Kerberos - Single Sign On ganz einfach

Jürgen Kühn
Trivadis GmbH
Düsseldorf

Schlüsselworte:

Kerberos, Advanced Security Option, Key Distribution Center, Ticket Granting Ticket, Service Ticket, Realm, External Authentication, Keytab File

Einleitung

Kerberos ist ein seit vielen Jahren verfügbares und in vielen Bereichen eingesetztes Authentierungsprotokoll. Seit Jahren ist Kerberos das Standardprotokoll bei der Benutzeranmeldung an Windows Clients innerhalb einer Microsoft Active Directory Domäne. Auch Oracle unterstützt die Anmeldung mittels Kerberos sowohl an der Datenbank als auch in vielen Komponenten der Fusion Middleware.

Allerdings umgibt die Konfiguration von Kerberos für Oracle Datenbanken gerade im Zusammenspiel mit Active Directory immer noch der Mythos des "zu Komplizierten". Viele Installationen werden zwar erfolgreich abgeschlossen, jedoch bleibt vereinzelt der Eindruck zurück, dass vieles nach dem Trial and Error Verfahren realisiert wurde und letztendlich niemand im Unternehmen genau weiß, warum Kerberos eigentlich funktioniert.

Der Vortrag stellt die Funktionsweise von Kerberos im Allgemeinen und insbesondere die Nutzung von Kerberos für die Anmeldung an Oracle Datenbanken im Zusammenspiel mit Microsoft Active Directory dar. Neben der Konfiguration werden auch mögliche Fallstricke und Unzulänglichkeiten beim Einsatz von Kerberos für Oracle Datenbanken angesprochen.

Kerberos

Kerberos - Single Sign On ganz einfach?

Kerberos ist in der Tat ein Authentisierungsprotokoll, das von sehr vielen Clients, Servern und Applikationen unterstützt wird. In der Windows Welt ist Kerberos seit Windows 2000 das Standardprotokoll für die Anmeldung an Domänencontroller.

Die Integration von Kerberos zwischen "systemfremden" Welten wie Windows und Unix bzw. Linux ist aber nicht immer einfach. Gerade die Kerberos Anmeldung von einem in eine Windows Domäne integrierten Windows Client aus an eine Oracle Datenbank auf einem Unix oder Linux Server ist aber eine interessante Einsatzmöglichkeit für Kerberos.

Der Name "Kerberos" für das Protokoll stammt angeblich vom dreiköpfigen Höllenhund aus Homers "Odyssee". Wenn man bedenkt, dass in einem Kerberos System drei Komponenten beteiligt sind, mag man dem zustimmen. Die drei Komponenten sind

- der Kerberos Client
- der Kerberos Service Provider
- das Key Distribution Center

Diese drei abstrakten Bezeichnungen lassen sich einfach auflösen in geläufigere Namen. Der Kerberos Client ist in diesem Fall nichts anderes als ein Windows Client, der Kerberos Service Provider ist der Oracle Datenbankserver, und das Key Distribution Center ist der Active Directory Domain Controller.

Bevor eine Kerberos Authentisierung stattfinden kann, müssen der Domänencontroller und der Datenbankserver einen nur diesen beiden bekannten geheimen Schlüssel austauschen. Dieser Schritt wird nur ein einziges mal ausgeführt bei der initialen Konfiguration von Kerberos zwischen diesen beiden Maschinen. Lediglich bei einem eventuellen Schlüsselwechsel muss der Schlüssel erneut ausgetauscht werden.

Wichtig ist, dass bei der Authentisierung eines Benutzers der Datenbankserver und der Domänencontroller keine Daten austauschen. Oft wir fälschlicherweise angenommen, dass der Datenbankserver bei der Authentisierung Kontakt zum Domänencontroller aufnimmt. Dies ist aber genau nicht der Sinn des Kerberos Ticketsystems, das hier kurz beschrieben wird.

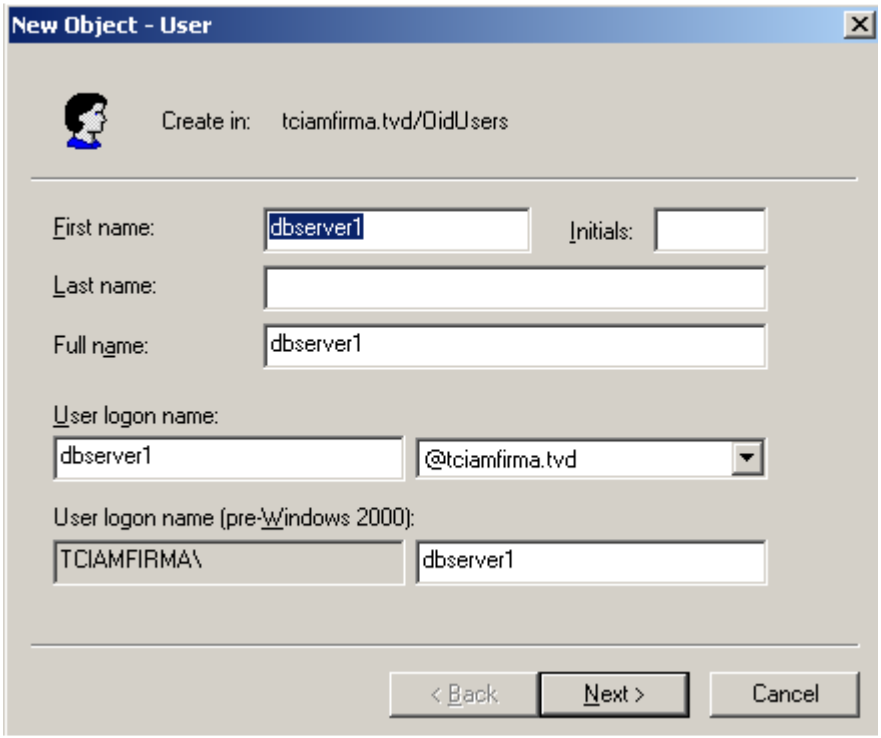
1. Der erste Schritt ist die Authentisierung des Benutzers am Domänencontroller. Nach der Eingabe von Benutzernamen und Passwort fordert der Client beim Domänencontroller ein so genanntes Ticket Granting Ticket (TGT) an. Der Domänencontroller prüft die Benutzer- und Anmeldedaten gegen seine interne Datenbank und stellt bei Erfolg ein TGT aus. Das TGT ist ein Authentisierungsnachweis für den Benutzer und bestätigt dessen erfolgreiche Anmeldung. Das TGT wird lokal auf dem Client zwischengespeichert und ist für einen bestimmten Zeitraum gültig.

2. Wenn der Benutzer einen Kerberos fähigen Dienst wie z.B. den Zugriff auf eine Oracle Datenbank nutzen möchte, fordert der Client beim Domänencontroller ein so genanntes Serviceticket (ST) für den Dienst an. Anstatt sich erneut mit seinem Passwort am Domänencontroller anzumelden, schickt der Client das gültige TGT als "Ausweis" an den Domänencontroller. Dieser überprüft die Gültigkeit des TGT und stellt dem Benutzer ein ST für den angeforderten Dienst aus. Das ST enthält dabei Daten, die nur der Datenbankserver, nicht jedoch der Client entschlüsseln und verifizieren kann.

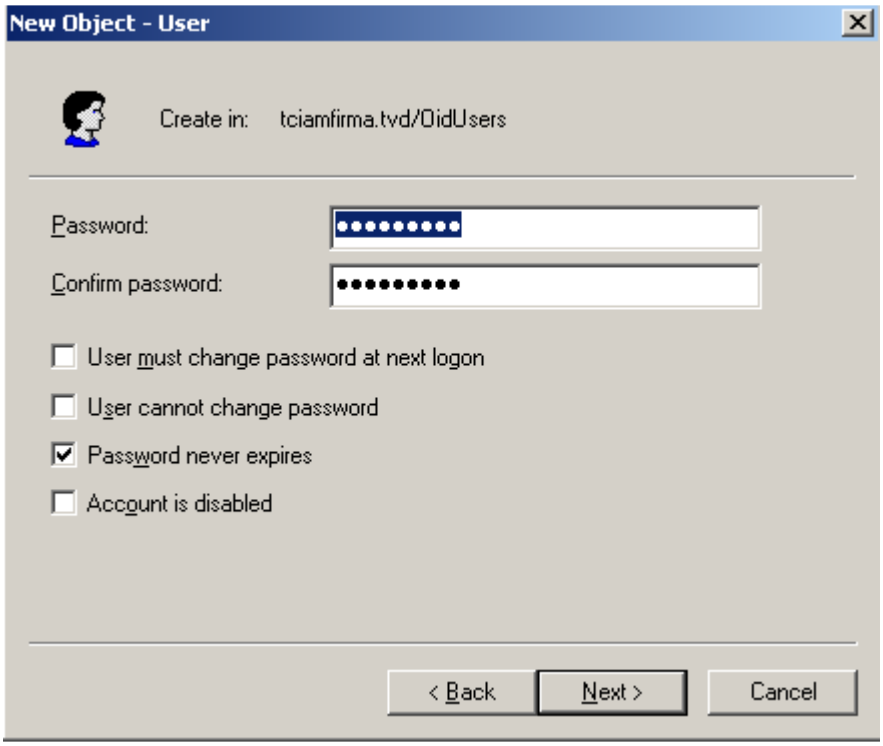
3. Der Client sendet das erhaltene ST an den Datenbankserver. Dieser überprüft das ST mit Hilfe des irgendwann einmal zwischen Domänencontroller und Datenbankserver ausgetauschten geheimen Schlüssels. Nach erfolgreicher Prüfung ist der Benutzer an der Datenbank angemeldet.

Anlegen eines Active Directory Kontos für den Datenbankserver

Zunächst muss für den Datenbankserver ein Benutzerkonto (kein Computerkonto) in einem beliebigen Zweig des Active Directory angelegt werden. In dem Beispiel wird der Benutzer mit dem Namen "dbserver1" angelegt:



Das Benutzerkonto kann mit minimalsten Rechten ausgestattet werden, weshalb es vertretbar ist, das Passwort nie ablaufen zu lassen:



Service Principal Name und keytab File

Der Client gibt bei der Anforderung eines Service Tickets den Service Principal Name (SPN) an. Anhand des SPN ermittelt der Domänencontroller das zugehörige Active Directory Konto, dessen geheimer Schlüssel für die Verschlüsselung des Service Tickets verwendet muss. Wie bereits beschrieben muss dieser Schlüssel dazu einmalig an den Datenbankserver übertragen werden. Dies geschieht über ein keytab File, dass mittels des Microsoft Tools "ktpass.exe" erstellt wird.

Der unten aufgeführte "ktpass" Befehl

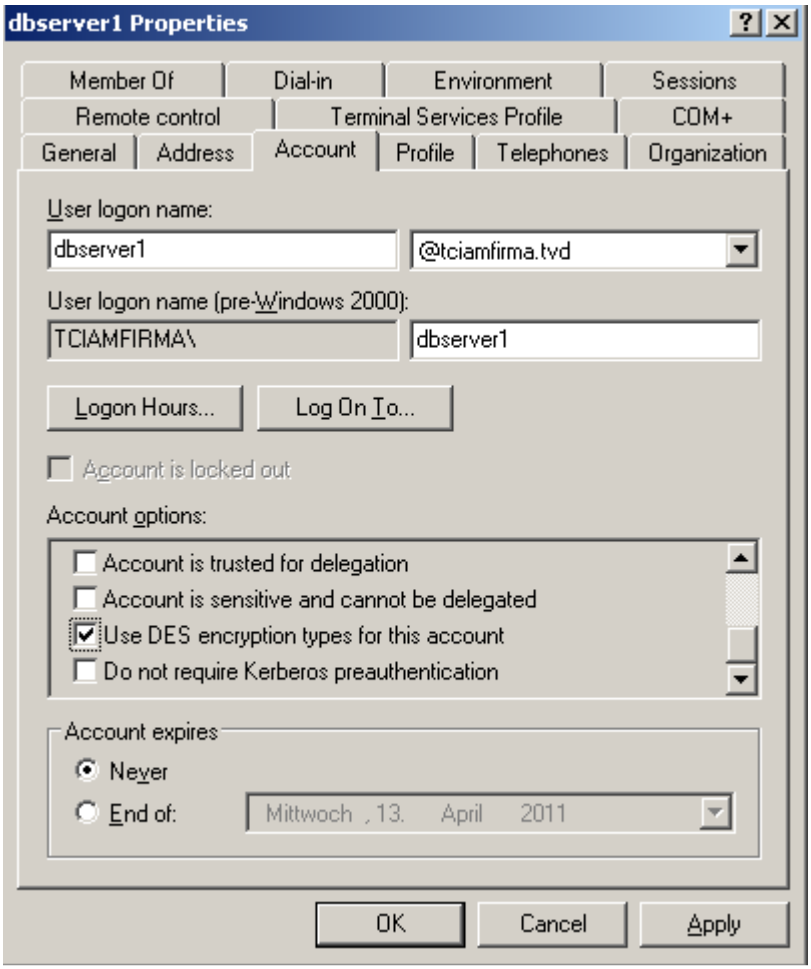
- setzt das Passwort für den AD User "dbserver1" auf den unter "-pass" angegebenen Wert.
- wählt mit "+desonly" DES als einzigen erlaubten kryptografischen Algorithmus aus (wird für Kerberos Kompatibilität mit Linux benötigt).
- setzt den Service Principal Name auf "oracle/dbserver1.tvd"
- erstellt das keytab File "dbserver1.keytab" für dbserver1

```
C:\Program Files\Support Tools>ktpass.exe -princ
oracle/dbserver1.tvd@TCIAMFIRMA.TVD -mapuser dbserver1 -pass oracle +desonly -
crypto des-cbc-md5 -out c:\dbserver1.keytab
Targeting domain controller: pdc.tciamfirma.tvd
Successfully mapped oracle/dbserver1.tvd to dbserver1.
```

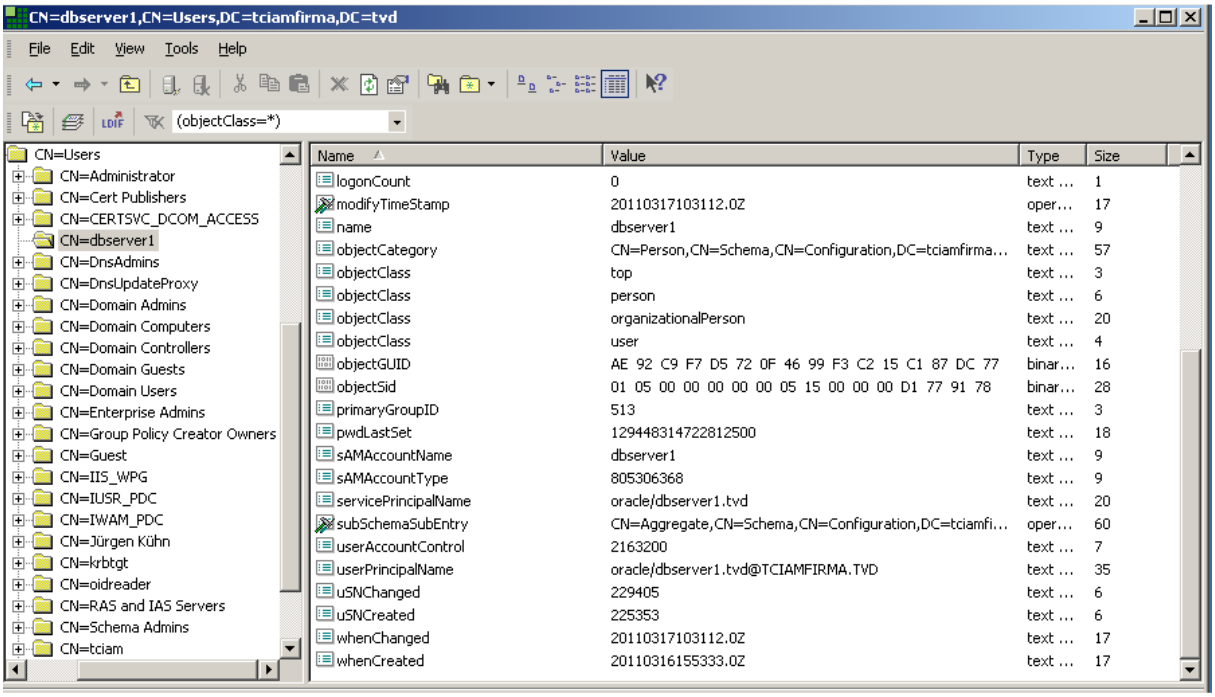
```
Password succesfully set!
WARNING: pType and account type do not match. This might cause  problems.
Key created.
Output keytab to c:\dbserver1.keytab:
Keytab version: 0x502
keysize 62 oracle/dbserver1.tvd@TCIAMFIRMA.TVD ptype 0 (KRB5_NT_UNKNOWN) vno 5
etype 0x3 (DES-CBC-MD5) keylength 8 (0x2054fd0145a754a1)
Account dbserver1 has been set for DES-only encryption.

C:\Program Files\Support Tools>
```

Die Auswahl von DES kann man in den Eigenschaften des Benutzerkontos sehen:



In einem LDAP Browser kann man auch den Service Principal Name erkennen:



Auch das Microsoft Tool "setspn" listet Service Principal Names auf:

```
C:\Program Files\Support Tools>setspn -L dbserver1
Registered ServicePrincipalNames for CN=dbserver1,DC=tciamfirma,DC=tvd:
    oracle/dbserver1.tvd

C:\Program Files\Support Tools>
```

Das erstellte keytab File "dbserver1.keytab" wird in ein frei wählbares Verzeichnis auf dem Datenbankserver kopiert, z.B. das TNS_ADMIN Verzeichnis.

Kerberos Konfiguration des Datenbankservers

Die Kerberos Konfiguration auf dem Datenbankserver umfasst die Erstellung der Kerberos Konfigurationsdatei "krb5.conf" und die Anpassung von "sqlnet.ora".

In "krb5.conf" werden im Wesentlichen die Zuordnung einer Kerberos Realm zu Windows Domänen sowie ein oder mehrere Key Distribution Center (KDC) eingetragen. Der KDC ist in diesem Falle der Domänencontroller.

```
####krb5.conf DB Server
[libdefaults]
default_realm = TCIAMFIRMA.TVD
clockskew=300

[realms]
TCIAMFIRMA.TVD = {
        kdc = pdc.tvd
}

[domain_realm]
.tvd = TCIAMFIRMA.TVD
tvd = TCIAMFIRMA.TVD                                # nicht sinnvoll
specialhost.tvd = OTHER.REALM
```

In der Datei "sqlnet.ora" wird die Kerberos Authentisierung für Oracle konfiguriert. Die unten stehenden Einträge stellen die Kerberos relevanten Einstellungen dar:

```
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=oracle
SQLNET.KERBEROS5_CONF=/u01/app/oracle/product/10.2.0/db_1/network/admin/krb5.conf
SQLNET.KERBEROS5_CONF_MIT=TRUE
SQLNET.AUTHENTICATION_SERVICES=(BEQ,KERBEROS5)
SQLNET.KERBEROS5_KEYTAB=/u01/app/oracle/product/10.2.0/db_1/network/admin/dbserver
1.keytab
#Wenn ein Ticket auf dem Unix Host benötigt wird
SQLNET.KERBEROS5_CC_NAME=/u01/app/oracle/product/10.2.0/db_1/network/admin/krb.tg
```

- SQLNET.AUTHENTICATION_KERBEROS5_SERVICE gibt den Service Namen an, der im Service Principal Name verwendet wird.
- SQLNET.KERBEROS5_CONF bezeichnet den Pfad zur Datei krb5.conf
- SQLNET.KERBEROS5_CONF_MIT legt fest, ob die MIT Kerberos Variante genutzt wird
- SQLNET.AUTHENTICATION_SERVICES enthält den zusätzlichen Eintrag KERBEROS5
- SQLNET.KERBEROS5_KEYTAB bezeichnet den Pfad zum keytab File
- SQLNET.KERBEROS5_CC_NAME bezeichnet den Pfad zu einer Datei,i in der eine eventuell auf dem Datenbankserver selbst angefordertes TGT gespeichert wird

Zuletzt wird in der Datenbank ein Kerberos Benutzer mit seinem Windows Benutzernamen als Externally Authenticated User angelegt.

```
SQL> create user "JUK@TCIAMFIRMA.TVD" identified externally;
User created.

SQL> grant connect, resource to "JUK@TCIAMFIRMA.TVD";
Grant succeeded.
```

Kerberos Konfiguration des Clients

Auch auf dem Client muss eine Kerberos Konfigurationsdatei vorliegen. Sie beinhaltet die gleichen Einträge wie die "krb5.conf" Datei auf dem Server.

Die "sqlnet.ora" auf dem Kerberos Client muss ebenfalls angepasst werden. Die Kerberos relevanten Einträge entsprechen denen des Servers. Lediglich der `SQLNET.AUTHENTICATION_KERBEROS5_SERVICE` Eintrag ist nicht erforderlich, weil der zu verwendende Servicename dem Client von Datenbankserver übermittelt wird.

```
####sqlnet.ora
SQLNET.KERBEROS5_CONF=C:\u01\app\oracle\product\10.2.0\client\network\admin\krb5.c
onf
SQLNET.KERBEROS5_CONF_MIT=TRUE
#SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=oracle #nur bei unix clients nötig
SQLNET.AUTHENTICATION_SERVICES=(BEQ, KERBEROS5)
SQLNET.KERBEROS5_CC_NAME = OSMSFT://
```

Anmeldung an der Datenbank

Auf einem Windows Client kann sich ein Benutzer direkt mit SQL*Plus an die Datenbank anmelden. Das zur Anforderung eines Service Tickets für Oracle erforderliche TGT liegt bereits seit der Anmeldung an der Domäne vor. Ein Aufruf von "okinit" ist daher nicht erforderlich.

```
C:\Program Files\Support Tools>sqlplus /@db10a

SQL*Plus: Release 10.2.0.1.0 - Production on Mi Okt 19 21:38:22 2011

Copyright (c) 1982, 2005, Oracle.  All rights reserved.


Verbunden mit:
Oracle Database 10g Enterprise Edition Release 10.2.0.4.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> show user
USER ist "JUK@TCIAMFIRMA.TVD"
SQL>
```

Nach der Anmeldung können die Tickets mit dem Oracle Tool "oklist" oder dem Microsoft Tool "klist.exe" angezeigt werden.

```
C:\Program Files\Support Tools>klist tickets

Cached Tickets: (2)

   Server: krbtgt/TCIAMFIRMA.TVD@TCIAMFIRMA.TVD
      KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
      End Time: 10/20/2011 7:38:02
      Renew Time: 10/26/2011 21:38:02
```

```
   Server: oracle/dbserver1.tvd@TCIAMFIRMA.TVD
      KerbTicket Encryption Type: Kerberos DES-CBC-MD5
      End Time: 10/20/2011 7:38:02
      Renew Time: 10/26/2011 21:38:02
```

```
C:\Program Files\Support Tools>oklist

Kerberos Utilities for 32-bit Windows: Version 10.2.0.1.0 - Production on 19-OKT
-2011 21:41:37

Copyright (c) 1996, 2004 Oracle.  All rights reserved.

Ticket cache: win2kcc
Default principal: juk@TCIAMFIRMA.TVD

   Valid Starting           Expires            Principal
19-Okt-2011 21:38:02  20-Okt-2011 07:38:02  krbtgt/TCIAMFIRMA.TVD@TCIAMFIRMA.TVD
        renew until 26-Okt-2011 21:38:02
19-Okt-2011 21:38:22  20-Okt-2011 07:38:02  oracle/dbserver1.tvd@TCIAMFIRMA.TVD
renew until 26-Okt-2011 21:38:02
19-Okt-2011 21:38:02  20-Okt-2011 07:38:02  host/pdc.tciamfirma.tvd@TCIAMFIRMA.T
VD      renew until 26-Okt-2011 21:38:02

C:\Program Files\Support Tools>
```

Fazit

Kerberos ist ein geeignetes Protokoll, dem Ziel eines Single Sign On näher zu kommen. Allein die Umstellung der Oracle Datenbankauthentisierung auf Kerberos ist eine deutliche Vereinfachung der Anmeldeprozesse. Darüber hinaus sind viele andere Applikationen Kerberos fähig, so dass einem weit verbreiteten Einsatz von Kerberos in Unternehmen nichts im Wege stehen sollte.

Kontaktadresse:

Jürgen Kühn
Trivadis GmbH
Werdener Str. 4-6
D-40227 Düsseldorf

Telefon: +49(0)211-58666470
Fax: +49(0)211-58666471
E-Mail Juergen.Kuehn@Trivadis.com
Internet: www.trivadis.com