Identity Workshop:
Introduction to Federated Identity

Brook Schofield, TERENA
Digital Inclusion Task Leader, GN3plus Project
25 June 2014
The Situation on Campus: Lots of Applications

- More applications for students and researchers
- Applications require authentication and authorization
Lots of Applications → Lots of Passwords

- One password for each application does not scale
- Tons of passwords to manage for users and service operators
- Varying degree of password security
- Increased helpdesk/user work due to password resets
- Collaborative usage of applications is difficult
Pick the fake UNNOBA login #1
Pick the fake UNNOBA login #2
Pick the fake UNNOBA login #3
Pick the fake UNNOBA login

#4

Preinscripción a carreras

Ayuda para conectarse

PASO1:
Para Preinscribirte por primera vez haz click en "Registrarse como Usuario"
Tu preinscripción no está completa hasta que presentes toda la documentación
solicitada y el formulario obtenido por este sistema, en el Departamento de Alumnos
de la Universidad (sede Junín o Pergamino) entre el 04/11/2013 y el 20/12/2013.

Antes de comenzar el proceso de preinscripción asegurarte de tener una dirección
de correo electrónico válida y que funcione correctamente.

PASO2:
Ingresá tu identificación
Si ya te registraste, podés ingresar para completar tus datos de la preinscripción,
escribiendo tu usuario (que es tu Nro. de Documento) y la clave que ingresaste
en el Paso 1.

¿Ya eres usuario del sistema?

Usuario:

Clave:

Registrarse como usuario
¿Olvidaste tu contraseña?

Desarrollado por Consorcio SiU
Pick the fake UNNOBA login #5
Pick the fake UNNOBA login ....the answer?
The Solution: Identity Management

- Campus Identity Management
  - One login name and password for users
  - Password entered only at home login
  - Integration of campus applications

- Expand beyond the campus
  - Create an (identity) federation
  - Multiple organisations/services agree on common technical and legal standards
  - Mutually trust each other's assertions
  - Collaborate, e.g. common e-learning

- First Academic Identity Federations started in mid-2000s
A family of services...

eduroam

eduGAIN
Web Single Sign On Technologies
Authentication services you use...
Hub&Spoke Federation with Central Login

~5% of all Federations
- FEIDE
- AAI@EduHr

Also used by
- Facebook
- Twitter
- Google+

Requires “trust” in the Operator
Hub&Spoke Federation with Central Login

~5% of all Federations
• FEIDE
• AAI@EduHr

Also used by
• Facebook
• Twitter
• Google+

Requires “trust” in the Operator
Hub&Spoke Federation with Distributed Login

~15% of Federations
- SURFconext
- WAYF (Denmark)
- SIR
- TAAT
- Confia

Operator can see the “content” of Auth messages
Hub&Spoke Federation with Distributed Login

~15% of Federations
• SURFconext
• WAYF (Denmark)
• SIR
• TAAT
• Confia

Operator can see the “content” of Auth messages
Full Mesh Federation

~80% of Federations
- COFRe
- CAFe
- InCommon
- UKAMF
- SWAMID
- HAKA
- AAF
- SWITCHaai
- ...

---

SAML Assertion Flow

Connection to User Directory
Full Mesh Federation

~80% of Federations

- COFRe
- CAFe
- InCommon
- UKAMF
- SWAMID
- HAKA
- AAF
- SWITCHaai
- ...

![Diagram of Full Mesh Federation](image-url)
Identity Federations
World Wide

Last update May 2014

31 Production Federations
17 Pilot Federations
Identity Federations in Europe

**Eastern Partnership**
- Armenia
- Azerbaijan
- Belarus
- Georgia
- Moldova
- Ukraine

**Throughout Europe**
- Albania
- Andorra
- Bulgaria
- Bosnia & Herzegovina
- Cyprus
- Luxembourg
- Macedonia
- Montenegro
- Slovakia

[Map showing production and pilot federations]
Identity Federations Are Traditionally National

All Federations:
- Support SAML2
- education & research
- Use same/similar user attributes
What Is it? …and How Does it Work?

- MDS fetches, aggregates and republishes metadata
- eduGAIN provides policy framework and standards to build trust
More "Realistic" Architecture
eduGAIN: Legal Trust and Profiles

- **eduGAIN Declaration (3 pages)**
  - Signed by each Member Federation
  - Contains 13 rules that federations promise to obey

- **eduGAIN Constitution (10 pages)**
  - Profiles for SAML, Metadata, Attributes, ...

- **GEANT Data Protection Code of Conduct**
  - Declaration of Service Providers to "behave well" with user data
  - Applicable in EU/EEA or similar
eduGAIN & Federations

1 April 2013

- 18 eduGAIN Members
- 2 Joining eduGAIN
- 9 Candidate Federation
eduGAIN & Federations

1 April 2014

- 24 eduGAIN Members
- 6 Joining eduGAIN
- 1 Candidate Federation
eduGAIN & Federations

15 April 2014

- 24 eduGAIN Members
- 7 Joining eduGAIN
- 0 Candidate Federation
eduGAIN & Federations

15 April 2014

- 24 eduGAIN Members
- 7 Joining eduGAIN
- 0 Candidate Federation
- 17 Other Federations
Technology

Policy
eduGAIN & Federation is about Trust