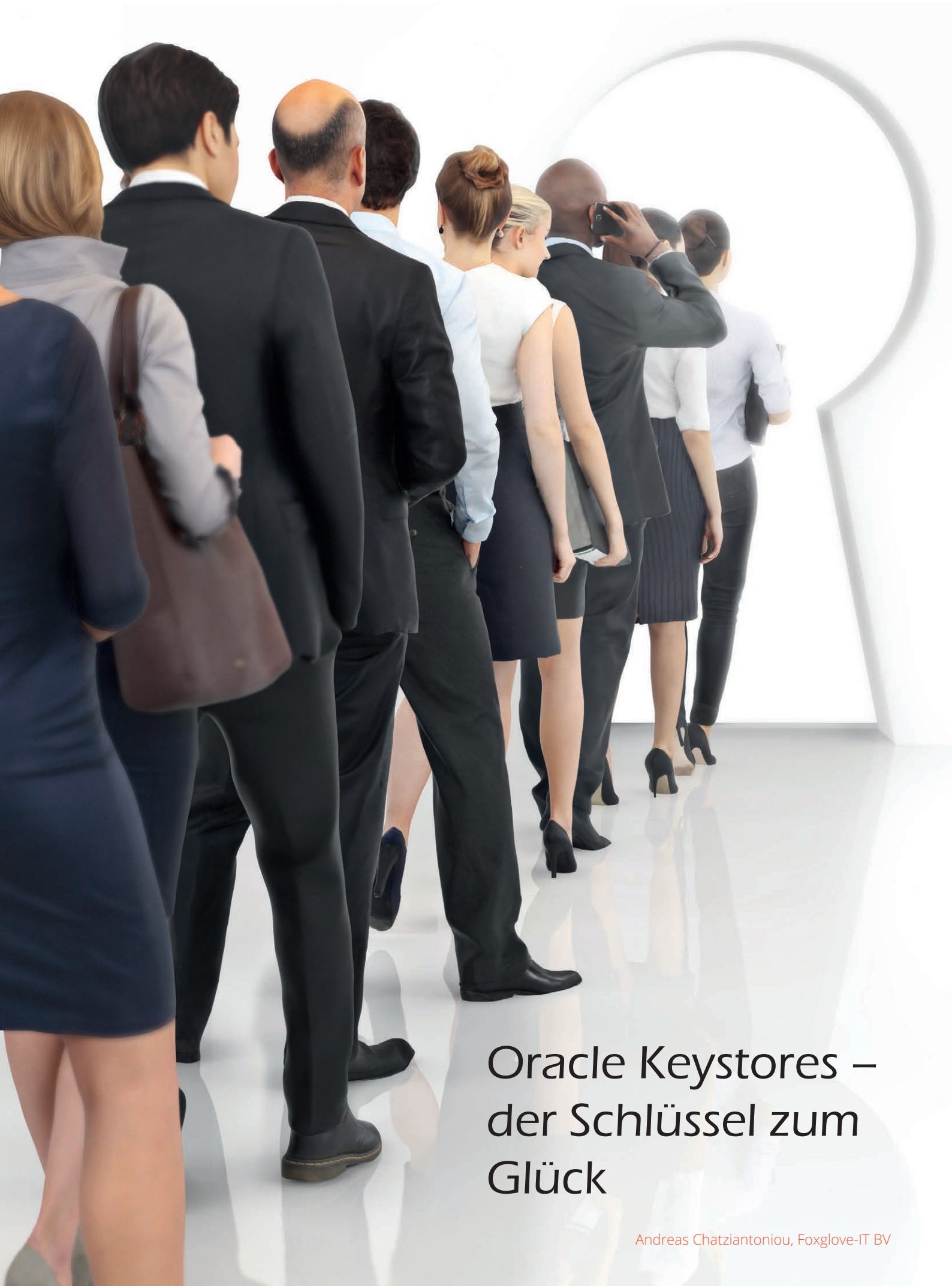

Oracle Keystores – der Schlüssel zum Glück

Andreas Chatziantoniou, Foxglove-IT BV

Seit WebLogic 12 gibt es im Rahmen der Oracle Platform Security Services (OPSS) den Keystore Service (KSS). Dieser Artikel zeigt anhand von Beispielen und einer End-to-End-Einbettung, wie die verschiedenen Fusion-Middleware-Komponenten mit OPSS und dem KSS arbeiten können. Außerdem werden die Unterschiede zum bisherigen Java-Keystore-Format (JKS) aufgezeigt.

„Security" ist seit Beginn der IT ein Thema. Betrachtet man die Komponenten eines IT-Systems, ist der Zugang zu den Daten wahrscheinlich der sensibelste Teil, auf dem Sicherheitsmechanismen greifen müssen. Denn wer die Daten kontrolliert, braucht sich nicht mehr um die verschiedenen Lagen der Zugangskontrolle in den darüberliegenden Schichten zu kümmern. Normalerweise bietet die Oracle-Datenbank genügend Möglichkeiten, um die Daten zu schützen – ob das nun die normalen Rollen und Rechte auf Tabellen sind, Virtual Private Database, Label Security, Transparent Data Encryption etc. Man kann davon ausgehen, dass die Daten nur denjenigen zugänglich sind, die diesen Zugang auch haben.

Eine Ebene höher – auf dem Niveau des Application-Servers – muss ein vergleichbares Konstrukt vorhanden sein, um die Zugangskontrolle zu implementieren. Die Oracle Keystores sind Teil der Oracle Platform Security Services. *Abbildung 1* zeigt deren Position innerhalb des OPSS.

Alle Keys des Oracle Keystore sind im zentralen OPSS Security Store abgelegt. Dieses kann entweder Datei-, LDAP- oder Datenbank-basiert sein – das wird beim Anlegen des OPSS Security Store festgelegt. Das Anlegen kann mithilfe des Repository Creation Utility (RCU), des Enterprise Manager oder per Skript erfolgen.

Das Konzept des KSS ist darauf ausgelegt, in einfachen Umgebungen zu funktionieren, bietet jedoch auch die Unterstützung für komplexe Set-ups. Die Datei-basierte Konfiguration ist sicherlich für Stand-alone-Umgebungen geeignet, läuft aber gegen die Grenze, wenn eine Hochverfügbarkeit erforderlich ist. Dann sollte der KSS in einem LDAP-Server beziehungsweise in einer Datenbank abgelegt sein. Diese müssen dann durch geeignete Mittel (LDAP-Replikation, Datenbank RAC, eventuell erweitert mit Data Guard) so eingerichtet sein, dass Multi-Datacenter-Set-ups unterstützt sind.

Abbildung 2 zeigt, wie eine Anwendung über das Credential Store Framework (CSF) den Credential Store (KSS) benutzt. Dabei holt das CSF die Credentials (Benutzername, Password, Keys etc.) aus dem Credential Store ab. Wichtig für den sicheren Betrieb der Anwendung ist die gleichzeitige Einbindung des Auditing, um die korrekte Funktionsweise der Anwendung zu überwachen.

Der Oracle Keystore Service enthält verschiedene Möglichkeiten zum Lifecycle Management. Diese sind unter anderem:

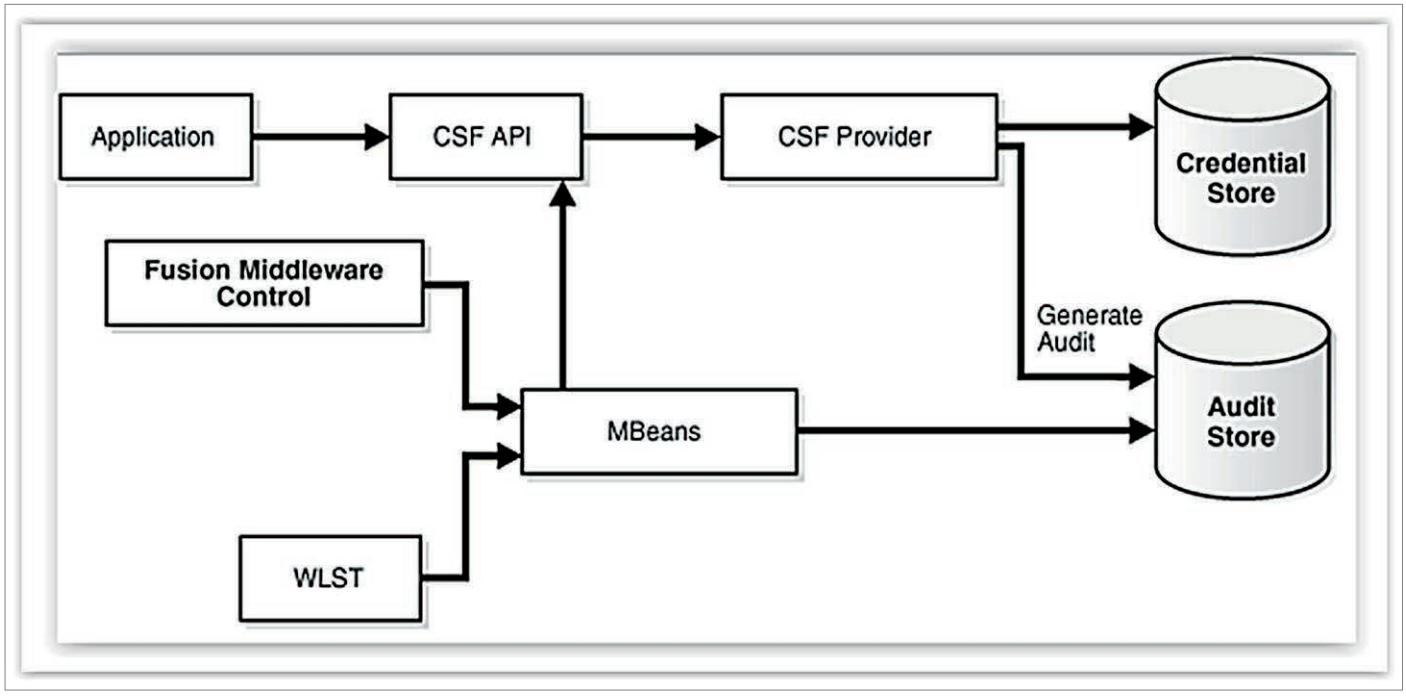

Abbildung 1: Die Position der Oracle Keystore innerhalb des OPSS

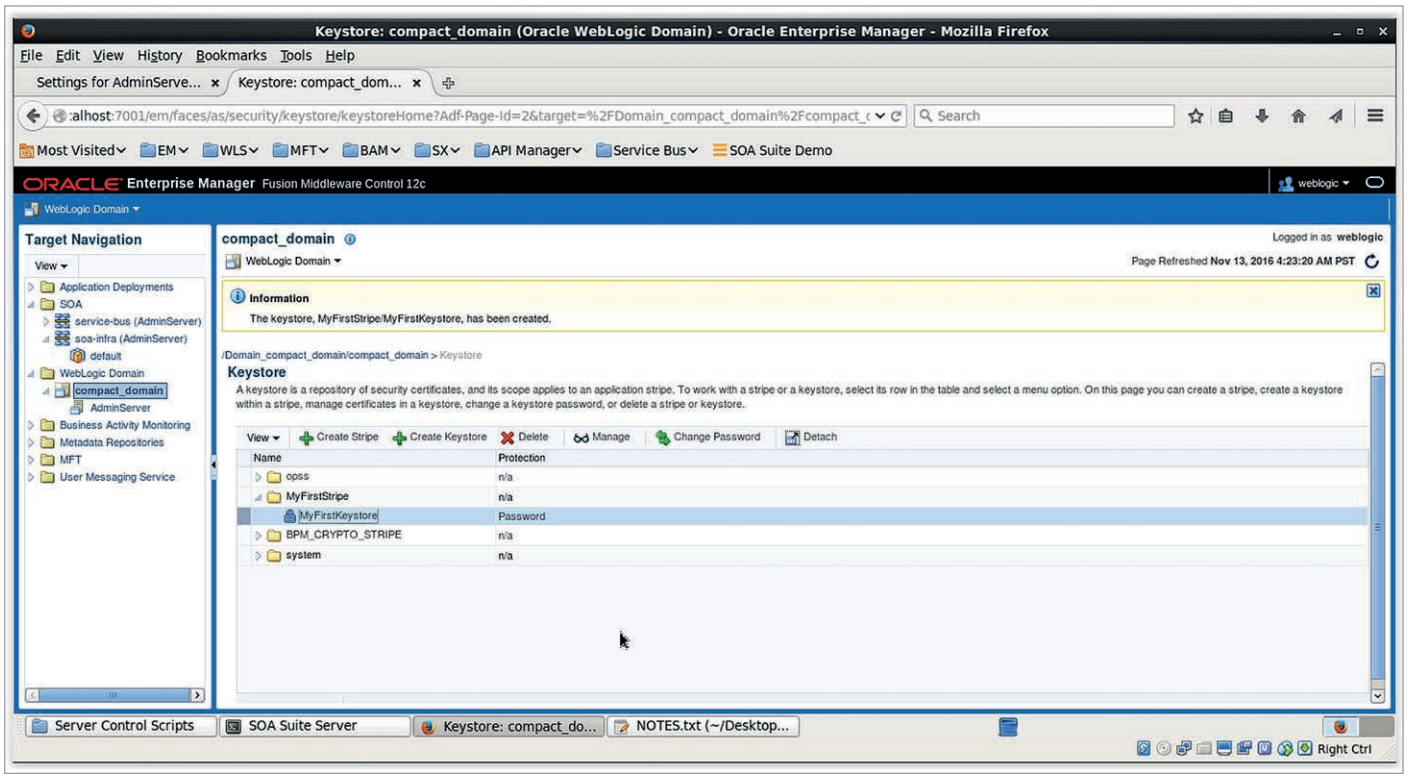

Abbildung 2: OPSS Security Services sind in den Management-Tools der Oracle Fusion Middleware integriert. Dadurch können die OPSS Security Policies und Konfigurationen mit den bekannten Werkzeugen (wie Fusion Middleware Console, WebLogic Scripting Tool, JMX MBeans) ausgeführt werden.

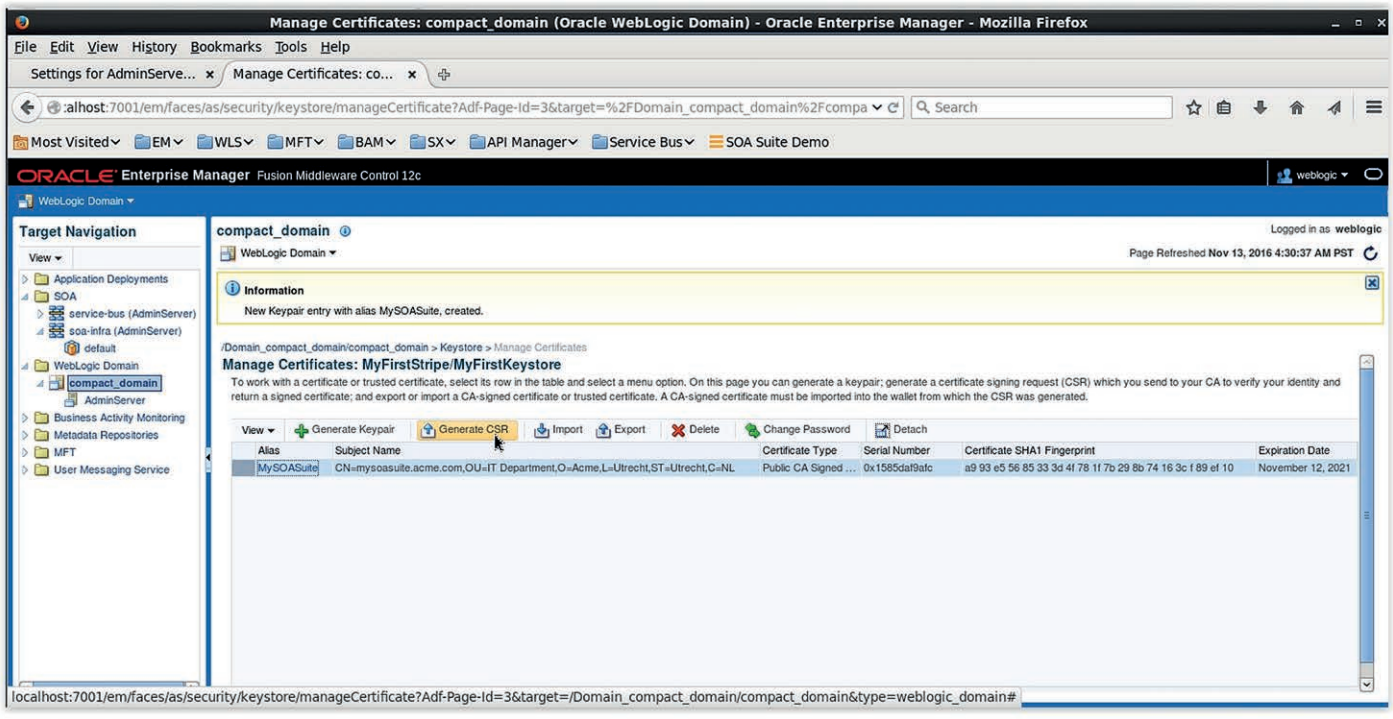

Abbildung 3: Ein Keystore in der FMW-Console

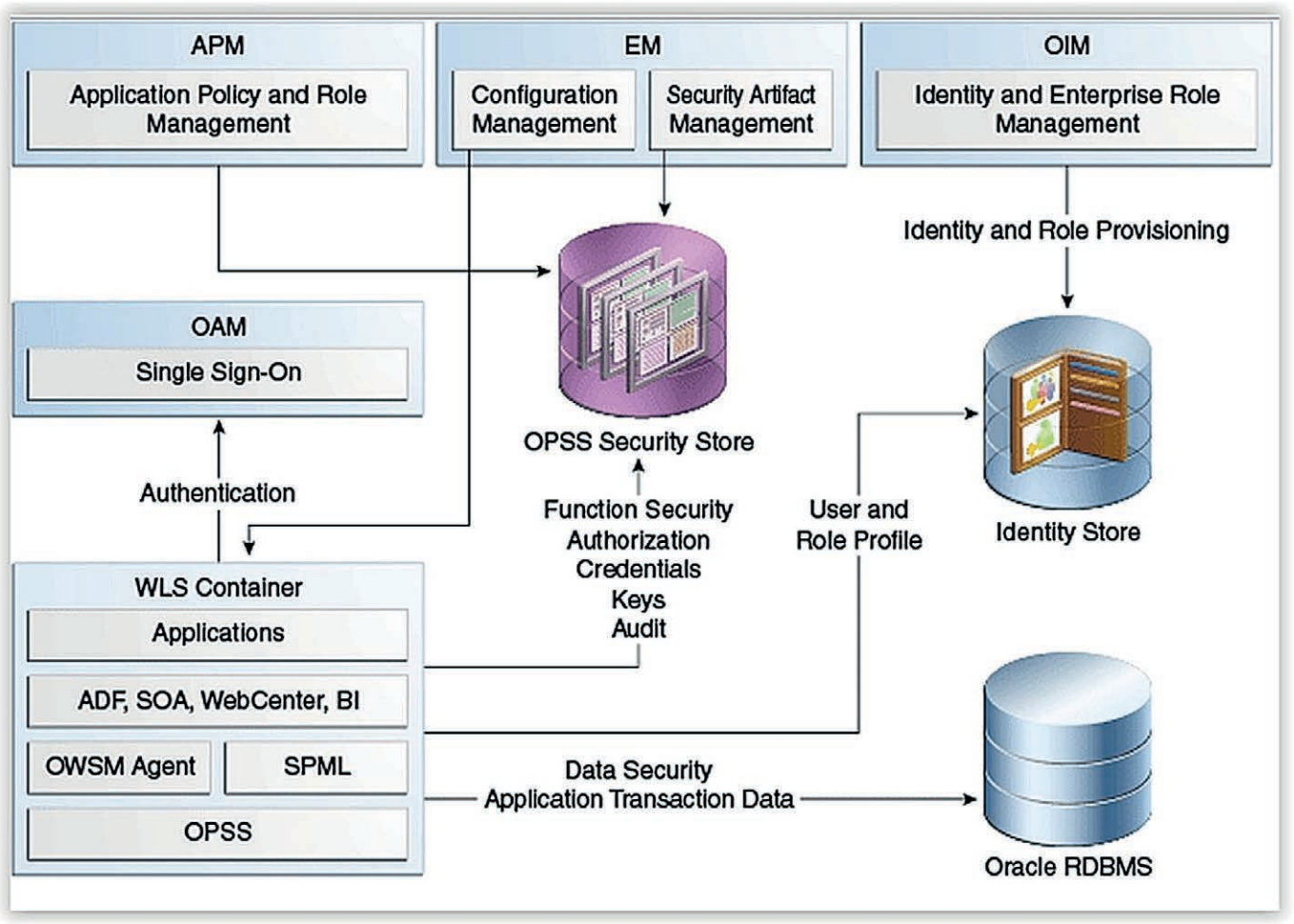

Abbildung 4: Ein Beispiel mit der FMW-Console

- Anlegen des KSS
- Update des KSS
- Löschen des KSS
- Import und Export
- Password-Änderung des KSS

Die Lifecycle-Management-Optionen sind im WebLogic Scripting Tool (WLST) und in der Fusion Middleware Console vorhanden. *Abbildung 3* zeigt einen Keystore in der Fusion Middleware Console.

Da die Sicherheit in IT-Systemen üblicherweise von Certificates abhängt, bietet der Oracle Keystore Service die Unterstützung des Certificate Management. Zu den Funktionen gehören:

- Anlegen eines Keypair
- Anlegen eines Certificate Signing Request
- Import und Export von Certificates
- Löschen eines Certificate

Auch hier sind alle Funktionen von der Fusion Middleware Console oder dem WLST ausführbar *(siehe Abbildung 4)*. Zudem können auch bestehende Certificates aus einem Java Keystore oder einer Oracle Wallet importiert werden.

Wie gezeigt, können Anwendungen die Daten des KSS benutzen, indem das CSF genutzt wird. Das CSF bietet ein API, mit dem die wichtigen Aktionen rund um den Credential Store ausgeführt werden können, wie Certificates aus einem Store holen, den Store und den Inhalt verifizieren oder die Zugangsdaten zum Store verändern. Dies erlaubt einem Entwickler dann, das Certificate aus dem Store zu extrahieren und dieses Certificate zum Verschlüsseln einzusetzen (beispielsweise mit der Java Cryptography Architecture).

Andreas Chatziantoniou
andreas@foxglove-it.nl