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:

- Enter your name and password for the server "ftp.ucsb.edu".
- Connect as: Guest or Registered User.
- Name: John Smith
- Password: [redacted]
- Remember this password in my keychain

Welcome to debian

- Username: softpedia
- Password: [redacted]
Why Federated Identity?

Why this doesn't work:

I'LL JUST USE THE SAME PASSWORD EVERYWHERE
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?

Large-scale resources (needs X.509 authn)
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
Danger: scary details ahead!

Backup slides
Federated Identity

Check who you are & Authorisation decision

Check who you are

Record information

Identity Provider (IdP)

Assertion

Service Provider (SP)

01/05/16
EGI-InSPIRE RI-261323
www.egi.eu
Types of cred-translation

1. in-band
2.  
3.  
4.  
5.  
6.  
7.  

1. out-of-band
2.  
3.  
4.  
5.  

IdP  CTS  Portal

SAML Delegation
Types of cred-translation

1. MyProxy-OAuth
2. SAML WebSSO
3. CSR
4. Portal
5. SAML
6. MyProxy-OAuth
7. Temp ID
8. X.509
9. Temp ID

IdP
Types of cred-translation

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