ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

AAI: SAP NetWeaver Integration

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

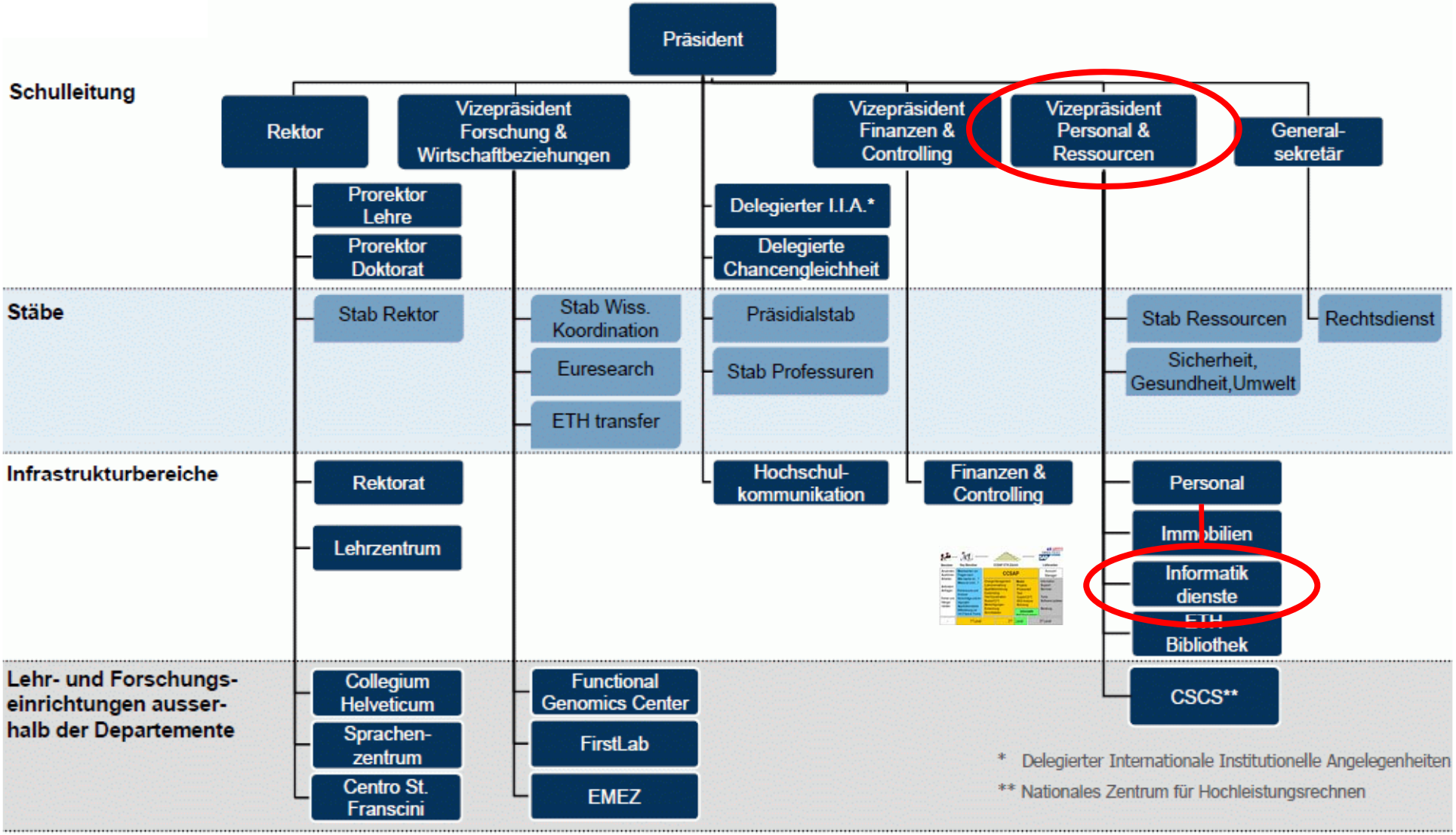
Agenda

- **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)



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 …
  - ….

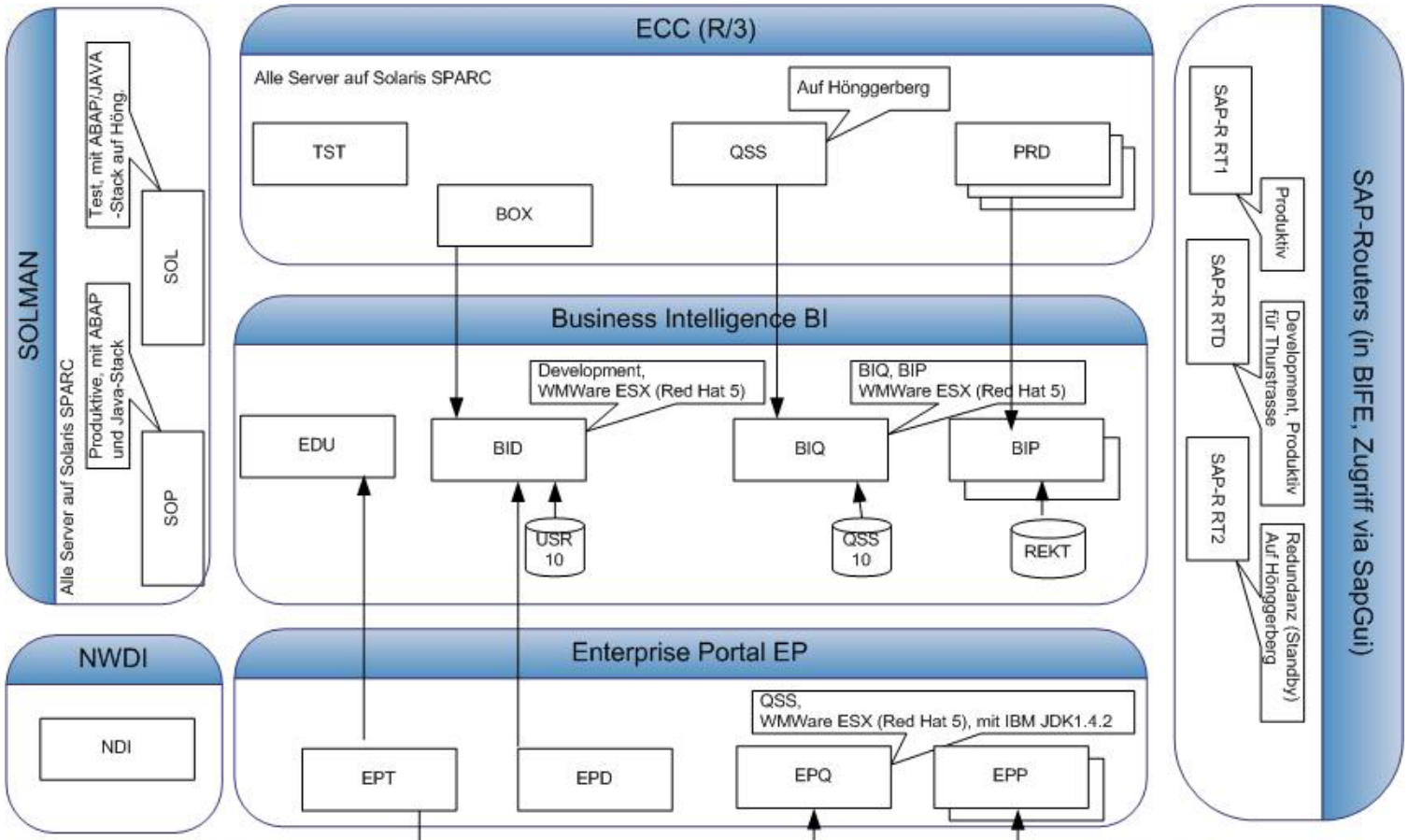
Facts and Figures ETH Zürich

- **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: Strategieumsetzung/Beratung, interne Koordination von übergreifenden Vorhaben
- **SAP Environment**
  - SAP R/3, 3’000 named User, ABAP, JAVA

ETHZ SAP system landscape



Netweaver Development Infrastruktur
Version :
WEB-AS 7.01 SP05
Oracle 10.2.0.4
VMWare ESX 4.0

Versionen :
WEB-AS 7.0 SP22
Oracle 10.2.0.4
BI SP 23
VMWare ESX 4.0
Mandant ist jeweils 330

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.

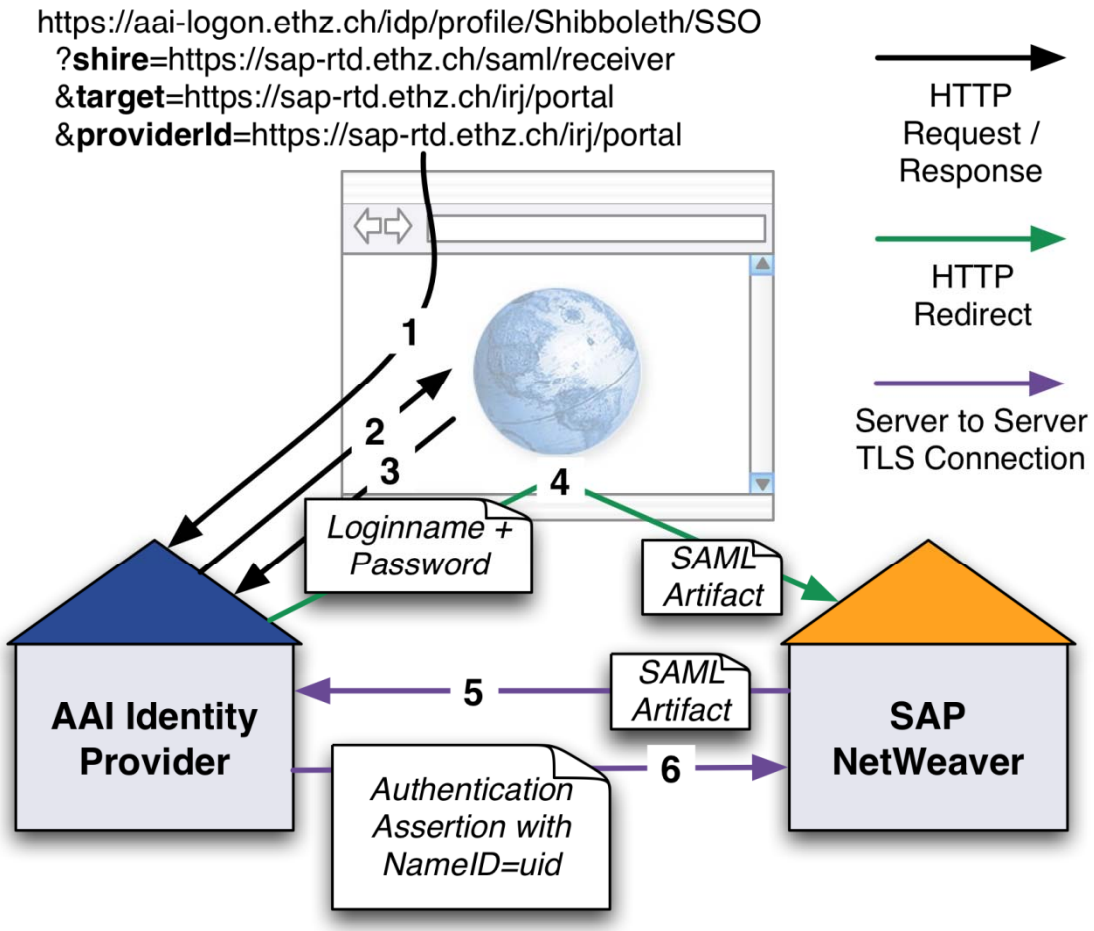
  - Prerequisites

    - Assertions must have exactly one AuthenticationStatement element. The authentication statement must have a NameIdentifier element.

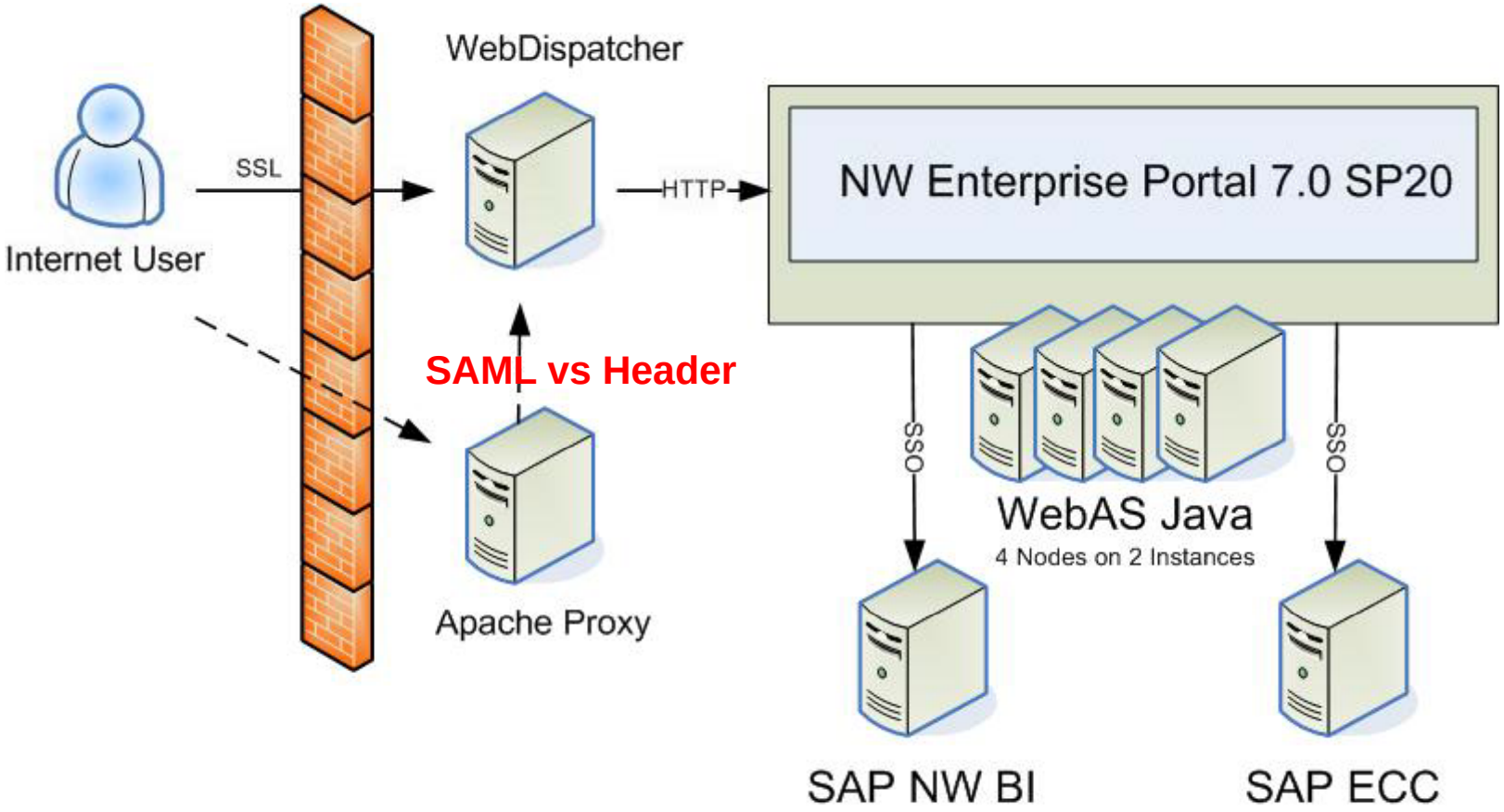
    - To protect the data exchange, SSL is required for the connection between the source and destination sites

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

SAP NetWeaver SAML 1.0 support (09/2009)



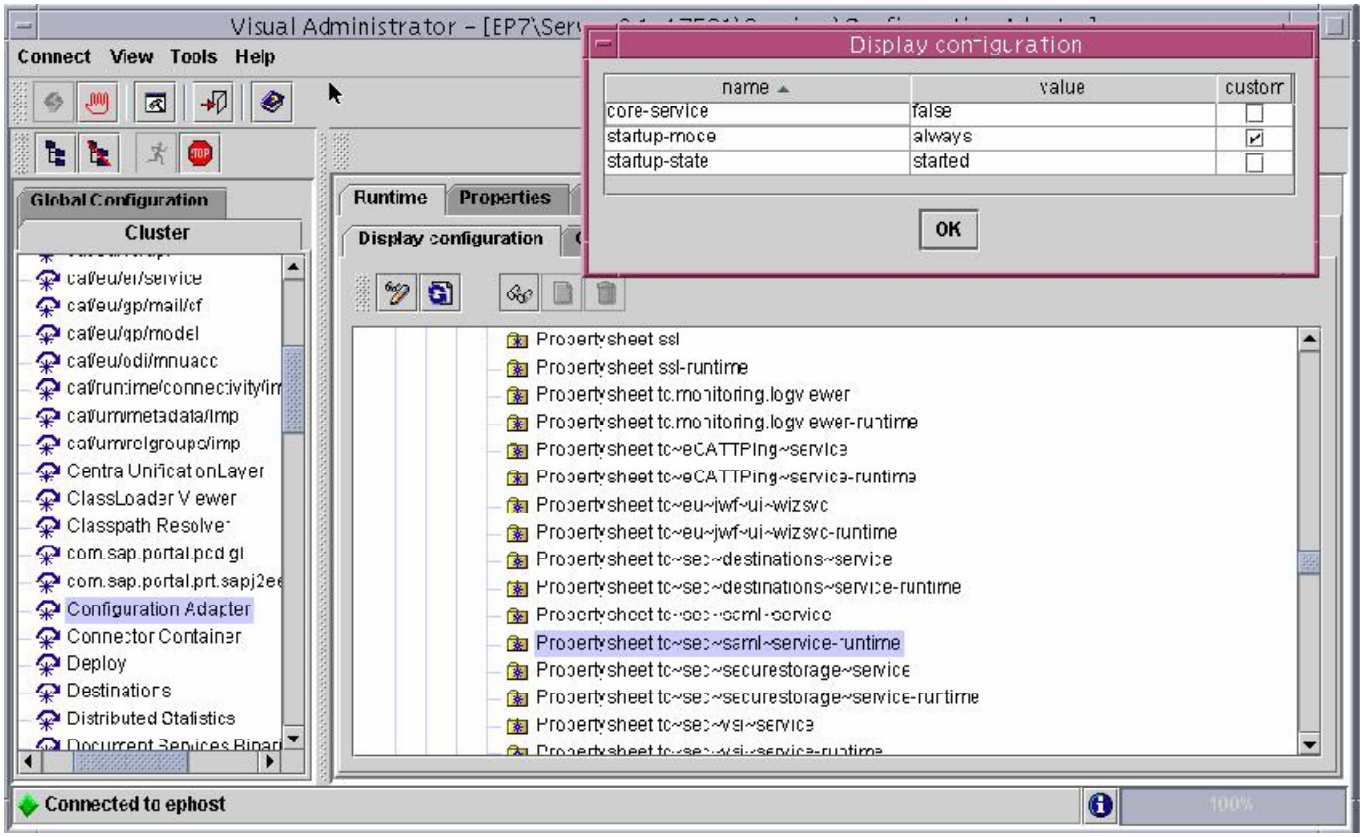
ETHZ SAP use case



SAP SAML configuration - overview

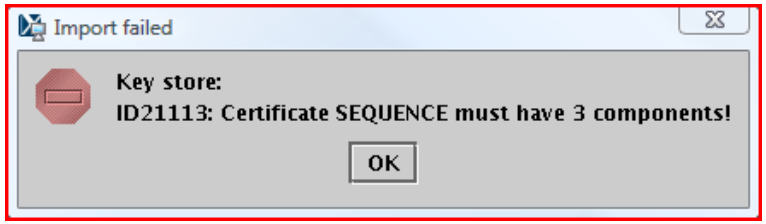
- Change the startup mode for SAML service
- Create SWITCH compatible certificate for Shibb. Auth.
- Create HTTP destination for IdP
- Configure SAML service parameter
- Add SAML login module stack

SAP SAML configuration – SAML Service



SAP SAML configuration – create Certificate

- **Create Certificate (no SAP NW VA standard)**
  - ./keygen.sh -y 3 -h #HOSTANAME# -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



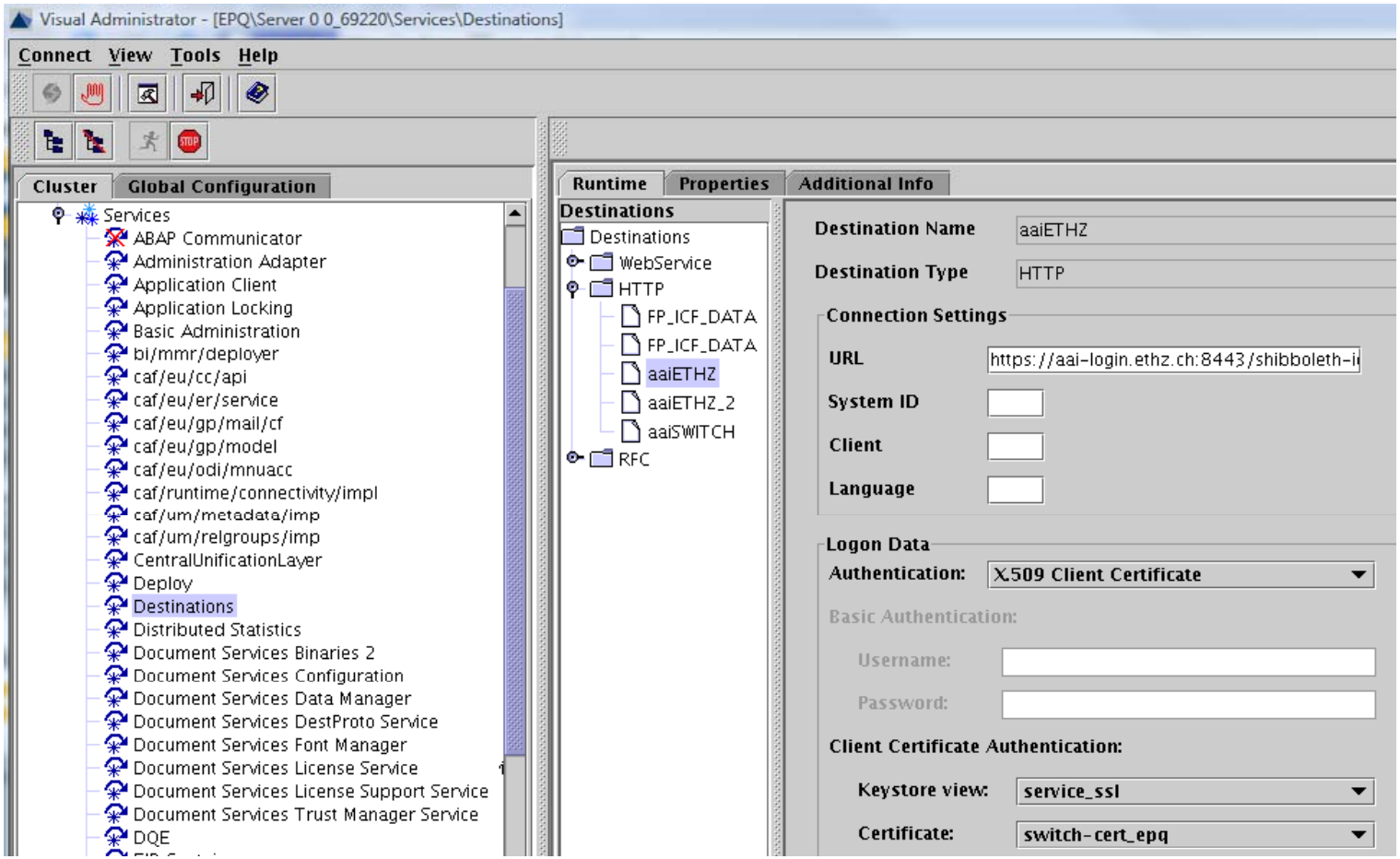
- **pkcs #12 certificate**
  - C:\Openssl\bin\openssl.exe pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in <Public Certificate Filename> -inkey <Private Key Filename> -out <PKCS#12 Filename> -name "<Display Name>"
  - openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export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

SAP SAML configuration – create Certificate

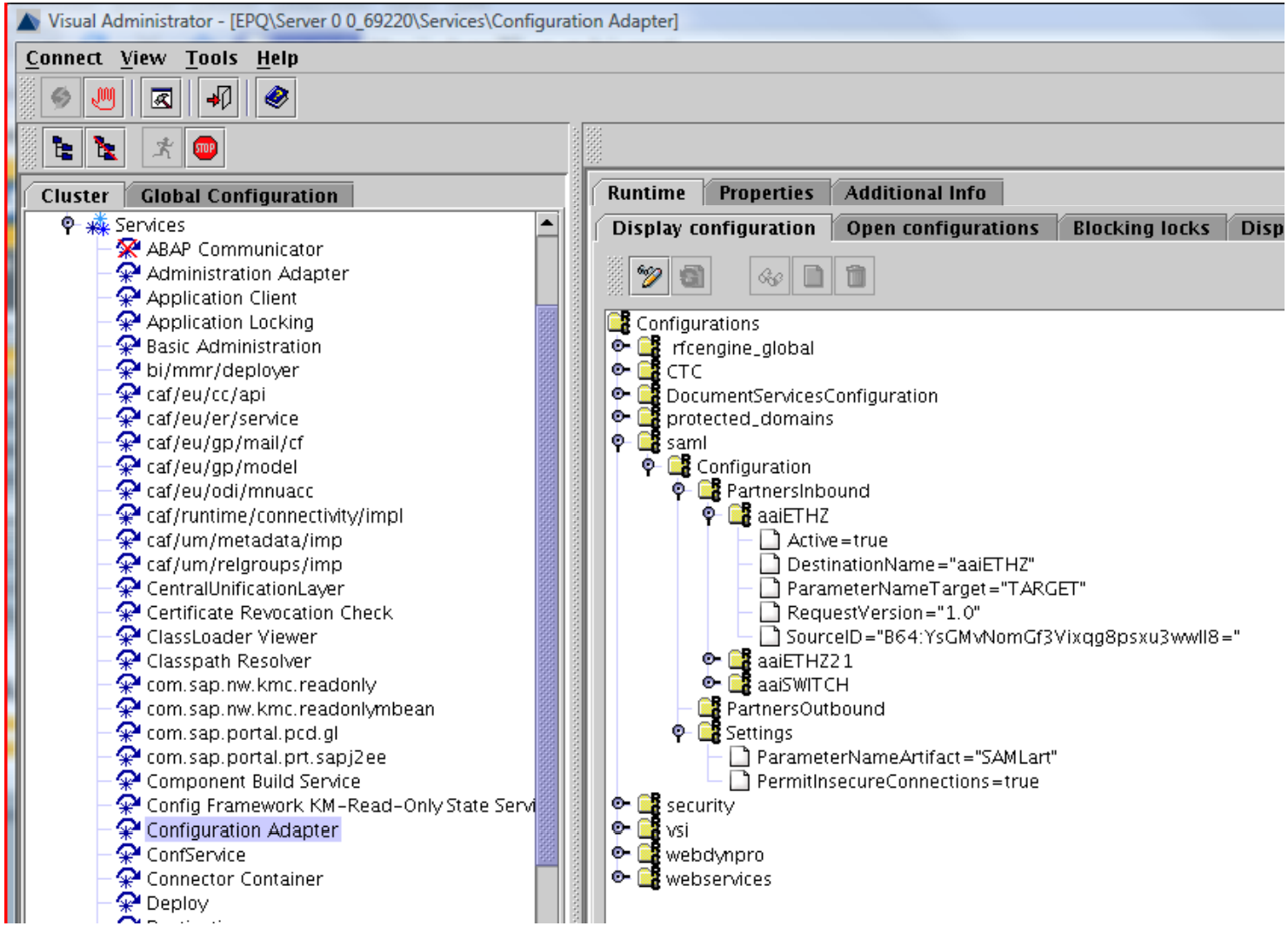
- **Load Certificae into NW key store**
  - Server -> Key Storage -> service_ssl: Entry -> Load “switch-cert2.pfx”

- **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

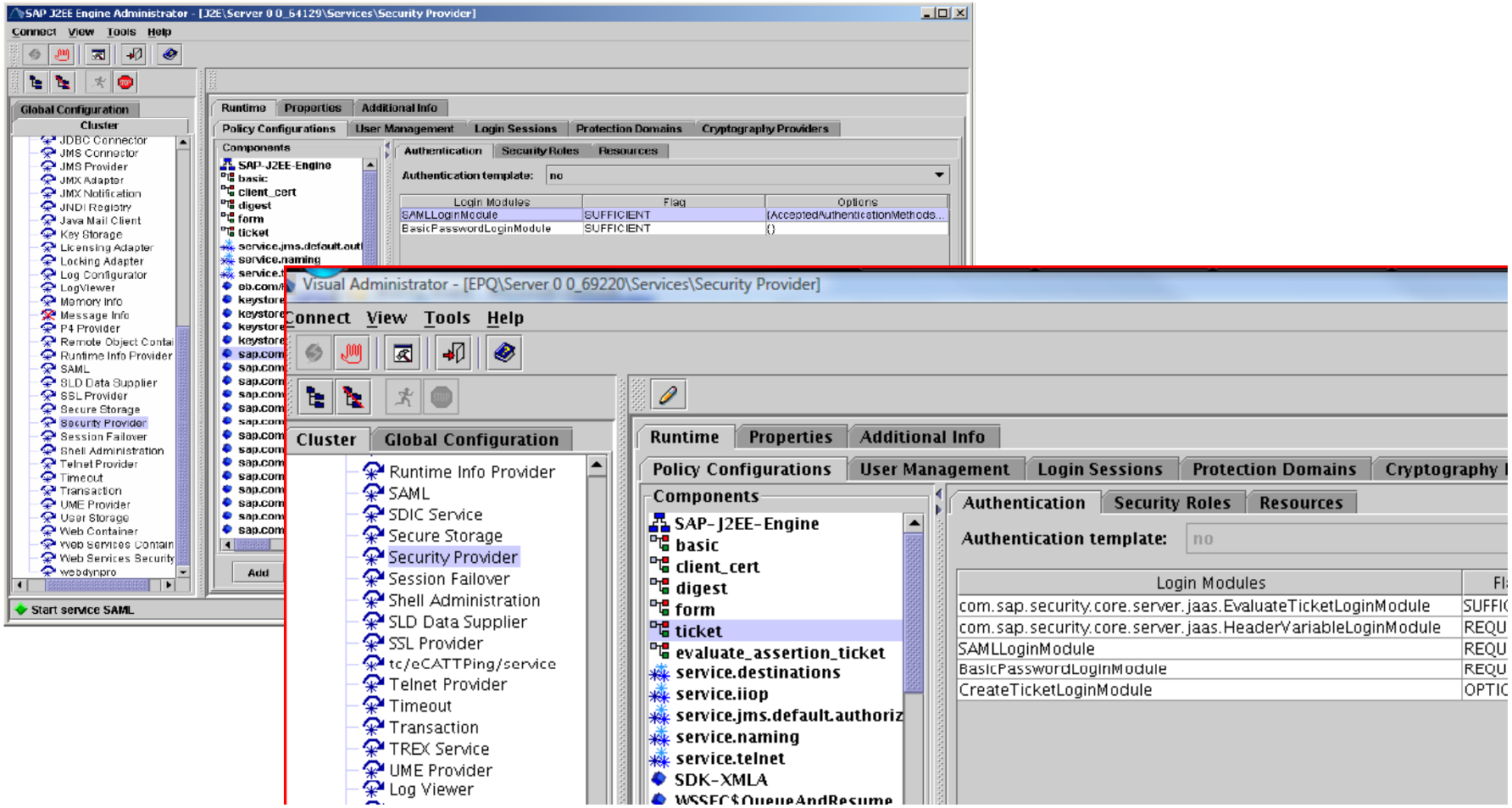
SAP SAML configuration – HTTP destination



SAP SAML configuration – SAML service



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:aaitest:nameIdentifier: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:

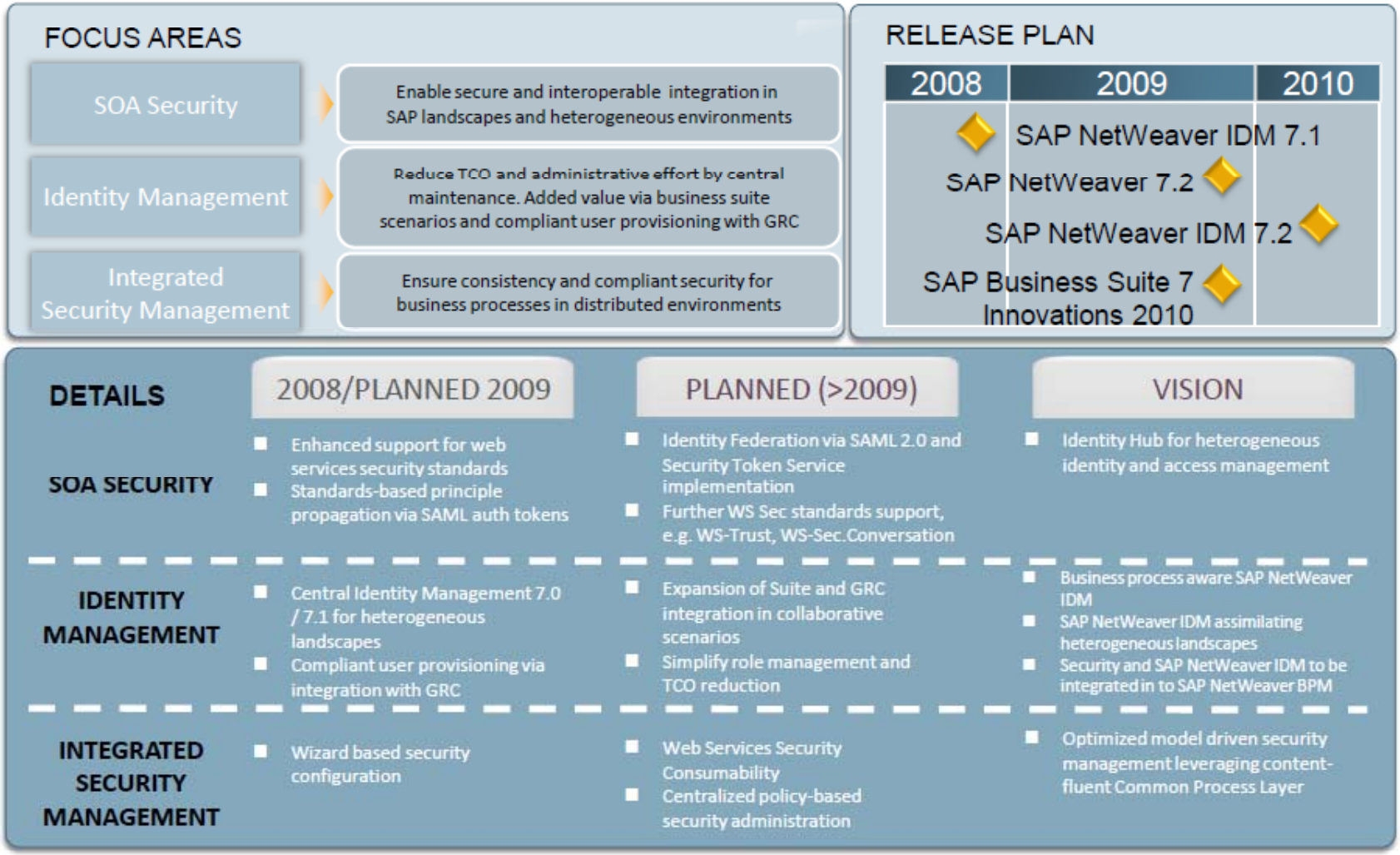
  <resolver:AttributeEncoder
  xsi:type="SAML1StringNameIdentifier"
  xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
  nameFormat="urn:mace:switch.ch:aaitest:nameIdentifier:principal" />

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



Questions and Answers

André Hunziker und André Wahlig, ETH Zürich Informatikdienste
Web: http://www.sap.ethz.ch / M@il: andre.hunziker@id.ethz.ch
andre.wahlig@id.ethz.ch