Sichere Webanwendungen mit dem elektronischen Personalausweis Teil 2

Olaf Heimburger
Oracle Deutschland B.V. & Co. KG
Berlin

Schlüsselworte
Sicherheit, Fusion Applications, Web Anwendungen, neuer Personalausweis, OIF, OAM, IDM.

Einleitung

Der erste Teil auf der DOAG 2011 zeigte die Grundlagen für die Integration des elektronischen Personalausweises mit Webanwendungen. Nun gehen wir einen Schritt weiter. Die Webanwendungen ist definiert und der IDM Stack ist bereits vorhanden. Nun brauchen wir nur noch den elektronischen Personalausweis zu integrieren?! Aber sicher!

Rückblende

Was hat sich in einem Jahr getan? Kaum wahrnehmbar werden die neuen Personalausweise ausgestellt. Der starke Ansturm durch nPA-Verweigerer vor dem Oktober 2010 ist Geschichte und die Normalität ist eingekehrt. Kartenlesegeräte gibt es mittlerweile schon beim Elektronikmarkt um die Ecke und die Gesundheitskarte wird nach und nach eingeführt. Es werden also weitere Infrastrukturen geschaffen.

Auf der anderen Seite reißen die Schlagzeilen der Einbrüche nicht ab. Es vergeht nahezu kein Tag ohne Meldungen über gestohlene sensible Daten. Werden die vorhandenen Infrastrukturen überhaupt genutzt?

Leider noch nicht, denn wir befinden uns noch in der Übergangszeit.

Hürden für den Einsatz

Gegen Einsatz spricht vieles. So sind die bestehenden Webanwendungen noch nicht breit, oder die Hardware (Kartenleser) steht nicht zur Verfügung. Oder, viel schwerwiegender, die Benutzer haben den neuen Personalausweis noch nicht. Aber, muss es denn alles mit einem Mal verfügbar sein (Big Bang) und diejenigen ausschließen die nicht über den neuen Personalausweis verfügen? Auf gar keinen Fall! Aber wie soll das gepflegt werden? Und wer hat die Zeit dazu?

Kriterien für den Einsatz

Die Kriterien für den Einsatz entsprechen den auf der DOAG 2011 im Teil 1 des Vortrages vorgestellten. Sie betreffen den Anwender, die Anwendung, die Hardware und die Software

Anwender

Wie bereits im ersten Teil postuliert, muss der Anwender in der Lage sein, die Anwendung mit möglichst wenig eigenem Aufwand verwenden zu können. Gerade für die Übergangszeit müssen bei der Anmeldung alternative Methoden erlaubt sein.

Anwendung
Auch hier stimmen die Anforderungen aus Teil 1 immer noch, die Technologiebasis muss einheitlich sein und für die Anwendung transparent sein. Am besten ändert sich gar nichts für die Anwendung sondern es werden zusätzliche Verfahren angeboten.

Implementierung
Bei der Implementierung sollte es immer möglich sein, Änderungen durch neue Konfigurationen zu erreichen. Neuentwicklungen die ggf. Varianten oder gar neue Produkte erfordern sollten weitgehend vermieden werden.

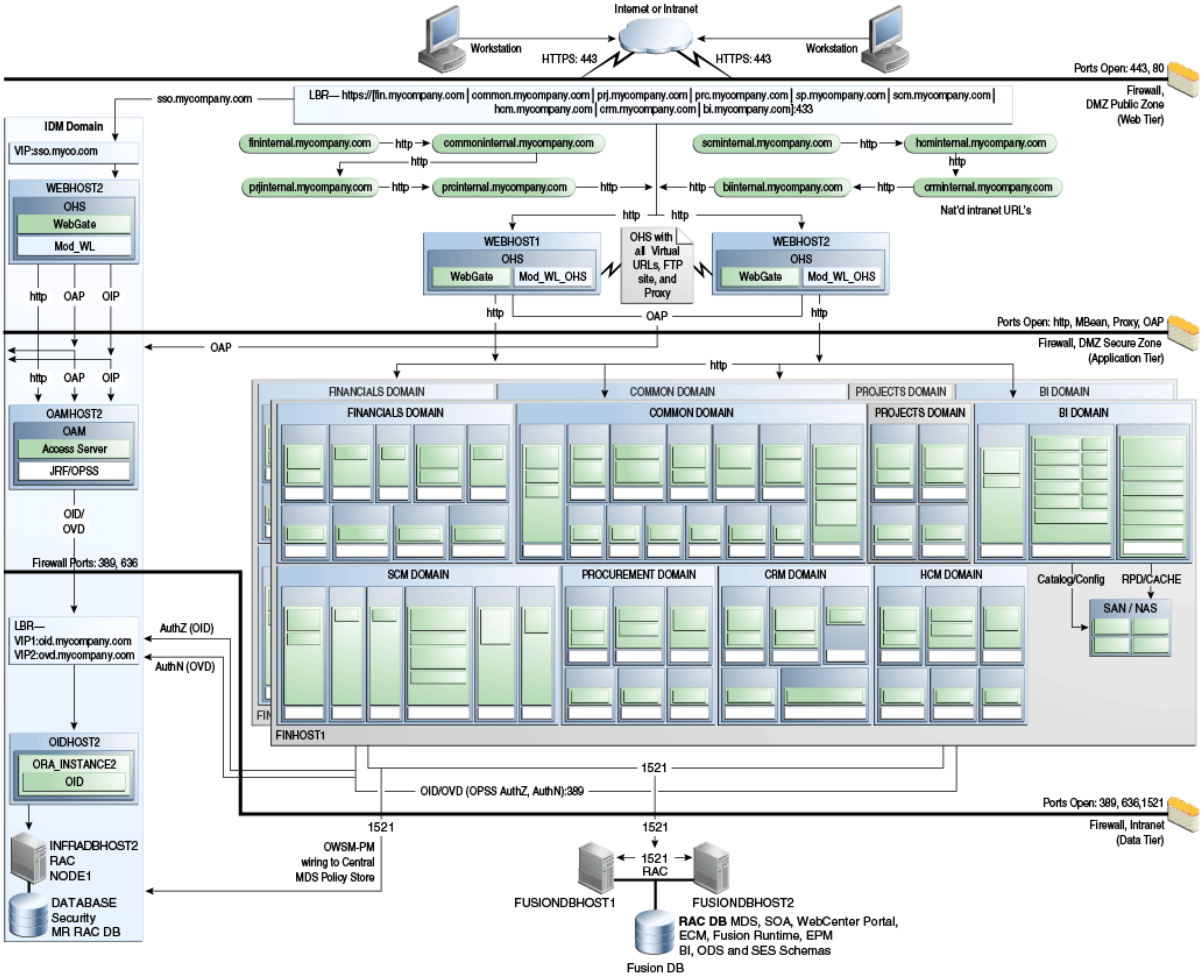
Hardware
Natürlich hat sich hier noch nicht viel geändert. Das Bedrohungspotential hat sich eher noch verstärkt und die Tricks sind rafinierter geworden. Möglichkeiten die Identifizierung der Anwender, die nicht den direkten Weg über manipulierbare Systeme gehen, vornehmen zu lassen sind dabei zu bevorzugen. Ideal ist immer noch der Kartenleser mit eigener Tastatur.

Schutz der Karte
Der neue Personalausweis enthält einen RFID-Chip der berührungslos auszulesen ist. Innerhalb einer bestimmten Entfernung ist dies möglich ohne das der Anwender dies merkt. Es wird daher empfohlen den neuen Personalausweis in einer abschirmenden Hülle aufzubewahren.

Fusion Applications
Unternehmensweite, kaufmännischen Anwendung bringen eine spezifische Qualität in die IT-Landschaft und erfordern Infrastrukturen die evt. vorher nicht geplant waren.

Fusion Applications ist hier keine Ausnahme. Die gute Nachricht ist aber, dass viele Bausteine schon mitgeliefert und bereits funktionsfähig installiert werden. Die wichtigste Komponente in der nachfolgenden Referenzarchitektur ist der Oracle Identity and Access Management Stack.

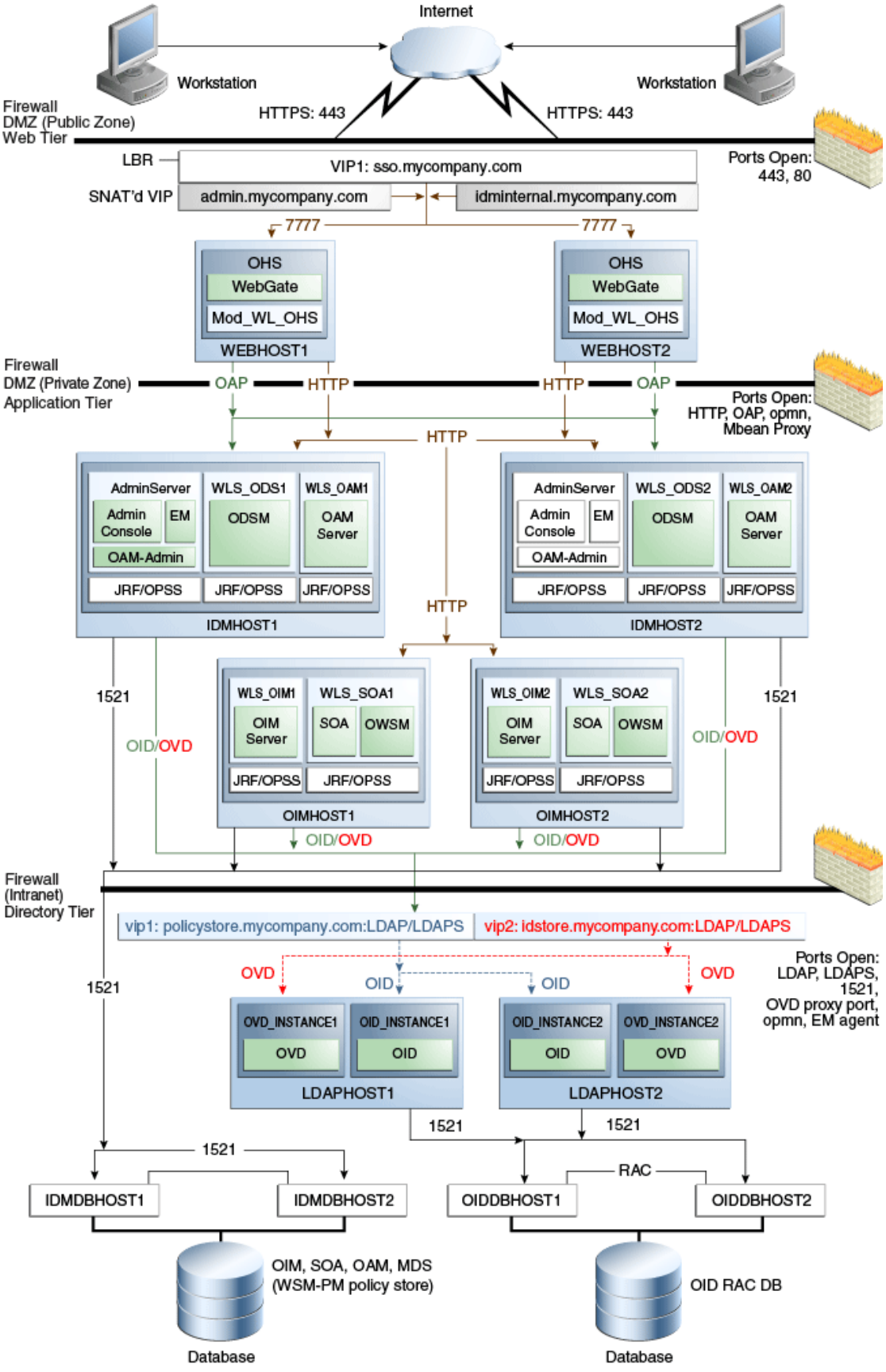
Eine typische Fusion Applications Architektur sieht wie folgt aus:



(Quelle: Fusion Applications Concepts Guide)

Oracle Identity and Access Management Stack

Der in Fusion Applications verwendete Oracle Identity and Accessmanagment Stack bietet vielfältige Möglichkeiten die Identifizierung der Anwender vornehmen zu können.


Internet
Workstation
Workstation
HTTPS: 443
HTTPS: 443
Firewall
DMZ (Public Zone)
Web Tier
LBR
VIP1: sso.mycompany.com
SNAT'd VIP
admin.mycompany.com
idminternal.mycompany.com
Ports Open:
443, 80
7777
7777
OHS
WebGate
Mod_WL_OHS
WEBHOST1
OHS
WebGate
Mod_WL_OHS
WEBHOST2
Firewall
DMZ (Private Zone)
Application Tier
OAP
HTTP
HTTP
OAP
Ports Open:
HTTP, OAP, opmn,
Mbean Proxy
HTTP
AdminServer
Admin Console
EM
OAM-Admin
WLS_ODS1
ODSM
WLS_OAM1
OAM Server
JRF/OPSS
JRF/OPSS
JRF/OPSS
IDMHOST1
AdminServer
Admin Console
EM
OAM-Admin
WLS_ODS2
ODSM
WLS_OAM2
OAM Server
JRF/OPSS
JRF/OPSS
JRF/OPSS
IDMHOST2
HTTP
1521
OID/OVD
WLS_OIM1
OIM Server
WLS_SOA1
SOA
OWSM
JRF/OPSS
JRF/OPSS
OIMHOST1
WLS_OIM2
OIM Server
WLS_SOA2
SOA
OWSM
JRF/OPSS
JRF/OPSS
OIMHOST2
1521
OID/OVD
OID/OVD
OID/OVD
Firewall
(Intranet)
Directory Tier
vip1: policystore.mycompany.com:LDAP/LDAPS
vip2: idstore.mycompany.com:LDAP/LDAPS
Ports Open:
LDAP, LDAPS,
1521,
OVD proxy port,
opmn, EM agent
1521
OVD
OID
OID
OVD
OVD_INSTANCE1
OVD
OID_INSTANCE1
OID
LDAPHOST1
OID_INSTANCE2
OID
OVD_INSTANCE2
OVD
LDAPHOST2
1521
1521
1521
RAC
IDMDBHOST1
IDMDBHOST2
OIDDBHOST1
OIDDBHOST2
OIM, SOA, OAM, MDS
(WSM-PM policy store)
Database
OID RAC DB
Database

Die zentrale Komponente ist dabei der Oracle Access Manager. Er dient als Schaltzentrale für die gewünschten Identifizierungsmethoden und sorgt, dafür dass nur authentifizierte und authorisierte Anwender an die erlaubten Stellen der Anwendung gelangen.

Einsatz des neuen Personalausweises
Damit der neue Personalausweis in dieser Architektur verwendet werden kann, müssen wir dem Oracle Access Manager das Produkt Oracle Identity Federation zur Seite stellen. Der Oracle Access Manager wird entsprechend konfiguriert und delegiert die Authentifizierung an Oracle Identity Federation. Ist die Authentifizierung erfolgreich, erlaubt der Oracle Access Manager den Zugang.

Das Ergebnis
Natürlich sind Worte nur leere Hülsen wenn die beschriebenen Ansätze nicht nachgeweisen werden können. Der Nachweis erfolgt während des Vortrages.

Kontaktadresse:
Olaf Heimburger
Oracle Deutschland B.V. & Co. KG
Schloßstr. 2
D-13507 Berlin

Telefon: +49 (0) 30 435 795-160
Fax: +49 (0) 30 435 795-419
E-Mail: olaf.heimburger@oracle.com
Internet: blogs.oracle.com/olaf