

AAI: SAP NETWEAVER INTEGRATION

André Hunziker and André Wahlig, ETH Zürich ID-BI – Februar 2010



Agenda

- **ETH Zürich**
 - Company profile
- **Introduction / Starting Point**
 - ETHZ SAP System Landscape
 - 3rd party SSO solution – selection process and solution
- **SAML Implementation**
 - SAP SAML support and configuration
 - Shibboleth Identity Provider 2.x custom configuration
 - Lessons learned
 - SAP SAML roadmap

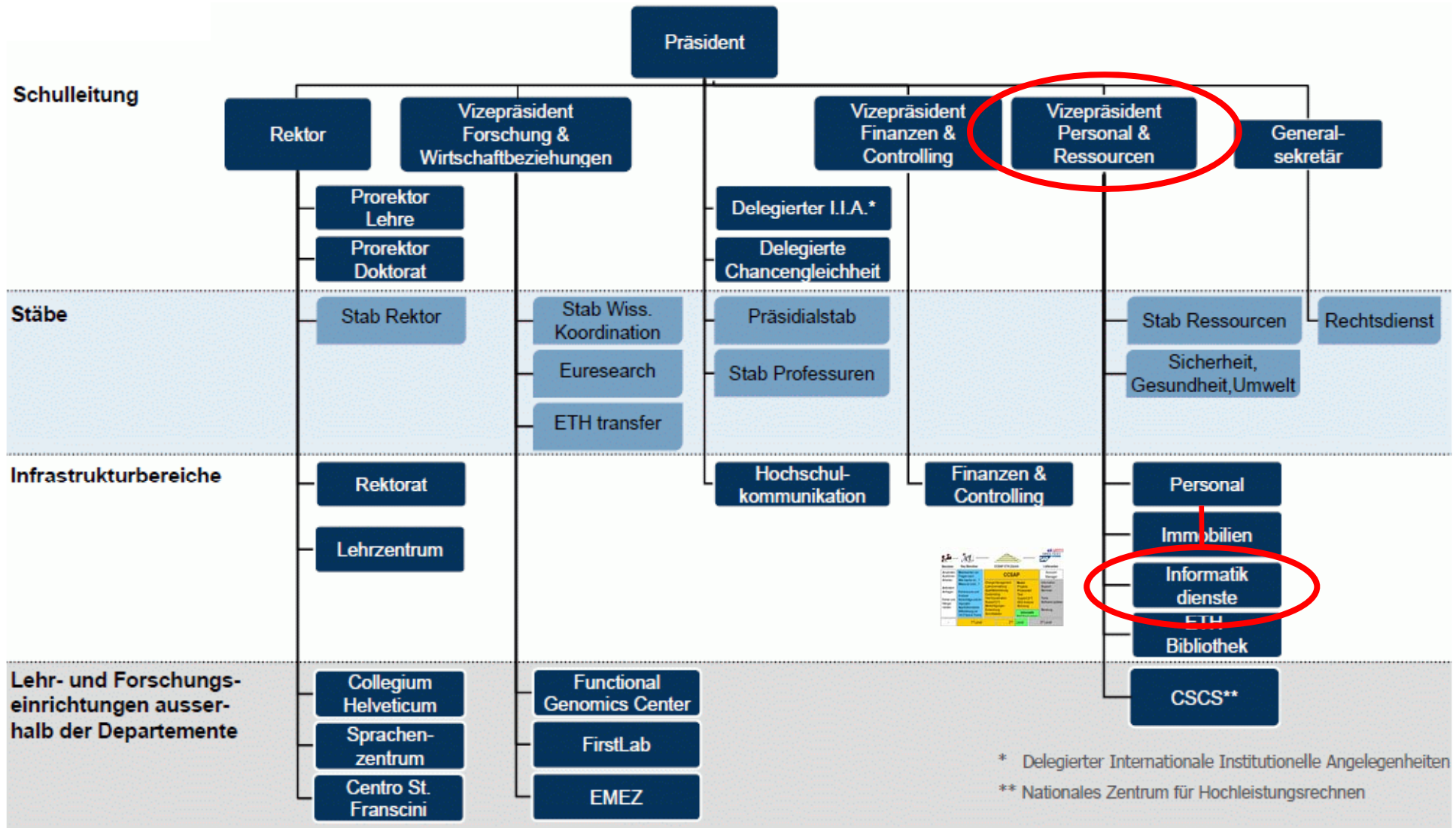
Campus City Zürich (Headquarters)



New Campus Science City



Organisation (01.10.2008)



* Delegierter Internationale Institutionelle Angelegenheiten

** Nationales Zentrum für Hochleistungsrechnen

Mission and Application ETH Zürich

[ref: <http://www.ethz.ch/about/missionstatement>]

■ Mission

- ETH Zurich imparts to its students the highest state of knowledge and practical skills. It seeks to enable young people to find their orientation in a complex and rapidly changing world, ...

■ Commitment

- In education, research, and services the ETH Zurich measures itself against the highest recognized international standards. It promotes science and scientific activity for their own sakes, ...

■ Application

- **Education:** The basis of education at ETH Zurich is formed by the core areas of engineering, ...
- **Research:** At the ETH Zurich teaching and research are closely linked. Equal standing is assigned ...
- **Location Zurich:** ETH Zurich benefits greatly from Zurich's urban setting. It feels closely tied to and responsible towards the city and ...

Facts and Figures ETH Zürich

■ Akademie

- Professuren 372
- Studenten 15'000

■ Organisation

- Organisationseinheiten: ~ 1'000 (Kostenstellen)
- Mitarbeiter: 9'000 [7'000 FTE]
- Gegründet 1855 als Polytechnische Hochschule Zürich
- Zwei Zentren/Lokationen, 150 Gebäude (alle in Zürich)

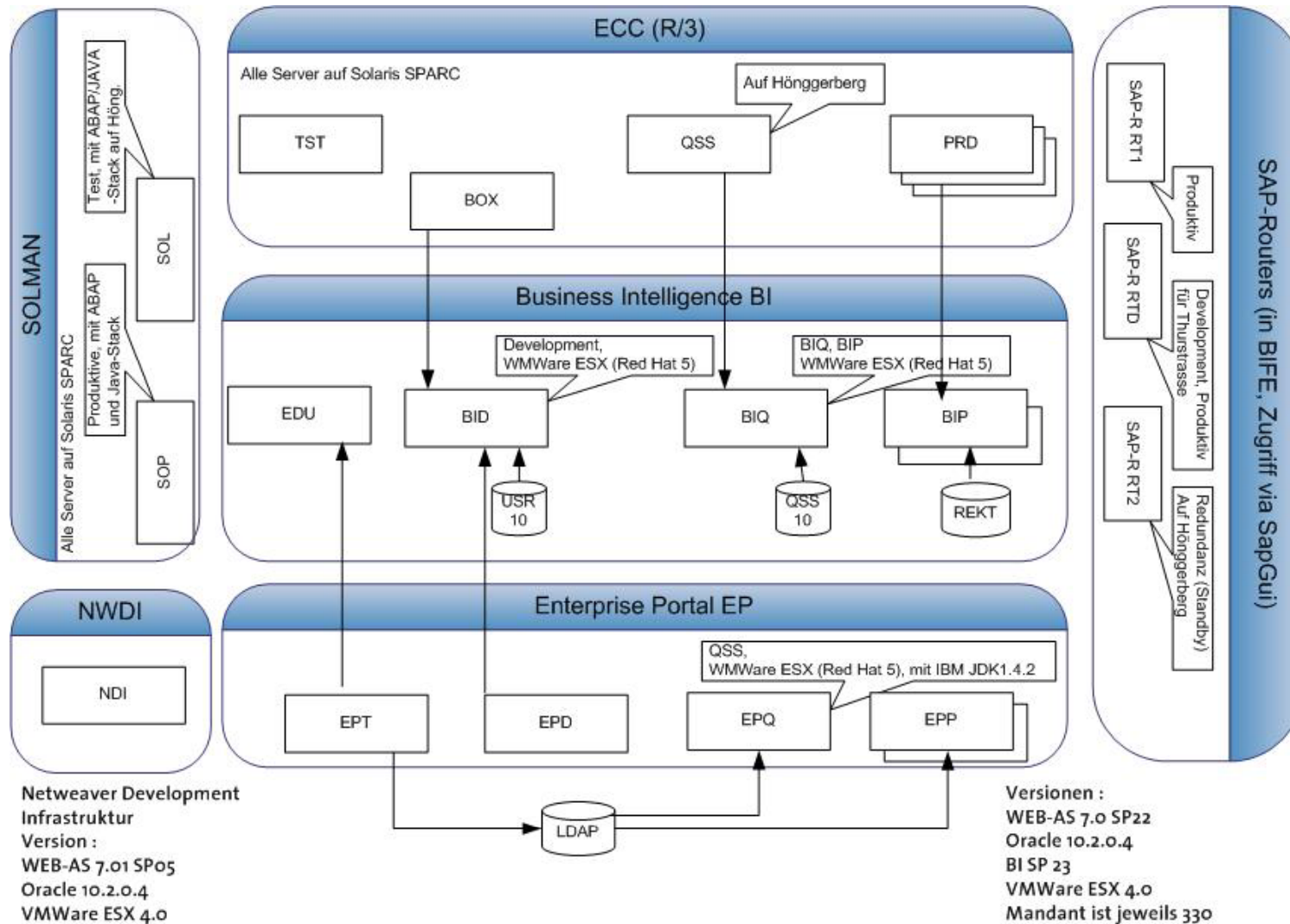
■ Finanzen

- 1.25 Mia CHF Jahresbudget [0.8 Mia EUR]
- ~ 20% finanziert über Drittmittel und Funds rising

Ausgangslage

- **Prozesse welche mit SAP abgewickelt werden**
 - «Nur» Support Prozesse in den Verwaltungseinheiten
 - **Finanzen** (Kreditoren, Debitoren, Anlagenwirtschaft, Steuern, Controlling, Budgetierung, Kameralistik (Fonds Management))
 - **Personal** (Pers. Management, Payroll, Org. Management)
 - **Logistik** (Material Management, S& D, Inventar)
- **Verantwortlichkeit**
 - Support: Support Desk, End-User Schulung, Applikationsbetrieb
 - Projekte: Eigenentwicklungen, Prozessberatung, Customizing
 - Externe Consultants: Überwachen / Qualitätssicherung externe Berater
 - Vertrag: SAP Lizenzverwaltung, Information/Koordination
 - Common Tasks: Strategiemsetzung/Beratung, interne Koordination von übergreifenden Vorhaben
- **SAP Environment**
 - SAP R/3, 3'000 named User, ABAP, JAVA

ETHZ SAP system landscape



Challenge and possible solutions

- **SAP NetWeaver Portal 3rd partySSO Connection**
 - External Webapplication
 - PHP application with SOAP support
- **SWITCH/Shibboleth integration**
 - Via header variable or SAML assertions
- **SAP WebServer Filter for SSO with Non-SAP Applications**
 - Old SAP standard – no further development (SAP Note 442401)
- **SAP Ticket Library**
 - Needs to be developed in 3rd party application (only Java and C)
- **Encrypted Link**
 - Custom development solution

Solution

■ SAML assertions

■ Use

You can use SAML for Single Sign-On in a scenario where a user is authenticated on an external authentication system that acts as an SAML authority. Based on this authentication, the user receives an SAML assertion (upon request) that he or she can use to access the AS Java.

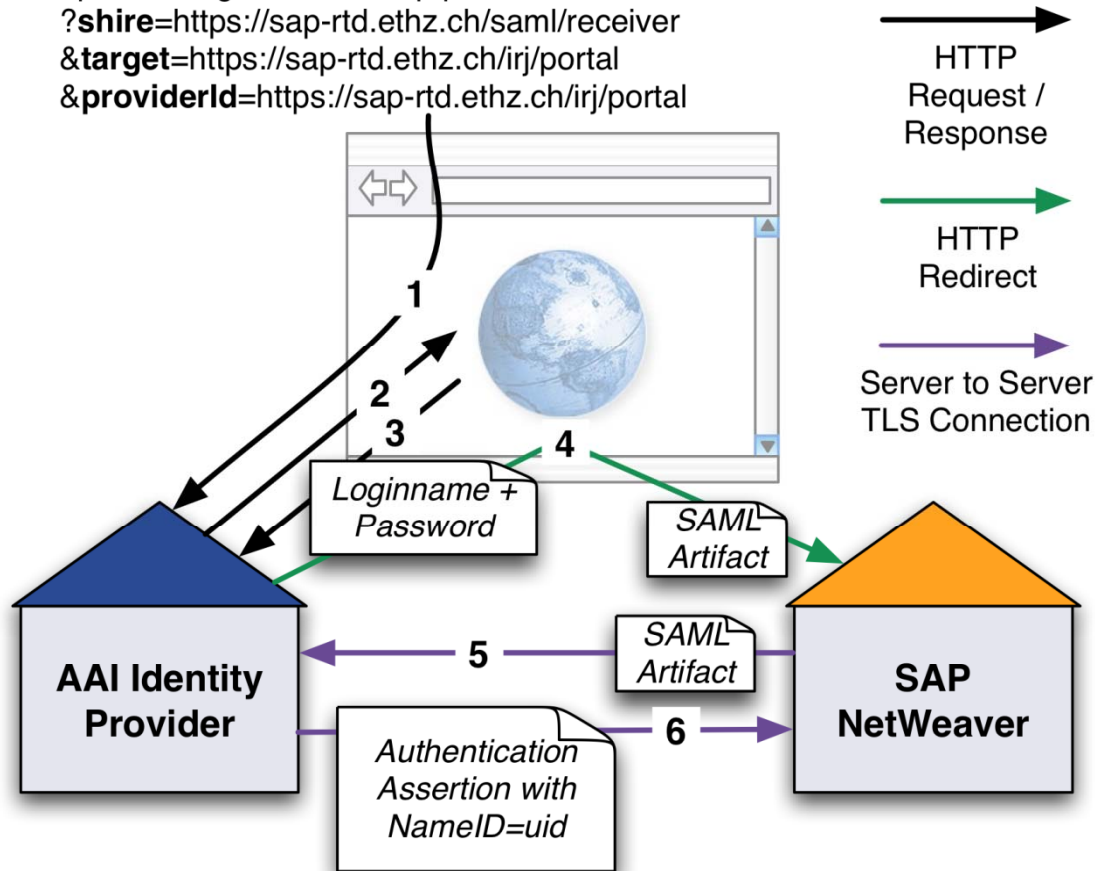
■ Prerequisites

- Assertions must have exactly one AuthenticationStatement element. The authentication statement must have a NameIdentifier element.
- To protect the data exchange, SSL is required for the connection between the source and destination sites

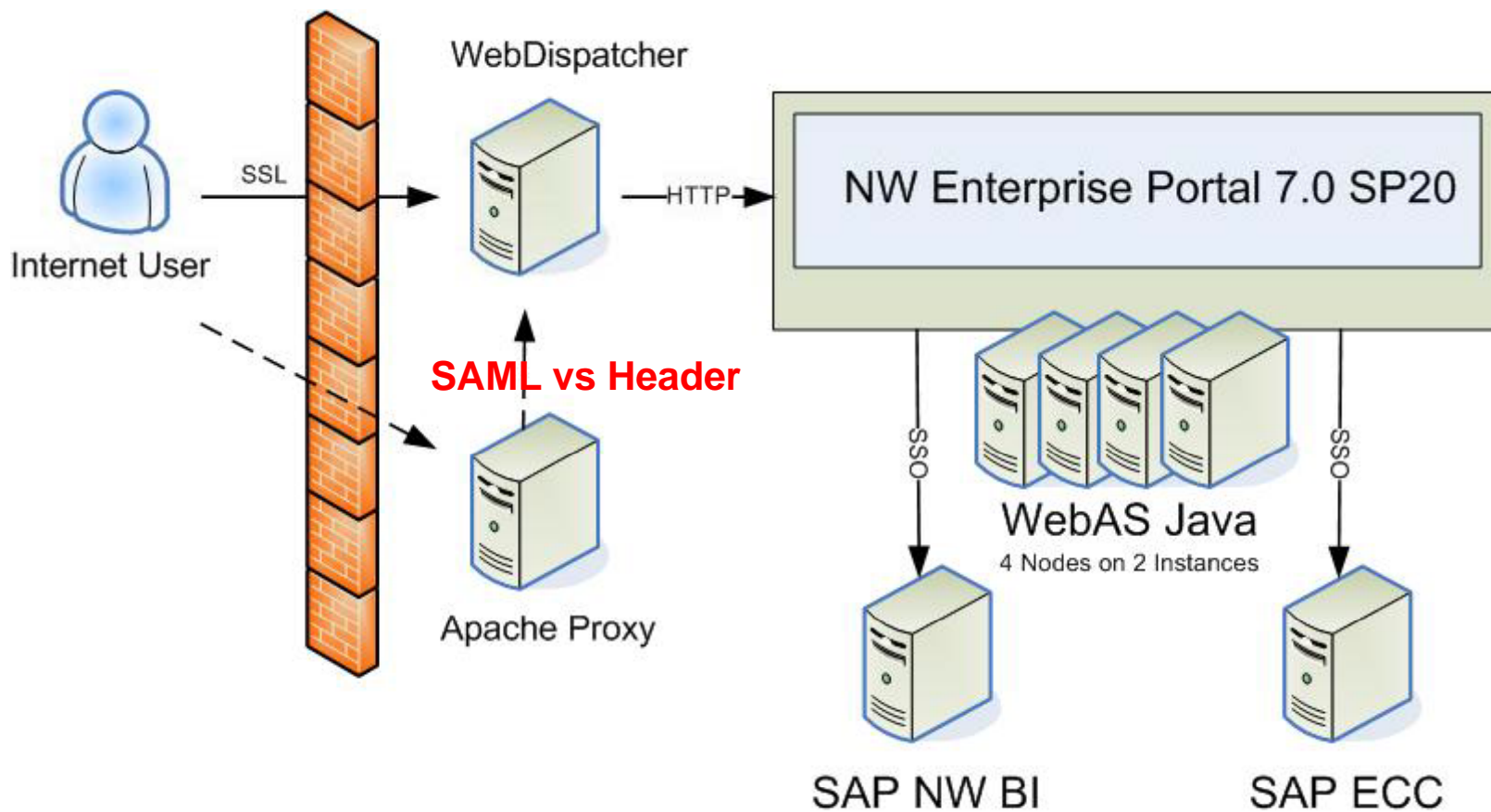
■ SAP Help: http://help.sap.com/saphelp_nw70/helpdata/en/d0/a3d940c2653126e10000000a1550b0/frameset.htm

SAP NetWeaver SAML 1.0 support (09/2009)

https://aai-logon.ethz.ch/idp/profile/Shibboleth/SSO
 ?shire=https://sap-rtd.ethz.ch/saml/receiver
 &target=https://sap-rtd.ethz.ch/irj/portal
 &providerId=https://sap-rtd.ethz.ch/irj/portal



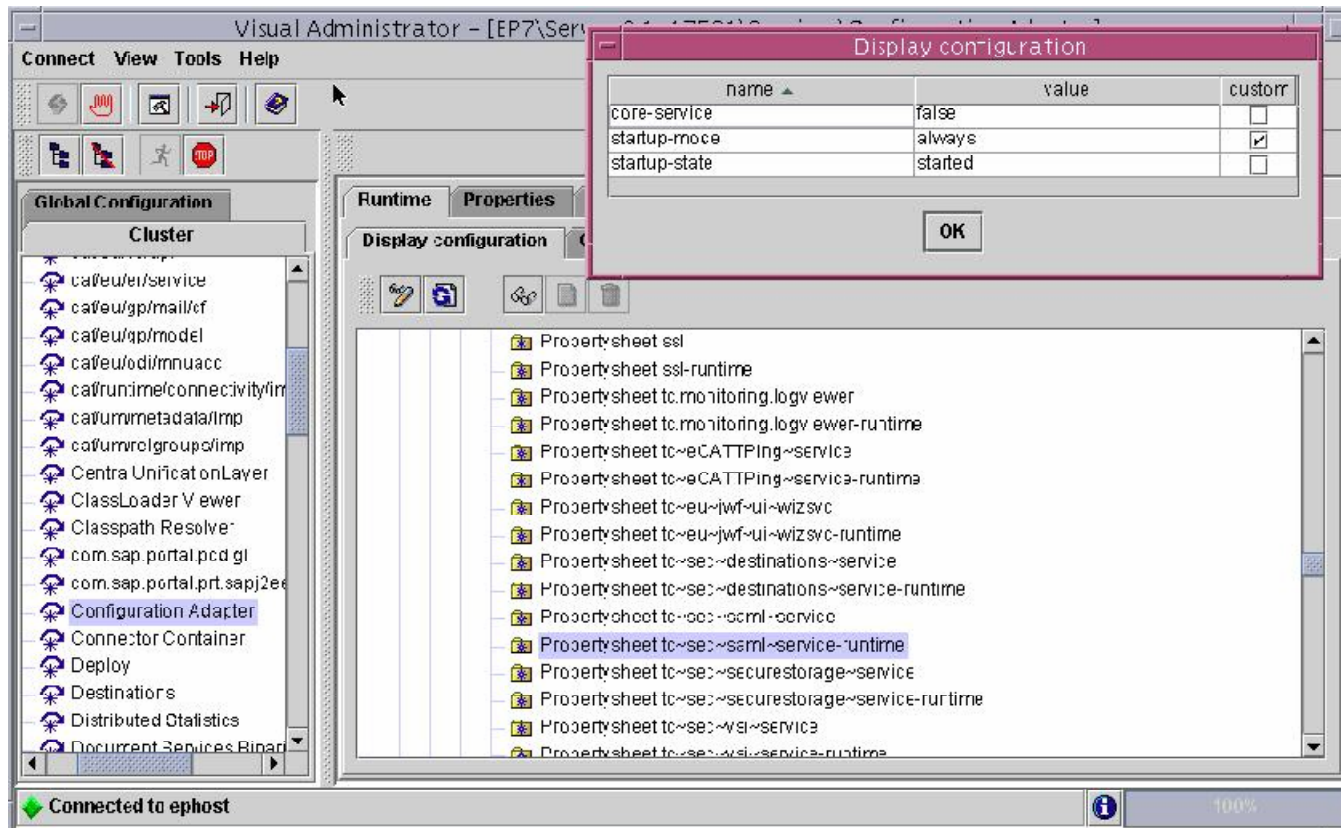
ETHZ SAP use case



SAP SAML configuration - overview

- **Change the startup mode for SAML service**
- **Create SWITCH compatible certificate for Shibb. Auth.**
- **Create HTTP destination for IdP**
- **Configure SAML service parameter**
- **Add SAML login module stack**

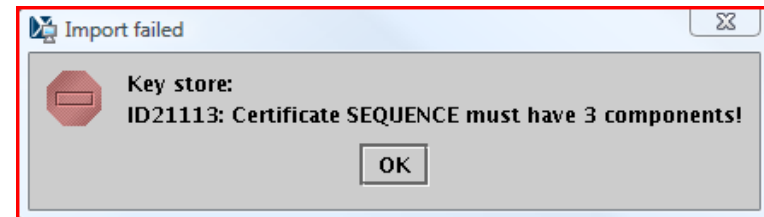
SAP SAML configuration – SAML Service



SAP SAML configuration – create Certificate

■ Create Certificate (no SAP NW VA standard)

- `./keygen.sh -y 3 -h #HOSTNAME# -e #ENTITYID#`
where `#ENTITYID` usually is `https://#HOSTNAME#/shibboleth`
- `./keygen.sh -y 3 -h sap-epq.ethz.ch -e https://sap-epq.ethz.ch:50001/irj/portal`
- Result: `sp-cert.pem` und `sp-key.pem`



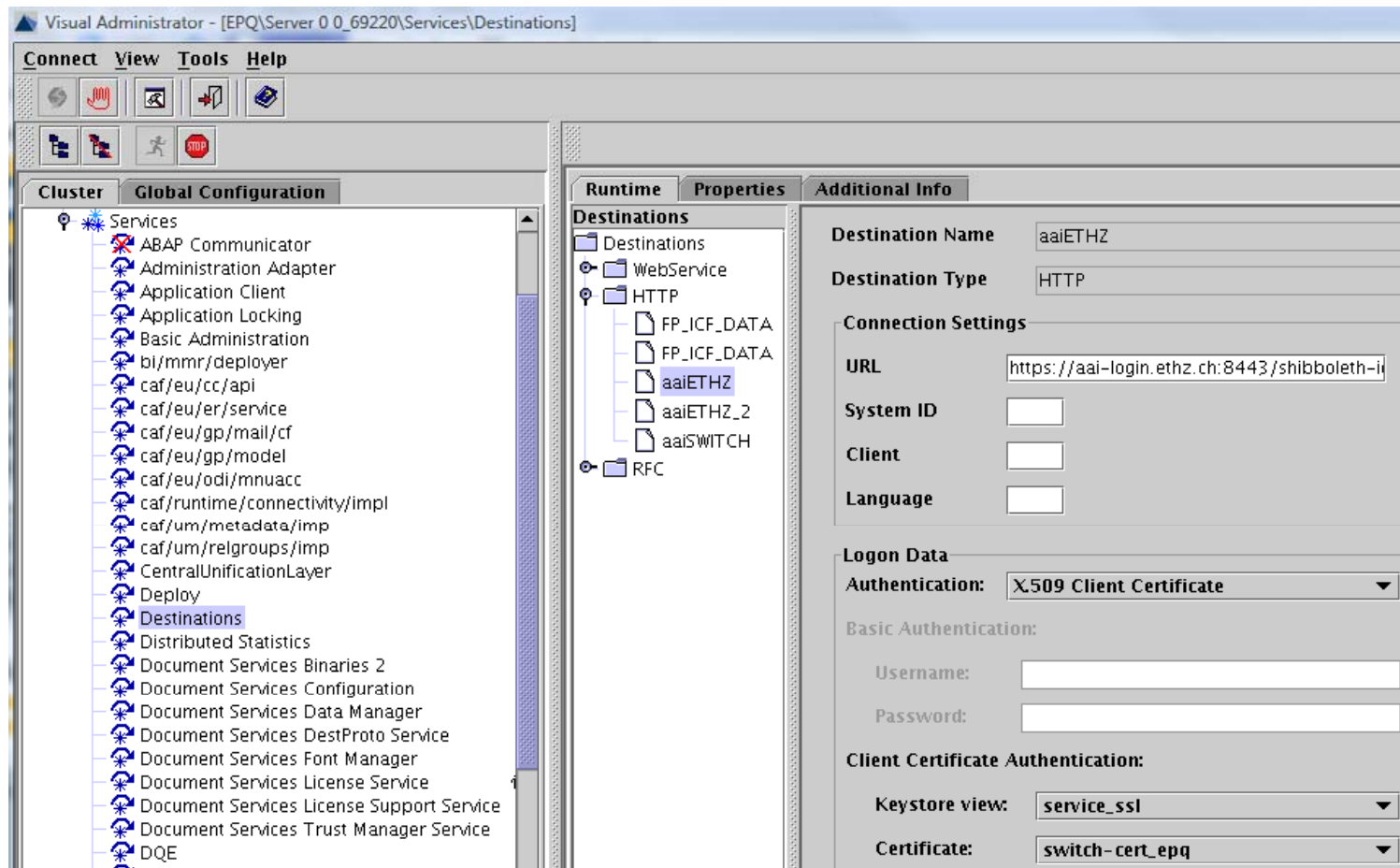
■ pkcs #12 certificate

- `C:\Openssl\bin\openssl.exe pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in <Public Certificate Filename> -inkey <Private Key Filename> -out <PKCS#12 Filename> -name "<Display Name>"`
- `openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in sp-cert.pem -inkey sp-key.pem -out switch-cert_tmp1.pfx -name "switch-cert2"`

SAP SAML configuration – create Certificate

- **Load Certificate into NW key store**
 - Server -> Key Storage -> service_ssl: Entry -> Load “switch-cert2.pfx”
- **Get fingerprint for Shibboleth config**
 - openssl x509 -fingerprint -sha1 -in /path/to/the/certificate.pem
 - sap-epq:eptadm 60> openssl x509 -fingerprint -sha1 -in sp-cert.pem

SAP SAML configuration – HTTP destination



SAP SAML configuration – SAML service

The screenshot shows the SAP Visual Administrator interface. The left pane displays a tree view of services, with 'Configuration Adapter' selected. The right pane shows the configuration details for the 'aaiETHZ' SAML service under the 'PartnersInbound' configuration.

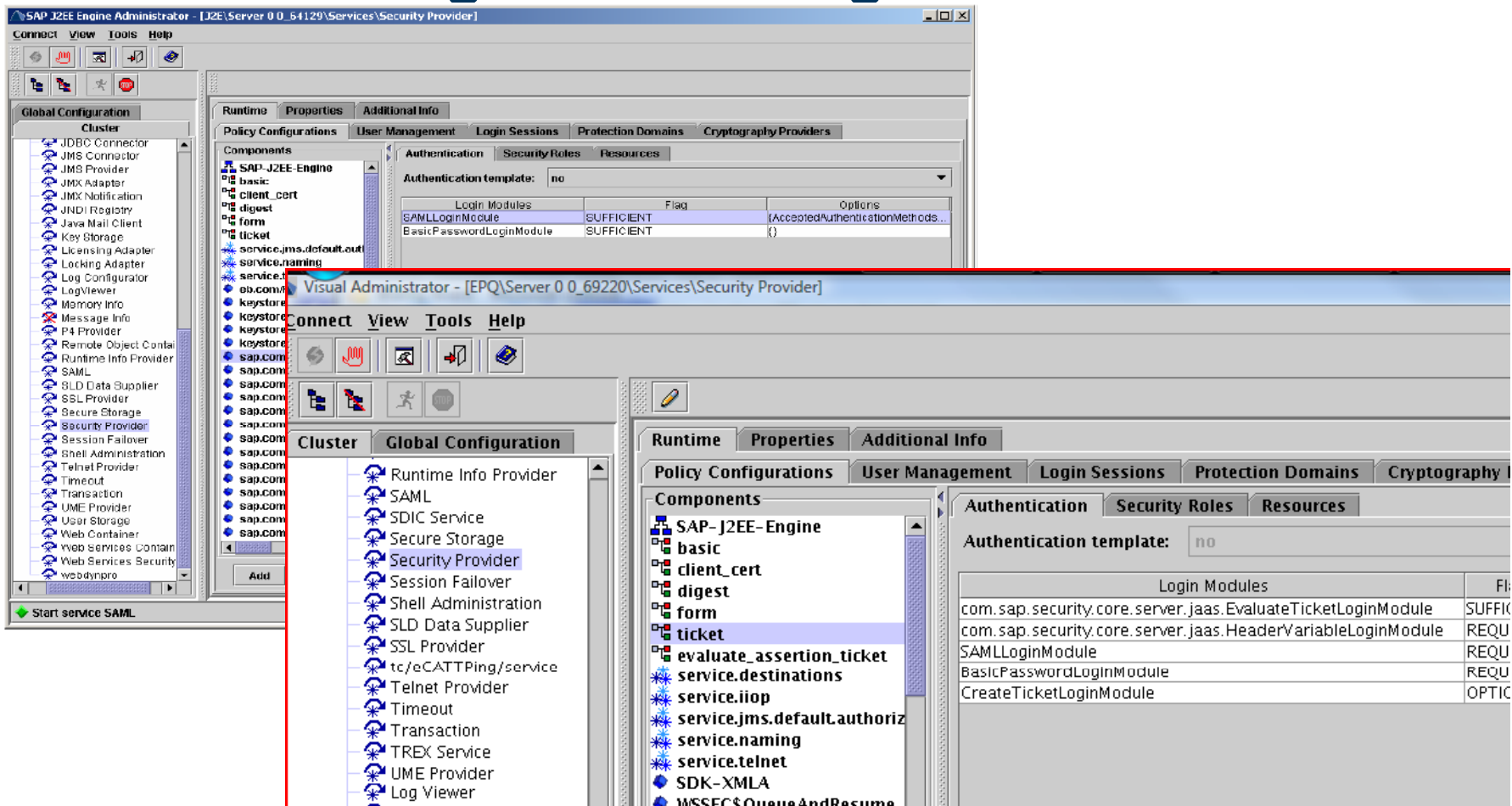
Configuration Details:

- Active = true
- DestinationName = "aaiETHZ"
- ParameterNameTarget = "TARGET"
- RequestVersion = "1.0"
- SourceID = "B64:YsGMvNomGf3Vixqg8psxu3wwlI8="

Other Settings:

- ParameterNameArtifact = "SAMLart"
- PermitInsecureConnections = true

SAP SAML configuration – Login module



- Adjust Firewall rules

Shibboleth Identity Provider 2.x custom configuration

- Create a metadata file for the SAP service as you would for standard Service Provider. Important is to include a custom NameIDFormat for in the EntityDescriptor, e.g.:

```
<NameIDFormat>urn:mace:switch.ch:aitest:namelidentifier:principal</NameIDFormat>
```

- Add <Metadataprovider> to relying-party.xml to load local metadata file with custom NameIDFormat value. E.g. with

```
<MetadataProvider  
id="FSMD-ETH-SAP"  
xsi:type="FilesystemMetadataProvider"  
xmlns="urn:mace:shibboleth:2.0:metadata"  
metadataFile="/opt/shibboleth-idp/metadata/metadata.sap.xml" />
```

- Extend the attribute-resolver.xml to configure an attribute that shall be used as SAP user name by adding a NameID encoder to the 'uid' or another AttributeDefinition:

```
<resolver:AttributeEncoder  
xsi:type="SAML1StringNameIdentifier"  
xmlns="urn:mace:shibboleth:2.0:attribute:encoder"  
nameFormat="urn:mace:switch.ch:aitest:namelidentifier:principal" />
```

Lessons Learned

- **Get all needed config data before starting implementation**

- **Pain Points**
 - AAI Session TimeOut 30min – could be increased
 - Disabled IPv6 on SAP server
 - Login Screen changes for SAP Portal

SAP SAML 2.0 support

FOCUS AREAS

- SOA Security → Enable secure and interoperable integration in SAP landscapes and heterogeneous environments
- Identity Management → Reduce TCO and administrative effort by central maintenance. Added value via business suite scenarios and compliant user provisioning with GRC
- Integrated Security Management → Ensure consistency and compliant security for business processes in distributed environments

RELEASE PLAN

2008	2009	2010
◆	SAP NetWeaver IDM 7.1	
	SAP NetWeaver 7.2 ◆	
	SAP NetWeaver IDM 7.2	◆
SAP Business Suite 7 Innovations 2010 ◆		

DETAILS	2008/PLANNED 2009	PLANNED (>2009)	VISION
SOA SECURITY	<ul style="list-style-type: none"> ■ Enhanced support for web services security standards ■ Standards-based principle propagation via SAML auth tokens 	<ul style="list-style-type: none"> ■ Identity Federation via SAML 2.0 and Security Token Service implementation ■ Further WS Sec standards support, e.g. WS-Trust, WS-Sec.Conversation 	<ul style="list-style-type: none"> ■ Identity Hub for heterogeneous identity and access management
IDENTITY MANAGEMENT	<ul style="list-style-type: none"> ■ Central Identity Management 7.0 / 7.1 for heterogeneous landscapes ■ Compliant user provisioning via integration with GRC 	<ul style="list-style-type: none"> ■ Expansion of Suite and GRC integration in collaborative scenarios ■ Simplify role management and TCO reduction 	<ul style="list-style-type: none"> ■ Business process aware SAP NetWeaver IDM ■ SAP NetWeaver IDM assimilating heterogeneous landscapes ■ Security and SAP NetWeaver IDM to be integrated in to SAP NetWeaver BPM
INTEGRATED SECURITY MANAGEMENT	<ul style="list-style-type: none"> ■ Wizard based security configuration 	<ul style="list-style-type: none"> ■ Web Services Security Consumability ■ Centralized policy-based security administration 	<ul style="list-style-type: none"> ■ Optimized model driven security management leveraging content-fluent Common Process Layer

Questions and Answers

André Hunziker und André Wahlig, ETH Zürich Informatikdienste

Web: <http://www.sap.ethz.ch> / Mail: andre.hunziker@id.ethz.ch
andre.wahlig@id.ethz.ch

