Seguridad para vendedores

Guía de cambios en el Sistema

Haga clic AQUÍ **para obtener información**
sobre el cumplimiento de la norma SHA-256.

Preparación de su integración para el futuro

Las amenazas de seguridad mundiales evolucionan constantemente y la seguridad de nuestros vendedores sigue siendo nuestra máxima prioridad. Para protegerse contra las amenazas tanto actuales como futuras, animamos a nuestros vendedores a que realicen los cambios siguientes en sus integraciones:

1. Dejar de utilizar el certificado raíz G2 de VeriSign
2. Actualizar la integración para que sea compatible con los certificados que usan el algoritmo SHA-256

¿Por qué cambiar?

El sector de las autoridades públicas de certificación (CA) sigue mejorando la seguridad de los certificados SSL. Con vistas al momento en que se pida usar el algoritmo de firma SHA-256 en 2016, ya no se admitirá el certificado raíz G2 de VeriSign, usado tradicionalmente para conectarse a los puntos finales de la API de PayPal y Notificación de pago instantánea (IPN).

¿Cuándo debo actuar?

Recomendamos que tome medidas cuanto antes para prepararse para estos cambios. Para obtener un calendario detallado, incluidas las fechas de cambio para los puntos finales de la API activos y del entorno de pruebas, consulte el micrositio sobre el cambio de certificados SSL entre 2015 y 2016 (en inglés).

NOTE: Es importante tener en cuenta que estos cambios tienen como finalidad solucionar los problemas de seguridad del sector y que no son exclusivos de PayPal. Cuando se hayan aplicado, mejorarán la privacidad y fiabilidad de sus integraciones de PayPal. Como los detalles de estos cambios varían en función del sistema, le recomendamos que se realicen con la ayuda de un administrador del sistema cualificado.

1. Dejar de utilizar el certificado raíz G2 de VeriSign

Problema: en el pasado, VeriSign emitía certificados SSL que tenían una cadena de confianza firmada por un certificado raíz G2 de 1024 bits. En los últimos años, el gobierno y el sector de las CA públicas han cambiado a certificados de 2048 bits más seguros, por lo que ahora VeriSign emite certificados SSL que tienen una cadena de confianza firmada por un certificado raíz G5 de 2048 bits emitido en 2006.

Nuestra respuesta: de acuerdo con los estándares del sector, PayPal dejará de aceptar conexiones seguras a los puntos finales de API/IPN que esperan que nuestro certificado o cadena de confianza esté firmado por el certificado raíz G2. Solo se realizarán correctamente las solicitudes de conexión segura que esperan que nuestro certificado o cadena de confianza esté firmado por el certificado raíz G5.

¿Qué debo hacer ahora?

Deje de utilizar conexiones SSL que dependan de los certificados raíz de VeriSign con un identificador G2, si su sistema actualmente exige el uso de este certificado raíz específico. El sector trabaja activamente para retirar progresivamente los certificados raíz de 1024 bits este año.

- No se admiten las conexiones seguras que se basan en nuestra cadena de certificados firmada por el certificado raíz G2:

Unidad organizativa	Autoridad pública de certificación principal de clase 3 **(G2)**
Número de serie	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Huella digital del certificado SHA1	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Se admiten las conexiones seguras que se basan en nuestra cadena de certificados firmada por el certificado raíz G5:

Nombre común	Autoridad pública de certificación principal de clase 3 de VeriSign **(G5)**
Número de serie	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Huella digital del certificado SHA1	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Siga estas directrices para asegurarse de que se conecta de forma segura mediante un certificado raíz G5 de VeriSign admitido:

1. **Compruebe el almacén de certificados.** Pida al proveedor de alojamiento de su sitio web o al administrador del sistema que compruebe que el certificado raíz G5 de VeriSign esté incluido en el almacén raíz utilizado por su código para la lógica de validación. Si es así, no es necesario hacer nada.
    - Consulte los siguientes vínculos para comprobar si dispone en su almacén de claves del certificado raíz G5 con Java, Linux o Windows.
2. **Compruebe los registros de errores.** Si el certificado raíz G5 de VeriSign no se ha descargado para sustituir al certificado raíz G2, puede ver mensajes de error parecidos a los siguientes:
    - Error de protocolo de enlace SSL: “No trusted certificate found” (No se ha encontrado ningún certificado de confianza)
    - Código de resultado -31: “The certificate chain did not validate, no local certificate found” (La cadena de certificados no se validó; no se ha encontrado ningún certificado local)
    - Código de resultado -8: “SSL connection failed” (Error de conexión SSL)
    - Error -1

    Para resolver estos problemas, realice una de las acciones siguientes:
    - Actualice su software a la versión más reciente que admita SHA-256.
    - Si se utiliza un almacén de claves para la validación/autenticación de certificados, instale el certificado raíz G5 de VeriSign en su almacén de claves.
3. **Obtenga un certificado raíz G5 de VeriSign.** Si el almacén de certificados o el cliente Java no incluyen el certificado raíz G5 de VeriSign, pídale al administrador de su sistema que lo descargue de VeriSign y lo guarde en el almacén de certificados, así como cualquier otro paquete de autenticación de conexiones SSL.
    - Descargar el certificado raíz G5 de VeriSign de Symantec
    - Descargar certificados SSL específicos del servidor (si lo requiere su servidor)

2. Actualizar al algoritmo de firma SHA-256

Problema: SHA-1 es un algoritmo criptográfico de 22 años de antigüedad, cuya eficacia peligra debido al aumento de la potencia informática. SHA-256 utiliza un algoritmo más sólido con valores hash de 256 bits.

Nuestra respuesta: a mediados de 2016, PayPal va a actualizar los certificados SSL en todos los puntos finales activos y del entorno de pruebas de SHA-1 a SHA-256 que es más sólido y robusto.

¿Qué debo hacer ahora?

Siga estas directrices para pasar de usar certificados SSL que utilizan el algoritmo de firma SHA-1 al algoritmo de firma SHA-256 más sólido:

1. **Compruebe el entorno.** Asegúrese de que su entorno admite los certificados SHA-256.
   - Para obtener una lista de hardware y software admitidos, consulte recursos en Internet, como DigiCert's SHA-2 Compatibility Guide (Guía de compatibilidad de SHA-2 de DigiCert) y Symantec's Supported Browser and Server List (Lista de navegadores y servidores admitidos de Symantec).
   - Si hay partes de su entorno que no admiten SHA-256, debe sustituirlas o cambiarlas antes de poder instalar los certificados nuevos.
   - Windows 2000 Server y algunas versiones de Windows XP pueden ser incompatibles con SHA-2. Este blog de PKI de Windows sobre SHA2 y Windows puede ayudarle a cambiar su entorno con parches y recomendaciones.
2. **Compruebe los certificados.** Si su entorno admite SHA-256, asegúrese de tener el certificado raíz G5 de VeriSign en su almacén de claves.

¿Tiene alguna duda?

Para obtener más datos y preguntas frecuentes, consulte el micrositio sobre el cambio de certificados SSL entre 2015 y 2016 (en inglés).

Gracias

Valoramos que preste atención inmediata a este problema y que entienda nuestra postura. Aunque reconocemos que estos pasos necesarios pueden provocar problemas de compatibilidad, no podemos dejar de destacar que este inconveniente a corto plazo se compensará notablemente por nuestra promesa conjunta a nuestros respectivos clientes de que mantendremos la seguridad de sus cuentas y datos financieros.