ORDIX AG

Kerberos und das Oracle

Die Nutzung von Kerberos in einer Solaris-Oracle-Umgebung

DOAG Konferenz
19. - 21.11.2013, Nürnberg

Veit Jäger
info@ordix.de
www.ordix.de

Agenda

ORDIX AG

- Einleitung
- Sicherheit & Komfort?
- Kerberos - die Reise beginnt
- Solaris - das Universum
- SSH - der sichere Weg
- NFS - der Packesel
- Das Oracle
- Fazit

Wie kommt man auf so ein Thema?

ORDIX AG

„Sicherheit wird groß geschrieben.“

„ Ich kann so nicht arbeiten!“

Sicherheit & Komfort?

Ein Widerspruch, oder?

ORDIX AG

- Sicherheit ..
  - … bedeutet Aufwand
  - … ist kompliziert
  - … behindert die Arbeit
- Komfort ..
  - … fällt nicht auf
  - … ist einfach
  - … erleichtert die Arbeit

Die Lösung: SSO

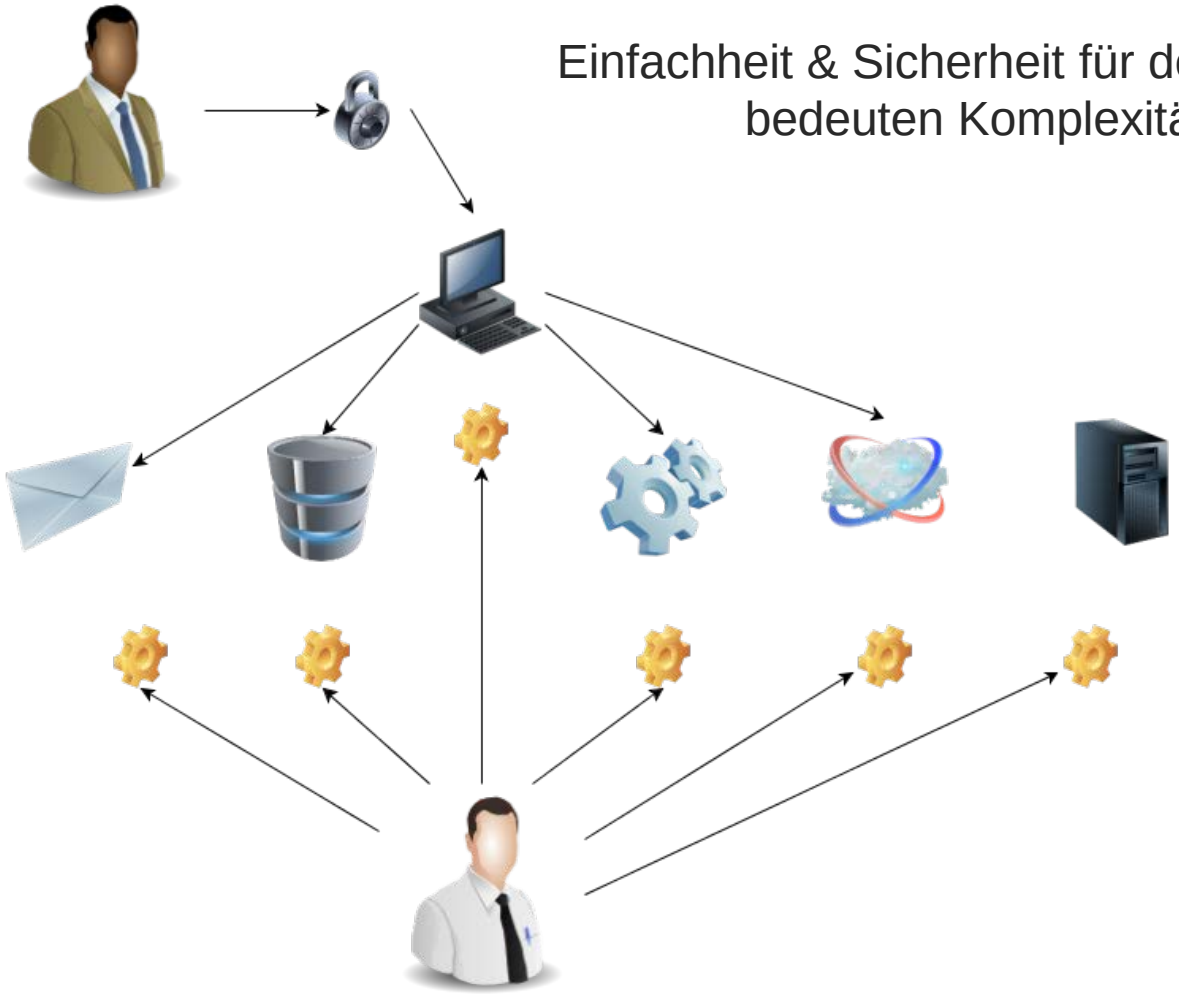
ORDIX AG

Single Sign On (SSO)

- Einmalige Anmeldung, wenig Aufwand
- Hohe Sicherheit
- Einfache Bedienung, grenzenloses Arbeiten möglich

Man kann nicht alles haben

ORDIX AG



Einfachheit & Sicherheit für den Anwender
bedeuten Komplexität für den Admin.

Kerberos - die Reise beginnt

Die Sprache lernen

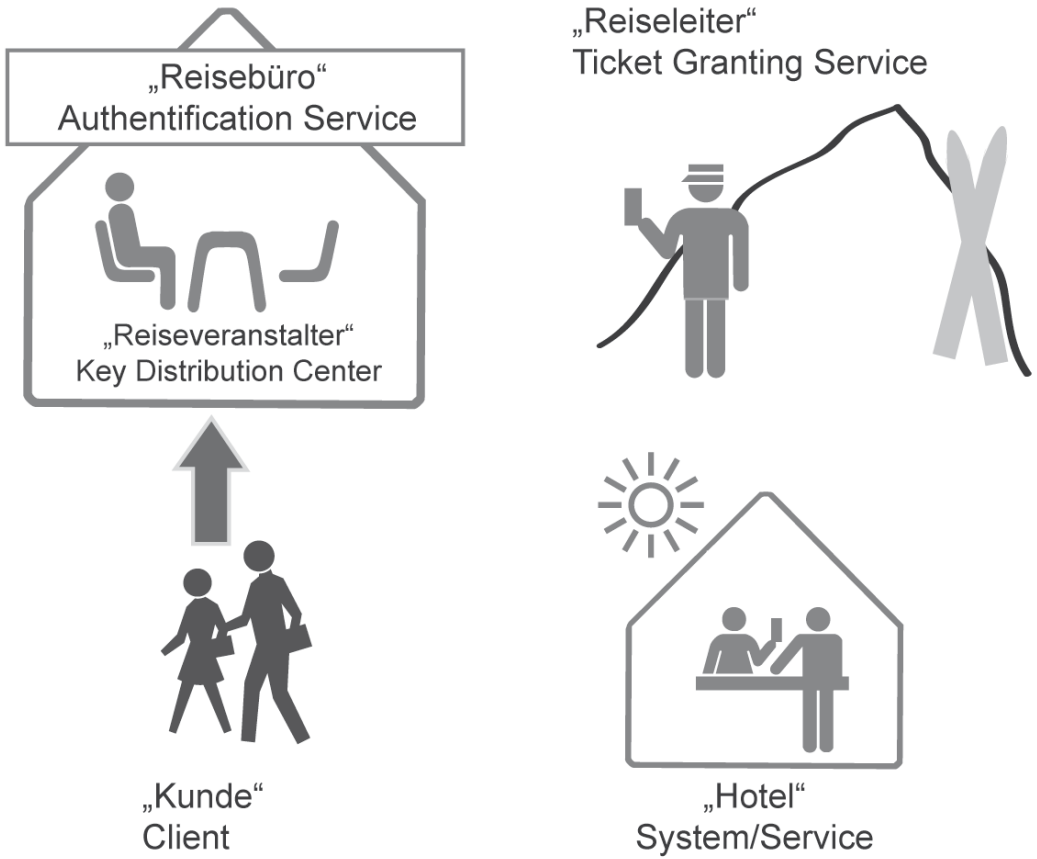
ORDIX AG

- Key Distribution Center KDC → Der Reiseveranstalter
- Authentication Service AS → Das Reisebüro
- Ticket Granting Service TGS → Reiseleiter Hr. TGS
- Ticket Granting Ticket TGT → Der Voucher
- Client → Kunde bzw. Anwender
- System/Service → Hotel, Museum oder das Oracle
- REALM → das (Solaris-) Universum

Die Beteiligten

ORDIX AG

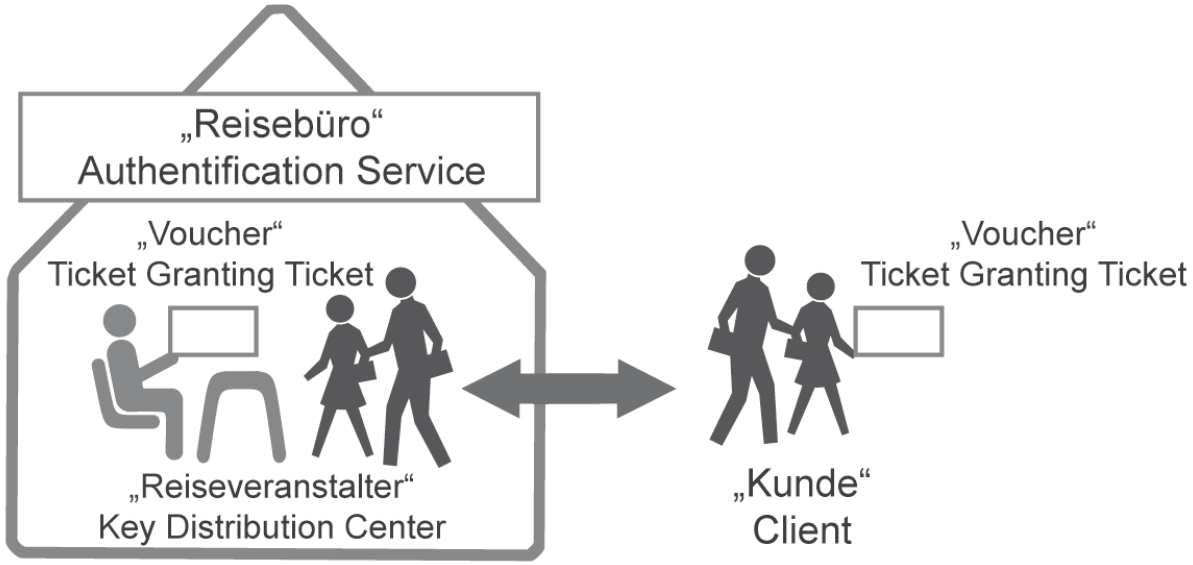
Die einzelnen Komponenten einer Kerberos-Umgebung:



Reise buchen & Voucher erhalten

ORDIX AG

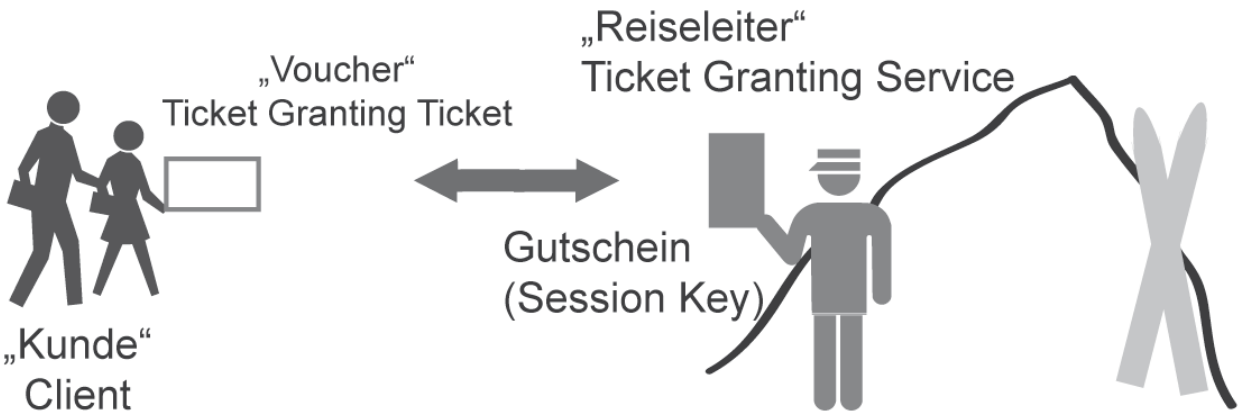
Als Analogie für eine Anmeldung in der Single-Sign-On-Umgebung:



Treffen mit dem Reiseleiter

ORDIX AG

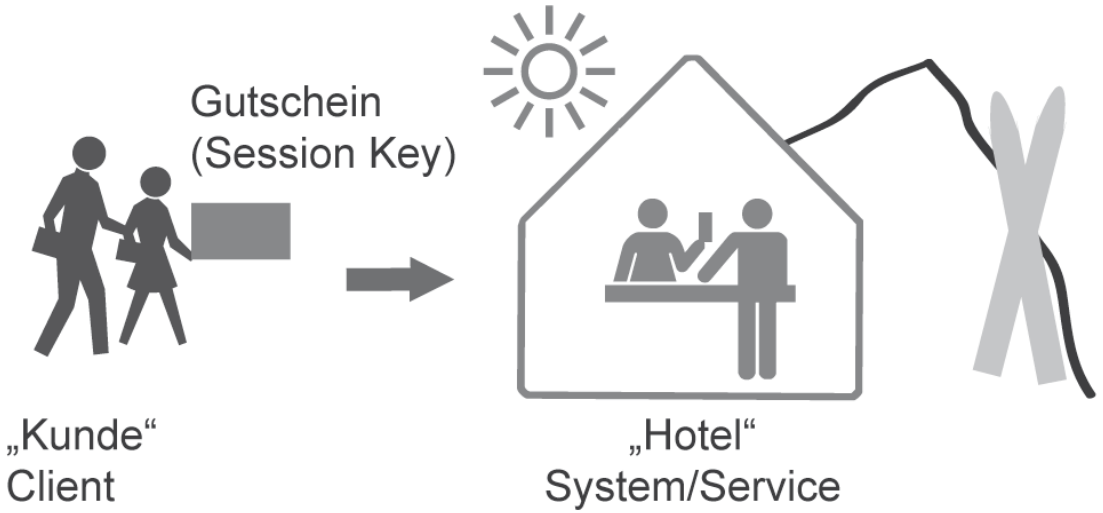
Im Hintergrund werden die erhaltenen Objekte verwaltet:



Urlaub genießen

ORDIX AG

Die Verwendung von Diensten:



Solaris - das Universum

Das Universum ist auf uns vorbereitet

ORDIX AG

Die notwendigen Pakete sind installiert:

```
# pkginfo | grep -i kerb
system      SUNWkdcr                      Kerberos V5 KDC (root)
system      SUNWkdcu                      Kerberos V5 Master KDC (user)
system      SUNWkrbr                      Kerberos version 5 support (Root)
system      SUNWkrbu                      Kerberos version 5 support (Usr)
```

Der Service für einen Kerberos Server ist vorbereitet:

```
# svcs -a | grep -i krb
disabled       17:16:48 svc:/network/security/krb5kdc:default
```

Und die Konfigurationen liegen bereit:

```
# ls /etc/krb5/k*.conf
/etc/krb5/kdc.conf
/etc/krb5/krb5.conf
```

Das Universum ist auf uns vorbereitet

ORDIX AG

Im ersten Schritt muss in der Konfiguration das REALM angegeben werden:

```
# grep ORDIX /etc/krb5/*
/etc/krb5/kadm5.acl:          */admin@ORDIX *
/etc/krb5/krb5.conf:          default_realm = ORDIX
/etc/krb5/krb5.conf:          ORDIX = {
```

SSH - der sichere Weg

SSH… warum denn damit?

ORDIX AG

- Secure Shell, der Name ist Programm
  - Sicherer als Alternativen (telnet, rsh, …)
  - Verschlüsselt die Verbindung
  - Authentifiziert die Benutzer

- In der Konfiguration muss Kerberos aktiviert werden

```
# grep -i kbd /etc/ssh/sshd_config
PAMAuthenticationViaKBDInt yes
```

NFS - der Packesel

NFSv4 - Noch nie gehört…

ORDIX AG

- Networkfilesystem
- Seit 2003 verabschiedet (RFS 3530)
- TCP-IP-basiert
- Verschlüsselung mit Hilfe von Kerberos
  - Anwender-Authentifizierung
  - Verschiedene Stufen der Datensicherheit:
    - Integrität
    - Integrität & Paketverschlüsselung

NFSv4 Domain vs. Kerberos REALM

ORDIX AG

Eine Domäne ist ein Herrschaftsbereich.

- Die NFSv4 Domain umfasst:
  - Anwender, es hilft ein eMail-ähnliches Konstrukt
  - Systeme, für die Zuordnung und Gültigkeit der Autorisierung
- Der Kerberos REALM
  - Ein Kerberos Server ist für alle Objekte in seinem REALM zuständig.
  - REALMs können verbunden werden
  - Gültigkeitsbereich für die Authentifizierung

Das Oracle

Das Oracle muss sich vorbereiten

ORDIX AG

- Oracle Advanced Security Paket installieren
  - Stellt das Modul „starke Authentifikation“ (u.a. Kerberos)
  - Gibt es für alle Enterprise-Editionen
  - Muss extra lizensiert werden

- Die Konfiguration für Oracle Advanced Security liegt in der **`sqlnet.ora`**
  - Einstellungen für die Kerberos-Umgebung:

```
SQLNET.AUTHENTICATION_SERVICES= (BEQ, KERBEROS5, TCPS)
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER= (SHA1, MD5)
SQLNET.KERBEROS5_CONF = /etc/krb5.conf
SQLNET.KERBEROS5_REALMS = /etc/krb5.realms
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
[…]
```

Oracle verbinden

ORDIX AG

- Anwender in der Datenbank anlegen und extern authentifizieren:

```
SQL > CREATE USER user IDENTIFIED EXTERNALLY AS `user@ordix.de`;
SQL > GRANT CREATE SESSION TO user;
```

- Anmeldung an der TNS-Instanz, ohne Kennwort:

```
# sqlplus /@instanz
```

Fazit

Dies ist ein persönliches Fazit!

ORDIX AG

- Die Arbeit der Anwender wird vereinfacht und erleichtert.
- Die allgemeine IT-Sicherheit steigt.
- Kerberos-Umgebungen benötigen ein durchdachtes Konzept.
- SSO ist nicht einfach in bestehende Umgebungen zu integrieren.

ORDIX AG

Zentrale Paderborn
Westernmauer 12 - 16
33098 Paderborn
Tel.: 05251 1063-0

Seminarzentrum Wiesbaden
Kreuzberger Ring 13
65205 Wiesbaden
Tel.: 0611 77840-00

Zentrales Fax:
0180 1 67349 0
0180 1 ORDIX 0

Weitere Geschäftsstellen
in Köln, Münster und Neu-Ulm

E-Mail: info@ordix.de
Internet: http://www.ordix.de

Vielen Dank für Ihre Aufmerksamkeit!