

# I have an IdP, now what?

## Rešitve AAI v univerzitetnih okoljih

## AAI solutions in university environs

Victoriano Giralt

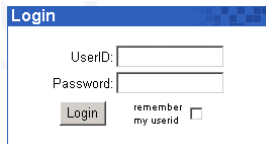
Central ICT Services  
Univerza v Malagi

Arnes Konferenca  
Kranjska Gora  
Sreda, 14.4.2010



# IdP

We can authenticate users and send attributes



**Login**

UserID:

Password:

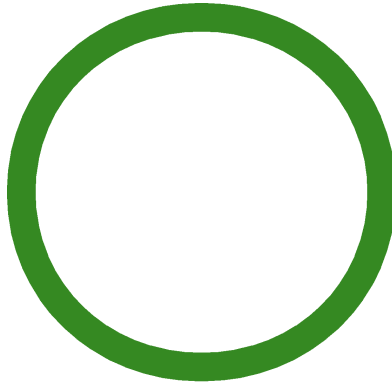
remember my userid



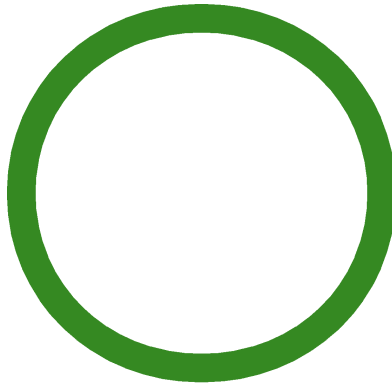
# We can federate



# We can federate



# We can federate



of trust



# What do we gain by federating

- Better and scalable access management
- Better and scalable identity management
- More services for users
- More users for services
- Better services



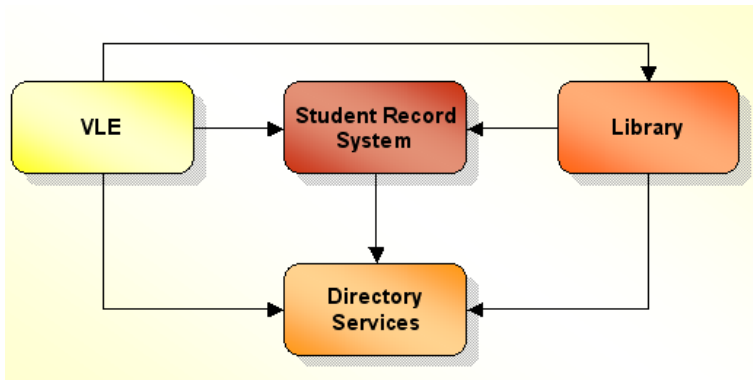
# The vision

Why federated identity is important in the University



# An ideal

## Enterprise Application Integration for Universities





# Is identity really so important?



# Two sides of one coin

Identity can be

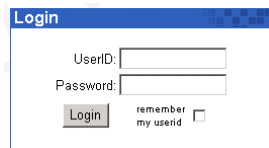
- A curse  $\Rightarrow$  anonymity
- A blessing  $\Rightarrow$  identity proofing



# What's an identity

in the digital world

A set of credentials and a set of attributes



Login

UserID:

Password:

Login  remember my userid



# The Dark Ages of Authentication

- There were no central credential repository
- Each and every application had its own
- Users were in the midst of their worst nightmare

Identity was very ill, it was totally fragmented



# The Enlightenment of Authentication

there IS a directory

- Directories appear
- We have a *centralised* credential repository
- We don't really know what to do with it
- Every application does its own authentication
- Fortunately, users only have to remember one set of credentials

Identity pieces were reunited again



# Identity in danger

The reunification of the identity makes it vulnerable



# Least privilege principle

or the parable of the significant other



# Least privilege principle

or the parable of the significant other

## Main characters





# Least privilege principle

or the parable of the significant other

## Main characters

The user



# Least privilege principle

or the parable of the significant other

## Main characters

The directory



# Least privilege principle

or the parable of the significant other

## Main characters

The application



# Least privilege principle

or the parable of the significant other



# Least privilege principle

or the parable of the significant other

## The plot



# Least privilege principle

or the parable of the significant other

## The plot



# Least privilege principle

or the parable of the significant other

## The plot



The user gives his credentials to the application.



# Least privilege principle

or the parable of the significant other

## The plot



The application gives the **user's** credentials to the directory





# Least privilege principle

or the parable of the significant other

## The plot



The application gets **user's access** to the directory



# Least privilege principle

or the parable of the significant other

## The plot



The user gets access to the application



# Least privilege principle

or the parable of the significant other

## The plot



Everyone is happy



# Least privilege principle

or the parable of the significant other

## The plot



Everyone is happy, right?



# Least privilege principle

or the parable of the significant other



# Least privilege principle

or the parable of the significant other

## A better plot



# Least privilege principle

or the parable of the significant other

## A better plot



# Least privilege principle

or the parable of the significant other

## A better plot



The user gives his credentials to the application.





# Least privilege principle

or the parable of the significant other

## A better plot



The application gives **its** credentials to the directory



# Least privilege principle

or the parable of the significant other

## A better plot



The application gets **application's access** to the directory



# Least privilege principle

or the parable of the significant other

## A better plot

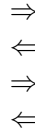


The application checks user's credentials with the directory

# Least privilege principle

or the parable of the significant other

## A better plot



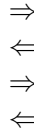
The user gets access to the application



# Least privilege principle

or the parable of the significant other

## A better plot



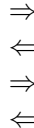
Everyone is happy



# Least privilege principle

or the parable of the significant other

## A better plot



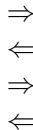
Everyone is happy, or not...



# Least privilege principle

or the parable of the significant other

## A better plot



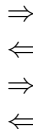
The application has access to the user credentials



# Least privilege principle

or the parable of the significant other

## A better plot



Can we trust our applications?

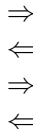




# Least privilege principle

or the parable of the significant other

## A better plot

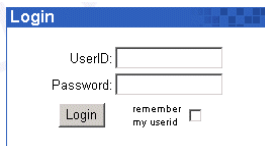


Can we trust our applications? All of them?



# A single point for authentication

We can protect credentials and attributes



Login

UserID:

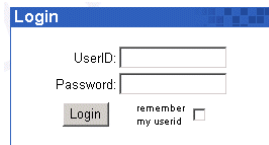
Password:

Login  remember my userid



# A single point for authentication

We can teach our users



**Login**

UserID:

Password:

remember my userid



# Rethinking the model

We need a new paradigm



# Old model

## rooms and walls

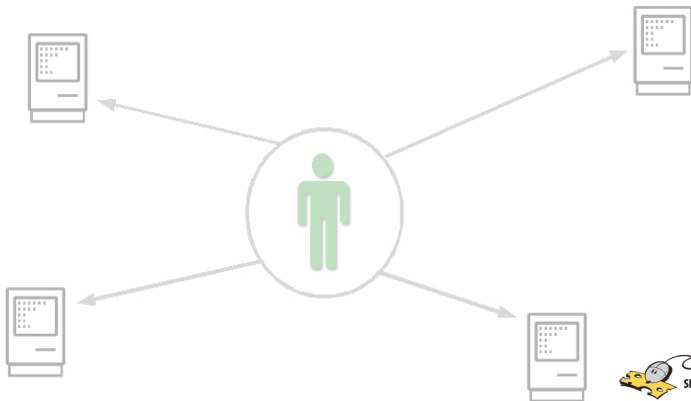


03:51:00



# Identity as a service

## User centric applications



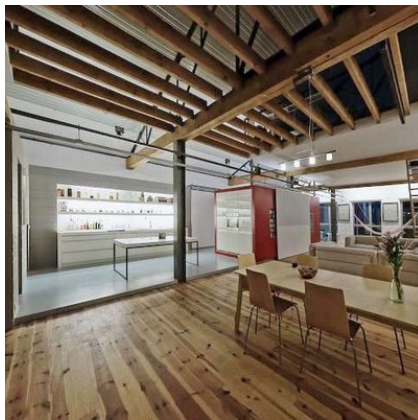
# Identity as a service

## User centric applications



# New model

an open seamless space





# Requirements

a building plan for our loft



# Requirements

a building plan for our loft

*Our* applications should



# Requirements

a building plan for our loft

*Our* applications should

- Collaborate among themselves
- Be centred around the user
- Reduce the burden on the user
- Integrate corporate data
- Account for previous user experience
- Best of breed applications for each service
- Reduce the barrier to entry



# Collaboration

use the identity to put the user in control

*Interoperability is the degree to which a provider and a consumer can successfully interface having never met*

*Coppeto, T.: Introduction To OSID V3 for developers*



# Central ICT clustered apps

Tools for collaborating

We want to provide tools for groups to work together



# Central ICT clustered apps

## Tools for collaborating

We want to provide tools for groups to work together

- Group management
- Wiki
- Blog
- Mailing list
- Web Forum
- Chat
- Web file sharing
- ...

all of them sharing the same credentials



# Central ICT clustered apps

## Tools for collaborating

We want to provide tools for groups to work together

- Group management
- Wiki
- Blog
- Mailing list
- Web Forum
- Chat
- Web file sharing
- ...

all of them sharing the session



# The quest for our goal





# The quest for our goal

A long and winding road



# The quest for our goal

A long and winding road



# The quest for our goal

A long and winding road



# The quest for our goal

we thought we had entered the gates of Hell



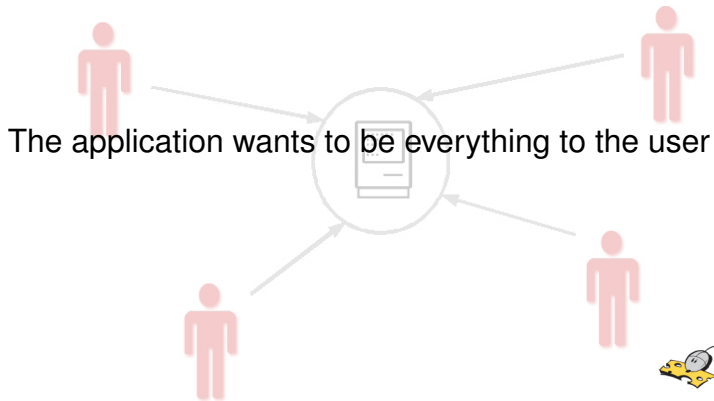
# Application centric

the paradigm of the monolithic platform



# Application centric

the paradigm of the monolithic platform



# The feature race

and endless rush to nowhere

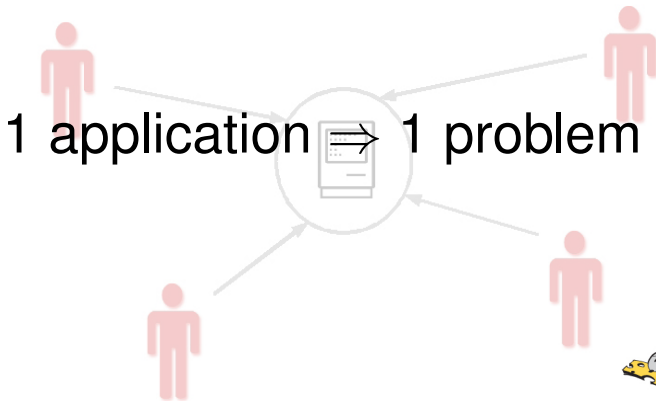


Severe case of kitchen sink syndrome



# The platform application

a cure for your problems





# The platform application

a cure for your problems?



Applications have an attitude



# The platform application

a cure for your problems?

There's one way for doing things



# The platform application

a cure for your problems?

There's one way for doing things



# Provisioning

bending processes to *the attitude*

It is possible to abide to the application's desires



# Provisioning

bending processes to *the attitude*

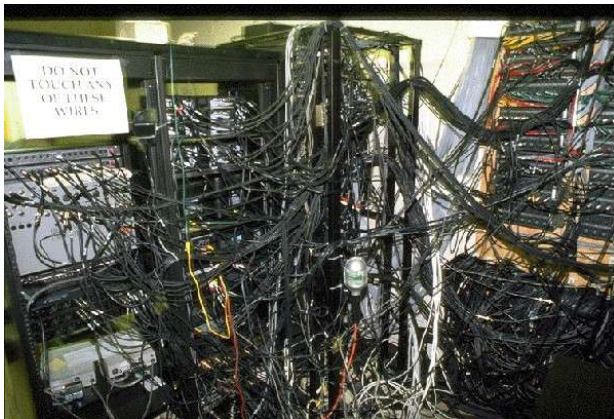
It is possible to abide to the application's desires

- Devising provisioning strategies
- Using not much extended technologies
- Reciting obscure incantations
- ...



# Provisioning

bending processes to *the attitude*



# Are we doomed?

what can developers and sysadmins do?



# FIAM

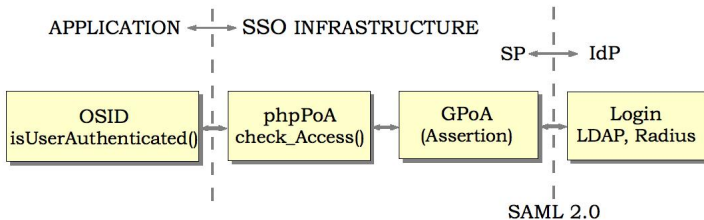
Federated Identity is coming to our rescue





# Authentication architecture

mechanism independence



# *The glue*

that holds pieces in place



# *The glue*

that holds pieces in place

We developed a mini framework for integrating apps



# *The glue*

that holds pieces in place

We developed a mini framework for integrating apps

- Minimal code modification
- Common operations
  - user logged in?
  - authenticate user
  - get attributes
  - close session
- Interchangeable identity transports



# Issues

we have found in our quest



# Issues

we have found in our quest

We have hit some walls along the way



# Issues

we have found in our quest

We have hit some walls along the way

- Session clash
- Cookie mixup
- Application user stores
- Tangled code
- Closed source
- ...



# We achieved many of our goals





# We achieved many of our goals

There is light at the end of the tunnel



# We achieved many of our goals



# We achieved many of our goals

Now



# We achieved many of our goals

## Now

- We have a good set of applications playing together
- We can easily incorporate external users
- We can easily connect services provided by others
- We are part of a 10 university virtual campus



# Tools

We have had some help

- SAML
- Simple SAML php
- Shibboleth
- memcached
- Django
- Sympa
- MediaWiki
- DokuWiki
- OIOSAML
- ...



# Enablers

The main accelerators for our work

- Open source applications
- Working with the community



# Enablers

The main accelerators for our work

- Open source applications
- Working with the community
- HTTP basic authentication
- Provisioning APIs



# Remaining needs

We desperately need

- User decoupling
- External authorization
- Forget about provisioning
- Proper group management
- Collaboration management:  
Virtual Environments → Collaborative Organizations
- Logout that really works
- Reach out of the web





# Hvala



# Hvala

there goes my remaining Slovene



?

?

?

?

Hvala

?

?

there goes my remaining Slovene

Questions?

answers not assured

?

?

?

?

