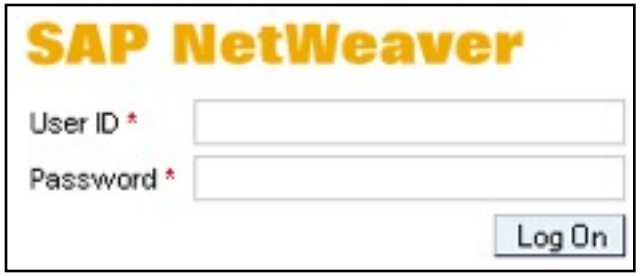
Enterprise Web-SSO mit CAS und OpenSSO

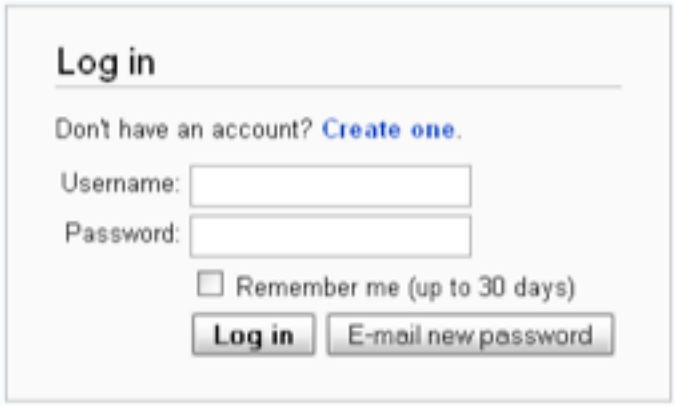
Agenda

- **Gründe** für SSO
- Web-**SSO** selbst gemacht
- Enterprise Web-SSO mit **CAS**
- Enterprise Web-SSO mit **SUN OpenSSO**
- **Federation**-Management
- Zusammenfassung

Gründe für SSO

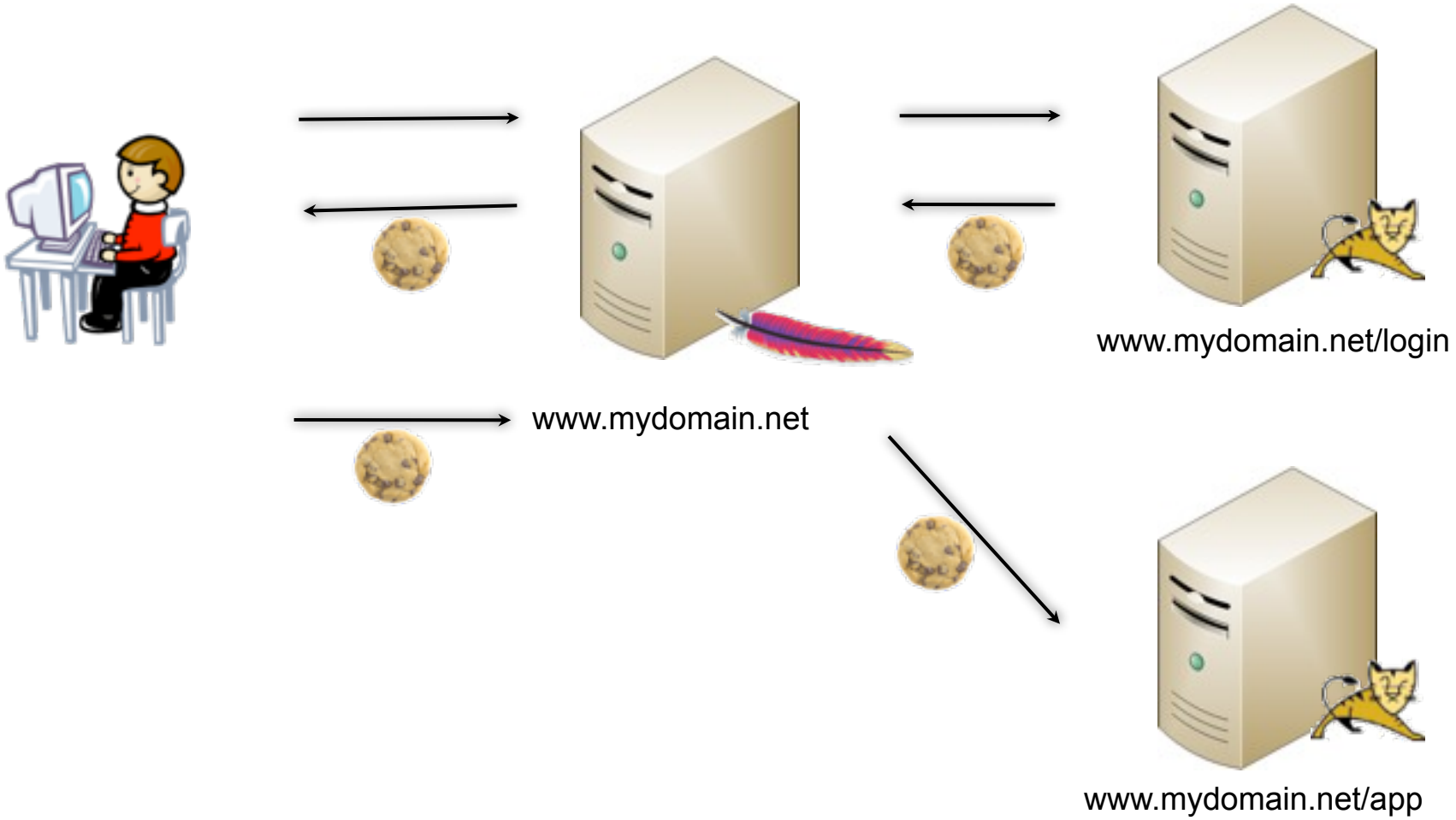
Logins im Inter- und Intranet





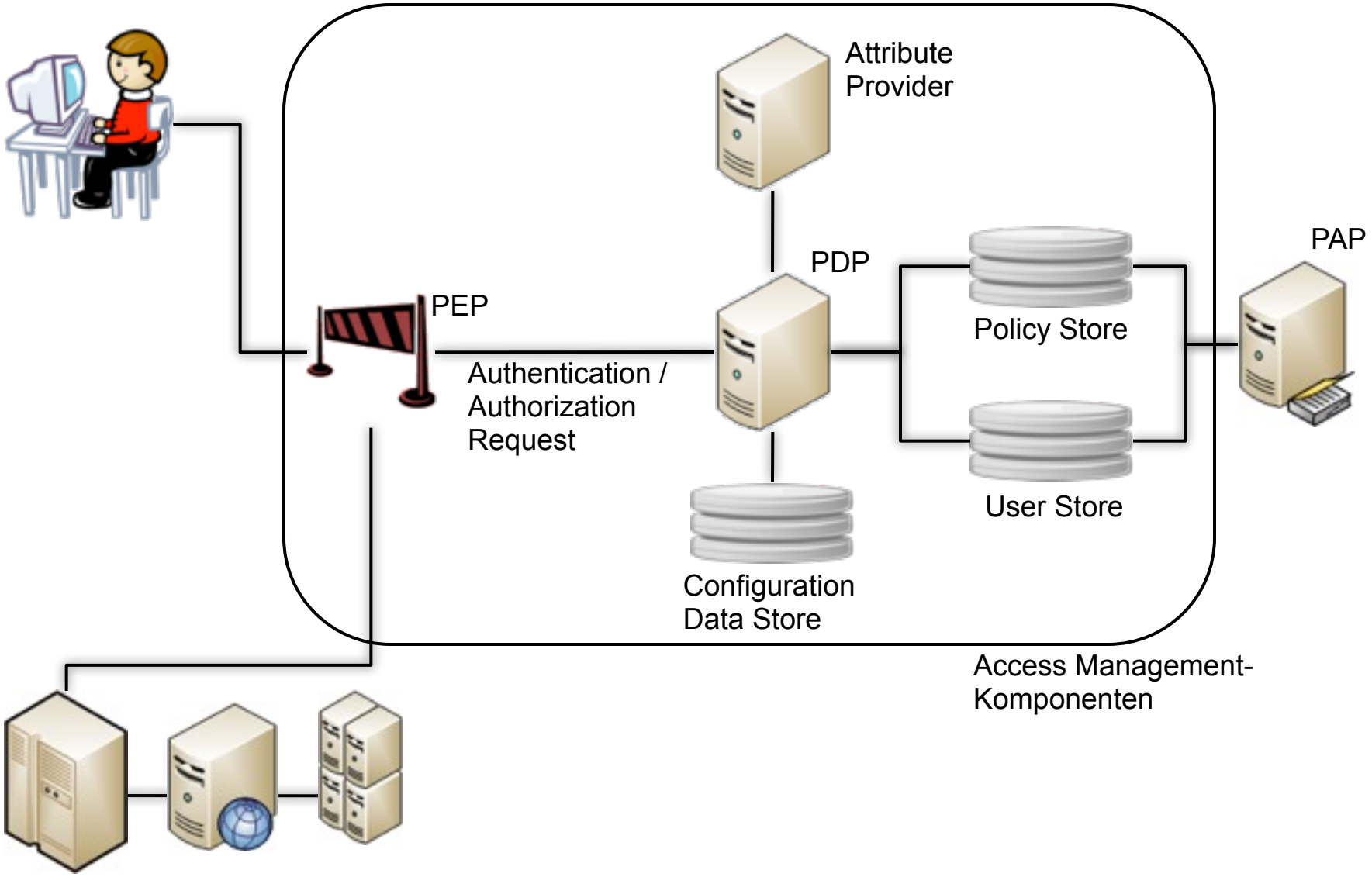
Web-SSO selbst gemacht

Web-SSO selbst gemacht



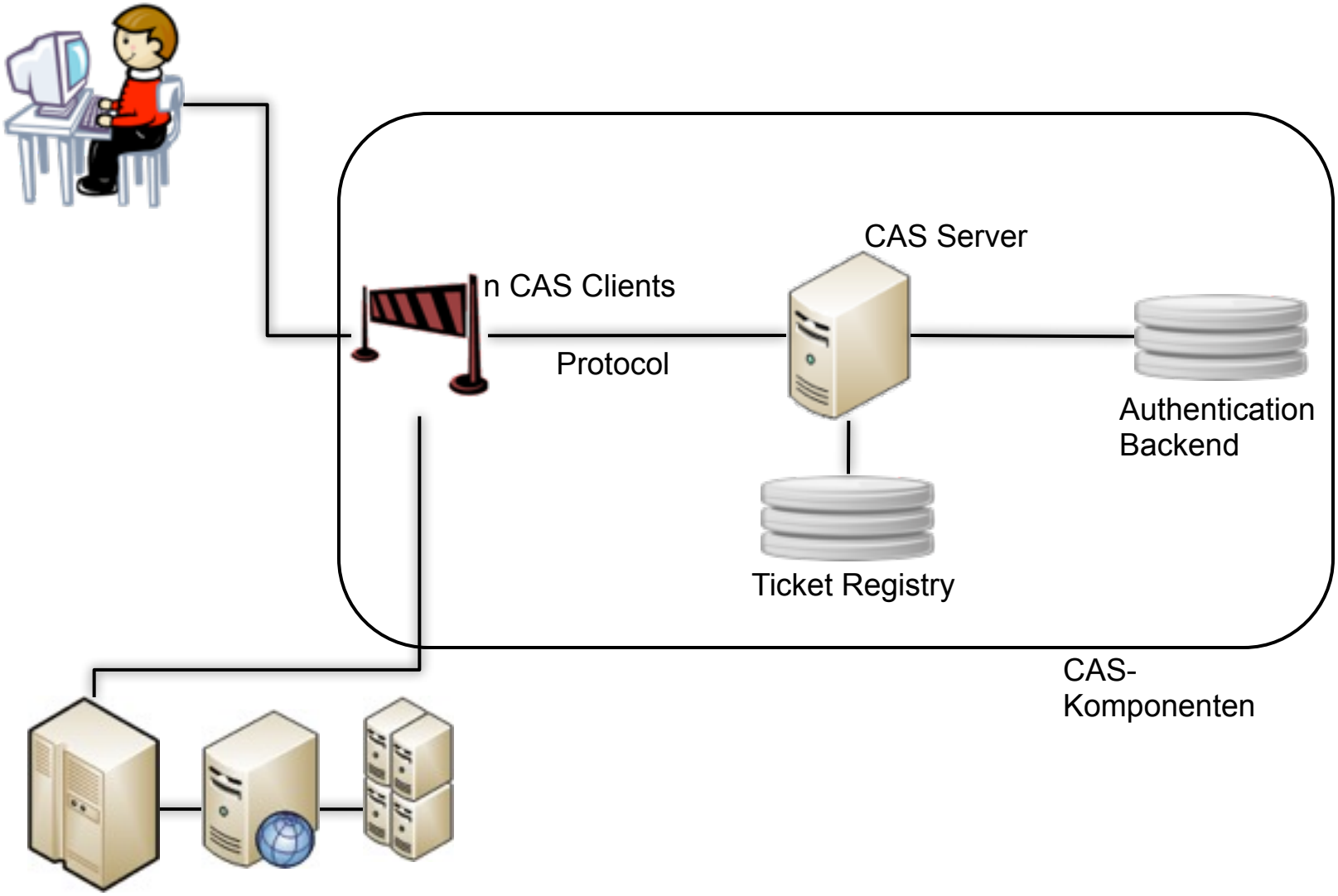
Enterprise Web-SSO

Zielarchitektur

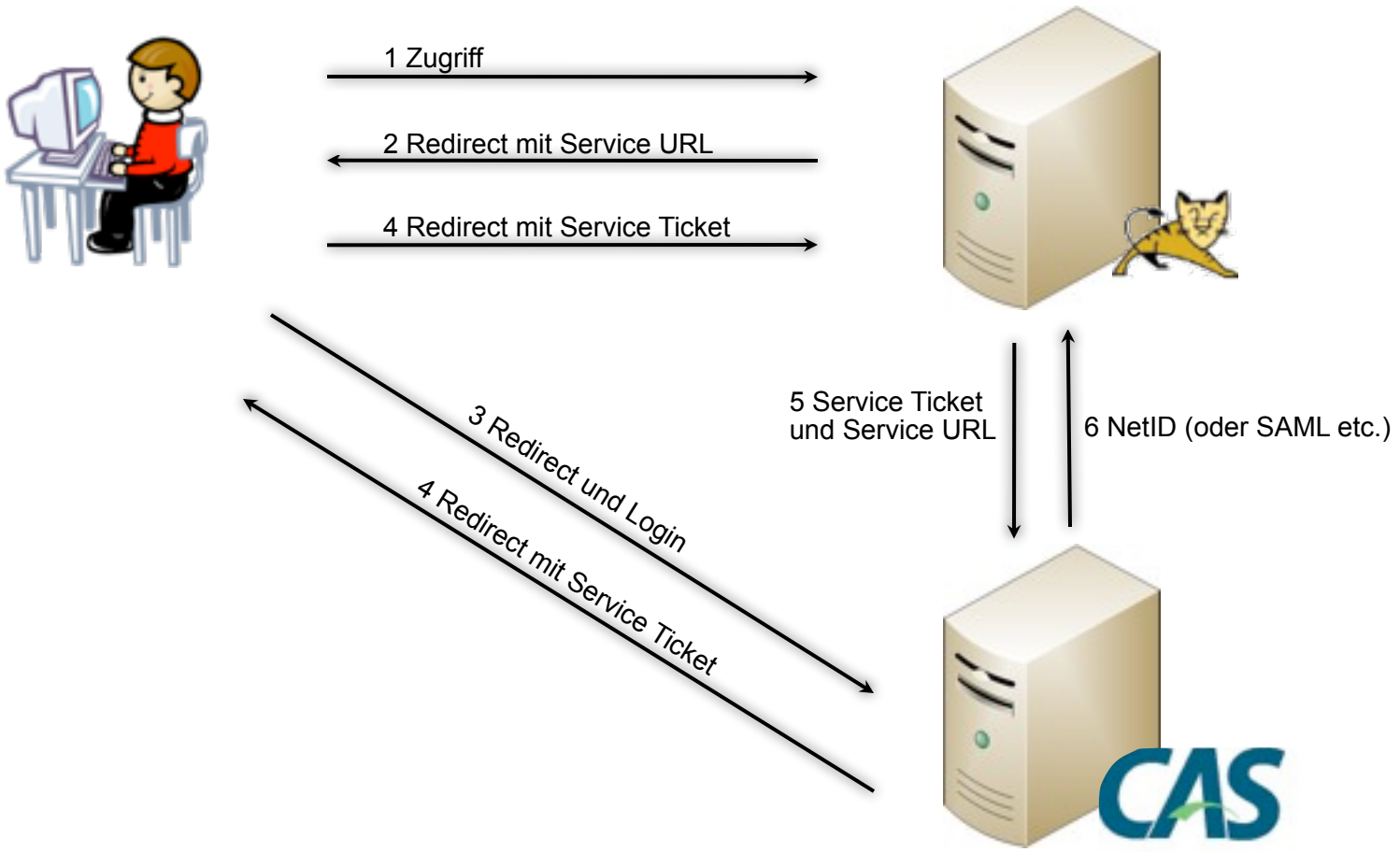


Enterprise Web-SSO mit CAS

CAS


CAS Server
n CAS Clients
Protocol
Authentication
Backend
Ticket Registry
CAS-
Komponenten

Enterprise Web-SSO mit CAS



CAS - Fähigkeiten

Server Component:

- open-source Java server component
- Web Application that runs in Tomcat e.g.
- Standards: e.g. Spring, Maven2
- Clustering: BerkeleyDB, JBossCache, Memcache, Database
- ... to implement a SSO solution in a matter of hours

Clients & Integration:

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

Protocolls:

- CAS1 / CAS2
- SAML 1.1
- Partial SAML2 (Google Apps, e.g. Gmail)
- also RESTful API

Back Ends:

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

Enterprise Web-SSO mit OpenSSO

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, …)
- Unterstützung einer Vielzahl von Client- und Serversystemen
- 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

Federation-Management:

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

Transparentes Access-Management

Identity-Services:

- Authentication
- Authorization
- Attributes & Audit Log

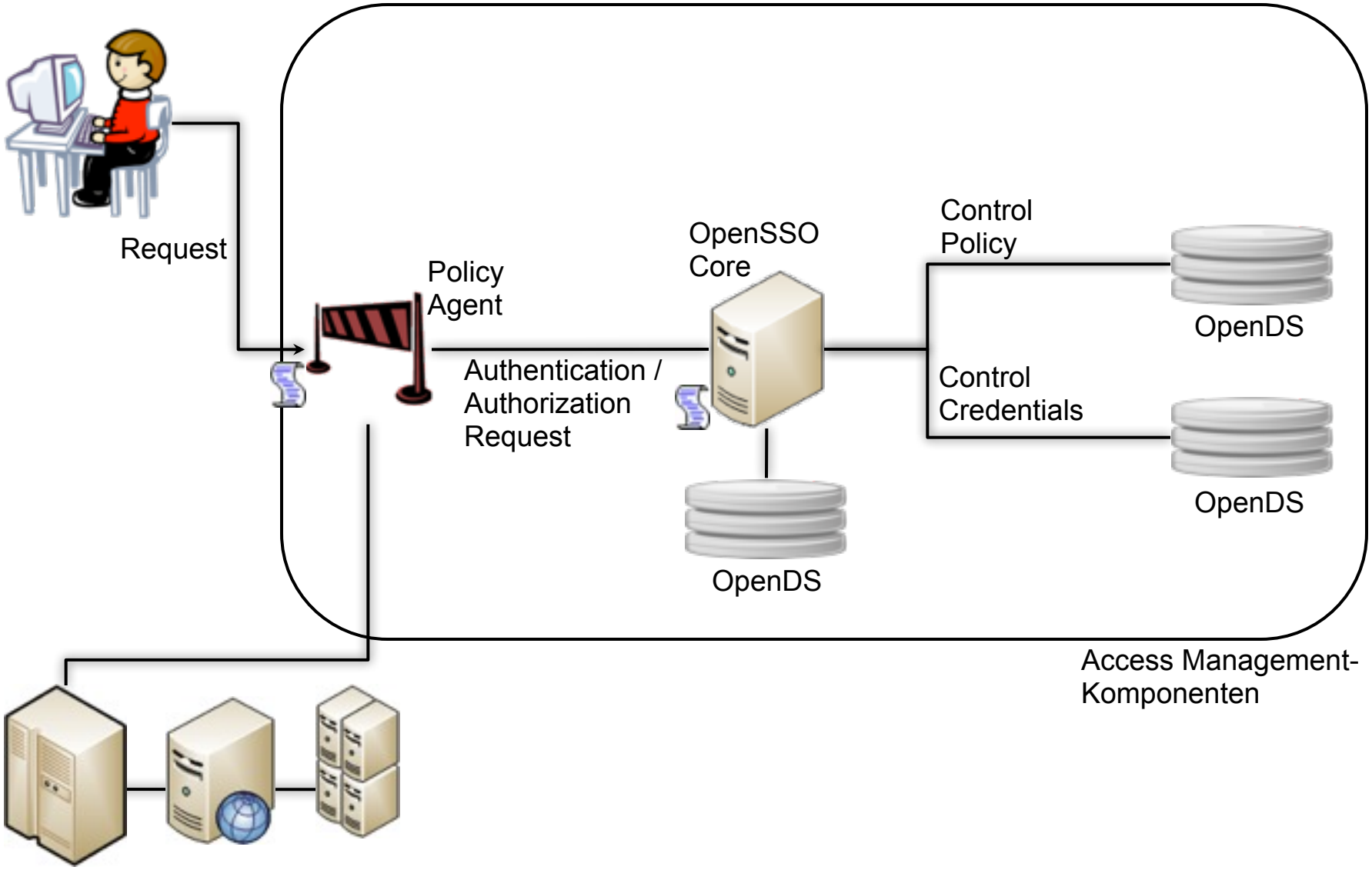
Web Service Security:

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

OpenSSO – Entwicklungen

- **Implementierung eigener:**
  - **Authentication Module**
    - `com.sun.identity.authentication.spi.AMLoginModule`
  - **Policy Evaluation Module**
    - `com.sun.identity.policy.PolicyManager`
  - **Authorization Module**
    - `com.sun.identity.policy.interfaces.Subject`
    - `com.sun.identity.policy.interfaces.Condition`
    - `com.sun.identity.policy.interfaces.Referral`
    - `com.sun.identity.policy.interfaces.ResponseProvider`
  - **neuer Webservices**
  - **Konfigurations- und User-Datastore Module**
- **Anpassung des User Interface**
- **Nutzung des Client SDK**

Verwendung Policy Agent (OpenSSO)

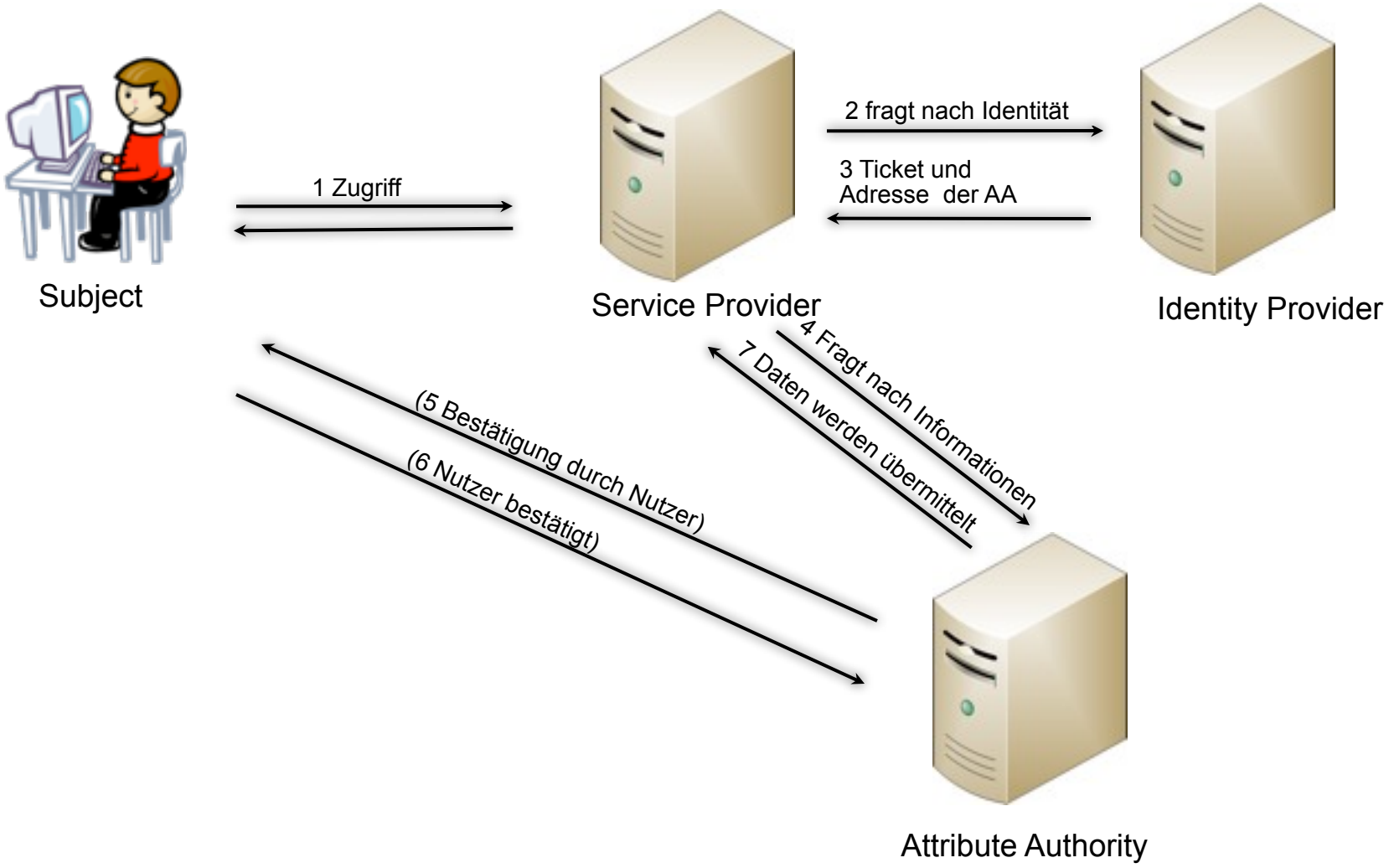


Federation Management

Rollen bei Federation

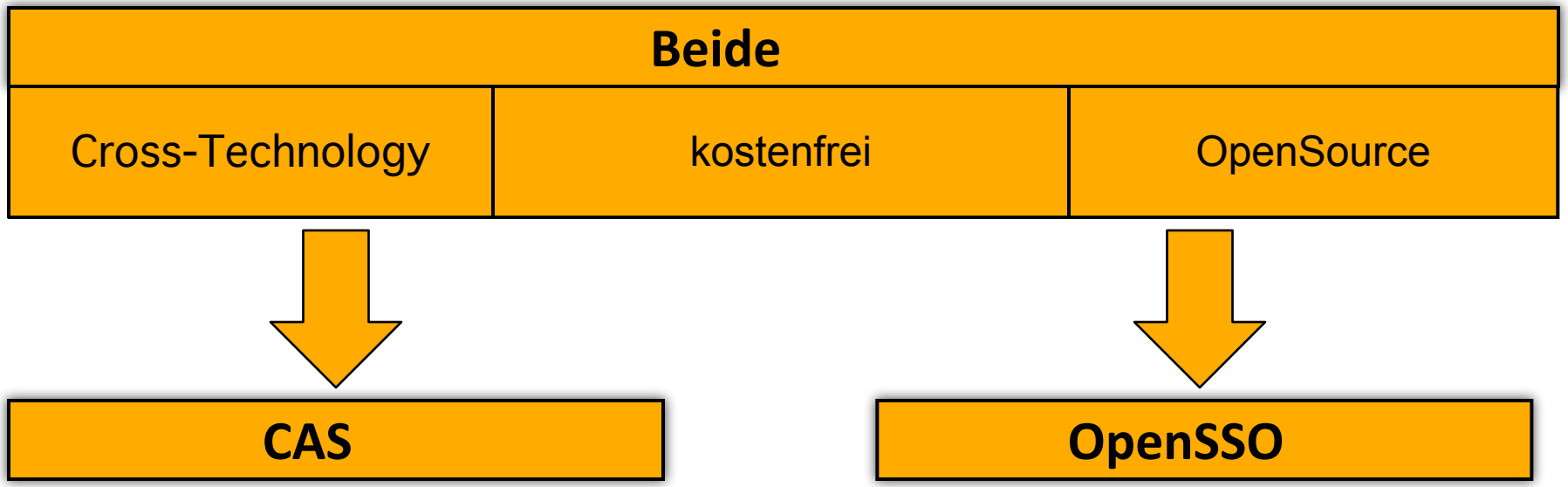
Subjects	Haben digitale Identitäten (z.B. Benutzer, Organisationen)
Identity Provider	Erstellt und verwaltet digitale Identitäten
Service Provider	Stellt Services (z.B. Applikationen) für Subjects zur Verfügung und benötigt dazu Identitäten bzw. deren Attribute
Attribute Authority	Kontrolliert Benutzerinformationen (z.B. zusätzliche Attribute)
Claim Transfomers	Übersetzen Informationen über Identitäten von einem Format in ein anderes (z.B. technisch X.500, Kerberos oder fachlich)

Rollen bei Federation (simplified)



Zusammenfassung

Besonderheiten CAS und OpenSSO



- Leichtgewichtig
- Spring-Integration

- Leicht handhabbar
- SUN Produktintegration

…vielen Dank für Ihre Aufmerksamkeit!

sebastian.glandien@acando.de

oliver.ochs@holisticon.de