# Kerberos Geheimnisse in der Oracle Datenbank Welt

**Helmut Eckstein**
**Pepperl+Fuchs GmbH**
**Mannheim**

**Suvad Sahovic**
**ORACLE Deutschland B.V. & Co. KG**
**Potsdam**

**Schlüsselworte:**

Oracle Datenbank Server, Kerberos, Oracle Advanced Security, Kerberos Authentication Adapter, Oracle SQL Developer, MS Excel, MS Access, Quest TOAD, Microsoft Active Directory, MS AD, DB Links, Authentisierung/Authentifizierung

**Einleitung**

Pepperl+Fuchs betreibt ein Rechenzentrum in Mannheim, in dem das ERP System M3 der Firma Infor und das CRM System Siebel der Firma Oracle zentral für alle Niederlassungen weltweit 24x7 zur Verfügung gestellt wird.
Alle weiteren Dienste und Anwendungen wie Mail-, File und Print, werden auf ca.250 Servern mit unterschiedlichen Betriebssystemen wie Windows,Linux und OS400 betrieben.
Der Betrieb der Systeme wird durch 35 Mitarbeiter geregelt.

Kerberos ist ein sicheres Authentifizierungsprotokoll für unsichere TCP/IP-Netzwerke.
In diesem Vortrag wird erläutert, wie die Oracle Datenbank Landschaft mit Microsoft Active Directory (Kerberos Server) angebunden werden kann, um die Vorteile eines zentralisierten Password Managements auszunutzen und um das Single Sign On (Kerberos basierend), welches bereits in weiten Teilen der Pepperl+Fuchs IT implementiert worden ist, weiter auszubauen.

In einer Live-Demo werden die Konfigurierbarkeit und die Funktionsweise der EndUser Tools wie Oracle SQL Developer, MS Excel, MS Access, etc. in Zusammenspiel mit dem Netzwerk Authentifizierungsprotokoll Kerberos vorgeführt.

**Pepperl+Fuchs IT**

Kerberos ist das strategische Netzwerk Authentifizierungsprotokoll bei Pepperl+Fuchs. Viele der IT Anwendungen bei Pepperl+Fuchs wurden bereits mit dem Kerberos Protokoll aktiviert. Mit der Einführung von Kerberos Protokoll in das Unternehmen ergaben sich viele Mehrwerte für das Business. Um einige zu erwähnen:

- Zentralisierte Benutzer-Authentifizierung durch den Kerberos Server hier MS Active Directory 2008 R2 -> zentrales Password Management;
- Single Sign On->Arbeitsfluss wird nicht gestört;
- Höhere Sicherheit durch das starke Authentifizierungsprotokoll Kerberos;

- Weniger Administrationsarbeit;
- Weniger User Helpdesk Anfragen,...etc

Anwendungen bzw. Tools, die momentan Kerberos Protokoll erfoglreich verwenden sind:

- CRM System Siebel
- ERP System M3/Workplace
- Eigene Apache/Tomcat Applikationen

Derzeit spielt die Oracle Datenbank eine wesentliche Rolle in der IT bei Pepperl+Fuchs und für folgende wichtige IT Services genutzt:

- Datawarehousing
- Dokumentensysteme wie N5
- Produktionsunterstützung wie Prüfsysteme und Etikettensoftware
- Eigen geschriebene Systeme wie EDM/Ewaplan
- Weitere Systeme Konsolidierungs und Planungssysteme

Die untersuchte Systemlandschaft besteht aus folgenden Systemen:

- 3 Oracle Datenbank Server Enterprise Edition 11g R2 mit Oracle Advanced Security
- 1 Microsoft Active Directory 2008 R2 als LDAP- und Kerberos Server
- …

Betriebssystem: RedHat Enterprise Linux 5(64 Bit) und MS Windows Server 2008 R2

**Microsoft Active Directory als Kerberos- und LDAP Server**

Der MS Active Directory (MS AD) in der Version 2008 R2 fungiert bei Pepperl+Fuchs als Kerberos- und LDAP Server für viele unternehmensweite Anwendungen. Um die vielen Datenbank Instanzen ebenso in die Kerberos Umgebung einzugliedern, bedarf es zwei wesentliche Schritte. Der erste Schritt ist die Oracle Datenbank dem MS Active Directory bekanntzumachen und der zweite Schritt ist die Datenbank für die Kerberos Authentifizierung vorzubereiten.

Wie erfolgt die Oracle Datenbank Bekanntmachung dem MS Active Directory? Dies passiert in dem man zunächst ein BenutzerAccount in MS AD für den DB Server erstellt. Der DB Server braucht die Keytab Datei und dafür wird zum erstellten BenutzerAccount ein „Service Principal Name“ (SPN) erstellt und gemapped. Genau dieser Service Principal Name für die spätere Client ServiceAnfrage verwendet. Kommt eine Client Anfrage zum Kerberos Service um ein Service Ticket sich ausstellen zu lassen, dann nutzt der Client genau den SPN als eindeutigen registrierten Namen aus MS AD.

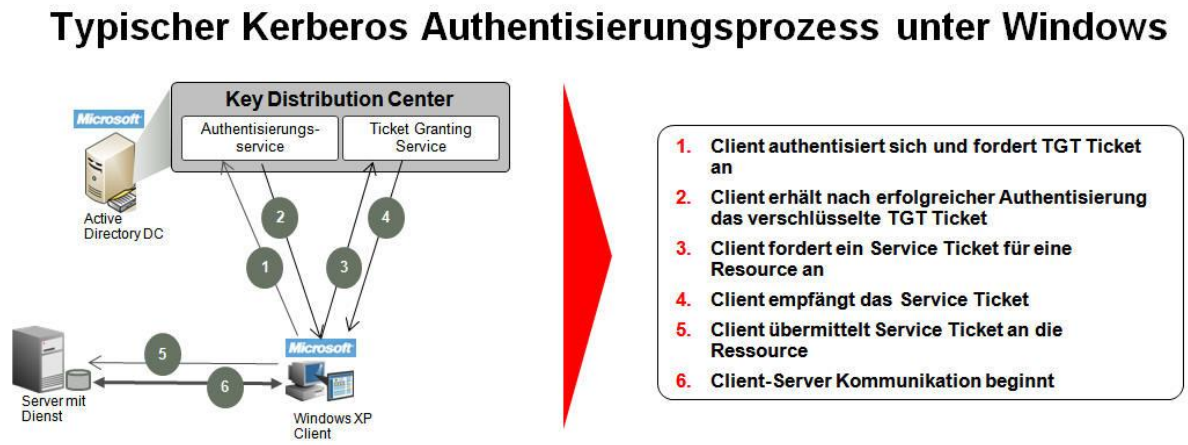


*Abb. 1: Kerberos Authentisierungsprozess*

Keytab Erstellung erfolgt auf dem MS DomainControler (MS Active Directory Server) mit dem Tool „KTPASS“ und wird dann auf sicherem Wege zum Oracle Datenbank Server transferiert.

Da sowohl bei MS Active Directory 2008 R2 als auch bei MS Windows 7 (als Client Workstation) per default DES Verschlüsselung für die Kerberos Authentifizierung deaktiviert ist, sollte dies vor der Keytab Erstellung berücksichtigt werden.

**Der Datenbank Server und Kerberos Protokoll**

Damit der Oracle Datenbank Server ebenso vom Kerberos Protokoll profitieren kann, muss man den DB Server zunächst dazu „befähigen“ Kerberos Protokoll zu verstehen und nutzen zu können. Die „Befähigung“ erfolgt durch den Kerberos Authentication Adapter, welcher als Kompomente zu Oracle Advanced Security gehört. Bei der Oracle Datenbank Enteprise Edition 11g R2 muss der Adapter nicht nachinstalliert werden, sondern ist bereits mitinstalliert und muss lediglich konfiguriert werden. Kerberos Konfiguration auf dem DB Server erfolgt entweder durch Oracle Net Manager

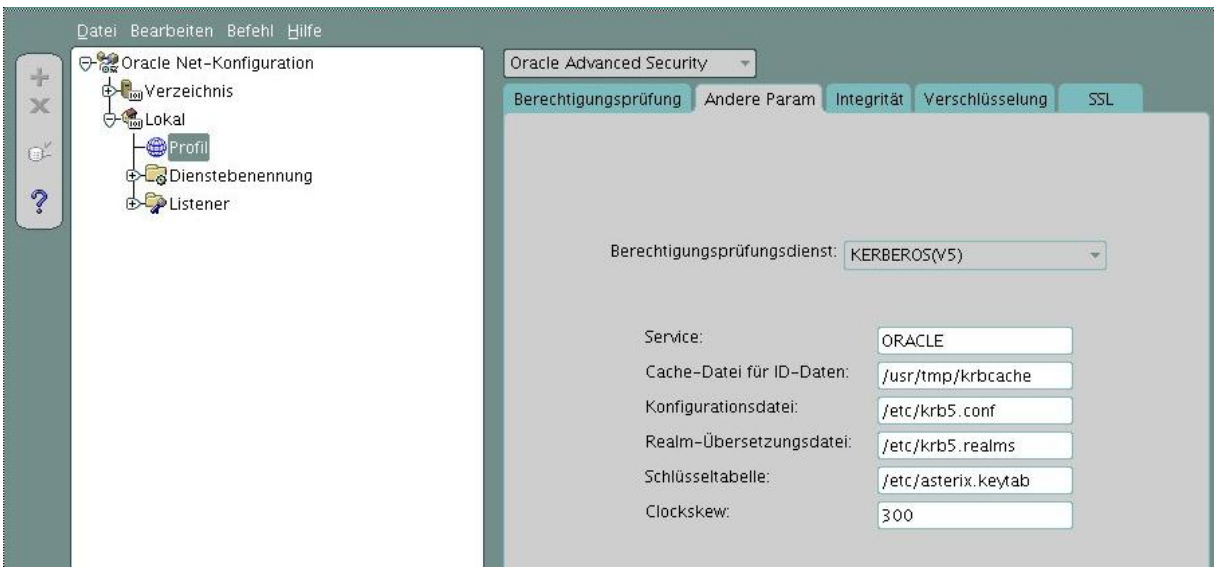


*Abb.2: Kerberos Konfiguration mit Oracle Net Manager*

oder durch Änderungen direkt in der slqnet.ora Datei.

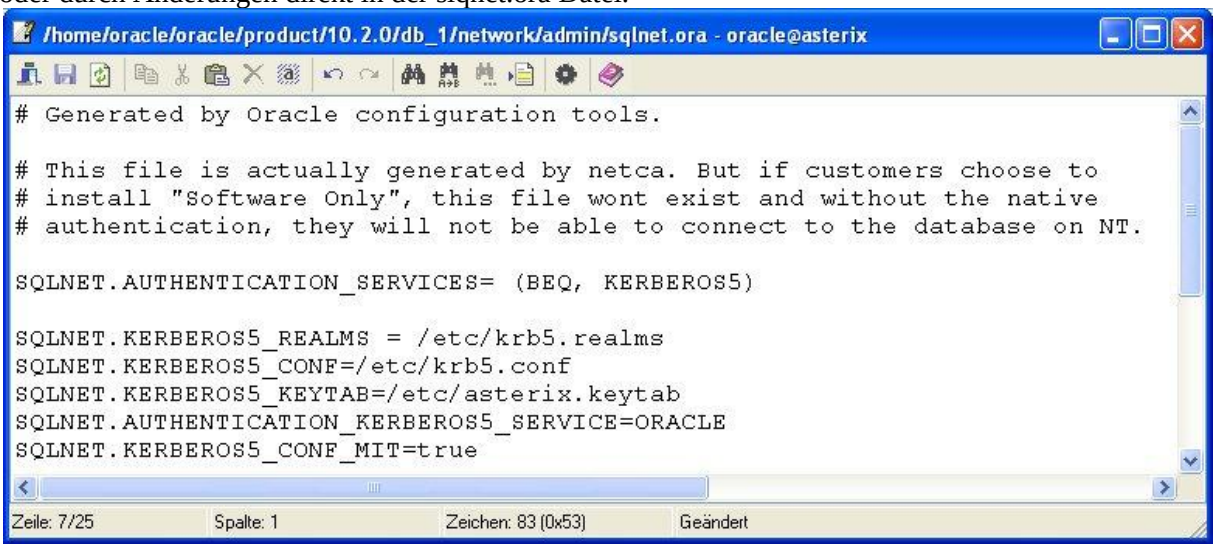


*Abb.3: Kerberos Konfiguration in der sqlnet.ora*

**Kerberos Authentifizierung mit der Datenbank testen**

Um die Kerberos Authentifizierung nun zu testen, braucht man einen Benutzer in der Datenbank der sich der Namenskonvention von MS AD anlehnt und als „identified externally“ angelegt wird. Sinvollerweise wäre es gut gleich auch „create session“ Privilege zu vergeben, um die erfolgreiche Benutzer Anmeldung per Kerberros verfolgen/demonstrieren zu können.

Hier ein Beispiel zur DB User Erstellung:

```
CREATE USER "SAHOVIC@DE.ORACLE.COM" IDENTIFIED EXTERNALLY;
GRANT CREATE SESSION TO "SAHOVIC@DE.ORACLE.COM";
```

Im ersten Schritt bevor der Benutzer sich per Kerberos Protokoll an der Datenbank anmeldet, muss der Benutzer zunächst im Besitz des Kerberos TGT Tickets sein. Dies erfolgt z.B. durch das Tool „okinit“.
Hier ein Beispiel wie man für den Benutzer SAHOVIC@DE.ORACLE.COM den TGT Ticket vom MS Active Directory anfordert.

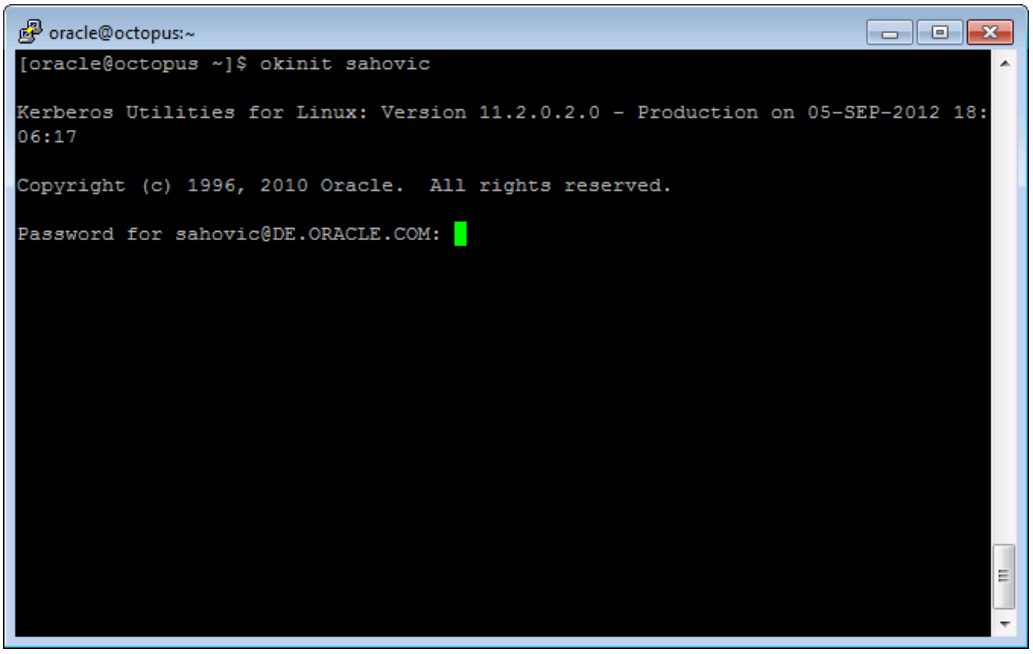


*Abb.4: Kerberos (TGT) Ticket mit okinit von MS Active Directory anfordern*

Mit dem Tool „oklist“ kann man nachprüfen, ob der TGT Ticket erfolgreich in Credential Cache abgelegt worden ist.

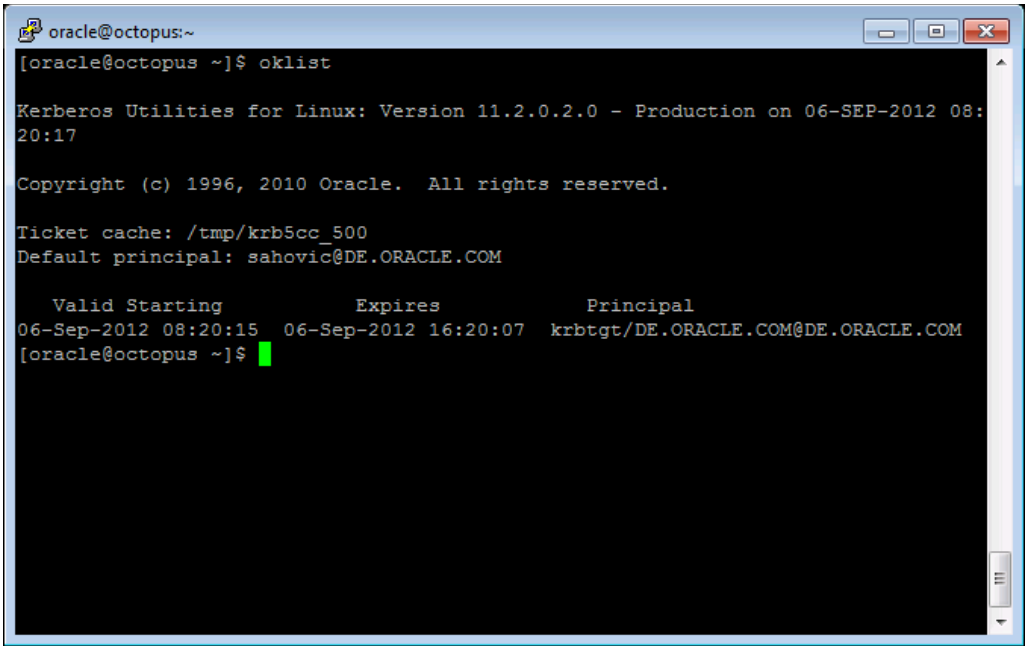


*Abb.5: TGT Ticket erfolgreich in Credential Cache abgelegt*

**Kerberos Authentifizierung mit dem MS Windows 7 gegen die Oracle Datenbank**

Damit MS Windows 7 als Client Workstation sich mit den Datenbank Tools ebenso gegen die Datenbank mit Kerberos authentifiziert, braucht es ein paar Konfigurationsschritte.
Zunächst muss auf der Workstation die Oracle Client Software installiert worden sein. Mit der Oracle Client Installation werden Libraries installiert, die dann später von den DB Tools (sqlplus, TOAD, SQL Developer,...) für die Kerberos Authentifizierung verwendet werden.

Konfigurationen für dieAuthentifizierung werden hierbei im ersten Schritt in sqlnet.ora vorgenommen. Da werden unter anderem auch Informationen hinterlegt, wo liegt die Kerberos Config Datei (krb5.ini) und welches Credential Cache für die Authentifizierung verwendet werden soll.

Anpassungen für die Kerberos Authentifizierung bei den einzelnen DB Tools sind einfach und schnell zu erledigen. Einzelheiten hierzu werden im Vortrag detailiert vorgestellt und live vorgeführt.

**Kontaktadresse:**

**Helmut Eckstein**
Manager Global IT/SIS
Lilienthalstraße 200
68307 Mannheim

Telefon: +49 (0) 621-776-1580
Fax: +49 (0) 621-776-1874
E-Mail: eckstein@de.pepperl-fuchs.com
Internet: www.pepperl-fuchs.com

**Suvad Sahovic**
Senior Systemberater
Oracle Deutschland B.V. & Co. KG
Schiffbauergasse 14
14467 Potsdam

Telefon: +49 (0) 331-2007-181
Fax: +49 (0) 331-2007-561
E-Mail: suvad.sahovic@oracle.com
Internet: http://www.oracle.com