embarcadero

InterBase XE7 OTW – Over the Wire Verschlüsselung

Theorie und Praxis

Über den Präsentator

- Matthias Eißing
- Senior Sales Consultant
  Embarcadero Germany GmbH
- InterBase seit InterBase 3.3/SCO
- Kontakt:
  - eMail: matthias.eissing@embarcadero.com
  - Skype: matthias.eissing
  - Twitter: @matthiaseissing
  - Blog: http://bit.ly/1xNxwNe
    http://community.embarcadero.com/index.php/blogs/blogger/listall/matthiaseissing

WARUM OTW VERSCHLÜSSELUNG?

Warum OTW Verschlüsselung?

- Alle Informationen, die zum InterBase Server geschickt werden, wie auch die Antworten des Servers sind unverschlüsselt.
- Dies ermöglicht eine leichtes Abgreifen der Daten

Die Verschlüsselung ersetzt nicht die Authentifizierung auf Basis von Benutzername/ Kennwort. Sie ergänzt diese

OTW: Die Grundlagen

- Die InterBase OTW Verschlüsselung basiert auf den SSL v3 und TLS v1 Protokollen
- SSL benutzt X.509 Zertifikate für die PKI (Public Key Infrastructure)
- Sowohl Server, als auch Client müssen die X.509 Zertifikate installiert haben

OTW: Zertifikate

- Alle Zertifikate müssen im PEM Format vorliegen
  - PEM = Privacy Enhanced Mail
- SERVER
  - IBSSL_SERVER_CERTFILE
    - CA signiertes Zertifikat mit privatem Schlüssel
  - IBSSL_SERVER_CAFILE
    - Zertifikat mit öffentlichem Schlüssel
- CLIENT
  - serverPublicFile
    - Zertifikat mit öffentlichem Schlüssel

Achtung:
privater Schlüssel!

Einrichten von OTW

- Sowohl Server, als auch Client müssen konfiguriert werden
- Generieren der Zertifikate
  - Benötigte Zertifikate
    - Public Key Zertifikat für den Server
    - Private Key + Server Zertifikat
  - Die Zertifikate können auch selbst mit OpenSSL erstellt werden
    - http://www.openssl.org/docs/apps/openssl.html

Einrichten des Clients

- Die Verschlüsselung wird über den Connection String innerhalb von InterBase angestoßen
- Die Parameter stehen vor dem Datenbankpfad
  - **ssl=true**
  - **serverPublicFile | serverPublicPath** |[clientCertFile]
  - [clientPassPhrase | clientPassPhraseFile]
- Beispiel:
  - `SQL> connect 'localhost/3065?ssl=true?serverPublicFile=C:\Certs2\ibserverCAfile.pem??:c:\db\employee.gdb'`

Einrichten des Servers

- Parameter in der IBSS_CONFIG Datei
  - C:\ProgramData\Embarcadero\InterBase\gds_db\secure\server
- Beispiel:

```
#IBSSL_SERVER_HOST_NAME=W2K8INTERBASE
IBSSL_SERVER_PORT_NO=3065
IBSSL_SERVER_CERTFILE=”C:\Certs2\ibserverCAfileServer.pem”
IBSSL_SERVER_PASSPHRASE=geheim123
```

Mehr Infos....

Embarcadero® InterBase XE7™

Operations Guide

Published November, 2014

DEMO

OpenSSL Zertifikate erstellen

```
openssl genrsa -aes256 -out c:\Certs2\key.pem 2048
```

- Generiert einen privaten Schlüssel
- Dieser wird mit einer Passphrase verschlüsselt
- Diese Passphrase wird vom InterBase Server benötigt

Achtung:
Zielverzeichnis muss existieren!

```
C:\OpenSSL-Win32\bin>openssl genrsa -aes256 -out c:\Certs2\key.pem 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.........+++
...................+++
e is 65537 (0x10001)
Enter pass phrase for c:\Certs2\key.pem:
Verifying - Enter pass phrase for c:\Certs2\key.pem:
```

OpenSSL Zertifikate erstellen

```
openssl req -new -key c:\Certs2\key.pem
  -out c:\Certs2\csr.pem
```

- Erzeugt einen Zertifizierungs Request

```
C:\OpenSSL-Win32\bin>openssl req -new -key c:\Certs2\key.pem -out c:\Certs2\csr.
pem
Enter pass phrase for c:\Certs2\key.pem:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Hessen
Locality Name (eg, city) []:Frankfurt
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Embarcadero
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Self-Signed Certificate
Email Address []:somebody@somewhere.invalid

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:geheim
An optional company name []:

C:\OpenSSL-Win32\bin>_
```

OpenSSL Zertifikate erstellen

```
openssl req -x509 -days 365 -key C:\Certs2\key.pem
  -in C:\Certs2\csr.pem
  -out C:\Certs2\ibserverCAfile.pem
```

- Signiert die Zertifizierungs Request mit dem eigenen, privaten Schlüssel

- Das erzeugte Zertifikat reicht für den Client.
- Für den Server kopiert man KEY.PEM und ibserverCAfile.pem zusammen (in eine Datei)

```
copy /b ibserverCAfile.pem+key.pem
ibserverCAfileServer.pem
```