Passage aux certificats SHA-2

Foire aux questions

Comment puis-je utiliser ce document ?

Cette FAQ fournit des réponses à certaines des questions les plus fréquemment posées par nos clients concernant notre intention de remplacer les certificats SHA-1 par les certificats SHA-2. Ce document sera hébergé sur http://www.opentext.com/campaigns/sha2.

Qu'est-ce que SHA-2 ?

SHA-2 est un algorithme de hachage cryptographique, publié pour la première fois par l'Agence Nationale de Sécurité américaine en 2001. SHA est l'acronyme de *Secure Hash Algorithm* (Algorithme de Hachage Sécurisé). Les fonctions de hachage SHA sont utilisées au sein des applications et protocoles de sécurité tels que TLS et SSL, et en conjonction avec des algorithmes à clé publique dans le cadre à la fois du chiffrement et des signatures électroniques.

Pourquoi OpenText passe-t-il des certificats SHA-1 aux certificats SHA-2 ?

Du fait des avancées récentes en matière d'attaques cryptographiques, les spécialistes de la sécurité réseau ont mis en garde contre l'utilisation de certificats SHA-1 qui pourrait laisser un pirate usurper du contenu, exécuter des attaques d'hameçonnage, ou réaliser des attaques dites de « l'homme du milieu ». Bien qu'OpenText™ Trading Grid™, OpenText Information Exchange, OpenText EasyLink GMS et OpenText EasyLink ICC.Net ne présentent pas cette vulnérabilité potentielle, nous sommes en train de passer aux certificats SHA-2 dans le cadre des efforts que nous déployons pour continuer à faire profiter nos clients du plus haut niveau d'intégrité et de sécurité des données.

Le hachage de chiffrement utilisé dans SHA-2 est bien plus puissant que dans SHA-1 et ne présente pas les mêmes vulnérabilités que ce dernier.

Pour savoir si vos systèmes internes prennent en charge SHA-2, veuillez consulter https://www.digicert.com/sha-2-compatibility.htm

Que fait OpenText afin de passer à SHA-2 ?

OpenText commencera à renouveler tous les certificats en tant que certificats SHA-2 une fois le certificat actuel arrivé à expiration. Nous prévoyons d'être complètement passés des certificats SHA-1 aux certificats SHA-2 d'ici au **1er janvier 2017**, date annoncée par Microsoft® à laquelle ce dernier cessera de prendre en charge les certificats SHA-1. Les certificats SHA-2 seront émis par notre autorité de certification actuelle, Comodo.

Remarque : *nous nous réservons le droit de mettre à niveau les certificats d'environnement de pré-production avant qu'ils n'arrivent à expiration pour laisser le temps aux clients de les essayer aux côtés de leurs partenaires commerciaux.*

En quoi suis-je concerné(e) ?

Si vous, ou votre partenaire commercial, utilisez FTPS, AS2, RosettaNet, OFTP, MQ, AS3 ou un autre protocole pour établir une connexion d'échange de message chiffré ou signé électroniquement à l'aide de Trading Grid™, Information Exchange, EasyLink GMS ou EasyLink ICC.Net, OpenText vous conseille de

vous préparer au remplacement des certificats SHA-1 par les certificats SHA-2 en vue de renforcer les mesures de sécurité.

Que dois-je faire ?

Pour amorcer ce changement et veiller au bon déroulement du processus de renouvellement des certificats :

1. Vérifiez auprès de votre prestataire de service ou fournisseur de logiciel que votre logiciel de communication prend bel et bien en charge les certificats SHA-2 émis par Comodo.
    a. Si c'est le cas, vous pourrez commencer à planifier votre transition vers le certificat SHA-2 bien plus sécurisé, une fois votre certificat OpenText à clé publique arrivé à expiration.
    b. Dans le cas contraire, et si votre fournisseur de logiciel de communication actuel ne peut vous aider, veuillez contacter votre Gestionnaire client OpenText afin d'aborder les options qui s'offrent à vous.
2. Contactez vos partenaires commerciaux et demandez-leur de vérifier à leur tour auprès de leur fournisseur de logiciel de communication que leur logiciel de communication prend bel et bien en charge les certificats SHA-2 émis par Comodo, notre fournisseur actuel de certification.

Le processus de renouvellement des certificats va-t-il changer ?

Aucun changement n'affectera les processus de renouvellement des certificats. Cependant, il se peut qu'OpenText renouvelle les certificats en tant que certificats SHA-2 avant qu'ils n'arrivent à expiration, pour des raisons de conformité, avant la date limite fixée au 1er janvier 2017.

Que faire si mon certificat OpenText à clé publique actuel arrive à expiration après le 31 décembre 2016 ?

OpenText prendra l'initiative de contacter les clients possédant actuellement des certificats OpenText SHA-1 à clé publique pour les aider à passer aux certificats SHA-2 avant la date limite fixée au 1er janvier 2017.

Quels sont les services affectés par ce changement ?

Ce changement affecte tous les certificats SSL de navigateur et certains protocoles de communication. Si vous vous connectez à OpenText à l'aide d'un navigateur Web moderne, vous n'êtes pas concerné(e) par la mise à niveau des certificats.

Remarque : *à l'heure actuelle, les clés de chiffrement SSH, PGP et GPG ne sont pas concernées.*

Quels sont les protocoles affectés par ce changement ?

Les protocoles suivants sont affectés par le passage aux certificats SHA-2 :

- AS2
- AS3
- HTTP sur SSL (HTTPS)
- FTP sur SSL (FTPS)

- RosettaNet
- MQ
- Sterling/IBM – Connect:Direct Secure Plus

Quelles fonctions de hachage SHA-2 OpenText prend-il actuellement en charge ?

OpenText prend actuellement en charge les certificats signés par les versions de SHA-2 suivantes :

- SHA256
- SHA384
- SHA512

À l'avenir, OpenText prévoit de prendre en charge d'autres types de certificats SHA-2. De plus amples informations seront communiquées au fur et à mesure.

Mon logiciel de communication ne prend pas en charge les certificats SHA-2. Que dois-je faire ?

Bien qu'OpenText recommande de passer aux certificats SHA-2 afin de préserver le plus efficacement possible l'intégrité et la sécurité des données, nous sommes conscients que certains clients ne peuvent pas prendre en charge les certificats SHA-2.

Si votre logiciel ne prend pas en charge les certificats SHA-2 ou auto-signés, l'équipe Certificates Exchange travaillera à vos côtés pour apporter une solution alternative qui sera valide pour une durée d'un an maximum. Après le 31 décembre 2015, OpenText ne permettra plus d'opter pour la délivrance de certificats autres. Début 2016, l'équipe Certificates Exchange désactivera toutes les options de délivrance de certificats SHA-1, exigeant des clients qu'ils passent à un certificat SHA-2 ou auto-signé. Si vous ne pouvez toujours pas prendre en charge les certificats SHA-2 à ce moment-là, l'équipe Certificates Exchange travaillera à vos côtés pour mettre en œuvre un certificat SHA-1 auto-signé.

Équipe Certificates Exchange

Email : CertificateExchange@opentext.com
Téléphone : 1-800-334-2255 x2378 (CERT)

Qui est Comodo ?

Comodo est la principale autorité de certification d'OpenText. Les autorités de certification sont des organismes dont le rôle est de délivrer et de gérer des certificats numériques. Pour plus d'informations, veuillez consulter le site Web de Comodo : www.comodo.com.

Pourquoi OpenText a-t-il changé pour Comodo ?

OpenText a choisi Comodo car celle-ci offre une gamme complète de certificats numériques dotés du meilleur chiffrement qui soit, ainsi que les capacités techniques et la souplesse permettant de répondre aux besoins de l'entreprise. En tant qu'Autorité de Certification (AC) WebTrust, Comodo répond aux

normes les plus strictes en matière de confidentialité, de fiabilité du système et de pratiques commerciales pertinentes par le biais d'audits indépendants certifiés.

Passer à Comodo pourrait-il avoir un impact sur mes services ?

Passer à un certificat émis par Comodo aura peu d'incidence sur les produits plus récents d'échange de fichiers. Comodo étant une Autorité de certification relativement récente, il se peut que les clients disposant de produits d'échange de fichiers plus anciens (> 10 ans) éprouvent des difficultés à charger les certificats racine et intermédiaires vers leur base de certificats. Pour plus d'informations, veuillez consulter le site Web de Comodo : www.comodo.com.

Remarque : *les clients disposant de produits d'échange de fichiers plus anciens ou d'un logiciel élaboré en interne doivent charger tous les certificats enchaînés (.p7b). Si vous utilisez les versions .cer, veillez à ce que les certificats Comodo soient tous les trois chargés dans votre base de certificats.*

Qui dois-je contacter pour plus d'informations ?

Pour de plus amples informations, les clients OpenText Trading Grid et Information Exchange peuvent contacter les Services d'assistance Cloud .

Les clients OpenText EasyLink GMS et ICC.Net peuvent contacter l'Assistance client OpenText EasyLink.

Pour les utilisateurs de Sterling Connect:Direct uniquement

Comment savoir si ma version du logiciel Sterling Connect:Direct est compatible avec SHA-2 ?

Pour de plus amples informations sur la prise en charge de SHA-2 concernant Sterling Connect:Direct, veuillez vous référer au guide de prise en charge SHA-2 disponible sur le site Web d'IBM. Vous pouvez accéder au guide en cliquant sur le lien suivant :

ftp://ftp.software.ibm.com/software/commerce/doc/mft/cdcommon/secplus_SHA2SupportForCD_Book.pdf

Voir ***Tableau 2. Logiciels compatibles avec SHA-2*** pour vérifier si votre version de Connect:Direct prend en charge SHA-2. Si votre version n'est pas compatible avec SHA-2, différentes options s'offrent à vous. Notamment :

1. Mettre à niveau votre logiciel Connect:Direct avec une version qui prend en charge SHA-2.
2. Contacter votre représentant OpenText afin d'installer/configurer un autre protocole pour la transmission des données.

Remarque : si vous ne faites qu'envoyer des fichiers **d'entrée** par le biais d'OpenText, vous n'aurez probablement aucun problème. Cependant, à moins que votre système ne prenne en charge les certificats SHA-2, OpenText ne pourra pas vous envoyer de fichiers de données.

Quelles sont les conditions préalables standards pour se connecter à OpenText à l'aide de Connect:Direct ?

Les conditions préalables standards sont les suivantes :

- OpenText installe/ajoute uniquement des certificats clients issus d'Autorités de certification racine et/ou des certificats intermédiaires dans sa base de confiance.
- Les certificats envoyés à OpenText ne peuvent être auto-signés. OpenText n'acceptera aucun certificat auto-signé.
- L'authentification client doit être désactivée.
- OpenText préfère que les certificats soient au format codé Base64.
- Toutes les suites de chiffrement doivent être ajoutées aux paramètres de Secure+.
- OpenText est configuré pour TLSv1.

Quels certificats dois-je installer sur mon système Connect:Direct pour pouvoir me connecter à OpenText ?

Les clients doivent installer les nouveaux certificats suivants comme fichiers séparés :

- Certificat public (devant normalement contenir les certificats dans la chaîne)
- Certificat intermédiaire (devant normalement contenir la chaîne avec juste l'AC racine)
- Certificat d'AC racine

Que faire des nouveaux certificats ?

Les clients doivent installer/ajouter les certificats appropriés à leurs paramètres de Secure+ pour le nœud Connect:Direct d'OpenText ou consulter leur propre interlocuteur technique et/ou l'assistance IBM.

Dois-je supprimer vos certificats antérieurs ?

La nécessité de supprimer les certificats antérieurs dépend de vos paramètres particuliers de Secure+ pour Connect:Direct. Veuillez consulter votre propre interlocuteur technique et/ou l'assistance IBM.

D'autres paramètres Secure+ sont-ils nécessaires pour prendre en charge SHA-2 ?

Non. Cependant, s'ils le souhaitent, les clients peuvent apporter les modifications suivantes :

- Ajouter toutes les suites de chiffrement aux paramètres de Secure+.
- Supprimer les suites de chiffrement médiocres ou décousues.

Dois-je essayer le certificat SHA-2 ?

OpenText conseille à ses clients d'essayer leur nouveau certificat pour s'assurer qu'il fonctionne comme prévu. En cas de problème, les clients doivent faire une demande de service produit auprès des Services d'assistance Cloud.

Que faire si mon certificat expire ?

Un certificat expiré révèle généralement l'expiration du certificat public et non de l'AC intermédiaire ou racine. Bien souvent, vous n'avez rien à faire concernant les certificats eux-mêmes car l'AC intermédiaire et/ou l'AC racine n'ont pas changé. Si l'AC intermédiaire et/ou l'AC racine sont nouvelles, veuillez les ajouter à votre base de confiance.

About OpenText

OpenText enables the digital world by simplifying, transforming, and accelerating enterprise information needs, on premises or in the cloud. For more information about OpenText Cloud Services (NASDAQ: OTEX, TSX: OTC) visit www.gxs.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn | Facebook

www.gxs.com/support | www.easylink.com/support

NORTH AMERICA +800 334 2255 • UNITED STATES +1 301 251 65100

OTHER LOCATIONS http://techsupport.gxs.com/regional-directories