CERN openlab

# 1000 things you always want to know about SSO but you never dare to ask

*6th Control System Cyber-Security Workshop (CS)2/HEP*

Luis Rodríguez Fernández

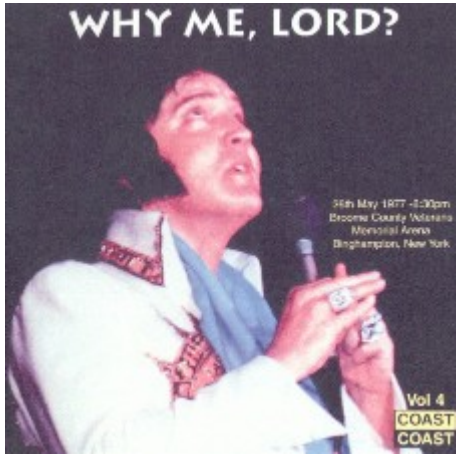
08/10/2017

# Agenda

Why me?
SSO. Why?
SSO. How?
Conclusions

# Agenda

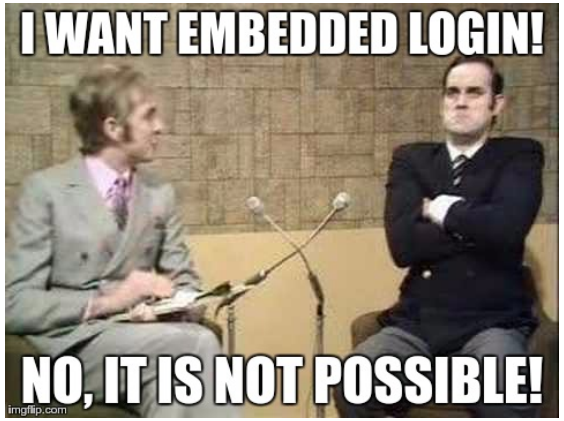
## Why me?

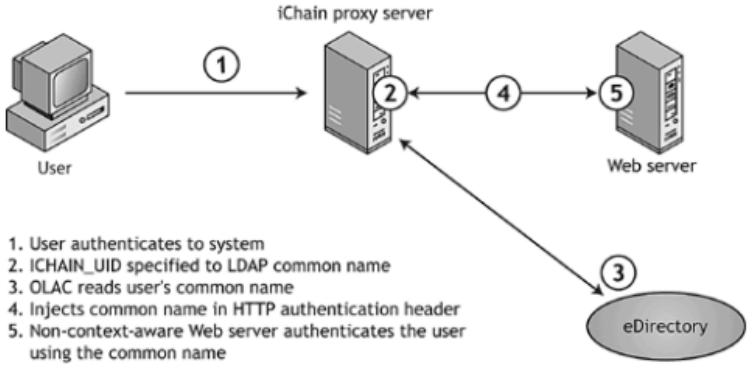


# Why me?

http://www.asturias.es
Vignette portal suite
SSO solution: **Novell iChain**
Problem:
- Information Architecture rules!
- Login form embedded home page
- iChain redirects to its on login page
- User eXperience degraded!
- Infinite discussions...

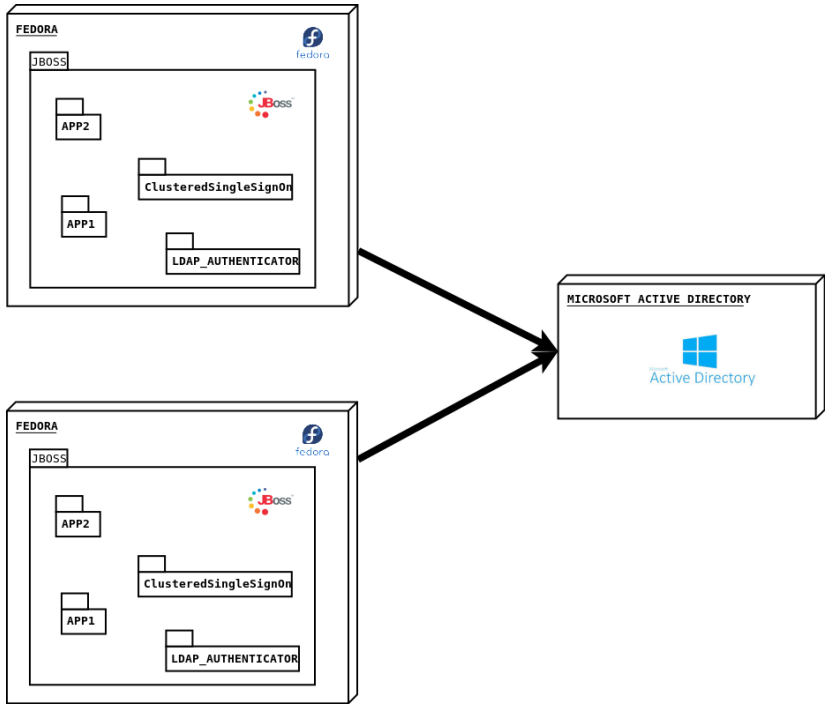
Lesson learned:
- Check the specs first!

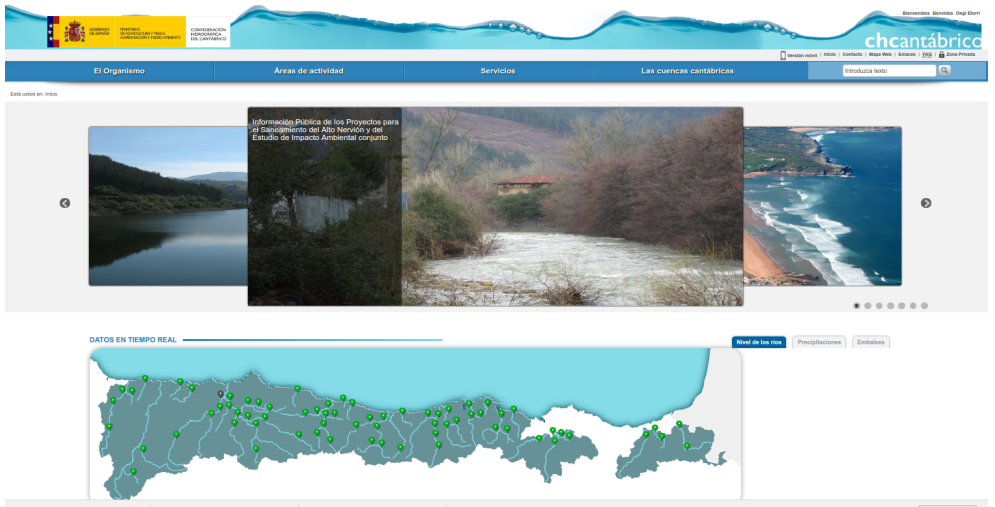



# Why me?

JBOSS Application Server
Different application context same cluster
**ClusteredSingleSignOn**
LDAP_Authenticator
Lesson learned:
  Keep it simple



# Why me?

Liferay Portal
Alfresco Content Management System
Mantis Bugtracker
**Central Authentication Server**
Lesson learned:
  Opensource works!




# Why me?

CERN Oracle WebLogic Applications

**Built-in SAML2 module**

Challenges:

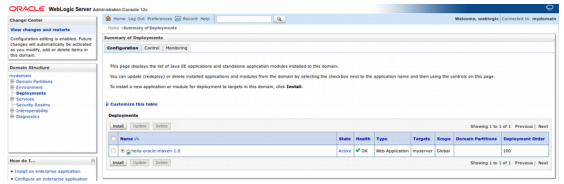
- Oracle Documentation
- Oracle Support
- Automate the setup
- Legacy

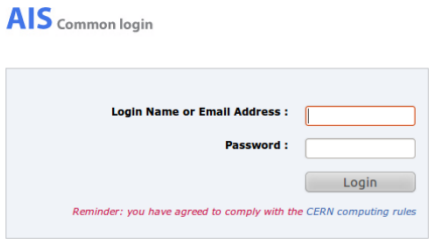
Lesson learned:

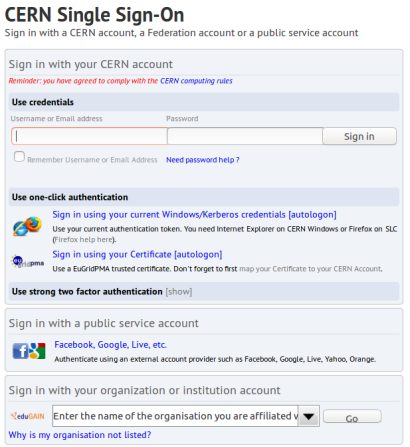
- Share your knowledge!

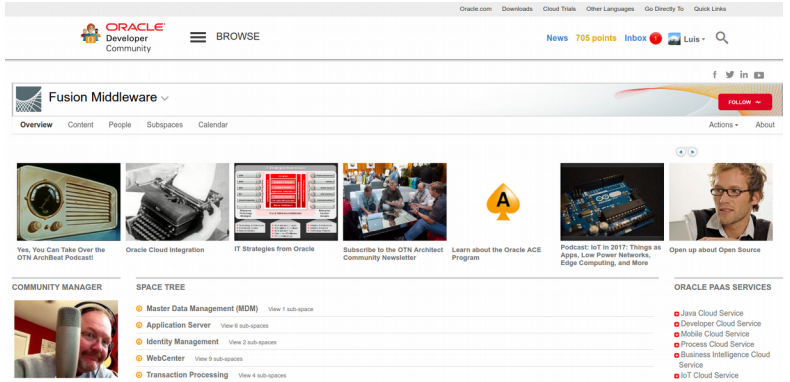
{ REST }

Jython



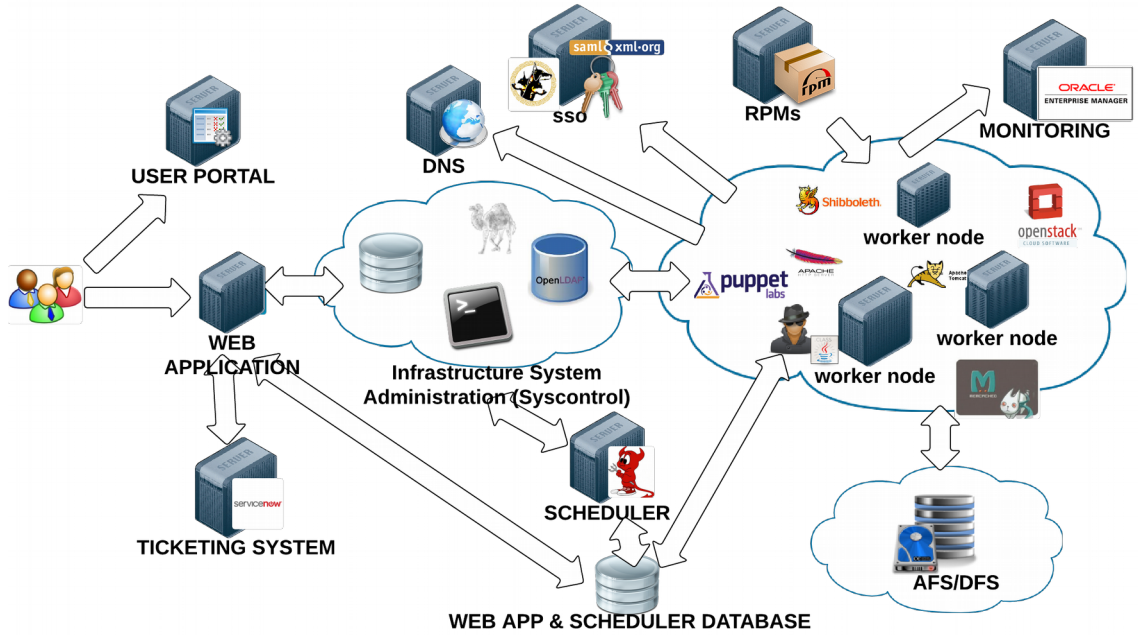


# Why me?

Java Web Hosting Service aka MWOD
PaaS
  Apache Tomcat as a Service
Stopped 04/10/2017
  Replace by openshift
**Shibboleth**
  Used by many other CERN IT Services
Lesson learned:
  Trust your IT!




# Why me?

CERN IT-DB-IMS
- 250~ Oracle WebLogic Clusters
- 40~ apache tomcat
- Web domains
  - 300~ production
  - 200~ non production

CERN openlab member
- Oracle collaboration

Asturias. Spain

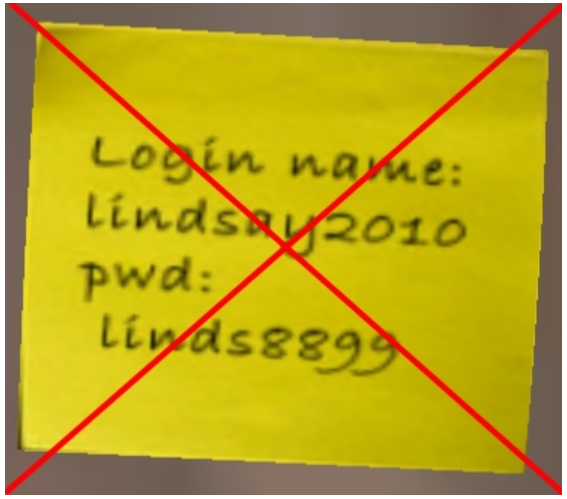
# SSO. Why?

# SSO. Why?

Benefit for the end **users**:
- Only one password to rule them all

Benefit for your **organization** security:
- Lower risk of phishing

Benefit for your **developers**:
- Delegate authentication implementation

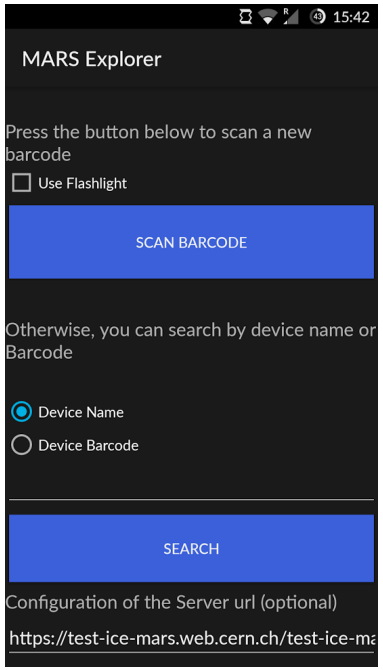


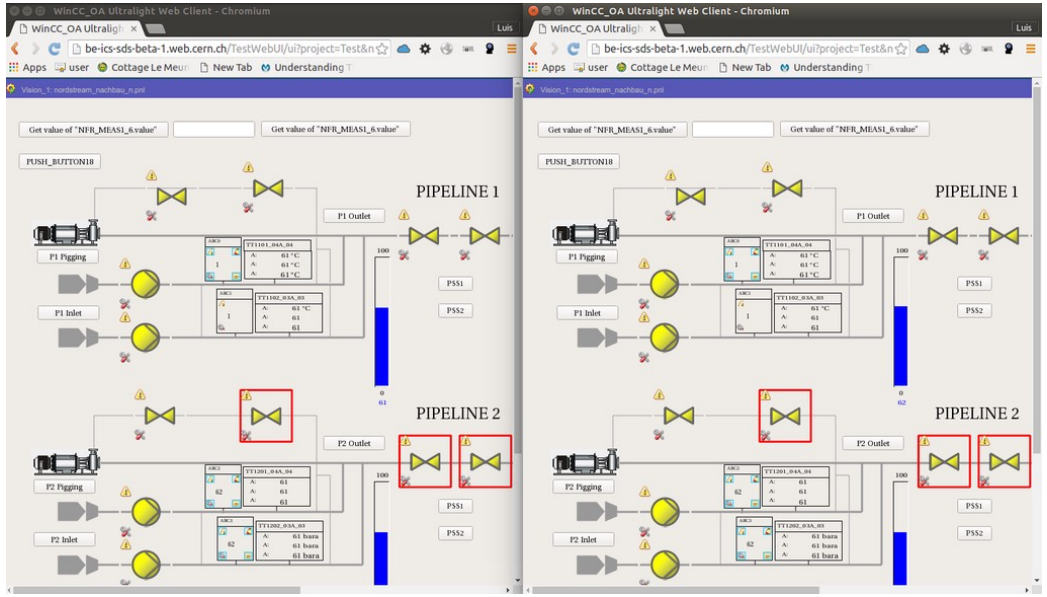

# SSO. Why?

## Web User Interfaces for control systems at CERN

WinCC_OA SCADA (BE-IC)
- Apache Tomcat
- Websockets
- CERN SSO

MARS explorer
- PLC barcode scanner
- Pique system EN-ICS



# SSO. How?

# SSO. How?

**CERN Identity Management Architecture**

User registered in Oracle Database

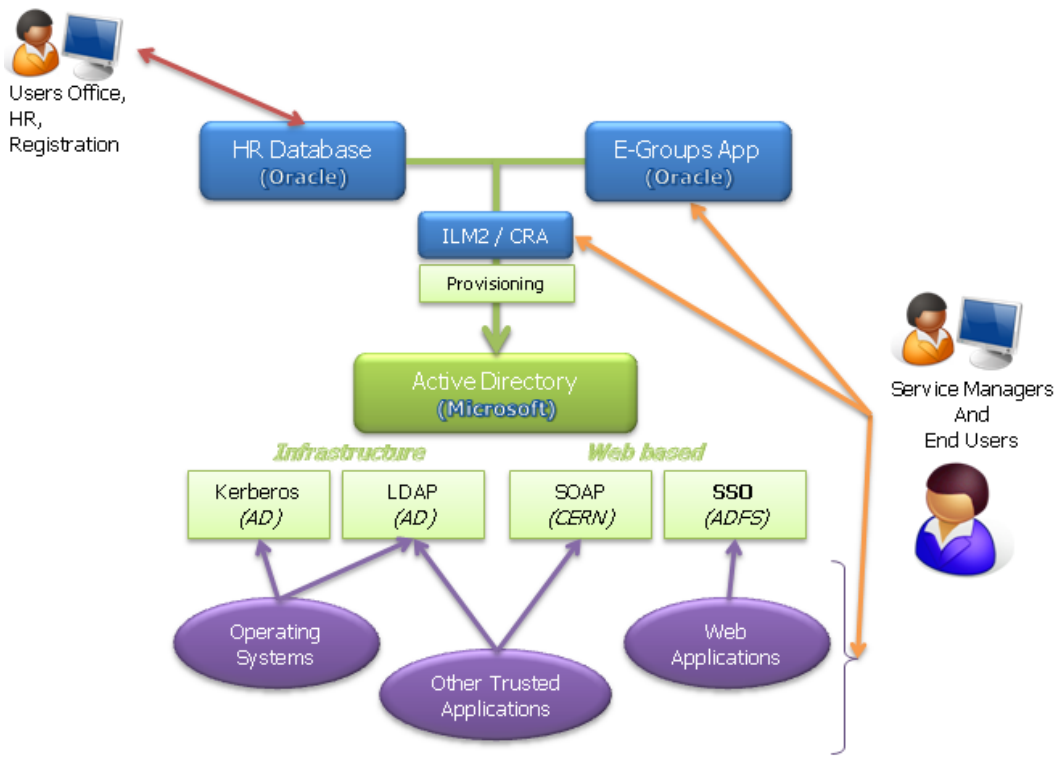
Member of groups and mailing lists

Owner of computing resources

Microsoft Active Directory

Authentication Providers

- Kerberos
- LDAP
- SOAP
- **SSO**

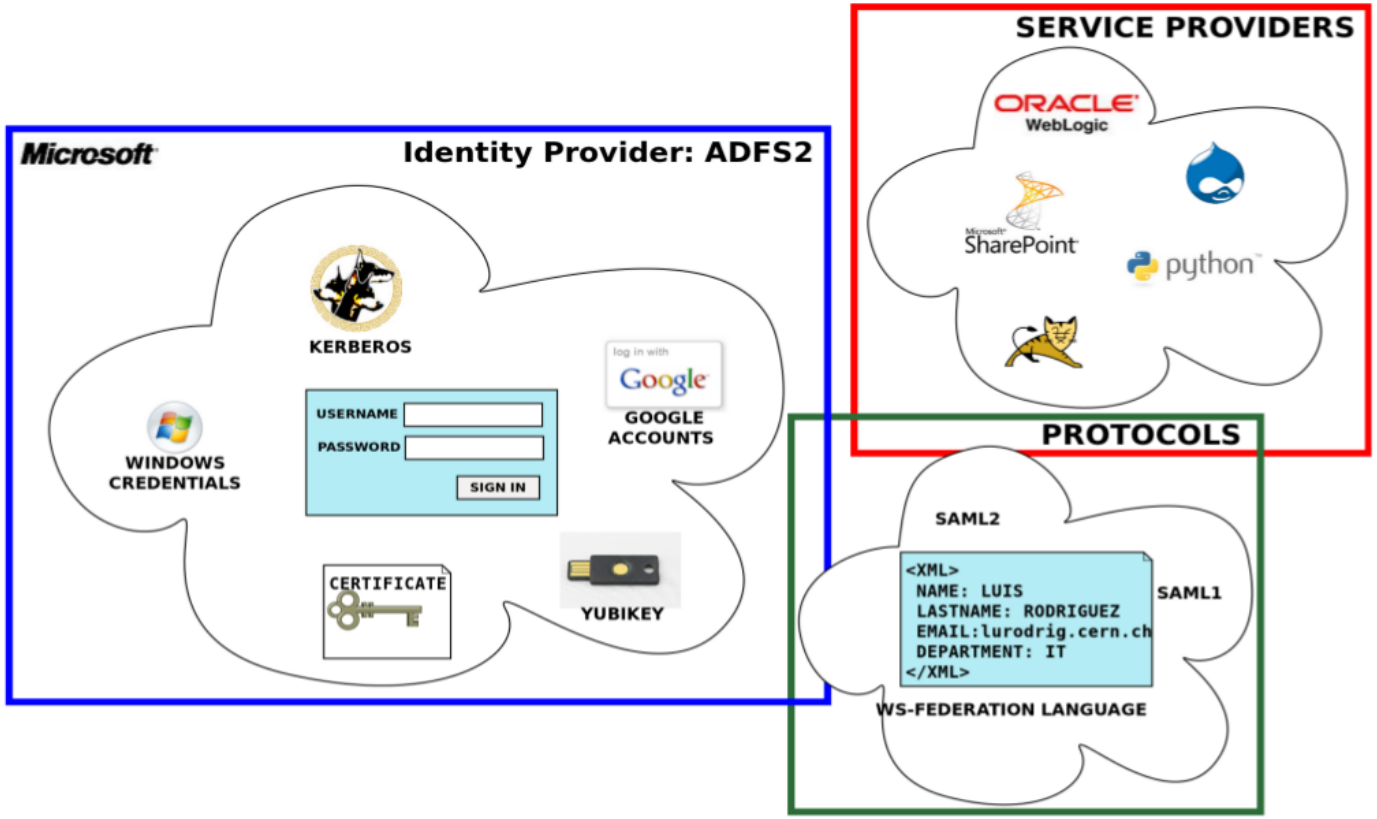


# SSO. How?

## CERN SSO. SAML2

Assertion:

*"This is Luis, his email is lurodrig@cern.ch, he has been authenticated via the login form and he works in the building 31"*



# SSO. How?

**Oracle WebLogic as SP**

SAML2 out-of-the-shelve

Custom

- WlsAttributeMapper:
  - Java Principals
- SAML2SLO: logout
- ssoFilters: apps integration
  - Legacy
  - Oracle APEX

Configuration

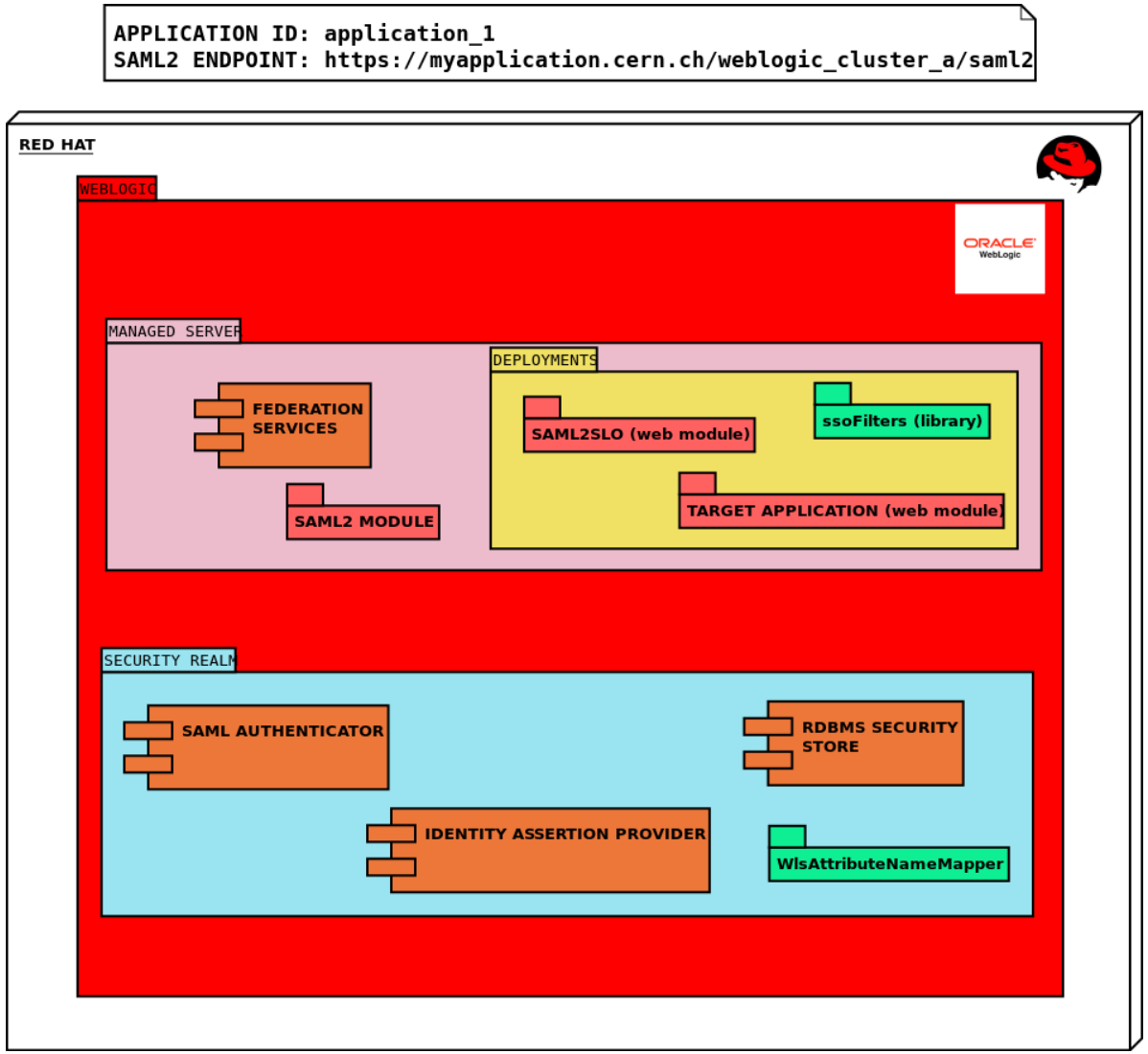
- EntityID + Certificate + Endpoints

IdP register

- Circle of trust

Oracle Database

- User session



# SSO. How?

**Shibboleth as SP**

Opensource

Shibboleth daemon

Memcached

  User session

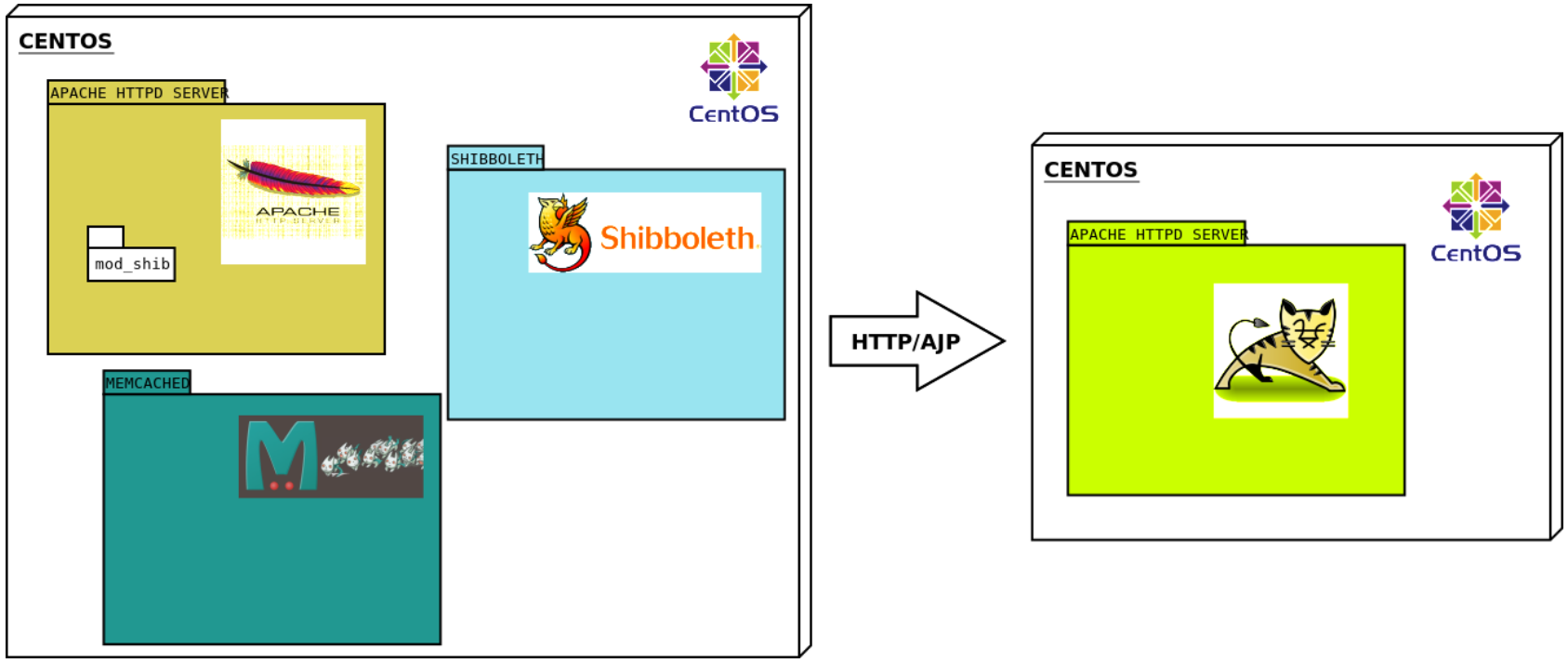
Apache httpd server

  mod_shib

Assertion data in

  HTTP: headers

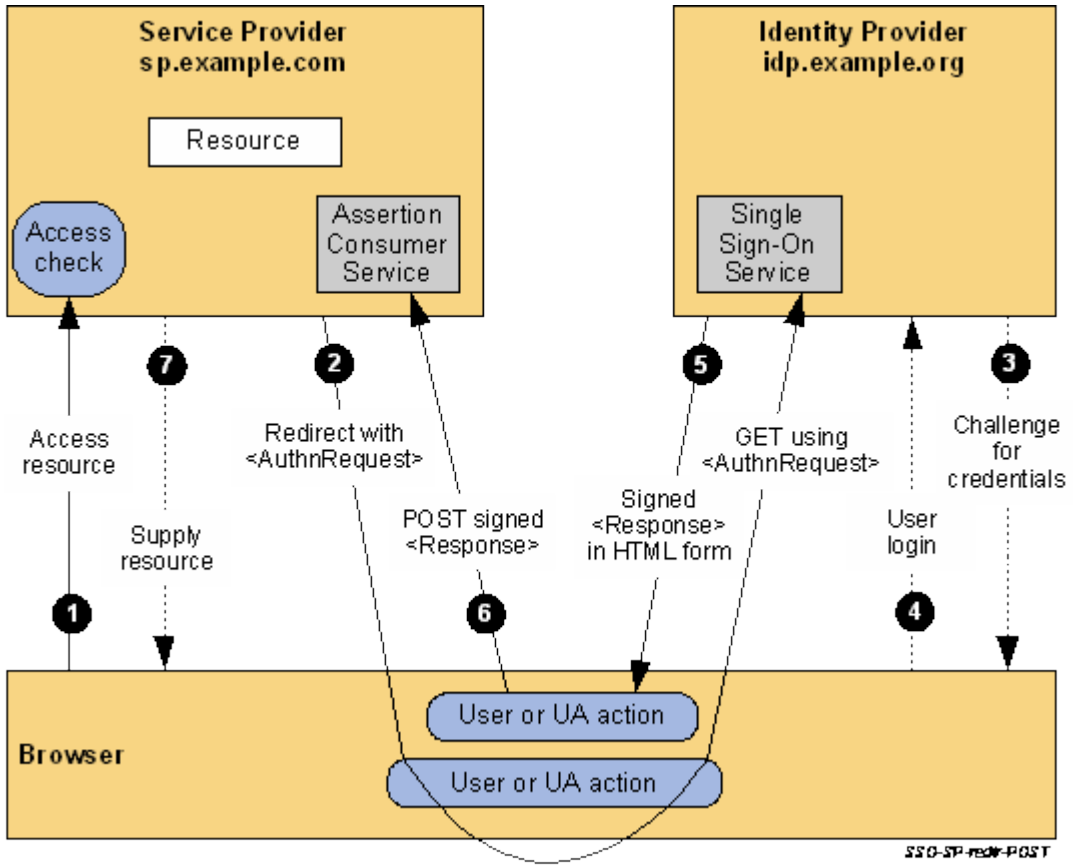
  AJP: attributes



# SSO. How?

## SAML2 Web Profile

### HTTP-POST Redirect Binding



# SSO. How?

**OAUTH2 in a nutshell**

- Security Framework for Authorization

Access tokens + HTTPS

Actors. Examples:

- Resource owner: end user
- Resource server: API
- Client: web site consuming API
- Authorization server:
  - Grants access with owner approval

# SSO. How?

## OAUTH2. The valet parking analogy

Car → protected resource
Car owner → resource owner
Car owner → authorization server
Parking attendant → client
Valet key → access token

# SSO. How?

## Oracle REST Data Services

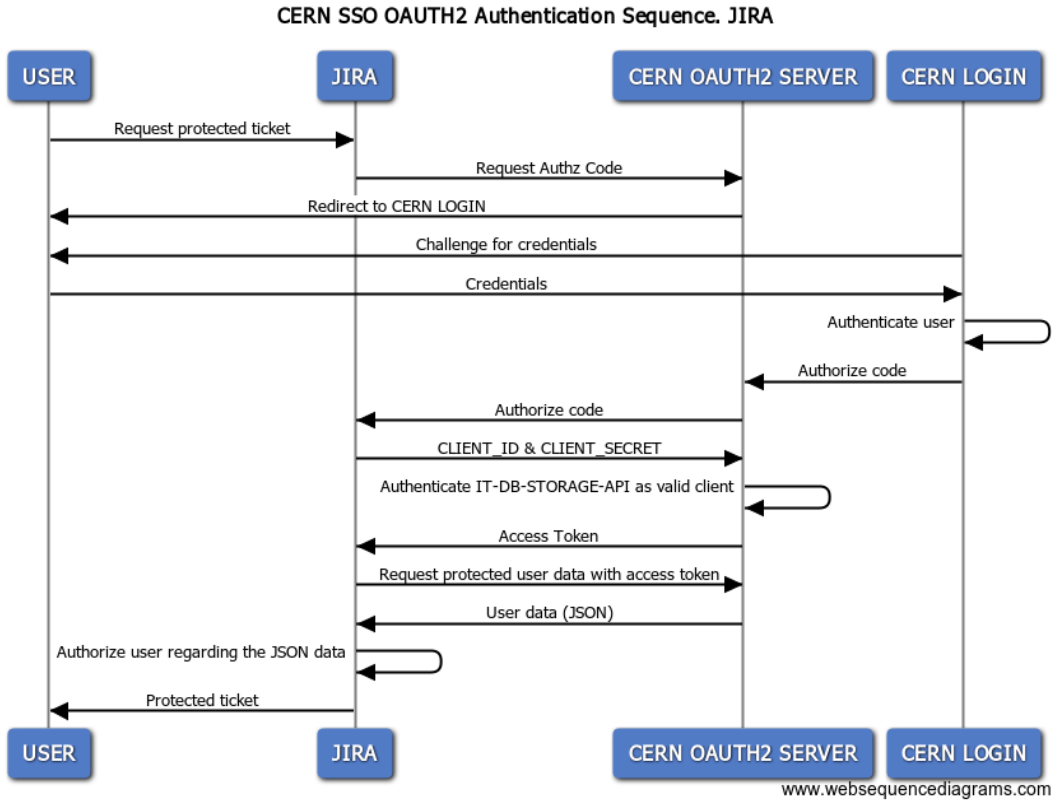
- Java Web module
- Translates HTTP verbs into SQL transtactions
  - GET /employee → SELECT * FROM employee...
  - PUT /employee → INSERT INTO employee (...
  - DELETE /employee/32 → DELETE FROM…
- OAUTH2 supported

# SSO. How?

## CERN OAUTH2. Authorization Service

- Authorization server
- Resource server: user data (json)
- Client credentials grant
- Machine-to-machine

Applications work as clients

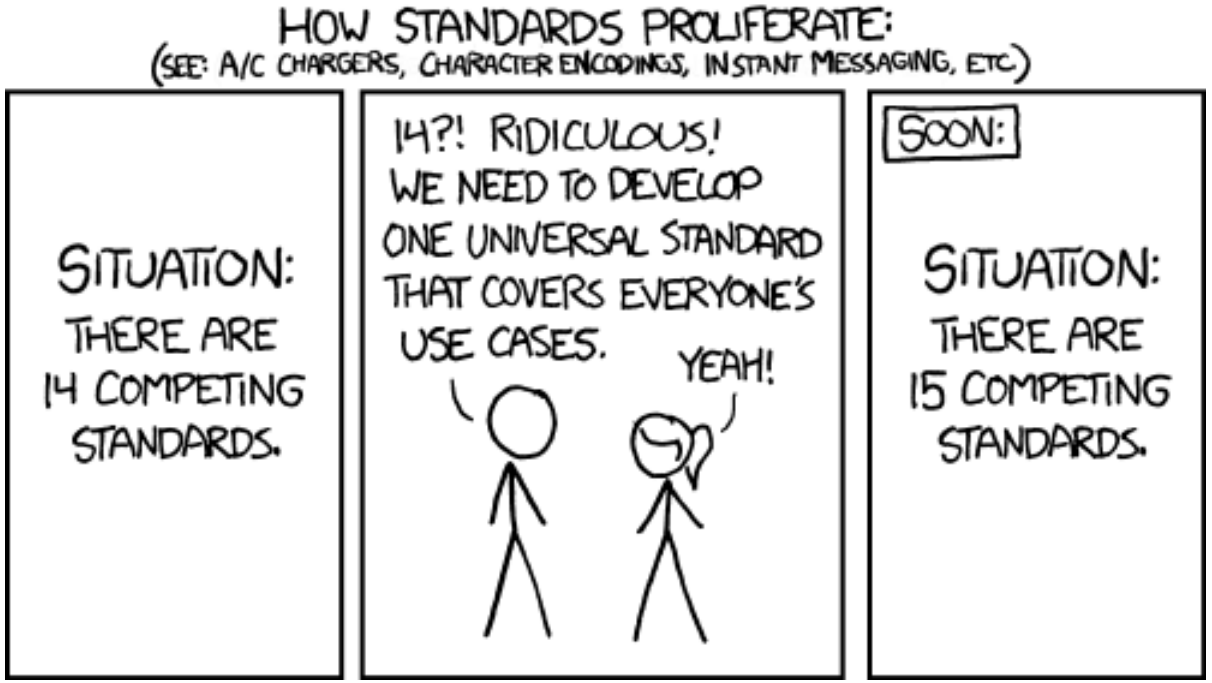


# Conclusions

# Conclusions

**Lessons learned**

- Check specifications
- Test, test, test!!!
- Keep it simple
- Opensource works
- Share your knowledge
- Do not reinvent the wheel!
  - Trust your IT
  - Follow standards
- Different scenarios
  - Web interfaces
    - SAML2 Web profile
  - APIs
    - OAUTH2



# Conclusions

Demo: Thursday 12th October, 17:45 - 18:15
**THSH302** - 1000 Things….


OpenAM

saml xml.org

ORACLE WEBLOGIC

spring

# QUESTIONS?

*luis.rodriguez.fernandez@cern.ch*

# References


Oracle Weblogic as a Service Provider for CERN Web Applications
http://openlab.cern/publications/presentations/weblogic-service-provider-cern-web-applications-apex-java-ee
Oracle Weblogic CERN SSO integration packages
https://github.com/cerndb/wls-cern-sso
Oracle Weblogic SAML2 Authorization
https://db-blog.web.cern.ch/blog/luis-rodriguez-fernandez/2015-02-oracle-weblogic-saml2-authorization
SSO with WebLogic 10.3.1 and SAML2
http://biemond.blogspot.com.es/2009/09/sso-with-weblogic-1031-and-saml2.html
ForgeRock OpenAM
https://github.com/ForgeRock/openam-community-edition
https://backstage.forgerock.com/docs/openam/11
Spring security SAML2
https://docs.spring.io/spring-security-saml/docs/1.0.0.RELEASE/reference/html/chapter-quick-start.html
https://github.com/spring-projects/spring-security-saml
Security Assertion Markup Language V2.0 Technical Overview
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.html
CERN SSO and Shibboleth
https://linux.web.cern.ch/linux/scientific6/docs/shibboleth.shtml
The OAUTH 2.O Authorization Framework
https://tools.ietf.org/html/rfc6749
OAUTH 2.0 in a nutshell – Simple Oriented Architecture
http://www.simpleorientedarchitecture.com/oauth-2-0-in-a-nutshell/
Developing Oracle RESTFul Services
https://twiki.cern.ch/twiki/bin/view/DB/DevelopingOracleRestfulServices
Oracle JET, ORDS & OAUTH2
https://db-blog.web.cern.ch/blog/luis-rodriguez-fernandez/2017-04-oracle-jet-ords-oauth2

# CONTACTS


***ALBERTO DI MEGLIO***
CERN openlab Head
alberto.di.meglio@cern.ch

***MARIA GIRONE***
CERN openlab CTO
maria.girone@cern.ch

***FONS RADEMAKERS***
CERN openlab CRO
fons.rademakers@cern.ch

***ANDREW PURCELL***
CERN openlab Communications Officer
andrew.purcell@cern.ch

***KRISTINA GUNNE***
CERN openlab Administration/Finance Officer
kristina.gunne@cern.ch


***www.cern.ch/openlab***