



Une filiale de **Generix Group**

Problème SSL avec les banques

Procédure de correctif

eBanks

Dernière version : 2.42

Table des matières

1.	Introduction.....	3
2.	Erreurs rencontrées	3
3.	eBANKS sous Windows	3
4.	eBANKS sous AS400	4

1. Introduction

Vous êtes utilisateur de l'appli d'échanges bancaires **eBANKS**.

Suite à la faille [Poodle](#) (voir [mailing octobre 2014](#)), les banques ont décidé de renforcer la sécurité des échanges (suppression d'ancien protocole tel que SSL et augmentation taille des clefs).

Afin de vous permettre de continuer d'utiliser vos services d'échanges bancaires, il est **obligatoire** de vous mettre à jour (version 2.42 au 26 juin 2017) et de modifier la JDK utilisée par **eBANKS**.

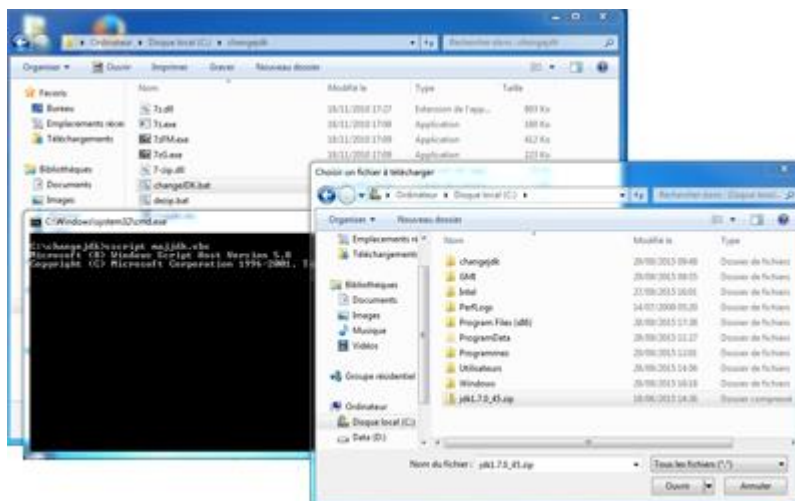
2. Erreurs rencontrées

Vos messages eBANKS peuvent avoir plusieurs libellés d'erreurs :

- SSLHandShakeException
- java.lang.ArrayIndexOutOfBoundsException: Array index out of range: 64

3. eBANKS sous Windows

1. **Stoppez les services "Moteur_ebanks" et "Jakarta4"**.
2. Mettez-vous à jour en suivant la [documentation](#).
3. Modifiez le JDK :
 - a. Téléchargez le fichier disponible [ici](#) (Si le lien ne fonctionne pas : <http://www.gmi-connectivity.com/DATA/changejdkbanks.zip>) et dézippez le contenu à la racine du poste.
 - b. Téléchargez la nouvelle JDK [ici](#) (Si le lien ne fonctionne pas : http://www.gmihebergement.fr/jdk1.7.0_45.zip) et placez le fichier à la racine du poste.
 - c. Exécutez avec les droits administrateurs, le programme "changeJDK.bat" se trouvant dans le dossier "changejdk" précédemment dézippé.
 - d. Une fenêtre s'ouvre vous demandant de sélectionner le fichier "jdk1.7.0_45.zip". **Il ne faut surtout pas le dézipper ou changer son nom**. Puis cliquez sur "Ouvrir".
 - e. Désinstallez le service Jakarta4 en cliquant sur "removeJakarta.bat" qui se trouve dans le dossier d'installation d'eBANKS.
 - f. Intallez le service Jakarta4 en cliquant sur "installJakarta.bat" qui se trouve dans le dossier d'installation d'eBANKS.
 - g. Redémarrez les services "Moteur_ebanks" et "Jakarta4".
 - h. Exemple de fenêtre



4. eBANKS sous AS400

Nous ne maintiendrons plus eBANKS sur la version V5R4 d'OS400.

Cette version d'OS400 ne permet plus de maintenant le niveau de sécurité requis par les serveurs bancaires.

Deux solutions ;

- 1- Faire évoluer sa version d'OSA400 afin de profiter des mises à jour,
- 2- Soit migrer eBANKS sur Windows.

Note : IBM ne maintient plus la version V5R4 depuis le 30/09/2016.

Pour corriger les problèmes « Array index out of range: 64 », il est nécessaire de posséder une JDK 1.6 minimum à jour.

Plus d'informations sur le site d'IBM disponible ci-dessous.

IBM. *IBM IV74069: LARGE PRE-MASTER SECRET GENERATED FROM 2048 BIT DH KEY NOT DIGES TED IN TLSV1 AND TLSV1.1 - France.* [en ligne].

Disponible sur : < <http://www-01.ibm.com/support/docview.wss?uid=swg1IV74069>

> (Consulté le 26/06/2017)

GMI vous recommande l'utilisation d'une JDK 1.7 et de modifier 3 fichiers.

/ebanks/MoteurEbics.sh

/ebanksMoteurEbicsD.sh

Dans ces deux fichiers ci-dessous, ajouter/remplacer les informations en rouge :

```
#
# $Id: startup.sh,v 1.6 2004/02/27 05:32:58 billbarker Exp $
#
# Copyright 1999-2004 The Apache Software Foundation
#
# Licensed under the Apache License, Version 2.0 (the "License");
# you may not use this file except in compliance with the License.
# You may obtain a copy of the License at
#
# http://www.apache.org/licenses/LICENSE-2.0
#
# Unless required by applicable law or agreed to in writing, software
# distributed under the License is distributed on an "AS IS" BASIS,
# WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
# See the License for the specific language governing permissions and
# limitations under the License.
#

# Shell script to startup the server
#!/bin/sh

EBICS=/ebanks
QIBM_CSSID=1252
CLASSPATH=:$EBICS:$EBICS/jar/runner.jar:$EBICS/jar/webserveur.jar:$EBICS/jar/db2_classes.jar:$EBICS
/jar/ebics.jar:$EBICS/jar/bcmail-jdk14-139.jar:$EBICS/jar/bcprov-jdk14-
139.jar:$EBICS/jar/activation.jar:$EBICS/jar/mail.jar:$EBICS/jar/commons-codec-
1.4.jar:$EBICS/jar/commons-collections.jar:$EBICS/jar/commons-logging-api.jar:$EBICS/jar/dom4j-
1.6.1.jar:$EBICS/jar/dom.jar:$EBICS/jar/jaxen-
1.1.1.jar:$EBICS/jar/xalan.jar:$EBICS/jar/xercesImpl.jar:$EBICS/jar/xmlsec-
1.4.3.jar:$EBICS/jar/ibmlog.zip:$EBICS/jar/struts-legacy.jar:$EBICS/jar/commons-
dbcp.jar:$EBICS/jar/commons-pool.jar:$EBICS/jar/postgresql-8.2-
506.jdbc2.jar:$EBICS/jar/jt400native.jar:$EBICS/jar/commons-httpclient-
3.0.1.jar:$EBICS/data:$EBICS/jar/smtp.jar:$EBICS/jar/fop.jar:$EBICS/jar/xmlgraphics-commons-
1.2.jar:$EBICS/jar/batik-all-1.6.jar:$EBICS/jar/xercesImpl.jar:$EBICS/jar/xml-apis.jar:$EBICS/jar/jcifs-
1.3.17.jar:
```

```
export QIBM_CSSID=1252
export EBICS
export CLASSPATH
export PATH

export JAVA_HOME=/QOpenSys/QIBM/ProdData/JavaVM/jdk626/32bit

exec /QOpenSys/QIBM/ProdData/JavaVM/jdk626/32bit/bin/java -Djava.version=1.6 -
Dnetworkaddress.cache.ttl=60 -Djava.awt.headless=true -classpath ${CLASSPATH} -Xms128M -Xmx256M
ebics.MoteurEbics
```

Note : Vérifier que le chemin en rouge existe sur votre AS400 et adapter-le si nécessaire.

/ebanks/tomcat-4.1.40/bin/setclasspath.sh

Dans ce script, modifier la partie :

```
var=$QSH_VERSION
sousver=${var:3:1}
if [ ${var:1:1} -lt 7 ]
then

    export JAVA_HOME=/Qibm/proddata/java400/jdk15

else
# print success
echo "Cas > 7"
if [ $sousver -lt 2]
then
export JAVA_HOME=/QOpenSys/QIBM/ProdData/JavaVM/jdk50/32bit
else
export JAVA_HOME=/QOpenSys/QIBM/ProdData/JavaVM/jdk60/32bit
fi
fi
java -version
```

Si vous êtes en version V7R1, modifier le chemin de la chaîne de caractère en vert.
Si vous êtes en version V7R2, modifier le chemin de la chaîne de caractère en bleu.

Une fois les modifications apportées, redémarrer le sous-système eBANKS.