Le groupe d'utilisateurs Progress du Québec

OpenEdge Chiffrage avec SSL

Paul Koufalis
Président
Progresswiz Consulting

Progresswiz

Progresswiz Informatique

- **Offre de l'expertise technique Progress, UNIX, Windows et plus depuis 1999**
- **Spécialisé en matière de performance, disponibilité des systèmes et planification de la continuité d'affaires**

Agenda

- **Introduction**
- **Pourquoi chiffrer**
- **Comment…**
  - **Démarrer serveur**
  - **Connecter client ABL, JDBC et ODBC**
- **Démo**
- **Questions**

Introduction

- **Qu'est-ce que c'est « SSL » ?**
  - ***Secure Sockets Layer***
  - **Chiffrage des communications**
- **Internet : HTTPS**
  - ***HTTP Tunneling through SSL***
- **Intranet : SSL OpenEdge**
  - ***TCP/IP tunneling through SSL***

Standards supportés

- **SSL Protocol Version 2.0/3.0**
  - **Transport Layer Security Working Group**
    - **Netscape**
- **TLS Protocol Version 1.0**
  - **Network Working Group RFC2246**
- **PKI x.509**
  - **PKIX Working Group**

Clés

- **OpenEdge utilise clé privée – clé publique**
- **Clé privé générée par OpenEdge**
  - **Envoyé à un CA**
    - ***Certificat Authority***
- **CA retourne la clé publique**
  - **Importé dans OpenEdge**

Certificats CA

- **Le CA est le « tiers de confiance* »**
  - **« Trusted authentication authority »**
  - **Signe les demandes de clé**
- **Client doit avoir certificat *root* du CA**
- **Certificats CA root connus distribués avec OE**
  - **RSA, Thawte, Verisign…**

*** Merci au grand dictionnaire terminologique**

Gestions des clés/certificats

- **OpenEdge gère ses clés dans $DLC**
  - **$DLC/keys pour les clés**
  - **$DLC/certs pour les certificats CA**
- **Outils**
  - **$DLC/bin/pkiutil**
  - **$DLC/bin/certutil**
  - **$DLC/java/jdk/bin/keytool**

Clé par défaut

- **OpenEdge fourni une clé test:**
  - **« default_server »**

```
Keystore entry: default_server
Certificate:
subject= /C=US/ST=NH/O=Progress Software
   Corporation/OU=Server Technologies/CN=Default
   Progress SSL Server
issuer= /C=US/ST=NH/O=Progress Software
   Corporation/OU=Server Technologies/CN=Progress Server
   Certificate Authority
notBefore=Feb 25 22:04:12 2004 GMT
notAfter=Feb 22 22:04:12 2014 GMT
```

JDBC/ODBC

- **Clients non-OpenEdge doivent gérer eux-mêmes leurs certificats**
  - **Java : keytool**
  - **ODBC : Fichier certificat**
  - **.Net : Microsoft Certificate Store Mgmt**

Pourquoi chiffrer?

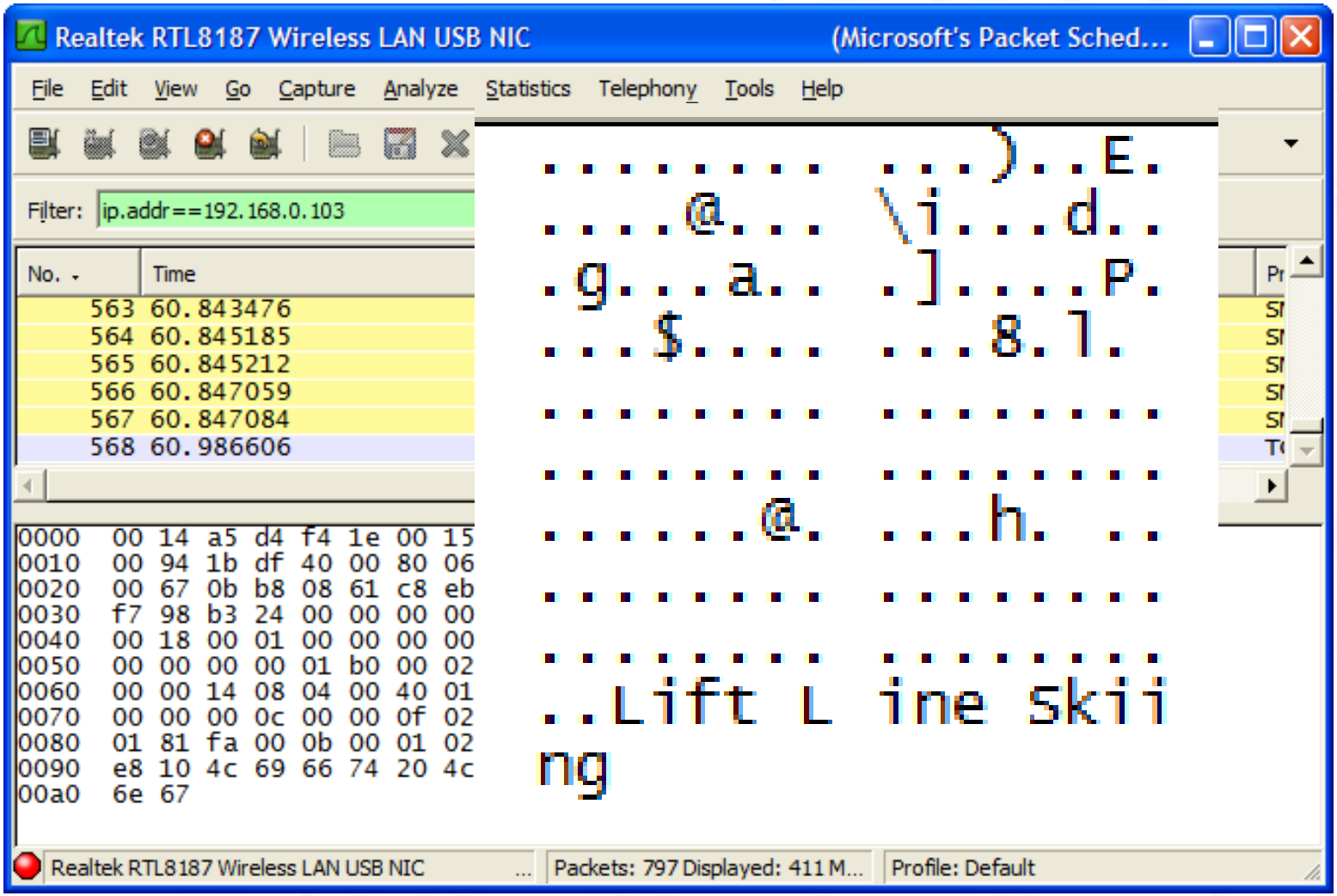
- **Données confidentielles**
- **Mots de passe**

- ***Sniffer* réseau gratuit et facile à utiliser**
  - **WireShark**

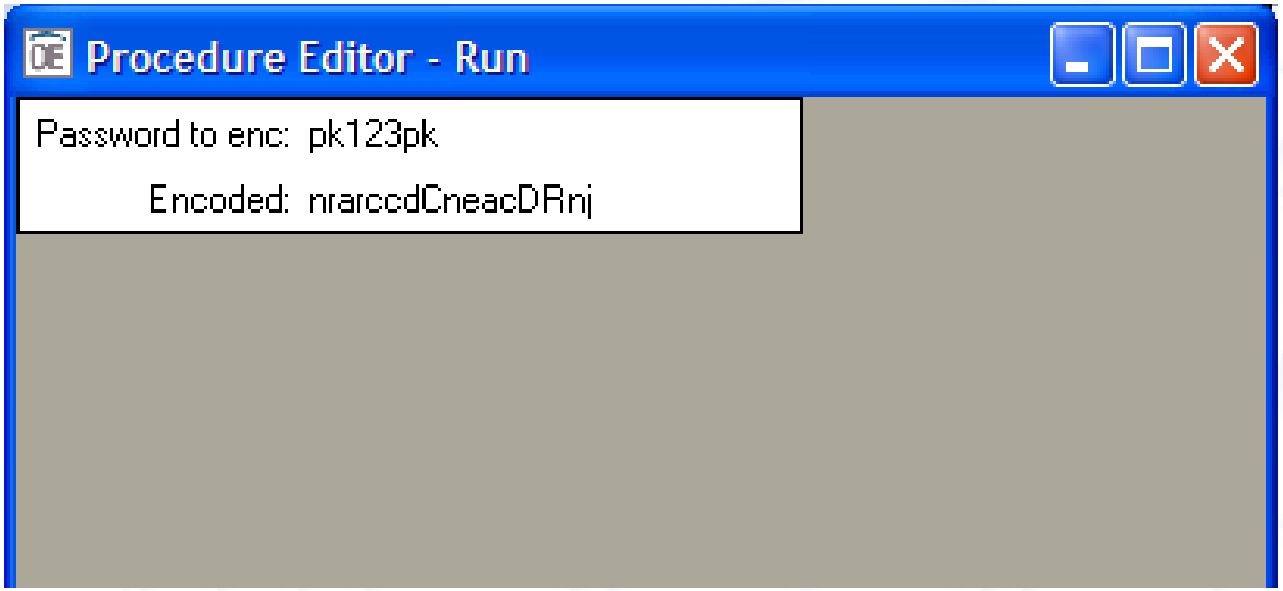
Exemple 1

```
FOR EACH customer FIELDS(name):
  DISPLAY NAME.
END.
```

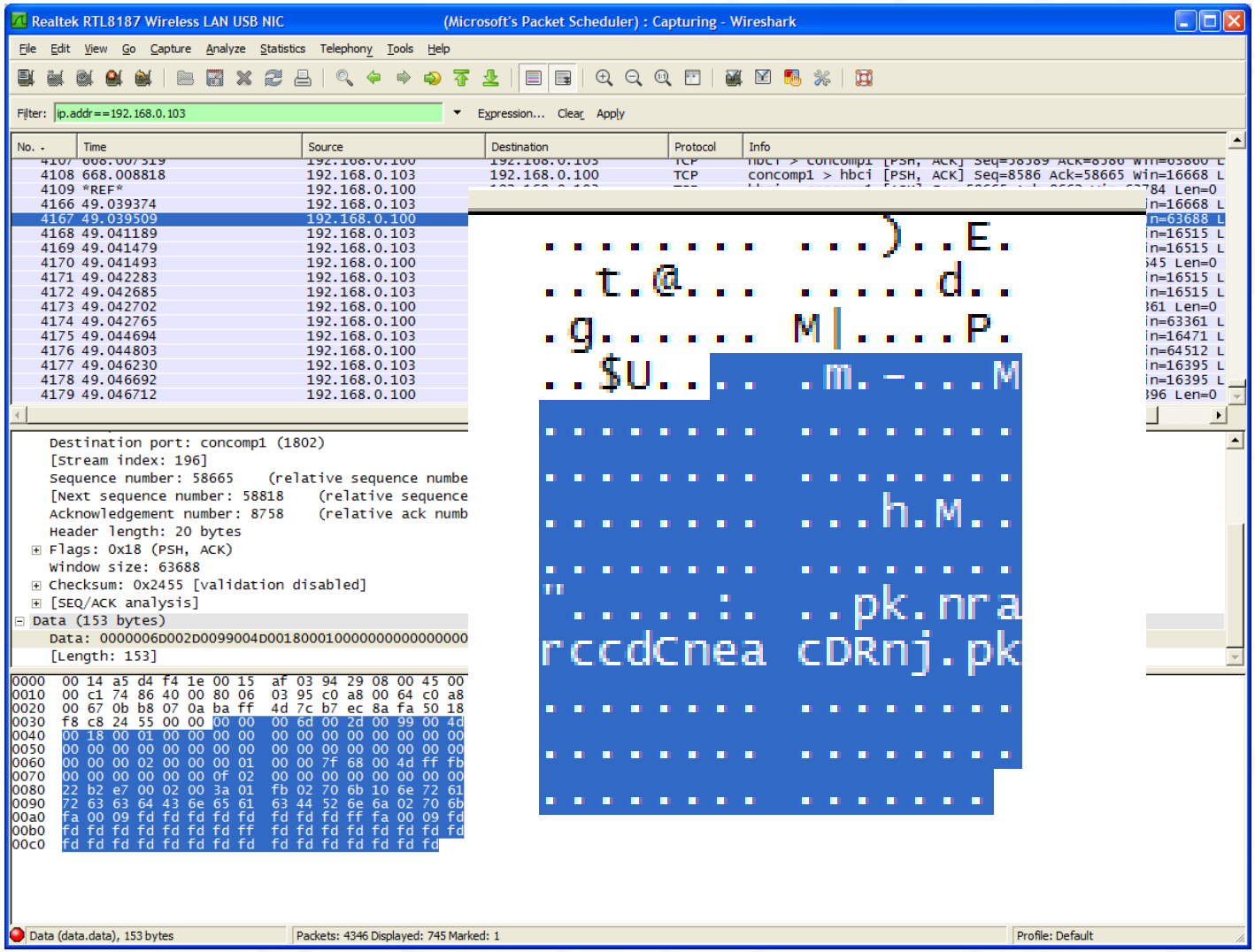
Sniffer réseau



Exemple 2



Sniffer réseau



Procédure

- Créer la demande
- Faire signer la demande
- Importer le certificat retourné
- Démarrer BD
- Connecter clients
  - ABL
  - JDBC
  - ODBC

Créer une demande de cert

```
C:\apps\openedge\wrk102a>pkiutil -newreq gupq
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
......++++++++++++
writing new private key to 'C:\apps\openedge\oe102a/keys/requests/gupq.pk1‘

Country Name (2 letter code) [US]:CA
State or Province Name (full name) []:QC
Locality Name (eg, city) []:
Organization Name (eg, company) []:Progresswiz
Organizational Unit Name (eg, section) []:
Server DNS name []:pckoup

You may now use the file C:\apps\openedge\oe102a/keys/requests/gupq.pk10 to
request a new Digital Certificate from a CA Certificate Authority.

After you obtain the new Digital Certificate from the CA use the -import
   command to insert the certificate into the keystore.
```


Faire signer la demande

- **Verisign, etc…**
  - **Envoyer le .pk10**
- **J'utilise un certificat CA créé avec OpenSSL**

```
C:\apps\openedge\wrk102a\sslkeys>openssl ca -config
   pk.conf -notext -out gupq.pem.cert -infiles
   C:\apps\openedge\oe102a/keys/requests/gupq.pk10

<détails omis...>

Certificate is to be certified until Feb  1 02:19:29
   2011 GMT (365 days)
Sign the certificate? [y/n]:y
```

Importer le certificat signé

- **Dans l'installation OpenEdge serveur**
  - **Attention au comportement bizarre de pkiutil (voir démo)**

```
C:\apps\openedge\wrk102a>pkiutil -import gupq
   sslkeys\gupq.pem.cert
Importing private key alias gupq:
Importing certificate file sslkeys\gupq.pem.cert

Enter keystore password to alias gupq: gupq
```

Valider

```
C:\apps\openedge\wrk102a>pkiutil –list

Keystore entry: gupq
Certificate:
subject= /C=CA/ST=QC/O=Progresswiz/CN=pckoup
issuer= /C=CA/ST=Some-State/O=Internet Widgits Pty Ltd
notBefore=Feb  1 02:19:29 2010 GMT
notAfter=Feb  1 02:19:29 2011 GMT
```

Importer le certificat du CA

- **Seulement si CA interne**
- **Certificats connus sont déjà installer avec OE**

```
C:\apps\openedge\wrk102a\ssl>certutil -import
   ..\sslkeys\pkca.crt

Importing trusted certificate to alias name: 39d36856
```

- **Nouveau fichier $DLC/certs/39d36856.0**

Distribuer certificat CA

- **Encore - seulement si demande signé par CA interne**
  - **Chaque client OpenEdge doit importer avec certutil -import**

Mot de passe

- **Lors de la création de la requête un mot de passe a été spécifié**
- **Générer le mot de passe encrypté:**

```
C:\apps\openedge\wrk102a\ssl>genpassword -password gupq
37273f36
```


Démarrer la BD

```
C:\apps\openedge\wrk102a\ssl>_mprosrv ssl -H pckoup -S
   5000 -ssl -keyalias gupq
-keyaliaspasswd 37273f36
```

- **Dans le .lg de la BD:**

```
SSL Encryption has been enabled for ALL TCP/IP
   connections to this database
SSL Key Alias Name (-keyalias): gupq
```

Attention!

- **Impossible d'avoir des connexions distantes chiffrées et non-chiffrées**
- **Tous les brokers démarrés utiliseront la même clé SSL**

Connecter un client ABL

```
prowin32 ssl –H pckoup –S 5000
```

- **Pas besoin de spécifié –ssl**
  - **Le serveur le dit au client**
- **Rien dans le .lg confirme que la connexion est SSL**
  - **À part les messages de démarrage**

Sans certificat CA

```
prowin32 ssl –H pckoup –S 5000
```

```
+------------------------------- Error --------------------------------+
¦ SSL error 12072 - SSL Client handshake failure (-54) unable to get local ¦
¦   issuer certificate: for 39d36856.0 in C:\apps\OpenEdge\oe102a\certs    ¦
¦                              occurred. (12168)                          ¦
¦ Error starting SSL handshake with the OpenEdge database server. (12167)  ¦
¦                                                                         ¦
¦ ----------------------------------------------------------------------- ¦
¦                                  <OK>                                   ¦
+-------------------------------------------------------------------------+
```

- **Dans le .lg de la BD**

```
Usernum 1 terminated abnormally.
```

Client JDBC

- **Créer un *keystore* Java avec keytool**
  - **$DLC/jdk/bin/keytool**

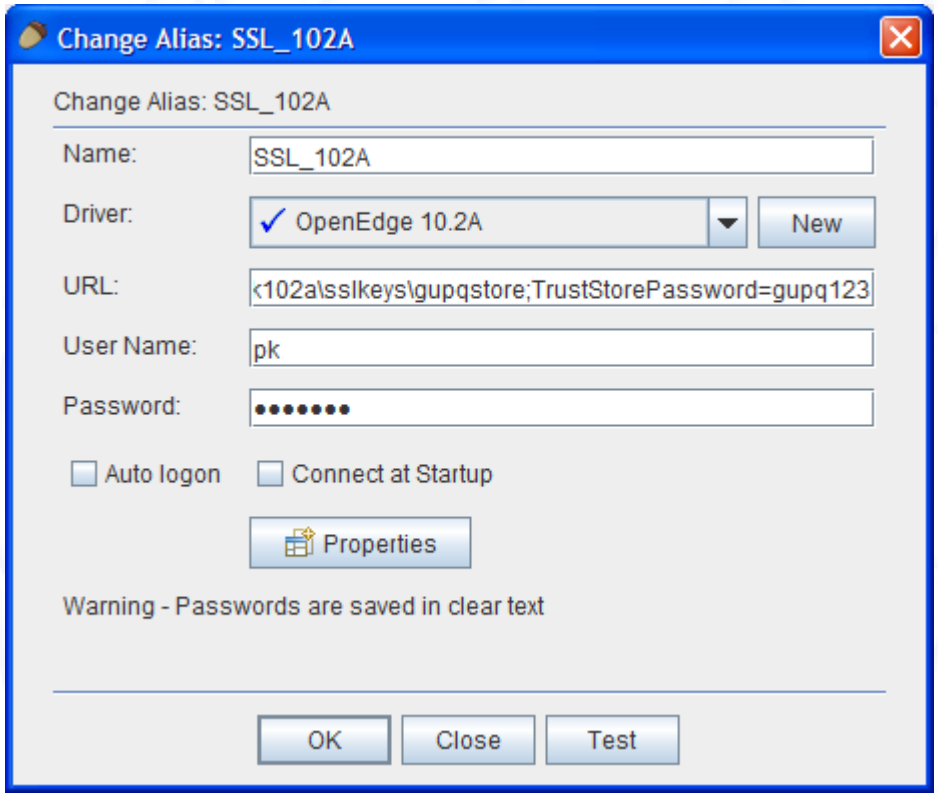
```
C:\apps\openedge\wrk102a\sslkeys>keytool -import -alias
   ca -file pkca.crt -keypass ca -keystore gupqstore -
   storepass gupq123
<snip...>
Trust this certificate? [no]:  y
Certificate was added to keystore
```

- **Fichier « gupqstore » créé**

Test JDBC

- **Squirrel SQL Client (gratuit)**

```
jdbc:datadirect:openedge://localhost:5000;databaseName=
   ssl;EncryptionMethod=ssl;Truststore=c:\apps\openedge\
   wrk102a\sslkeys\gupqstore;TrustStorePassword=gupq123
```



Test JDBC

- **Sans paramètres SSL:**

```
SSL_102A_NOSSLPARAMS: [DataDirect][OpenEdge JDBC
   Driver]SSL Mismatch.  Encryption method in client and
   server must match.
```

Client ODBC

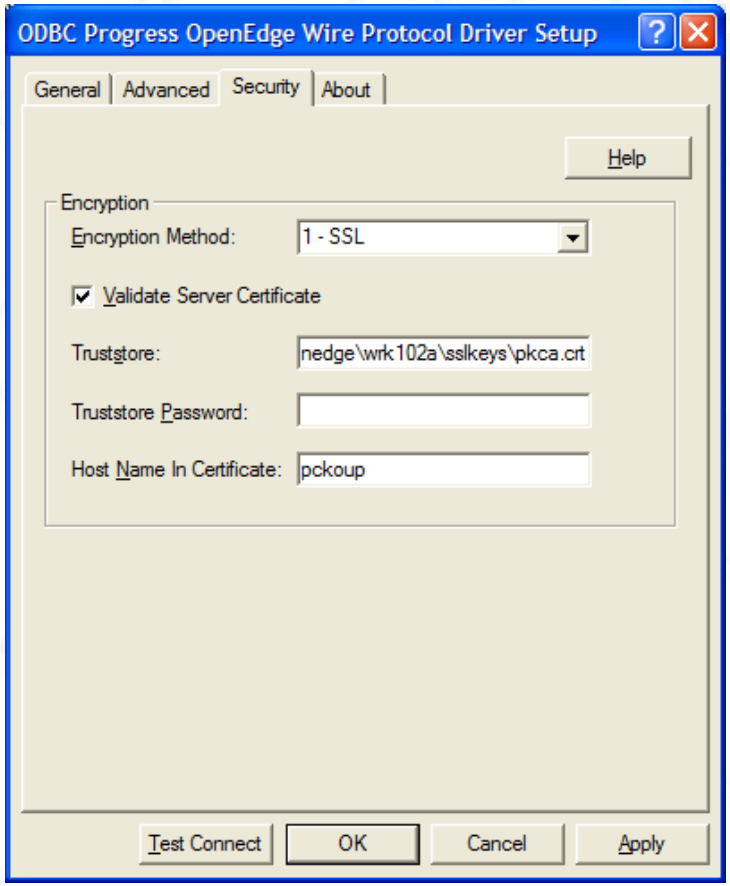
- **Un peu plus compliqué**
- **Vraiment mais vraiment pas du tout documenté**
  - **Rien dans la doc ni dans le KB**

Client ODBC

- **OE 10.1C SP 4 et plus**
  - **Avant ça…pas certain**
  - **Il y avait un bug…**
- **Copier pgcrypto.dll et pgss123.dll dans %windir%**
- **Créer DSN dans administrateur ODBC**

DSN ODBC

- Créer DSN comme d'habitude
- Spécifier encryption SSL
- Fichier certificat CA dans « TrustStore »
- Aucun mot de passe n'est nécessaire



Démo

- **Démarrage de serveur**
- **Connexion client ABL**
- **Connexion client JDBC**
- **Connexion client ODBC**

Questions ?

Informatique Progresswiz

- **Questions ou commentaires?**
  pk@progresswiz.com
- **PPTs, articles et outils disponible au**
  www.progresswiz.com

Merci !

