Scenario Planning and Reporting: AAI

Paul Millar
Why Federated Identity?

A quick introduction

Disclaimer: I'm skipping over many of the details ...
"It's been a global effort, a global success. It has only been possible because of the extraordinary achievements of the experiments, infrastructure and the grid computing."

Rolf Heuer, the Director General of CERN
Why Federated Identity?

Typical user reaction to X.509 (client) certificates
Why Federated Identity?

What they want is used to:

- Windows Server 2008 Standard
- FTP login dialog
- Debian login dialog
- User name: softpedia
- Password: ********
Why Federated Identity?

Why this doesn't work:

I'LL JUST USE THE SAME PASSWORD

EVERYWHERE
Why Federated Identity?

Federated Identity allows users to reuse their password safely...

... and finding out who just authenticated
Why Federated Identity?

EGI FedCloud is (currently) using X.509 for authentication

Unfortunately SAML is not compatible with X.509
Why Federated Identity?

We want SAML to work with X.509

We have to make this fit into the hole made for this using nothing but this
Why Federated Identity?

Federation

CTS

Science Gateway

Large-scale resources
(needs X.509 authn)
Menu: today's specials...

Diego: the FedCloud AAI survey
David: LoA and reverse-LoA
Peter: “The Future” – the EGI AAI Pilot and AARC
Diego: “The here and now” – per-user sub-proxies

Discussion per-user sub-proxies – next steps
Federated Identity

Check who you are & Authorisation decision

Check who you are

Identity Provider (IdP)

Record information

Assertion

Service Provider (SP)
Types of cred-translation
Types of cred-translation

1. Firefox
2. CSR
3. TempID
4. MyProxy-OAuth
5. SAML
6. SAML WebSSO
7. IdP
8. Portal
9. X.509

IdP -> MyProxy-OAuth -> Portal
SAML WebSSO -> MyProxy-OAuth

01/05/16
EGI-InSPIRE RI-261323
Types of cred-translation

Diagram stolen from http://pos.sissa.it/archive/conferences/162/150/EGICF12-EMITC2_150.pdf