Europe Latin America Collaborative e-Infrastructure for Research Activities

TICAR2014

Brook Schofield, TERENA ● TICAR 2014 ● 24th April 2014

About me…

- Brook Schofield
- mailto:schofield@terena.org
- skype://brookschofield
- tel:+31651553991
- http://terena.org/~schofield
- linkedin.com/in/brookschofield

I work at TERENA.

eduGAIN Task Leader in the GN3plus Project.

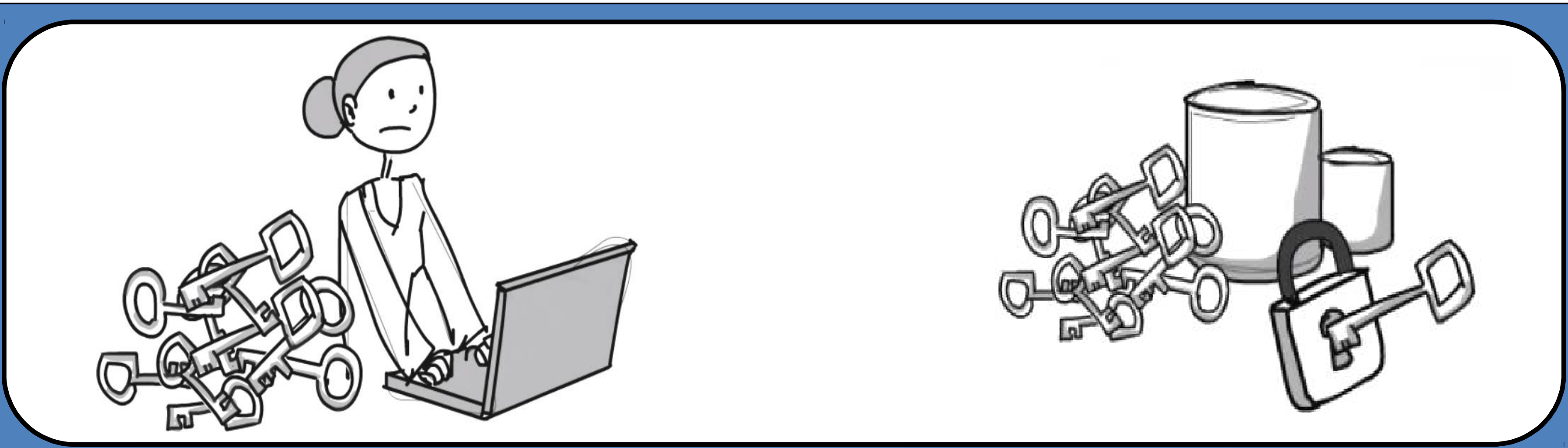
eduroam Global Governance Secretary.

The Situation on Campus: Lots of Applications

Europe Latin America Collaborative e-Infrastructure for Research Activities

- More applications for students and researchers
- Applications require authentication and authorization

Lots of Applications
□ Lots of Passwords

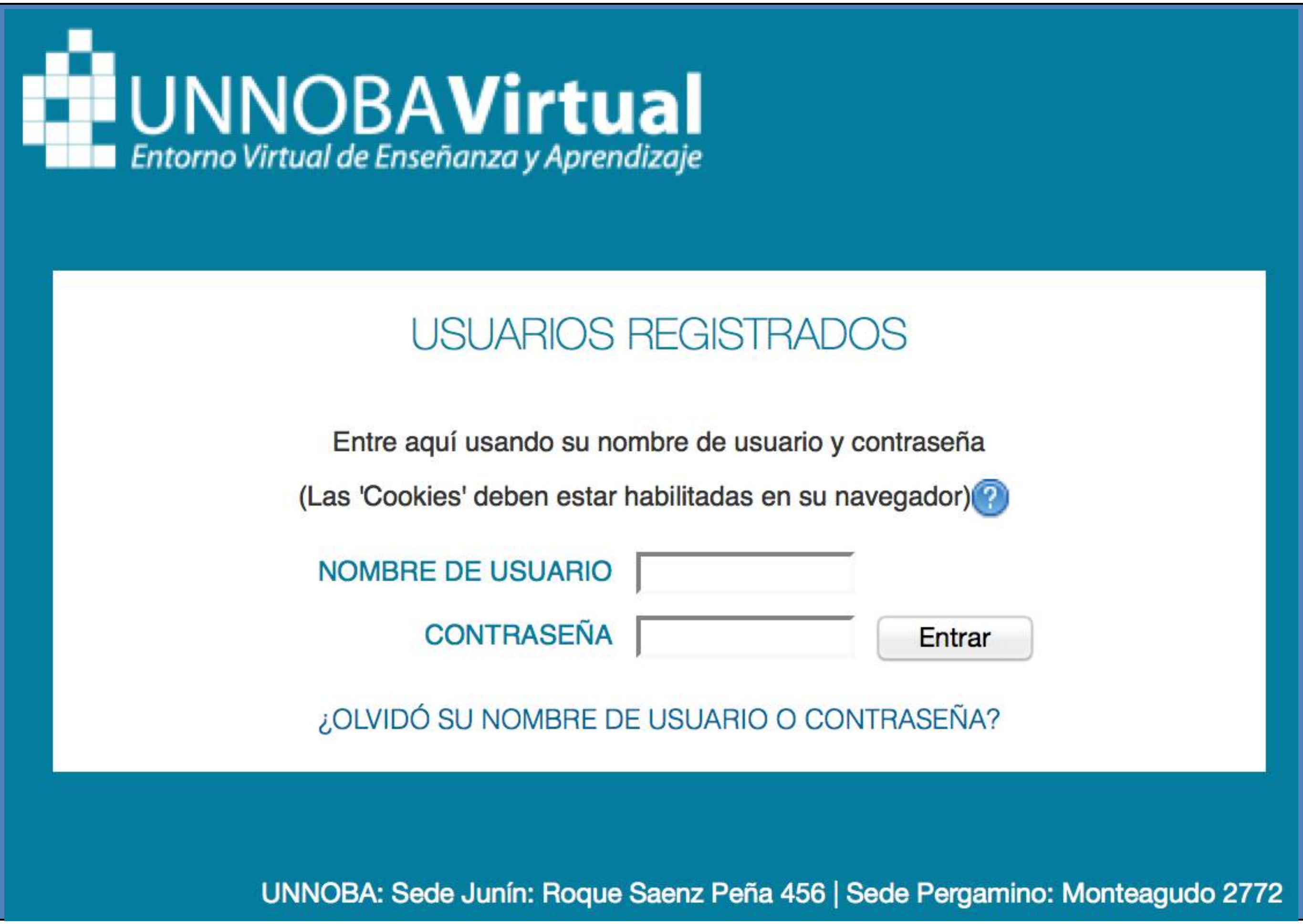


- One password for each application does not scale
- Tons of passwords to manage for users and service operators
- Varying degree of password security
- Increased helpdesk/user work due to password resets
- Collaborative usage of applications is difficult

The Solution: Identity Management

- Create an (identity) federation:
  - Multiple organisations/services agree on common technical and legal standards
  - Deploy Identity and Service Providers
  - Mutually trust each other's assertions
  - Collaborate, e.g. common e-learning
- One login name and password for users
- Password entered only at home login page
- Many countries have national academic identity federations today!
- First Academic Identity Federations started in mid-2000s

Pick the fake UNNOBA login #1



UNNOBAVirtual

Entorno Virtual de Enseñanza y Aprendizaje

USUARIOS REGISTRADOS

Entre aquí usando su nombre de usuario y contraseña

(Las 'Cookies' deben estar habilitadas en su navegador)

NOMBRE DE USUARIO

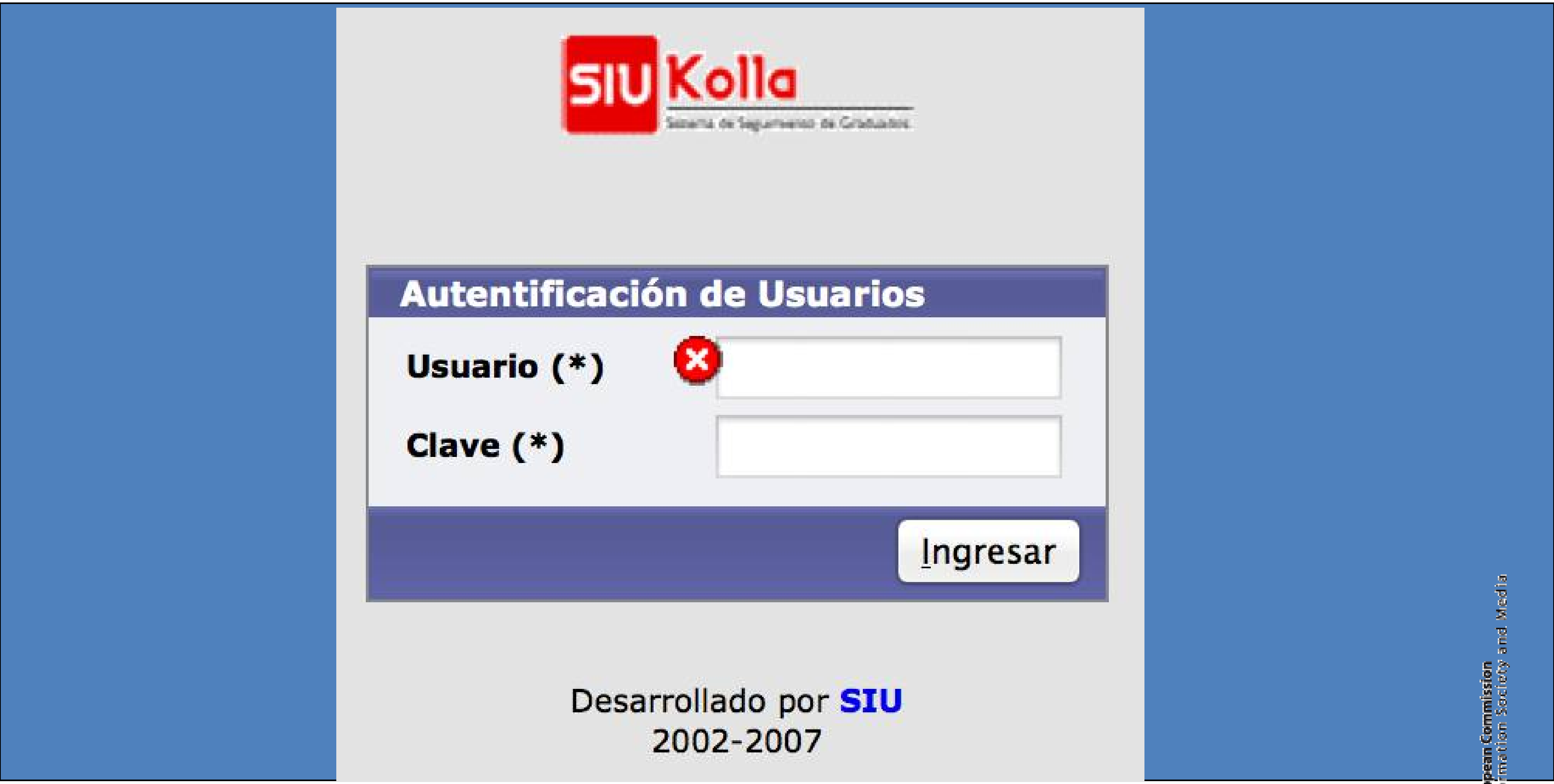
CONTRASEÑA

¿OLVIDÓ SU NOMBRE DE USUARIO O CONTRASEÑA?

UNNOBA: Sede Junín: Roque Saenz Peña 456 | Sede Pergamino: Monteagudo 2772

Pick the fake UNNOBA login #2

Europe Latin America
Collaborative e-Infrastructure
for Research Activities



SIU Kolla
Sistema de Seguimiento de Graduados

Autentificación de Usuarios

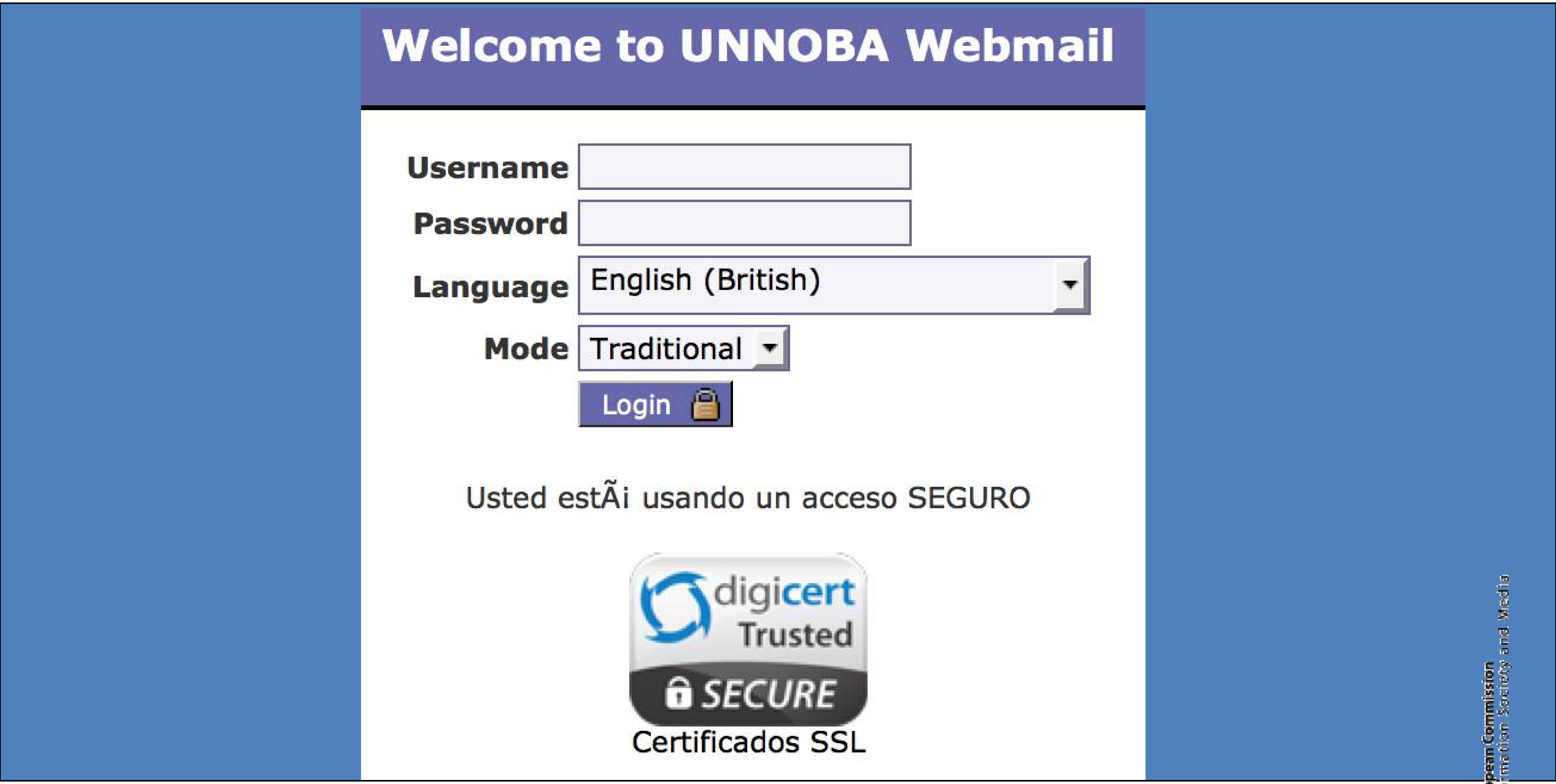
Usuario (*)	☒
Clave (*)	

Desarrollado por **SIU**
2002-2007

e-infrastructure

European Commission
Information Society and Media

Pick the fake UNNOBA login #3



Welcome to UNNOBA Webmail

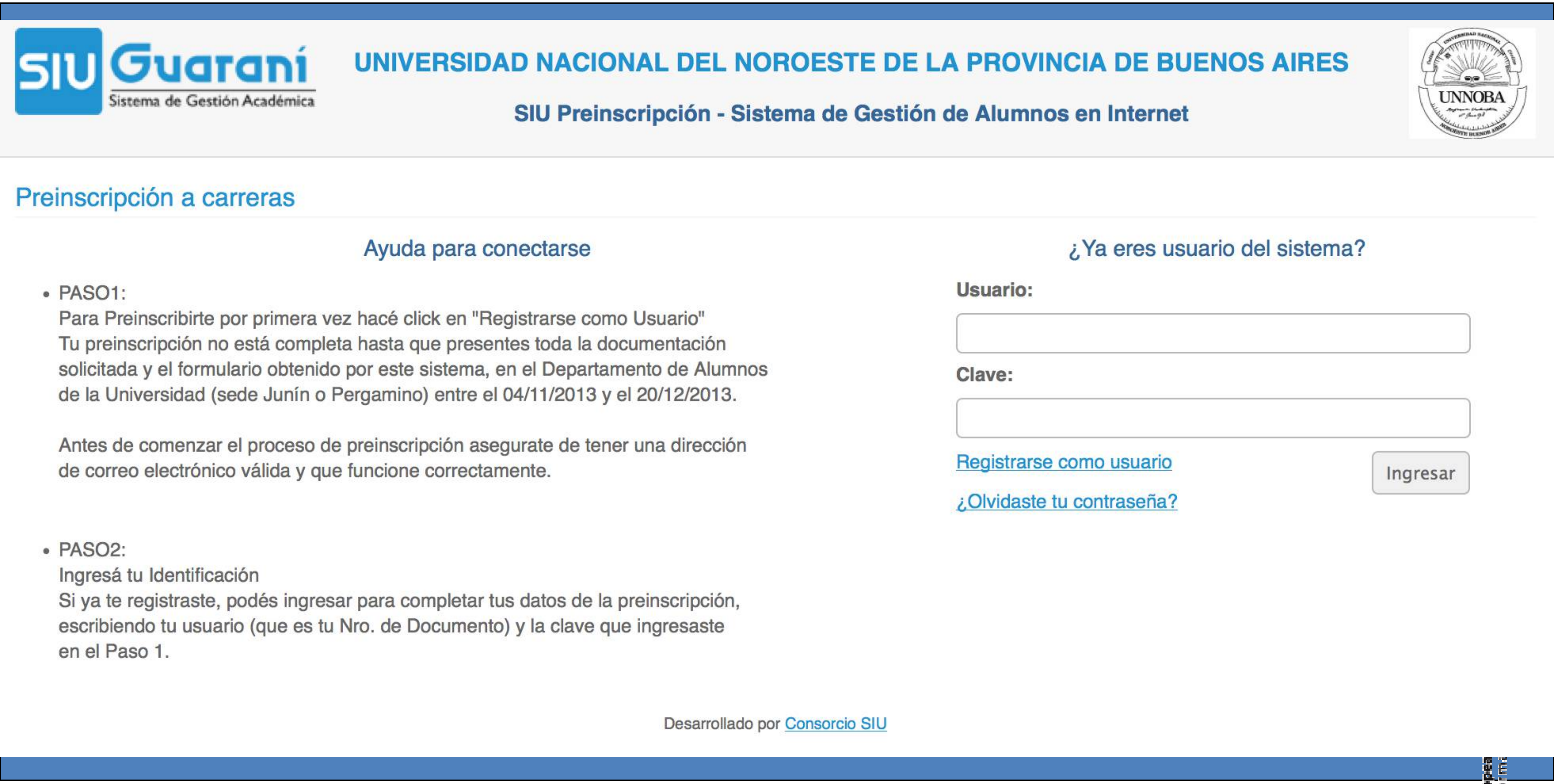
Username	
Password	
Language	English (British)
Mode	Traditional

Usted estÃi usando un acceso SEGURO

Certificados SSL

Pick the fake UNNOBA login #4

elcira
Europe Latin America
Collaborative e-Infrastructure
for Research Activities



UNIVERSIDAD NACIONAL DEL NOROESTE DE LA PROVINCIA DE BUENOS AIRES

SIU Preinscripción - Sistema de Gestión de Alumnos en Internet

Preinscripción a carreras

Ayuda para conectarse

- PASO1:
  Para Preinscribirte por primera vez hacé 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 asegurate 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:

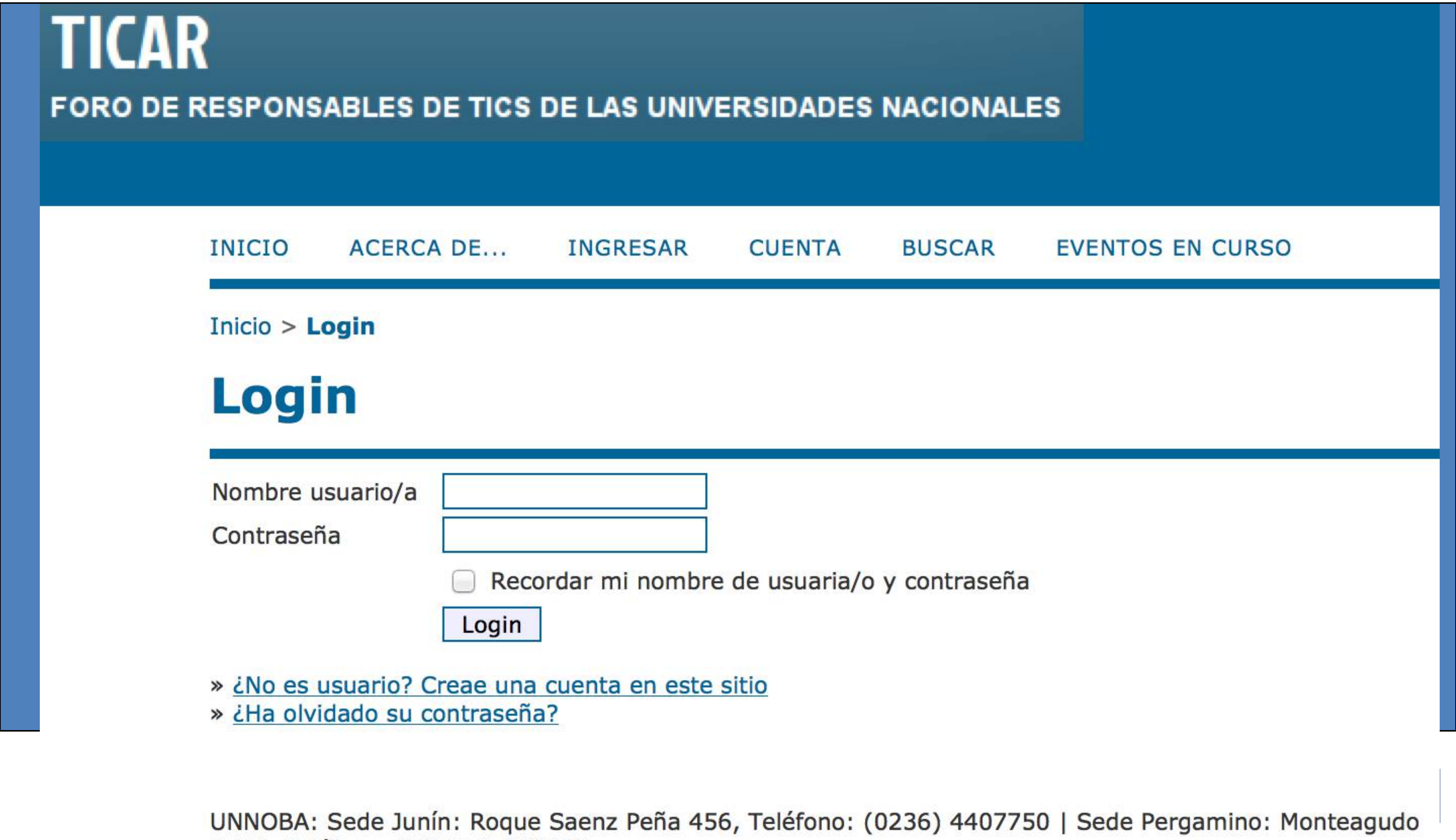
Clave:

Desarrollado por Consorcio SIU

e-infrastructure

Pick the fake UNNOBA login #5

elcira
Europe Latin America
Collaborative e-Infrastructure
for Research Activities



TICAR

FORO DE RESPONSABLES DE TICS DE LAS UNIVERSIDADES NACIONALES

INICIO ACERCA DE... INGRESAR CUENTA BUSCAR EVENTOS EN CURSO

Inicio > **Login**

Login

Nombre usuario/a

Contraseña

□ Recordar mi nombre de usuaria/o y contraseña

Login

» ¿No es usuario? Creae una cuenta en este sitio
» ¿Ha olvidado su contraseña?

UNNOBA: Sede Junín: Roque Saenz Peña 456, Teléfono: (0236) 4407750 | Sede Pergamino: Monteagudo

Pick the fake UNNOBA login

Europe Latin America Collaborative e-Infrastructure for Research Activities

- 1 - ?
- 2 - ?
- 3 - ?
- 4 - ?
- 5 - ?

European Commission
Information Society and Media

e-infrastructure

Pick the fake UNNOBA login

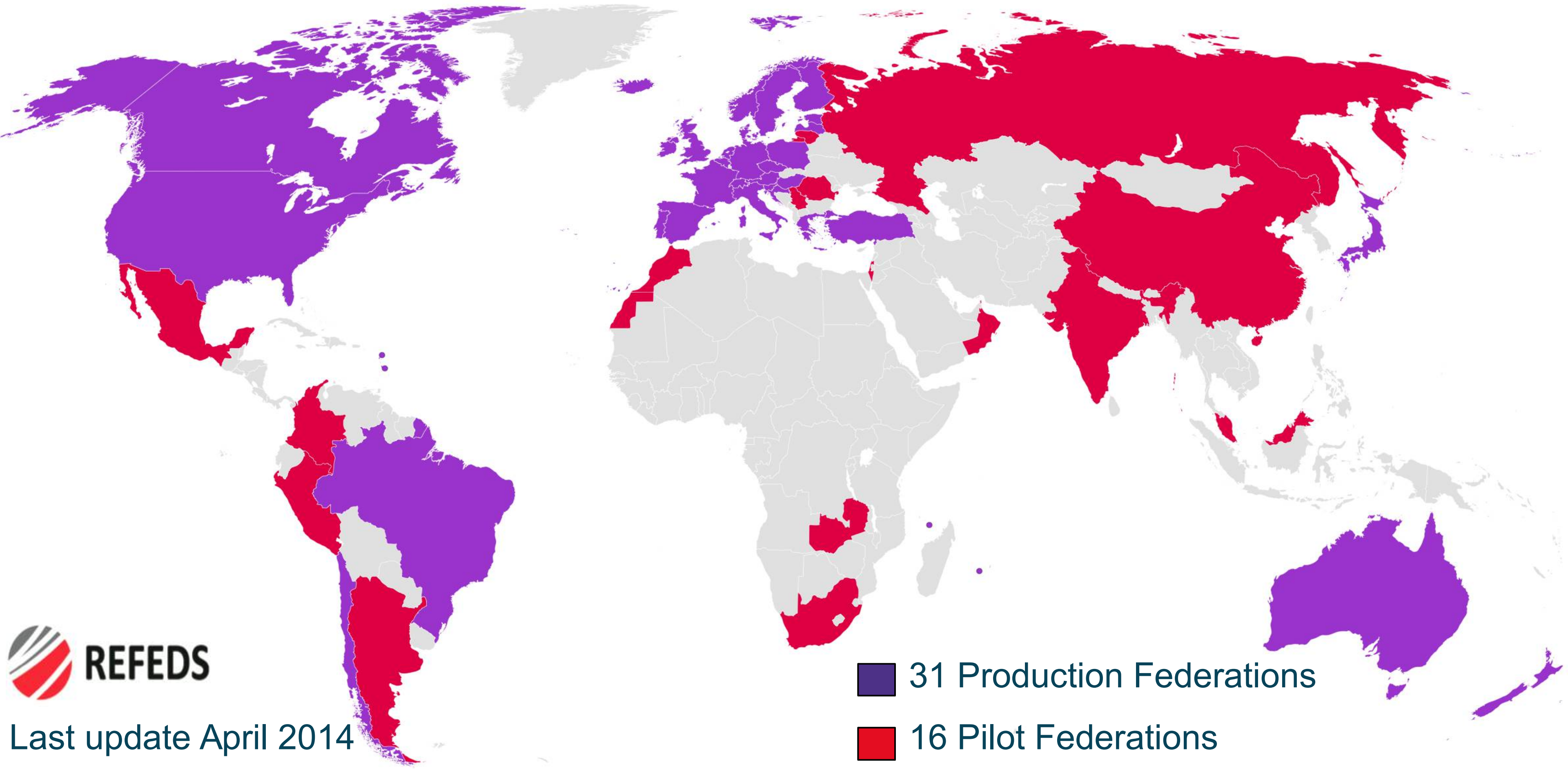
- All these pages are legitimate
- How do your users know?
- Phishing attempts are easy with so much variation
- User education is impossible – or very hard

Authentication services you already use…

Identity Federations World Wide

elcira

Europe Latin America
Collaborative e-Infrastructure
for Research Activities



REFEDS

Last update April 2014

🟪 31 Production Federations

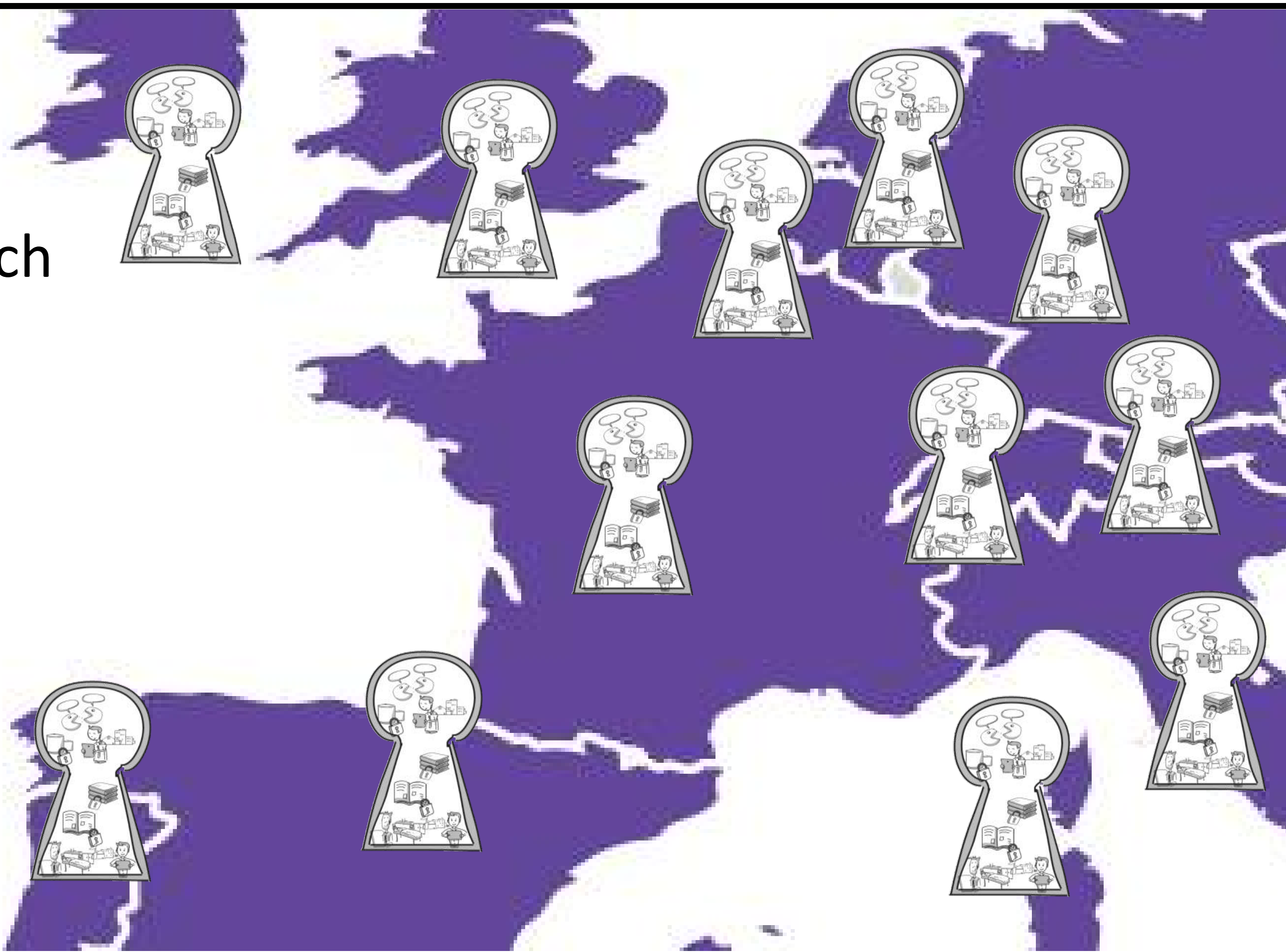
🟥 16 Pilot Federations

e-infrastructure

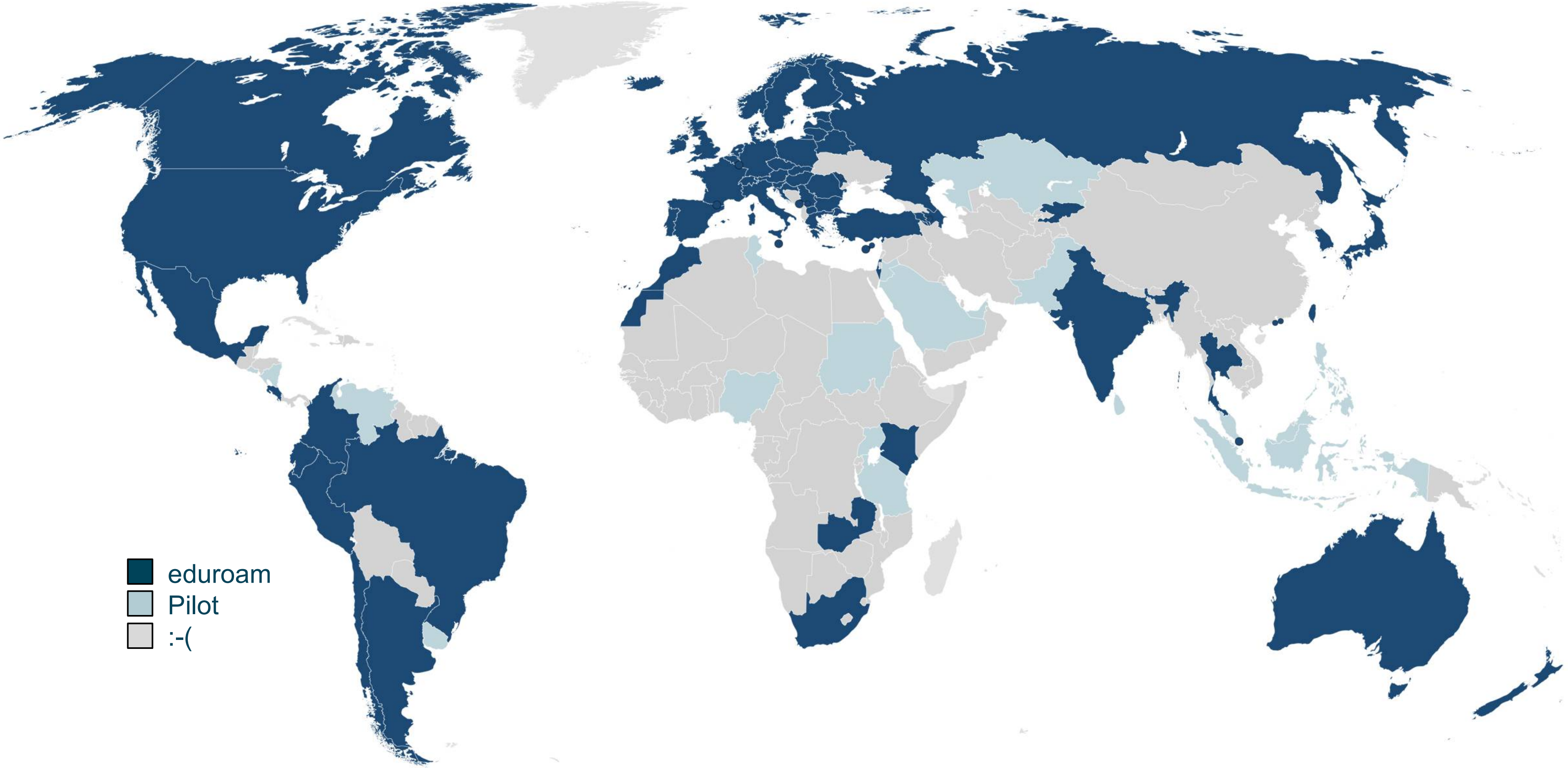
Identity Federations Are Traditionally National

All Federations:

- Support SAML2
- education & research
- Use same/similar user attributes



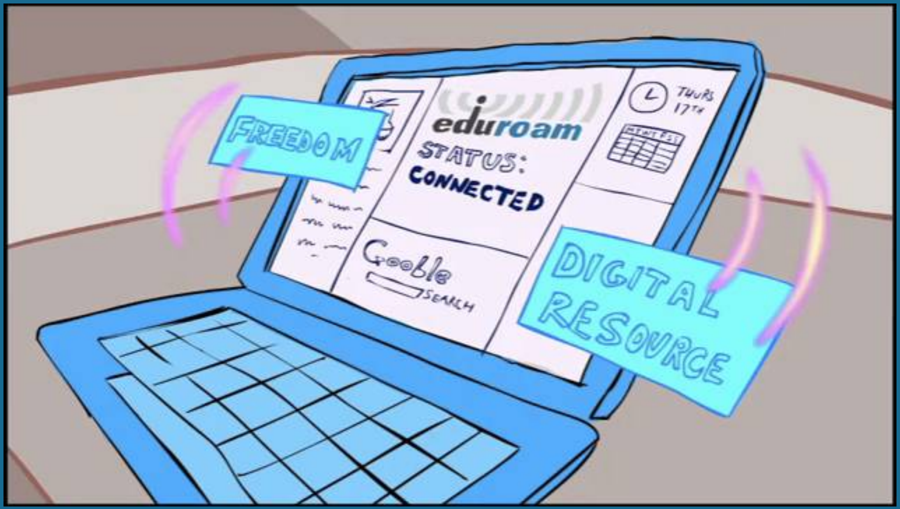
eduroam – roam across borders



eduroam

education roaming

Secure Wireless Service for Research and Education



What is eduroam?

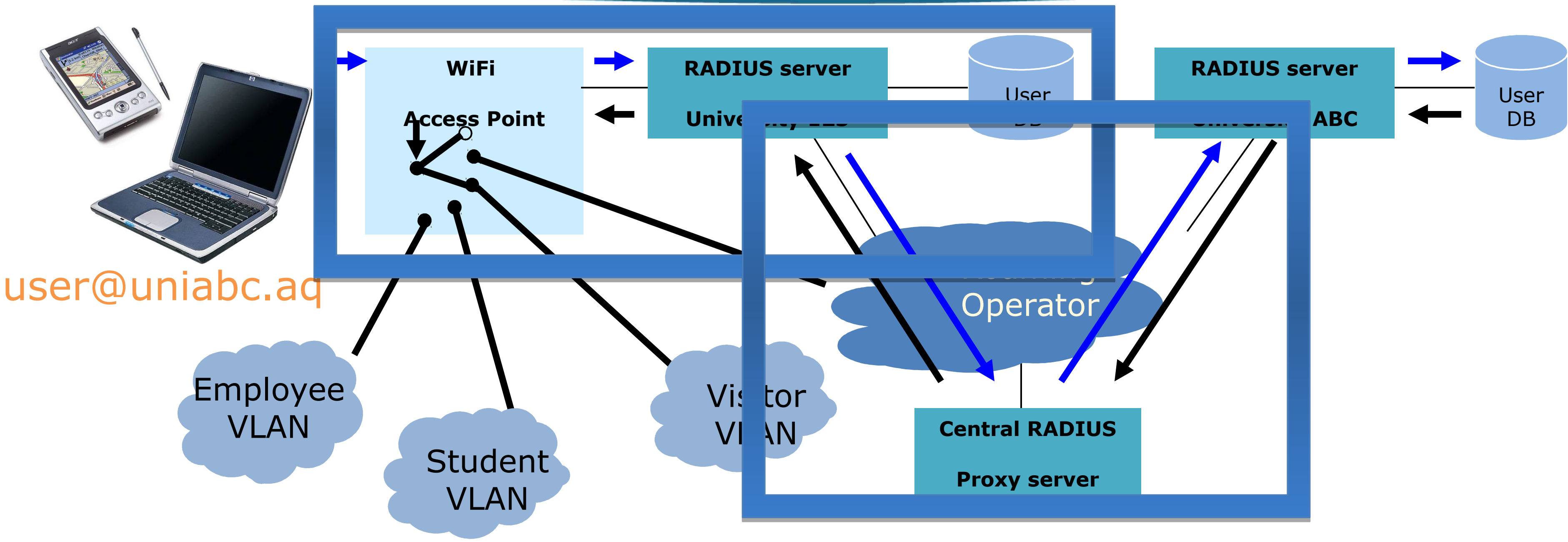
eduroam is a global wireless roaming network, based on:

- WPA2 & 802.1X (network access control)
- RADIUS (infrastructure to transport credentials)
- Trust fabric (RADIUS hierarchy and policy)
- No web splash screen portal or shared passwords

Started in the TERENA Task Force “Mobility”

eduroam = education roaming

eduroam Infrastructure

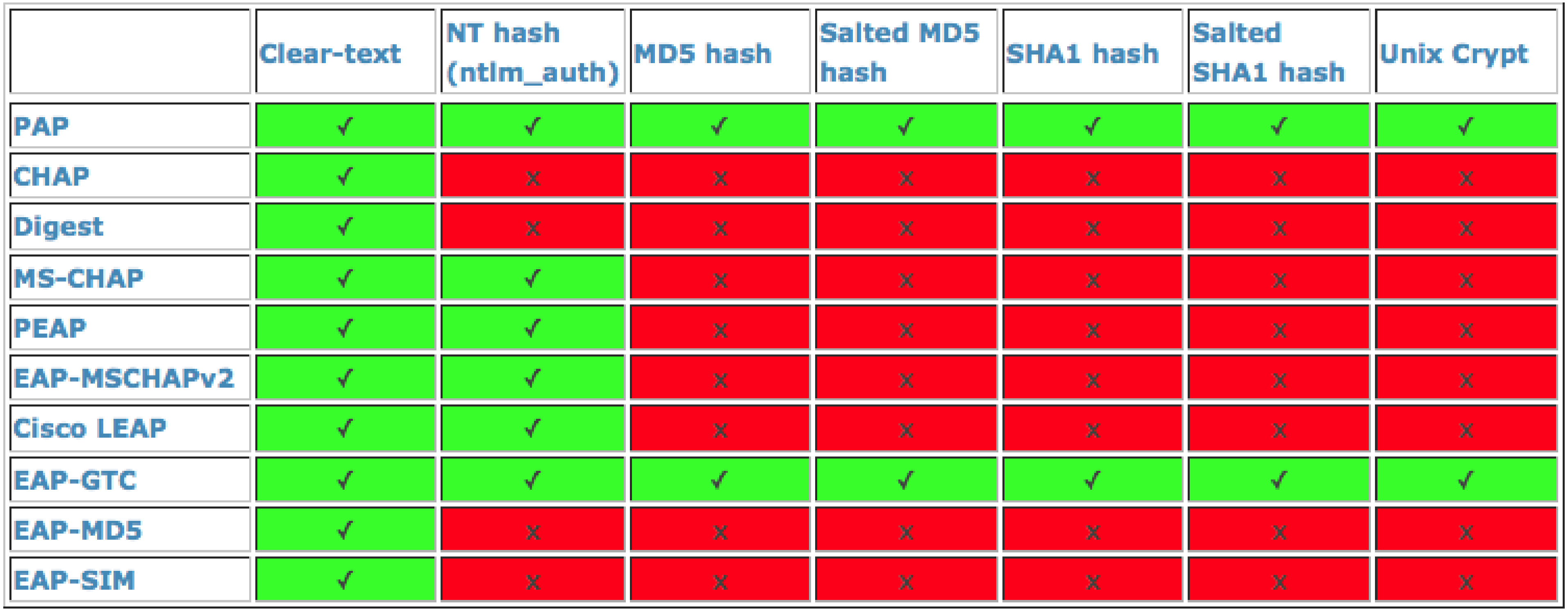


signaling

data

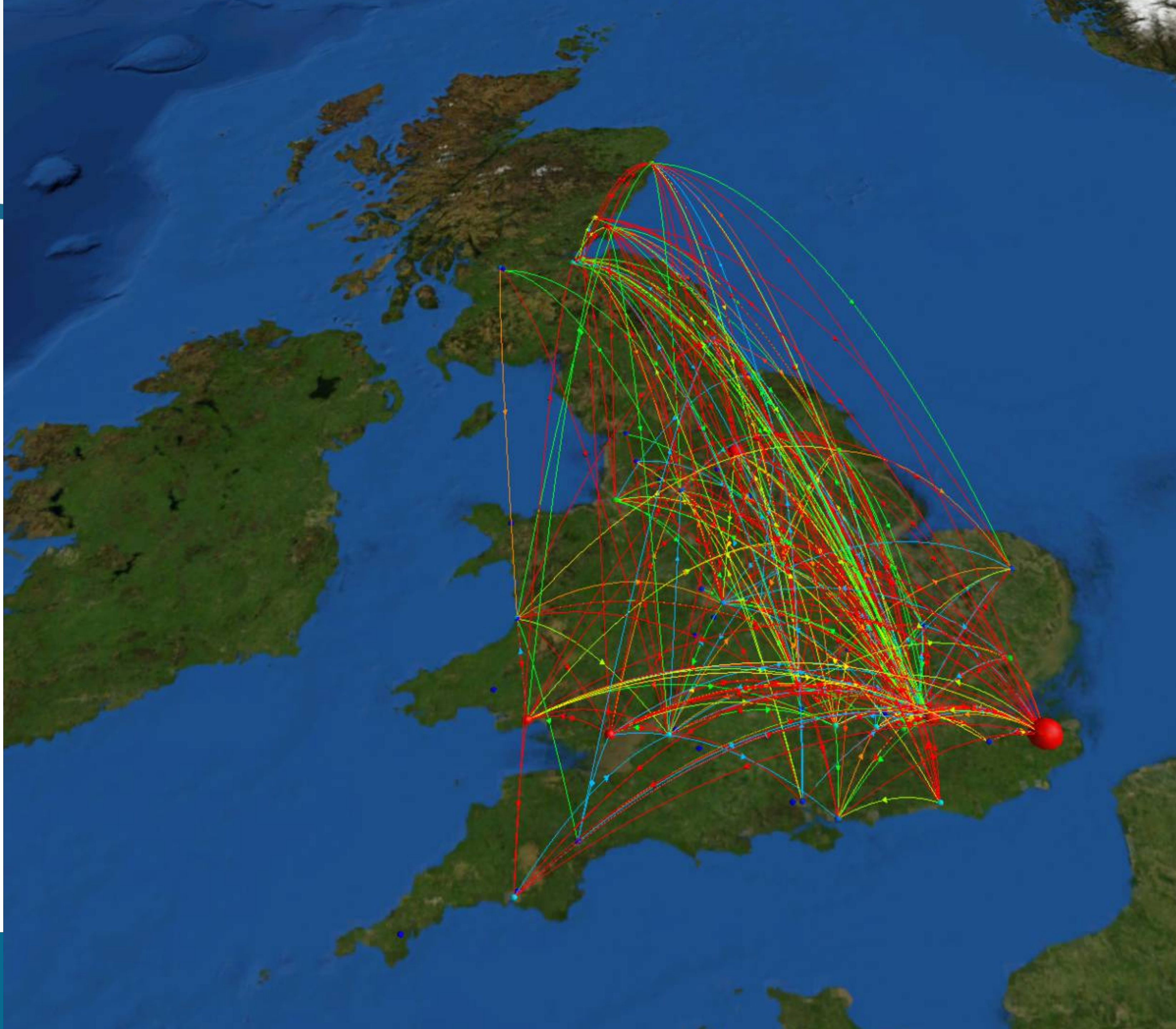
- Trust based on national policy
- Security based on 802.1X/RADIUS
- VLAN assignment to separate users

Flexible password storage infrastructure...



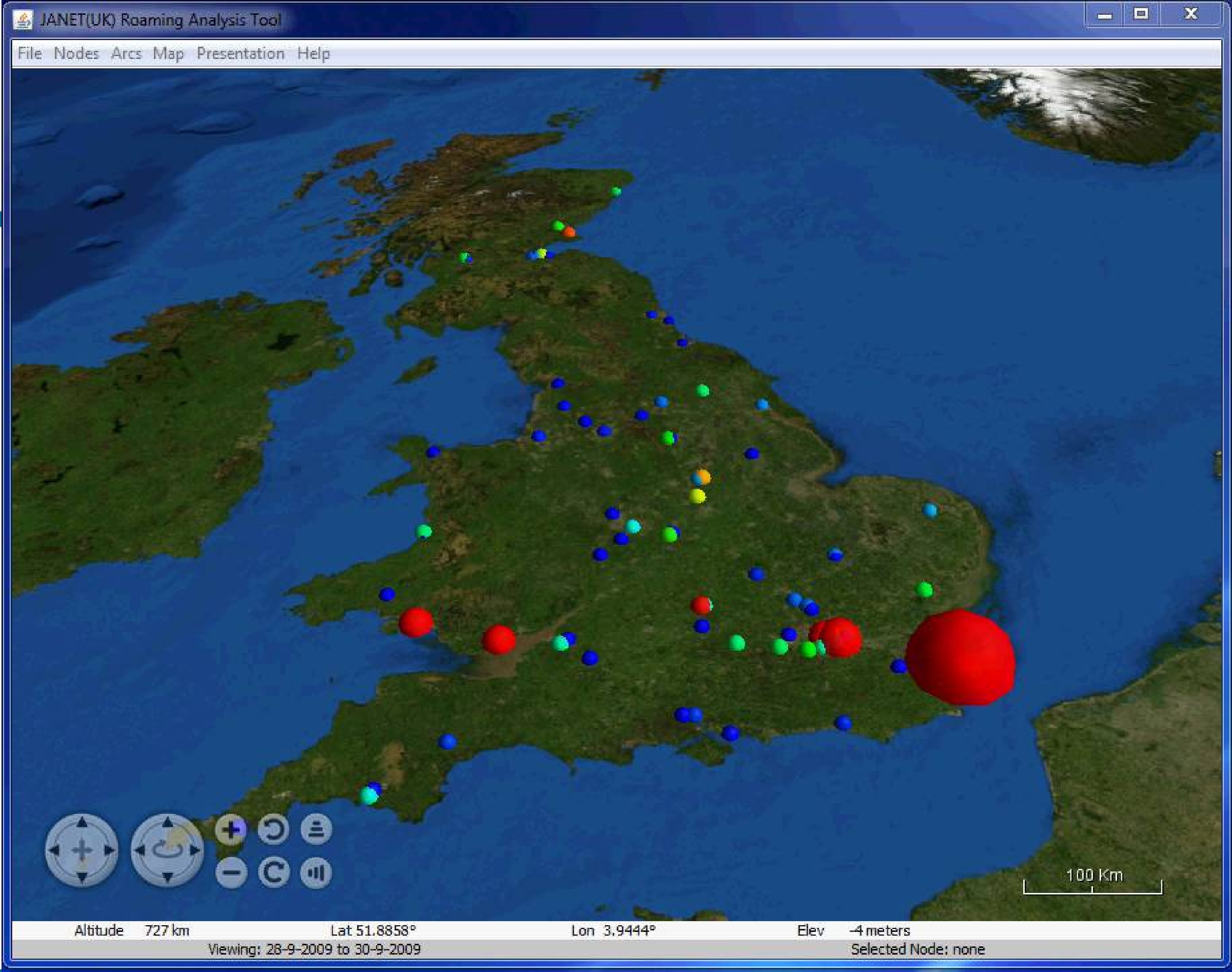
	Clear-text	NT hash (ntlm_auth)	MD5 hash	Salted MD5 hash	SHA1 hash	Salted SHA1 hash	Unix Crypt
PAP	✓	✓	✓	✓	✓	✓	✓
CHAP	✓	✗	✗	✗	✗	✗	✗
Digest	✓	✗	✗	✗	✗	✗	✗
MS-CHAP	✓	✓	✗	✗	✗	✗	✗
PEAP	✓	✓	✗	✗	✗	✗	✗
EAP-MSCHAPv2	✓	✓	✗	✗	✗	✗	✗
Cisco LEAP	✓	✓	✗	✗	✗	✗	✗
EAP-GTC	✓	✓	✓	✓	✓	✓	✓
EAP-MD5	✓	✗	✗	✗	✗	✗	✗
EAP-SIM	✓	✗	✗	✗	✗	✗	✗

http://deployingradius.com/documents/protocols/compatibility.html



janet

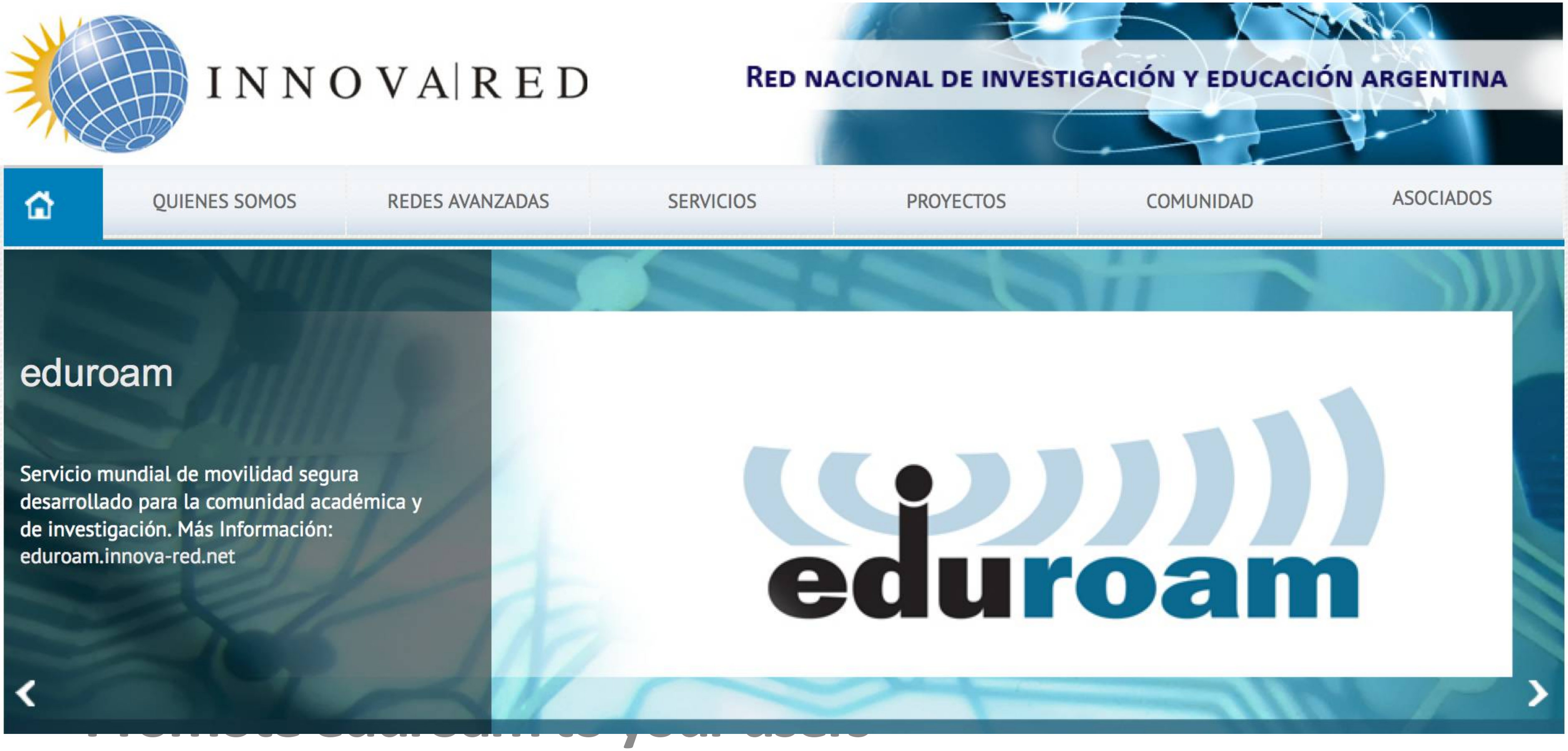
insert logo



Altitude 727 km Lat 51.8858° Lon 3.9444° Elev -4 meters

Viewing: 28-9-2009 to 30-9-2009 Selected Node: none

How do I join eduroam?



INNOVA|RED

RED NACIONAL DE INVESTIGACIÓN Y EDUCACIÓN ARGENTINA

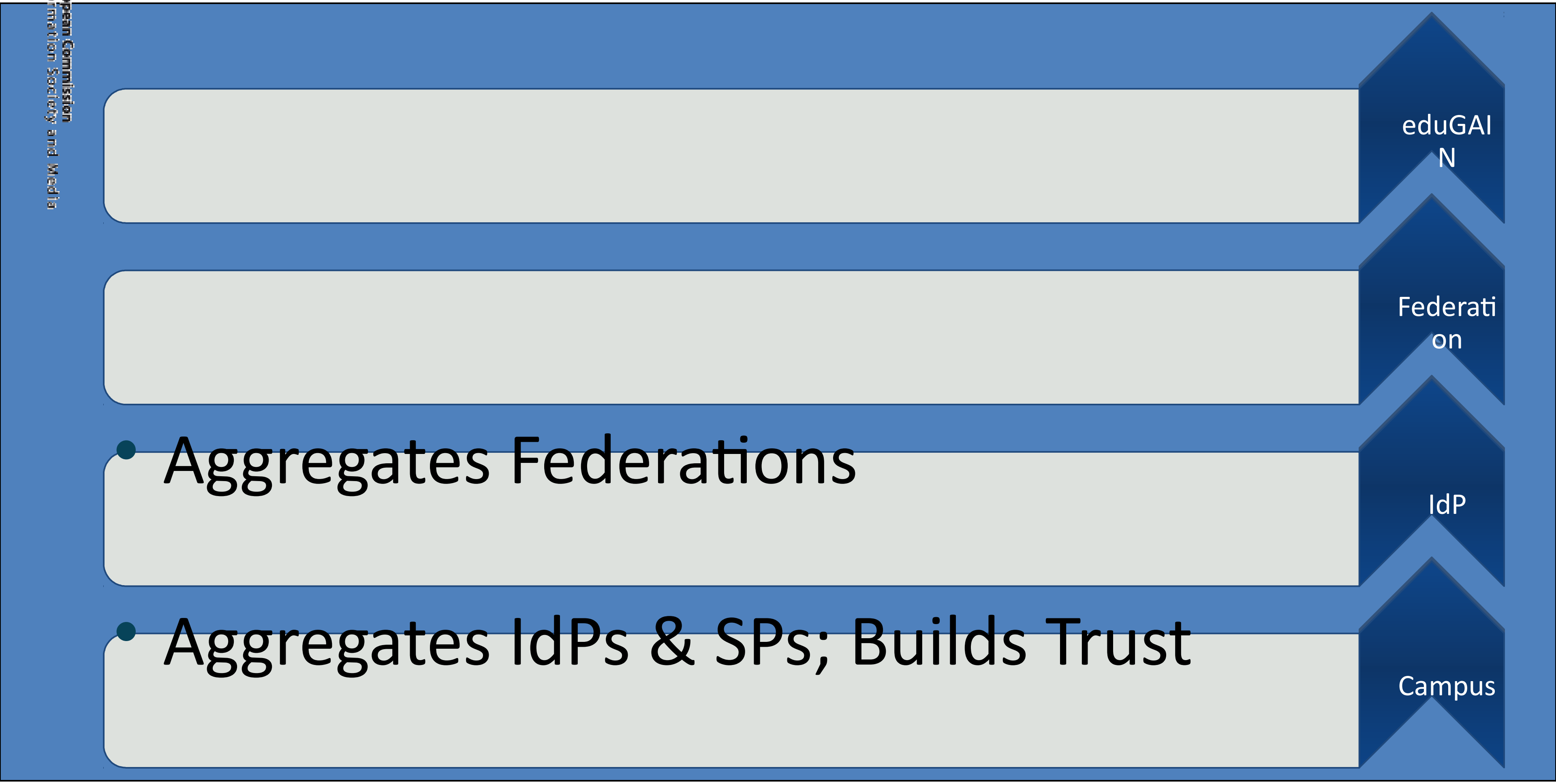
eduroam

Servicio mundial de movilidad segura desarrollado para la comunidad académica y de investigación. Más Información: eduroam.innova-red.net

*G*lobal *A*uthentication *IN*frastructure

eduGAIN

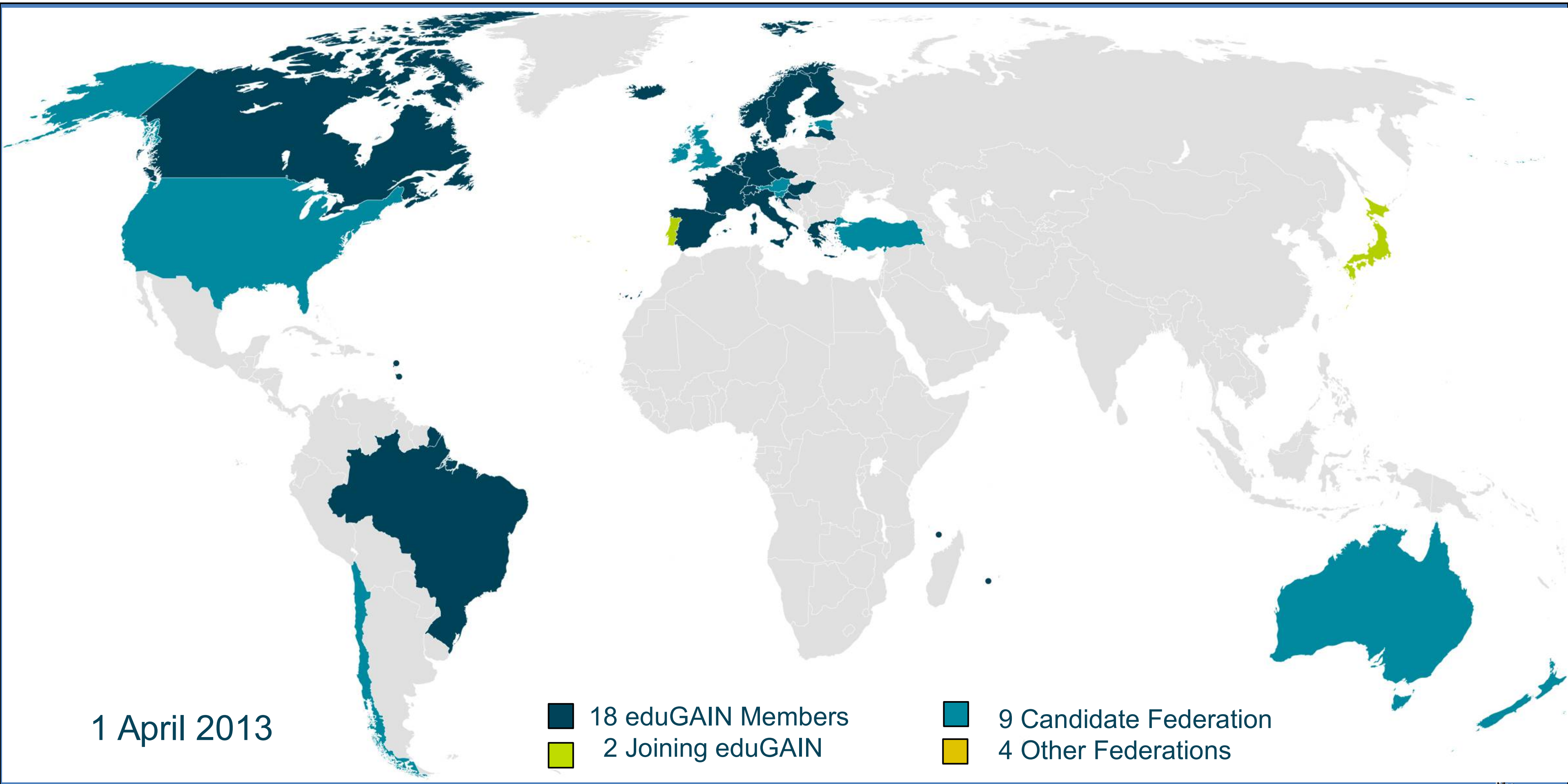
Federation Development



- Aggregates Federations
- Aggregates IdPs & SPs; Builds Trust
- Expose Campus IdM via SAML/RADIUS
- Username/Password Store for AuthN

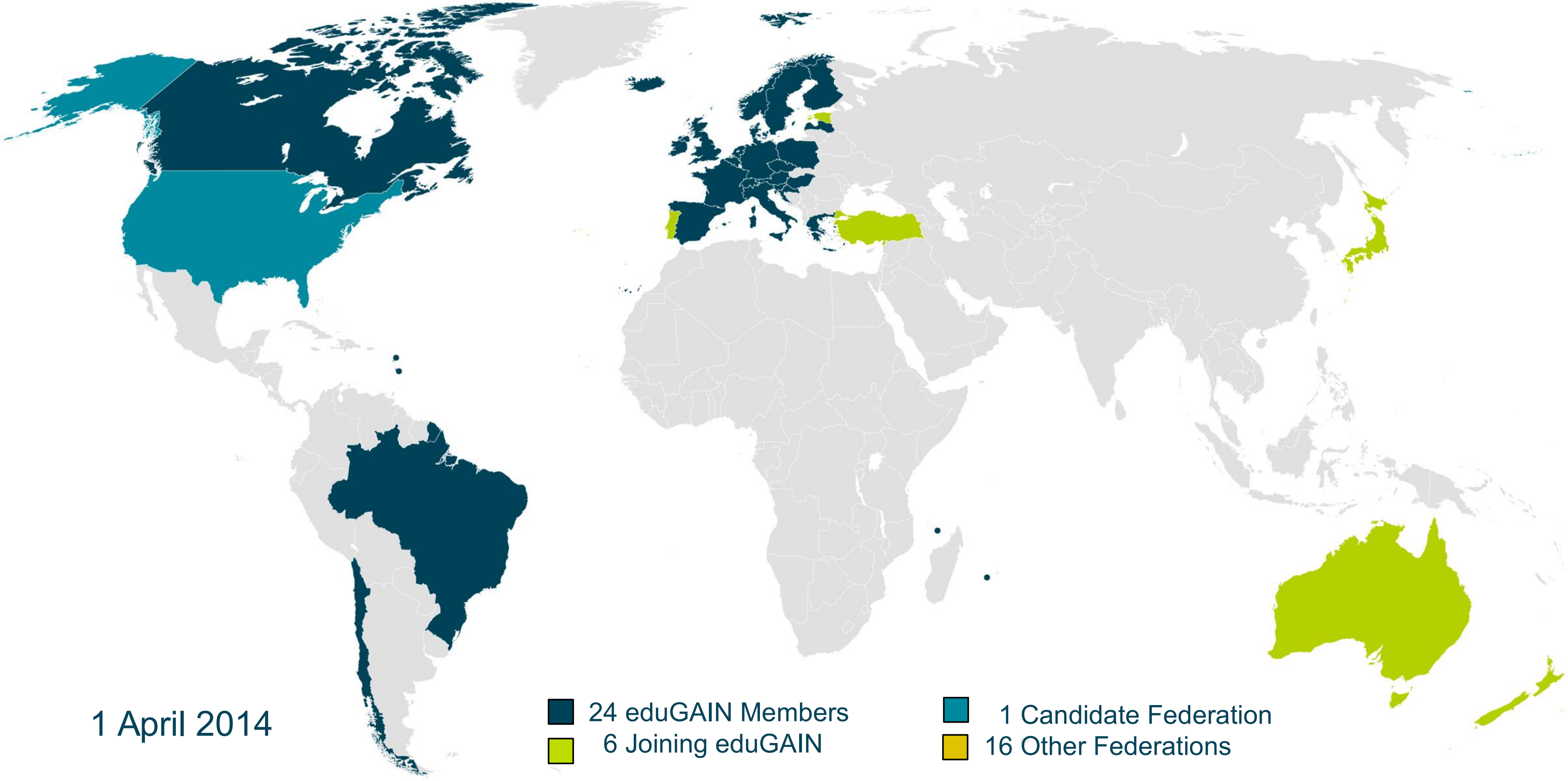
eduGAIN & Federations

Europe Latin America Collaborative e-Infrastructure for Research Activities



eduGAIN & Federations

elcira
Europe Latin America
Collaborative e-Infrastructure
for Research Activities

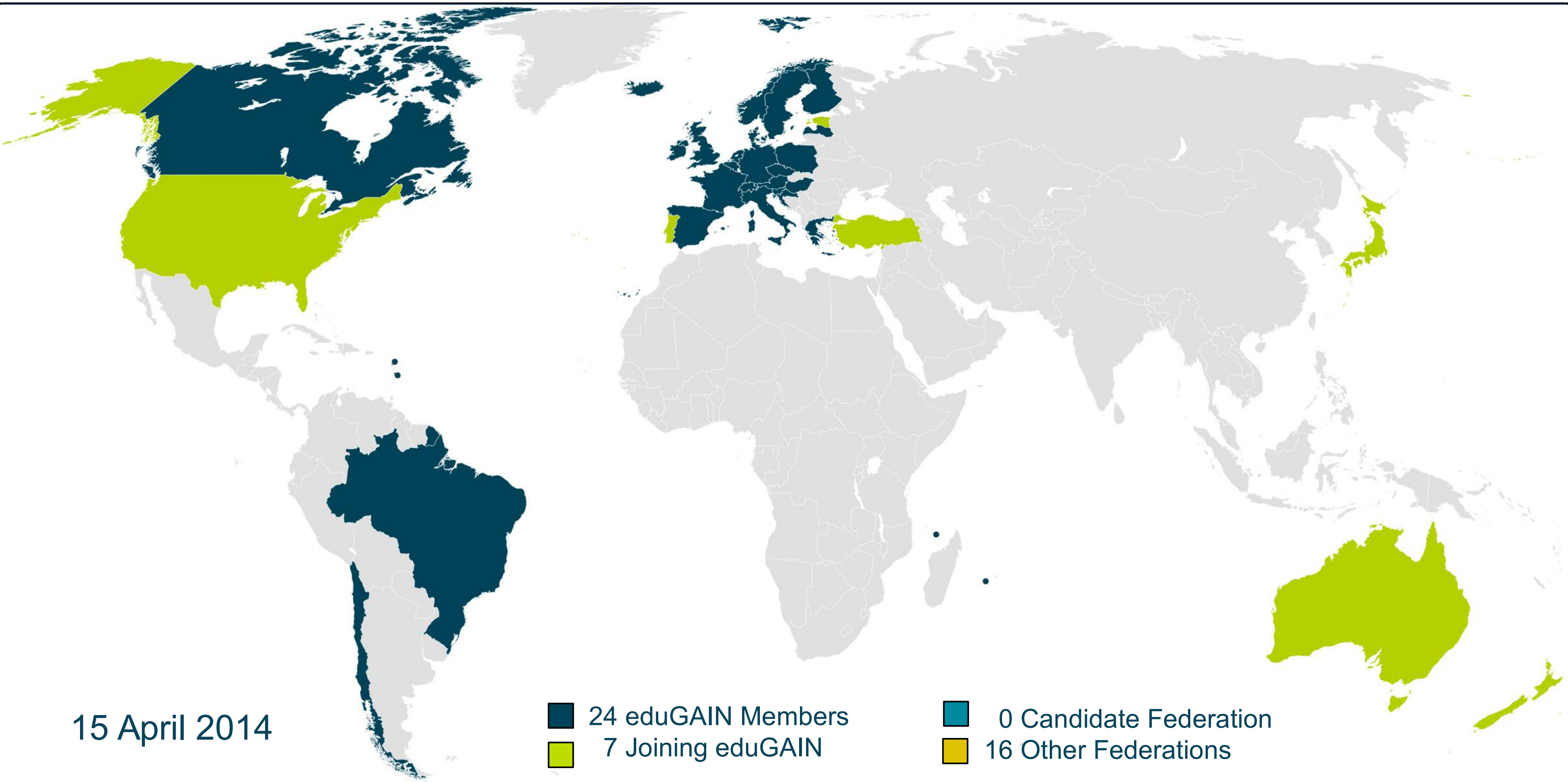


1 April 2014

e-infrastructure

eduGAIN & Federations

elcira
Europe Latin America
Collaborative e-Infrastructure
for Research Activities

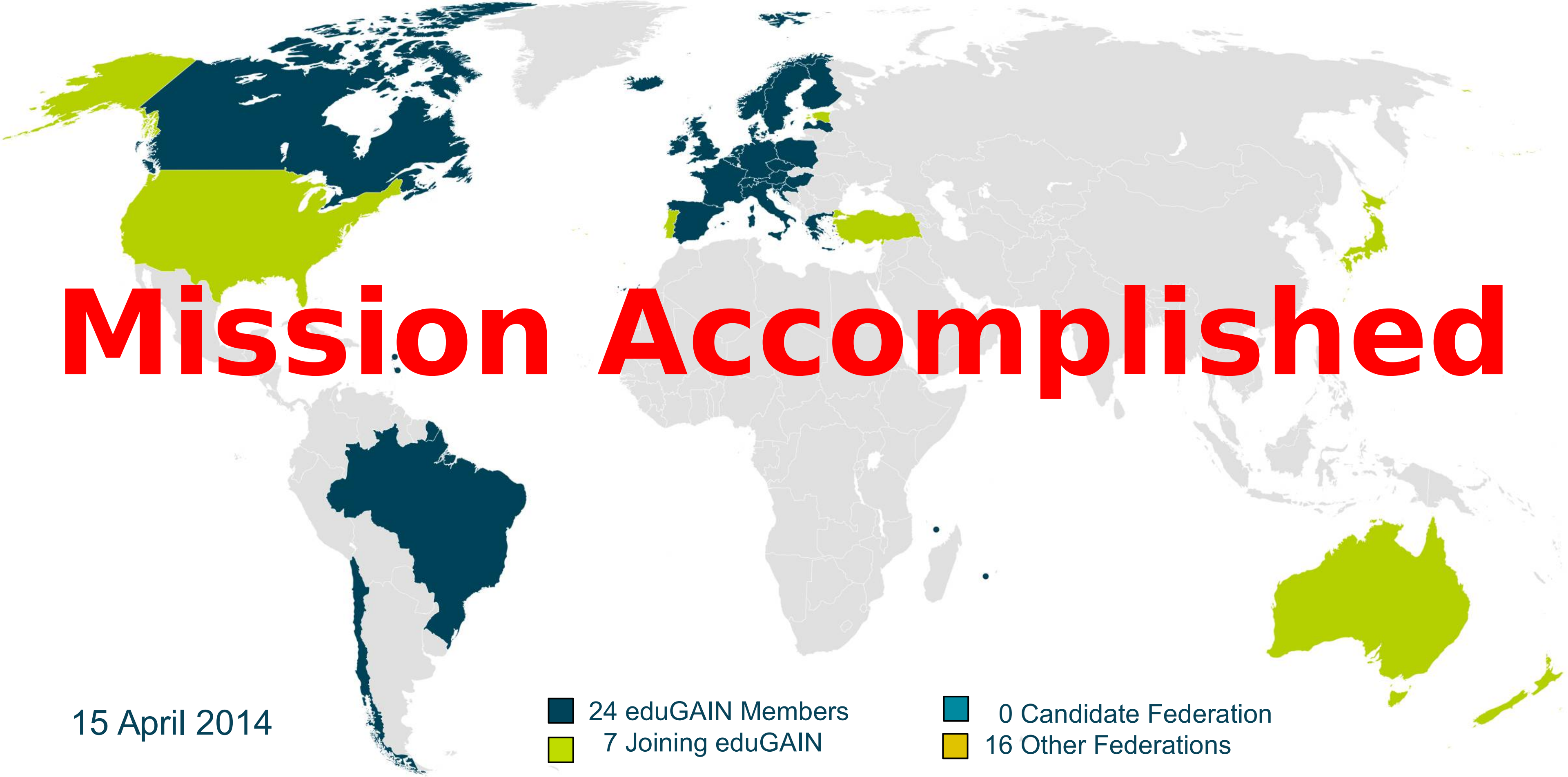


15 April 2014

🟦 24 eduGAIN Members
🟩 7 Joining eduGAIN
🟦 0 Candidate Federation
🟨 16 Other Federations

e-infrastructure

eduGAIN & Federations



Mission Accomplished

15 April 2014

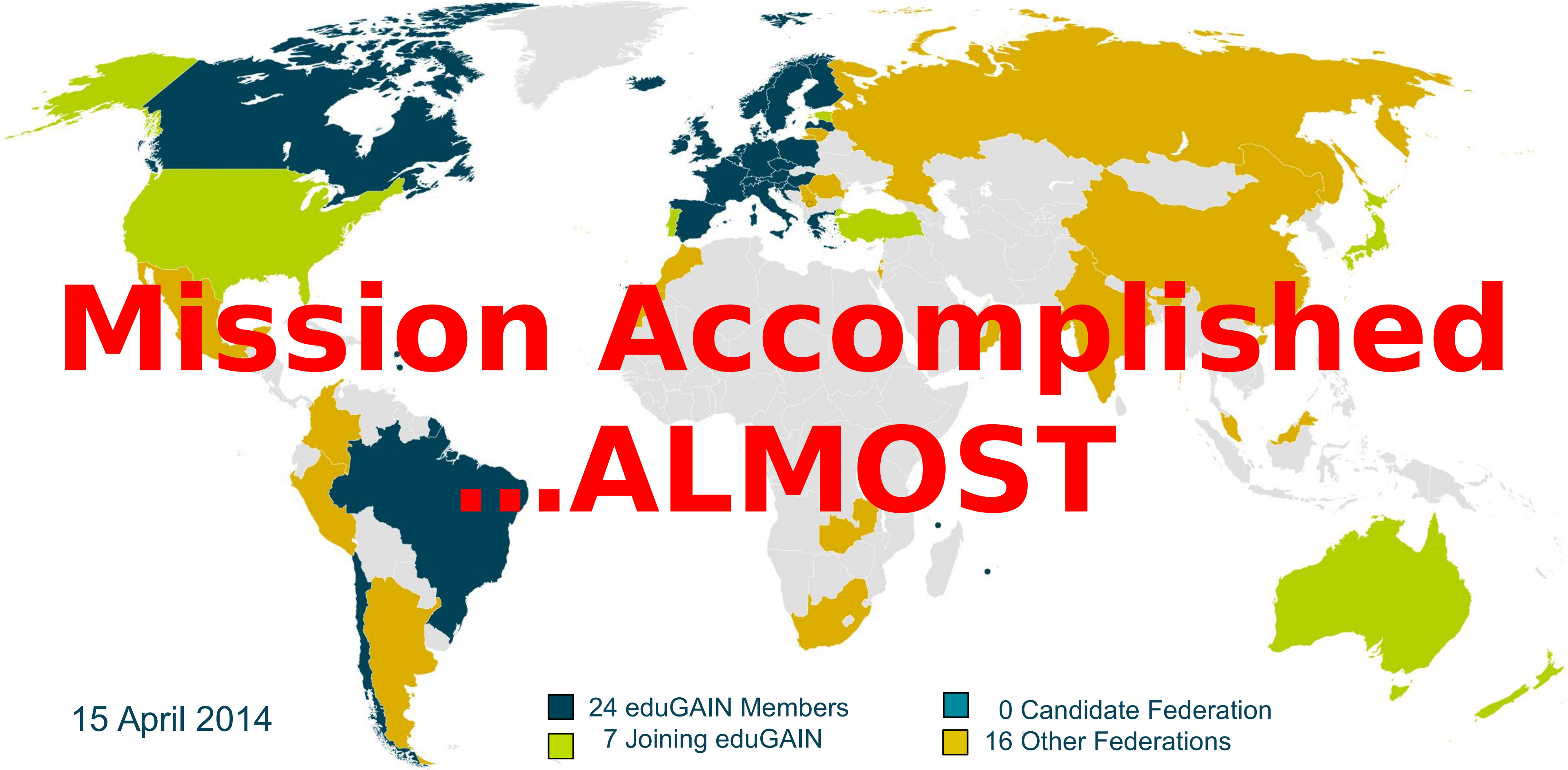
■ 24 eduGAIN Members

■ 7 Joining eduGAIN

■ 0 Candidate Federation

■ 16 Other Federations

eduGAIN & Federations



Mission Accomplished ...ALMOST

15 April 2014

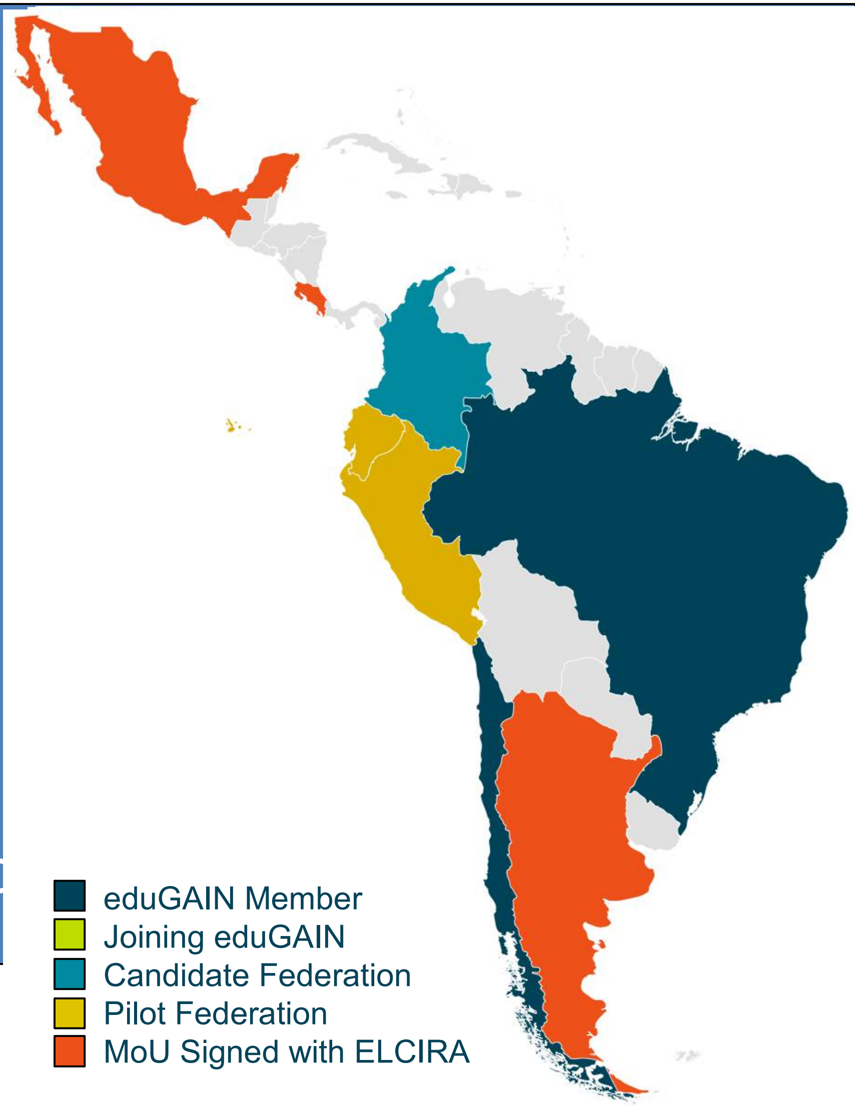
■	24 eduGAIN Members	🟦	0 Candidate Federation
🟩	7 Joining eduGAIN	🟨	16 Other Federations

Identity Federations and Latin America

elcira

Europe Latin America
Collaborative e-Infrastructure
for Research Activities

- eduGAIN Participant
  - Brazil (CAFe)
  - Chile (COFRe)
- eduGAIN Candidate
  - Colombia (COLFIRE)
- Pilot Federation
  - Ecuador, Peru
- Emerging Federations
  - Argentina, Costa Rica, Mexic



e-infrastructure

* MATE (Argentina)

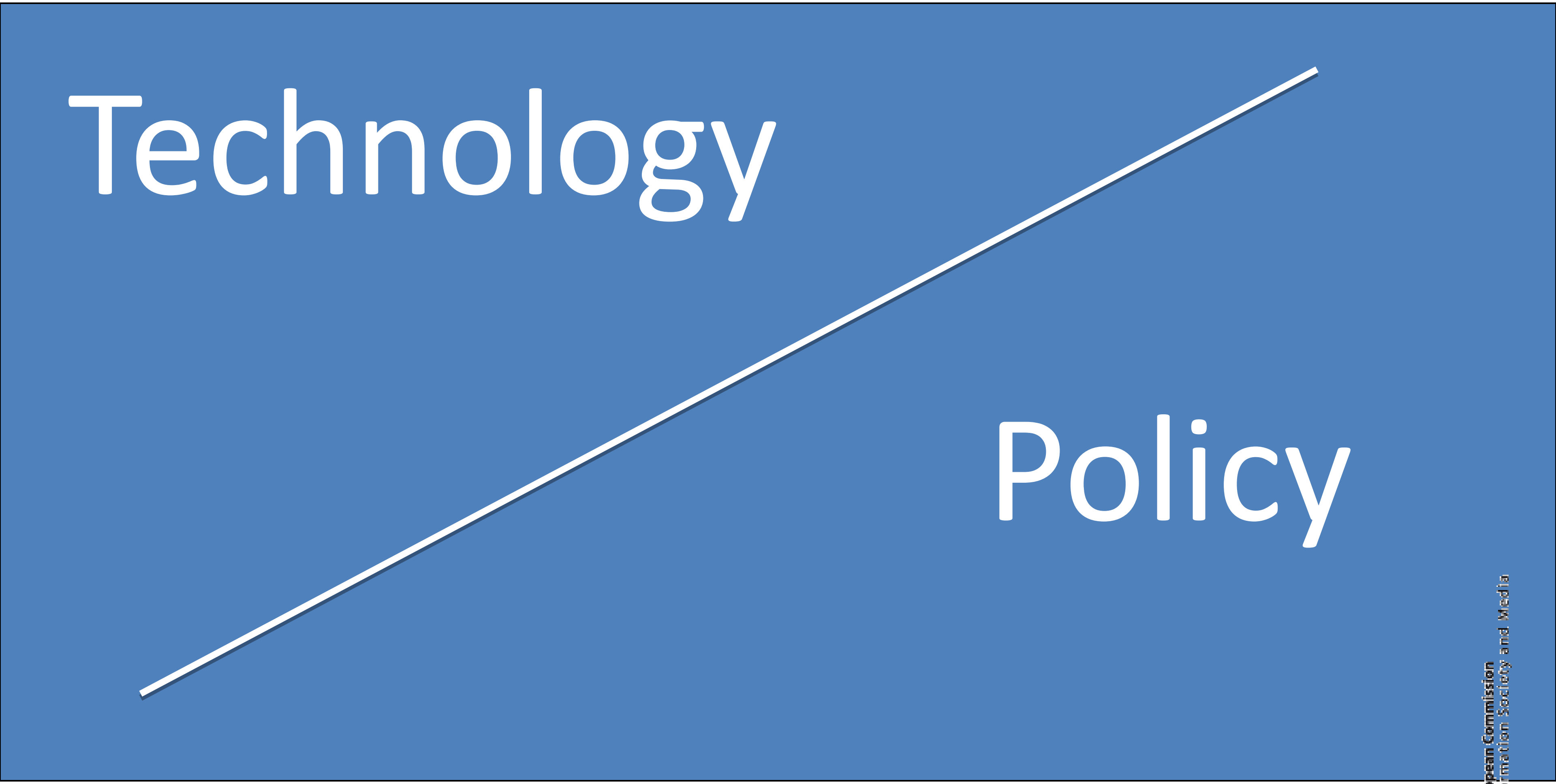
- MATE run by INNOVA|RED

  Marco para el Acceso a la Tecnología y la Educación (MATE)
  Model for Access to Technology and Education (MATE)

- Started operation in late 2013
- Joined eduGAIN in early-2014 ;-)

- *This is NOT their logo (nor their name)!!

Federation Development



Technology

Policy

Federation Development

Technology
== Pilot

Policy
==Production

Federation Development

Technology
=>Campus

Policy
=>Innova|RED

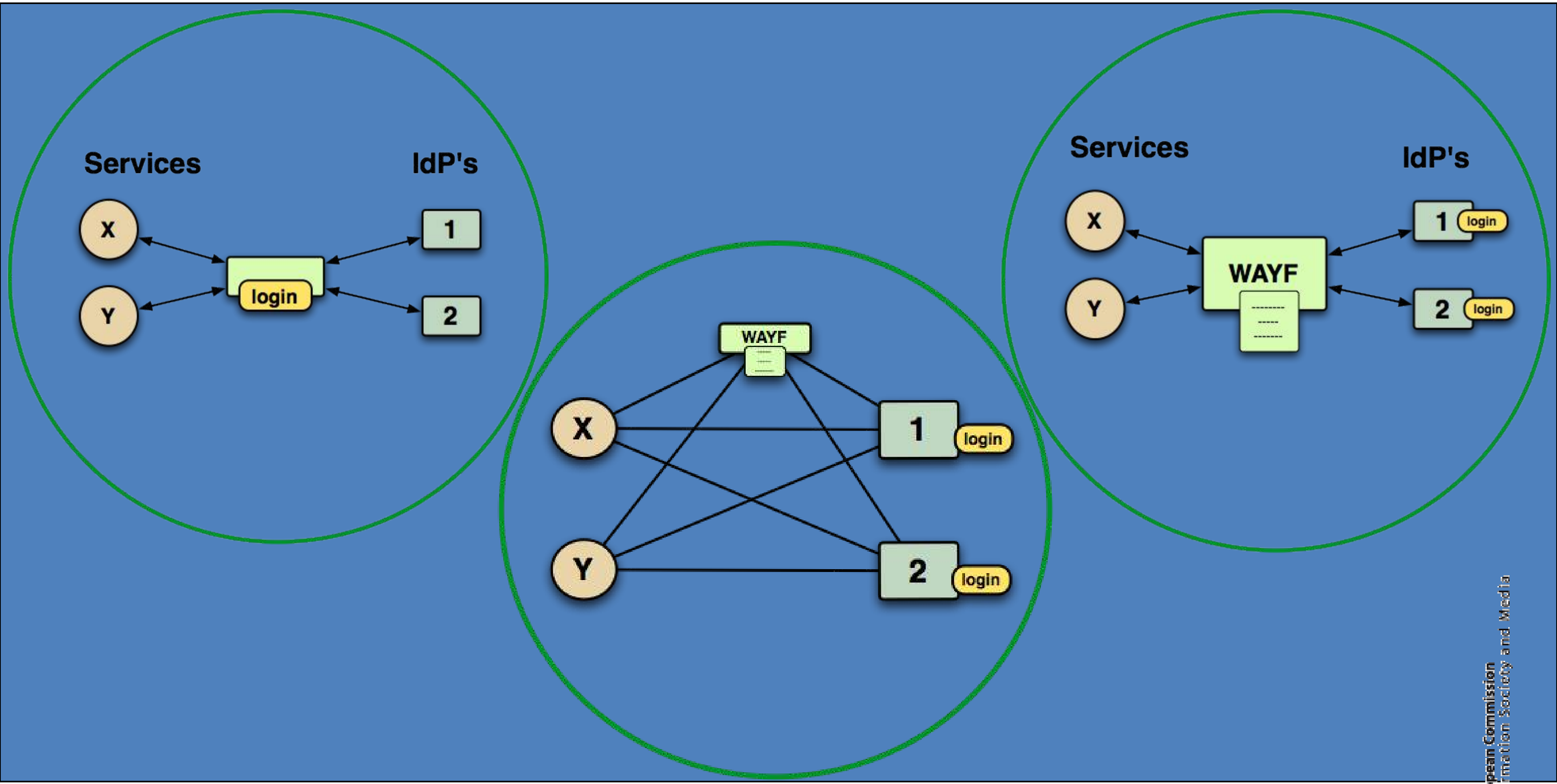
Technology == Pilot

- Federation Core Services
  - “Routing”
  - Discovery
- Federation “Entities” (IdPs/SPs)
  - Shibboleth
  - simpleSAMLphp
  - PySAML
  - ADFS

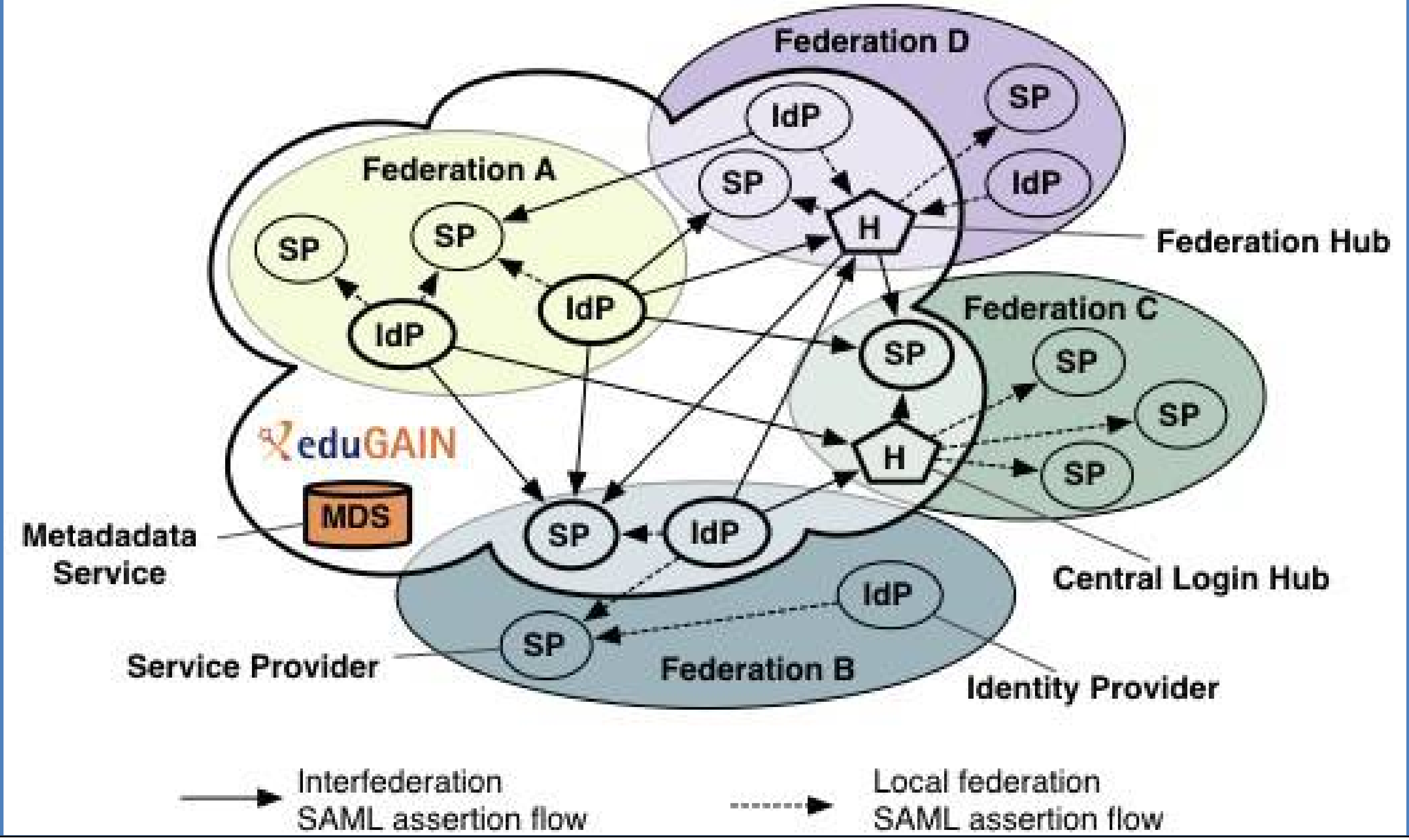
Technology == Pilot

- Innova|RED as Federation Operator
  - “Routing”
  - Discovery
- Campus, Content Providers, Research Infrastructures
  - Shibboleth
  - simpleSAMLphp
  - PySAML
  - ADFS

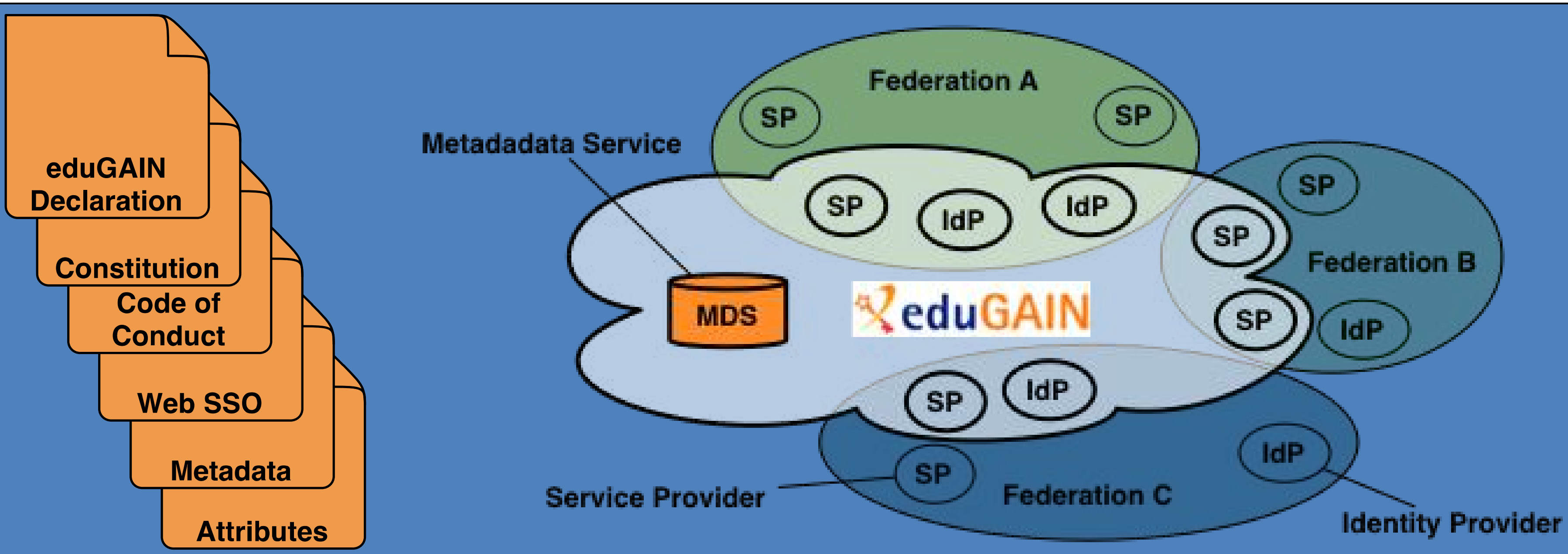
Federation Architectures



More "Realistic" Architecture



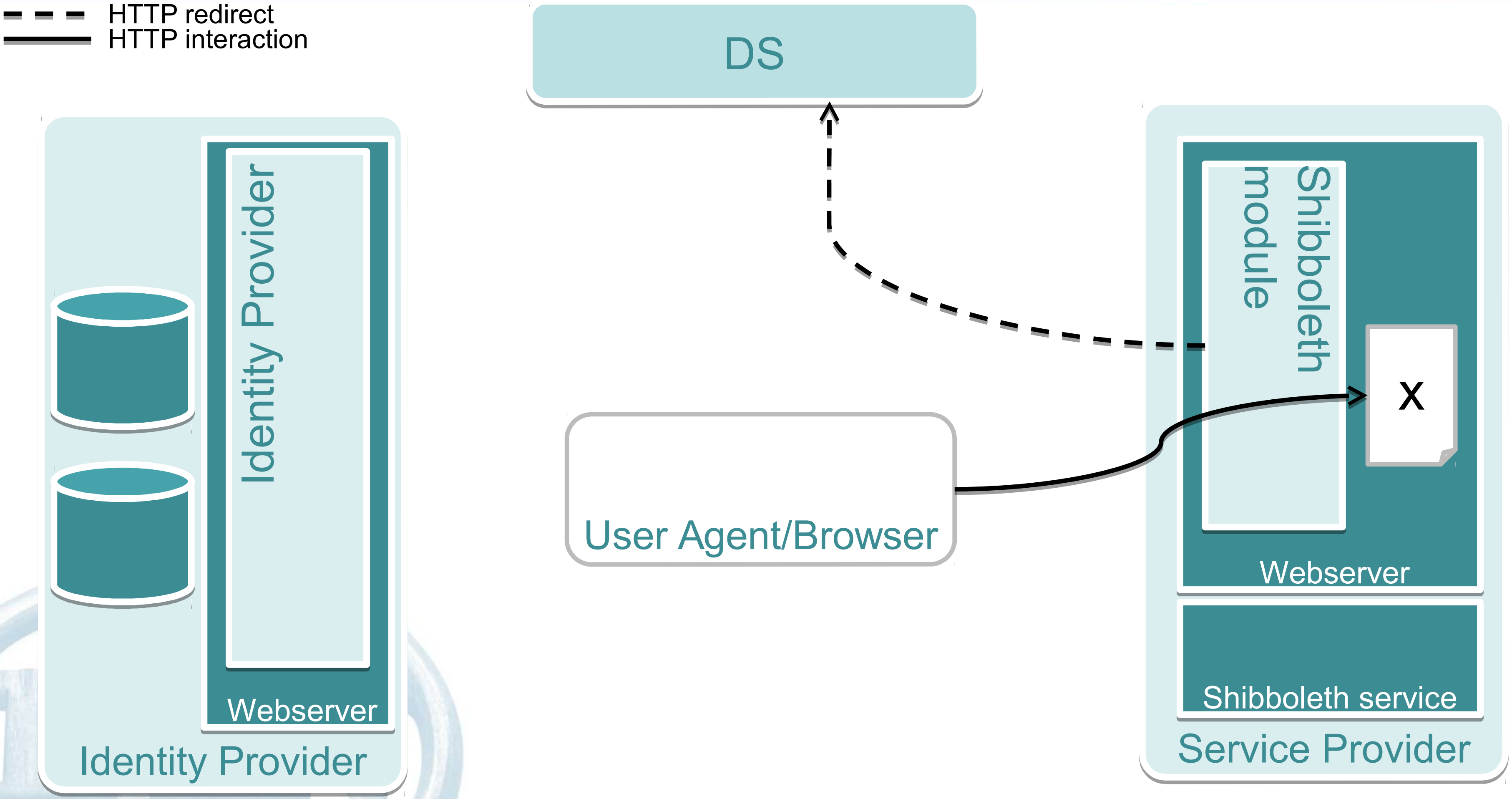
What is eduGAIN?



- MDS fetches, aggregates and republishes metadata

Web Single Sign On

Architecture SAML/Shibboleth v2.x

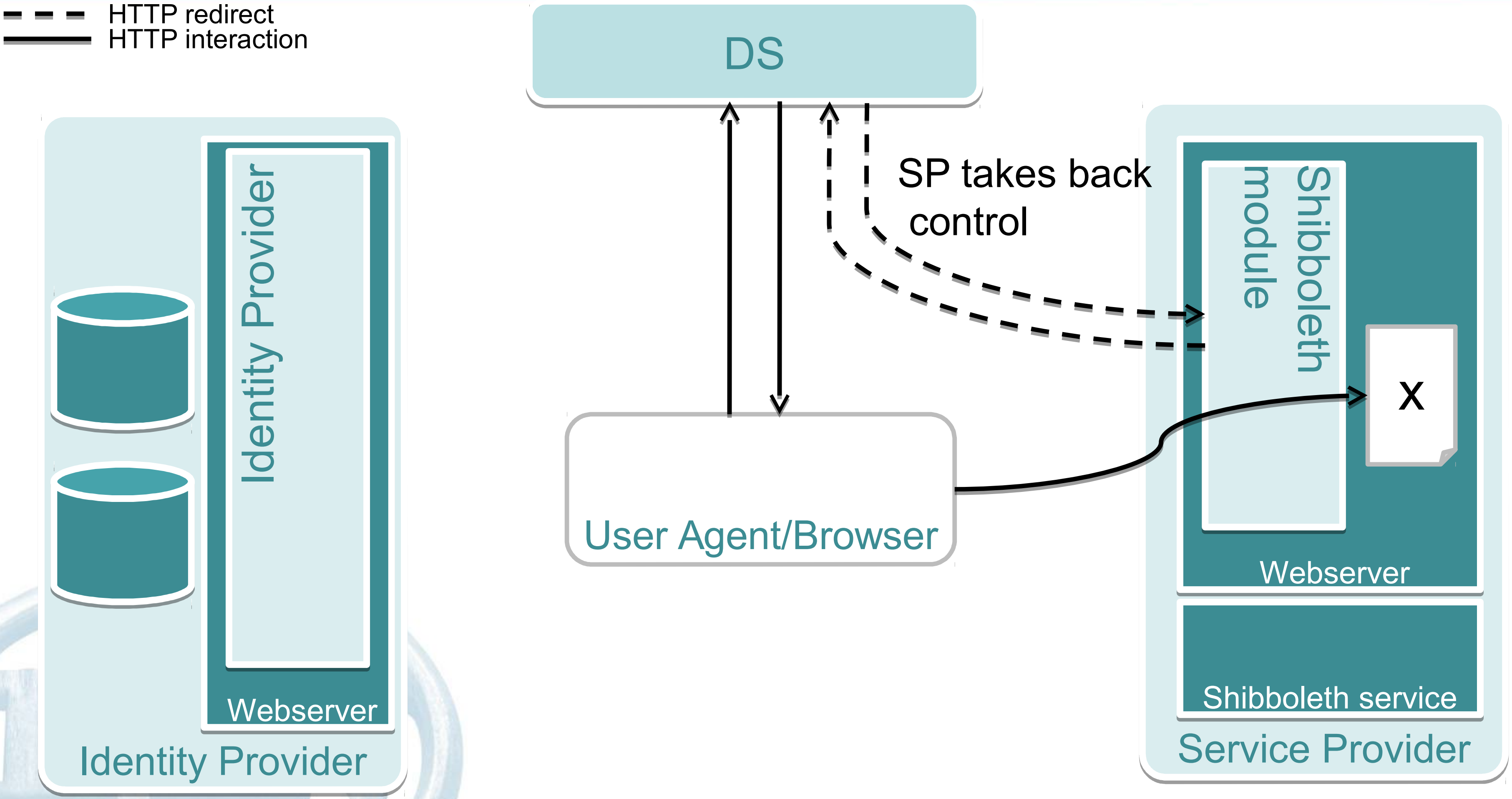


SAML2.0 profile: Web browser SSO + HTTP POST binding

Initial request from UA to document X

No active Shibboleth session, UA redirected to DS

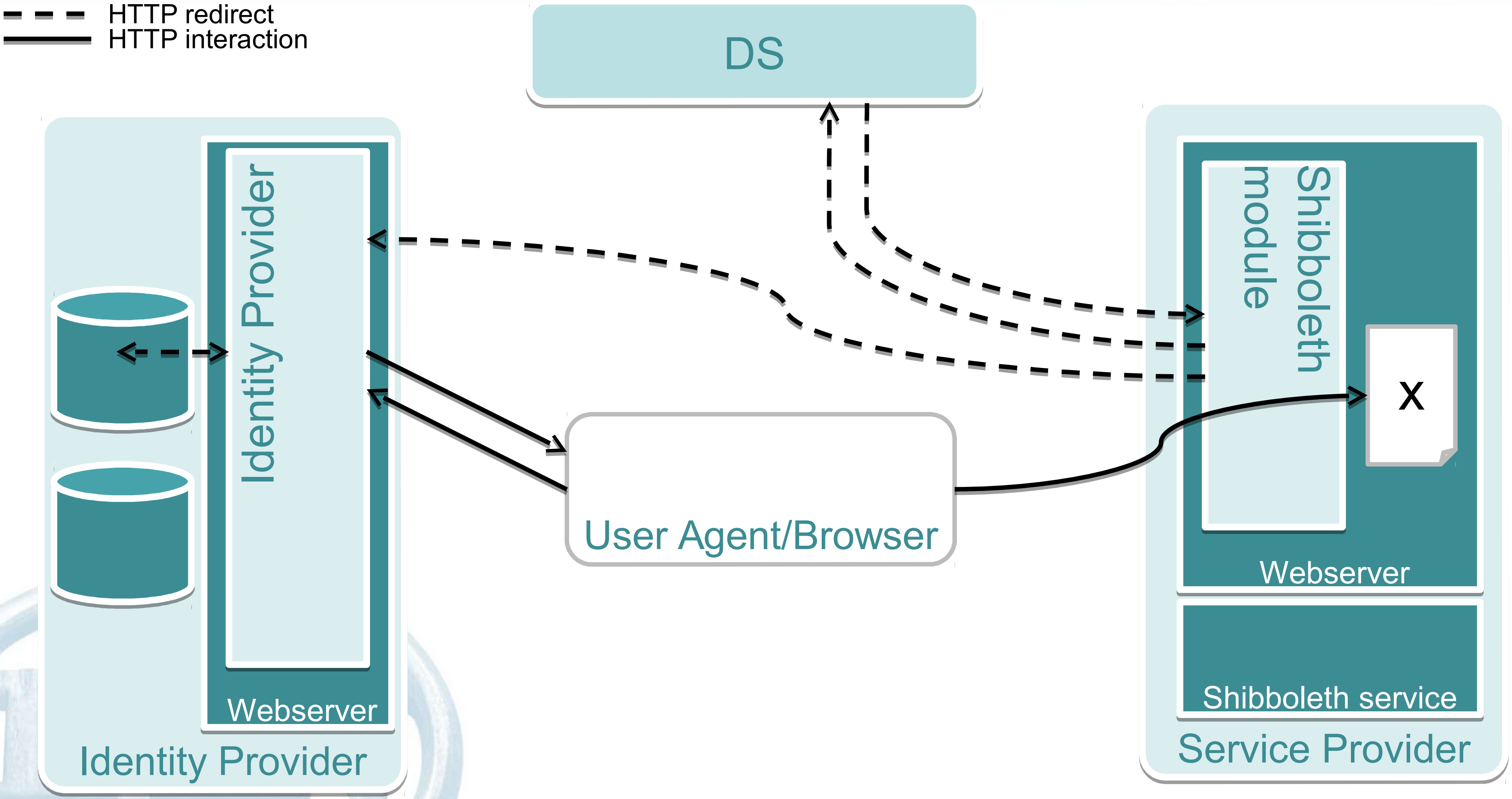
Architecture SAML/Shibboleth v2.x



DS asks UA to choose an IdP (if not already set in cookie)

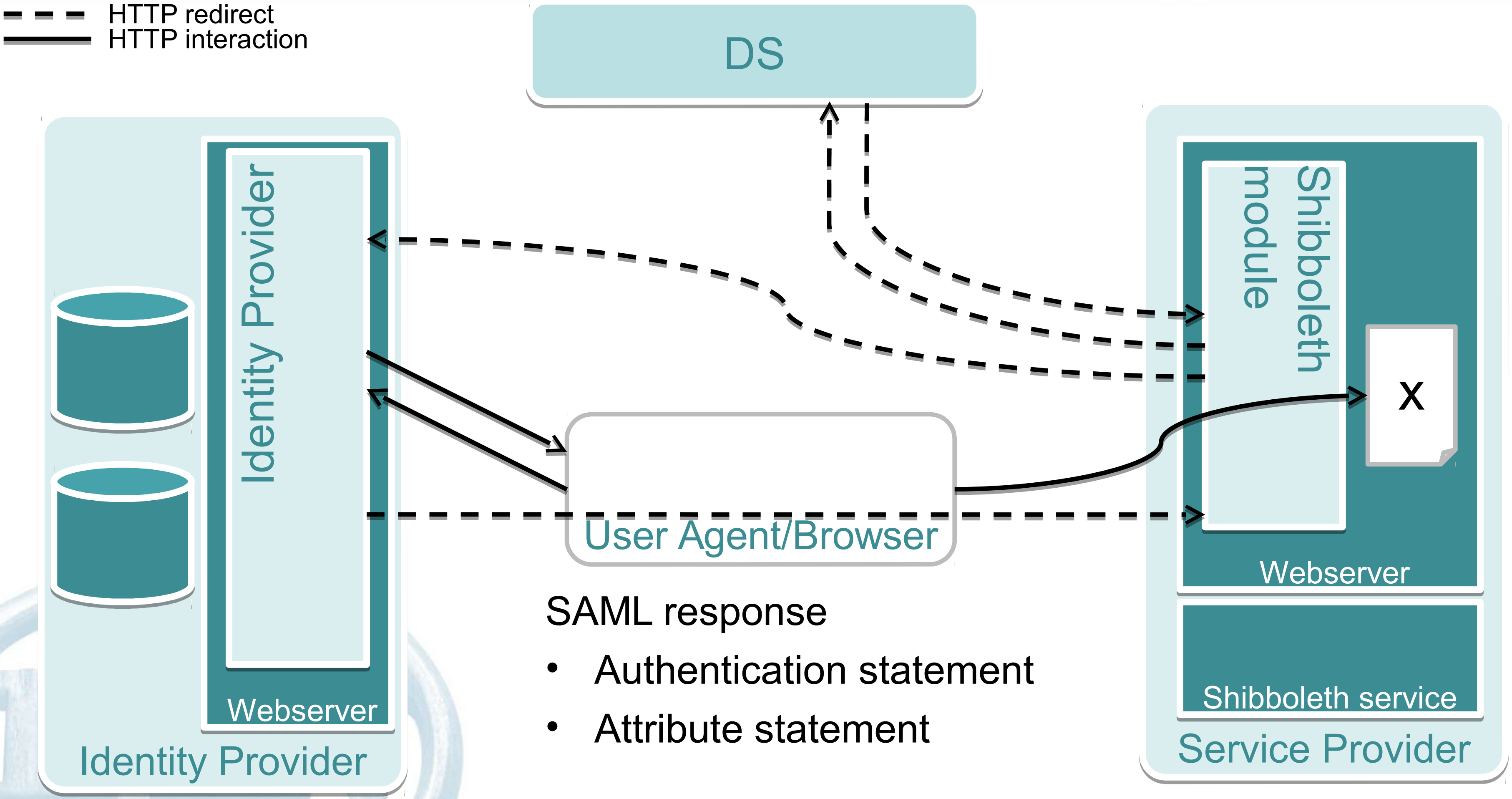
Redirect UA back to SP with selected IdP as parameter.

Architecture SAML/Shibboleth v2.x



SP sends SAML Authentication request to the IdP.
IdP prompts the UA for credentials, if necessary.
IdP uses backend to verify credentials (LDAP, ADDS, SQL, etc)

Architecture SAML/Shibboleth v2.x

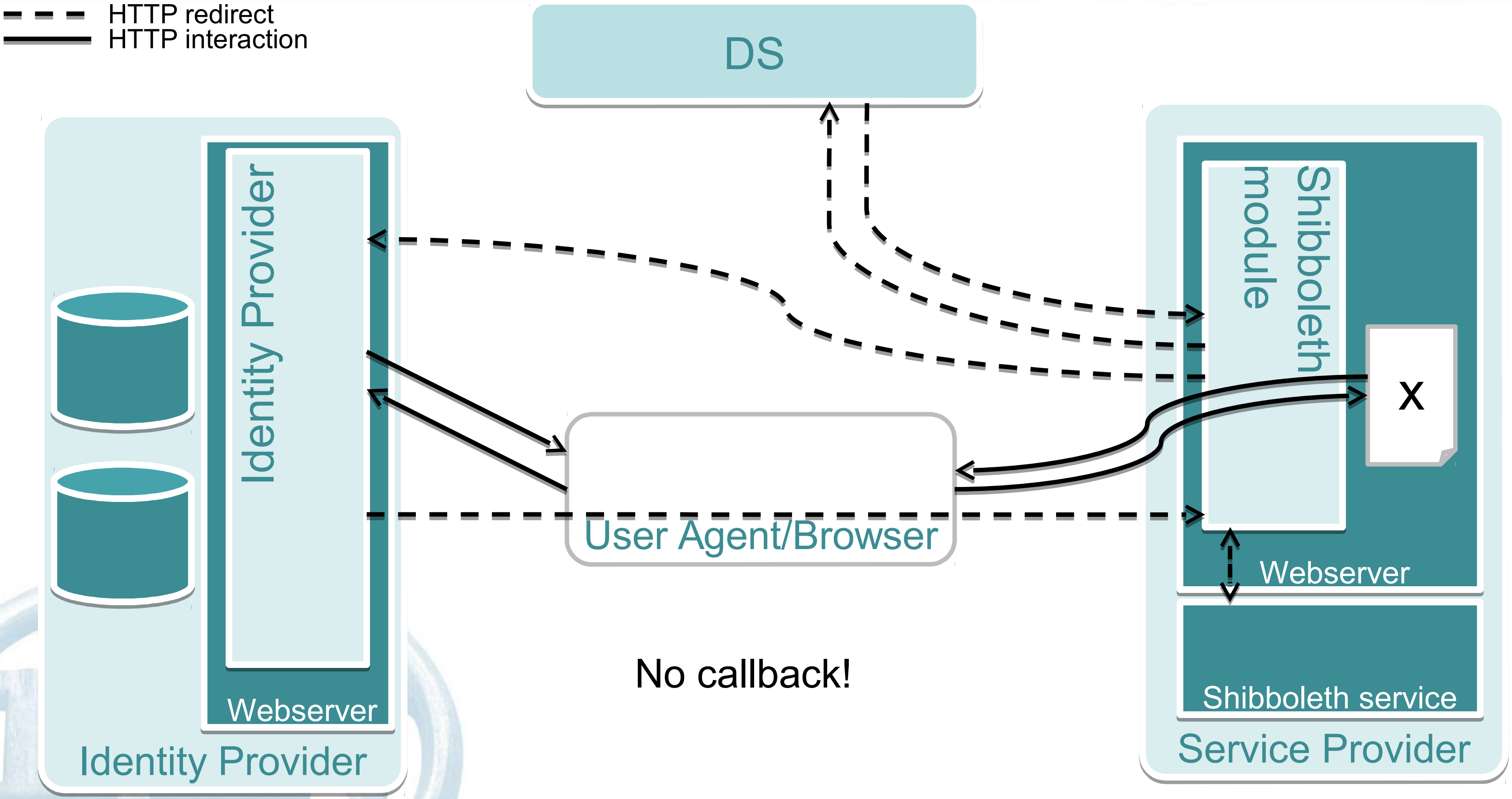


SAML response

- Authentication statement
- Attribute statement

The IdP resolves and filters the principal's attribute information and constructs a SAML assertion. This assertion can optionally be signed and/or encrypted. Next, the IdP POSTs a response to the SP

Architecture SAML/Shibboleth v2.x

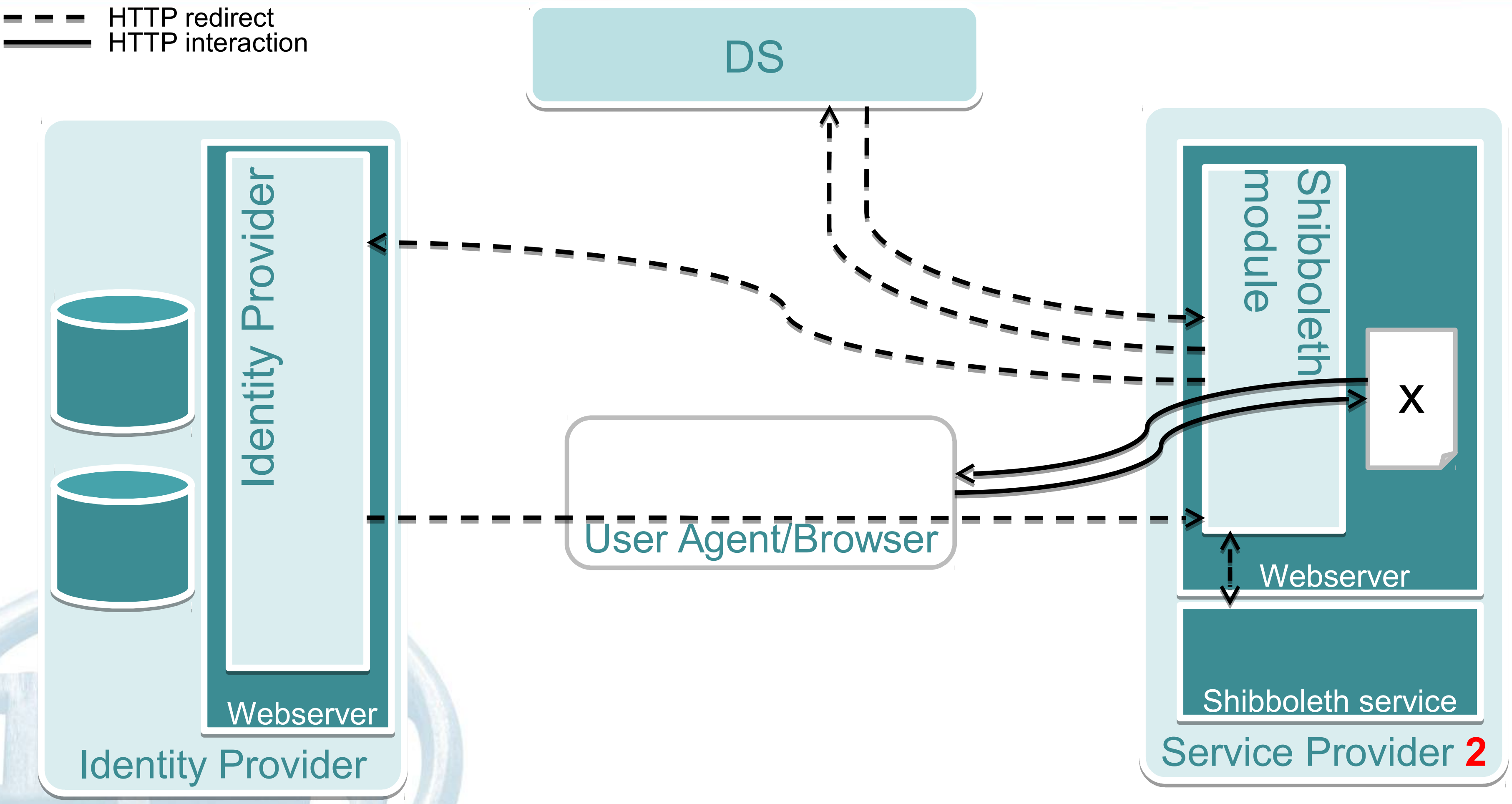


No callback!

The Shibboleth service decrypts, verifies and filters the response and gives it to the Shibboleth module (via RPC or TCP).

The Shibboleth module or Webserver will authorise the

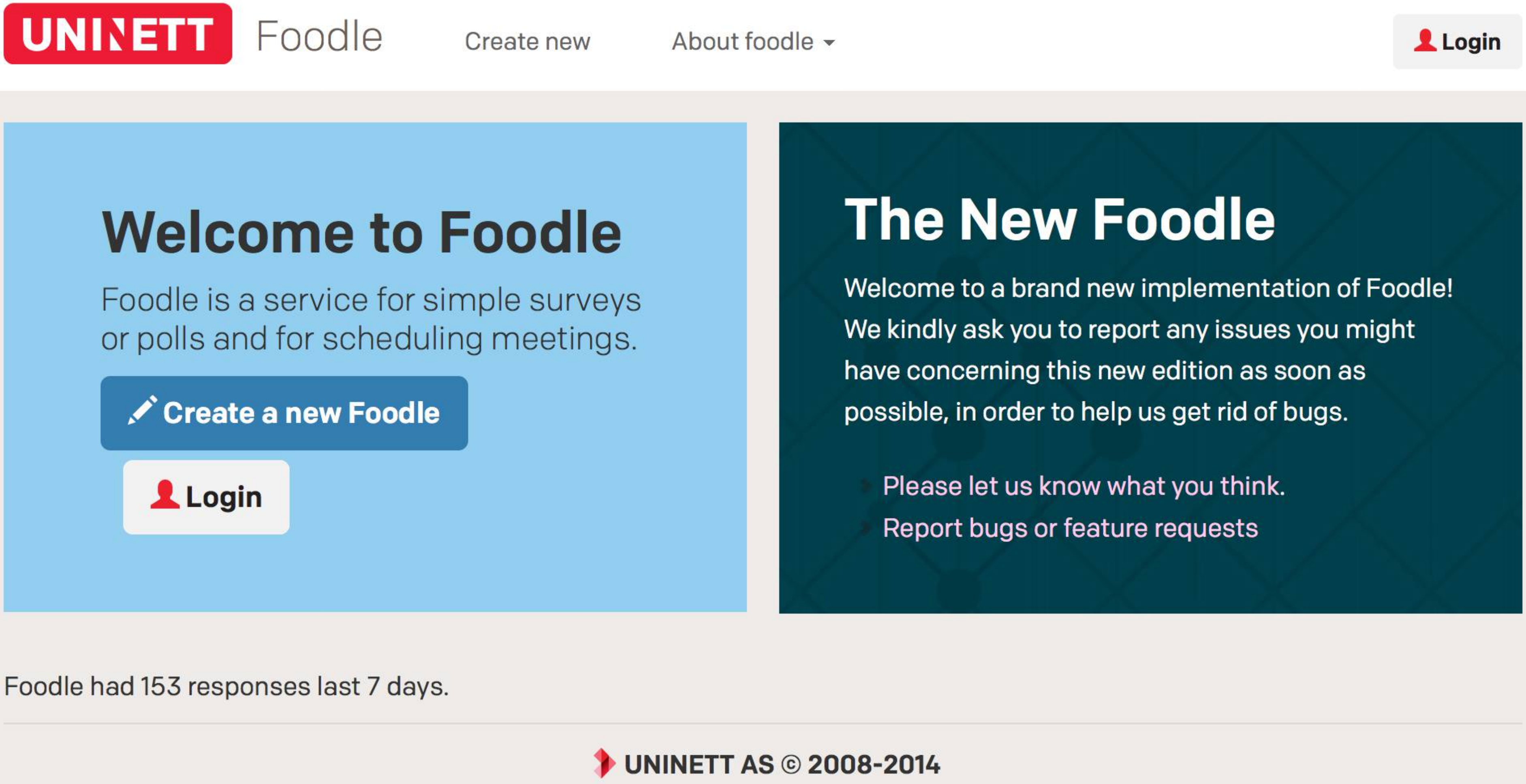
Architecture SAML/Shibboleth v2.x



Again, the active sessions with every component will provide the single sign-on experience.

Try it for yourself…

- Visit http://foodl.org



Welcome to Foodle

Foodle is a service for simple surveys or polls and for scheduling meetings.

The New Foodle

Welcome to a brand new implementation of Foodle! We kindly ask you to report any issues you might have concerning this new edition as soon as possible, in order to help us get rid of bugs.

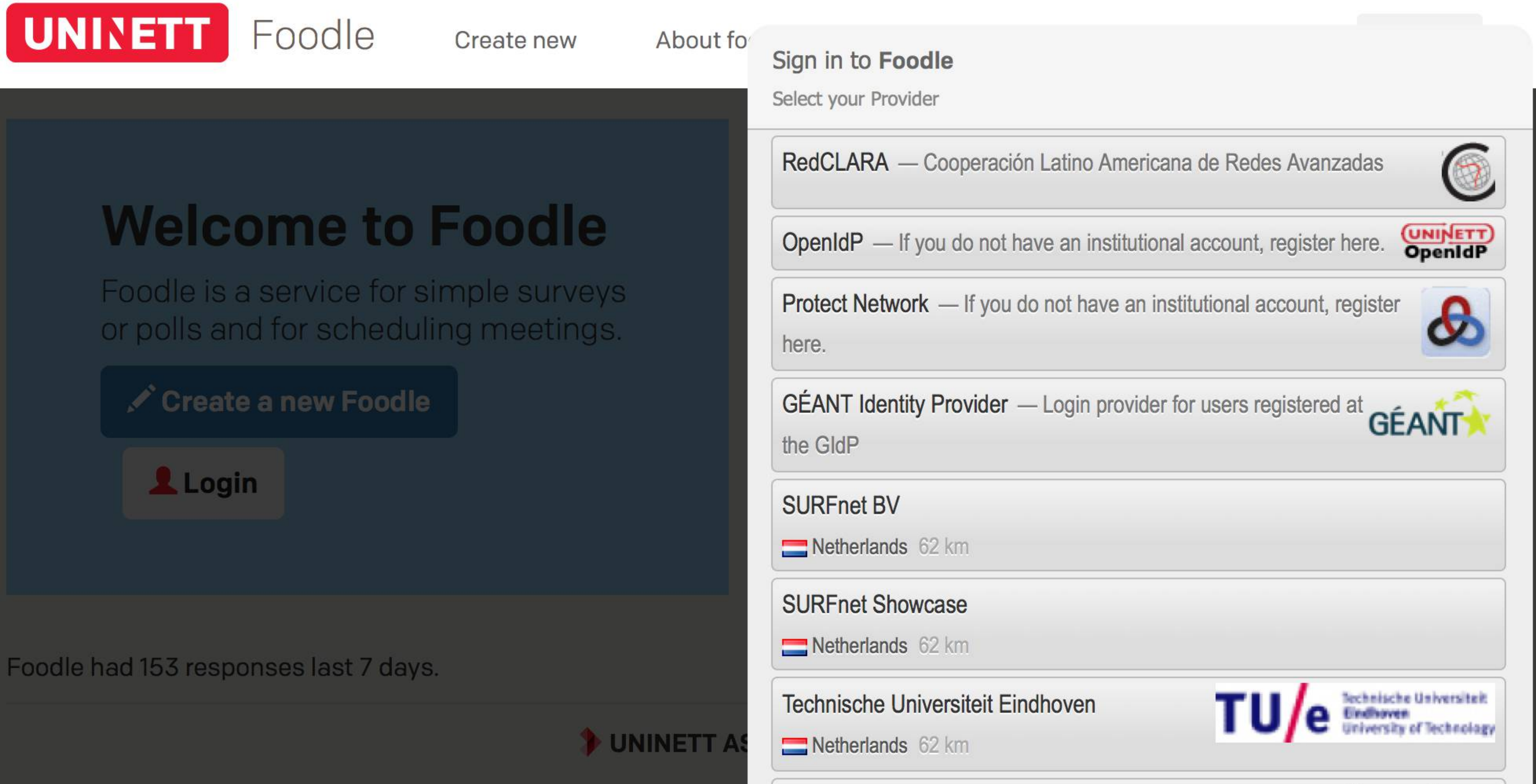
- Please let us know what you think.
- Report bugs or feature requests

Foodle had 153 responses last 7 days.

UNINETT AS © 2008-2014

Try it for yourself…

- Visit http://foodl.org



UNINETT Foodle

Create new

About fo

Welcome to Foodle

Foodle is a service for simple surveys or polls and for scheduling meetings.

Foodle had 153 responses last 7 days.

UNINETT AS

Sign in to **Foodle**

Select your Provider

RedCLARA — Cooperación Latino Americana de Redes Avanzadas

OpenIdP — If you do not have an institutional account, register here.

Protect Network — If you do not have an institutional account, register here.

GÉANT Identity Provider — Login provider for users registered at the GIdP

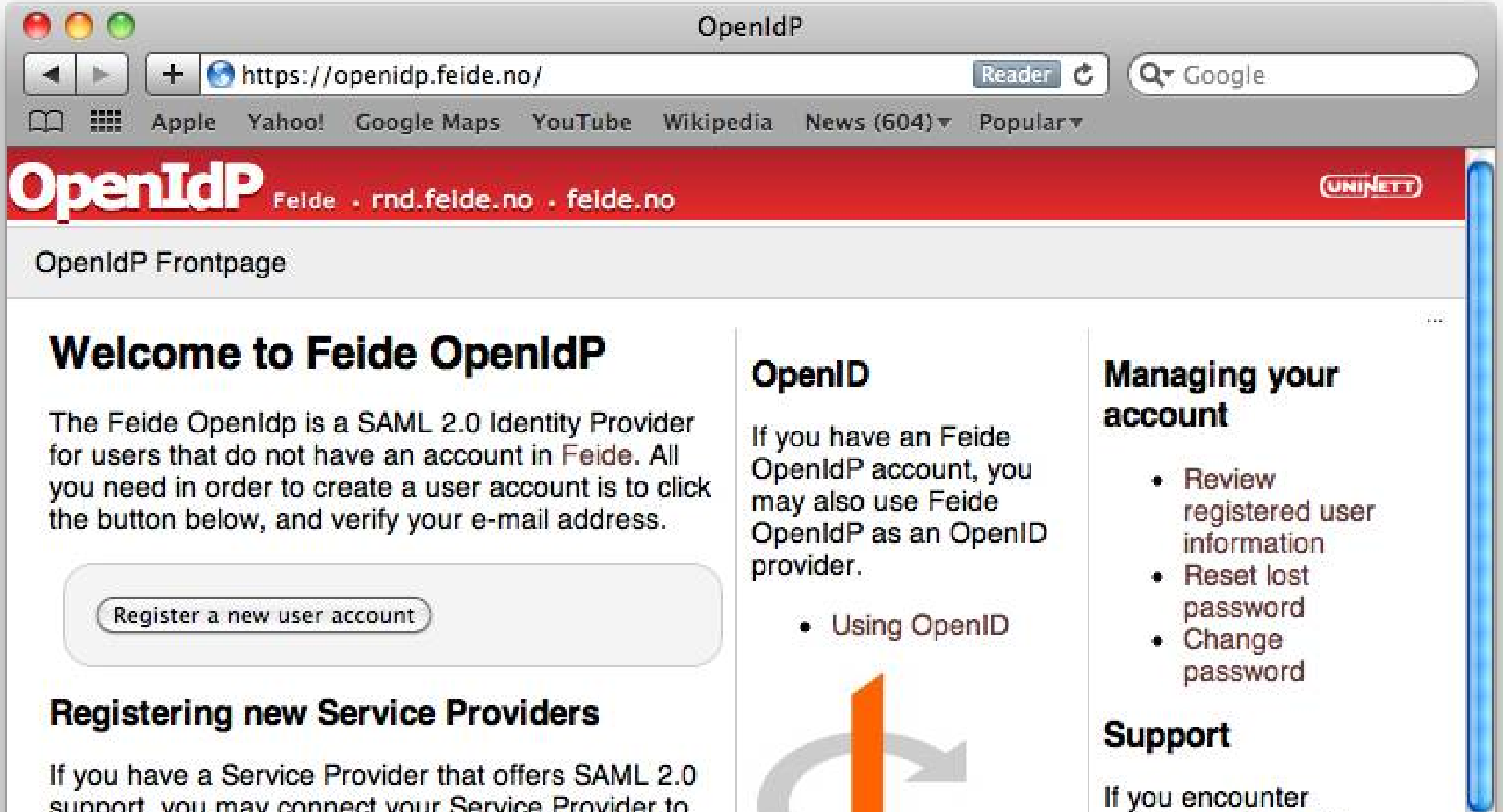
SURFnet BV
Netherlands 62 km

SURFnet Showcase
Netherlands 62 km

Technische Universiteit Eindhoven
Netherlands 62 km

Homeless? Use OpenIdP…

- Visit https://openidp.feide.no/



OpenIdP Frontpage

Welcome to Feide OpenIdP

The Feide OpenIdp is a SAML 2.0 Identity Provider for users that do not have an account in Feide. All you need in order to create a user account is to click the button below, and verify your e-mail address.

Register a new user account

Registering new Service Providers

If you have a Service Provider that offers SAML 2.0 support, you may connect your Service Provider to

OpenID

If you have an Feide OpenIdP account, you may also use Feide OpenIdP as an OpenID provider.

- Using OpenID

Managing your account

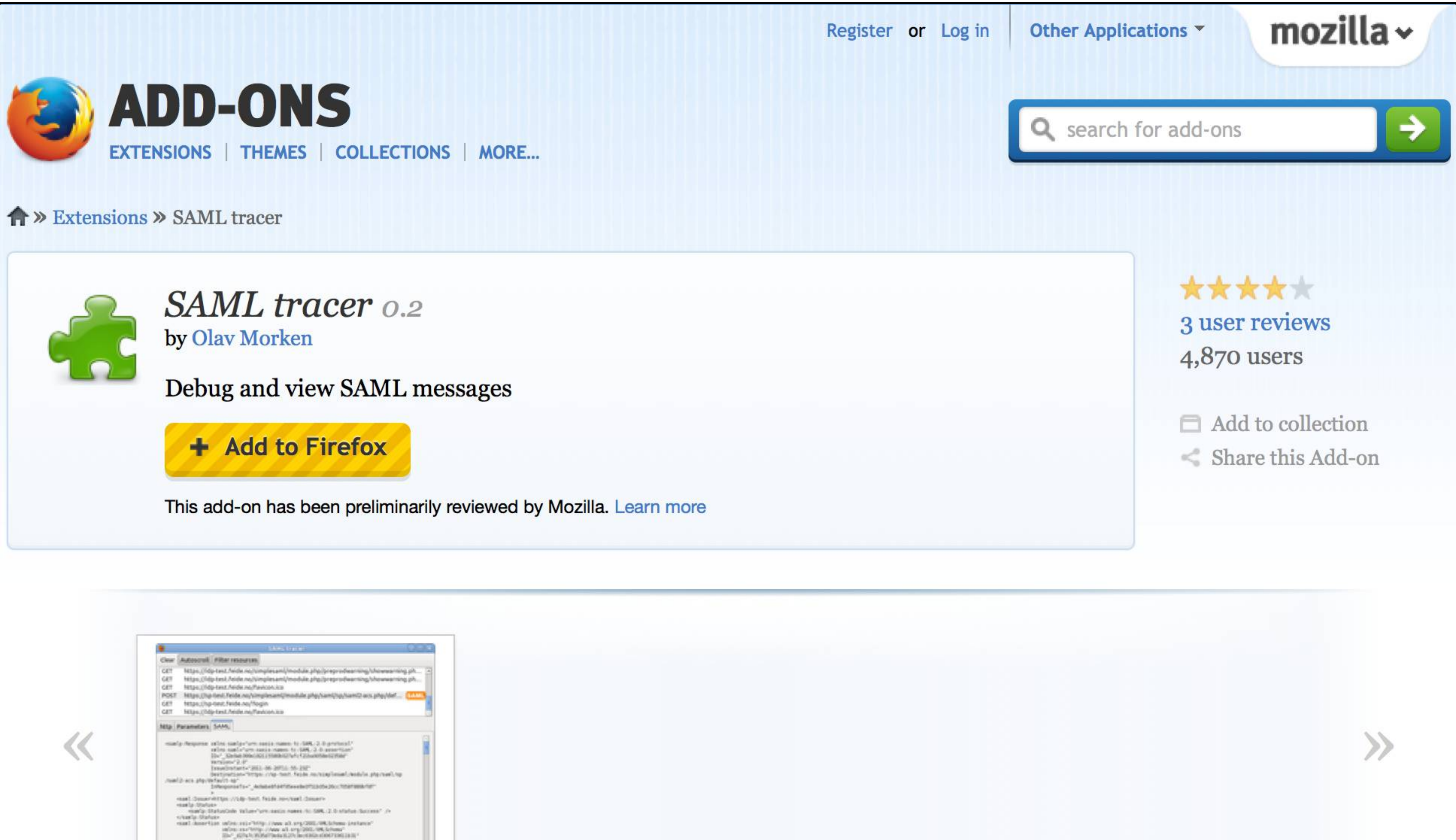
- Review registered user information
- Reset lost password
- Change password

Support

If you encounter

SAML tracer for Firefox

Europe Latin America
Collaborative e-Infrastructure
for Research Activities



Register or Log in | Other Applications | mozilla

ADD-ONS

EXTENSIONS | THEMES | COLLECTIONS | MORE...

search for add-ons

» Extensions » SAML tracer

SAML tracer 0.2

by Olav Morken

Debug and view SAML messages

+ Add to Firefox

This add-on has been preliminarily reviewed by Mozilla. Learn more

★★★★☆

3 user reviews

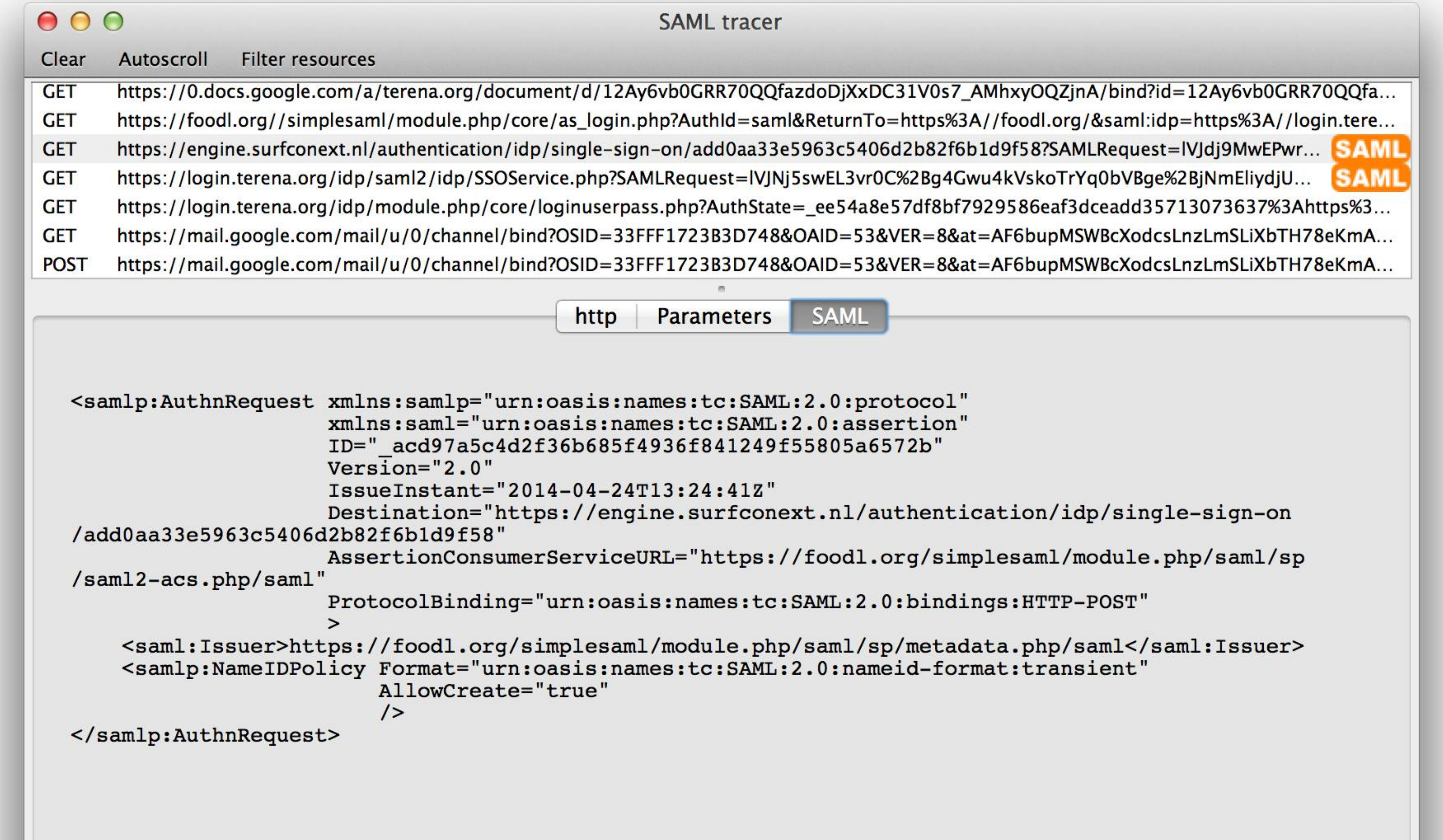
4,870 users

Add to collection

Share this Add-on

« »

SAML tracer for Firefox

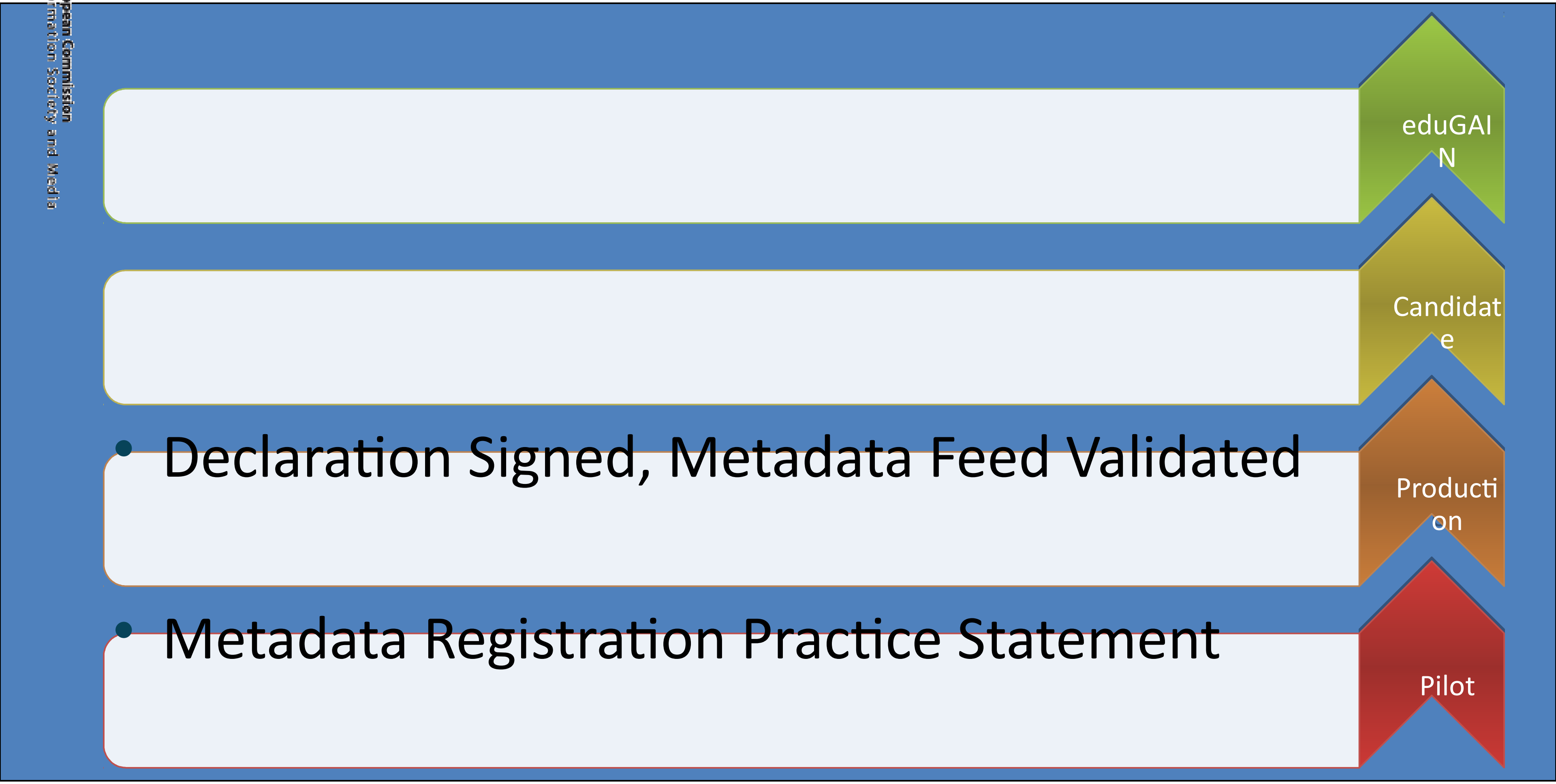


```
GET    https://0.docs.google.com/a/terena.org/document/d/12Ay6vb0GRR70QQfazdoDjXxDC31V0s7_AMhxyOQZjnA/bind?id=12Ay6vb0GRR70QQfa...
GET    https://foodl.org//simplesaml/module.php/core/as_login.php?AuthId=saml&ReturnTo=https%3A//foodl.org/&saml:idp=https%3A//login.tere...
GET    https://engine.surfconext.nl/authentication/idp/single-sign-on/add0aa33e5963c5406d2b82f6b1d9f58?SAMLRequest=lVJdj9MwEPwr...  SAML
GET    https://login.terena.org/idp/saml2/idp/SSOService.php?SAMLRequest=lVJNj5swEL3vr0C%2Bg4Gwu4kVskoTrYq0bVBge%2BjNmEliydjU...  SAML
GET    https://login.terena.org/idp/module.php/core/loginuserpass.php?AuthState=_ee54a8e57df8bf7929586eaf3dceadd35713073637%3Ahttps%3...
GET    https://mail.google.com/mail/u/0/channel/bind?OSID=33FFF1723B3D748&OAID=53&VER=8&at=AF6bupMSWBcXodcsLnzLmSLiXbTH78eKmA...
POST   https://mail.google.com/mail/u/0/channel/bind?OSID=33FFF1723B3D748&OAID=53&VER=8&at=AF6bupMSWBcXodcsLnzLmSLiXbTH78eKmA...
```

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    ID="_acd97a5c4d2f36b685f4936f841249f55805a6572b"
                    Version="2.0"
                    IssueInstant="2014-04-24T13:24:41Z"
                    Destination="https://engine.surfconext.nl/authentication/idp/single-sign-on
/add0aa33e5963c5406d2b82f6b1d9f58"
                    AssertionConsumerServiceURL="https://foodl.org/simplesaml/module.php/saml/sp
/saml2-acs.php/saml"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    >
    <saml:Issuer>https://foodl.org/simplesaml/module.php/saml/sp/metadata.php/saml</saml:Issuer>
    <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                        AllowCreate="true"
                        />
</samlp:AuthnRequest>
```

Federation Development Criteria

- Name, Webpage, Metadata Feed
- Policy for IdPs & SPs
- Metadata Registration Practice Statement
- Declaration Signed, Metadata Feed Validated



What to NOT focus on?

- Waiting until …
  - Innova|RED has their federation in “production”.
  - Argentina is a member of eduGAIN.
  - a “killer app” is found.

- “Other” or Future Federation Technologies
  - OpenID Connect + OAuth are being explored.
  - Hub&Spoke gateways already exist.

More that one choice is good…

- simpleSAMLphp
  - PHP
  - Multi-lingual support
- Shibboleth
  - IdP is Java, SP is C/mod_shib
  - Runs within Apache Tomcat
- PySAML2
  - Python
- Many plug-ins or modules available for common tools.
- Benefits are greater than using LDAP.

What to focus on?

Europe Latin America Collaborative e-Infrastructure for Research Activities

- Federating your campus systems
  - Talk to your researchers, staff & students
- Investigate key services
  - Intranet and Website
  - Webmail
    - Google Apps for Education, Microsoft 365
  - e-Learning – Moodle
  - Talk to your librarian about Journal Access
  - Find your own "killer app".

Interfederation Use Cases

Researchers

Often work together in international research projects, which operate many web-based services that need authentication. Services are in different countries/federations. Thanks to Interfederation researchers can use their institution's account.

Lecturers

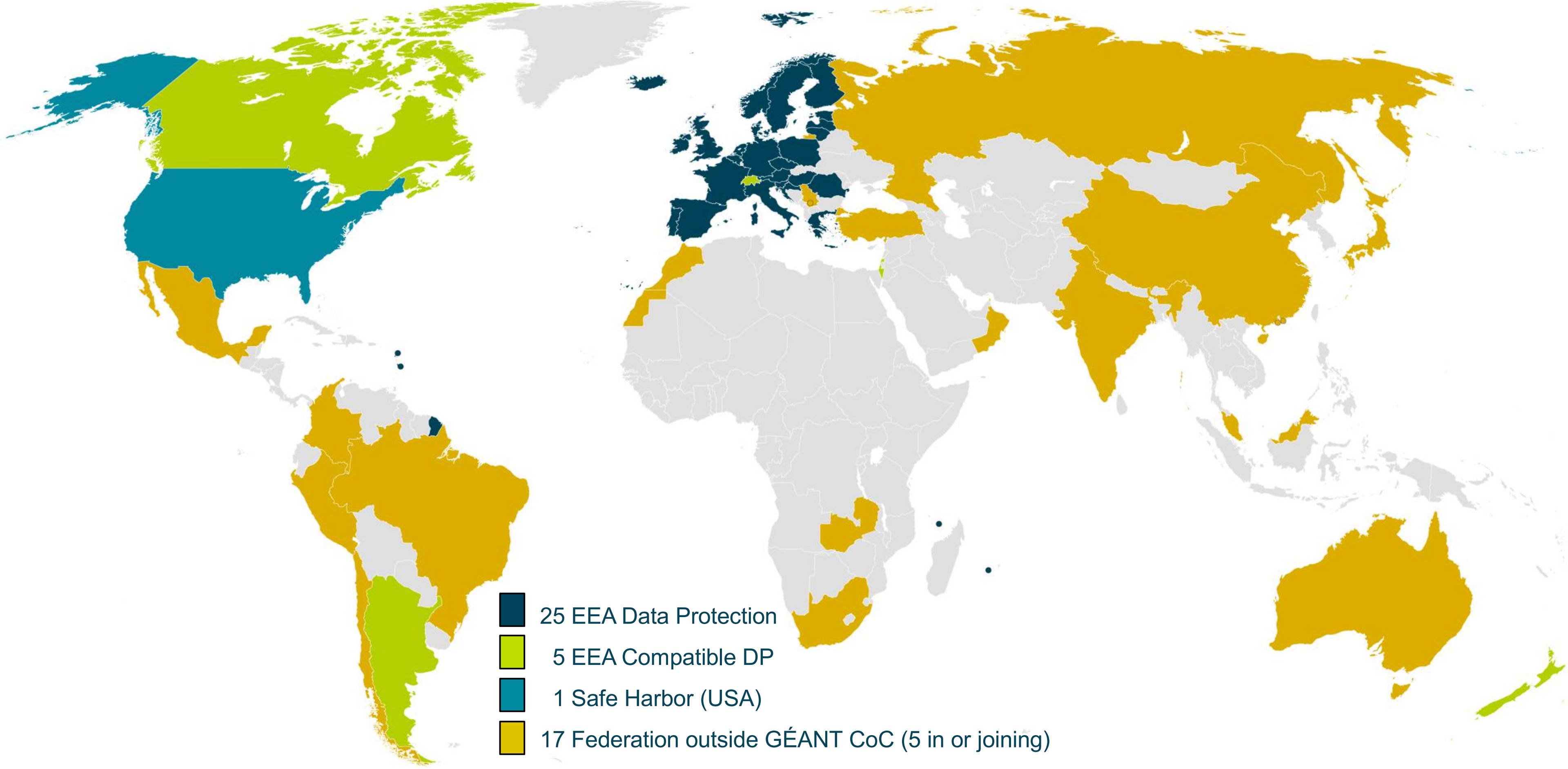
Can start e-learning collaborations across country borders. Create (costly) e-learning content collaboratively or easier "sell" it to other universities abroad.

Content Publishers

Companies like Elsevier/Thomson Reuters/etc. already joined multiple identity federations. Cumbersome for them and for federation operators.

Thanks to Interfederation: Join one, be connected to many!

GÉANT Code of Conduct

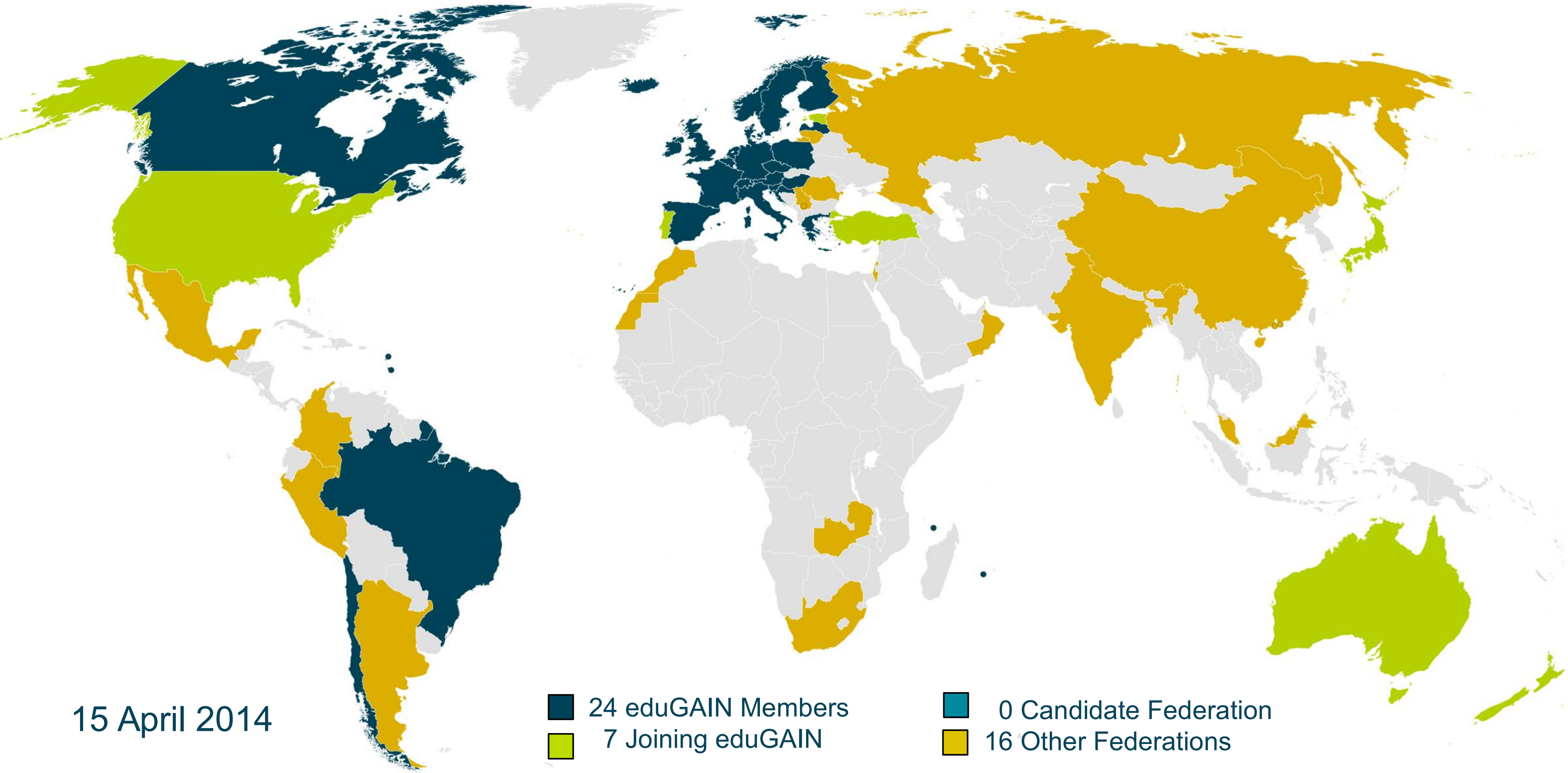


- 25 EEA Data Protection
- 5 EEA Compatible DP
- 1 Safe Harbor (USA)
- 17 Federation outside GÉANT CoC (5 in or joining)

Next steps…

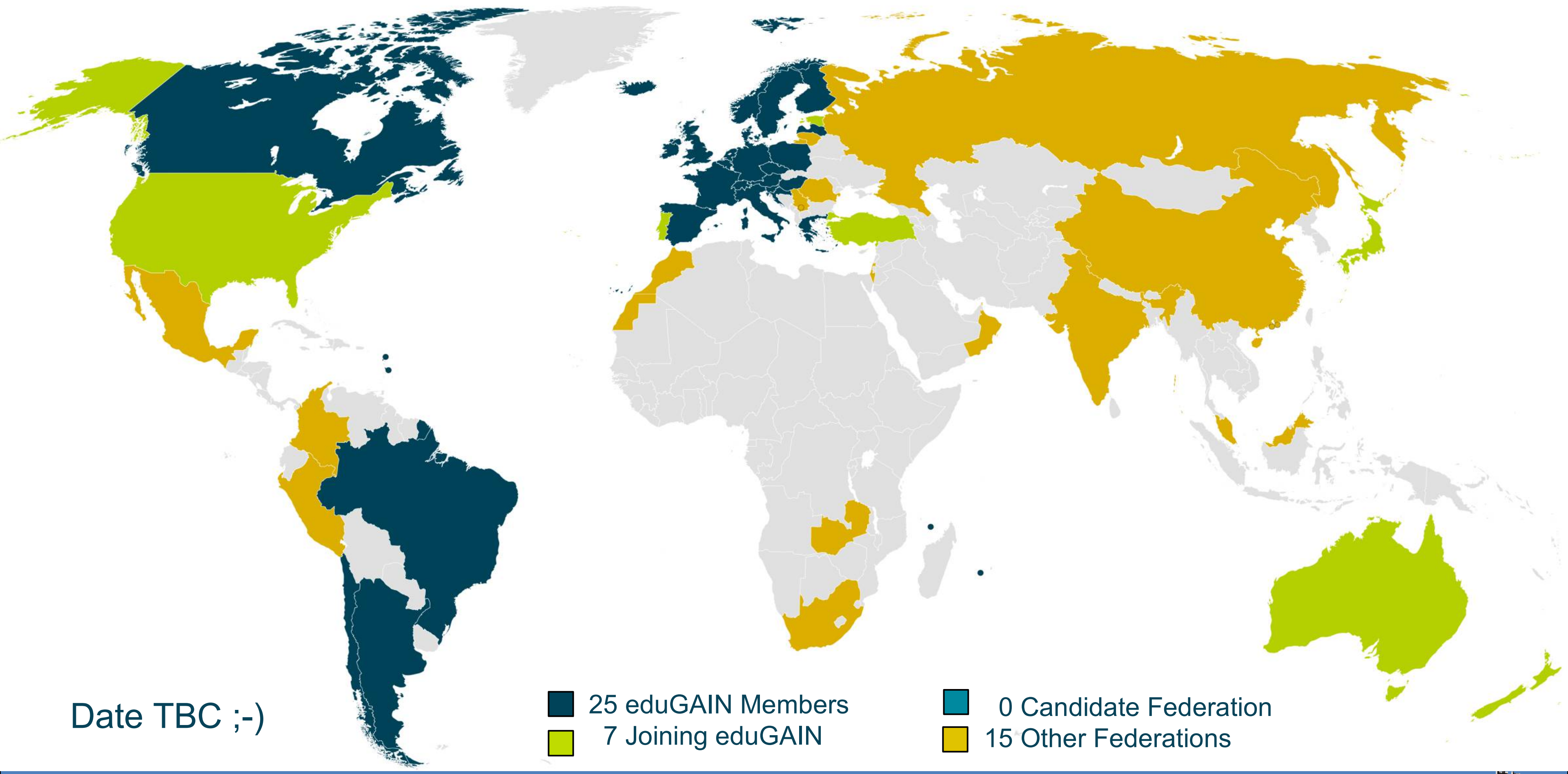
- Deploy eduroam □ Use it at TICAR2015
- Pick a campus federation architecture:
  - Hub&Spoke or Mesh
- Deploy an IdP
  - PySAML2, simpleSAMLphp, Shibboleth
- Connect with Innova|RED
- Connect with the community
  - Argentina, Latin America and Globally
- Federate your services

eduGAIN & Federations



15 April 2014

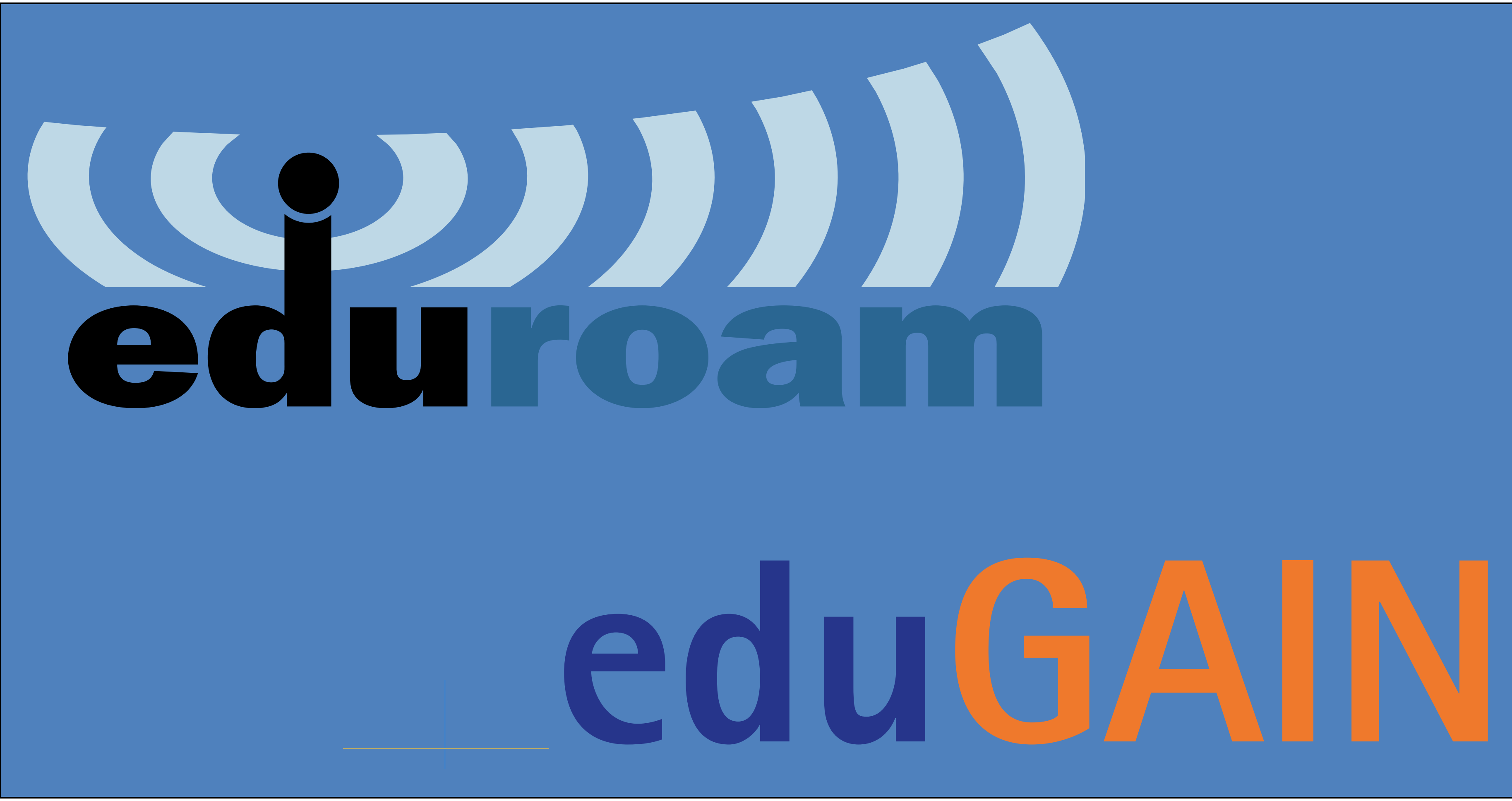
eduGAIN & MATE



Date TBC ;-)

- 🟦 25 eduGAIN Members
- 🟩 7 Joining eduGAIN
- 🟦 0 Candidate Federation
- 🟨 15 Other Federations

A family of services



</end>

Brook Schofield
schofield@terena.org