

Federated Identity and Privacy

in Higher Education Environments

Victoriano Giralt

Central ICT Services
University of Málaga
co-chair of TERENA TF-EMC²

EEMA e-Identity Interoperability Conference
Biel/Bienne
March 28th, 2012

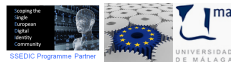
Those
who do not know
their past
cannot understand
their present



UCLouvain Programme Partner



Those
who do not know
their past
are forced
to repeat it



Those
who do not know
their past
will reinvent the wheel



Athens

again greeks at start of civilization



all started in ancient Greece



Athens

again greeks at start of civilization



not quite



Athens

again greeks at start of civilization



it was really JISC in the UK that started this in August 1999



Athens

again greeks at start of civilization

Development of a JISC Authentication Service

JISC's Committee for Electronic Information gave the go-ahead last week to develop a JISC Authentication Service, based on the successful ATHENS access management system.

it was really JISC in the UK that started this in August 1999

Norman Wiseman

Thu, 19 Nov 1998 16:30:45 +0000

ATHENS@JISMAIL.AC.UK

<https://www.jiscmail.ac.uk/cgi-bin/webadmin?A2=athens;e01bbb21.98>



Athens

again greeks at start of civilization



access to library resources, the problem for the solution



PAPI, A-Select

Spanish and Dutch follow pretty close



- January 1st, 2001
A PAPI Guide for Beginners hits the web
<http://papi.rediris.es/perl/pod/PAPI-gb.html>

- January 1st, 2002

In 2002 Alfa & Ariss has been awarded with a development contract by SURFnet for the developments of A-Select. . .

<https://www.surfgroepen.nl/sites/surf-idm/a-select/Lists/ASelect%20history/DispForm.aspx?ID=1>



WebISO and Shibboleth

Americans were not standing still

- August 2nd, 2002
oldest dated information on Internet2 WebISO site

<http://middleware.internet2.edu/webiso/>



- June 1st, 2003
Shibboleth 1.0 released after 3 years work

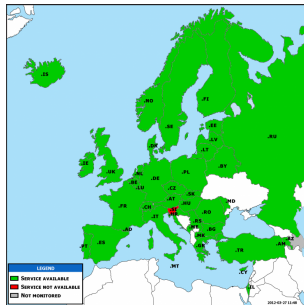
<http://shibboleth.internet2.edu/project.html>



eduroam®

federate outside the web

The Americas ←



→ Asia and Pacific



Privacy

from the ground up



Privacy

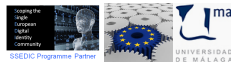
from the ground up



Privacy

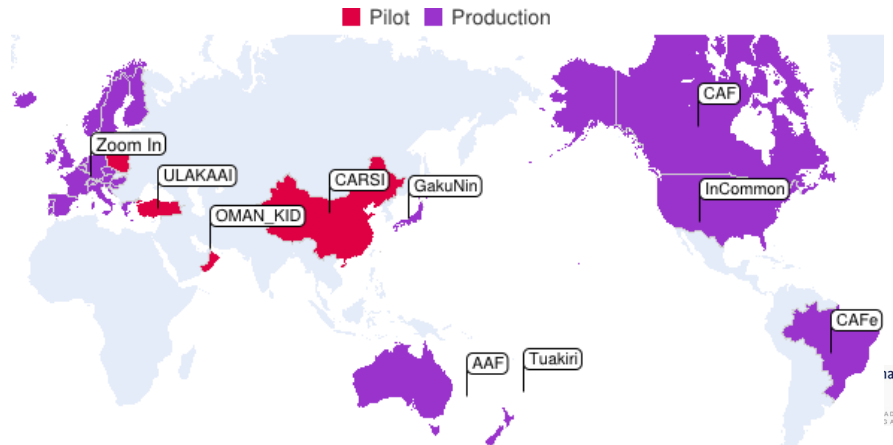
from the ground up

- eduPersonTargetedId
- SAML NameId permanent
- SAML NameId transient



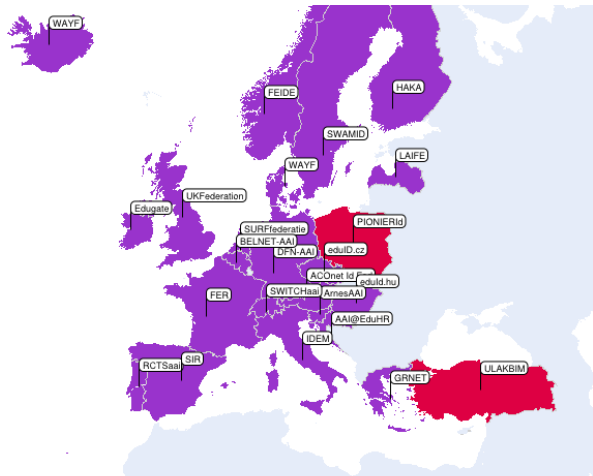
HiEd Federations

spanning the globe



HiEd Federations

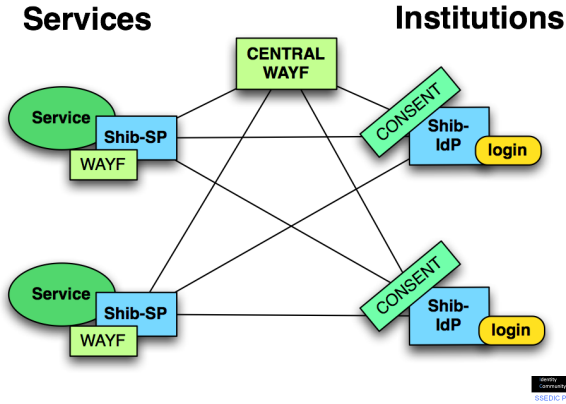
covering Europe



Mesh

Two different forms of federation

Meshed federation

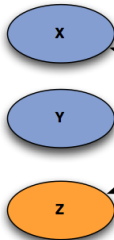


Hub & Spoke

Two different forms of federation

Hub & Spoke federation

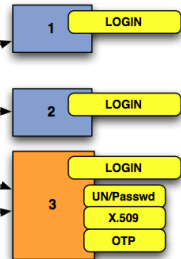
Services



Trusted 3rd party



Institutions



Possible agreement

Hub&Spoke model



Interfederation

the Kalmar2 union



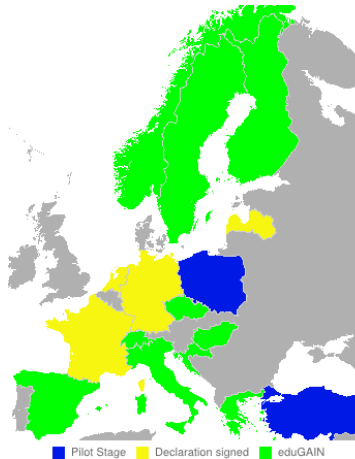
SECEDIC Programme Partner



UNIVERSIDAD DE MÁLAGA

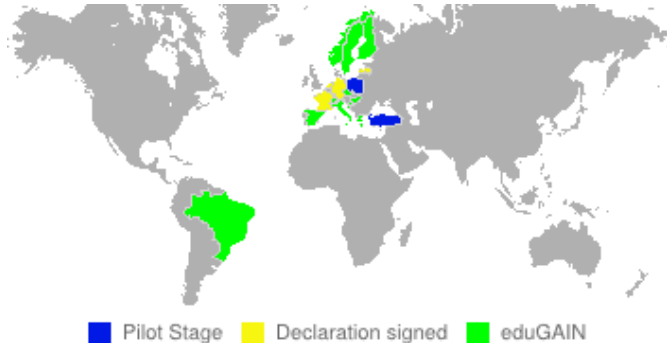
Interfederation

edugain: started in Europe



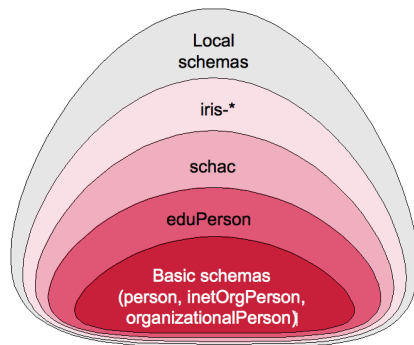
Interfederation

edugain: reaching out for the globe



Interoperability

semantics is key



Interoperability

protocol adaptation



Interoperability

protocol adaptation

- June 17th, 2002


Ken has succeeded in starting a discussion about integrating Shibboleth with PAPI

<http://middleware.internet2.edu/MACE/minutes/MACE-17-June-2002.html>



Interoperability

protocol adaptation

Protocols supported by the SIR hub 

- PAPI v.1
- SAML 1.1 / Shibboleth 1.3
- SAML 2 / Interoperable SAML2 Profile / Shibboleth 2
- eduGAIN SAML 1.1 profile
- OpenID versions 1 and 2
- Proprietary Protocols
 - Put some text here
 - Microsoft Live@Edu SSO
 - MSDN Academic Alliance
 - Wiley Trusted Proxy Server



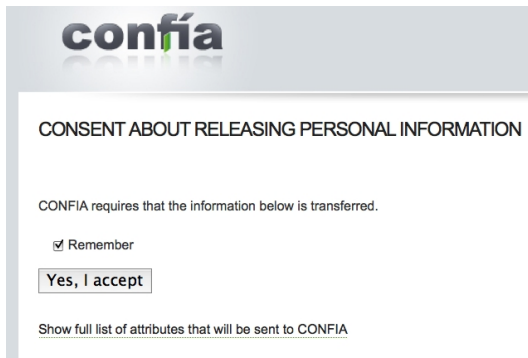
Privacy

there are many ways to look at privacy in education



Privacy

then, we need to involve the user




The image shows a screenshot of a web form titled "confía" (CONFIA). The form is titled "CONSENT ABOUT RELEASING PERSONAL INFORMATION". Below the title, it states "CONFIA requires that the information below is transferred." There is a checked checkbox labeled "Remember". Below that is a button labeled "Yes, I accept". At the bottom, there is a link that says "Show full list of attributes that will be sent to CONFIA".



Privacy

then, we need to involve the user



1/198

CONTRIA requires that the information below is transferred.

Remember

Show all list of attributes that will be sent to CONTRIA

| |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Organization Name Empresa Constructor S/G |
| Display Name Empresa Constructor S/G |
| Endowment regarding the service <ul style="list-style-type: none"> Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios |
| Primary location España |
| Person's principal name at home organization 01-00000000@unma.es |
| @work name Empresa |
| Alternative mail <ul style="list-style-type: none"> 01-00000000@unma.es 01-00000000@unma.es |
| Alternative mail 01-00000000@unma.es |
| Initials of the person <ul style="list-style-type: none"> Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios Un acceso a los datos de identificación legal de los usuarios de la red de acceso a los servicios |
| Mail |



SEIG-EDC Programme Partner



UNIVERSIDAD DE MÁLAGA

Applications

the art of domestication

Applications are key to the success of ...

Jon Shamah at EEMA e-Identity Interoperability, Biel/Bienne, 2012
and many others before and after him 😊



Applications

the art of domestication



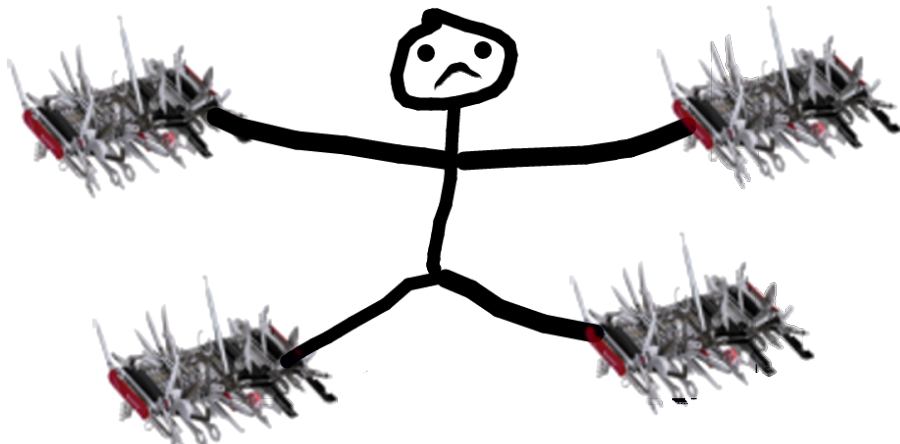
Programme Partner



UNIVERSIDAD
DE MÁLAGA

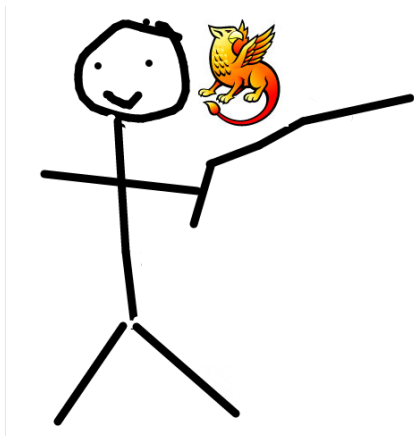
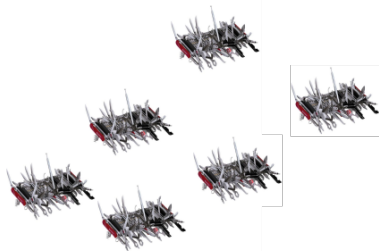
Applications

the art of domestication



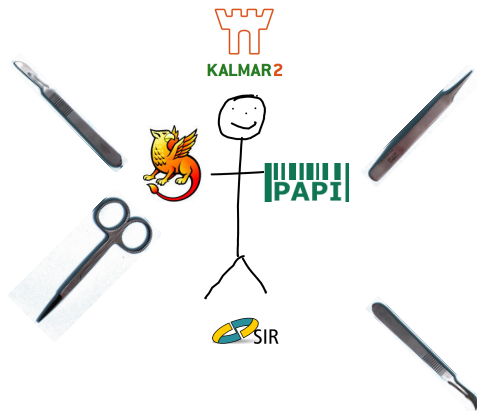
Applications

the art of domestication



Applications

the art of domestication



Refeds

global federation politics



16 million users across thousands of institutions



SCEDHC Programme Partner



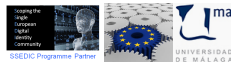
Refeds

global federation politics

- PEER → Public Endpoint Entity Registry
- LEGO → Linked Education and Government Online
- Attribute Release Working Group recommendations
- Barriers for Service Providers document



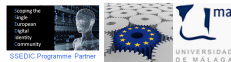
The future
is
now



Federate outside the web

We still use other Internet protocols in HiEd

- RADSec
<http://tools.ietf.org/html/draft-ietf-radext-radsec-12>
- Project Moonshot
<http://project-moonshot.org/>
- SAML-SASL
<http://tools.ietf.org/html/draft-ietf-kitten-sasl-saml-09>



Delegated authentication

do I trust your credentials?

SP ↔



↔ IdP



Delegated authentication

do I trust your credentials?



SECEDIC Programme Partner



UNIVERSIDAD DE MÁLAGA

Delegated authentication

do I trust your credentials?



Digital natives are arriving at universities



Delegated authentication

do I trust your credentials?



Digital natives like their social networks
Social logins for Identity Federations

(CC) <http://icon.leau.net>



Groups

people from everywhere



(CC) <http://www.lumaxart.com/>



Groups

people from everywhere

- Grouper
- COmanage
- OAuth2
- Virtual Organizations
- SOAP queries to mail list managers
- ...



Groups

people from everywhere



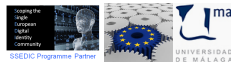
References

do not [blindly] trust my words

<http://eduroam.org/> <http://www.refeds.org/>
<http://www.wayf.dk/> <http://papi.rediris.es/>
<http://shibboleth.net/> <http://edugain.org/>
<http://www.internet2.edu/comanage/>
<http://www.internet2.edu/grouper/>
<http://www.rediris.es/sir/>



Thank you



Thank you

Questions?

answers not assured

