Luis Rodriguez Fernandez. CERN IT

Weblogic as a Service Provider for CERN Web Applications: APEX & Java EE

UKOUG 04/12/2013

lurodrig@cern.ch

AGENDA

- About CERN
- Why SSO?
- CERN SSO
- The challenge: integrate JEE and APEX applications
- The implementation choice: Weblogic as Service Provider
- Issues
- Conclusions

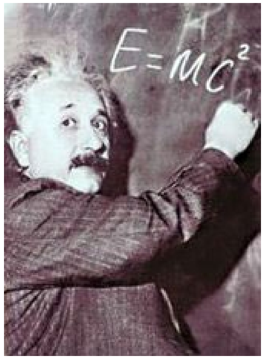
AGENDA

- **About CERN**
- SSO or not SSO?
- CERN SSO
- The challenge: integrate JEE and APEX applications
- The implementation choice: Weblogic as Service Provider
- Issues
- Conclusions

About CERN

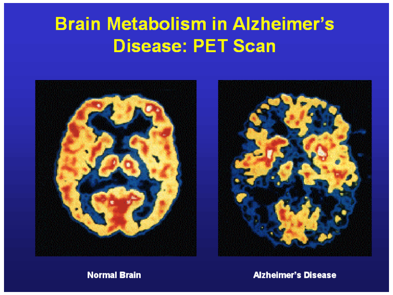
Push forward the frontiers of knowledge:

- E.g. the secrets of the Big Bang …what was the matter like within the first moments of the Universe’s existence?
- The Higgs Boson Particle!!!
- Fundamental research



Develop new technologies for accelerators and detectors:

- Information technology - the **Web** and the **GRID**
- Medicine - diagnosis and therapy


Brain Metabolism in Alzheimer’s Disease: PET Scan

Train scientists and engineers of tomorrow

Unite people from different countries and cultures

About CERN

About CERN

WHERE THE WEB WAS BORN

In the offices of this corridor, all the fundamental technologies of the World Wide Web were developed.

Started in 1990 from a proposal made by Tim Berners-Lee in 1989, the effort was first divided between an office in building 31 of the Computing and Networking Division (CN) and one in building 2 of the Electronics and Computing for Physics Division (ECP).

In 1991 the team came together in these offices, then belonging to ECP. It was composed of two CERN staff members, Tim Berners-Lee (GB) and Robert Cailliau (BE), aided by a number of Fellows, Technical Students, a Cooperant and Summer Students.

At the end of 1994 Tim Berners-Lee left CERN to direct the WWW Consortium (W3C), a world-wide organization devoted to leading the Web to its full potential. The W3C was founded with the help of CERN, the European Commission, the Massachusetts Institute of Technology (MIT), the Institut National pour la Recherche en Informatique et en Automatique (INRIA), and the Advanced Research Projects Agency (ARPA).

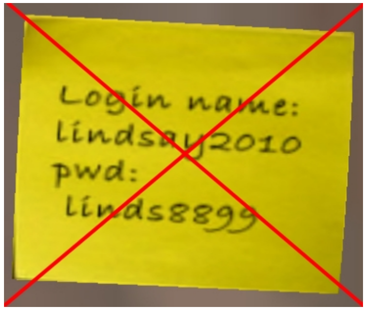
In 1995 Tim Berners-Lee and Robert Cailliau received the ACM Software System Award for the World Wide Web. In 2004, Tim Berners-Lee was awarded the First Millennium Technology Prize by the Finnish Technology Award Foundation.

The CERN Library
June 2004

AGENDA

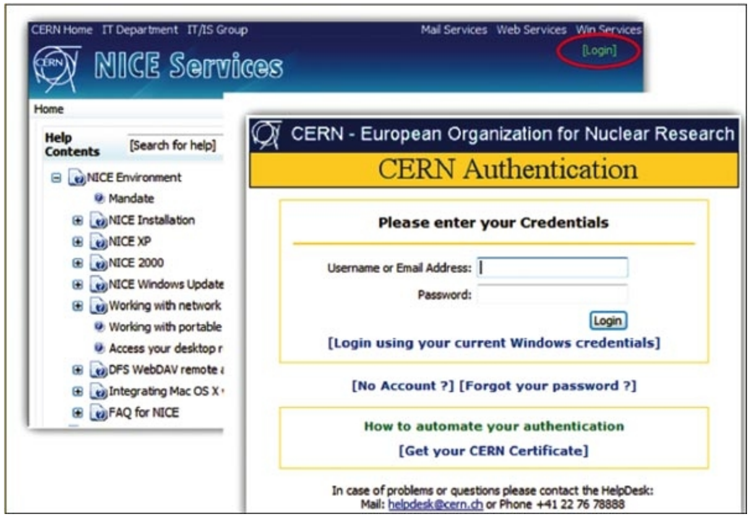
- About CERN
- **Why SSO?**
- CERN SSO
- The challenge: integrate JEE and APEX applications
- The implementation choice: Weblogic as Service Provider
- Issues
- Conclusions

Why SSO?



- Benefit for the **end users**: only one username-password for rule them all.
- Benefit for the **system security**: it is improved!
- Benefit for the **developers**: no need to build any custom authentication system.

AGENDA



CERN - European Organization for Nuclear Research

CERN Authentication

Please enter your Credentials

Username or Email Address:

Password:

[Login using your current Windows credentials]

[No Account ?] [Forgot your password ?]

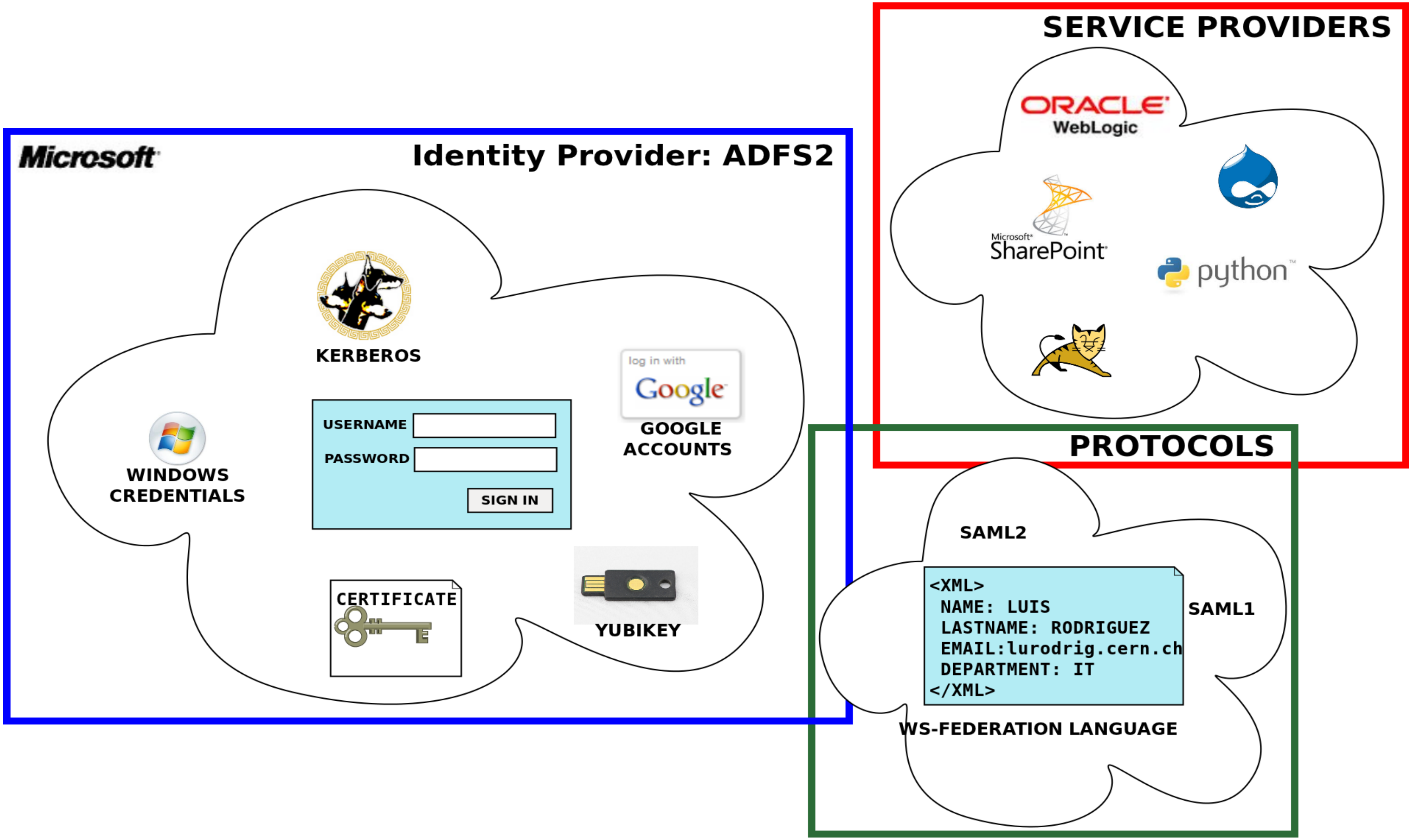
How to automate your authentication

[Get your CERN Certificate]

In case of problems or questions please contact the HelpDesk:
Mail: helpdesk@cern.ch or Phone +41 22 76 78888

- About CERN
- Why SSO?
- **CERN SSO**
- The challenge: integrate JEE and APEX applications
- The implementation choice: Weblogic as Service Provider
- Issues
- Conclusions

CERN SSO



SERVICE PROVIDERS

ORACLE WebLogic

Microsoft SharePoint

python

Microsoft

Identity Provider: ADFS2

KERBEROS

WINDOWS CREDENTIALS

USERNAME

PASSWORD

SIGN IN

log in with Google

GOOGLE ACCOUNTS

CERTIFICATE

YUBIKEY

PROTOCOLS

SAML2

SAML1

```
<XML>
 NAME: LUIS
 LASTNAME: RODRIGUEZ
 EMAIL:lurodrig.cern.ch
 DEPARTMENT: IT
</XML>
```

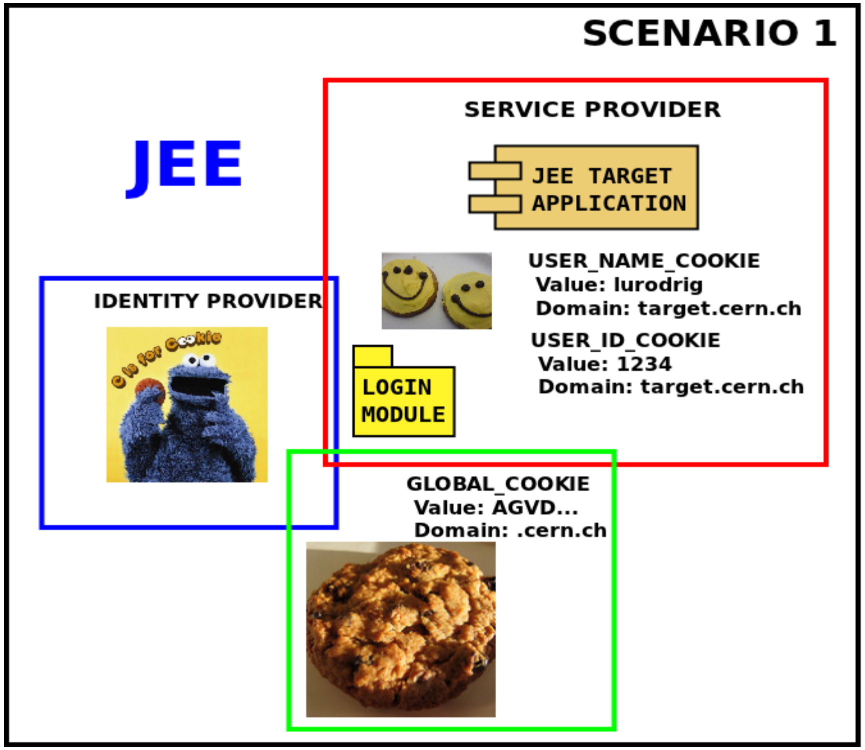
WS-FEDERATION LANGUAGE

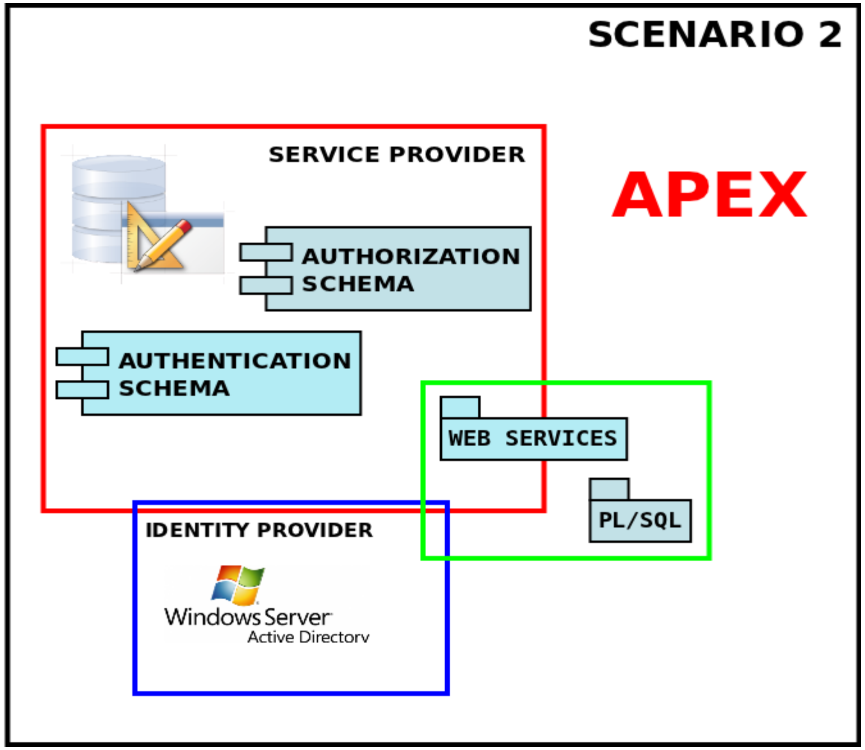
AGENDA

- About CERN
- Why SSO?
- CERN SSO
- **The challenge: integrate JEE and APEX applications**
- The implementation choice: Weblogic as Service Provider
- Issues
- Conclusions

The challenge

- JEE applications: legacy login system
- APEX: custom auth & authz schema



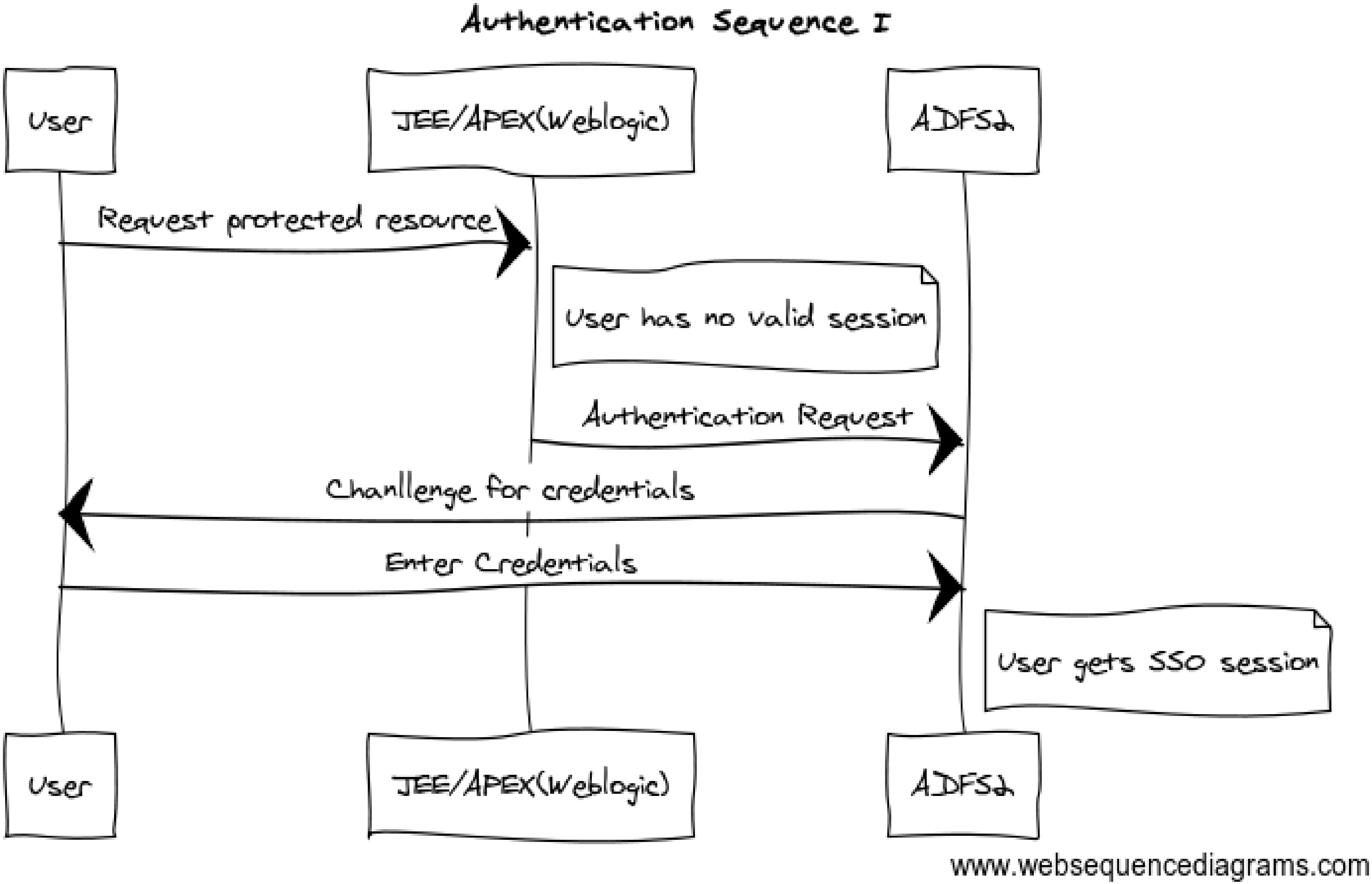


AGENDA

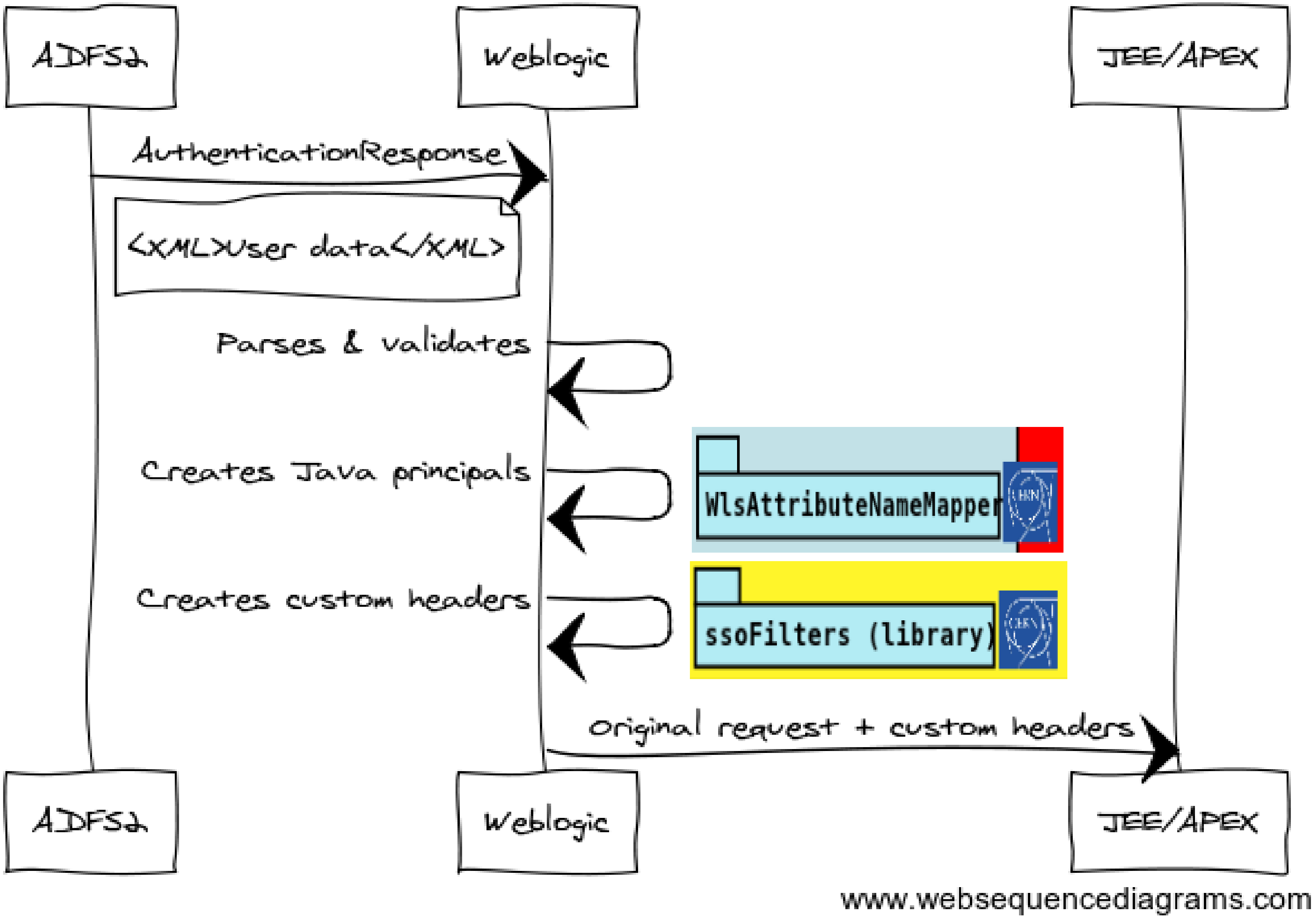
- About CERN
- Why SSO?
- CERN SSO
- The challenge: integrate JEE and APEX applications
- **The implementation choice: Weblogic as Service Provider**
- Issues
- Conclusions

The implementation choice

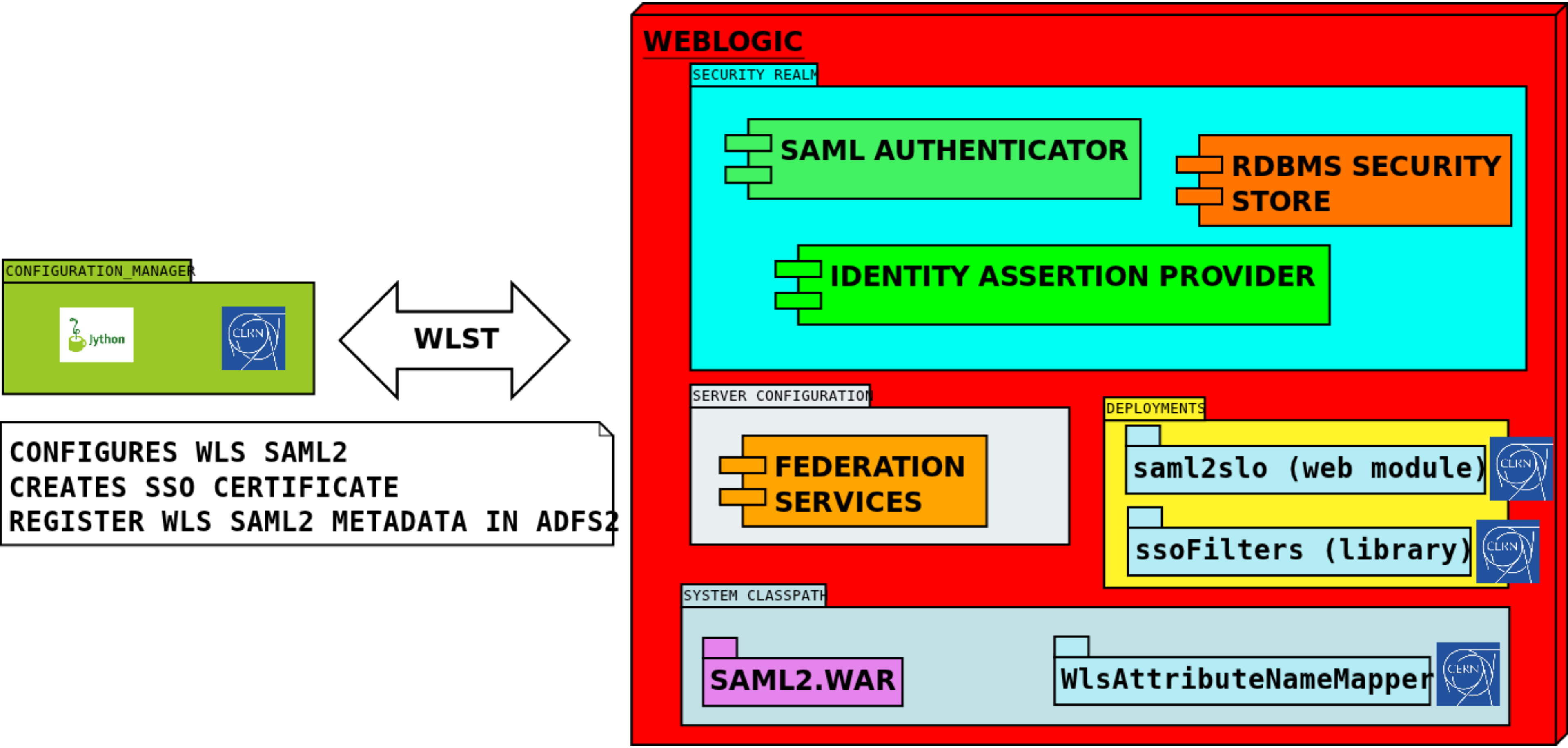
- **Weblogic** as the **Service Provider**
- Why? Because it “speaks” a lot of languages!
  - SAML1
  - **SAML2:**
    - Security enhanced: signed messages
    - More flexible: HTTP-POST, HTTP-REDIRECT, SOAP...
- Weblogic: “natural choice” for us


Authentication Sequence I
User
JEE/APEX(Weblogic)
ADFS2
Request protected resource
User has no valid session
Authentication Request
Chanllenge for credentials
Enter Credentials
User gets SSO session
User
JEE/APEX(Weblogic)
ADFS2
www.websequencediagrams.com

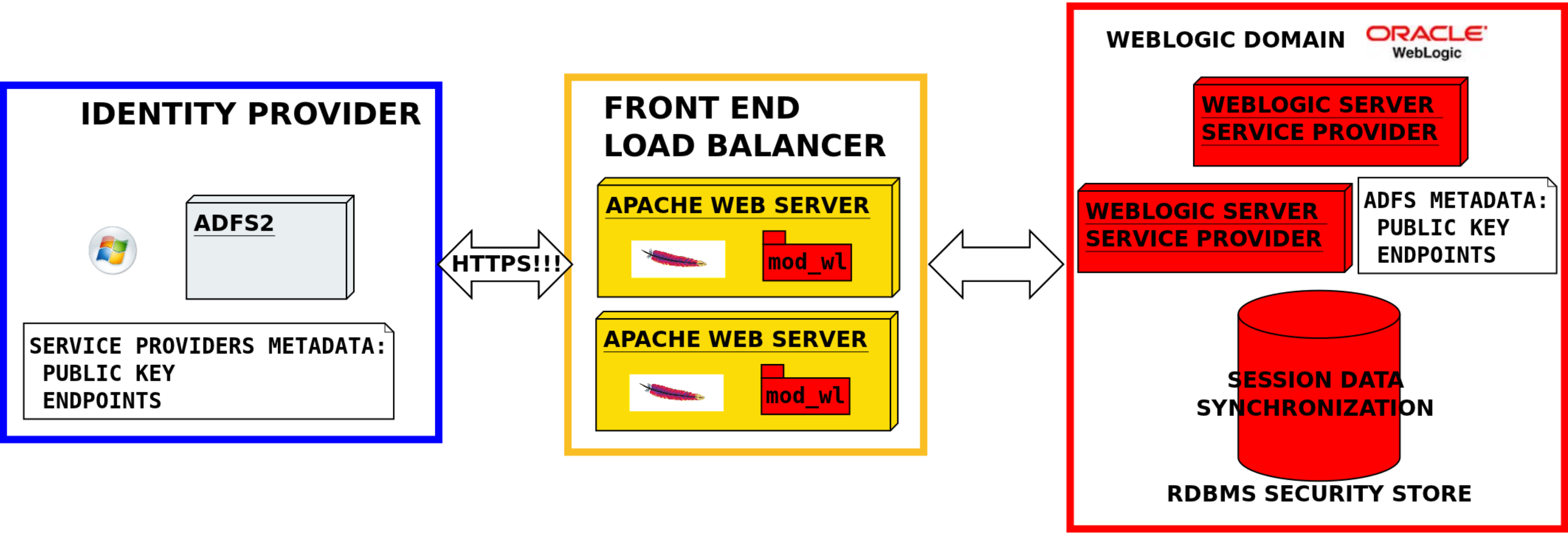
Authentication Sequence II



The implementation



The implementation



IDENTITY PROVIDER

ADFS2

SERVICE PROVIDERS METADATA:
PUBLIC KEY
ENDPOINTS

HTTPS!!!

FRONT END
LOAD BALANCER

APACHE WEB SERVER

mod_wl

APACHE WEB SERVER

mod_wl

WEBLOGIC DOMAIN

WEBLOGIC SERVER
SERVICE PROVIDER

WEBLOGIC SERVER
SERVICE PROVIDER

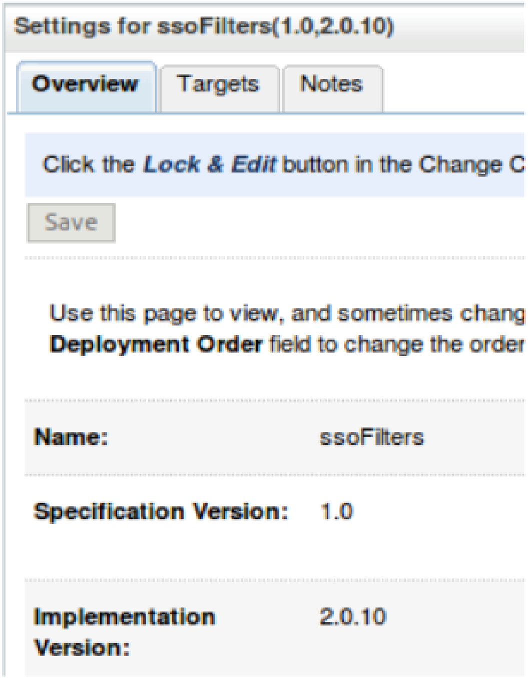
ADFS METADATA:
PUBLIC KEY
ENDPOINTS

SESSION DATA
SYNCHRONIZATION

RDBMS SECURITY STORE

The implementation. JEE scenario

- No code changes in the target application:
  - Descriptors: MANIFEST.MF & web.xml

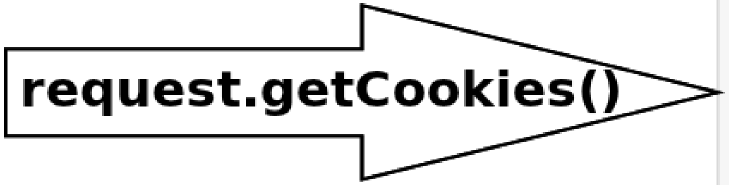


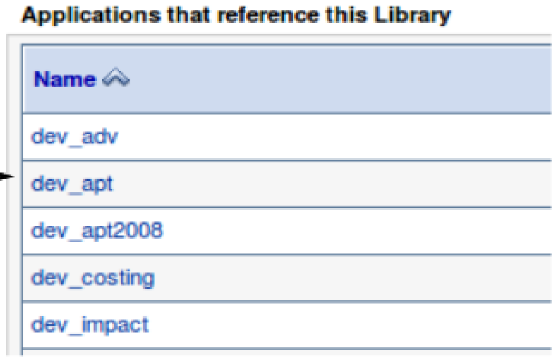
Settings for ssoFilters(1.0,2.0.10)

Click the *Lock & Edit* button in the Change C

Use this page to view, and sometimes chang
Deployment Order field to change the order

Name:	ssoFilters
Specification Version:	1.0
Implementation Version:	2.0.10



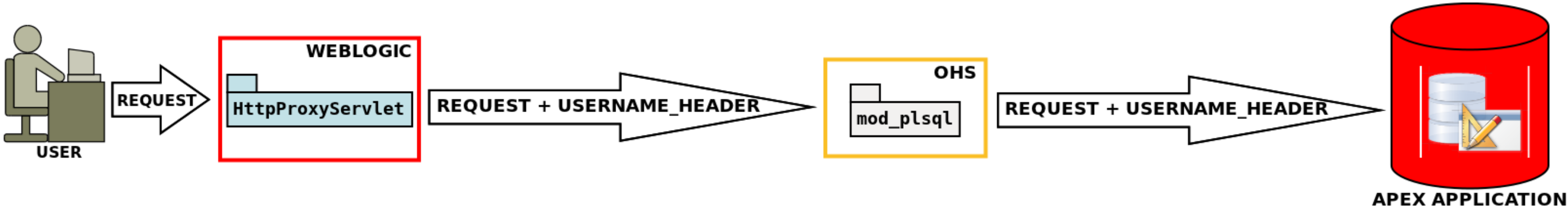


Applications that reference this Library

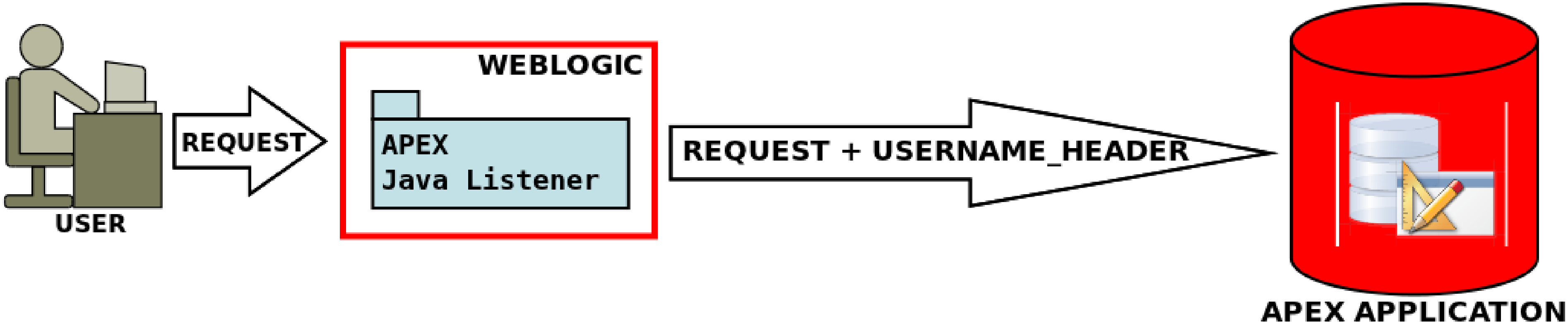
Name
dev_adv
dev_apt
dev_apt2008
dev_costing
dev_impact

The implementation. APEX scenario

- WLS + HttpProxyServlet + OHS (mod_plsql)

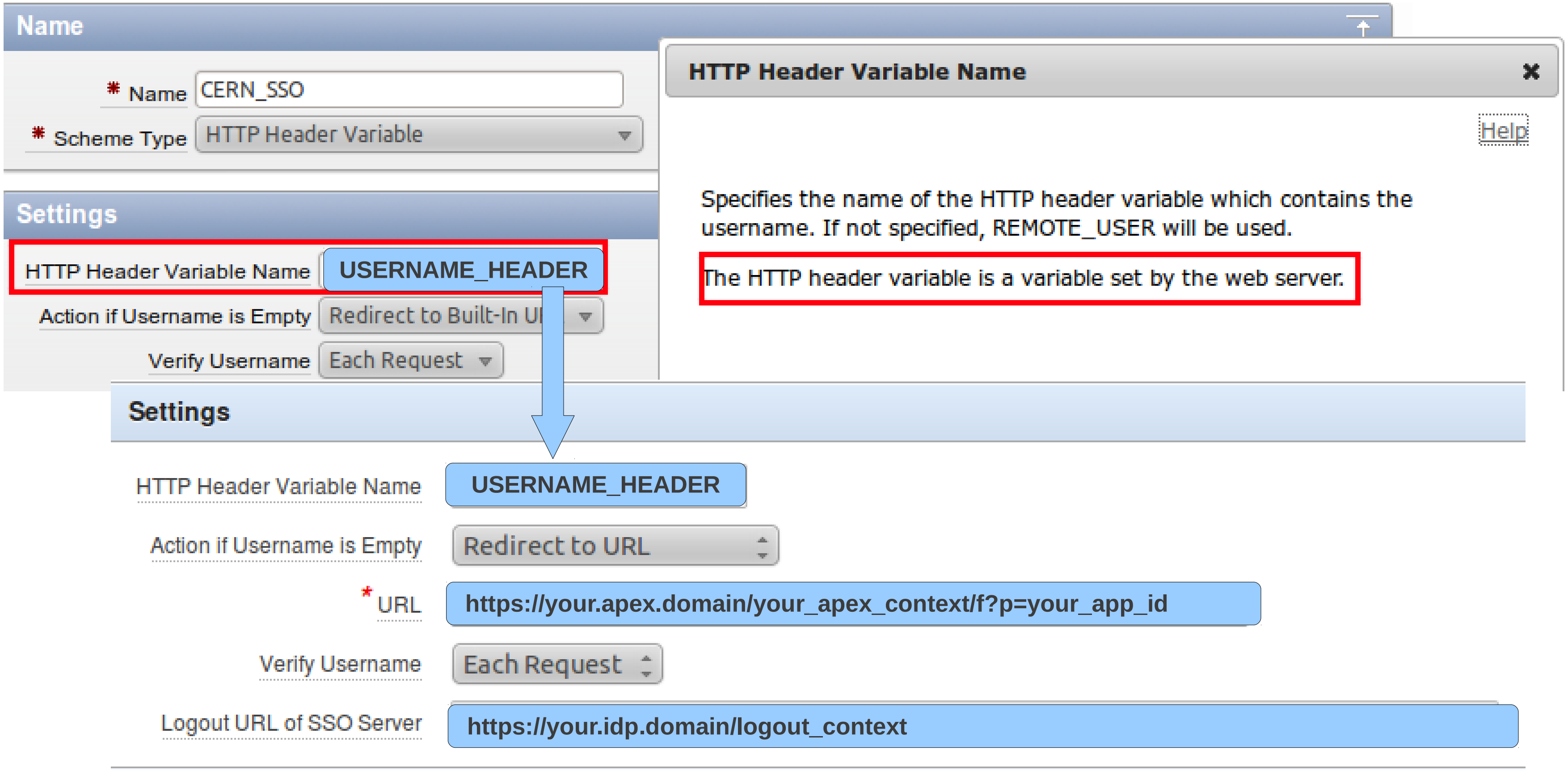


- WLS + APEX Java Listener



The implementation. APEX scenario

- Application side



Name

* Name: CERN_SSO

* Scheme Type: HTTP Header Variable

Settings

HTTP Header Variable Name: USERNAME_HEADER

Action if Username is Empty: Redirect to Built-In UI

Verify Username: Each Request

HTTP Header Variable Name

Help

Specifies the name of the HTTP header variable which contains the username. If not specified, REMOTE_USER will be used.

The HTTP header variable is a variable set by the web server.

Settings

HTTP Header Variable Name: USERNAME_HEADER

Action if Username is Empty: Redirect to URL

* URL: https://your.apex.domain/your_apex_context/f?p=your_app_id

Verify Username: Each Request

Logout URL of SSO Server: https://your.idp.domain/logout_context

AGENDA

- About CERN
- SSO or not SSO?
- CERN SSO
- The challenge: integrate JEE and APEX applications
- The implementation choice: Weblogic as Service Provider
- **Issues**
- Conclusions

Issues

- Technical
- Security
- SAML2 constraints
- Weblogic constraints
- User requirements

Technical issue: TimeSkew

- **Problem**: **intermittent 403 errors**.
- **Where**: Weblogic running in OVM
- **Cause:** time difference between IdP and SP machines (ntpd got crazy)
- **Log traces**: weblogic managed server:

```
Security:090377Assertion is not yet valid (NotBefore condition).
```

- **Solution**: Microsoft Forums (social.technet.microsoft.com)
  - **Skew the SAMLP NotBefore in ADFS2 v2**: set back the NotBefore value 2 minutes before the creation of the response

Technical issue: Custom Headers Lost I

- **Problem**: **your custom headers never reach the target application**
- **Where**: WLS (10.3.4, 10.3.5) with HttpProxyServlet
- **Cause**: *Bug 10381400 - httpproxyservlet sets content length/type on original request instead of wrapped*
- **Log traces**: unfortunately no
- **Solution**: Oracle Support
  - For WLS < 10.3.6 apply patch: 10381400

Technical issues: Custom Headers Lost II

- **Problem**: **your custom headers get lost, sometimes**
- **Where**: WLS with HttpProxyServlet → OHS, third party app server...
- **Cause**: HttpProxyServlet does not take into account the "Connection:close" header
- **Log traces**: wl_proxy.log

weblogic.servlet.proxy.HalfOpenSocketRetryException: status line is null

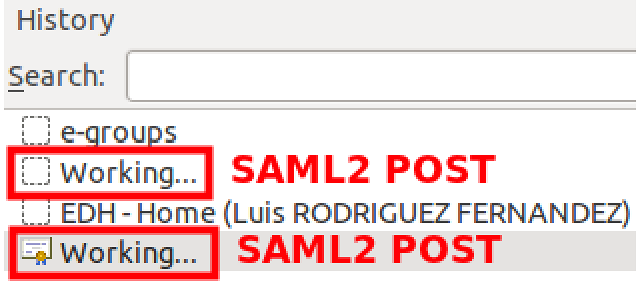
- **Solution**: Oracle Support
  - 1391665.1 - HalfOpenSocketRetryException Received While Using the HttpClusterServlet as a Proxy:
    - KeepAliveEnabled=false => Disable connection pool

Security: APEX authentication

- **Problem**: **username header injection**
- **Where**: APEX applications with HTTP Header Authentication Schema
- **Cause**: **any DB user** can execute the **f procedure**
- **Solution**: CERN
  - Ensure that **only** the **APEX_PUBLIC_USER** executes the f procedure

SAML2 constraints: back button

- **Problem**: **user clicks the back button and gets a 403 error**
- **Where**: WLS with SAML2.0 Federation Services enabled
- **Scenarios**:
  - Successful login
  - Link to another application (SAML2)



History

Search:

e-groups

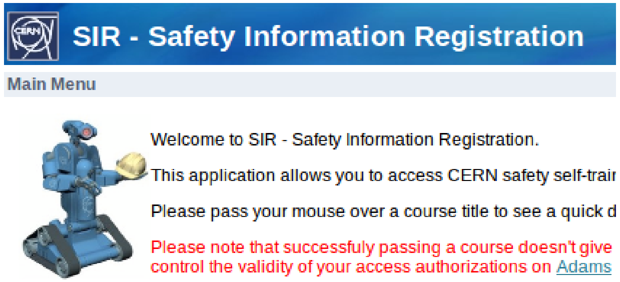
Working... SAML2 POST

EDH - Home (Luis RODRIGUEZ FERNANDEZ)

Working... SAML2 POST

- **Cause**: the history of your browser is “polluted” with the SAML2 protocol requests
- **Solution**: CERN
  - Intercepts 403 error and shows a more user friendly page

SAML2 constraints: post method body lost



SIR - Safety Information Registration

Main Menu

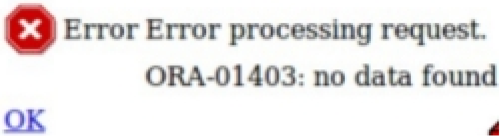
Welcome to SIR - Safety Information Registration.

This application allows you to access CERN safety self-trair

Please pass your mouse over a course title to see a quick d

Please note that successfuly passing a course doesn't give control the validity of your access authorizations on Adams

- **Problem**: **application timeout**
- **Where**: APEX applications in “kiosk mode”:
  - Web browser only
  - Windows credentials authentication



Error Error processing request.

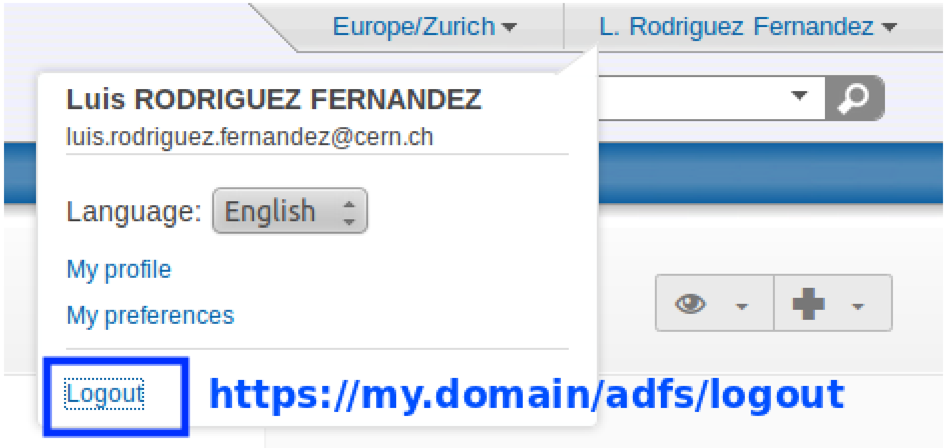
ORA-01403: no data found

- **Scenario**:
  - WLS timeout
  - User access the application and get an error
- **Cause**: the original APEX POST request becomes a GET after pass by WLS & ADFS2 → all the post parameters are lost → ORA-01403
- **Solution**: CERN
  - Increase WLS timeout
- **Alternative solution**: Oracle Technology Network
  - Modify the apex.submit() method

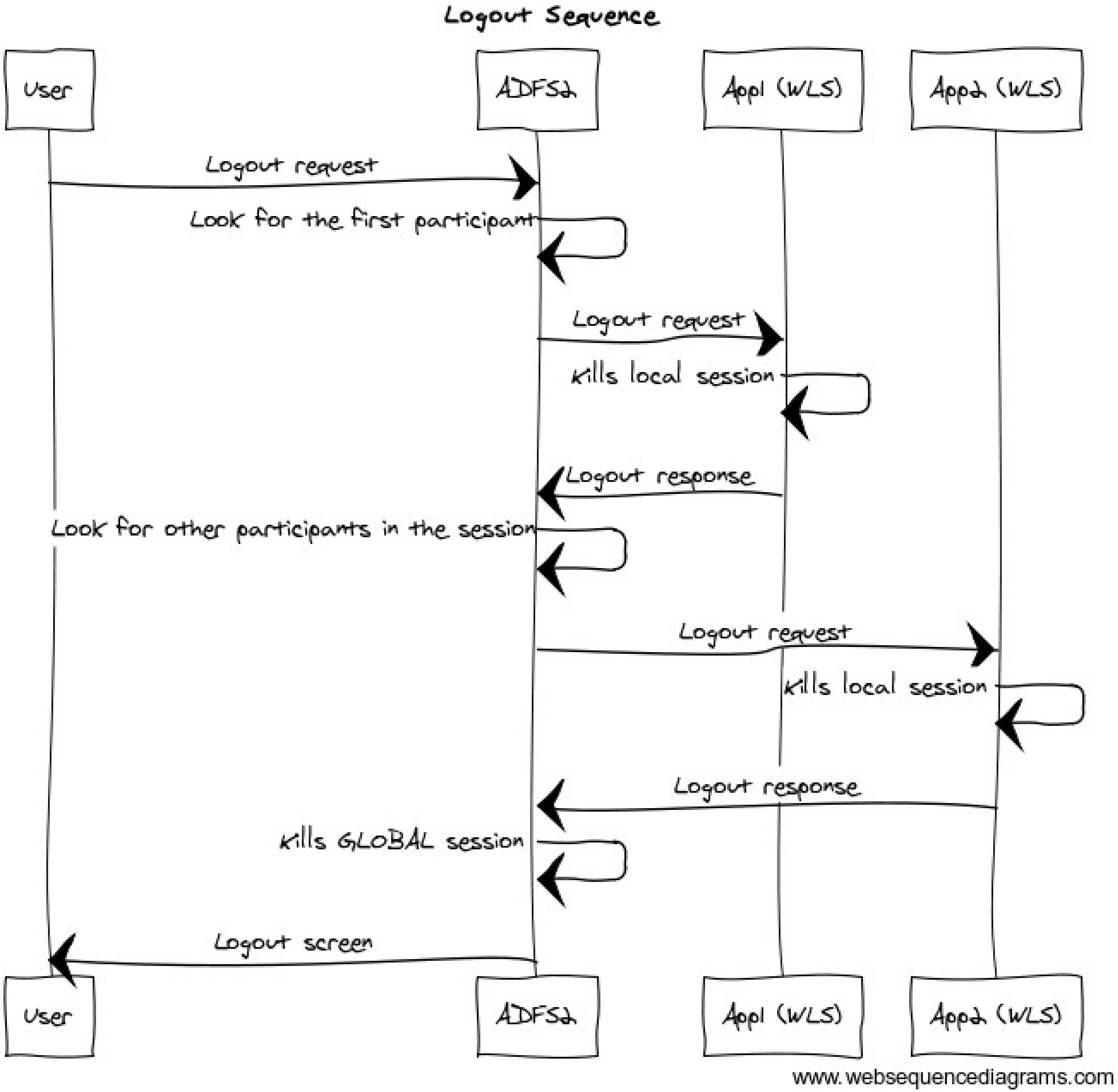
SAML2 constraints: logout protocol

- **Problem**: **if any of the participants (SP) in the session fails, the whole logout process fails**

SAML2 constraints: logout protocol



https://my.domain/adfs/logout

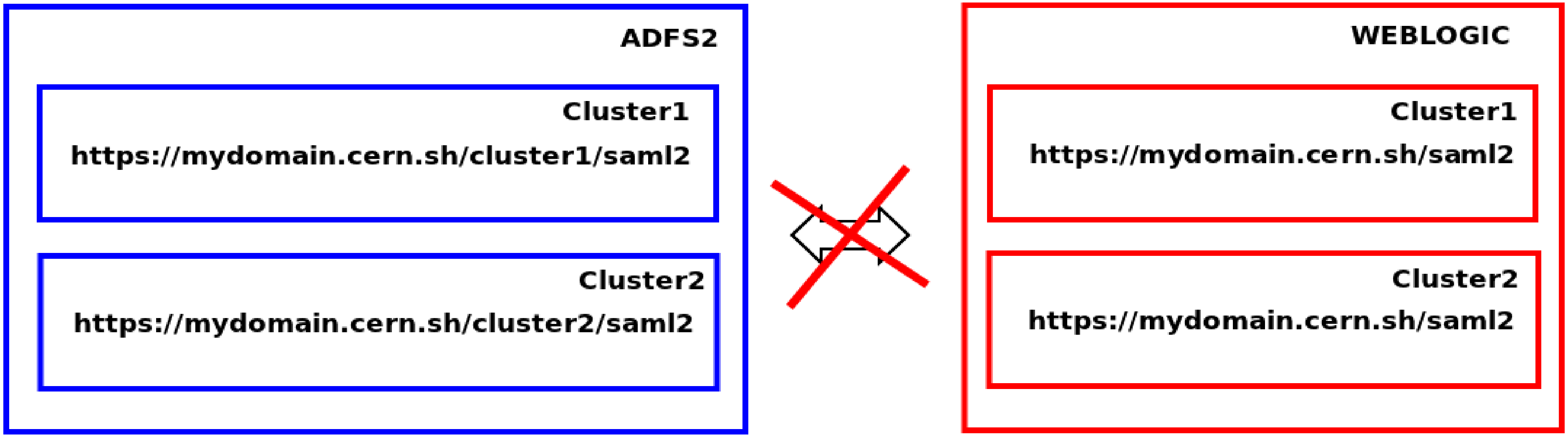

Logout Sequence
User
ADFS2
App1 (WLS)
App2 (WLS)
Logout request
Look for the first participant
Logout request
Kills local session
Logout response
Look for other participants in the session
Logout request
Kills local session
Logout response
Kills GLOBAL session
Logout screen
User
ADFS2
App1 (WLS)
App2 (WLS)
www.websequencediagrams.com

SAML2 constraints: logout protocol

- **Problem**: **if any of the participants (SP) in the session fails, the whole logout process fails**
- **Where**: WLS as SP with ADFS2 as IdP
- **Scenario**:
  - User login and "visits" different applications (SP)
  - One of the applications logout module fails
- **Cause**: ADFS2 logout implementation
- **Solution**:
  - Delete cookies or close the browser

Weblogic constraints: saml2 context mandatory

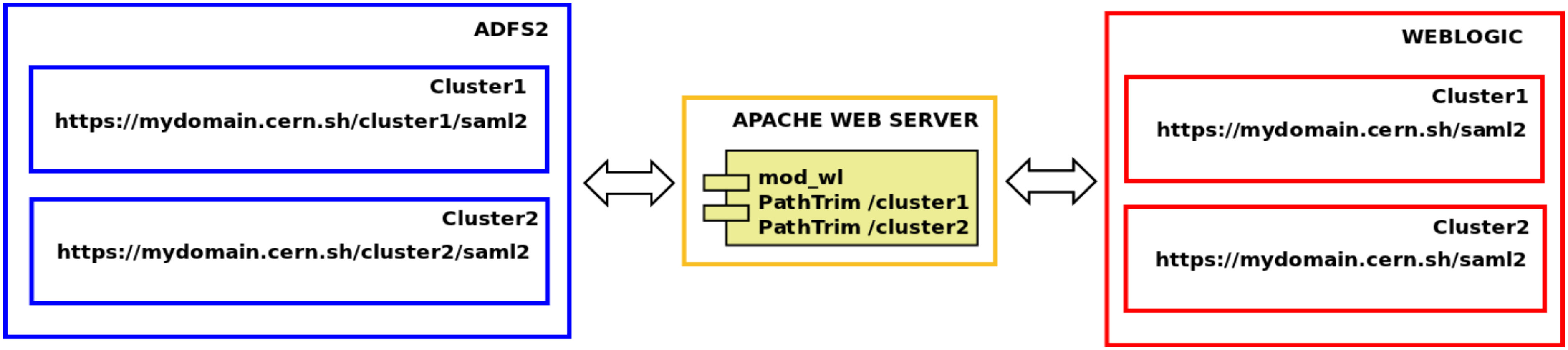
- **Problem**: **only one SAML2 cluster per domain**
- **Scenario**:


ADFS2
Cluster1
https://mydomain.cern.sh/cluster1/saml2
Cluster2
https://mydomain.cern.sh/cluster2/saml2
WEBLOGIC
Cluster1
https://mydomain.cern.sh/saml2
Cluster2
https://mydomain.cern.sh/saml2

- **Cause**: WLS force you to use /saml2 for your federation services endpoints

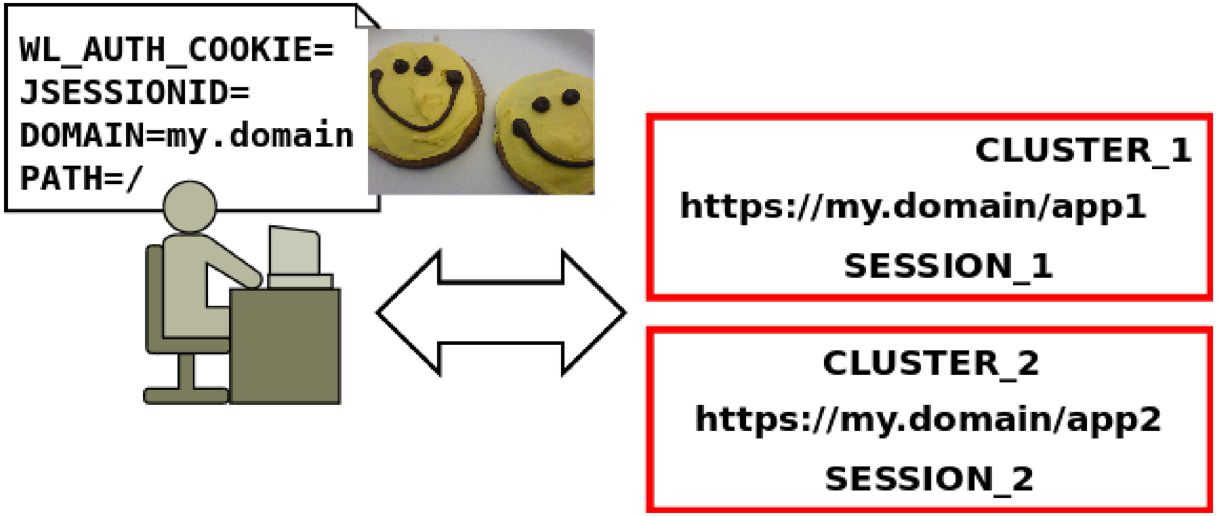
Weblogic constraints: saml2 context mandatory

- **Solution**: CERN
  - **PathTrim** parameter in mod_wl: *specifies the string trimmed by the plug-in from the {PATH}/{FILENAME} portion of the original URL, before the request is forwarded to WebLogic Server.*


ADFS2
Cluster1
https://mydomain.cern.sh/cluster1/saml2
Cluster2
https://mydomain.cern.sh/cluster2/saml2
APACHE WEB SERVER
mod_wl
PathTrim /cluster1
PathTrim /cluster2
WEBLOGIC
Cluster1
https://mydomain.cern.sh/saml2
Cluster2
https://mydomain.cern.sh/saml2

Weblogic constraint: session issues

- **Problem**: **application session data lost**
- **Where**: WLS as SP
- **Cause**: saml2 module forces you to use “/” in the cookie-path
- **Scenario:**



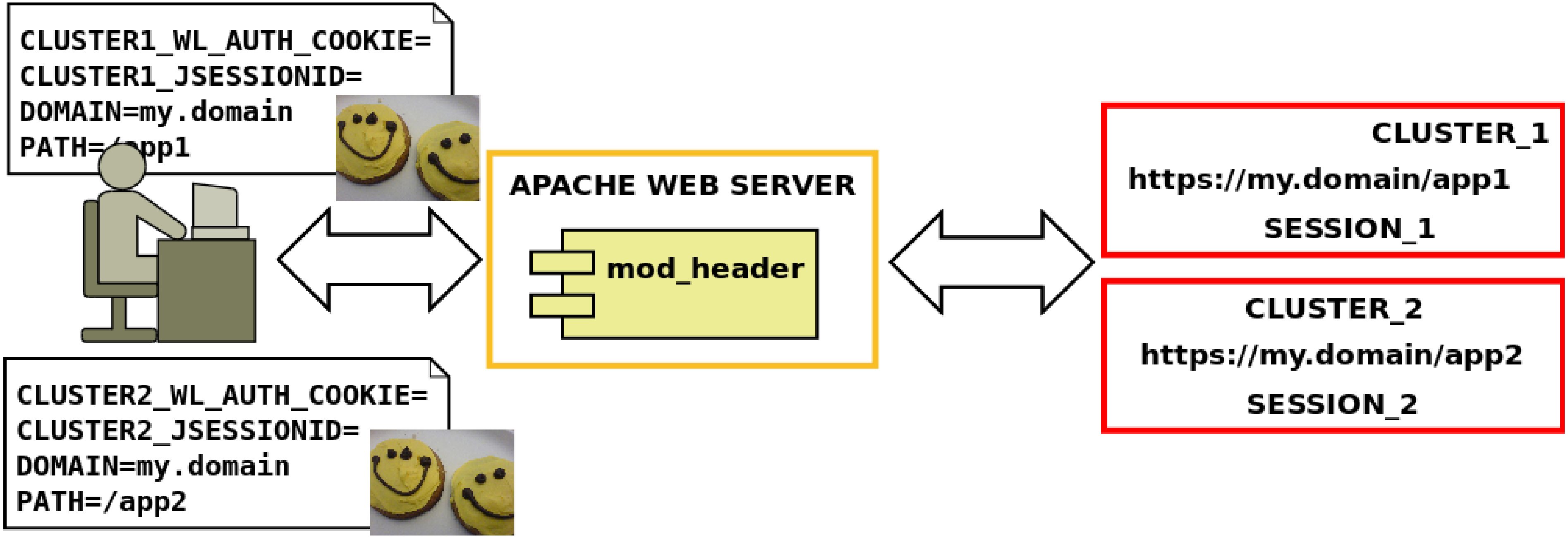
```
WL_AUTH_COOKIE=
JSESSIONID=
DOMAIN=my.domain
PATH=/
```

CLUSTER_1
https://my.domain/app1
SESSION_1

CLUSTER_2
https://my.domain/app2
SESSION_2

Weblogic constraint: session issues

- **Solution**: CERN
  - Cookie rewrite



CLUSTER1_WL_AUTH_COOKIE=
CLUSTER1_JSESSIONID=
DOMAIN=my.domain
PATH=/app1

CLUSTER2_WL_AUTH_COOKIE=
CLUSTER2_JSESSIONID=
DOMAIN=my.domain
PATH=/app2

APACHE WEB SERVER

mod_header

CLUSTER_1
https://my.domain/app1
SESSION_1

CLUSTER_2
https://my.domain/app2
SESSION_2

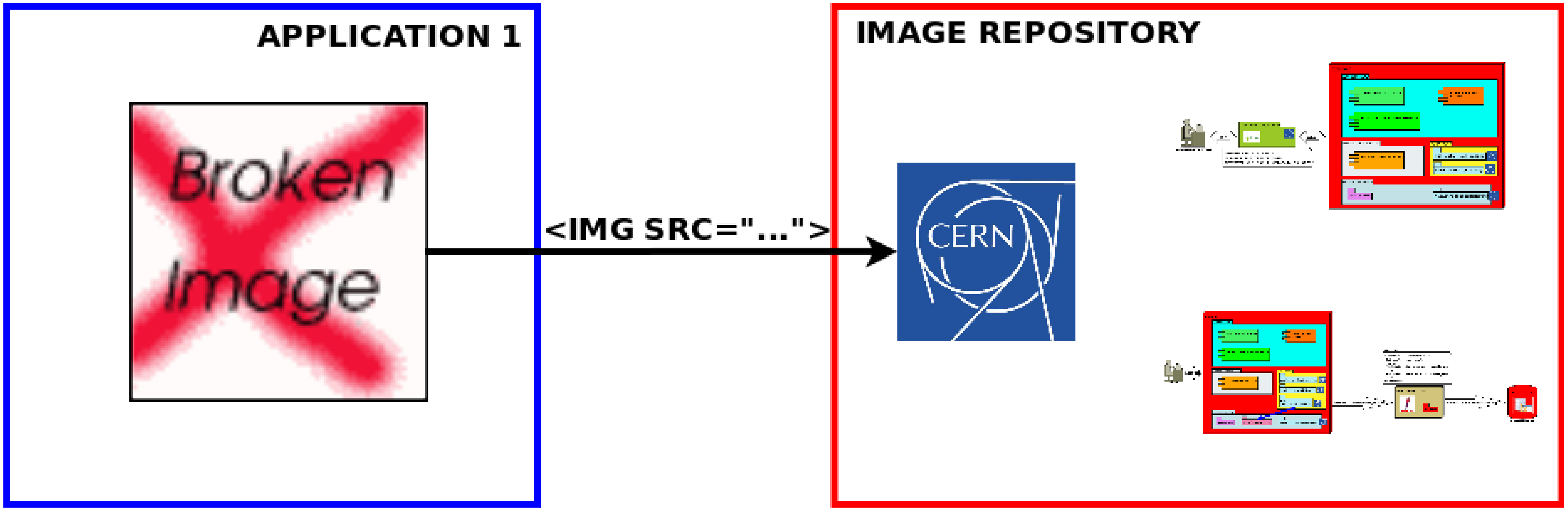
Weblogic constraint: RDBMS bound

- **Problem**: **all the WLS domain members in FAILED_NOT_RESTARTABLE**
- **Where**: WLS with RDBMS Security Store
- **Cause**: WLS can not connect with the Database
- **Log traces**: Weblogic (AdminServer, managed servers)

  SQLException --> Security Services Unavailable
- **Note:** Weblogic Clusters + SAML 2.0 = It is **REQUIRED**
- **Solution**:
  - Verify connection settings

User requirements: get images from different domains

- **Problem**: **broken images (404 error)**
- **Scenario**:



User requirements: get images from different domains

- **Cause**: img request falls in the exchange of messages between the SP and the WLS
- **Solution**: CERN
  - Pre-initialized a session in application 2 (refer in an iframe a protected resource in app2)
  - Embedd the image in an Iframe

AGENDA

- About CERN
- SSO or not SSO?
- CERN SSO
- The problem: integrate JEE and APEX applications
- The implementation choice: Weblogic as Service Provider
- Issues
- **Conclusions**

Conclusions

- It works! Some figures:
  - ~31000 “signins” per day
  - ~5000 “signouts”
- The hard work:
  - Workaround the SAML2 & WLS constraints
  - Fit the requirements of the legacy systems
- WLS does not provide the SLO:
  - CERN saml2slo OpenSource (coming soon, hopefully)

Useful resources

- Oracle Support:
  - Km Note 1298818.1 - WLS Proxy Servlet (weblogic.servlet.proxy.HttpProxyServlet) does not consider the Header values from the wrapped request
  - Bug 10381400 - httpproxyservlet sets content length/type on original request instead of wrapped
  - 1391665.1 - HalfOpenSocketRetryException Received While Using the HttpClusterServlet as a Proxy
- Oracle Documentation:
  - Using Web Server Plug-Ins with Oracle WebLogic Server: http://docs.oracle.com/cd/E23943_01/web.1111/e14395/intro.htm
  - Configuring Single Sign-On with Web Browsers and HTTP Clients: http://docs.oracle.com/cd/E24329_01/web.1211/e24422/saml.htm#SECMG301

Useful resources

- Community:
  - SSO with Weblogic 10.3.1 and SAML2: http://biemond.blogspot.ch/2009/09/sso-with-weblogic-1031-and-saml2.html
  - Construct a signed SAML2 logout request: http://stackoverflow.com/questions/8150096/construct-a-signed-saml2-logout-request
  - Adding Http Headers to Requests: http://www.tidytutorials.com/2009/11/adding-headers-to-requests-in-filters.html
  - Servlet Filters: Removing Cookies: http://www.codersrevolution.com/index.cfm/2008/7/11/Java-Servlet-Filters-Part-2-Removing-Cookies
- SAML2 docs (OASIS):
  - SAML V2.0 Technical Overview: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.pdf
  - SAML V2.0 Documentation index: http://docs.oasis-open.org/security/saml/Post2.0/

Questions?

- **lurodrig@cern.ch**
- **uo67113@gmail.com**

Credits

Photos:

- flicker.com
  - Cookie Monster. Michelle O'Connell
  - Smiling Cookies. Andrew Fort
  - YubiKey 2.0. Yubico
  - Hamlet. Dave Hamster
  - Post it. Eileen Kramer
  - Big Cookie. Glenn Fleishman
  - Tetris. Jameson Gagnepain
  - CERN. Artur Wiecek
  - Talk nerdy to me. Stacie Biehler
  - Eric Cantona. Duncan Hull
- Other:
  - Broken Bridge. Andreas Grabner