Banque et Etablissement de Paiement

Sécurisation
DES COMMUNICATIONS EBICS

Introduction

Le Comité Français d'Organisation et de Normalisation Bancaires (CFONB) a publié le 16/07/2015 la communication n°2015-0042 concernant le renforcement de la **sécurité EBICS** : Face à une augmentation alarmante de la fraude sur les virements bancaires, le protocole **TLS** devra être utilisé en lieu et place du SSL **dans tous les échanges EBICS**, et ce dès le **1er octobre 2015**.

Afin de prendre en compte tous les aspects liés à cette **modification de la sécurité** nous rappellerons rapidement ce qu'est le SSL et le TLS puis nous proposerons un **modèle de configuration** qui permet de mettre en œuvre les recommandations du CFONB.

Un dernier chapitre traitera **des impacts** sur les contextes des clients de la banque et fournira des précisions sur le parc des clients de Cedricom qui utilisent les logiciels Cedripack , Optichèque ou la solution Sycomore.

Définition SSL/TLS

Le **SSL** et le **TLS** sont des protocoles de cryptage qui garantissent pleinement la sécurité des communications pour tous les mails échangés. Ces systèmes sont largement utilisés pour garantir la **sécurité des communications sur internet**.

L'acronyme SSL *signifie "Secure Socket Layer".* C'est un protocole permettant l'échange de données de manière sécurisée. Lorsque vous utilisez Internet, ce protocole nous permet de communiquer en évitant qu'une tierce partie puisse falsifier ou altérer le contenu de vos messages.

L'acronyme TLS *signifie "Transport Layer Security".* Il s'agit là aussi d'un protocole de sécurité, assurant la confidentialité des informations échangées entre des applications et leurs utilisateurs sur internet.

TLS fait également en sorte d'éviter que des tiers puissent altérer ou falsifier vos messages.

Il est constitué de deux couches :

- le Protocole **TLS Record** (enregistrement)
- et le Protocole **TLS Handshake** (poignée de main)

Le premier fournit une connexion sécurisée grâce aux méthodes comme DAE (Data Encryption Standard, ou "standard de cryptage de données" en français). Il peut également être utilisé sans cryptage.

Le second protocole, lui, permet au serveur et à l'ordinateur de s'identifier l'un à l'autre puis de choisir ensemble un algorithme de cryptage et des clés secrètes avant de commencer à s'envoyer des données ou des messages.

Source information :
https://fr.mailjet.com/support/qu-est-ce-que-le-ssl-et-le-tls-est-ce-que-cela-securise-mes-communications,32.htm

Historique :

- SSLV3 a été publié en 1996.
- L'implémentation corrigeant les défauts de cette version est TLSv1.0 (2001).
- Viennent ensuite les versions TLSv1.1 puis v1.2 qui sont des refontes du standard TLS.

L'application Apache gère les accès https des clients et fait appel à la librairie OpenSSL qui prend en charge les protocoles de sécurité.

Les versions **2.2.11** et **2.2.22** d'Apache prennent en charge les niveaux TLS1.0, TLS1.1 et TLS1.2

CEDRICOM recommande de disposer du socle technique **Apache 2.4.12 / Openssl 1.01** pour des raisons de sécurité.

Cedricom dispose d'experts à même de vous accompagner dans cette démarche, n'hésitez pas à contacter votre référent Cedricom ou à envoyer un mail à commercial@cedricom.com

Cedricom

Renforcement de la sécurité & Paramétrage serveur

Ce **paramétrage** s'effectue sur le **serveur APACHE**. Il doit être effectué par l'administrateur système du site ou l'application serveur EBICS est utilisée.

Plusieurs cas doivent être considérés en fonction de la version d'Apache dont vous disposez.

Désactiver SSLv2 et SSLv3 sur votre serveur Apache

Dans votre configuration Apache, par exemple :

Configuration générale au serveur :

```
/etc/apache2/conf/httpd.conf
```

Module SSL / configuration SSL :

```
/etc/apache2/conf/sites-enable/ssl.conf
```

Votre configuration de site :

```
<VirtualHost *:443>
```

Retrouvez le paramètre SSLProtocol pour désactiver SSLv2 et SSLv3, par exemple :

```
<VirtualHost *:443>
ServerName www.monsite.fr
DocumentRoot /var/www/www.monsite.fr
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCertificateFile chemin/certificat-xxxx.cer
SSLCertificateKeyFile chemin/clefprivee-
xxxw.key
SSLCertificateChainFile chemin/chain-xxx.txt
</Virtual Host>
```

Relancer ensuite Apache

Dans cette configuration avancée,
Nous recommandons aussi de la configuration suivante pour les protocoles / algorithmes d'échange de clefs et de chiffrement :

```
SSLHonorCipherOrder On
SSLCipherSuite
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:DH+
AES:ECDH+3DES:DH+3DES:RSA+AESGCM:RSA+AES:RSA+3D
ES:!aNULL:!MD5:!DSS
```

Impacts outils clients

En ce qui concerne les outils clients Cedricom,

- Les logiciels **Cedripack** et **Solutions Chèques** sont compatibles avec les recommandations du CFONB. Les utilisateurs sous maintenance disposant de versions anciennes ont été avertis. Ils disposent d'un **accès libre** à notre service d'assistance et aux téléchargements des dernières **mises à jour**.

- La solution SaaS **Sycomore est compatible**, Cedricom garantit les niveaux de sécurité recommandés par le CFONB.

Cedricom recommande aux clients qui n'utilisent pas ses produits de se retourner vers **leur éditeur**. Il faudra alors obtenir une **version compatible**.

Si certaines **banques** envisagent d'utiliser uniquement la **version TLS 1.2**, cela pourrait occasionner des **ruptures de service** pour les clients qui utilisent des solutions obsolètes.

Cedricom

7, rue de la Motte d'Ille
BP 43107 – 35831 BETTON Cedex

Téléphone : +33 (0)2 99 55 49 48
Télécopie : +33 (0)2 99 55 49 49
http://www.cedricom.com

Cedricom