Segurança do Comerciante

Guia de Atualização do Sistema

Clique AQUI para mais informações sobre conformidade com a norma SHA-256.

Proteja a sua integração a pensar no futuro

As ameaças de segurança globais estão em constante mudança e a segurança dos nossos comerciantes continua a ser a nossa maior prioridade. Para proteção contra ameaças atuais e futuras, recomendamos que os nossos comerciantes façam as seguintes atualizações às suas integrações:

1. Descontinuar a utilização do Certificado de Raiz VeriSign G2
2. Atualizar a integração para suportar certificados que usem o algoritmo SHA-256

Porquê mudar?

A indústria da Autoridade de Certificados (AC) públicos continua a melhorar a segurança dos certificados SSL. Em preparação para a utilização obrigatória do algoritmo de assinatura SHA-256 em 2016, o Certificado de Raiz VeriSign G2, que tem sido tradicionalmente usado na ligação à API do PayPal e endpoints de Notificação de Pagamento Instantâneo (IPN), deixará de ser suportado.

Quando é que será preciso agir?

Recomendamos que aja assim que possível para se preparar para estas alterações. Para obter mais detalhes, incluindo as datas de atualização para os endpoints API Live e Sandbox, consulte o microsite de Alteração de Certificado SSL 2015-2016.

NOTE: É importante sublinhar que estas alterações dizem respeito a questões de segurança da indústria em geral, não sendo exclusivas do PayPal. Depois de implementadas, irão melhorar a privacidade e a fiabilidade das suas integrações PayPal. Uma vez que os detalhes destas alterações variam consoante o sistema, recomendamos que estas sejam feitas com a ajuda de um administrador de sistemas qualificado.

1. Descontinuação da utilização do Certificado de Raiz VeriSign G2

A questão: No passado, a VeriSign emitiu certificados SSL que tinham uma cadeia de fidedignidade assinada pelo Certificado de Raiz G2 de 1024 bits. Nos últimos anos, as autoridades governamentais e a indústria de AC públicos fizeram a evolução para certificados de 2048 bits mais seguros, pelo que a VeriSign emite atualmente certificados SSL que têm uma cadeia de fidedignidade assinada por um Certificado de Raiz G5 de 2048 bits, emitido em 2006.

A nossa resposta: Em conformidade com as normas da indústria, o PayPal deixará de aceitar ligações seguras a endpoints API/IPN que estejam à espera que a nossa cadeia de certificados/fidedignidade seja assinada por um Certificado de Raiz G2. Apenas os pedidos de ligação segura que estejam à espera que a nossa cadeia de certificados/fidedignidade seja assinada pelo Certificado de Raiz G5 resultarão em ligações seguras bem-sucedidas.

O que fazer?

Descontinue a utilização de ligações SSL que se baseiem em Certificados de Raiz VeriSign com um identificador G2, caso o seu sistema solicite de momento a utilização deste Certificado de Raiz em específico. A indústria está a trabalhar ativamente para cessar este ano a utilização de Certificados de Raiz de 1024 bits.

- Não são suportadas ligações seguras que se baseiem na nossa cadeia de certificados assinada pelo Certificado de Raiz G2:

Unidade organizacional	Class 3 Public Primary Certification Authority - **G2**
Número de série	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Fingerprint SHA1 do certificado	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- São suportadas ligações seguras que se baseiem na nossa cadeia de certificados assinada pelo Certificado de Raiz G5:

Nome comum	VeriSign Class 3 Public Primary Certification Authority - **G5**
Número de série	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Fingerprint SHA1 do certificado	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Siga estas orientações para garantir que está a estabelecer ligação segura utilizando um Certificado de Raiz G5 VeriSign suportado:

1. **Verifique o seu arquivo de certificados.** Solicite ao parceiro de hosting onde o seu site se encontra alojado ou ao administrador de sistemas para verificar se o Certificado de Raiz G5 VeriSign está incluído no arquivo de raiz que está a ser usado pelo seu código para lógica de validação. Se assim for, não é necessário fazer mais nada.
    - Consulte as ligações seguintes para verificar o seu arquivo de chaves no que concerne à presença do Certificado de Raiz G5 usando Java, Linux ou Windows.
2. **Verifique os registos de erro.** Se o Certificado de Raiz G5 VeriSign não tiver sido descarregado para substituir o Certificado de Raiz G2, poderão surgir mensagens de erro semelhantes a estas:
    - SSL handshake error, “No trusted certificate found”
    - Result code -31, “The certificate chain did not validate, no local certificate found”
    - Result code -8, “SSL connection failed”
    - -1 error

    Para resolver este tipo de problemas, siga uma das seguintes opções:
    - Atualize o seu software para a versão mais recente com suporte SHA-256.
    - Se o arquivo de chaves for usado para validação/autenticação de certificados, instale o Certificado de Raiz G5 VeriSign no seu arquivo de chaves.
3. **Obtenha um Certificado de Raiz G5 VeriSign.** Se o seu arquivo de certificados ou cliente Java não incluir o Certificado de Raiz G5 VeriSign, peça ao seu administrador de sistemas para o descarregar a partir da VeriSign e guardar no arquivo de certificados, assim como quaisquer outros pacotes de autenticação de ligação SSL.
    - Descarregue o Certificado de Raiz G5 VeriSign da Symantec
    - Descarregue certificados SSL para servidores específicos, se tal for solicitado pelo seu servidor

2. Faça a atualização para o algoritmo de assinatura SHA-256

A questão: O SHA-1 é um algoritmo de encriptação com 22 anos que tem sido ameaçado pelo aumento da capacidade dos sistemas de computação. O SHA-256 usa um algoritmo mais poderoso, com valores hash de 256 bits.

A nossa resposta: Em meados de 2016, o PayPal irá atualizar os certificados SSL em todos os endpoints Live e Sandbox do SHA-1 para o mais poderoso e robusto SHA-256.

O que fazer?

Siga estas orientações para fazer a transição da utilização de certificados SSL que utilizam o algoritmo de assinatura SHA-1 para o reforçado algoritmo de assinatura SHA-256:

1. **Verifique o seu ambiente.** Certifique-se de que o seu ambiente suporta certificados SHA-256.
   - Consulte os recursos online, nomeadamente o Guia de Compatibilidade SHA-2 da DigiCert e a Lista de servidores e browsers suportados da Symantec, para obter indicações sobre o hardware e software suportado.
   - Se houver partes do seu ambiente que não suportam SHA-256, deverá substituir ou atualizar essas partes antes de poder implementar os novos certificados.
   - O Windows Server 2000 e algumas versões do Windows XP podem ser incompatíveis com SHA-2. Poderá obter ajuda neste blogue de Windows PKI sobre SHA-2 e Windows, onde encontrará correções e recomendações para atualizar o seu ambiente.
2. **Verifique os seus certificados.** Se o seu ambiente suportar SHA-256, certifique-se de que tem o Certificado de Raiz G5 VeriSign no seu arquivo de chaves.

Tem alguma dúvida?

Para obter mais informações e respostas às perguntas frequentes, consulte o microsite de Alteração de Certificado SSL 2015-2016.

Obrigado!

Agradecemos a sua atenção imediata para este problema e a sua compreensão pela nossa abordagem. Apesar de reconhecermos que estas medidas necessárias podem causar problemas de compatibilidade, não podemos deixar de realçar que esta inconveniência de curto-prazo é suplantada pela nossa promessa conjunta aos nossos clientes de que manteremos as suas contas e os seus dados financeiros seguros.