Sichere Webanwendungen mit den neuen Personalausweis
Der Geschichte zweiter Teil

Olaf Heimburger
CISSP, Principal Solution Architect
The A-Team
Oracle Deutschland B.V. & Co KG

Szene 1

Eine normale Webanwendung

Das ist Alice

Alice möchte ins Netz

Browser

URL eingeben

WebServer

URL kenne ich
Sie ist öffentlich
Also anzeigen.

Browser

Screenshot Anwendung

Browser

Klicken auf geschützten Bereich

WebServer

Oooh, da darf aber nicht jeder ran.
Login Seite anzeigen!

Browser

Login-Seite anzeigen.

Also, Alice, du must jetzt deine Informationen eingeben.

WebServer

Aha, das sind also die Login Informationen. Dann frage ich erstmal die Benutzerverwaltung…

LDAP

Hallo WebServer, gibt mir die Informationen.
Aha, Alice und ihr Passwort.

Super, alles richtig.

WebServer

OK, laut Benutzerverwaltung
stimmen die Daten von Alice!
Hallo Alice! Willkommen!

Browser

Hallo Alice! Willkommen!

Welche Probleme gibt es hier?

HTTP Anmeldeformate (Basic, Form-based, Certificate-based)
Individuell je Anwendung
Kein Single Sign-on

Szene 2

Eine normale Webanwendung?

Das ist Alice

Alice möchte ins Netz

Browser

URL eingeben

WebServer mit Agent

Was ist mit dieser URL?
Darf ich sie so einfach zeigen?

OAM Server

Knifflig, welche URL?

Lass mal sehen…

OAM Server – Policy prüfen

URL A passt und ist öffentlich

also einfach anzeigen!

WebServer mit Agent

OK, anzeigen ohne weitere Abfrage erlaubt. Na dann…

Browser

Screenshot Anwendung

Browser

Klicken auf geschützten Bereich

WebServer mit Agent

Was ist mit dieser URL?
Darf ich sie so einfach zeigen?

OAM Server

Knifflig, welche URL?

Lass mal sehen…

OAM Server – Policy prüfen

URL B passt und ist geschützt!

Kenne ich den Benutzer schon?

Nein, also brauche ich mehr Informationen!

OAM Server

Sende Redirect zur Login-Seite an Browser

Browser

OK, ich soll mir die URL C laden, na dann mal los…

OAM Server

Also die Login-Seite soll es sein, hier ist sie.

Browser

Login-Seite

Alice

Benutzername und Passwort
eingeben und Anmelden drücken…

OAM Server – Anmeldung

Her mit den Informationen!

Aha, also dann frage ich mal die Benutzerverwaltung…

LDAP

Hallo WebServer, gibt mir die Informationen.
Aha, Alice und ihr Passwort.

Super, alles richtig.

OAM Server – Anmeldung

Prima, alles OK.
Das merke ich mir und sage dem Agenten Bescheid…

WebServer mit Agent

Aha, Alice darf diese Seiten sehen und ich soll mir das merken…
Ich bin doch nicht blöd, das macht Alice für mich!

Hallo Alice! Willkommen!

Browser

Hallo Alice! Willkommen!

Welche Probleme gibt es hier?

HTTP Basic, HTTP Form-based, HTTP Certificate-based, Kerberos
Single Login
Single Sign-on
Standard Lösung
Keine zusätzliche Entwicklung nötig
Erweiterbar

Szene 3

Eine normale Webanwendung!

Das ist Alice

Alice möchte ins Netz

Browser

URL eingeben

WebServer mit Agent

Was ist mit dieser URL?
Darf ich sie so einfach zeigen?

OAM Server

Knifflig, welche URL?

Lass mal sehen…

OAM Server – Policy prüfen

URL A passt und ist öffentlich

also einfach anzeigen!

WebServer mit Agent

OK, anzeigen ohne weitere Abfrage erlaubt. Na dann…

Browser

Screenshot Anwendung

Browser

Klicken auf geschützten Bereich

WebServer mit Agent

Was ist mit dieser URL?
Darf ich sie so einfach zeigen?

OAM Server

Knifflig, welche URL?

Lass mal sehen…

OAM Server – Policy prüfen

URL B passt und ist geschützt!

Kenne ich den Benutzer schon?

Nein, also brauche ich mehr Informationen!

OAM Server

Sende Redirect zur Login-Seite an Browser

Browser

OK, ich soll mir die URL C laden, na dann mal los…

OAM Server

Also die Login-Seite soll es sein, hier ist sie.

Browser

Login-Seite

Alice

Benutzername und Passwort
eingeben und Anmelden drücken…

OAM Server – Anmeldung

Her mit den Informationen!

Aha, also dann frage ich mal die Benutzerverwaltung…

LDAP

Hallo WebServer, gibt mir die Informationen.
Aha, Alice und ihr Passwort.

Super, alles richtig.

OAM Server – Anmeldung

Prima, alles OK.
Das merke ich mir und sage dem Agenten Bescheid…

WebServer mit Agent

Aha, Alice darf diese Seiten sehen und ich soll mir das merken…
Ich bin doch nicht blöd, das macht Alice für mich!

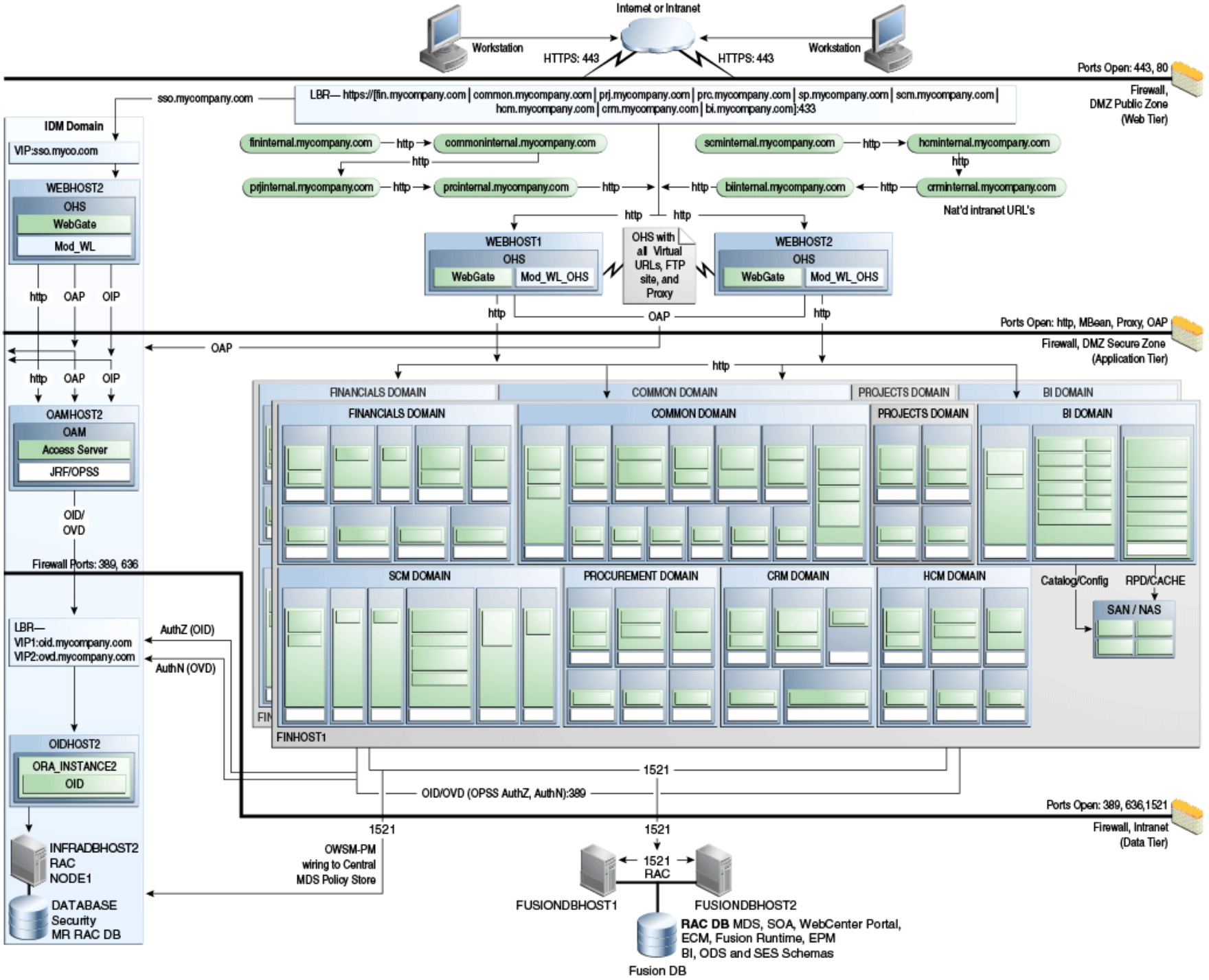
Hallo Alice! Willkommen!

Browser

Hallo Alice! Willkommen!

Welche Probleme gibt es hier?

HTTP Basic, HTTP Form-based, HTTP Certificate-based, Kerberos
Single Login
Single Sign-on
Standard Lösung
Keine zusätzliche Entwicklung nötig, keine Änderung an Anwendung
Erweitert um SAML 2.0 Support
Kartenleser notwendig


Internet or Intranet
Workstation
HTTPS: 443
HTTPS: 443
Workstation
Ports Open: 443, 80
Firewall,
DMZ Public Zone
(Web Tier)
sso.mycompany.com
LBR— https://[fin.mycompany.com | common.mycompany.com | prj.mycompany.com | prc.mycompany.com | sp.mycompany.com | scm.mycompany.com | hcm.mycompany.com | crm.mycompany.com | bi.mycompany.com]:433
IDM Domain
VIP:sso.myco.com
WEBHOST2
OHS
WebGate
Mod_WL
fininternal.mycompany.com
commoninternal.mycompany.com
scminternal.mycompany.com
hcminternal.mycompany.com
prjinternal.mycompany.com
prcinternal.mycompany.com
biinternal.mycompany.com
crminternal.mycompany.com
Nat'd intranet URL's
http
WEBHOST1
OHS
WebGate
Mod_WL_OHS
OHS with all Virtual URLs, FTP site, and Proxy
WEBHOST2
OHS
WebGate
Mod_WL_OHS
OAP
OIP
Ports Open: http, MBean, Proxy, OAP
Firewall, DMZ Secure Zone
(Application Tier)
OAMHOST2
OAM
Access Server
JRF/OPSS
OID/
OVD
Firewall Ports: 389, 636
FINANCIALS DOMAIN
COMMON DOMAIN
PROJECTS DOMAIN
BI DOMAIN
SCM DOMAIN
PROCUREMENT DOMAIN
CRM DOMAIN
HCM DOMAIN
Catalog/Config
RPD/CACHE
SAN / NAS
FINHOST1
LBR—
VIP1:oid.mycompany.com
VIP2:ovd.mycompany.com
AuthZ (OID)
AuthN (OVD)
OIDHOST2
ORA_INSTANCE2
OID
1521
OID/OVD (OPSS AuthZ, AuthN):389
Ports Open: 389, 636,1521
Firewall, Intranet
(Data Tier)
INFRADBHOST2
RAC
NODE1
DATABASE
Security
MR RAC DB
OWSM-PM
wiring to Central
MDS Policy Store
1521
RAC
FUSIONDBHOST1
FUSIONDBHOST2
RAC DB MDS, SOA, WebCenter Portal,
ECM, Fusion Runtime, EPM
BI, ODS and SES Schemas
Fusion DB

Mehr Informationen!

olaf.heimburger@oracle.com
blogs.oracle.com/olaf