

14.–17. 09. 2009
in Nürnberg



Herbstcampus

Wissenstransfer
par excellence

Einer für alle

Enterprise Web-SSO mit CAS und OpenSSO

Sebastian Glandien

Acando GmbH

Oliver Ochs

Holisticon AG

Agenda

- Gründe für SSO
- Web-SSO selbst gemacht

- Enterprise WEB-SSO
 - mit CAS
 - mit OpenSSO
- Federation Management

- Zusammenfassung und Ausblick
 - CAS und OpenSSO
 - OpenID
 - OAuth

Gründe für SSO

Logins im Inter- und Intranet



Windows-Anmeldung

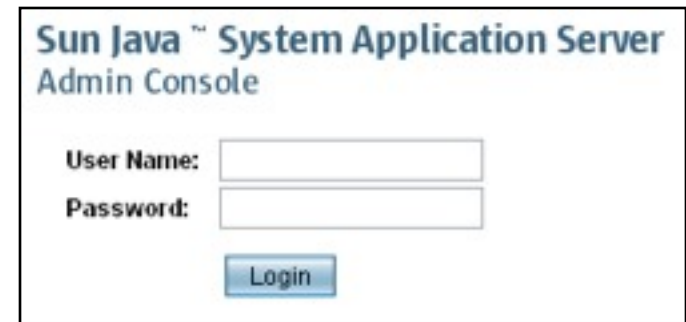
Microsoft
Windows Server 2003
Standard Edition

Copyright © 1985-2003 Microsoft Corporation

Benutzername:

Kennwort:

OK Abbrechen Optionen >>



Sun Java™ System Application Server
Admin Console

User Name:

Password:

Login

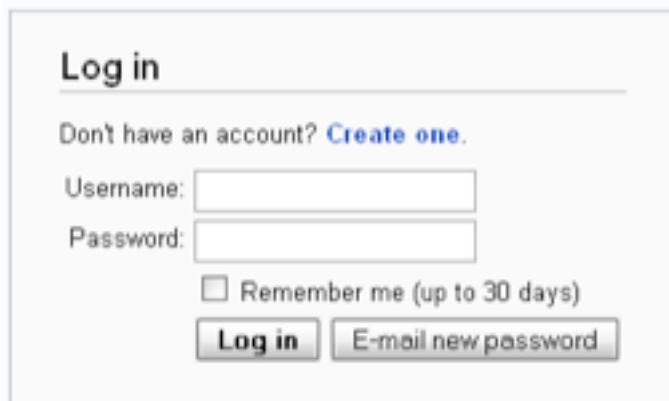


SAP NetWeaver

User ID *

Password *

Log On



Log in

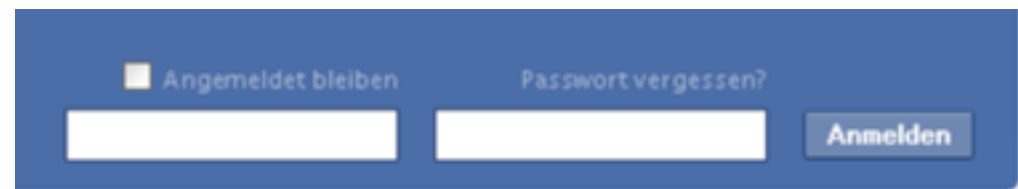
Don't have an account? [Create one.](#)

Username:

Password:

Remember me (up to 30 days)

Log in E-mail new password

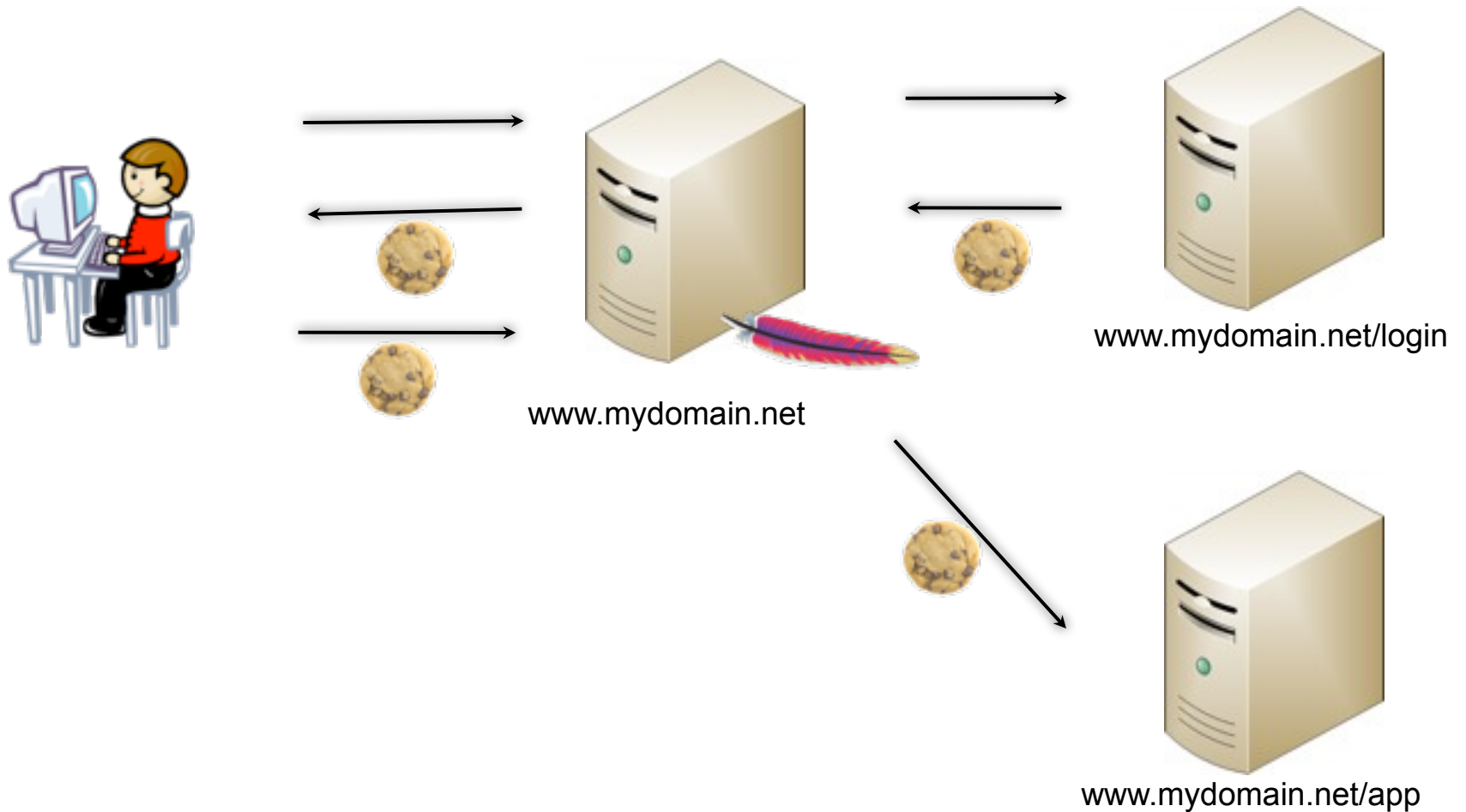


Angemeldet bleiben [Passwort vergessen?](#)

Anmelden

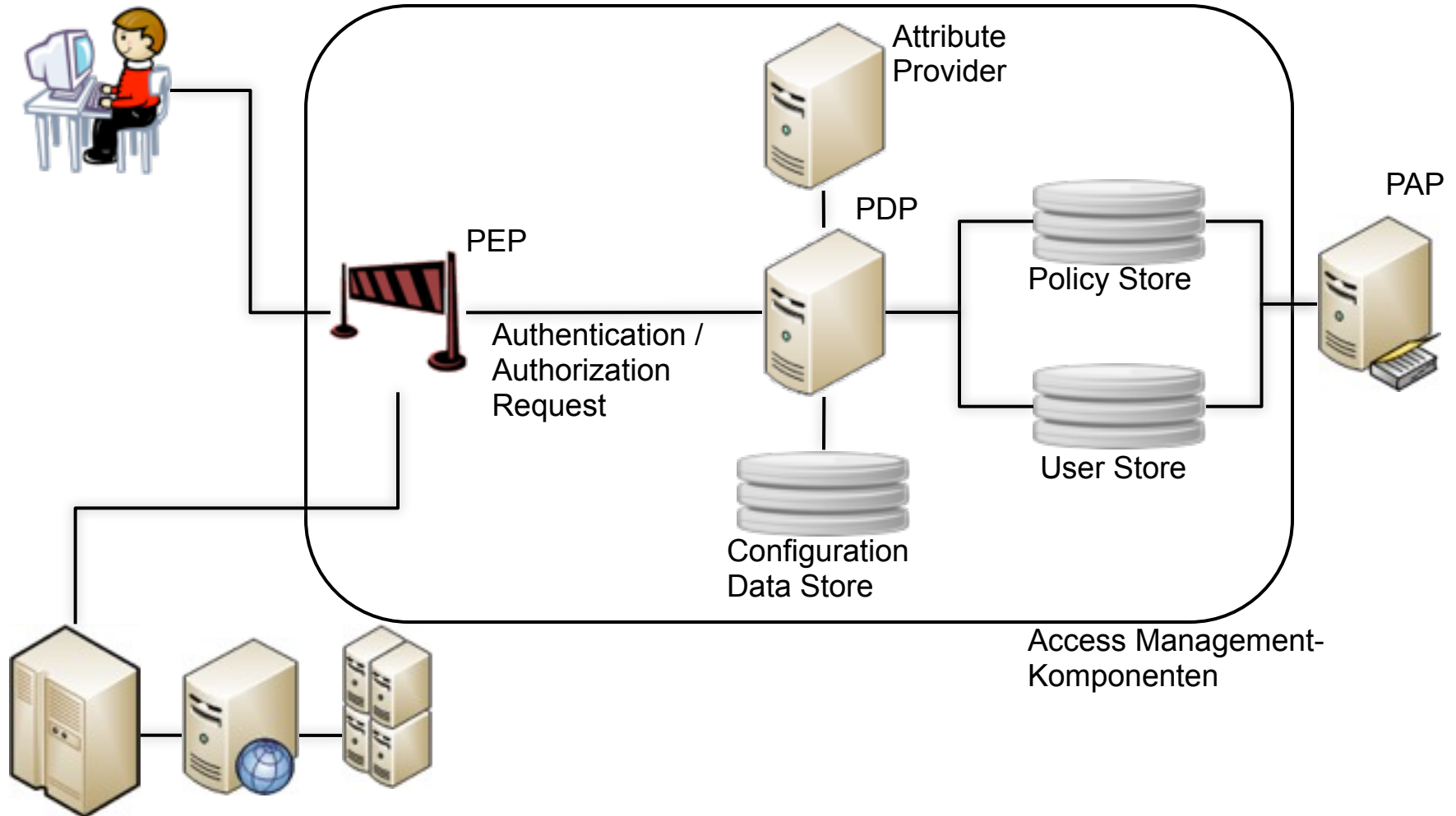
Web-SSO selbst gemacht

Web-SSO selbst gemacht



Enterprise WEB-SSO

Zielarchitektur

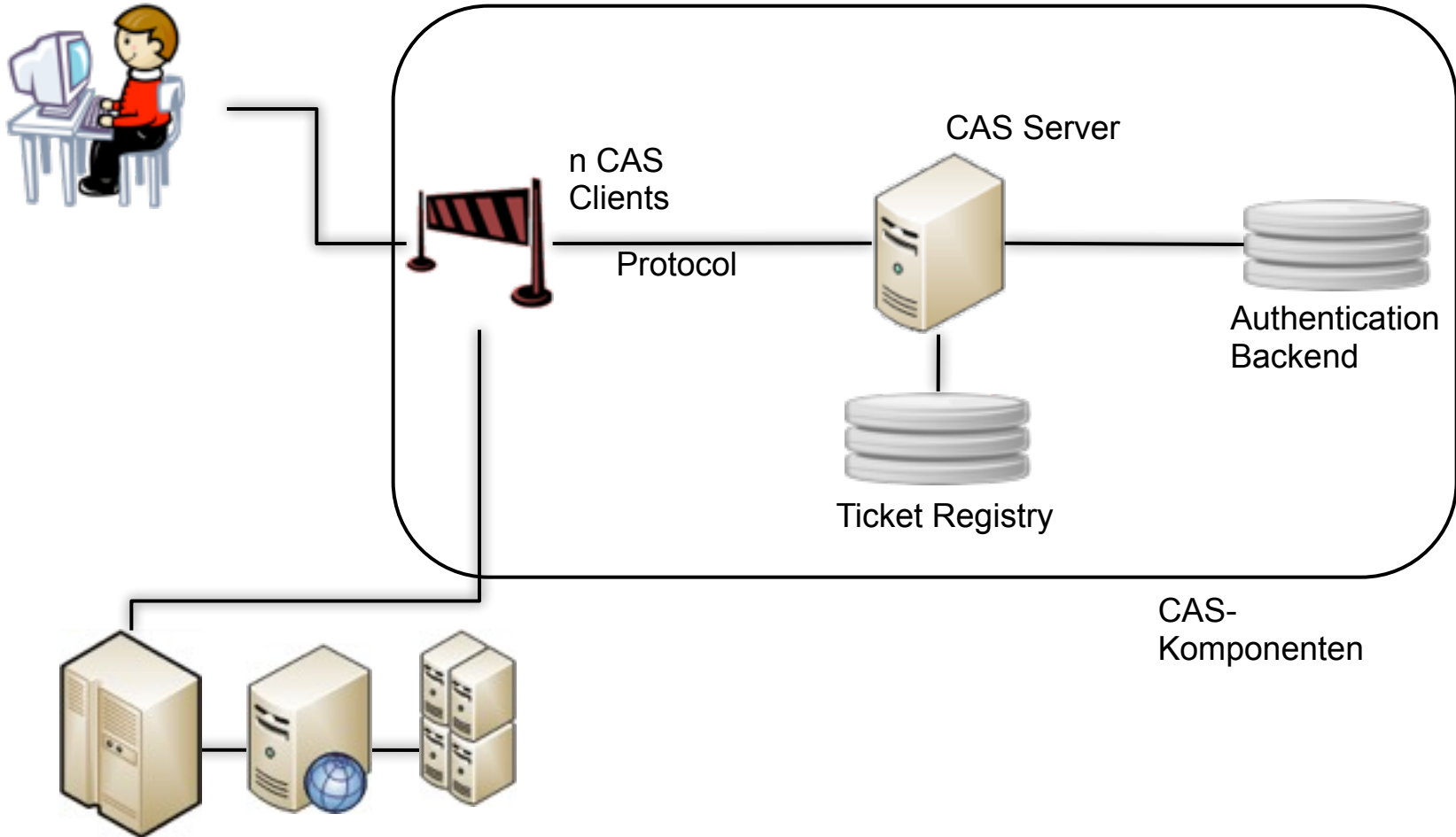


Enterprise Web-SSO mit CAS

CAS – Projektübersicht

- Enworfen von Shawn Bayern / Yale
 - Weiterentwickelt von Drew Mazurek / Yale
 - Seit 2004 JA-SIG Project unter Scott Battaglia
-
- CAS 1: Single Sign On
 - CAS 2: Proxy Authentication
 - CAS 3: WebServices und Sign Out über SAML

CAS – Architektur




CAS – Fähigkeiten

Server Component:

- open-source Java server component
- Web Application runs in Tomcat e.g.
- Standards: e.g. Spring, Maven2
- Clustering:
BerkeleyDB, JBossCache,
Memcache, Database

Clients & Integration:

- Java (Servlet-Filter oder Spring Security)
- Net, PHP, Perl, Apache
- Ruby, Python (Zope)
- Joomla, Wordpress, Drupal, Alfresco, Twiki
- Mantis, Jira
- Liferay and others



Implement a SSO
solution in a matter
of hours

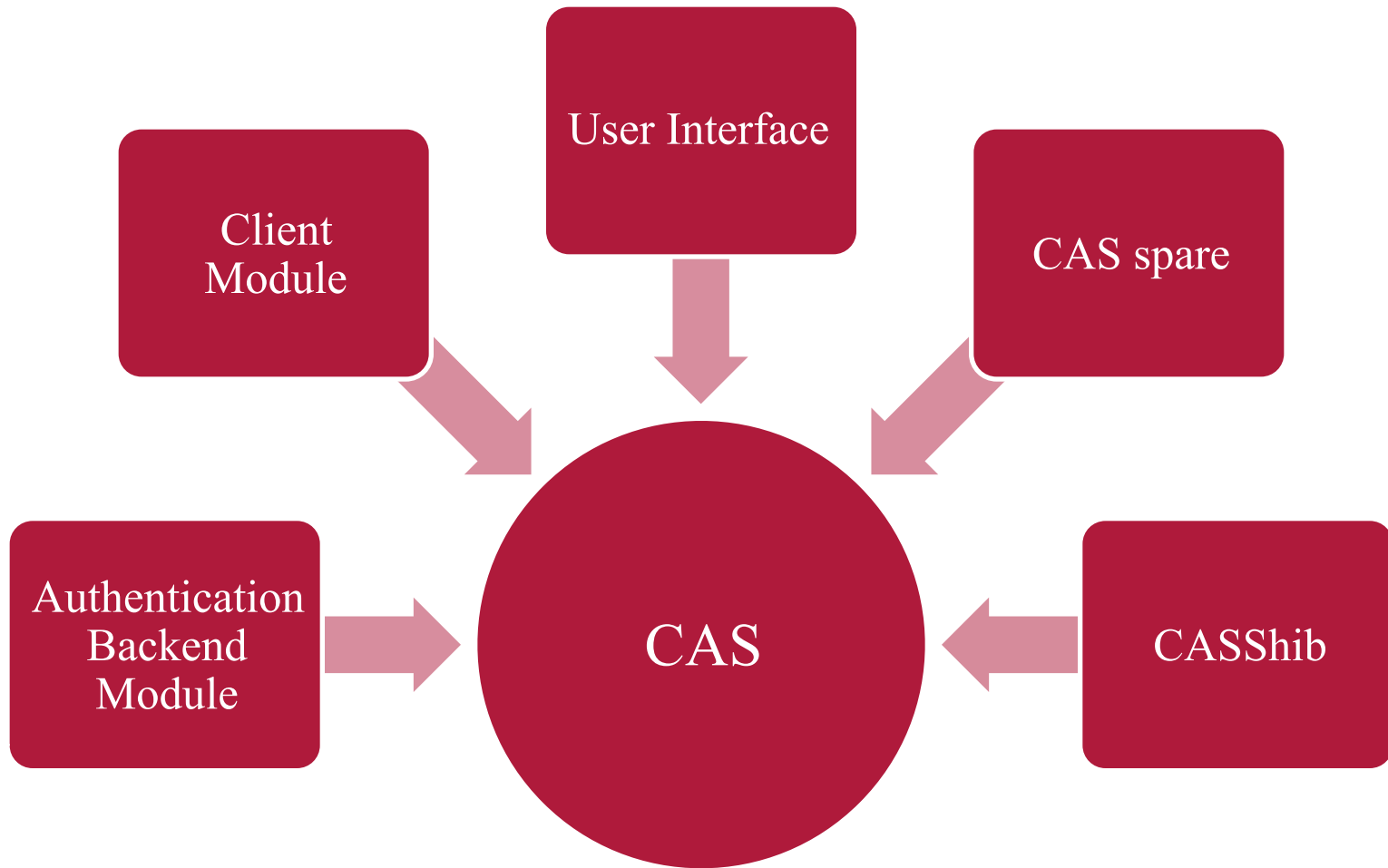
Protocols:

- CAS1 / CAS2
- SAML 1.1, Partial SAML2 (Google Apps)
- RESTful API

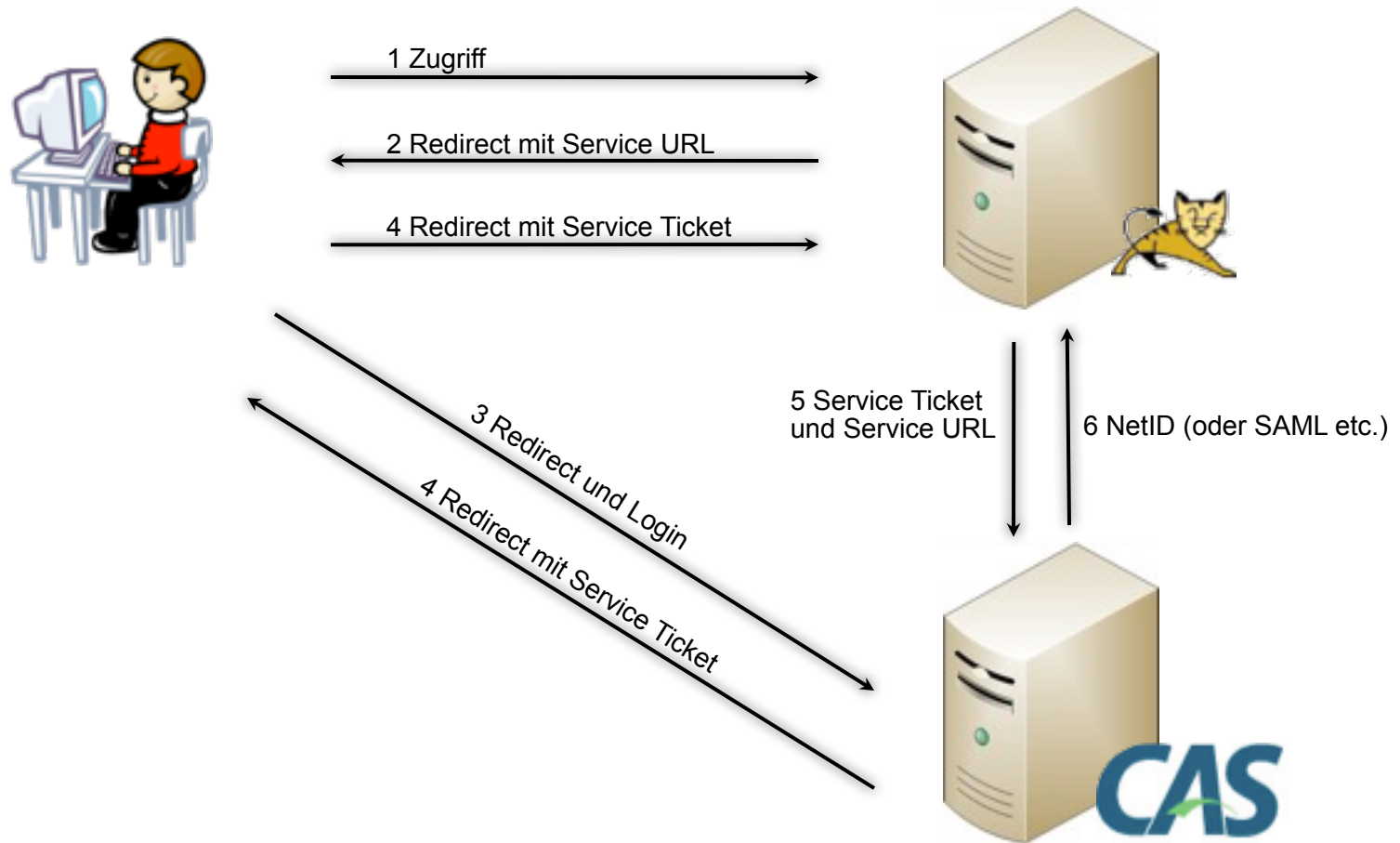
Back Ends:

- LDAP (e.g. Microsoft Active Directory)
- Databases, RADIUS
- X.509 certificates
- Simple API

CAS – Entwicklungen & Erweiterungen

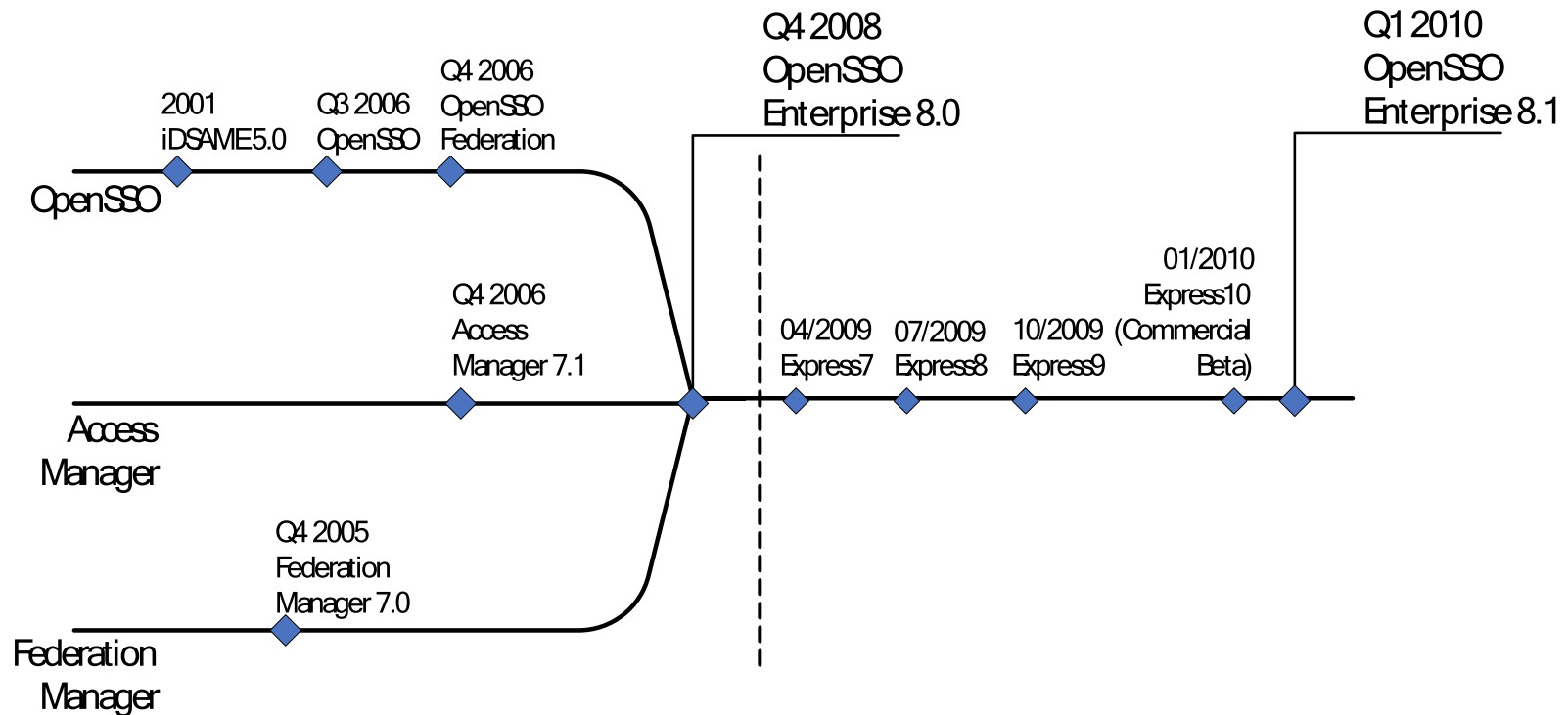


CAS – Beispiel



Enterprise Web-SSO mit OpenSSO

OpenSSO - Entstehung



OpenSSO – Übersicht

- Open Source Projekt aus dem Sun IAM-Produktportfolio
- besteht aus ca. 800 Projektmitglieder
- 15 externe Committer

- 100% Java
- unter der CDDL lizenziert
- Standard-basiert (SAML, XACML, ...)
- Integrierte Lösung für SSO, Authorization, Personalization, Federation und Webservices-Security

OpenSSO – Fähigkeiten



Access-Management:

- Ticket-granting Cookie
- Authentication-Chaining
- LDAP/AD, Certificate, SecureI, Unix, Windows NT, JDBC, WindowsDesktopSSO (Kerberos)
- Authorization
- Policy-Agents
- Web, J2EE, WSP, WSC, STS Client

**Transparentes
Access-
Management**

Federation-Management:

- Definition vertrauenswürdiger Beziehungen
- Identity Provider + Service Provider = Circle of Trust
- Federating identities
- Fedlets (HTTP Post Profile)
- Federation SSO ohne OpenSSO Enterprise

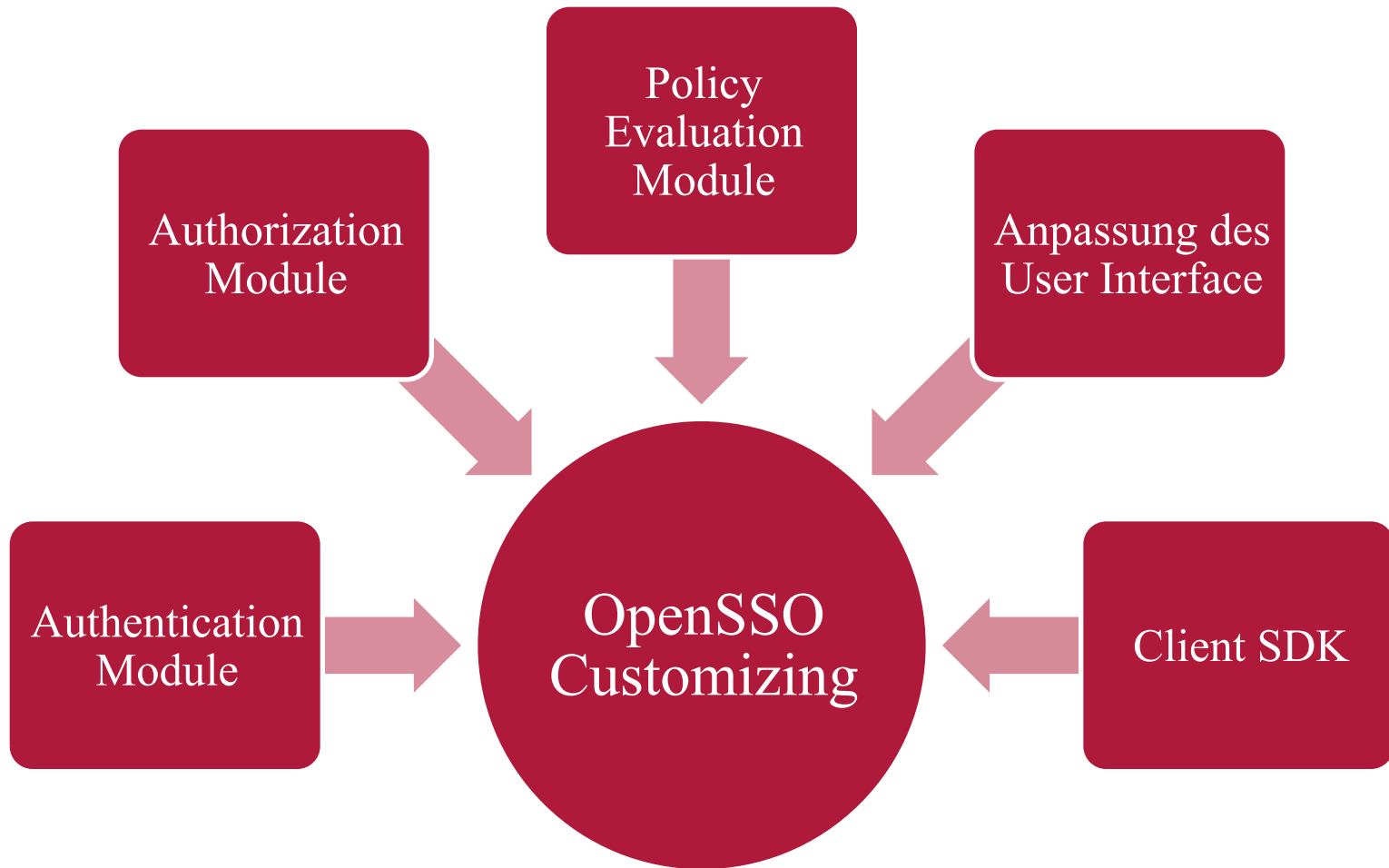
Identity-Services:

- Authentication
- Authorization
- Attributes & Audit Log

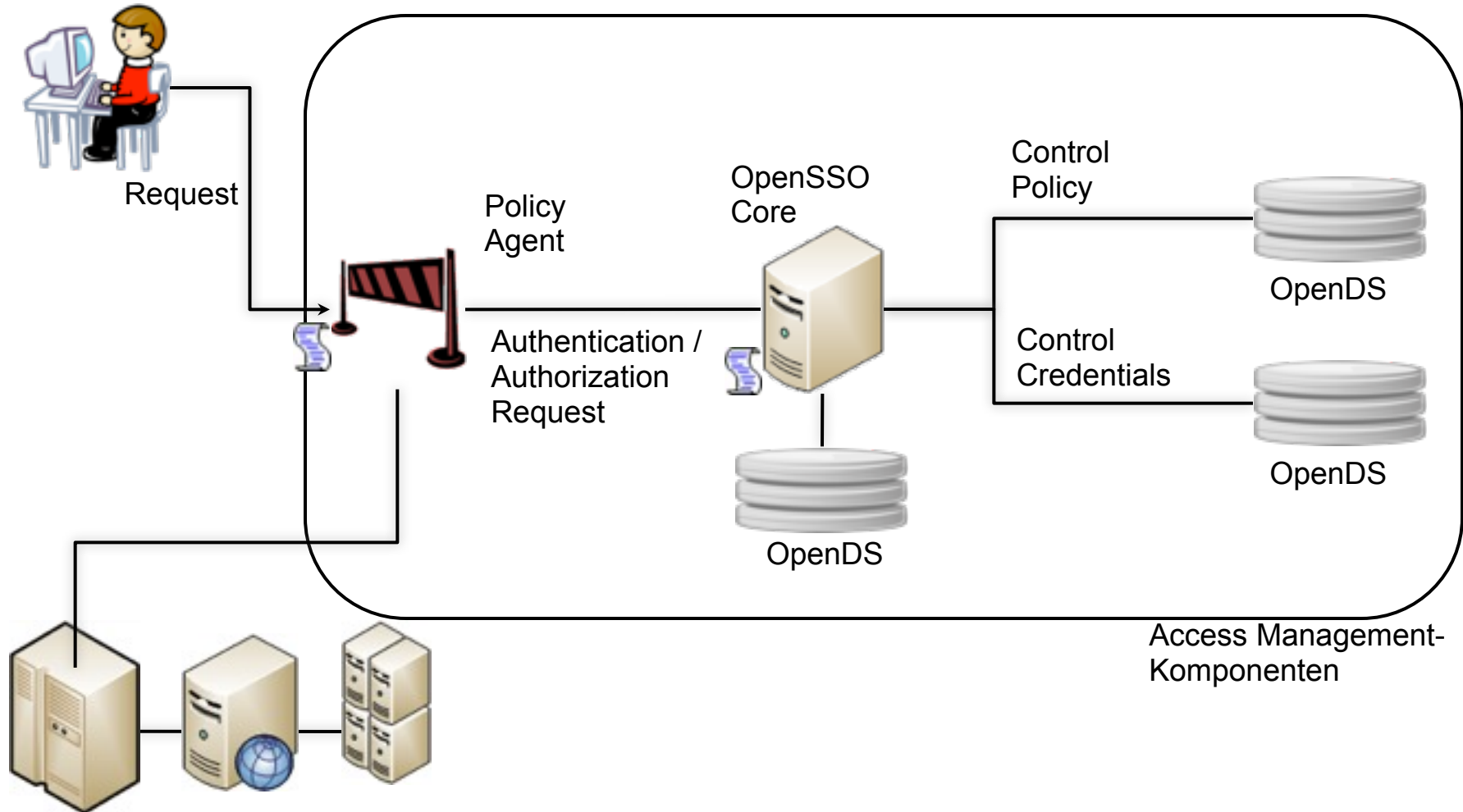
Web Service Security:

- Message Level Security
- WS-*
- XML-Encryption und –Signature
- beinhaltet JSR196 Provider

OpenSSO – Entwicklungen



Verwendung Policy Agent (OpenSSO)



Federation Management

Federation

- Standards, Technologien & Vereinbarungen
- zum Austausch von Personen- und Berechtigungsinformationen
- zwischen autonomen Bereichen (z.B. Unternehmen).

Rollen im Federation Management

Subjects

Haben digitale Identitäten (z.B. Benutzer, Organisationen)

Identity Provider

Erstellt und verwaltet digitale Identitäten

Service Provider

Stellt Services (z.B. Applikationen, geschützte Ressourcen) zur Verfügung

Attribute Authority

Kontrolliert Benutzerinformationen (Attribute)

Claim Transformers

Übersetzen Informationen von einem Format in ein anderes (sowohl technisch als auch fachlich)

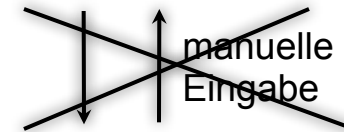
Federation – Use Case



Subject auf bahn.de



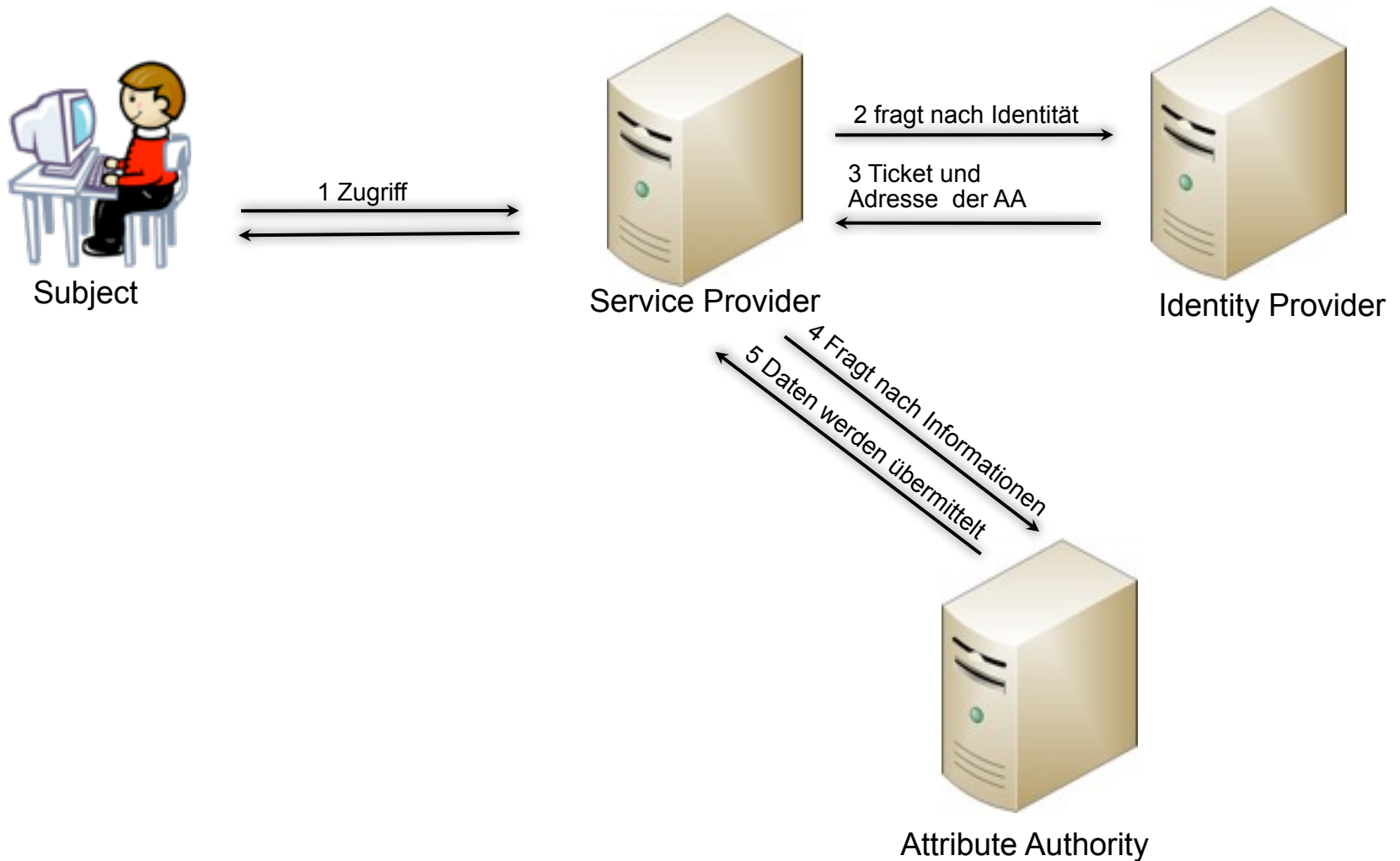
Subject auf sixt.de



transparenter Austausch



Federation – Beispiel



Identity-Mapping / Account-Linking



- username: oochs
- age: 32
- dateOfBirth: 30.03.1977
- role: developer



- username: 203303030
- age: 18+
- street:
- zipCode:
- city:
- role: customer

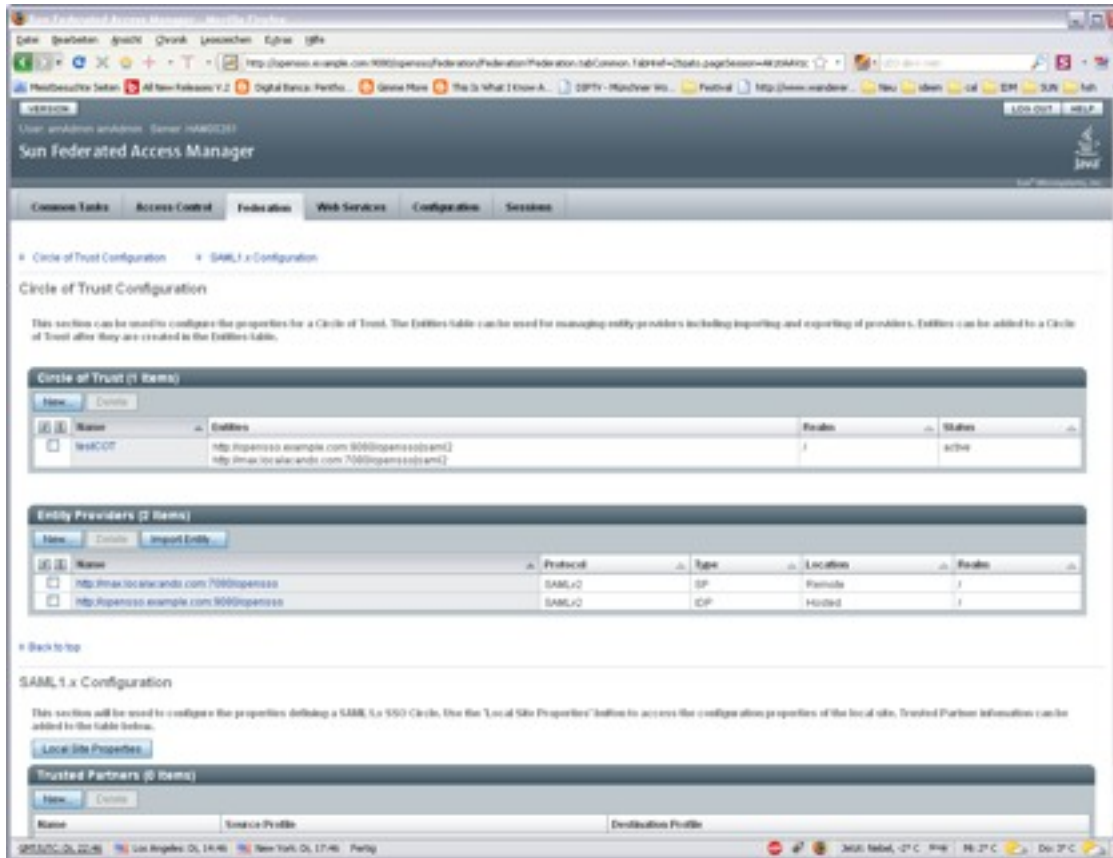
Gründe für SAML

- Beschränkungen von Browser-Cookies
- Vereinheitlichung von SSO-Mechanismen
- Web-Services
- Federation
- Zunehmende Verbreitung in Web-Produkten:
 - SAP-Netweaver
 - OpenSSO, Shibboleth, Athens, etc.

Security Assertion Markup Language (SAML)

- seit 2001 im OASIS-Kosortium entwickelt (u.a. SUN, IBM, Nokia und SAP)
- Setzt sich zusammen aus:
 - Assertions und Protocols (Core)
 - Bindings
 - Profiles
- Kernbestandteil bilden die Assertions (vertrauenswürdige Aussagen)
 - Authentication Assertion
 - Attribute Assertion
 - Authorization Decision Assertion

Konfiguration eines Circle of Trust



The screenshot shows the Sun Federated Access Manager configuration interface. The main navigation bar includes: **Common Tasks**, **Access Control**, **Federation**, **Web Services**, **Configuration**, and **Sessions**. The current view is **Circle of Trust Configuration** under **SAML 1.x Configuration**.

Circle of Trust Configuration

This section can be used to configure the properties for a Circle of Trust. The Entities table can be used for managing entity providers including importing and exporting of providers. Entities can be added to a Circle of Trust after they are created in the Entities table.

Circle of Trust (1 Items)

Name	Entities	Enabled	Status	
<input type="checkbox"/>	testCOT	http://openso.example.com:8080/openso/saml http://max.localandis.com:7080/openso/saml	<input checked="" type="checkbox"/>	Active

Entity Providers (2 Items)

Name	Protocol	Type	Location	Enabled	
<input type="checkbox"/>	http://max.localandis.com:7080/openso	SAMLv2	SP	Remote	<input checked="" type="checkbox"/>
<input type="checkbox"/>	http://openso.example.com:8080/openso	SAMLv2	IDP	Hosted	<input checked="" type="checkbox"/>

SAML 1.x Configuration

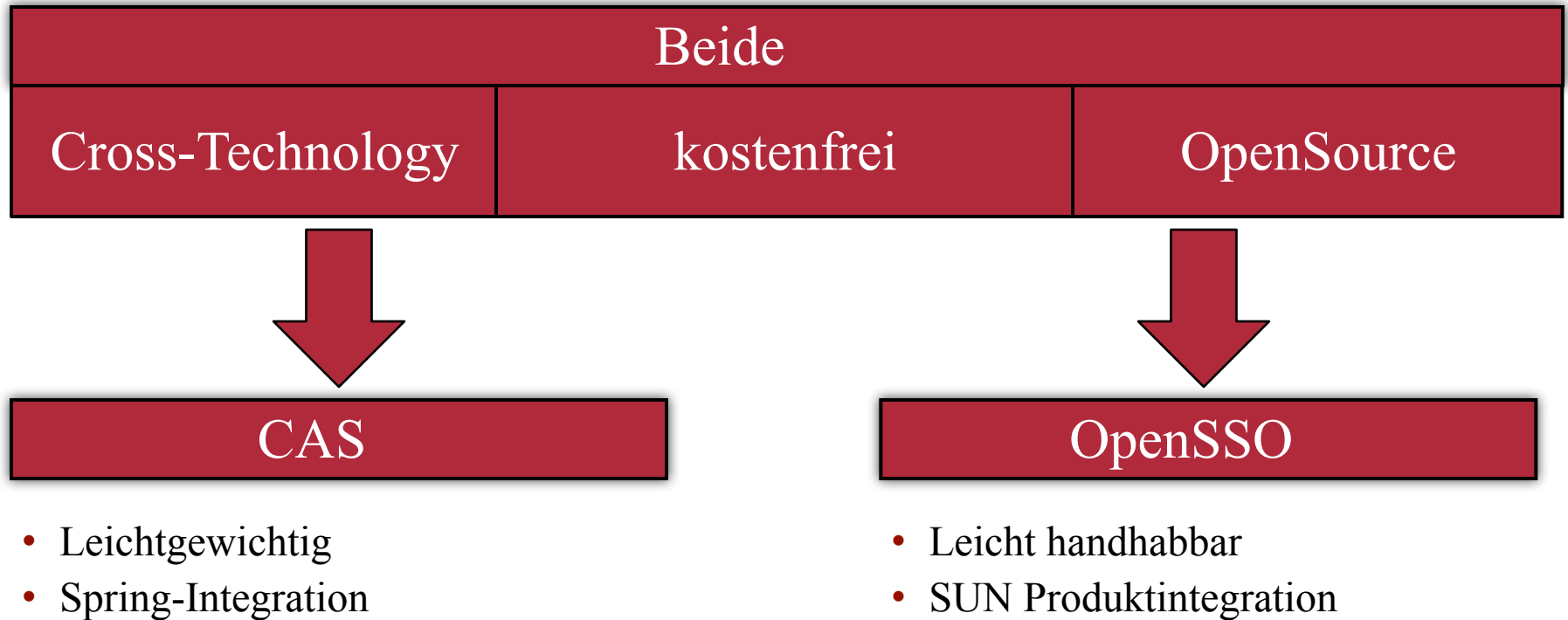
This section will be used to configure the properties defining a SAML 1.x SSO Circle, that the "Local Site Properties" before to access the configuration properties of the local site. Trusted Partner information can be added to the table below.

Trusted Partners (0 Items)

Name	Source Profile	Destination Profile
------	----------------	---------------------

Zusammenfassung

Zusammenfassung



Ausblick

CAS 4

- Federation über OpenID
- Attributes
- Backend-Warnings

OpenSSO

- Express 8
 - Mobile One Time Password
 - MySQL User Store Support
 - Fedlet for .NET
 - Active Directory Integration Improvements
- Express 9
 - Entitlement Enforcement
 - Service Level Monitoring
 - Reverse Proxy with Password Replay

OpenID

- Subject haben URL-basierten Identitäten
- Login beim Service Provider durch Eingabe der OpenID (URL)
- Weiterleitung zum OpenID-Identity-Provider
- Login beim OpenID-Provider
- Bestätigung der Anmeldung
- Festlegen der Attribute (Attribute Authority)
- Redirect zurück zum Service Provider

- Dezentral (jeder kann sein eigener OpenID-Provider sein)
- Kontrolle über Attribute und Services beim Nutzer

OAuth

- Zugriff auf geschützte Ressourcen (kein SSO)
- Service Provider: verwaltet geschützte Ressourcen
- Consumer: Anwendung, die Zugriff auf Ressource braucht
- Protected Resources: geschützte Ressource
- Zugriff über Tokens

14.–17. 09. 2009
in Nürnberg



Herbstcampus

Wissenstransfer
par excellence

Vielen Dank!

Sebastian Glandien (Acando GmbH)
Oliver Ochs (Holisticon AG)