the international group of services and identity providers using Federated Login
- Has become common practice within Research and Education

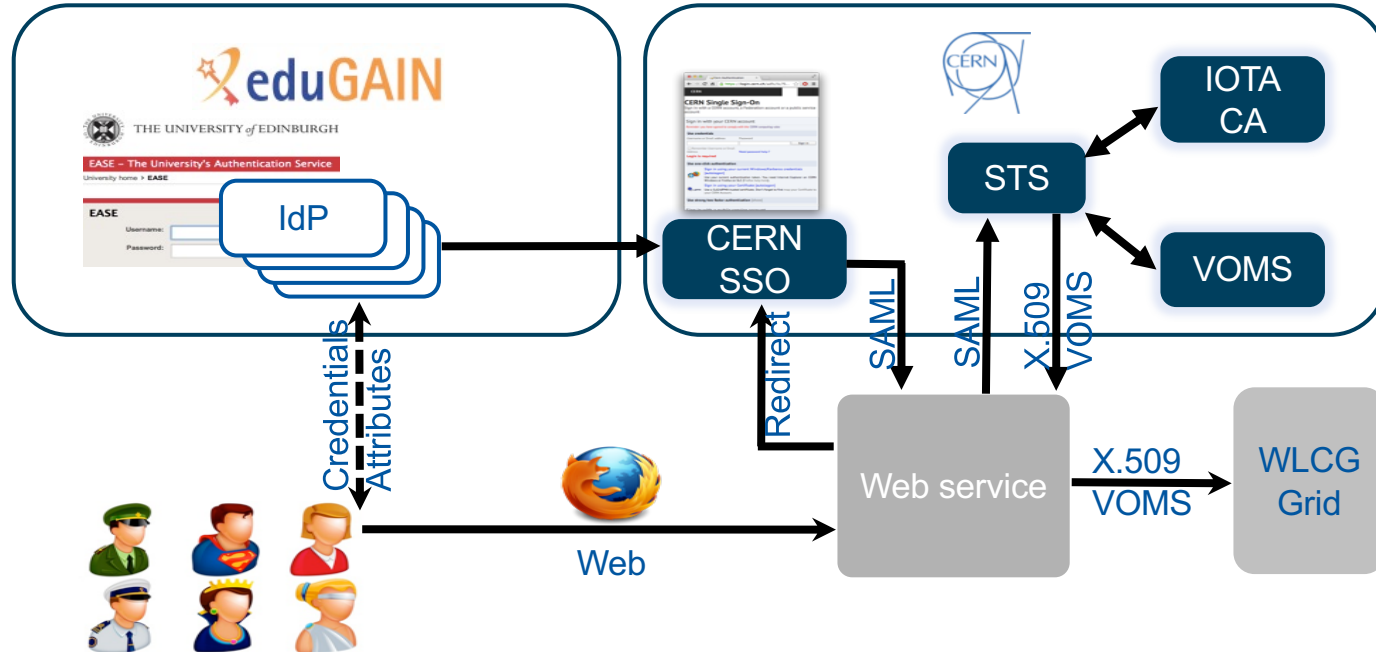
## CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

The screenshot displays the CERN Single Sign-On interface. It is divided into three main sections:

- Sign in with your CERN account:** This section includes a reminder to agree to CERN computing rules. It features a "Use credentials" section with input fields for "Username or Email address" and "Password", a "Sign in" button, and a checkbox for "Remember Username or Email Address" with a link to "Need password help?". Below this is a "Use one-click authentication" section with two options: "Sign in using your current Windows/Kerberos credentials [autologon]" (requiring Internet Explorer or Firefox on SLC) and "Sign in using your Certificate [autologon]" (requiring a EuGridPMA certificate).
- Sign in with a public service account:** This section includes a link to "Facebook, Google, Live, etc."
- Sign in with your organization or institution account:** This section is highlighted with an orange border. It features the eduGAIN logo, a dropdown menu for "Enter the name of the organisation you are affiliated with...", and a "Go" button.

# How can I implement X509 free?



# Components

## CERN SSO

- A "Single Sign On" (SSO) endpoint is required to configure your service as a CERN Service Provider. Shibboleth or Mellon are the recommended technologies to use and are supported by CERN IT. A user's SAML Assertion can be exported from the local SSO Service and sent to STS for transformation to an x.509 certificate.

## STS

- The "Security Token Service" (STS) takes SAML tokens, or username and password pairs, and transforms them into x.509 certificates. STS uses the IOTA CA to generate short-lived certificates for users registered with their WLCG Virtual Organisation (VO) in VOMS.

## IOTA CA

- The "Identifier Only Trust Assurance" (IOTA) Certificate Authority (CA) issues short-lived x.509 certificates to STS clients. IOTA Certificates will only be issued to users from Virtual Organisations (VOs) that employ strong identity vetting, such as WLCG VOs.

# Authorise users with VOMS?

- VOMS authorisation requires users with X509 certificate ( for now 😊)
  - We need a way to map the SAML Id to the VOMS records
- For some VOs, you are ready to go
  - Currently all users have CERN IDs, since they all have CERN accounts
  - The nickname contains the CERN ID, e.g. jsmith, of the user
- Working with VOMS devs to:
  - Access VOMS via SSO, so to enable association SAML Id -> VOMS record
  - Provide a smooth VOMS registration process for future users without a certificate

## SAML Assertion

```
<AttributeStatement>
  <Attribute Name="EmailAddress">

<AttributeValue>hannah.short08@gmail.com</AttributeValue>
</Attribute>
  <Attribute Name="CommonName">
    <AttributeValue>jsmith</AttributeValue>
  </Attribute>
</AttributeStatement>
```

## VOMS Record

```
<Record>
  <Personal information />
  <Certificates />
  <Groups and Roles />
  <Attributes >
    <Attribute Name="nickname">
      <AttributeValue>jsmith</AttributeValue>
    </Attribute>
  </Attributes>
</Record>
```



# Example Services – ATLAS

## PanDA (Bigpanda)

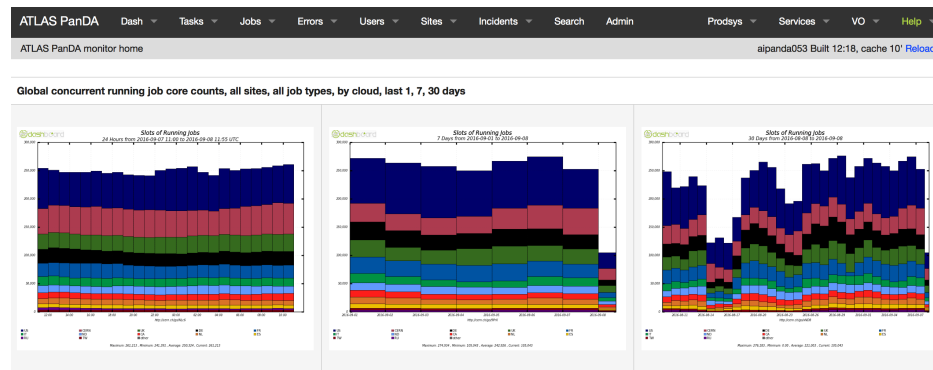
What is it?

- Jobs monitoring service for ATLAS
- Contacts additional services that require certificates

In progress

Why enable federated access?

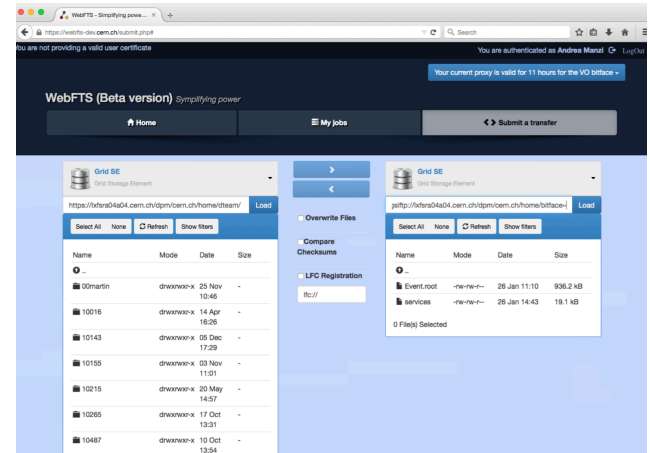
- Security – logs are open to wide audience and should be controlled by user certificates
- Finer granularity of user control possible with SSO – e-groups, user groups etc



# Example Service – WebFTS (pilot)

- What is it?
  - <https://webfts.cern.ch>
  - Web based tool to transfer files between grid/cloud storages
  - Modular protocol support
    - gsiftp, http(s), xrootd and srm
    - Cloud extensions: dropbox, CERNBox
  - Initial development funded by EUDAT
- Why enable Federated Access?
  - X509 delegation is needed to let WebFTS access the grid on users behalf
  - We are trying to replace user certificate delegation with transparent access via Identity Federation
  - <https://webfts-dev.cern.ch> (contact us for testing)

Pilot



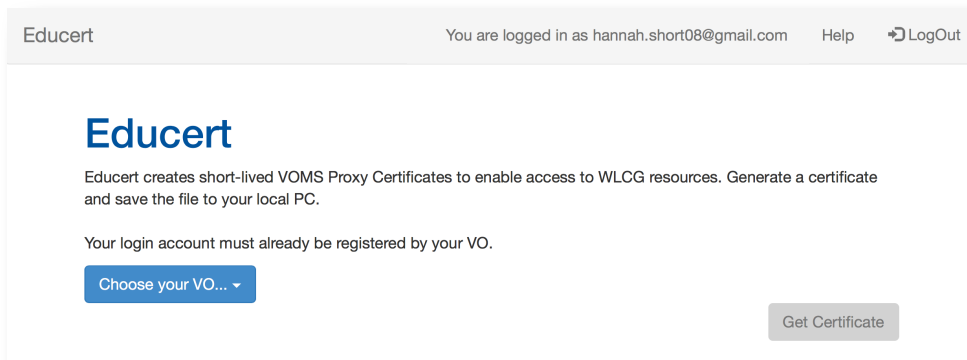
The screenshot shows the WebFTS (Beta version) web interface. The page title is "WebFTS (Beta version) simplifying power". The user is authenticated as Andrea Manzoni. The interface includes a navigation bar with "Home", "My jobs", and "Submit a transfer" buttons. Below the navigation bar, there are two panels for "Grid SE" (Grid Storage Element). The left panel shows a file list with columns for Name, Mode, Date, and Size. The right panel shows a "Compare Checksums" section with a table of files and their sizes.

Name	Mode	Date	Size
00martin	drwxrwx	25 Nov 10:46	-
10016	drwxrwx	14 Apr 16:28	-
10143	drwxrwx	05 Dec 17:29	-
10155	drwxrwx	03 Nov 11:01	-
10215	drwxrwx	20 May 14:57	-
10265	drwxrwx	17 Oct 13:31	-
10487	drwxrwx	10 Oct 13:54	-

Name	Mode	Date	Size
Event.root	-rwxr-x	28 Jan 11:10	936.2 kB
services	-rwxr-x	28 Jan 14:43	19.1 kB

# Not only Web: CLI Access

- The primary use case for SAML (the protocol used for Federated Login) is Web-Based Authentication whereas our users spend their life on the command line
- Several Command Line solutions exist (ECP, CiLogon, Moonshot) but
  - Require configuration at home organisations (takes time and resources), or,
  - Are not yet available for Europe
- At CERN, a prototype service, Educert, is available for generating GridProxy certificates for download



# Command Line Access

Educert

You are logged in as hannah.short08@gmail.com Help ↪ LogOut

Downloads — -bash — 171x48

```
Last login: Thu Aug 4 09:17:00 on ttys000
lxminu-32:~ rwartel$ cd Downloads/
lxminu-32:Downloads rwartel$ curl -O https://educert.cern.ch/certs/ddeai25a139558c7bba46b3453dd6611.pem
% Total % Received % Xferd Average Speed Time Time Time Current
         Dload Upload Total Spent Left Speed
100 9832 100 9832 0 0 109k 0 --:--:-- --:--:-- --:--:-- 110k
lxminu-32:Downloads rwartel$ openssl
openssl> openssl
lxminu-32:Downloads rwartel$ openssl x509 -in ddeai25a139558c7bba46b3453dd6611.pem -noout -text
Certificate:
    Data:
      Version: 3 (0x2)
      Serial Number: 1258255408 (0x4aff7430)
      Signature Algorithm: sha512WithRSAEncryption
      Issuer: DC=ch, DC=cern, DC=sts, O=Organization, CN=rwartel
      Validity
        Not Before: Aug 4 14:31:54 2016 GMT
        Not After : Aug 5 14:31:54 2016 GMT
      Subject: DC=ch, DC=cern, DC=sts, O=Organization, CN=1258255408
      Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            00:83:3a:99:fd:35:22:66:8d:7b:65:5e:c1:29:a2:
            02:77:6f:75:55:40:80:ac:fb:b5:14:2b:9f:34:7b:
            fc:a5:34:72:43:2d:ae:2d:52:3b:6c:33:71:e5:49:
            ea:2f:07:03:93:10:d0:b5:8e:1e:f1:a5:b7:2c:27:
            e7:52:93:2d:ad:32:b0:61:12:60:ef:ae:6c:14:f8:
            c6:8e:4d:fe:c7:e2:b0:58:0c:9c:f2:2a:f2:9a:2d:
            1c:d2:f7:a8:fa:14:54:3c:80:81:ab:1f:ac:b6:e4:
            ce:5a:49:e7:64:ac:7b:54:13:38:f7:d7:29:cc:a3:
            12:00:d6:ca:39:c5:8f:17:ce:99:c5:a9:18:e0:92:
            63:f4:3c:0d:3f:c9:c1:4c:3f:b3:5e:5b:61:9a:3e:
            bd:8e:f1:f4:b4:94:11:7e:0b:47:64:91:51:7c:45:
            17:d9:27:53:84:fe:d4:0e:b0:66:37:30:1e:08:57:
            1e:9a:a0:00:b0:c3:52:f0:f6:2f:88:df:ad:78:9c:
            51:bf:4a:c1:4f:bf:07:ed:01:56:c4:28:2f:25:40:
            31:41:d0:5b:4a:2e:56:34:3d:14:5b:f0:68:eb:fc:
            ed:2c:65:95:02:be:d9:d9:77:12:f5:fb:05:03:86:
            d9:08:74:1b:57:52:8c:43:ca:5e:8d:00:7f:52:41:
            42:af
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Key Usage: critical
        Digital Signature, Key Encipherment, Data Encipherment
      Proxy Certificate Information: critical
        Path Length Constraint: 0A
        Policy Language: Inherit all
```


Educert

Educert creates short-lived VOMS Profiles

Your login account must already be registered

bitface

Certificate Generated!



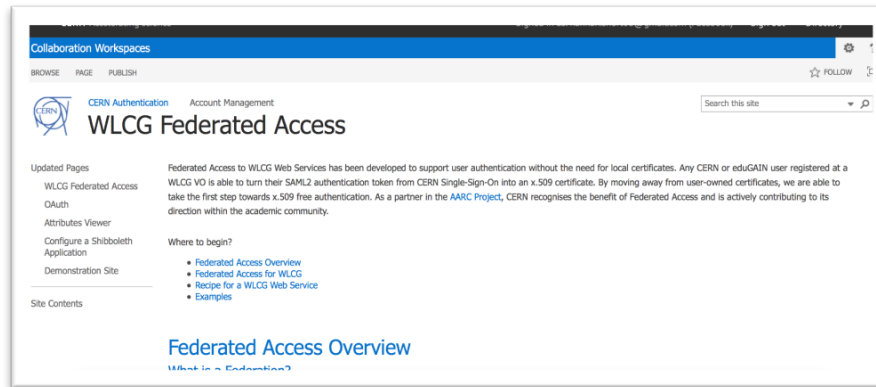
# Kipper

- Kipper is a set of utilities hiding to clients SAML and STS client logic
- Provides as well JS/PHP/Python functions for X509 handling
- WebFTS/Panda integration and EduCERT rely on it
- Kipper, STS and EduCERT software are available on the CERN Gitlab
- <https://gitlab.cern.ch/sts>



# Conclusions

- CERN WLCG IOTA CA has been accepted by IGTF and distributed to sites
- WLCG Web and CLI uses cases are both covered
- VOMS identities linking is the next step, but some VOs are ready ( ATLAS)
- The final goal will be the registration in VOMS without X509 certificate



<https://espace.cern.ch/authentication/CERN%20Authentication/WLCG%20Federated%20Access.aspx>