

AA enabling a closed source legacy application

Jan Du Caju

ICT security officer

K.U.Leuven

Belgium

AA enabling a closed source legacy application

Introduction: context association K.U.Leuven

Case: AA enabling SAP

The gory details: configuring the components

General: AA enabling by means of a reverse
proxy

Conclusions

AA enabling a closed source legacy application

Introduction: context association K.U.Leuven

Case: AA enabling SAP

The gory details: configuring the components

General: AA enabling by means of a reverse proxy

Conclusions

Introduction: context association K.U.Leuven

educational landscape reflects
political situation



association K.U.Leuven
1 university and 12 schools
of higher education

Need for resource sharing

2004: Shibboleth for institutional
and inter-institutional web
resources



Introduction: context association K.U.Leuven

Every institution of association K.U.Leuven has its own central AAI (Authentication and Authorization Infrastructure incl. Shibboleth IdP)

Resources

e-learning: Blackboard and other coupled education apps

library: Ex Libris, and access to scientific papers, publications and databases

work place context: Horde webmail, groupware and inter-institutional offers

research context: HPC et al

administrative and organizational context: SAP

Federations

K.U.Leuven (institutional)

Association K.U.Leuven

K.U.Leuven - UZLeuven (university hospital)

Not yet :-\ a national federation at NREN level (Belnet)

AA enabling a closed source legacy application

Introduction: context association K.U.Leuven

Case: AA enabling SAP

The gory details: configuring the components

General: AA enabling by means of a reverse
proxy

Conclusions

Case : AA enabling SAP

Administrative and organizational applications: SAP

K.U.Leuven: Campus management, HR, FI, ...

Corona project: 6 institutions of association K.U.Leuven for implementing SAP campus management

SAP access control possibilities

Basic authentication

Digest

Form

Client certificate

Evaluate assertion ticket (SAML)

SAPssoTicket

Goals:

password does not pass the application

use an AAI component

Case: AA enabling SAP

SAP access control via evaluation of an assertion ticket

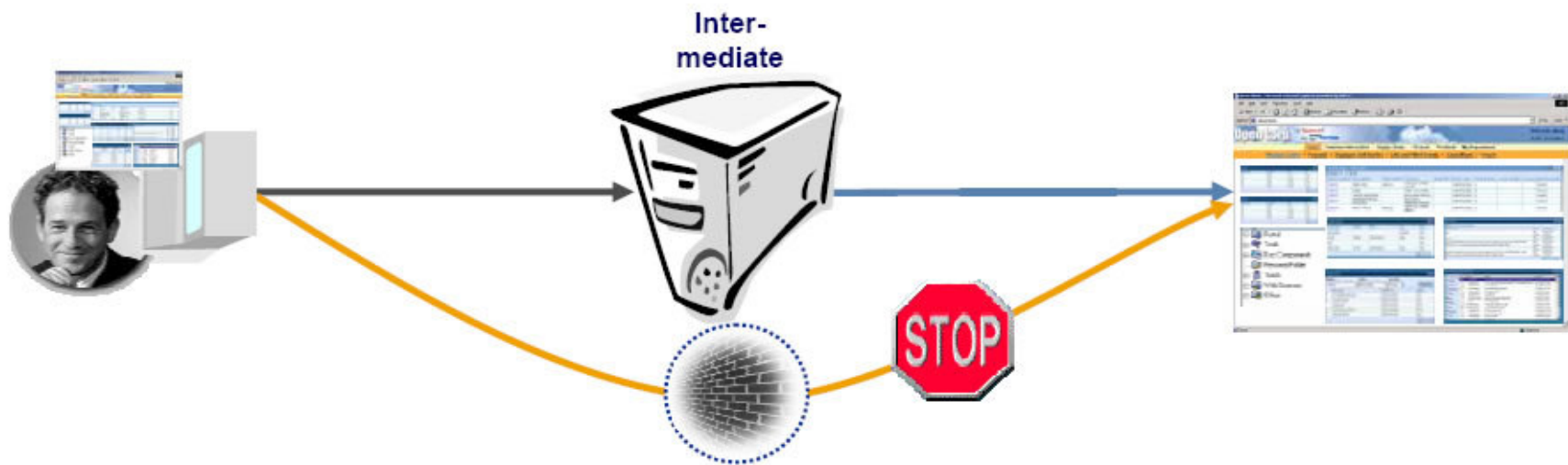
Problem: SAP speaks a subset of SAML1.1 :-)

- Assertions must not contain the elements Condition and AudienceRestrictionCondition
- Assertions must have exactly one AuthenticationStatement element which must have a NameIdentifier element
- If present, the elements AuthorizationDecisionStatement and AttributeStatement are ignored
- Creating or verifying digital signatures is not supported

SAP considers to implement SAML2.0 sometime in the future :-)

Case: AA enabling SAP

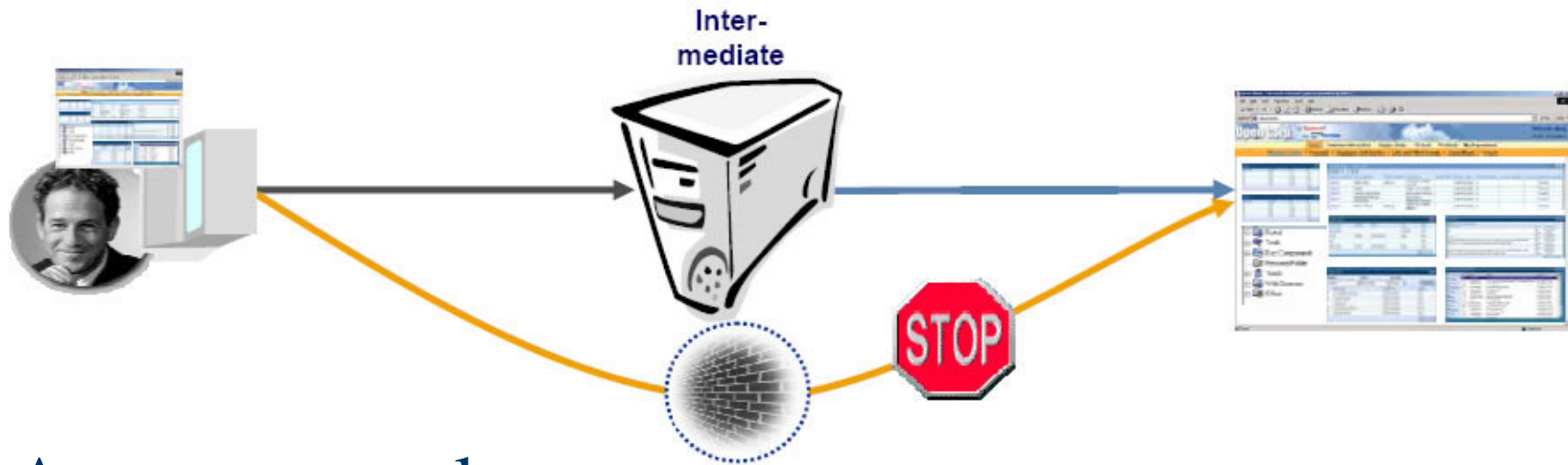
Shibboleth enabled reverse proxy in front of SAP servers



Extra layer of security

Usage of AAI Shibboleth component for general access control

Case: AA enabling SAP



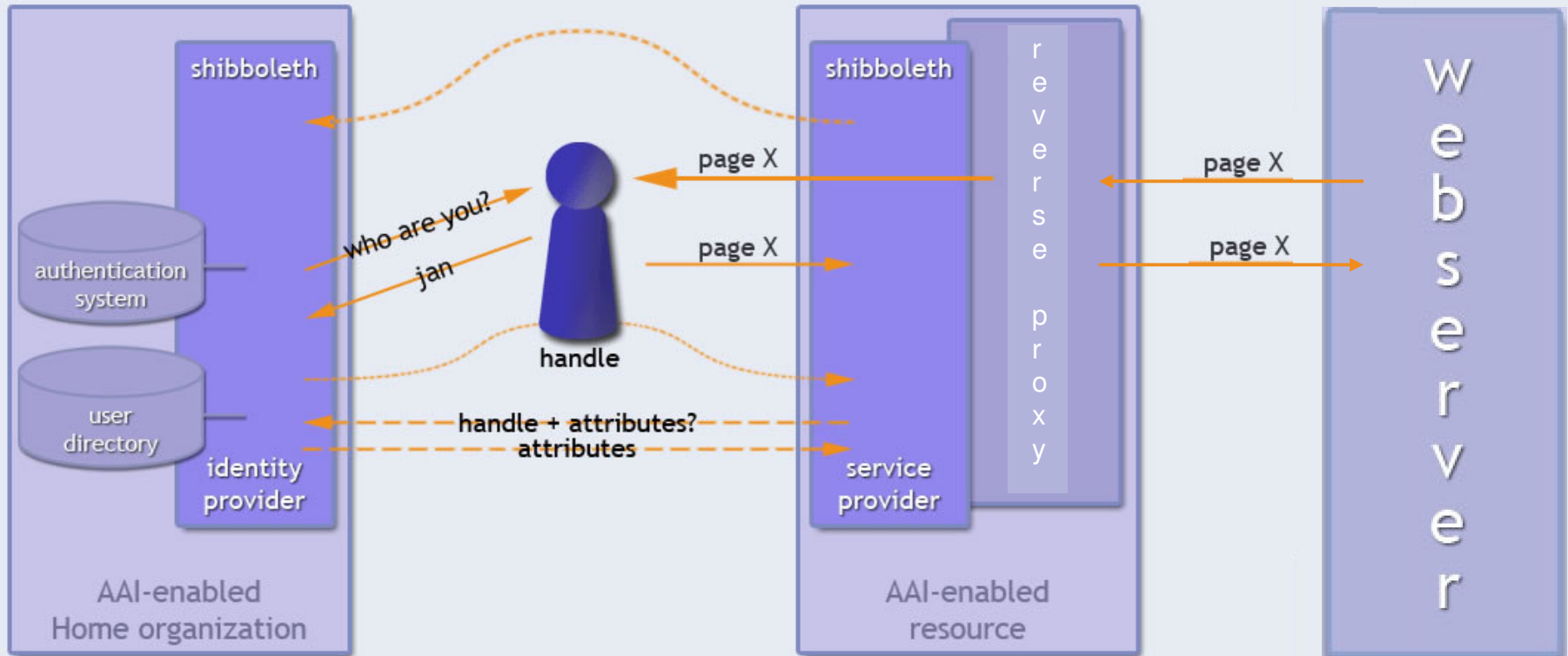
Access control

Reverse proxy access control via Shibboleth
(mod_shib)

Only general access control, application specific authZ
remain in application

SAP access control via a valid SAPsoticket obtained
at J2EE-engine (SAP portal)

Case: AA enabling SAP



Access control via SAP SSO ticket

JAVA and ABAP web apps

access via browser

SAP SSO ticket in cookie

ABAP non-web apps

access via a client: SAPgui

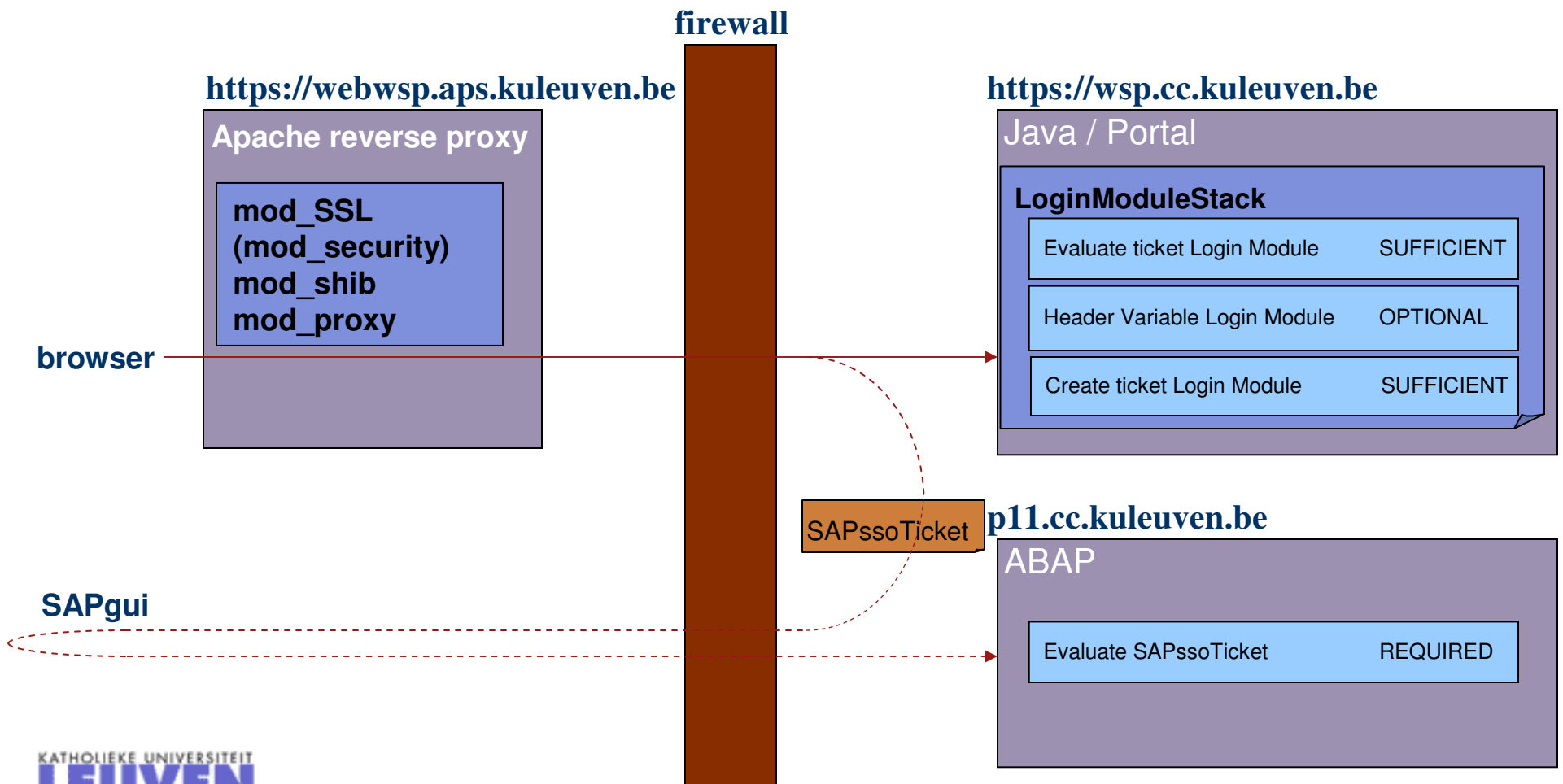
link or URL (in SAP portal) to a SAPgui Shortcut file

associated in Windows with the SAPgui client

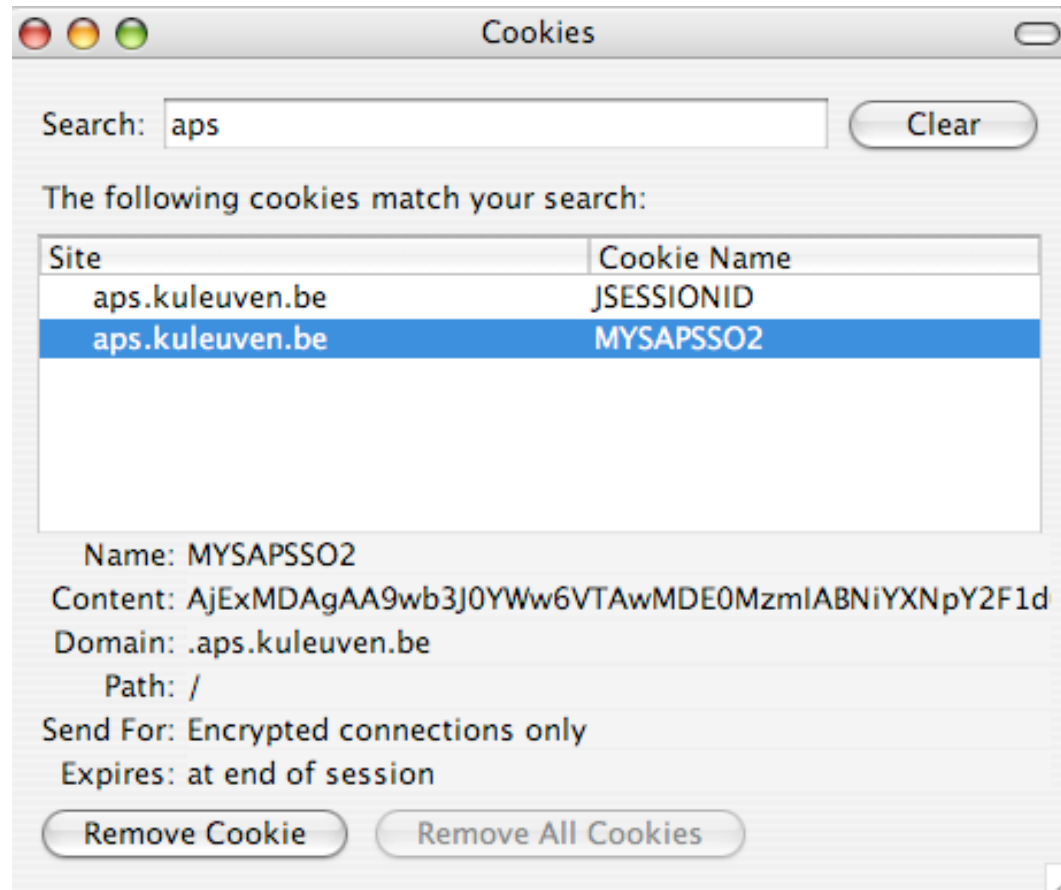
contains SAP SSO ticket

Accessing SAP applications

JAVA and ABAP web apps (link in SAP portal or in WAS)
 ABAP non-web app via link to a SAPgui shortcut file



Accessing SAP JAVA and ABAP web apps



AA enabling a closed source legacy application

Introduction: context association K.U.Leuven

Case: AA enabling SAP

The gory details: configuring the components

General: AA enabling by means of a reverse
proxy

Conclusions

Configuration overview

Communication reverse proxy and SAP portal:

Vhost `webwsp.asp.kuleuven.be`

Adjusting SAP LoginModuleStack

Configuration of access to SAP servers

SAP transactions : `rz10` and `strustsso2`

Vhost webwsp.aps.kuleuven.be

SSL enabled

```
# communication to browser
SSLEngine On
SSLCertificateFile /etc/pki/webwsp.aps.kuleuven.be.crt
SSLCertificateKeyFile
    /etc/pki/webwsp.aps.cc.kuleuven.be.key
# mutual certificate authentication with SAP
SSLProxyEngine On
SSLProxyCACertificateFile /etc/pki/ca-bundle.crt
SSLProxyMachineCertificateFile /etc/pki/webwsp.pem
SSLProxyVerify require
SSLProxyVerifyDepth 3
```

Vhost webwsp.aps.kuleuven.be (continued)

Protected with Shibboleth

authorization based on affiliation

header shib-person-uid must be set

```
<Location />  
AuthType shibboleth  
ShibRequireSession on  
require affiliation member  
</Location>
```

Reverse proxy

```
ProxyPass / https://wsp.cc.kuleuven.be:8098/ retry=2  
ProxyPassReverse / https://wsp.cc.kuleuven.be:8098/  
ProxyVia Off  
ProxyPreserveHost On
```

Login Module Stack of J2EE - engine

Visual administrator

Security Provider

SAP-J2EE-engine

| Login Modules | Flag | Options |
|---|------------|---|
| com.sap.security.core.server.jaas.EvaluateTicketLoginModule | SUFFICIENT | {ume.configuration.active=true} |
| com.sap.security.core.server.jaas.HeaderVariableLoginModule | OPTIONAL | {ume.configuration.active=true, Header=shib-person-uid} |
| com.sap.security.core.server.jaas.CreateTicketLoginModule | SUFFICIENT | {ume.configuration.active=true} |

transaction rz10

Allow access with SAPssotickets

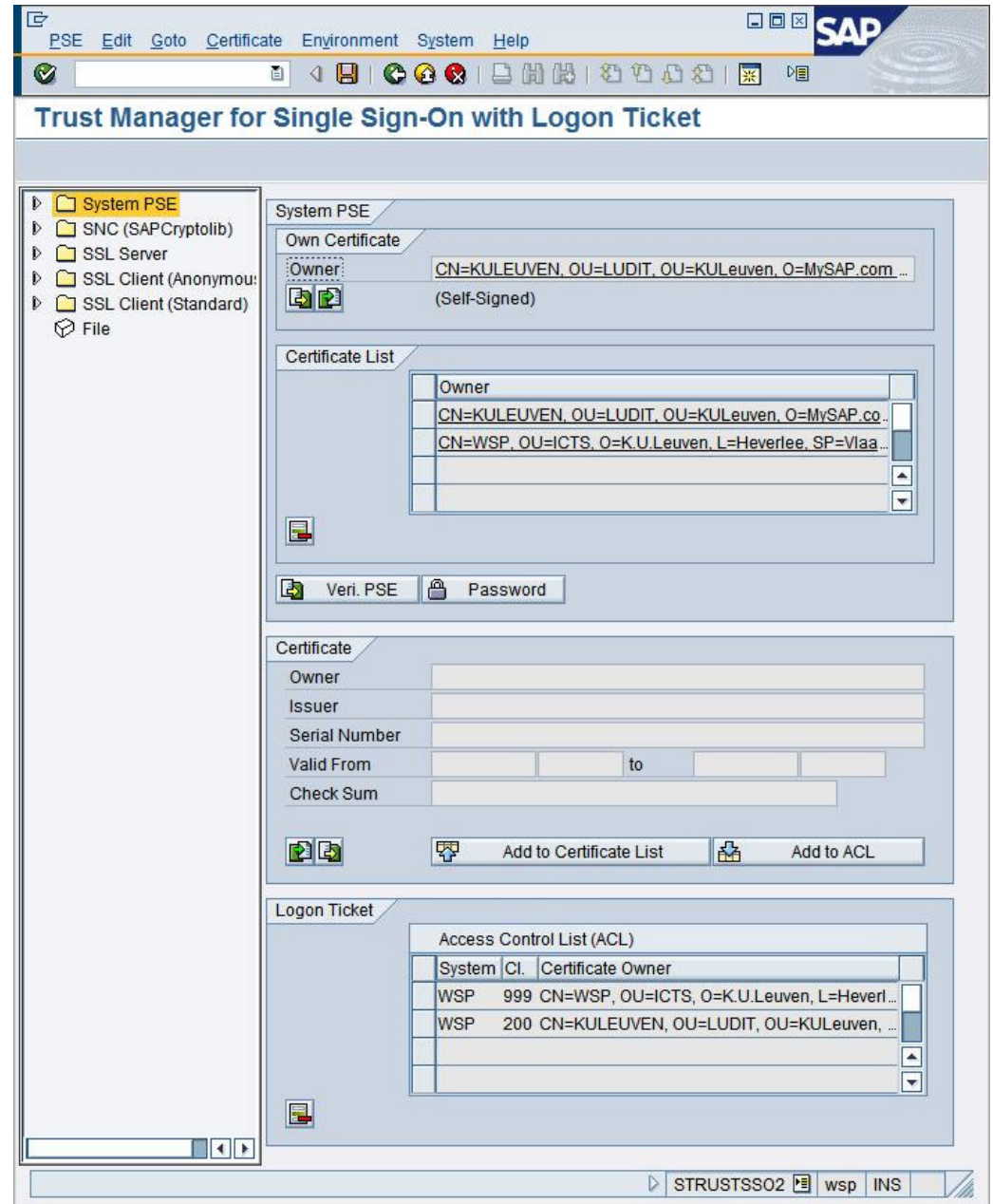
The screenshot displays the SAP transaction RZ10 interface. The title bar reads 'Display Profile 'DEFAULT' Version '000079''. The main area shows a table with one row of parameter data:

| Parameter name: | Status | Seq. no. |
|--------------------------|--------|----------|
| login/accept_sso2_ticket | Active | 16 |

Below the table, the 'Parameter val.' field contains the value '1'. The 'Unsubstituted standard value' and 'Substituted standard value' fields also contain '1'. The 'Comment' field is empty. The status bar at the bottom shows 'RZ10' and 'wsp INS'.

transaction strustsso2

Configure which
SAPsotickets are
allowed (signed by)



AA enabling a closed source legacy application

Introduction: context association K.U.Leuven

Case: AA enabling SAP

The gory details: configuring the components

General: AA enabling by means of a reverse proxy

Conclusions

AA enabling via reverse proxy

remote_user in backend server

- complex rewrite rules
- use another header variable released by IdP
e.g. shib-person-uid

Security (spoofing): only uid is passed no password

- mutual certificate authentication between proxy and backend server
- persistent connection over ssl (keep-alive) is not yet :-/ possible with Apache mod_proxy
- firewall filtering

AA enabling a closed source legacy application

Introduction: context association K.U.Leuven

Case: AA enabling SAP

The gory details: configuring the components

General: AA enabling by means of a reverse proxy

Conclusions

Conclusion

AA enabling a closed source legacy application

- dependent on application
- one possibility: by means of a Shibboleth enabled reverse proxy in front of the app

Credits

Philip Brusten

Jan Van der Velpen

URL's

<http://kuleuven.be/english>

<http://associatie.kuleuven.be/eng>

<http://shib.kuleuven.be>