Sécurité des marchands

Guide de mise à niveau du système

Cliquez ICI pour des informations sur la conformité à la norme SHA-256.

Garantissez votre intégration à l'avance

Les menaces informatiques à l'échelle mondiale changent constamment et la sécurité de nos marchands continue d'être notre priorité. Pour qu'ils soient protégés contre les menaces actuelles et éventuelles, nous encourageons nos marchands à effectuer les mises à niveau suivantes pour leurs intégrations :

1. Cesser l'utilisation du certificat racine G2 VeriSign
2. Mettre à jour votre intégration pour qu'elle prenne en charge des certificats utilisant l'algorithme SHA-256

Pourquoi ce changement ?

L'autorité de certification (AC) publique du secteur continue d'accroître la sécurité des certificats SSL. Pendant la période préparatoire à l'application des exigences d'utilisation de l'algorithme de signature SHA-256 en 2016, le certificat racine G2 VeriSign, qui était historiquement utilisé pour connecter les extrémités de l'API PayPal et de la Notification instantanée de paiement (IPN) ne sera plus pris en charge.

Quand dois-je agir ?

Nous vous recommandons de vous préparer à ces changements. Pour consulter le calendrier détaillé, y compris les dates de mise à niveau des extrémités d'API Live et des extrémités d'API de l'environnement de test, consultez le microsite concernant les modifications de certificats SSL en 2015-2016.

NOTE: Veuillez noter que ces modifications répondent aux préoccupations relatives à la sécurité qui sont répandues dans le secteur et ne concernent pas uniquement PayPal. Lorsqu'elles seront mises en application, elles amélioreront la confidentialité et la fiabilité de vos intégrations PayPal. Puisque les détails de ces modifications varient selon les systèmes, nous vous recommandons de les effectuer avec l'aide d'un administrateur système qualifié.

1. Cesser l'utilisation du certificat racine G2 VeriSign

Le problème : Par le passé, VeriSign a émis des certificats SSL dont la chaîne de confiance était signée par un certificat racine G2 de 1 024 bits. Ces dernières années, les autorités de certification de l'état et du secteur public sont passés à des certificats plus sécurisés de 2 048 bits; VeriSign émet donc maintenant des certificats SSL dont la chaîne de confiance est signée par un certificat racine G5 de 2 048 bits émis en 2006.

Notre réponse : Conformément aux normes de l'industrie, PayPal n'acceptera plus de garantir la sécurité des connexions aux extrémités d'API et de NOTIFICATION INSTANTANÉE DE PAIEMENT qui s'attendent à ce que notre certificat ou chaîne de confiance soient signés par le certificat racine G2. Seules les demandes de connexion sécurisée qui s'attendent à ce que notre certificat ou chaîne de confiance soient signés par le certificat racine G5 obtiendront avec succès des connexions sécurisées.

Ce que vous devez faire…

Cesser l'utilisation des connexions SSL qui sont basées sur les certificats racine VeriSign avec un identifiant G2, si votre système permet actuellement l'utilisation de ce certificat racine particulier. L'industrie travaille activement à éliminer progressivement les certificats racine de 1 024 bits au cours de l'année.

- Les connexions sécurisées qui sont basées sur notre chaîne de certificat signée par le certificat racine G2 ne sont pas prises en charge :

Unité organisationnelle	Autorité de certification principale publique de classe 3 – **G2**
Numéro de série	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Certificat SHA1 empreinte digitale	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Les connexions sécurisées qui sont basées sur notre chaîne de certificat signée par le certificat racine G5 sont prises en charge :

Nom courant	Autorité de certification principale publique de classe 3 Verisign – **G5**
Numéro de série	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Certificat SHA1 empreinte digitale	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Veuillez suivre ces instructions pour vous assurer de vous connecter de manière sécurisée à l'aide d'un certificat racine G5 VeriSign pris en charge :

1. **Vérifiez votre stockage de certificats.** Demandez à votre hébergeur de site Web ou à votre administrateur système de vérifier que le certificat racine G5 VeriSign est inclus dans le stockage racine utilisé par votre code pour la validation logique. Si c'est le cas, aucune action n'est requise.
    - Consultez les liens suivants pour nous permettre de vérifier votre stockage de clés pour y détecter la présence du certificat racine G5 à l'aide de Java, Linux ou Windows.
2. **Vérifiez votre journal des erreurs.** Si le certificat racine G5 VeriSign n'a pas été téléchargé pour remplacer le certificat racine G2, vous pourriez voir des messages d'erreur semblables aux suivants :
    - Erreur d'établissement d'une liaison SSL, « Aucun certificat fiable disponible »
    - Code de résultat 31, « Échec de validation de la chaîne du certificat, aucun certificat local disponible »
    - Code de résultat 8, « Échec de la connexion SSL »
    - -1 erreur

    Pour résoudre ces problèmes, effectuez l'une des actions suivantes :

    - Mettez à jour votre logiciel à la version la plus récente qui prend en charge SHA-256.
    - Si un stockage de clés est utilisé pour l'authentification ou la validation du certificat, installez le certificat racine G5 VeriSign dans votre stockage de clés.
3. **Obtenez un certificat racine G5 VeriSign.** Si votre stockage de certificats ou votre client Java ne comprennent pas le certificat racine G5 VeriSign, demandez à votre administrateur système de le télécharger à partir de VeriSign et de l'enregistrer dans le stockage de certificats, ainsi que tout autre ensemble d'authentifications de connexions SSL.
    - Téléchargez le certificat racine G5 VeriSign de Symantec
    - Téléchargez les certificats SSL propres aux serveurs, si requis par votre serveur

2. Mettre à jour l'algorithme de signature SHA-256

Le problème : SHA-1 est un algorithme cryptographique de 22 ans qui est menacé par l'augmentation de la puissance informatique. SHA-256 utilise un algorithme plus sécuritaire avec un condensé numérique de 256 bits.

Notre réponse : PayPal met à niveau les certificats SSL sur toutes les extrémités Live et les extrémités d'environnement de test, à partir de SHA-1, jusqu'au plus fort et plus robuste SHA-256 au milieu de l'année 2016.

Ce que vous devez faire…

Veuillez suivre ces instructions pour effectuer la transition dans l'utilisation des certificats SSL qui utilisent des algorithmes de signature SHA-1 aux algorithmes de signatures plus robustes SHA-256 :

1. **Vérifiez votre environnement.** Assurez-vous que votre environnement prend en charge les certificats SHA-256.
   - Reportez-vous aux ressources en ligne, telles que le guide de compatibilité SHA-2 de DigiCert et la liste de Symantec des serveurs et navigateurs pris en charge, pour obtenir la liste des équipements et logiciels pris en charge.
   - Si une partie de votre environnement ne prend pas en charge SHA-256, vous devez remplacer ou mettre à niveau ces éléments avant de pouvoir mettre en application les nouveaux certificats.
   - Le serveur de Windows 2000 et quelques versions de Windows XP peuvent être incompatibles avec SHA-2. Ce blogue de Windows PKI sur SHA2 et Windows peut vous aider avec des correctifs et des recommandations pour la mise à niveau de votre environnement.
2. **Vérifiez vos certificats.** Si votre environnement prend en charge SHA-256, assurez-vous d'avoir le certificat racine G5 VeriSign dans votre stockage de clés.

Vous avez encore des questions ?

Pour obtenir des informations supplémentaires et pour afficher les questions/réponses, veuillez consulter le microsite concernant les modifications de certificats SSL en 2015-2016.

Merci !

Nous vous remercions de l'attention que vous voudrez bien porter à ce problème et de votre compréhension envers notre approche. Nous reconnaissons que ces mesures nécessaires peuvent causer des problèmes de compatibilité, mais nous tenons à souligner à quel point cet inconvénient à court terme est fortement compensé par notre promesse envers nos clients respectifs à assurer la sécurité de leurs comptes et de leurs informations financières.