

The role of authentication and eID interoperability in the access to scientific databases

Fernando M. Silva
Instituto Superior Técnico
Lisboa, Portugal



13-14 November 2013, UP

Outline

- About Técnico Lisboa
- Access to scientific resources
- Authentication and eID
- eID interoperability
 - ID Federations
 - National eID
 - European developments on eID interoperability
 - Academic and research eID interoperability
- Authentication infrastructure at Técnico Lisboa
- Future trends and challenges

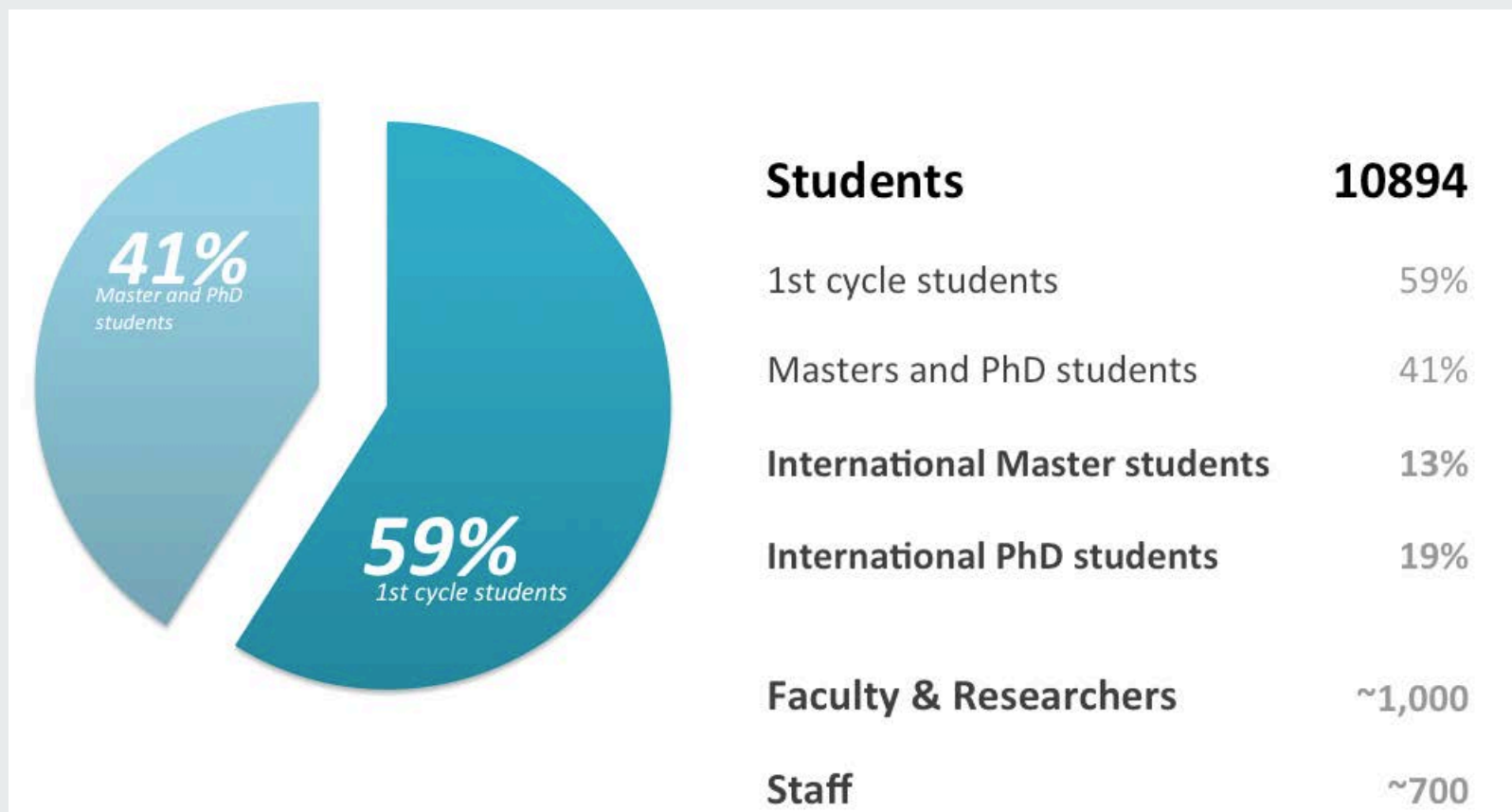


TÉCNICO LISBOA

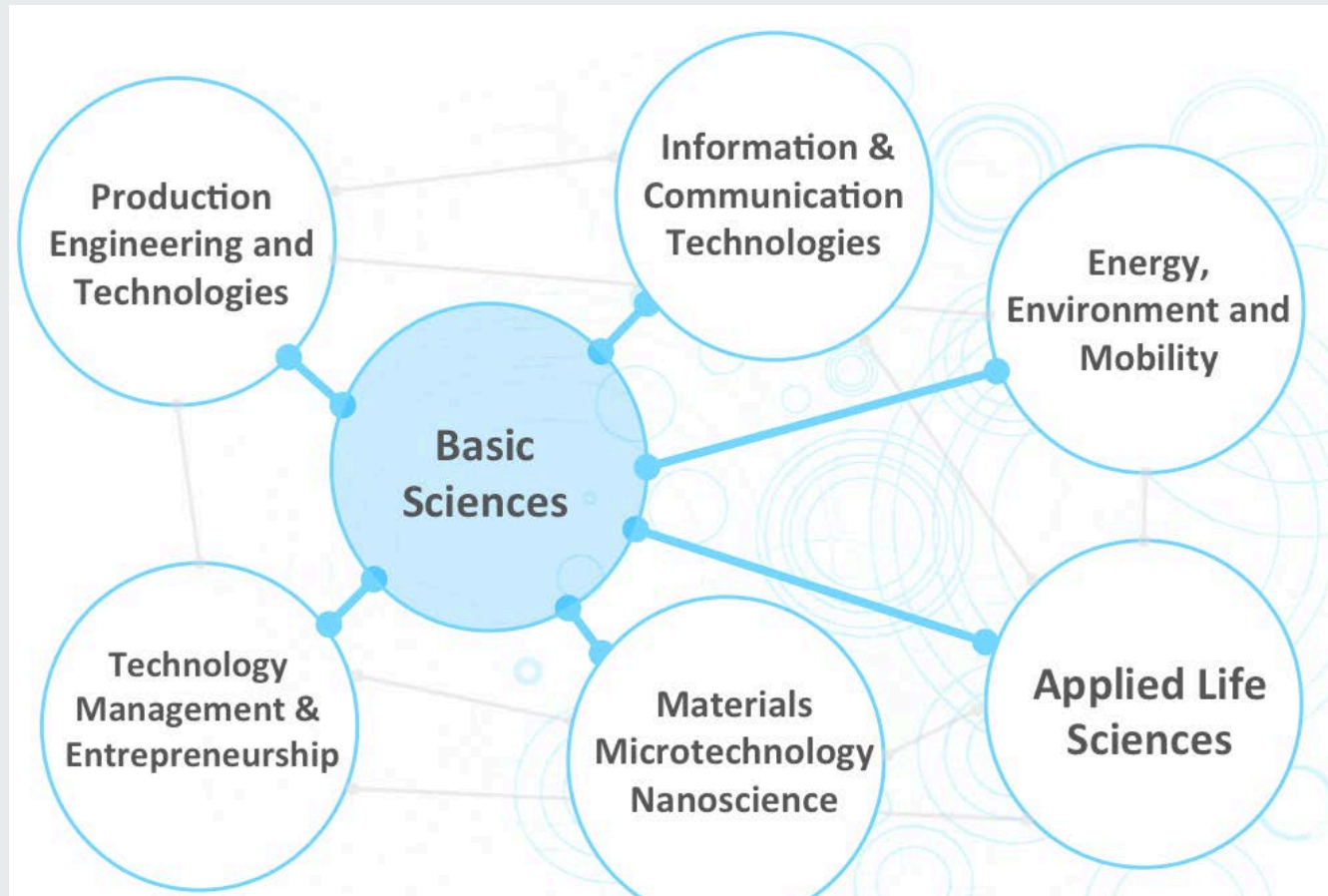
About Técnico Lisboa



Facts & Figures



Research & education areas



Graduate programmes

- Bioengineering and Nanosystems
- Biotechnology
- Chemistry
- Complex Transport Infrastructure Systems (w/ MIT)
- Computer Science and Engineering
- Construction and Rehabilitation
- Information Systems and Computer Engineering
- Materials Engineering
- Mathematics and Applications
- Mining and Geological Engineering
- Naval Architecture and Marine Engineering
- Pharmaceutical Engineering
- Structural Engineering
- Territorial Engineering
- Transport Infrastructure Engineering
- Transport Planning and Operation
- Urban Studies and Territorial Management
- Communication Networks Engineering
- Electronics Engineering
- Engineering and Industrial Management
- Information Systems and Computer Engineering
- **Aerospace Engineering**
- **Architecture**
- **Biological Engineering**
- **Biomedical Engineering**
- **Biomedical Technologies**
- **Chemical Engineering**
- **Civil Engineering**
- **Electrical and Computer Engineering**
- **Engineering and Water Management**
- **Environmental Engineering**
- **Mechanical Engineering**
- **Petroleum Engineering**
- **Technological Physics Engineering**

Doctoral programmes

- Aerospace Engineering
- Architecture
- Bioengineering
- Biomedical Engineering
- Biotechnology
- Chemical Engineering
- Chemistry
- Civil Engineering
- Climate Changes and Sustainable Development Policy
- Computational Engineering
- Computer Science and Engineering
- Electrical and Computer Engineering
- Engineering and Management
- Engineering and Public Policy
- Environmental Engineering
- Geo-Resources
- Information Security
- Information Systems and Computer Engineering
- Leaders for the Technical Industries
- Materials Engineering
- Mathematics
- Mechanical Engineering
- Naval Architecture and Marine Engineering
- Physics
- Refining, Petrochemical and Chemical Engineering
- River Restoration and Management
- Statistics and Stochastic Processes
- Sustainable Energy Systems
- Technological Change and Entrepreneurship
- Technological Physics Engineering
- Territorial Engineering
- Transportation



Access to scientific resources

- Open data is a standard approach for delivering and publishing scientific data

– **Open data**
+
– **Open source**
+
– **Open access**



**Open
knowledge**

Authenticated access

- User authentication is still required in the access to scientific resources in many real case scenarios
 - Legal constraints
 - Authorization constraints
 - Access auditing and monitoring
 - Other practical or functional reasons
 - Mandatory registration
 - ...

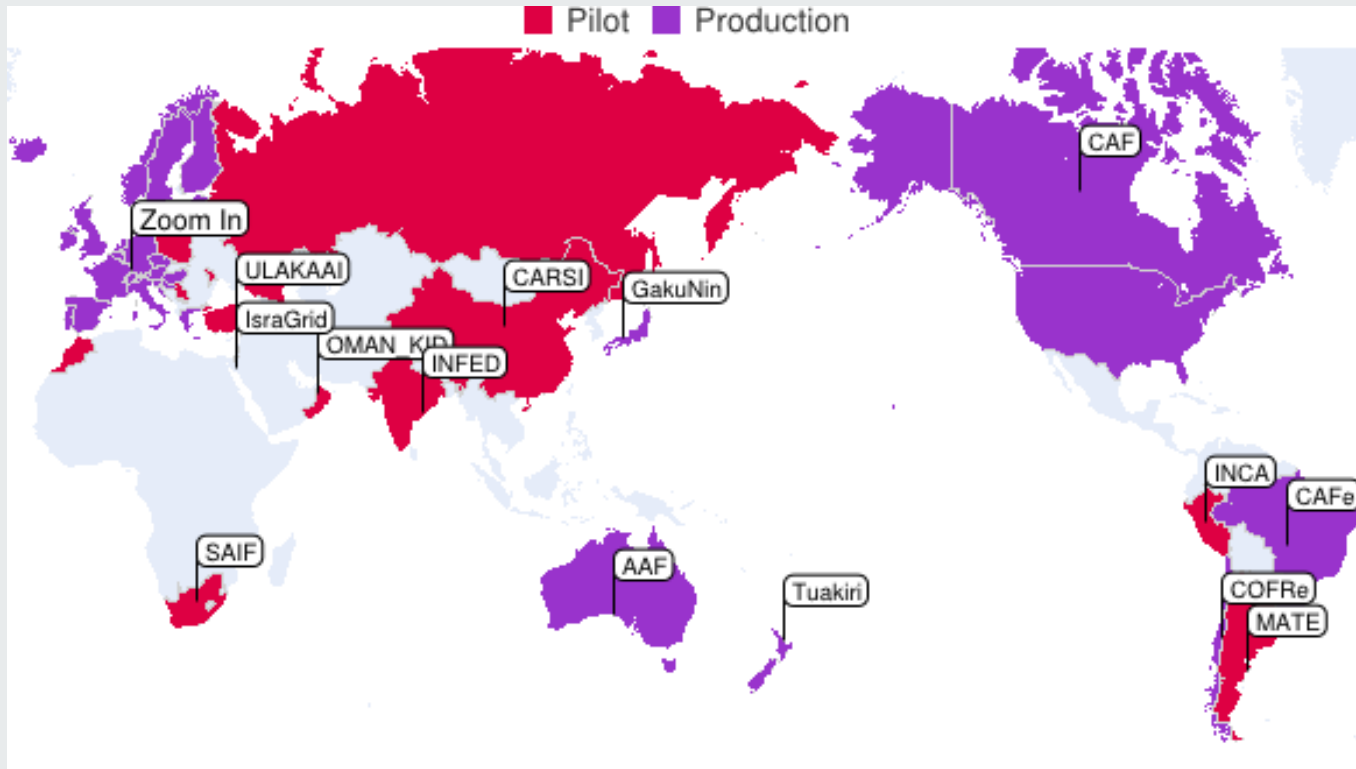
When registration / authentication is required

- Internal/institutional users
 - Internal users may usually provide a fairly strong authentication by providing local access credentials
- External users
 - In many real cases scenarios, a simple user registration is required in order to increase the confidence and user id reliability on data access
 - User registration is often performed adopting a simple e-mail authentication
 - Of course, e-mail authentication provides a quite “weak” user authentication for auditing and legal purposes.

Federated identity management

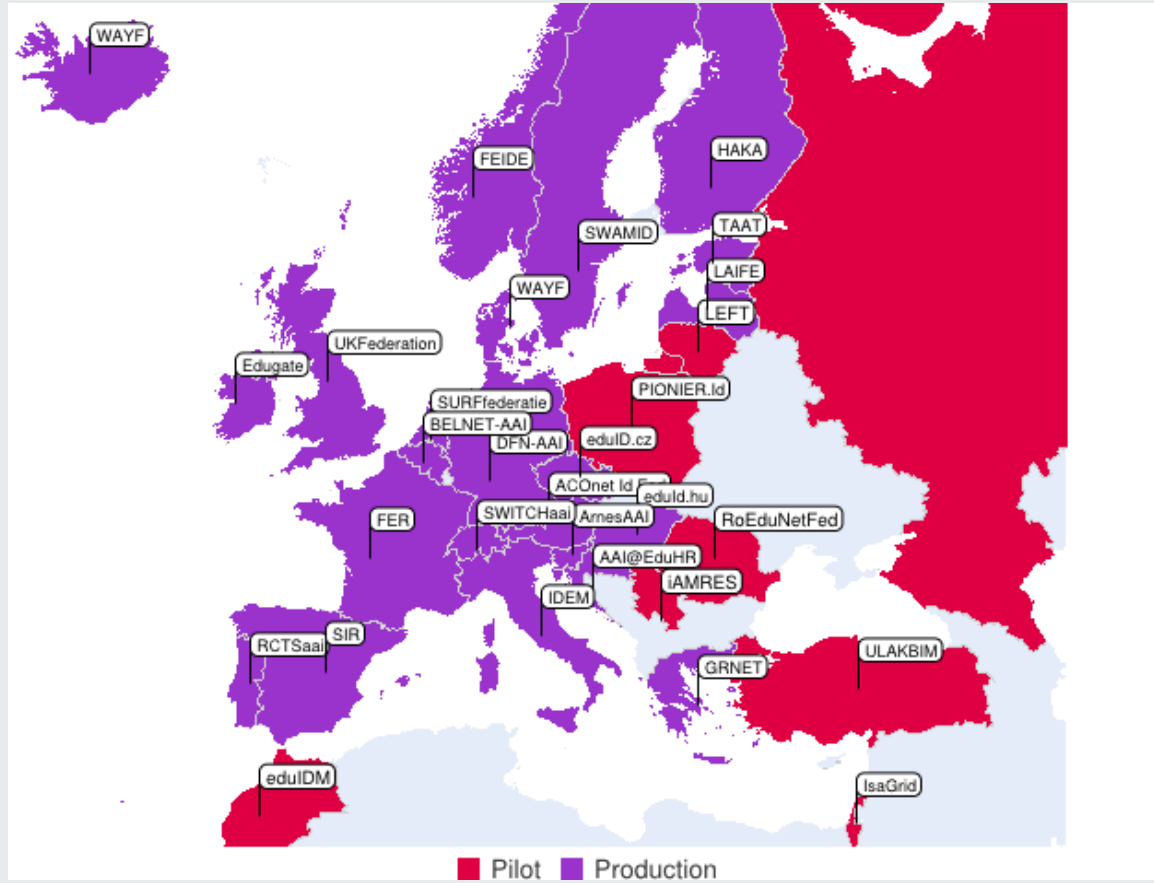
- Solution for providing user authentication and access across organizations
- Common practice in academic and scientific organizations
 - Infrastructures mostly built around SAML and associated technologies
- Further to provide cross organization authentication, identity federation are an excellent solution for providing authenticated services to *userless* organizations
 - NREN services
 - Portugal: RCTSaaI identity federation

Research and education ID federations



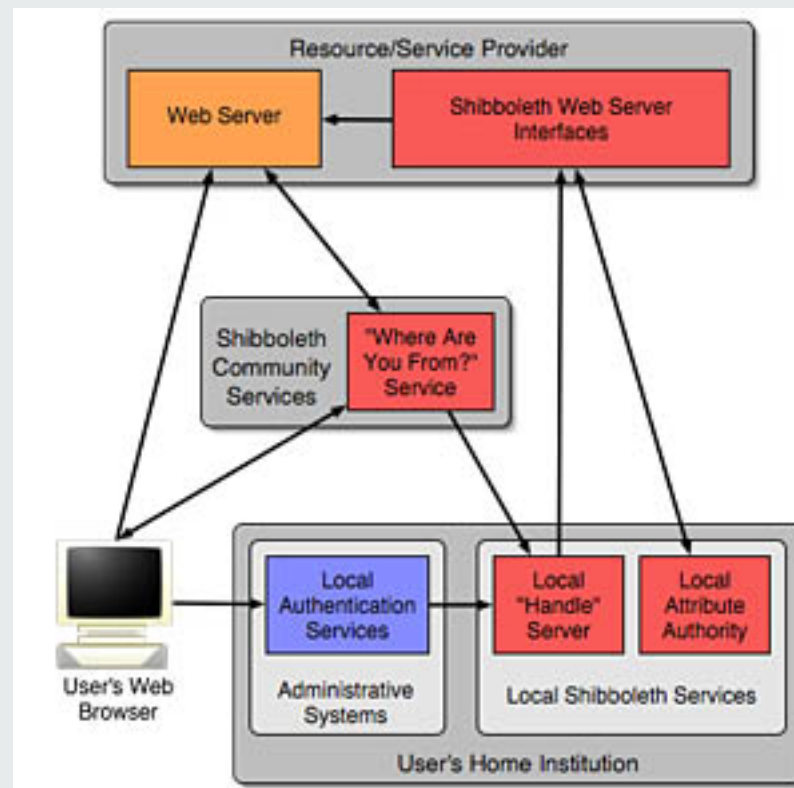
Source: *refeds.org*

Research and education ID federations in Europe



Source: refeds.org

Shibboleth authentication and authorization model



eID authentication: going national

- In the last few years, many countries started the integration of eID in national identity ID cards
 - National eID systems may be a convenient source of user authentication and authorization in several scenarios
 - Reliable underlying user authentication process
 - Strong authentication through physical security tokens
 - Support of broader authentication scenarios
 - Conventional eID federations (e. g., academic) are domain specific

National eID interoperability

- eID interoperability is a major pre-condition for the delivery of cross borders e-services
- The EU has been promoting eID interoperability in several LSP projects addressing authentication and cross border services



EU LSPs for promoting cross border services



Cross-Border
procedures



e-health



e-justice



e-procurement

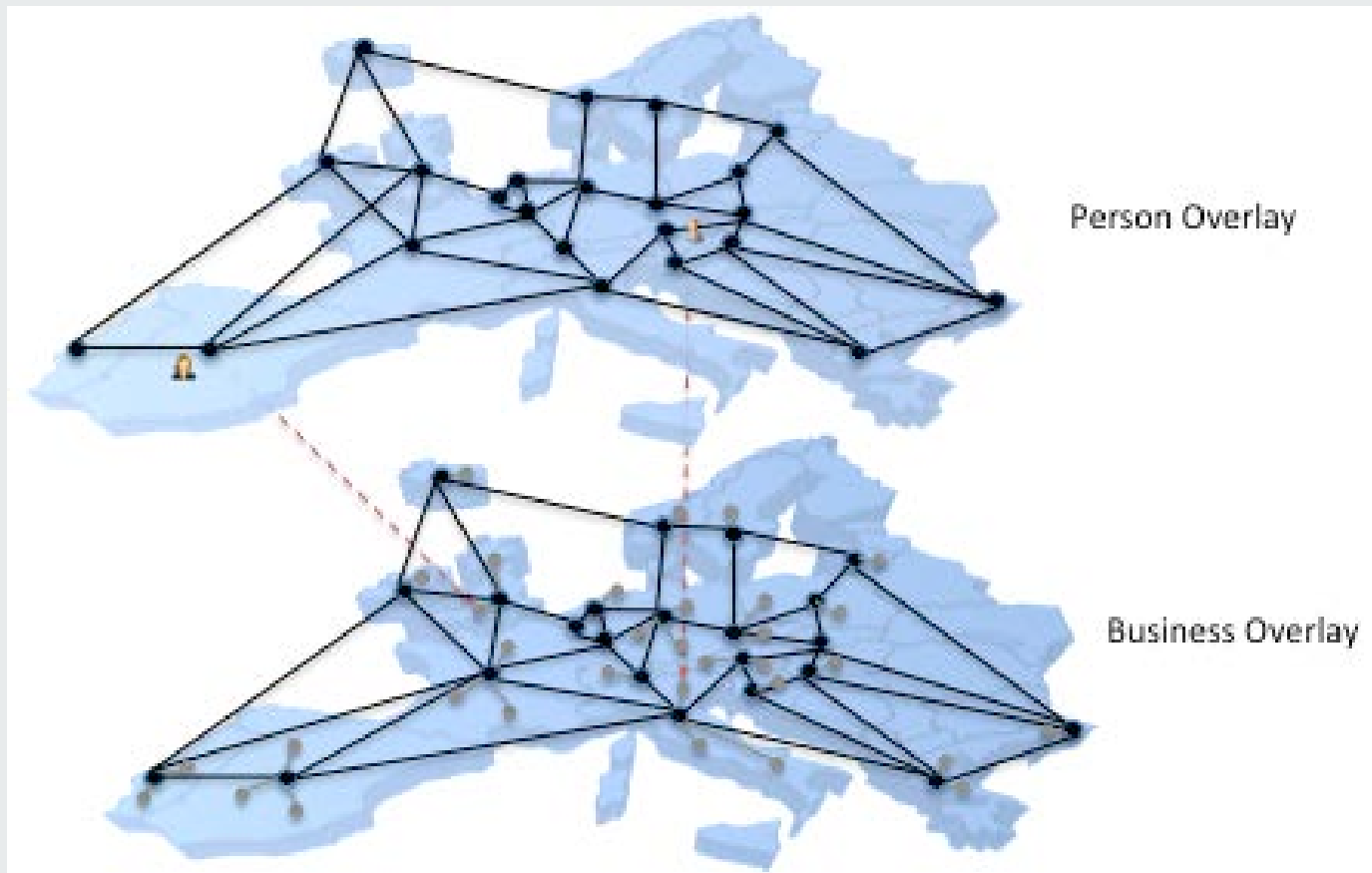


eID Authentication,
mandates &
representation

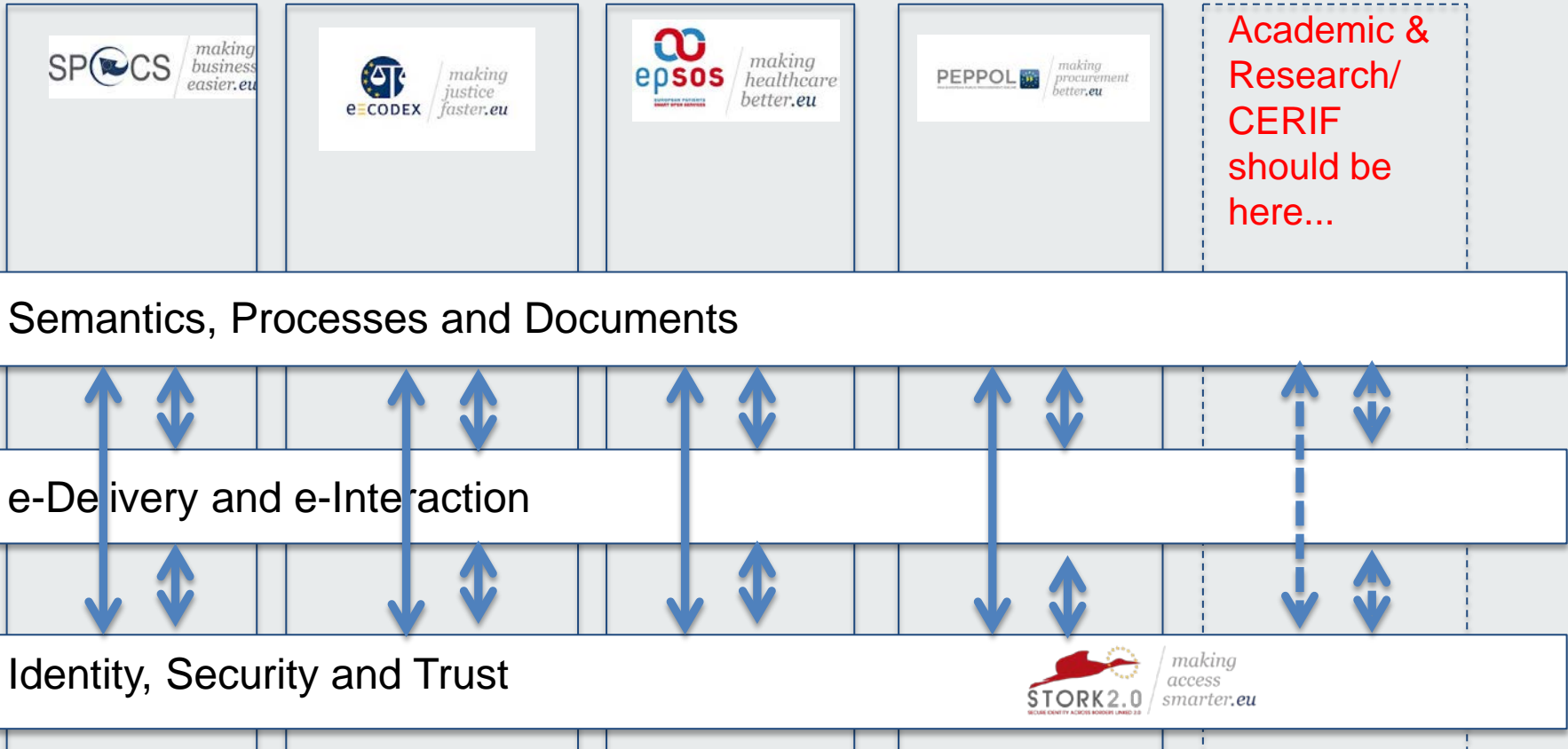


*moving
services
forward.eu*

Generic view of coupling of eLD and LSPs



Academic and research area in last LSP... is missing

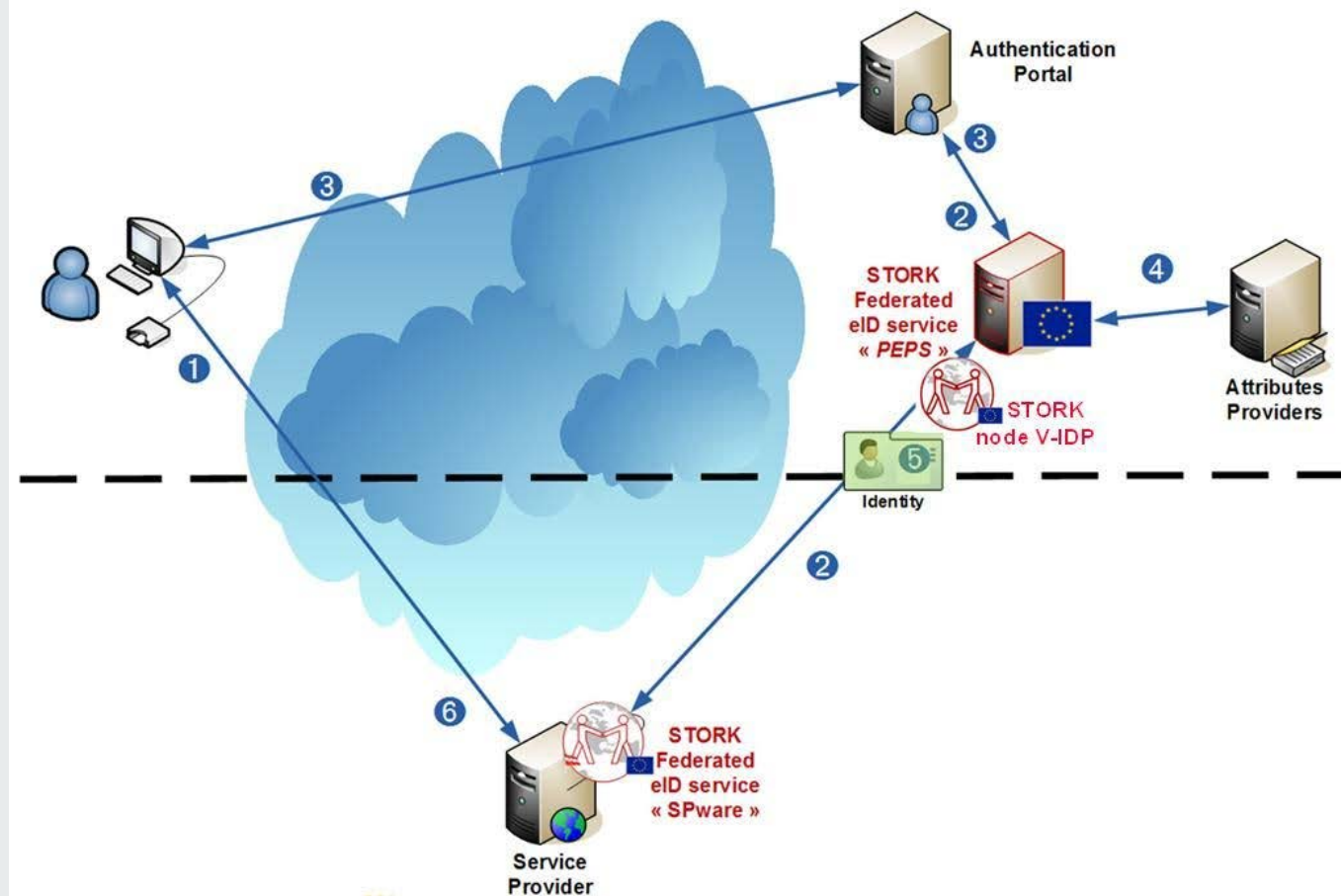


Stork 2.0 authentication model

Stork project



- eID integration and interoperability
- Implementation of a proxy service (PEPS) in each member state
- Optional support of a V-IdP for distributed solutions



Authentication model at Técnico Lisboa

Single IdP infrastructure for all ICT services:

- Academic information services
- Mail
- VoIP
- ERP systems
- Procurement services
- WiFi (eduroam) access
- CPU resources
- Storage resources
- Web services
- Desktop access
- ...



eID building blocks

Local authentication infrastructure

LDAP (OpenLDAP)

Authentication backend: Kerberos

RADIUS (FreeRadius)

Single Sign-On (SSO) support

Central Authentication Service (Yale University)

ID federation support

Shibollet, OpenSAML - National Academic federation RCTSaai, FCCN

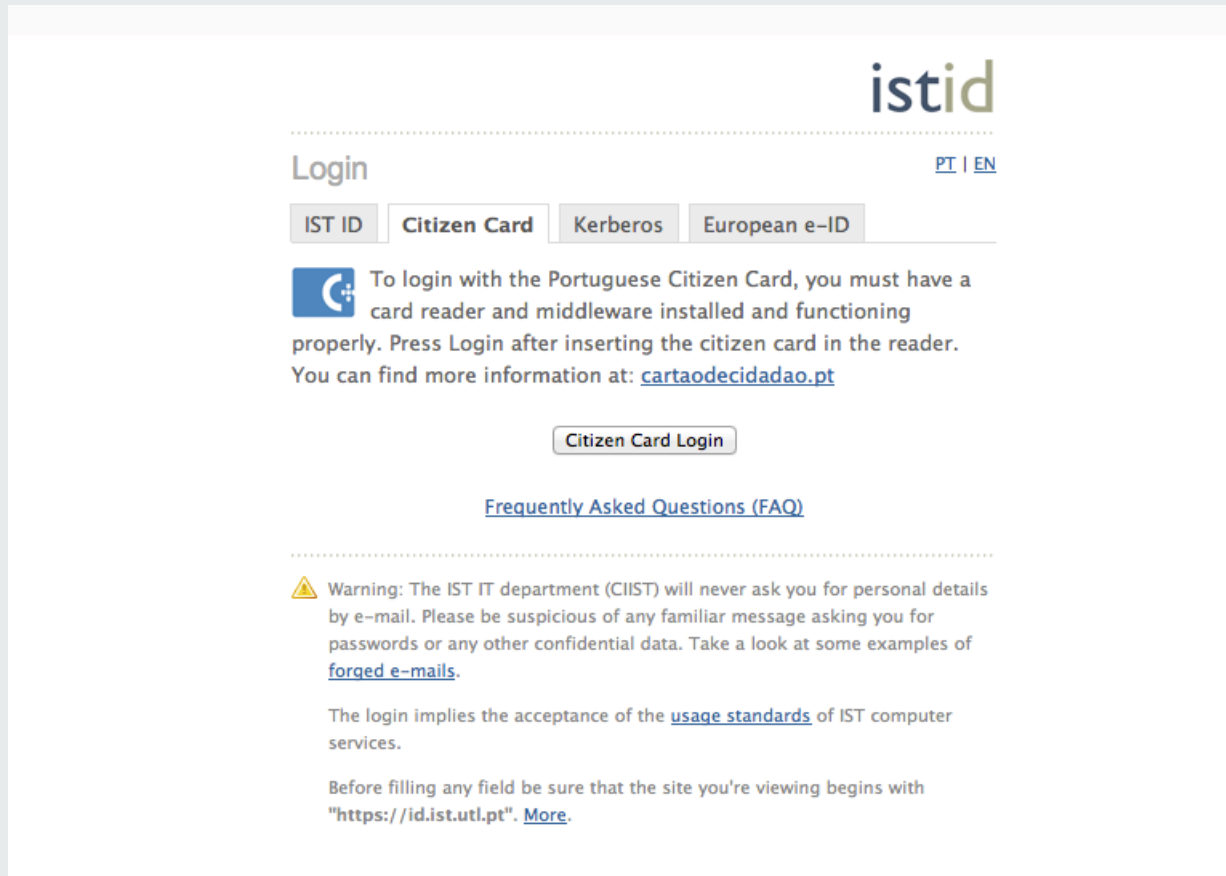
RADIUS – Eduroam access (FCCN / TERENA)

National eID support (*cartão de cidadão*)

Support of eID interoperability platform

STORK, Stork 2.0 eSENS

SSO login




The screenshot shows the istid login page. At the top right is the 'istid' logo. Below it is a 'Login' section with a language selector 'PT | EN'. There are four tabs: 'IST ID', 'Citizen Card', 'Kerberos', and 'European e-ID'. The 'Citizen Card' tab is selected. Below the tabs is a blue icon of a citizen card and a text block explaining that a card reader and middleware are required. A 'Citizen Card Login' button is centered below the text. Further down is a 'Frequently Asked Questions (FAQ)' link. At the bottom, there is a warning icon and text about not sharing personal details via email, and a note about accepting usage standards and the required URL.

istid


Login [PT](#) | [EN](#)

IST ID Citizen Card Kerberos European e-ID

 To login with the Portuguese Citizen Card, you must have a card reader and middleware installed and functioning properly. Press Login after inserting the citizen card in the reader. You can find more information at: cartaodecidadao.pt

[Citizen Card Login](#)

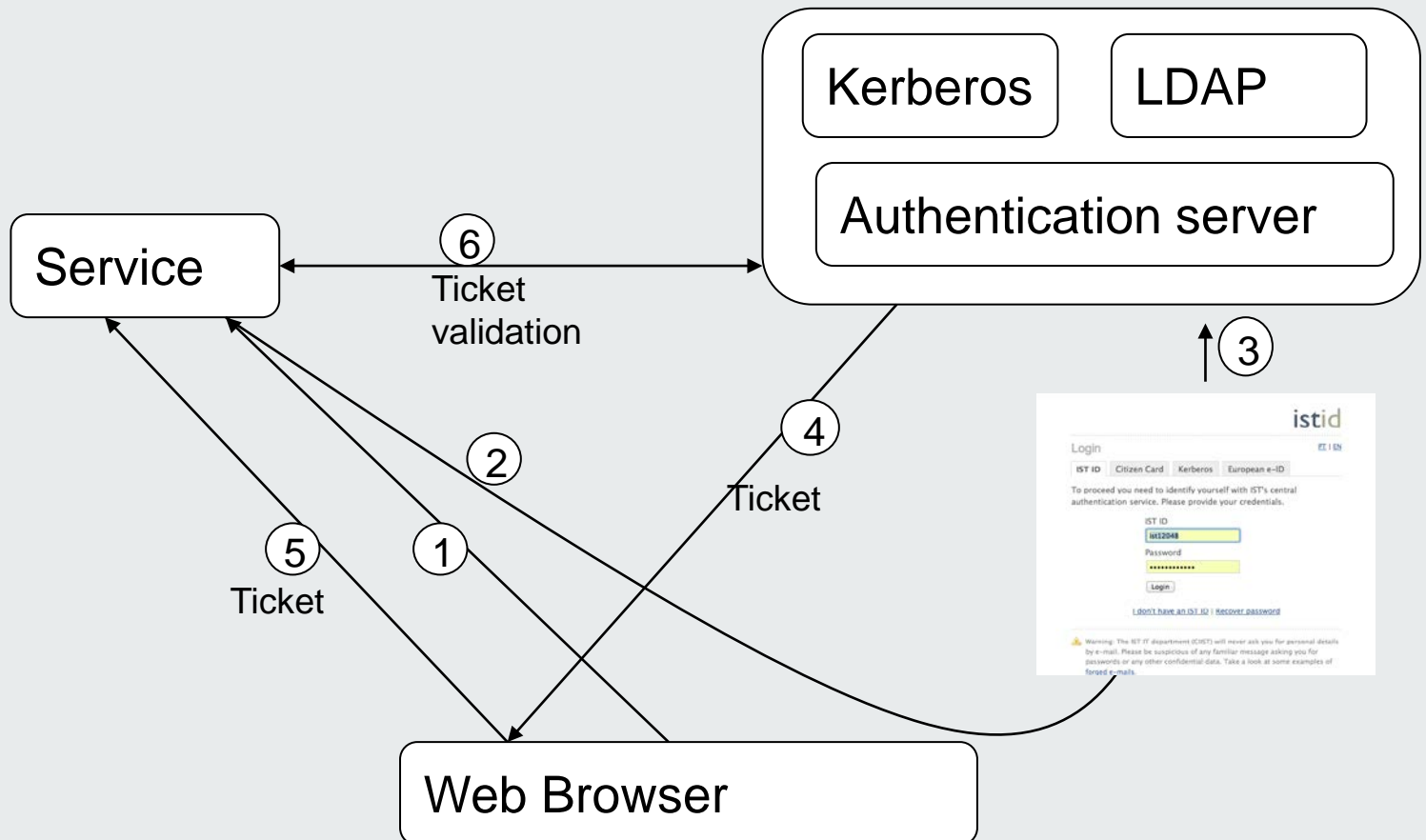
[Frequently Asked Questions \(FAQ\)](#)

 Warning: The IST IT department (CIIST) will never ask you for personal details by e-mail. Please be suspicious of any familiar message asking you for passwords or any other confidential data. Take a look at some examples of [forced e-mails](#).

The login implies the acceptance of the [usage standards](#) of IST computer services.

Before filling any field be sure that the site you're viewing begins with "https://id.ist.utl.pt". [More](#).

SSO: CAS model



Client implementation: authentication request

Case 1: PHP code

```
<?php
  include_once('CAS/CAS.php');
  phpCAS::client(CAS_VERSION_2_0,'id.ist.utl.pt',443,'cas');
  phpCAS::forceAuthentication(); // Force authentication: browser redirected to IdP IF not authenticated
// If the code reaches this step, the user has already been authenticated by the CAS server
  $user = phpCas::getUser();

//   [Specific server processing]

  phpCAS::logout(); // Logout
?>
```

Case 2: mod_auth_cas installed on apache server

Fill the .htaccess in selected directories

```
AuthType CAS
AuthName "IST Network Services"
require user
```

Conclusions

- Authenticated access to scientific resources by external users can be easily provided by eID federations
 - Complexity is often hidden to the client process;
 - National eID systems offer a general purpose powerful authentication infrastructure
 - European eID authentication is already made possible by existing tools and infrastructures.
- Extension of cross border services in European LSPs must be extended to research & academic domains.
 - Active promotion required...

Thank you for your attention