



WLCG Update

Hannah Short,
CERN Computer Security



Agenda

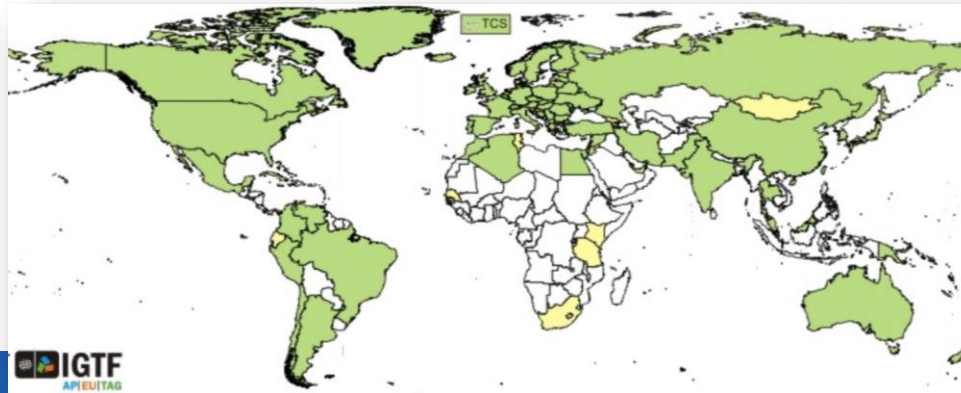
- Background
- Implementation
- Barriers
- Summary

Current Solution – x509

The Interoperable Global Trust Federation (IGTF) controls a list of Certificate Authorities (CAs) able to issue certificates

Users approach their local CA to obtain a personal certificate and undergo identity vetting via a Registration Authority

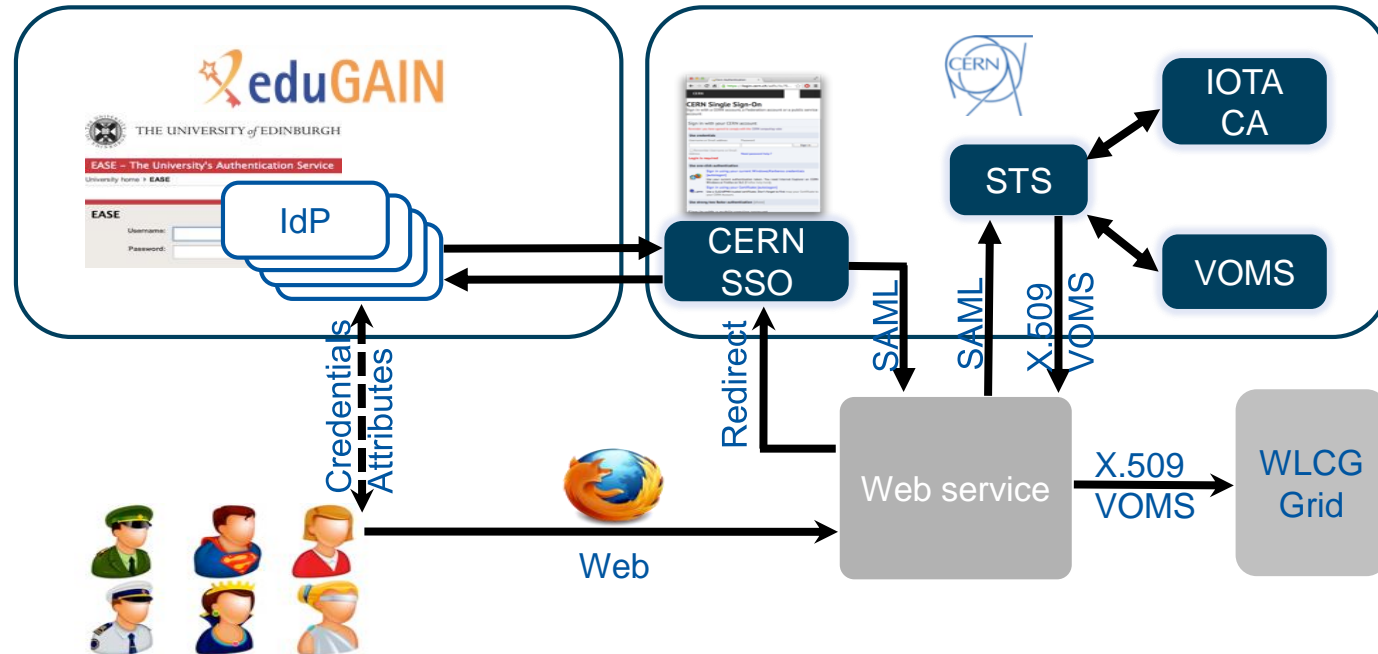
Users register their new certificate in VOMS



Past 5 years at WLCG

- 2012 Contributed to FIM4Rv1
- 2012/13 Token translation service integrated with VOMS, STS, developed under EMI Project
- 2015 STS integrated with WebFTS as a pilot
- 2015 Joined AARC project as security task leader
- 2016 Packaged STS for puppet installation and produced documentation
- 2016 ATLAS's monitoring service starting development work to enable SAML authentication and access control

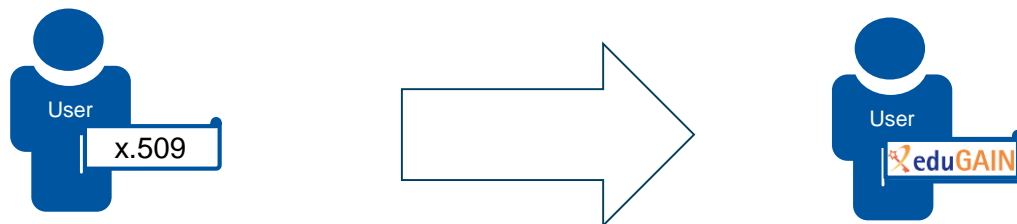
Implementation



What does WLCG need from Federated Access?

- 1 Trustworthy eduGAIN users
- 2 Web and Command Line access
- 3 VOMS Authorisation

1. Trustworthy eduGAIN Users



How can eduGAIN tokens be as trustworthy as x.509 certificates?

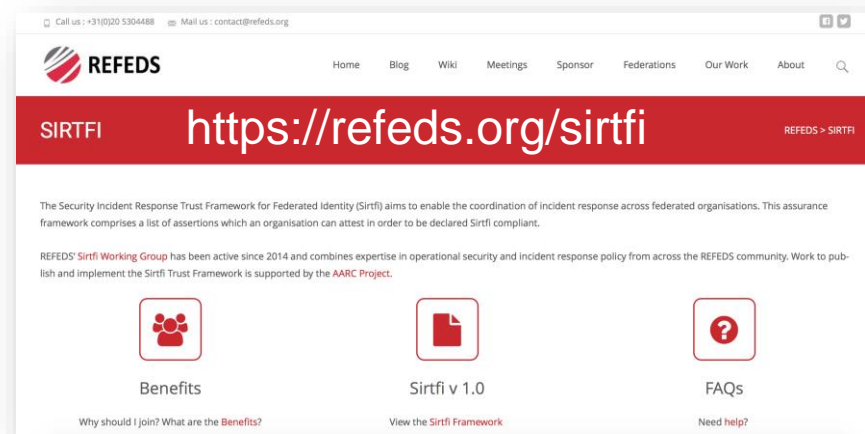
- Restrict eduGAIN to trusted partners
 - Sirtfi
 - Research & Scholarship
- Restrict access to known users
 - Create token translation layer to convert SAML 2.0 token from eduGAIN to required x.509
 - EduGAIN token transformed into x.509 ONLY if the user is registered in VOMS for the relevant experiment

Sirtfi

The Security Incident Response Trust Framework for Federated Identity is a flag for organisations that:

- Have a good baseline in operational security
- Provide a security contact point for emergencies
- Are able and willing to participate in incident response

These are organisations we want to work with!



Research & Scholarship

A flag for organisations that

- Serve the Research & Education community
- Agree to release the attributes
 - Name
 - Email
 - Unique Identifier



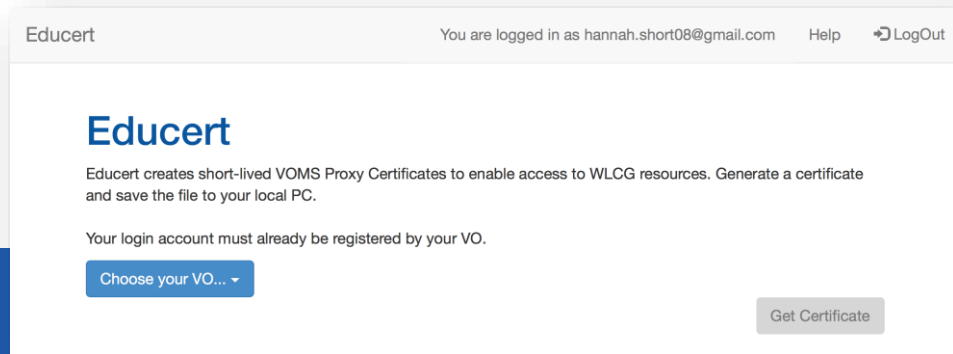
Implement Research and
Scholarship Entity Category

CERN SSO requires this set of attributes, users from these organisations should be able to log in without a problem

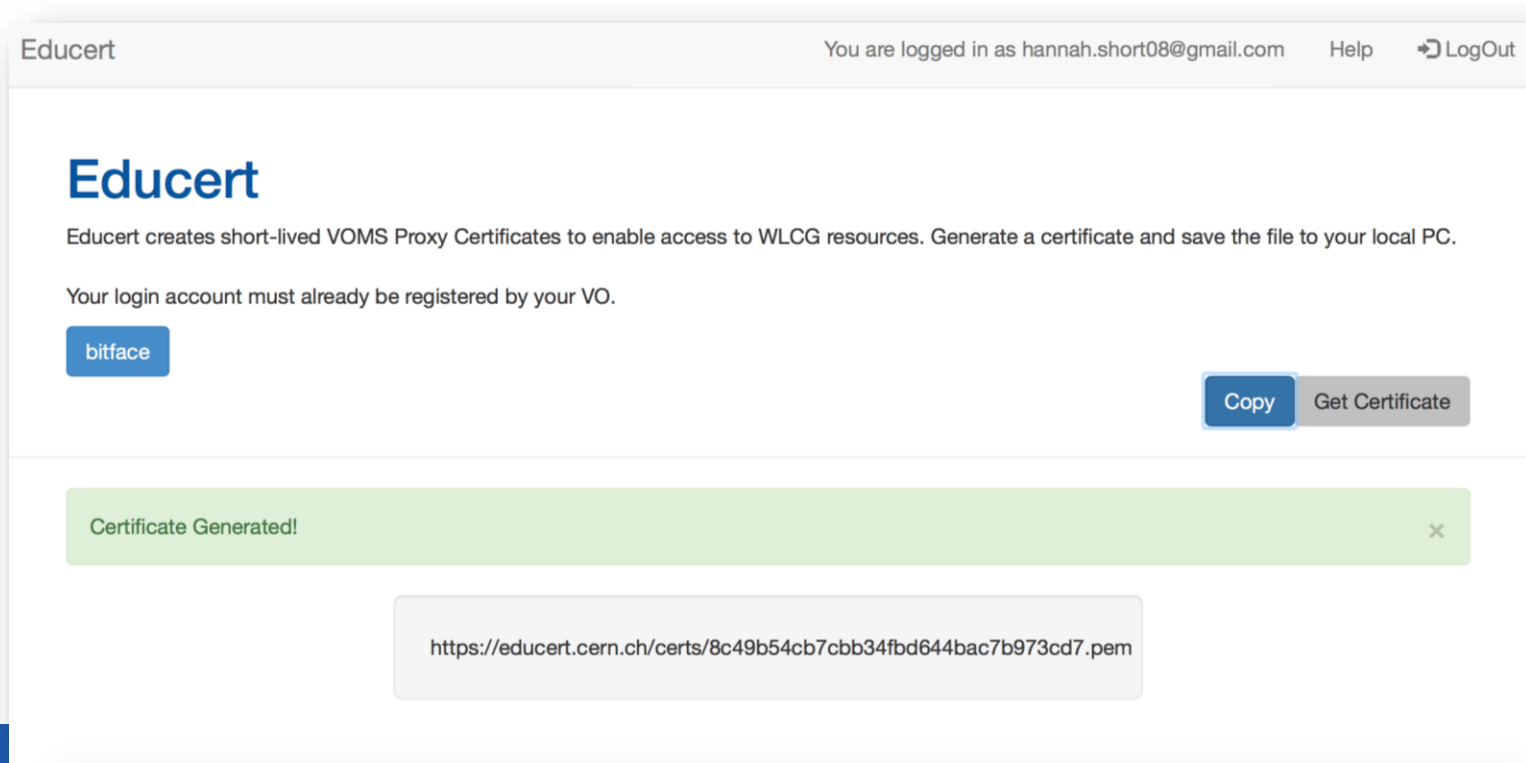


2. Web and Command Line Access

- 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
- A prototype service, Educert, developed for generating GridProxy certificates for download



2. Web and Command Line Access



The screenshot shows the Educert web interface. At the top, the user is logged in as hannah.short08@gmail.com. The main heading is "Educert". Below it, a message states: "Educert creates short-lived VOMS Proxy Certificates to enable access to WLCG resources. Generate a certificate and save the file to your local PC." A note indicates that the user's login account must be registered by their VO. There are two buttons: "bitface" and "Copy Get Certificate". A green notification bar says "Certificate Generated!". Below this, a code block contains the URL: `https://educert.cern.ch/certs/8c49b54cb7cbb34fbd644bac7b973cd7.pem`.

2. Web and Command Line Access

```
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/ddea125a139558c7bba46b3453dd6611.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$ opens
lxminu-32:Downloads$ openssl x509 -in ddea125a139558c7bba46b3453dd6611.pem -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1258255408 (0x4eff7430)
        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=rwartel, 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:
                02:77:67:75:55:40:80:ac:fb:b5:14:2b:9f:34:7b:
                fc:a5:34:72:43:20:ae:2d:52:3b:6c:33:71:e5:49:
                ea:2f:07:03:93:10:d0:b5:8e:1e:ff: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:fd: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:b0:66:37:3d:1e:88:57:
                1e:9a:a8:00:b0:c3:52:f0:f6:2f:88:df:ad:78:9c:
                51:bf:4a:c1:4f:bf:87:ed:01:56:c4:28:2f:25:40:
                31:41:d8:5b:4a:2e:56:34:3d:14:5b:f0:60:eb:fc:
                ed:2c:65:95:02:be:d9:d9:77:12:f9:fb:05:03:06:
                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
```

3. VOMS Integration

Transparent access to WLCG resources (controlled via x.509) only granted when the incoming token matches with a VOMS record. STS then adds the IOTA DN to the VOMS record on the first time it is used.

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

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

HNSciCloud

- Helix Nebula Science Cloud pre-commercial procurement project to find a cloud provider to satisfy computing demands of multiple research communities (including WLCG)
- SAML2.0 consumption part of tender specification
- In practice this requires the cloud provider to do significant development work (including proxies, token translation, etc)
- Considering policy aspect, Sirtfi, CoCo, MFA, LoA?

How is it all going?

- Experiments want a browser independent, command-line access mechanism
- One STS instance is required per web service, per VO... this is not an easy conversion! Providing a central service would help
- Little trust in operational capability of eduGAIN so far (fingers crossed that this is improving as we speak!)

