

ORACLE®



ORACLE[®]

Real World Single Sign-on mit ADF Faces

Olaf Heimburger

Senior Solution Architect IDM & SOA

Verfügbare Technologien

- Oracle AS SSO
- OpenId
- SAML 2.0
- Oracle Access Manager SSO

OpenID

- Breite Anwendung
 - Google, Yahoo, flickr, myspace, facebook, VeriSign, AOL
 - US Behörden
- Anwender verwaltet seine Identität
- Anwender kann eigenen Server aufsetzen

OpenID Login

Sign In

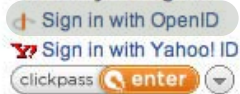
E-mail / AIM Screen Name:

Password:

Remember me

[Forgot password?](#)

Other ways to sign in:



Sign in to Plaxo using OpenID

A site identifying itself as all sites matching
http://anything.plaxo.com
has asked us for confirmation that
http://cocaman.myopenid.com/
is your identity URL.

The site also asked for additional information. It did not provide a link to the policy on data it collects. This is the persona we're going to send to plaxo.com:

Corsin Camichel

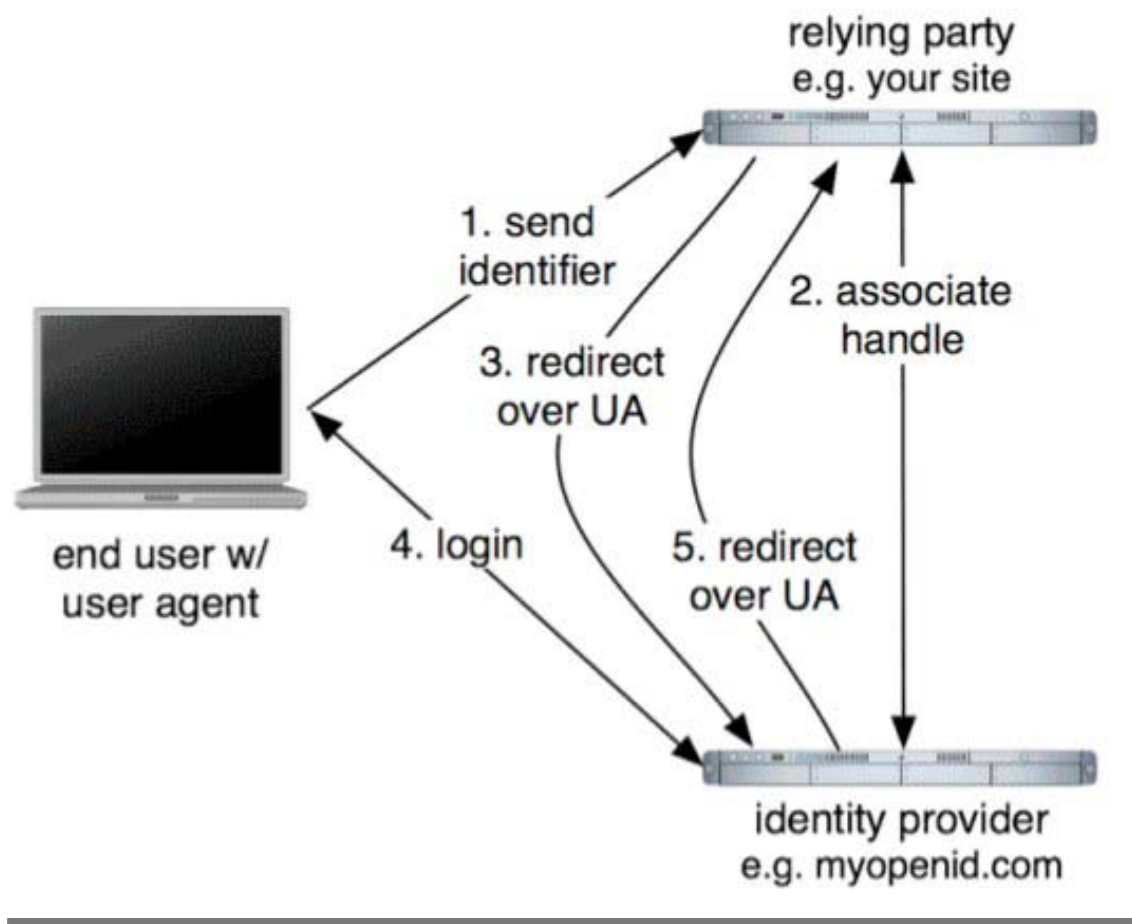


[Change this image](#)

Full Name	Corsin Camichel
Nickname	cocaman
Gender	Male
Birth Date	18 October, 1985
E-mail	cocaman@gmail.com
Postal Code	7031
Country	Switzerland
Language	English
Time Zone	Europe/Zurich

[Edit this persona](#)
[Delete this persona](#)

OpenID im Detail

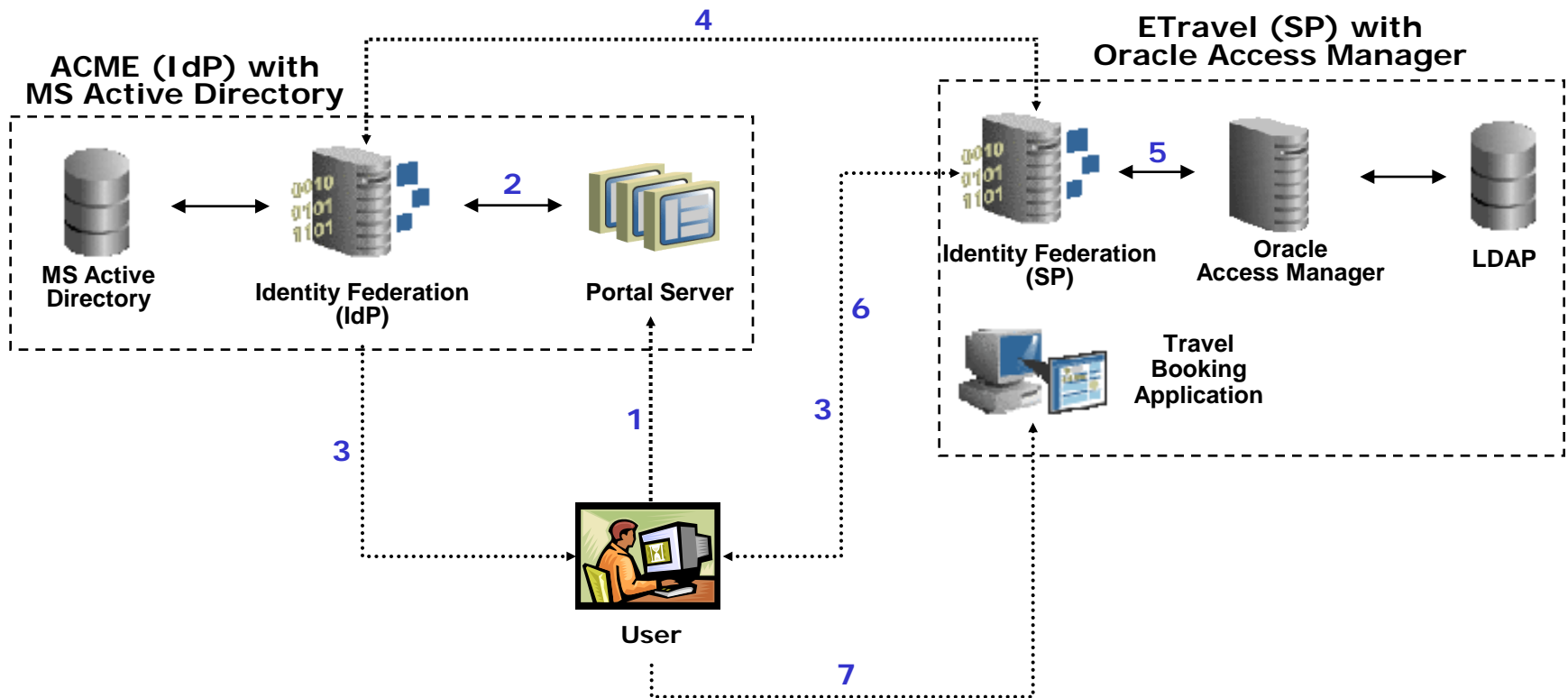


SAML 2.0

- Ideal für verteilte Identitäten
- Netzwerk des Vertrauens
- Identitäts-Provider
- Service-Provider
- Webanwendungen
- SOA-Anwendungen

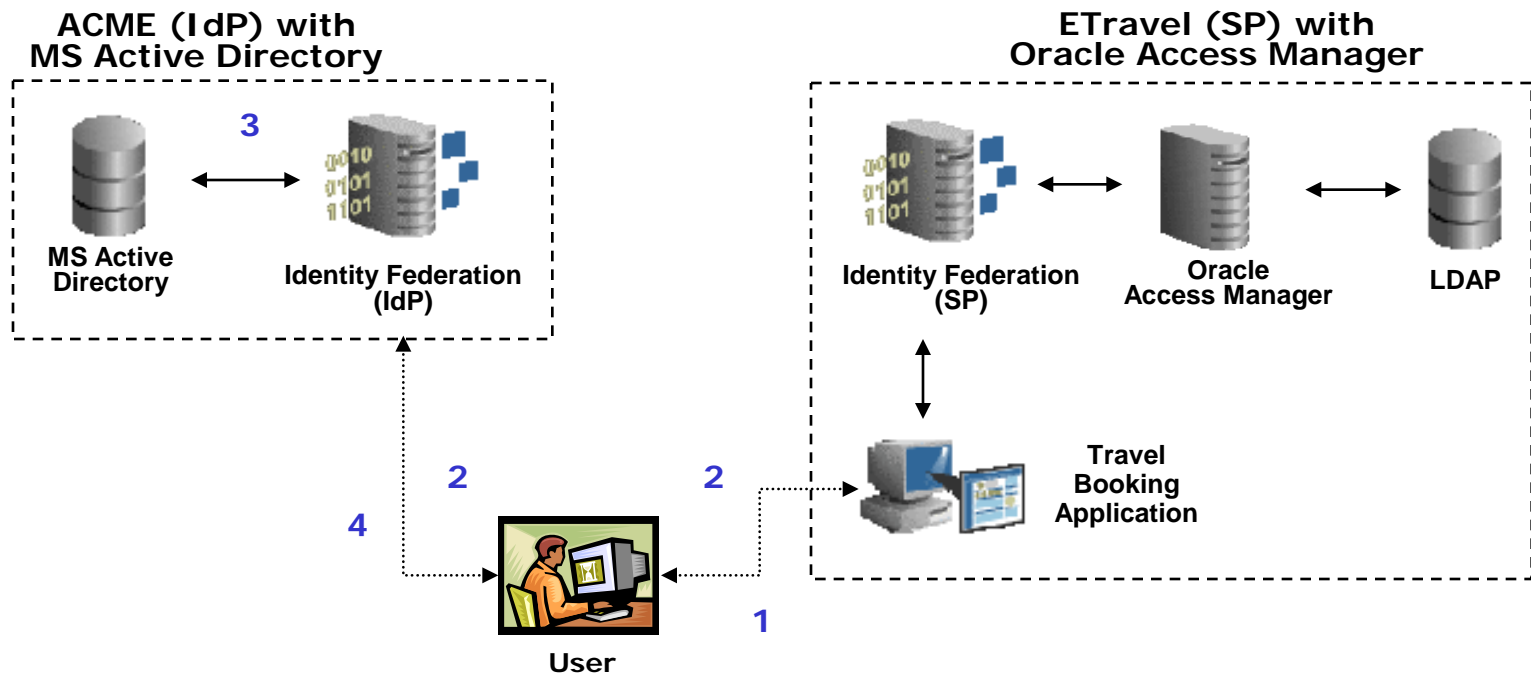
SAML 2.0: IdP-Initiated Browser Artifact Profile

The SAML Browser Artifact Profile passes a single sign-on assertion from the identity provider to the service provider by a reference, or artifact. The service provider then will de-reference the artifact through back channel communications and will pull the assertion directly from the identity provider.



SAML 2.0: SP-Initiated Browser POST Profile

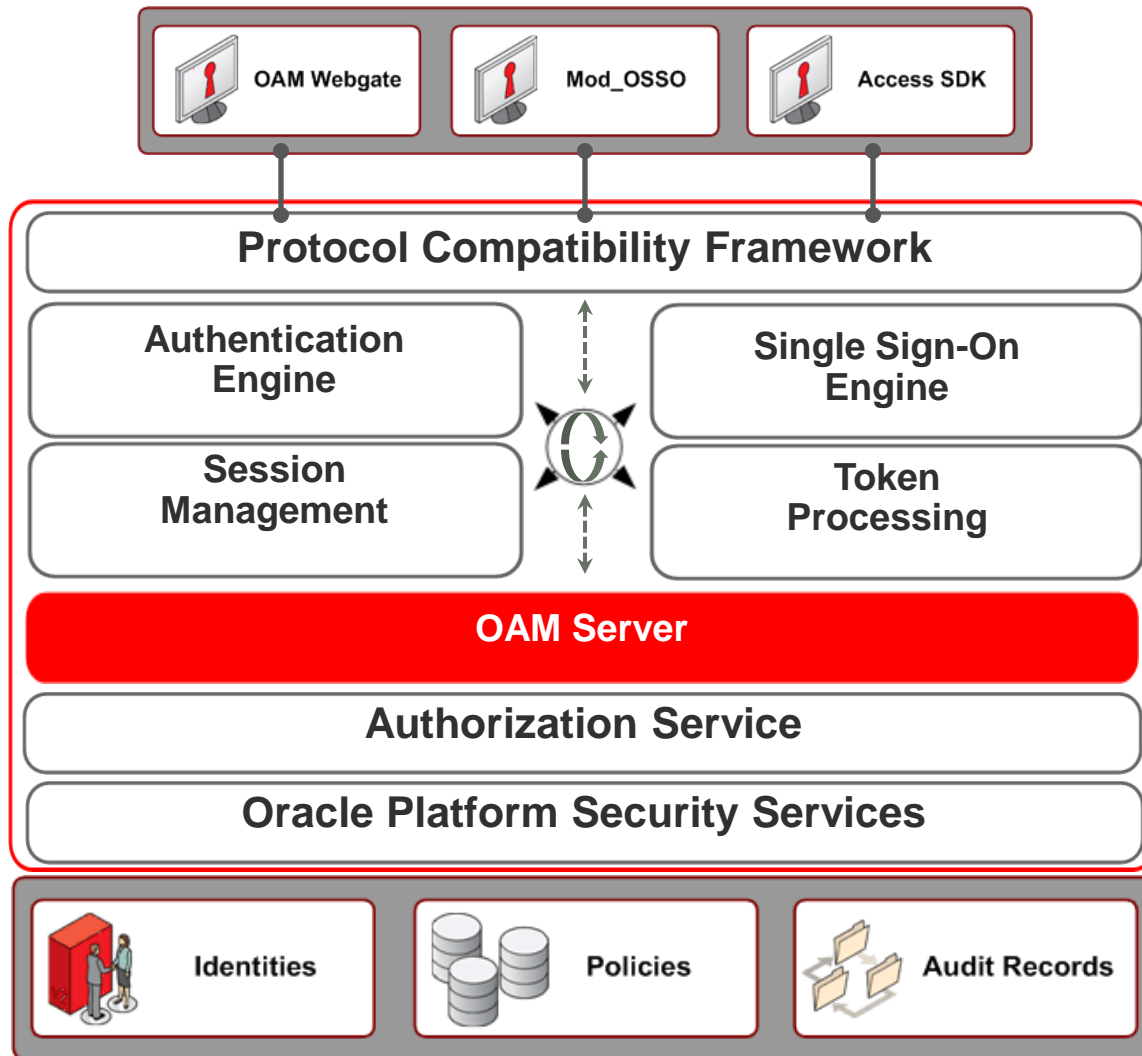
The SAML Browser POST Profile passes an SSO assertion by value via HTTP. No back-channel communication is needed in this case. In effect, the identity provider "pushes" the assertion to the service provider.



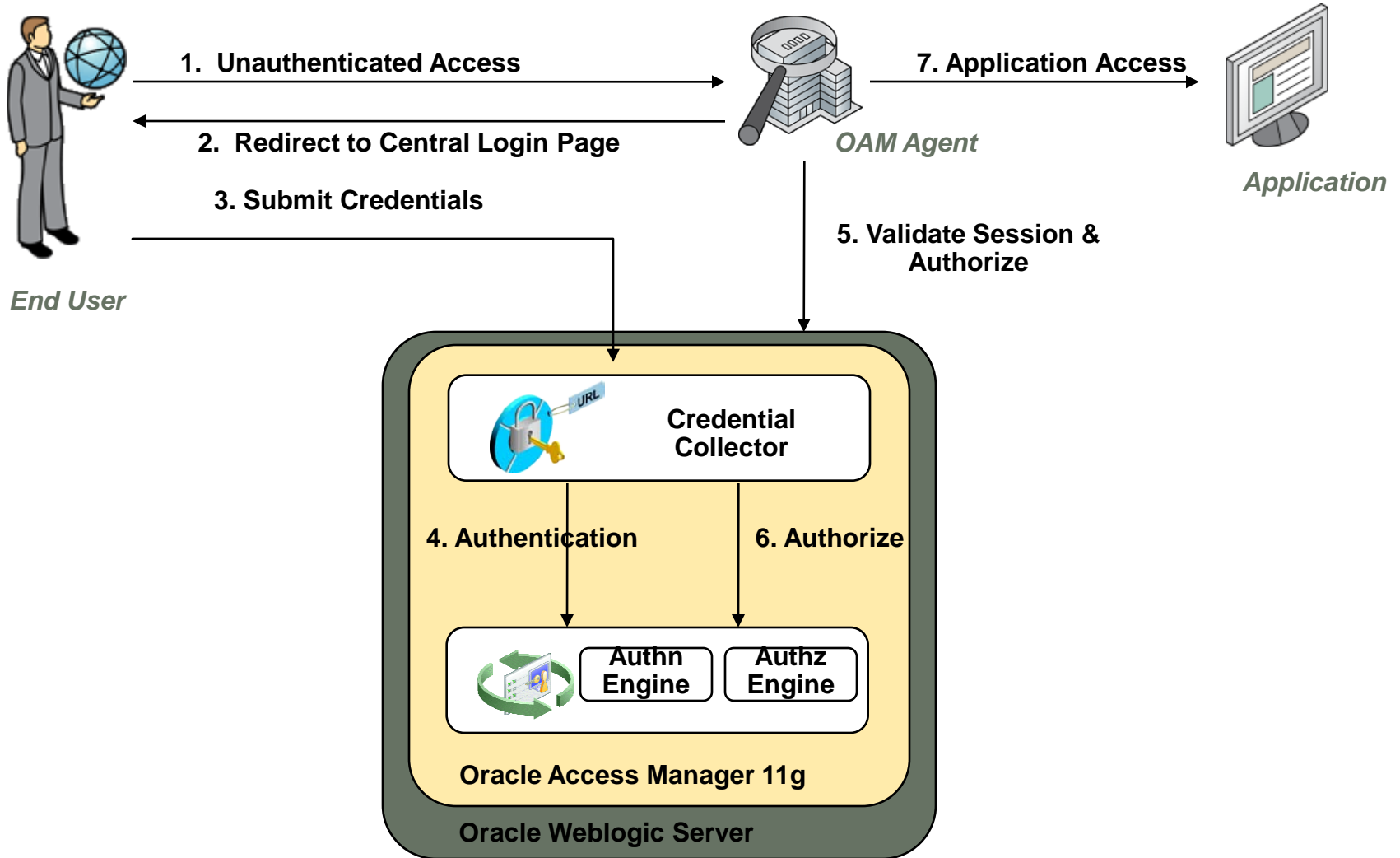
Oracle Access Manager (OAM)

- Absicherung von Ressourcen (URLs)
 - Authentifizierung
 - Autorisierung
- Unterschiedliche Klienten
 - Desktop, Browser, Fat-Client
- Unterschiedliche Mechanismen
 - Kerberos/WNA, SAML, Browser Login, Stand-alone

OAM Architektur



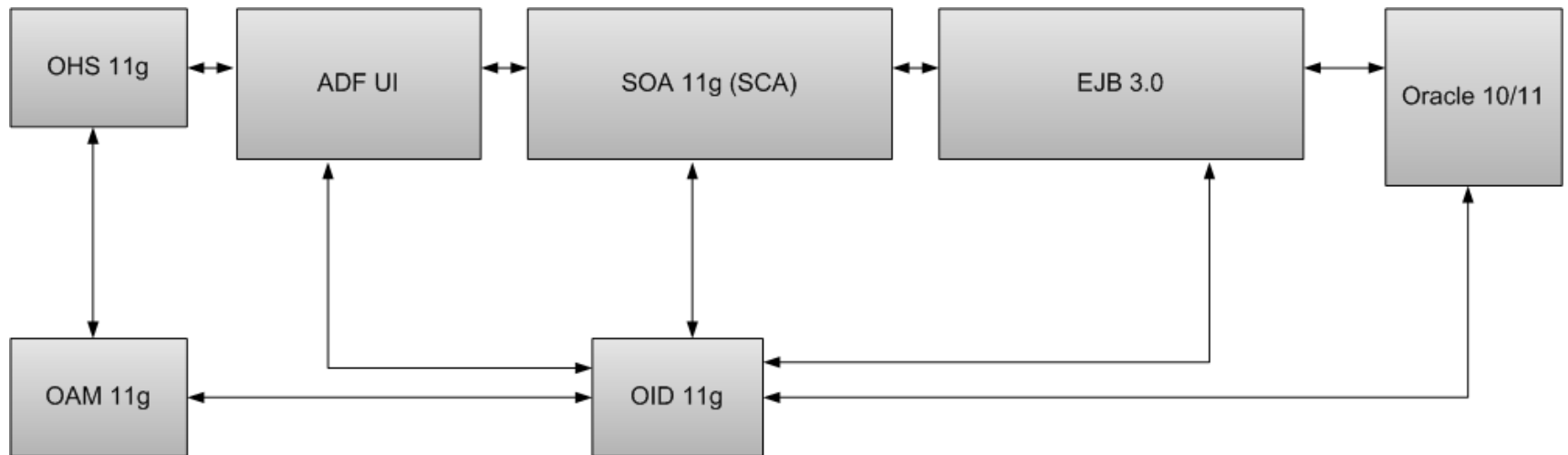
OAM Access Control



Beispielanwendung

- ADF Faces
- ADF Security
- OAM Login

Beispielanwendung



Hardware and Software Engineered to Work Together

ORACLE®