



Cliquez [ICI](#) pour des informations sur la conformité à la norme SHA-256.

Préparer votre intégration pour l'avenir

Les menaces de sécurité mondiales évoluent continuellement, et la sécurité de nos marchands demeure notre priorité absolue. Nous encourageons nos marchands à se protéger des menaces actuelles et futures en prenant les mesures suivantes pour mettre à jour leurs intégrations :

1. Cesser d'utiliser le certificat racine VeriSign G2
2. Mettre à jour l'intégration pour prendre en charge les certificats utilisant l'algorithme SHA-256

Pourquoi ce changement ?

Le secteur des organismes de certification (OC) publics améliore constamment la sécurité des certificats SSL. En vue de l'application obligatoire de l'algorithme de signature SHA-256 en 2016, le certificat racine VeriSign G2, qui était antérieurement utilisé pour se connecter aux points de terminaison API et IPN (notification instantanée de paiement), ne sera plus pris en charge.

Quand prendre les mesures nécessaires ?

Nous vous recommandons de vous préparer à ces changements. Pour connaître le calendrier précis, y compris les dates de mise à jour pour les points de terminaison API de production et de test, consultez le [microsite sur la modification des certificats SSL 2015-2016](#).

NOTE: les modifications visent à résoudre des problèmes de sécurité qui ne sont pas spécifiques à PayPal, mais qui concernent l'ensemble des entreprises du secteur. Leur mise en œuvre améliorera la confidentialité et la fiabilité de vos intégrations PayPal. Les détails de ces modifications varient selon le système concerné, nous vous recommandons de les effectuer avec l'aide d'un administrateur système qualifié.

1. Cesser d'utiliser le certificat racine VeriSign G2

Le problème : dans le passé, VeriSign émettait des certificats SSL dont la chaîne de confiance était signée par un certificat racine G2 de 1 024 bits. Ces dernières années, les gouvernements et organismes de certification (OC) publics ont adopté des certificats plus sécurisés de 2 048 bits. VeriSign émet donc désormais des certificats SSL avec une chaîne de confiance signée par un certificat racine G5 de 2 048 bits, émis en 2006.

Notre réaction : conformément aux normes en vigueur dans le secteur, nous n'accepterons plus les connexions sécurisées aux points de terminaison API/IPN qui prévoient une signature de notre chaîne de certificat ou de confiance par le certificat racine G2. Seules les demandes de connexion sécurisée exigeant que la chaîne de certificat ou de confiance soit signée par le certificat racine G5 permettront l'établissement de connexions sécurisées.

Ce que vous devez faire

Cessez d'utiliser les connexions SSL qui dépendent de certificats racines VeriSign avec un identifiant G2, si votre système requiert actuellement l'utilisation de ce certificat racine particulier. Le secteur tente [d'éliminer les certificats racines de 1 024 bits d'ici la fin de l'année](#).

- Les connexions sécurisées qui dépendent de la signature de notre chaîne de certificat par le certificat racine G2 ne sont pas prises en charge :

Unité organisationnelle	Organisme de certification primaire public de classe 3 – G2
Numéro de série	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Empreinte SHA1 du certificat	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Les connexions sécurisées qui dépendent de la signature de notre chaîne de certificat par le certificat racine G5 sont prises en charge :

Nom courant	Organisme de certification primaire public de classe 3 VeriSign – G5
Numéro de série	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Empreinte SHA1 du certificat	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Suivez les instructions suivantes pour vous assurer que vous effectuez une connexion sécurisée à l'aide d'un certificat racine G5 VeriSign pris en charge :

- Vérifiez votre mémoire de certificats.** Demandez à votre hébergeur Web ou à votre administrateur système de vérifier que le certificat racine G5 VeriSign est présent dans la mémoire de certificats racine qui est utilisée par votre code pour la logique de validation. Si c'est le cas, aucune action n'est requise.
 - Cliquez sur les liens suivants pour voir si votre mémoire de clés contient le certificat racine G5 avec [Java](#), [Linux](#) ou [Windows](#).
- Consultez vos journaux d'erreurs.** Si le certificat racine VeriSign G5 n'a pas été téléchargé pour remplacer le certificat racine G2, des messages d'erreur peuvent s'afficher :
 - Erreur de négociation SSL, "Certificat de source sûre introuvable"
 - Code de résultat -31, "La chaîne de certificat n'a pas été validée : certificat local introuvable"
 - Code de résultat -8, "La connexion SSL a échoué"
 - Erreur -1

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

- Mettez à jour votre logiciel vers la version la plus récente compatible avec SHA-256.
 - Si une mémoire de clés est utilisée pour la validation/l'authentification du certificat, installez le certificat racine VeriSign G5 dans votre mémoire de clés.
- Obtenez un certificat racine VeriSign G5.** Si votre mémoire de certificats ou le client Java ne renferme pas le certificat racine VeriSign G5, demandez à votre administrateur système de le télécharger auprès de VeriSign et de l'enregistrer dans la mémoire de certificats. Demandez-lui également de télécharger tout autre outil d'authentification disponible pour la connexion SSL.
 - Téléchargez le [certificat racine VeriSign G5 de Symantec](#).
 - Téléchargez les [certificats SSL spécifiques](#) à votre serveur si nécessaire.

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

Le problème : SHA-1 est un algorithme cryptographique vieux de 22 ans, qui est menacé par la puissance grandissante des ordinateurs. L'algorithme SHA-256 est plus fort, car il utilise des valeurs de hachage de 256 bits.

Notre réaction : nous allons mettre à jour les certificats SSL pour tous les points de terminaison de production et de test pour remplacer SHA-1 par SHA-256, qui est supérieur, au milieu de 2016.

Ce que vous devez faire

Suivez les instructions suivantes pour passer des certificats SSL utilisant l'algorithme de signature SHA-1 aux certificats utilisant l'algorithme SHA-256, plus robuste :

1. **Vérifiez votre environnement.** Assurez-vous que votre environnement prend en charge les certificats SHA-256.
 - Consultez des ressources en ligne, telles que le guide [DigiCert's SHA-2 Compatibility Guide](#) et la liste [Symantec's Supported Browser and Server List](#), pour obtenir une liste du matériel et des logiciels pris en charge.
 - Si des éléments de votre environnement ne prennent pas en charge SHA-256, vous devez les remplacer ou les mettre à jour avant de mettre les nouveaux certificats en application.
 - Windows 2000 Server et certaines versions de Windows XP peuvent être incompatibles avec le SHA-2. Cet [article du "Windows PKI blog" sur le SHA2 et Windows](#) peut vous aider en proposant des correctifs et des recommandations pour mettre à jour votre environnement.
2. **Vérifiez vos certificats.** Si votre environnement prend en charge SHA-256, assurez-vous que vous avez le certificat racine VeriSign G5 dans votre mémoire de clés.

Vous avez des questions ?



Pour obtenir des informations supplémentaires et consulter les questions-réponses, rendez-vous sur le [microsite sur la modification des certificats SSL 2015-2016](#).

Merci !

Merci de votre compréhension et de l'attention que vous portez à ce problème. Nous savons que ces changements peuvent créer des problèmes de compatibilité, mais nous tenons vraiment à souligner combien cette gêne temporaire nous permettra d'assumer nos engagements de sécurité envers nos utilisateurs communs.