Confía

Design and implementation details of the Public Andalusian Universities Identity Federation

Victoriano Giralt[6] Jesus Gordillo[3] Victor Hernández[2]
Luís Meléndez[4] Manuel Ramos[7] Ernesto Revilla[8]
José Ruiz[5] Francisco Sánchez[1]

[1]International University of Andalusia [2]"Pablo de Olavide" University

[3]University of Cádiz [4]University of Córdoba [5]University of Granada

[6]University of Málaga [7]University of Seville [8]Yaco Sistemas, SL

EUNIS
Warsaw
June 24th 2010

Dream

A dream

ten universities, one campus

IN CLIMINE SAPIENTIA UNIVERSITAS ALMERIENSIS
UCA
Universidad de Cádiz
UNIVERSIDAD D CÓRDOBA
Universidad de Huelva
UNIVERSITAS GIENNENSIS
uma
UNIVERSIDAD DE MÁLAGA
unia
Universidad Internacional de Andalucía
UNIVERSIDAD
SEVILLA
AÑO 1997
PABLO OLAVIDE
UNIVERSIDAD DE SEVILLA

confia

A dream

ten universities, one campus

Campus Andaluz Virtual
CAV

(Andalusian Virtual Campus)

A nightmare

ten LMSs, ten IAM systems

A nightmare

ten LMSs, ten IAM systems

For the first three academic terms, the system required

A nightmare

ten LMSs, ten IAM systems

For the first three academic terms, the system required

- Personal information exchange amongst universities

A nightmare

ten LMSs, ten IAM systems

For the first three academic terms, the system required

- Personal information exchange amongst universities
- Course enrollment exchange amongst universities

A nightmare

ten LMSs, ten IAM systems

For the first three academic terms, the system required

- Personal information exchange amongst universities
- Course enrollment exchange amongst universities
- Assigning credentials to each user in every LMS

A nightmare

ten LMSs, ten IAM systems

For the first three academic terms, the system required

- Personal information exchange amongst universities
- Course enrollment exchange amongst universities
- Assigning credentials to each user in every LMS
- Credential distribution

A nightmare

ten LMSs, ten IAM systems

A nightmare

ten LMSs, ten IAM systems

All this resulted in

A nightmare

ten LMSs, ten IAM systems

All this resulted in

- High administration overload

A nightmare

ten LMSs, ten IAM systems

All this resulted in

- High administration overload
- Users with ten sets of credentials

A nightmare

ten LMSs, ten IAM systems

All this resulted in

- High administration overload
- Users with ten sets of credentials
- Wrong personal data

A nightmare

ten LMSs, ten IAM systems

All this resulted in

- High administration overload
- Users with ten sets of credentials
- Wrong personal data
- High error rates

A new dream

we want a federation

A dream come true

we will get our federation

A dream come true

we will get our federation

Political backing

A dream come true

we will get our federation

Political backing

- Technical committee formed

A dream come true

we will get our federation

Political backing

- Technical committee formed
- Funds assigned off Digital University project

A dream come true

we will get our federation

Political backing

- Technical committee formed
- Funds assigned off Digital University project
- Procurement for a contract launched

A dream come true

we will get our federation

Political backing

- Technical committee formed
- Funds assigned off Digital University project
- Procurement for a contract launched
- Contract granted

Design

Services

one driving force for a federation

Services

one driving force for a federation

We need to support three different LMSs

Services

one driving force for a federation

We need to support three different LMSs

- Moodle

Services

one driving force for a federation

We need to support three different LMSs

- Moodle
- Ilias

Services

one driving force for a federation

We need to support three different LMSs

- Moodle
- Ilias
- WebCT

Identity transport

moving personal data around

Identity transport

moving personal data around

Easy decision: SAML 2

Identity transport

moving personal data around

Easy decision: SAML 2

- SAML2 interoperability

Identity transport

moving personal data around

Easy decision: SAML 2

- SAML2 interoperability
- Web SSO profile

Identity transport

moving personal data around

Easy decision: SAML 2

- SAML2 interoperability
- Web SSO profile
- http redirect binding for AuthN

Identity transport

moving personal data around

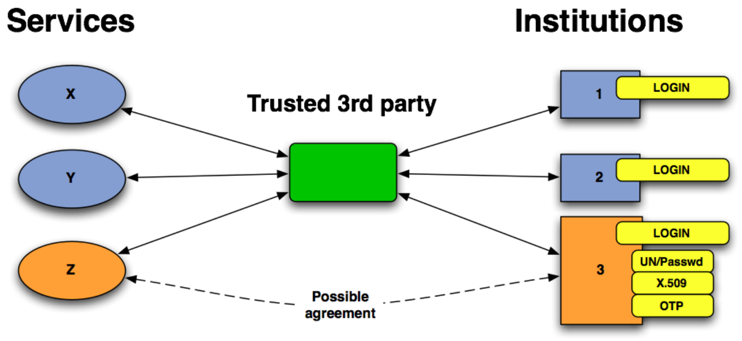
Easy decision: SAML 2

- SAML2 interoperability
- Web SSO profile
- http redirect binding for AuthN
- http POST binding for assertions

Trust fabric

how is our federation organised

Hub & Spoke federation



Trust fabric

establishing trust

Trust fabric

establishing trust

Heavy use of X.509 and cryptography

Trust fabric

establishing trust

Heavy use of X.509 and cryptography

- TCS certificates for relaying parties

Trust fabric

establishing trust

Heavy use of X.509 and cryptography

- TCS certificates for relaying parties
- Spanish *legal* X.509 certificates for administrators

Trust fabric

establishing trust

Heavy use of X.509 and cryptography

- TCS certificates for relaying parties
- Spanish *legal* X.509 certificates for administrators
- OCSP

Trust fabric

establishing trust

Heavy use of X.509 and cryptography

- TCS certificates for relaying parties
- Spanish *legal* X.509 certificates for administrators
- OCSP
- CRLs

Trust fabric

establishing trust

Heavy use of X.509 and cryptography

- TCS certificates for relaying parties
- Spanish *legal* X.509 certificates for administrators
- OCSP
- CRLs
- Signed *and* encrypted assertions

Attributes

the language for identity information

Attributes

the language for identity information

Three schemas

Attributes

the language for identity information

Three schemas

- eduPerson

Attributes

the language for identity information

Three schemas

- eduPerson
- SCHAC

Attributes

the language for identity information

Three schemas

- eduPerson
- SCHAC
- irisEduPerson

Attributes

the language for identity information

Attributes

the language for identity information

Three sets of attributes

Attributes

the language for identity information

Three sets of attributes

- Mandatory

Attributes

the language for identity information

Three sets of attributes

- Mandatory
- Recommended

Attributes

the language for identity information

Three sets of attributes

- Mandatory
- Recommended
- Optional

Software

no wheel reinventing here

Software

no wheel reinventing here

Openness is our motto

Software

no wheel reinventing here

Openness is our motto

We do not care about what you use

Software

no wheel reinventing here

Openness is our motto

We do not care about what you use

As log as it speaks SAML2

Software

no wheel reinventing here

Openness is our motto

- We do not care about what you use
- As log as it speaks SAML2
- An conforms to our profile

Software

no wheel reinventing here

Openness is our motto

- We do not care about what you use
- As log as it speaks SAML2
- An conforms to our profile
- But . . .

Software

no wheel reinventing here

Openness is our motto

- We do not care about what you use
- As log as it speaks SAML2
- An conforms to our profile
- But . . .
- If you cannot, we can translate

Software

no wheel reinventing here

Openness is our motto

- We do not care about what you use
- As log as it speaks SAML2
- An conforms to our profile
- But . . .
- If you cannot, we can translate
- And . . .

Software

no wheel reinventing here

Openness is our motto

- We do not care about what you use
- As log as it speaks SAML2
- An conforms to our profile
- But . . .
- If you cannot, we can translate
- And . . .
- We prefer Open Source

Software

no wheel reinventing here

Software

no wheel reinventing here

SimpleSAMLphp in the core

Software

no wheel reinventing here

SimpleSAMLphp in the core

- Lightweight

Software

no wheel reinventing here

SimpleSAMLphp in the core

- Lightweight
- Easy to install, integrate, maintain, develop

Software

no wheel reinventing here

SimpleSAMLphp in the core

- Lightweight
- Easy to install, integrate, maintain, develop
- Well documented

Software

no wheel reinventing here

SimpleSAMLphp in the core

- Lightweight
- Easy to install, integrate, maintain, develop
- Well documented
- Scalable and modular

Software

no wheel reinventing here

SimpleSAMLphp in the core

- Lightweight
- Easy to install, integrate, maintain, develop
- Well documented
- Scalable and modular
- Multiprotocol

Software

no wheel reinventing here

SimpleSAMLphp in the core

- Lightweight
- Easy to install, integrate, maintain, develop
- Well documented
- Scalable and modular
- Multiprotocol
- Easy to write attribute filters

Software

no wheel reinventing here

SimpleSAMLphp in the core

- Lightweight
- Easy to install, integrate, maintain, develop
- Well documented
- Scalable and modular
- Multiprotocol
- Easy to write attribute filters
- Widely used

Software

no wheel reinventing here

SimpleSAMLphp in the core

- Lightweight
- Easy to install, integrate, maintain, develop
- Well documented
- Scalable and modular
- Multiprotocol
- Easy to write attribute filters
- Widely used
- Open Source

Software

no wheel reinventing here

Software

no wheel reinventing here

A code of coding conduct

Software

no wheel reinventing here

A code of coding conduct

- Reuse others code

Software

no wheel reinventing here

A code of coding conduct

- Reuse others code
- Contribute your code

Build

IdP

the source of identities

IdP

the source of identities

- Multiple SSO methods

IdP

the source of identities

- Multiple SSO methods
  - Pure SAML

IdP

the source of identities

- Multiple SSO methods
  - Pure SAML
  - PAPI

IdP

the source of identities

- Multiple SSO methods
  - Pure SAML
  - PAPI
  - OpenSSO

IdP

the source of identities

- Multiple SSO methods
  - Pure SAML
  - PAPI
  - OpenSSO
  - ...

IdP

the source of identities

- Multiple SSO methods
  - Pure SAML
  - PAPI
  - OpenSSO
  - . . .
- Attribute filters

IdP

the source of identities

- Multiple SSO methods
  - Pure SAML
  - PAPI
  - OpenSSO
  - . . .
- Attribute filters
- Multiple source attribute collector

IdP

the source of identities

- Multiple SSO methods
  - Pure SAML
  - PAPI
  - OpenSSO
  - . . .
- Attribute filters
- Multiple source attribute collector
  - LDAP

IdP

the source of identities

- Multiple SSO methods
  - Pure SAML
  - PAPI
  - OpenSSO
  - . . .
- Attribute filters
- Multiple source attribute collector
  - LDAP
  - SQL

IdP

the source of identities

- Multiple SSO methods
  - Pure SAML
  - PAPI
  - OpenSSO
  - . . .
- Attribute filters
- Multiple source attribute collector
  - LDAP
  - SQL
  - SOAP

IdP

the source of identities

- Multiple SSO methods
  - Pure SAML
  - PAPI
  - OpenSSO
  - . . .
- Attribute filters
- Multiple source attribute collector
  - LDAP
  - SQL
  - SOAP
- Course provisioning information

SP

services for users

SP

services for users

Develop, improve or adapt code in the LMSs for

SP

services for users

Develop, improve or adapt code in the LMSs for

- Federated login

SP

services for users

Develop, improve or adapt code in the LMSs for

- Federated login
- *On the fly* user provisioning

SP

services for users

Develop, improve or adapt code in the LMSs for

- Federated login
- *On the fly* user provisioning
- *On the fly* course enrollment

SP

services for users

Develop, improve or adapt code in the LMSs for

- Federated login
- *On the fly* user provisioning
- *On the fly* course enrollment
- SAML based access control

Hub

the data processor

Hub

the data processor

Common services

Hub

the data processor

Common services

- Explicit user consent

Hub

the data processor

Common services

- Explicit user consent
- Attribute validator

Hub

the data processor

Common services

- Explicit user consent
- Attribute validator
- Automatic metadata distribution

Hub

the data processor

Common services

- Explicit user consent
- Attribute validator
- Automatic metadata distribution
- Federated metadata manager with alternative AuthN

Hub

the data processor

Common services

- Explicit user consent
- Attribute validator
- Automatic metadata distribution
- Federated metadata manager with alternative AuthN
- Attribute release policy, with editor

Hub

the data processor

Common services

- Explicit user consent
- Attribute validator
- Automatic metadata distribution
- Federated metadata manager with alternative AuthN
- Attribute release policy, with editor
- Federated monitoring tools

Hub

the data processor

Common services

- Explicit user consent
- Attribute validator
- Automatic metadata distribution
- Federated metadata manager with alternative AuthN
- Attribute release policy, with editor
- Federated monitoring tools
- Periodic certificate validation

Deliver

Federation identity

visibility to users

Federation identity

visibility to users

The federation needs to be *visible* on the *Net*

Federation identity

visibility to users

The federation needs to be *visible* on the *Net*

- Internet domain

Federation identity

visibility to users

The federation needs to be *visible* on the *Net*

- Internet domain
  - CONFIA.aupa.info

Federation identity

visibility to users

The federation needs to be *visible* on the *Net*

- Internet domain
  - CONFIA.aupa.info
- Visual identity

Federation identity

visibility to users

The federation needs to be *visible* on the *Net*

- Internet domain
  - CONFIA.aupa.info
- Visual identity
  - Identifying federated access

Federation identity

visibility to users

The federation needs to be *visible* on the *Net*

- Internet domain
  - CONFIA.aupa.info
- Visual identity
  - Identifying federated access
  - Common resources

Federation identity

visibility to users

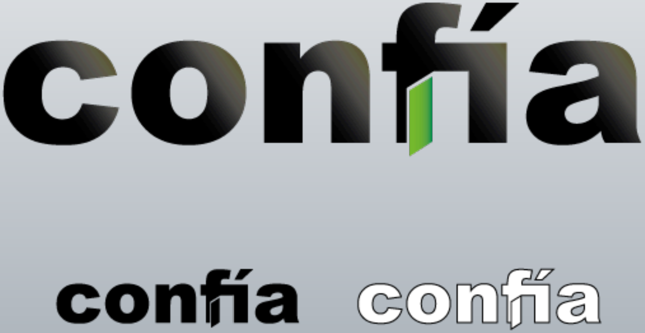
The federation needs to be *visible* on the *Net*

- Internet domain
  - CONFIA.aupa.info
- Visual identity
  - Identifying federated access
  - Common resources
  - Marketing material

Federation identity

visual identity

CONFÍA opens doors for you from your University



A working federation

measuring success

A working federation

measuring success

Usage of our federated virtual campus

A working federation

measuring success

Usage of our federated virtual campus

- 9000 students

A working federation

measuring success

Usage of our federated virtual campus

- 9000 students
- 100 courses

A working federation

measuring success

Usage of our federated virtual campus

- 9000 students
- 100 courses
- 15000 authentications / month

A working federation

measuring success

Usage of our federated virtual campus

- 9000 students
- 100 courses
- 15000 authentications / month
- $<$ 5 *problems* / month

Code

for sharing with others

All code produced is available at

- Upstream distribution points for
  - + SimpleSAMLphp
  - + JANUS
  - + Moodle
  - + Ilias
- https://forja.rediris.es/projects/confia/

Grow

New developments

creativity never sleeps

New developments

creativity never sleeps

Future plans for the federation

New developments

creativity never sleeps

Future plans for the federation

- Add more services

New developments

creativity never sleeps

Future plans for the federation

- Add more services
  - Federated SSH

New developments

creativity never sleeps

Future plans for the federation

- Add more services
  - Federated SSH
  - Federated Help Desk

New developments

creativity never sleeps

Future plans for the federation

- Add more services
  - Federated SSH
  - Federated Help Desk
  - . . .

New developments

creativity never sleeps

Future plans for the federation

- Add more services
  - Federated SSH
  - Federated Help Desk
  - . . .
- Connect to other federations

New developments

creativity never sleeps

Future plans for the federation

- Add more services
  - Federated SSH
  - Federated Help Desk
  - . . .
- Connect to other federations
  - SIR

New developments

creativity never sleeps

Future plans for the federation

- Add more services
  - Federated SSH
  - Federated Help Desk
  - . . .
- Connect to other federations
  - SIR
  - EduGAIN

New developments

creativity never sleeps

Future plans for the federation

- Add more services
  - Federated SSH
  - Federated Help Desk
  - . . .
- Connect to other federations
  - SIR
  - EduGAIN
  - . . .

Summary

Keys to our success

- Political will
- Previous experience reuse
- Open source
- Internal know how
- Enthusiastic commercial partner

Thank you

Thank you

Questions?

answers not assured