



UPORTOaai

The Authentication and Authorization Infrastructure at the University of Porto

Dublin – Ireland, 16th June 2011

José Sousa (jasousa@reit.up.pt)
Rui Ramos (rramos@reit.up.pt)
Sérgio Afonso (safonso@reit.up.pt)
Lígia Ribeiro (lmr@reit.up.pt)

Summary



100

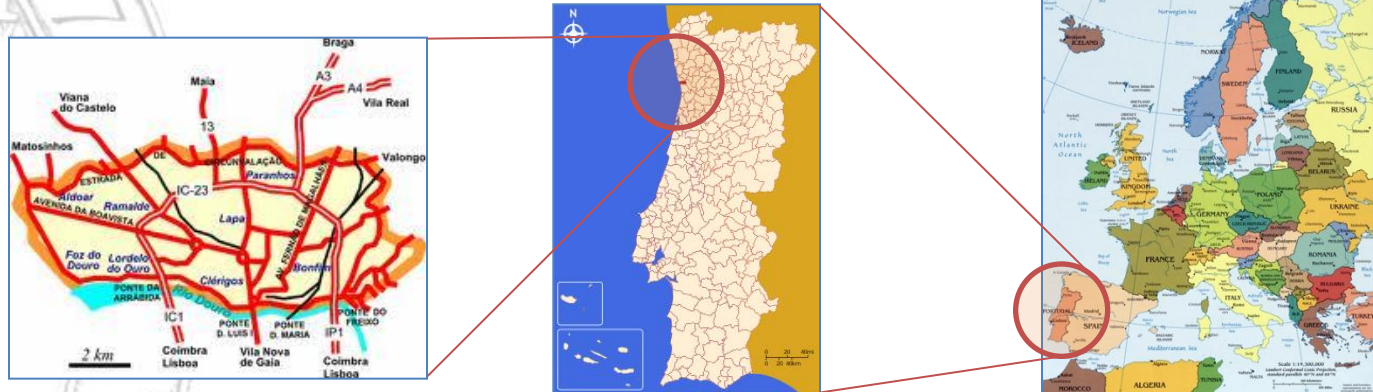
U.PORTO

UNIVERSIDADE
DO PORTO

- Introduction
- U.Porto AAI Project
 - Starting point
 - Implementation
 - Federated services
 - Results
- Limitations and future work
- Technical implementation and examples

- Location

- Porto is the second city of Portugal and the centre of an urban region with a population of over one million.



- Origins

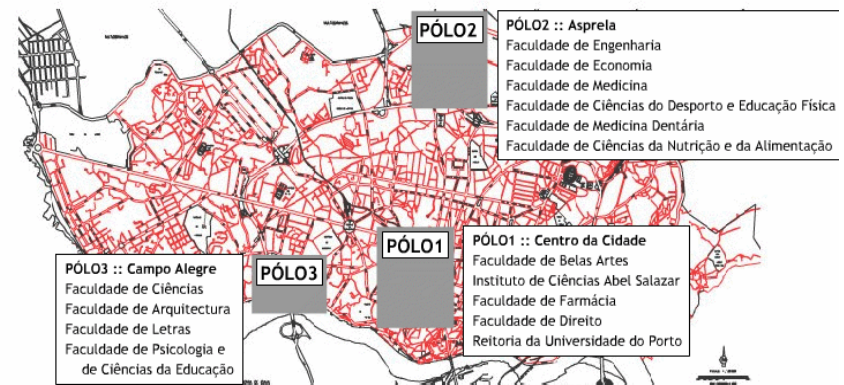
- 22nd March **1911**: The University of Porto was created by decree of the first Portuguese Republican Government, on offspring of older schools (origins dating back to the 18th century)
- May **2009**: new statutes were published and U.PORTO is nowadays a public foundation, under private law



University of Porto



- **14 Faculties + 1 Business School**
- 61 R&D Institutes
- ~ 700 Study programs
- ~ **31.000 Students**
- ~ 1.920 Teachers and researchers (FTE)
- ~ 1.650 Technical and administrative staff (FTE)
- Geographic dispersion
 - 3 locations (pole 1, 2 and 3)



U.PortoAAI Starting Point



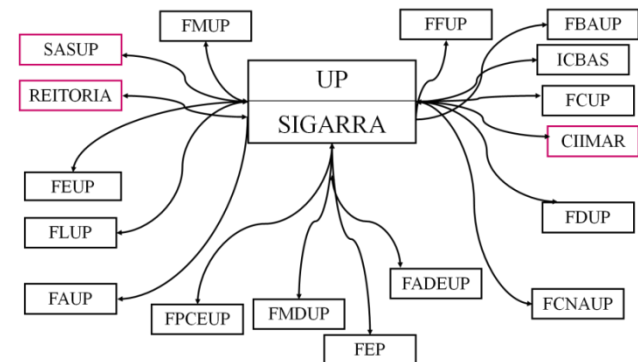
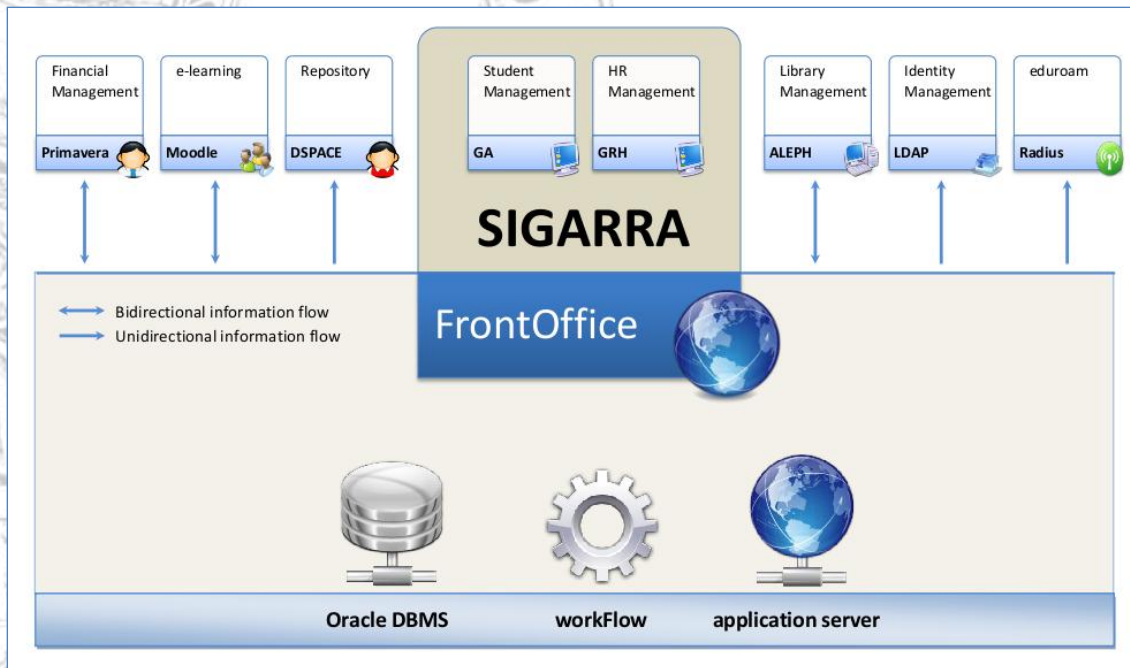
- **Reasons**

- lack of a **data repository** for local authentication
- **difficulty of managing credentials**
- distributed architecture needed (**geographic dispersion**)

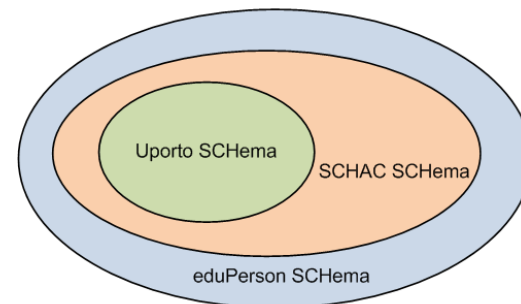
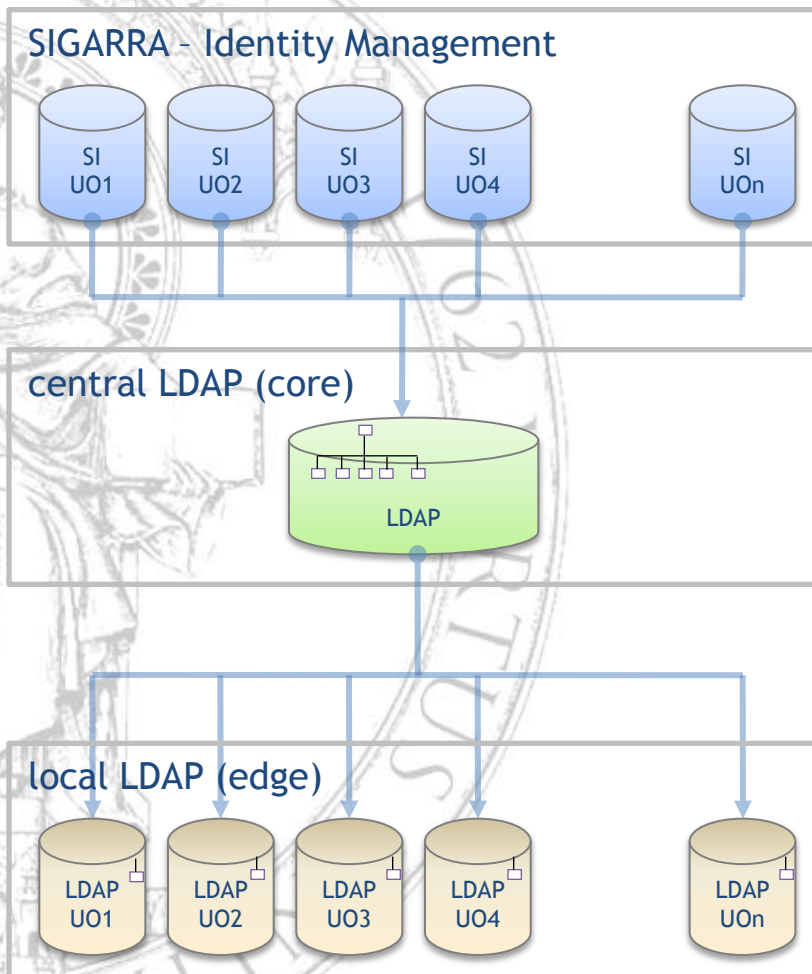
- **Initial vision**

- Information System (**SIGARRA**) “feeds” a central **LDAP (core)** with identities – 1 branch per faculty
- **Identity Management module in SIGARRA** with automated **synchronization with LDAP (core)**
- Central **LDAP (core)** “feeds” the local LDAPs (**edge** - faculties) with the respective faculty branch. Local services (mail, www) use this local LDAP
- Central **LDAP (core)** may be used for central services authentication (and/or allows **failover**)

- Information System of U.PORTO
 - 1 SIGARRA instance per Faculty, with their own identities
 - U.PORTO SIGARRA (aggregates information from the various SIGARRA)
 - independent authentication for each SIGARRA
 - Identity Management module



U.Porto AAI Project



ObjectClass	Description
person	see RFC 2256
organizationalPerson	see RFC 2256
inetOrgPerson	see RFC 2789
eduPerson	Developed by Internet2, Standard in Higher Education, with the highest incidence in the U.S
SCHAC	Terena TF-EMC2, SCHEMA for Academia.
UportoPerson	Created by the University of Porto with the aim of housing local attributes needs

Implementation



- Identity Management module – SIGARRA
 - Identities are in SIGARRA – back office (HR and GA)
 - Identities are exported from SIGARRA to LDAP core (automated)
- LDAP repository with U.Porto identities
 - LDAP core synchronized from SIGARRA
 - LDAP edge synchronized from LDAP core
- Identity Provider (IdP)
 - Analysis of IdP solutions (**Shibboleth** and **simpleSAMLphp**)
 - **Shibboleth** was selected
 - most used platform
 - easier attributes control
 - Shibboleth more difficult to learn
 - change layout and texts

U. PORTO aai
Infraestrutura de Autenticação e Autorização

U.PORTO Identity Provider

Requisitou o acesso a <https://sigarra.up.pt/shibboleth> que requer autenticação.
Insira o seu Utilizador e Senha e pressione o botão de login para continuar.

Utilizador:
Senha:

Remover aprovações

Introduza o utilizador no seguinte formato: utilizador@instituição.up.pt (ex: login@fep.up.pt)

Implementation



- Where Are You From (WAYF)
 - each **faculty may configure its own IdP**
 - central services
 - change layout and texts
- uApprove
 - Works in latest IdP release
- Service Provider (SP)
 - SIGARRA was the **first federated service**
 - Rebuild Shibboleth source to Apache 1.3 /Oracle AS/ RH 4
 - Keep redundancy of SP under ALTEON (SSL offload)
 - SIGARRA needed some adaptations (oracle PL/SQL)

U. PORTO aai
Infraestrutura de Autenticação e Autorização

Confirma os dados a serem enviados para 'sigarra.up.pt':

Digital ID Card	
edu:PersonAffiliation	member
affiliase	
edu:PersonPrimaryAffiliation	affiliate
edu:PersonOrg:InIDN	ouc:reit,ouc:up,c:pt
UPortoMec	420046
organizationalUnit	Reitoria da Universidade do Porto
Mail	safonso@reit.up.pt
CommonName	Sérgio Nuno Figueiredo da Cruz Afonso
Surname	Afonso
UPortoUser:Status	A
Organization	Universidade do Porto
GivenName	Sérgio

Não apresente novamente esta página. Concordo com o envio automático no futuro dos dados acima apresentados.

Cancelar Confirmar

U. PORTO aai
Infraestrutura de Autenticação e Autorização

Selecione a sua Organização de Origem

No sentido de aceder ao recurso em 'sigarra.up.pt' deverá autenticar-se.

Reitoria Seleccione

Selecione a sua Organização de Origem ...

- Faculdade de Ciências da Nutrição e Alimentação
- Faculdade de Arquitectura
- Serviços de Acção Social da Universidade do Porto
- Instituto de Ciências Biomédicas Abel Salazar
- Faculdade de Letras
- Faculdade de Medicina Dentária
- Faculdade de Engenharia
- Faculdade de Belas Artes
- Faculdade de Farmácia
- Faculdade de Psicologia e de Ciências da Educação
- Centro Interdisciplinar de Investigação Marinha e Ambiental
- Faculdade de Desporto
- Faculdade de Direito
- Faculdade de Economia
- Faculdade de Medicina
- Reitoria
- Faculdade de Ciências

Instant SSL Certificate Secured

Federated Services



- Information System (SIGARRA) – www.up.pt
- Thematic Repository (DSpace) – repositorio.up.pt
- Campus software – atlas.up.pt
- Learning Management System (Moodle) – ready to production
- Library System (ALEPH) - testing phase
- Already integrated with the national federation RCTSaaITCS
www.rctsaai.fccn.pt/RCTSaaI/SERVICOS-federados2.php
 - ARARA
 - COLIBRI
 - TCS
 - B-ON
 - Filesender
 - DreamSpark
 - Terena.org

Results



- Access Stats (since March 2010)

```
# ./stats.sh

18 unique relying parties
2288 unique userids
22194 logins

logins      | relyingPartyId
-----|-----
19          | https://wiki.finesource.eu
6163       | https://www.fe.up.pt
9          | https://filesender.fccn.pt/simplesaml/module.php/saml/sp/metadata.php/default-sp
2          | http://shibboleth.metapress.com/shibboleth-sp
4          | https://www.annualreviews.org/shibboleth
376        | https://www.arara.pt
13967      | https://sigarra.up.pt/shibboleth
721        | https://atlas.up.pt/shibboleth
2          | https://sp.tshhosting.com/shibboleth
28         | https://repositorio-dev.up.pt/shibboleth
7          | https://scauth.scopus.com/
233        | https://cast.fccn.pt/shibboleth
5          | https://elearning.ul.pt
125        | https://tcs.fccn.pt
268        | https://repositorio-tematico.up.pt/shibboleth
175        | https://webconference.fccn.pt/shibboleth
51         | https://downloads.channel8.msdn.com/shibboleth-sp
50         | https://sdauth.sciencedirect.com/
```

- Users feedback

- The lack of **global-logout** option causes concern

Limitations and Future Work



- R&D Institutes without SIGARRA

- **Problem:**

- Almost all R&D Institutes have their own IS different from SIGARRA. Their identities do not exist in LDAP core.

- **Solution :**

- H 1: R&D institute must have local LDAP -> replication to central LDAP central -> use central IdP
 - H 2: R&D institute must have local LDAP -> sets IdP local -> integrates in UPORTOaai (wayf)

- SIGARRA Authentication to users outside of U. PORTO

- **Problem:**

- To allow users from other Universities, with federated authentication, to access SIGARRA

- **Solution :**

- Integration / revision of SIGARRA to use RCTSaai federation (Portuguese NREN)



SECURE IDENTITY ACROSS BORDERS LINKED PROJECT

- National e-ID card
- Implemented only in SIGARRA service
- Future **integration with IdP** to be used on federated services

	DE - Deutschland
	EE - Eesti
	ES - España
	IS - Ísland
	LU - Luxembourg
	PT - Portugal
	SI - Slovenija
	FI - Suomi
	SE - Sverige

Technical implementation



- IdP Architecture
- Discovery Service
- IdP Failover
- Monitoring and Statistics
- SP ATLAS
- SP Thematic Repository

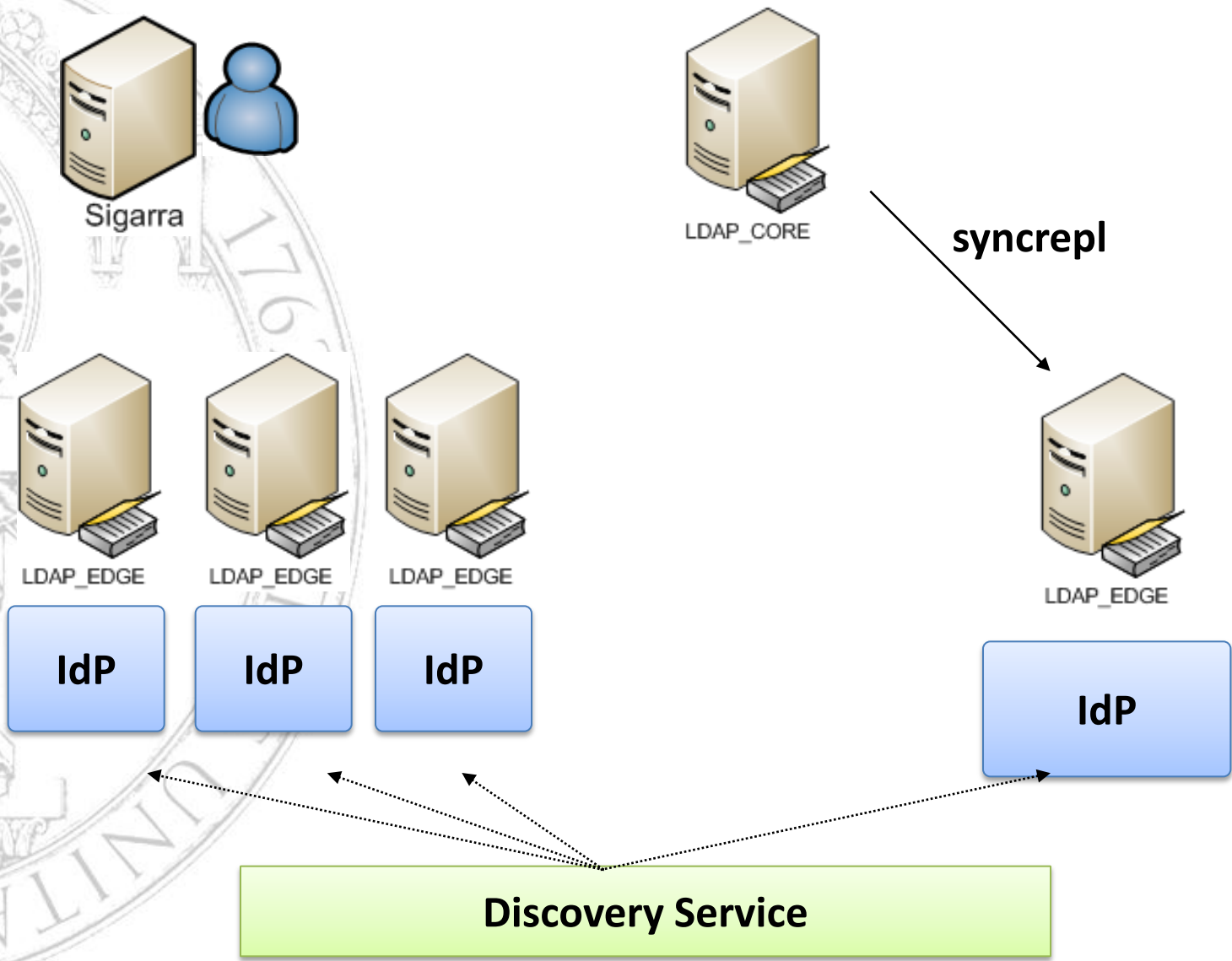
IdP Architecture



100

U. PORTO

UNIVERSIDADE DO PORTO



IdP Architecture



- In the initial architecture each organizational unit would have their own data repository (LDAP server) and IDP.
- This configuration would make the existence of at least 14 IDP's in the starting phase of the project.
- The inclusion of this list in the National Federation (RCTSaai) would become a problem, not only for the Federation management but also for the users itself.
- The solution was to create a local Discovery Service (WAYF)

Discovery Service



- The present WAYF implementation is the one developed by SWITCH with some local changes.

More information at: <http://www.switch.ch/aai/support/tools/wayf.html>

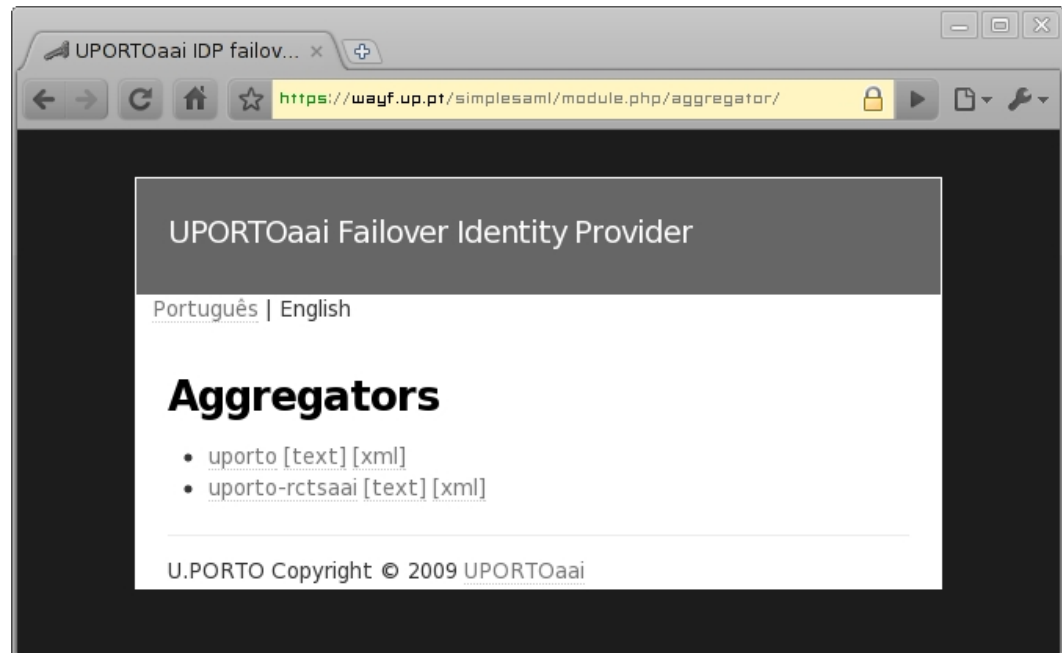
- Our modification allows to dynamically change the list of IDPs according to their state and use the failover IdP in case of need.



Discovery Service



- Although users have to make an additional step by choosing their local institution, this configuration gives some flexibility in the management of Federated Services and IdPs.
- We also configured a Metadata aggregator in this component, which allows to have several profiles according to future needs.
- This aggregator is implemented as a plug-in in SimpleSAMLphp framework



IdP HA/Failover



- We estimate a large number of authentications due to the high number of users at U.PORTO and the shibbolization of new services.
- This increases the reliability of the architecture, which lead us to have some HA or Failover mechanisms.

... so we start by checking the IdP states.

IdP HA/Failover



- Check IDP state (Shibboleth 2.1.5)
- Handler /Status

```
<ProfileHandler xsi:type="Status">  
  <RequestPath>/Status</RequestPath>  
</ProfileHandler>
```

Using this servlet it's possible to obtain a string with the IdP state

```
https://{IDP}/idp/profile/Status
```

IdP HA/Failover



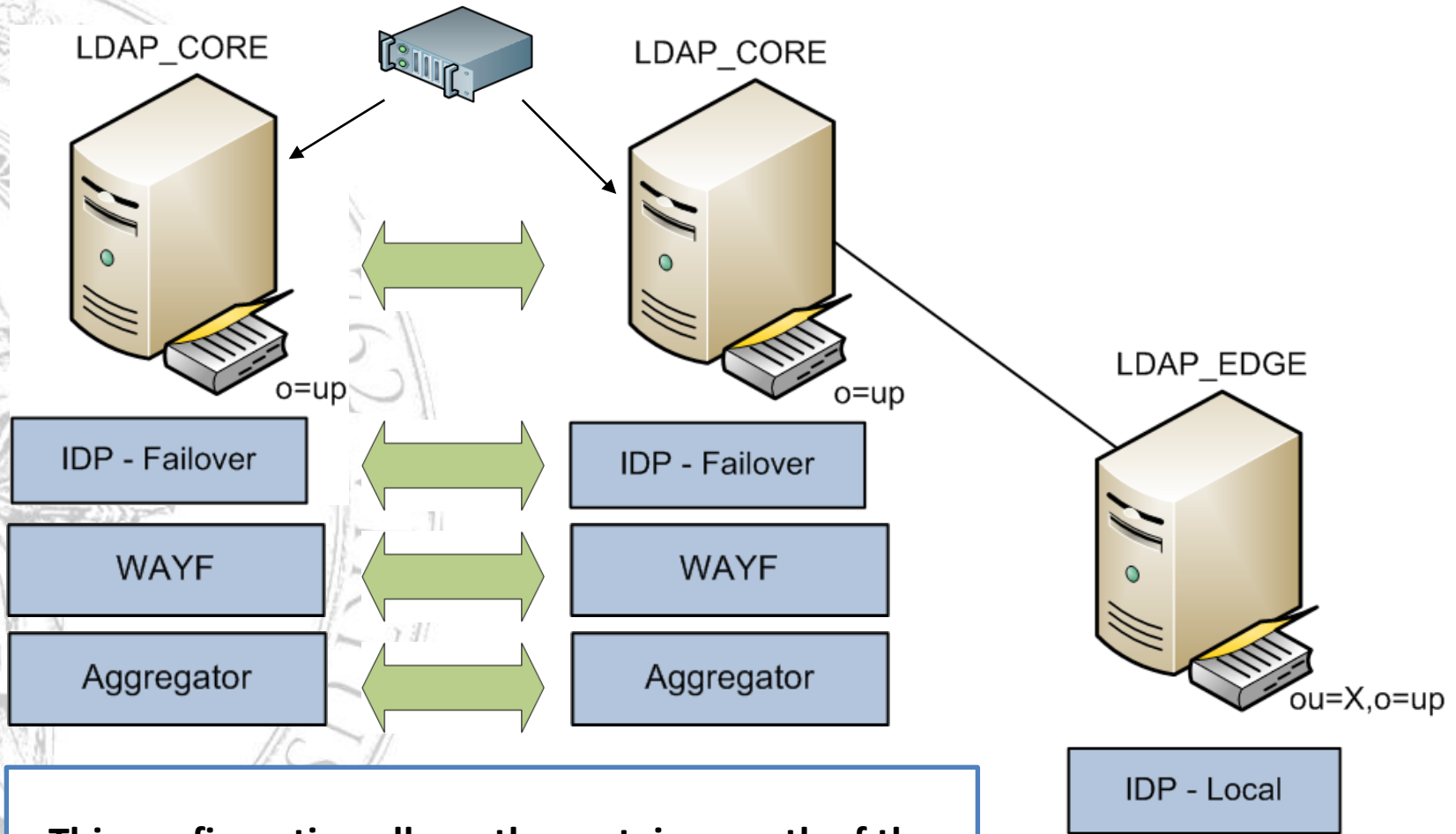
- We created a perl script `getstatus.pl` which is executed via cron and registers to a local file the several IdP states.

```
fcnaup https://aai.fcna.up.pt/idp/shibboleth fail
faup https://aai.fa.up.pt/idp/shibboleth fail
icbas https://aai.icbas.up.pt/idp/shibboleth fail
flup https://aai.fl.up.pt/idp/shibboleth fail
...
fep https://aai.fep.up.pt/idp/shibboleth fail
fmup https://aai.fm.up.pt/idp/shibboleth fail
reit https://aai.reit.up.pt/idp/shibboleth ok
fcup https://aai.fc.up.pt/idp/shibboleth fail
```

- We changed the WAYF code so that it takes into account this file and change the selection dropbox value to use the Failover IdP.

```
...
<option value="https://wayf.up.pt/idp/shibboleth">Faculdade de Economia</option>
<option value="https://wayf.up.pt/idp/shibboleth">Faculdade de Medicina</option>
<option value="https://aai.reit.up.pt/idp/shibboleth">Reitoria</option>
...
```

IdP HA/Failover



This configuration allows the sustain growth of the infrastructure ensuring the availability of services as local deployments are being made.

IdP HA/Failover

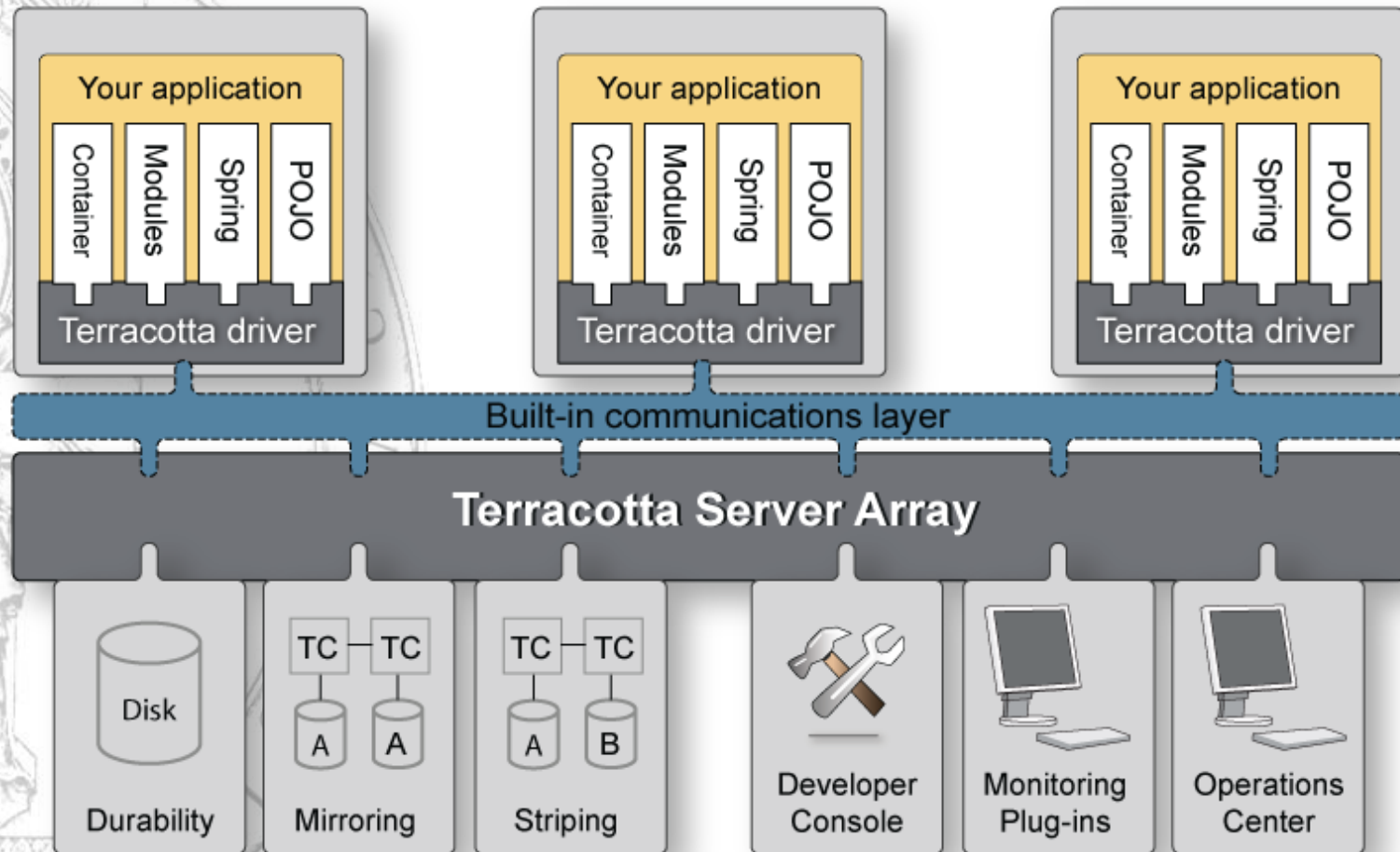


U. PORTO

UNIVERSIDADE
DO PORTO

- We synchronize the LDAP directories in mirror-mode using OpenLDAP syncrepl mechanism
- This requires version 2.4 in order for mirror-mode to work
- The Discovery Service and Aggregator are synchronized between host using rsync
- The Identity Providers much share a common space for session management, we used Terracotta for that purpose

IdP HA/Failover



Monitoring and Statistics



- IdP centralized logging (IDP_AUDIT)
- Regular expression rule at the Central Logging system
- Capture expressions are written to a Relation Database
- This allow us to have authentication statistics from the several Identity Providers
- Nagios checks for the several services

- Software Service for the U.PORTO community
- Access control by IP and user access list
- Configured Apache Federated access to a <Directory> directive with access control
- Identity Provider releases attribute SoftwareRoles with user profiles (ex: REIT,REIT-CT,UPORTO)

```
# REITORIA
<LocationMatch /Software/REITORIA/*>
  AuthType shibboleth
  ShibRequireSession On
  ShibRequestSetting redirectToSSL 443
  require SoftwareRoles REITORIA
  require SoftwareRoles Administrator
</LocationMatch>
```

SP Thematic Repository



- Dspace platform (version 1.6)
- Shibboleth authentication activated
- Created DspaceRoles attribute of type 'script'

```
...  
// ALFA users  
if ( UPortoNEE.getValues().get(0).equals("1")) {  
    DSpaceRoles.getValues().add("ALFA");  
}  
  
// BDart Admin and BDart Submit  
  
// Isabel Barroso - BDart Administrator - UPortoNMec: 123456  
  
if (UPortoNMec.getValues().get(0).equals("123456")) {  
    DSpaceRoles.getValues().add("BDART_ADMIN");  
}  
...  

```

Questions



100

U. PORTO

UNIVERSIDADE
DO PORTO



Thank you for your attention!