Segurança do vendedor

Guia de upgrade do Sistema

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

Garanta uma integração duradoura

As ameaças globais à segurança de sistemas estão sempre mudando, mas a segurança de nossos vendedores continua sendo a nossa principal prioridade. Para protegê-lo contra ameaças atuais e futuras, estamos incentivando nossos vendedores a fazer os seguintes upgrades em suas integrações:

1. Descontinuar o uso do Certificado Raiz G2 da VeriSign
2. Atualizar sua integração para oferecer suporte a certificados que usam o algoritmo SHA-256

Por que mudar?

O setor de Autoridade de Certificação (CA) pública continua a aprimorar a segurança dos certificados SSL. Para deixar nossas integrações preparadas para a utilização do algoritmo de assinatura SHA-256 obrigatório em 2016, o Certificado Raiz G2 da VeriSign, que sempre foi usado para estabelecer a conexão com os endpoints de API e da Notificação Instantânea de Pagamento (NPI) do PayPal, não será mais suportado. Se você não atualizou sua integração para suportar certificados que utilizam o algoritmo SHA-256 em sua integração inicial com o PayPal, recomendamos que você o faça assim possível. O PayPal usa o algoritmo SHA-256 para fazer uma verificação dupla de segurança de sua conexão com nossos servidores e aumentar a segurança do compartilhamento de todos os dados de pagamento.

Quando eu preciso fazer essas alterações?

Recomendamos que você tome as medidas necessárias o mais rápido possível para se preparar para essas alterações. Para conhecer o cronograma detalhado, incluindo as datas de upgrade dos endpoints de API em ambientes de produção e em Sandbox (modo seguro), consulte o 2015-2016 SSL Certificate Change Microsite.

NOTE: É importante observar que essas mudanças estão sendo feitas para solucionar problemas de segurança de todo o setor e não apenas do PayPal. Quando implementadas, elas aumentarão a privacidade e a confiabilidade de suas integrações com PayPal. Como os detalhes dessas alterações variam de acordo com o sistema, recomendamos que sejam feitas com a ajuda de um administrador de sistemas qualificado.

1. Descontinuar o uso do Certificado Raiz G2 da VeriSign

O problema: Anteriormente, a VeriSign emitia certificados SSL que continham uma trust chain assinada por um Certificado Raiz G2 de 1024 bits. Nos últimos anos, o governo e o setor de CA pública passaram a usar certificados de 2048 bits mais seguros. Por isso, agora a VeriSign emite certificados SSL que contêm uma trust chain assinada por um Certificado Raiz G5 de 2048 bits emitido em 2006.

Nossa resposta: Em conformidade com os padrões do setor, o PayPal não aceitará mais conexões seguras para os endpoints de API/NPI que esperam que nosso certificado/trust chain seja assinado pelo Certificado Raiz G2. Apenas solicitações de conexão segura que esperam que nosso certificado/trust chain seja assinado pelo Certificado Raiz G5 resultarão em conexões seguras.

O que você precisa fazer...

Descontinue o uso das conexões SSL que utilizam Certificados Raiz da VeriSign com o identificador G2, caso a integração de seu sistema exija o uso desse Certificado Raiz específico. Todo o setor está trabalhando ativamente para descontinuar os Certificados Raiz de 1024 bits este ano.

- Não há suporte para conexões seguras que dependem de nossa cadeia de certificados assinados pelo **Certificado Raiz G2:**

Unidade organizacional	Autoridade de certificação principal pública de classe 3 - **G2**
Número de série	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Certificado SHA1 com impressão digital	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Há suporte para conexões seguras que dependem de nossa cadeia de certificados assinados pelo **Certificado Raiz G5**:

Nome comum	Autoridade de Certificação principal pública de classe 3 da VeriSign - **G5**
Número de série	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Certificado SHA1 com impressão digital	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Siga estas diretrizes para garantir que você esteja estabelecendo uma conexão segura usando um Certificado Raiz G5 da VeriSign com suporte:

1. **Verifique seu repositório de certificados.** Peça ao seu administrador de sistemas ou ao host do seu site para verificar se o Certificado Raiz G5 da VeriSign está no repositório raiz usado por seu código para validação lógica. Se estiver, nenhuma ação será necessária.
    - Consulte os links abaixo para verificar se o Certificado Raiz G5 usando Java, Linux ou Windows se encontra em seu repositório principal.

2. **Consulte os logs de erro.** Se o Certificado Raiz G5 da VeriSign não tiver sido baixado para substituir o Certificado Raiz G2, você poderá receber mensagens de erro semelhantes a estas:

   - SSL handshake error, “No trusted certificate found” - Erro de handshake do SSL, "Nenhum certificado confiável encontrado"
   - Result code -31, “The certificate chain did not validate, no local certificate found” - Código do resultado -31, "A cadeia de certificados não validou. Nenhum certificado local encontrado"
   - Result code -8, “SSL connection failed” - Código de resultado -8, "Falha na conexão de SSL"
   - -1 error - Erro -1

   Para resolver esses problemas, escolha uma das soluções abaixo:

   - Atualize seu software para a versão mais recente com suporte para SHA-256.
   - Se houver um repositório principal usado para validação/autenticação de certificado, instale o Certificado Raiz G5 da VeriSign no repositório principal.

3. **Obtenha um Certificado Raiz G5 da VeriSign.** Se seu repositório de certificados ou cliente Java não tiver o Certificado Raiz G5 da VeriSign, peça ao seu administrador de sistemas para baixá-lo do site da VeriSign e salvá-lo no repositório de certificados, bem como outros pacotes de autenticação de conexão SSL.

   - Baixe o Certificado Raiz G5 da VeriSign desenvolvido pela Symantec
   - Baixe certificados SSL de servidor específicos, se exigido por seu servidor

2. Atualize o algoritmo para o algoritmo de assinatura SHA-256

O problema: O SHA-1 é um algoritmo de criptografia com 22 anos de idade que está sendo ameaçado pelo desenvolvimento dos sistemas de computação. O SHA-256 usa um algoritmo mais robusto com valores de hash de 256 bits.

Nossa resposta: O PayPal está fazendo o upgrade de certificados SSL em todos os endpoints de ambientes de produção e Sandbox (modo seguro) do SHA-1 para o SHA-256, mais seguro e robusto. Esse upgrade será concluído no meio de 2016.

O que você precisa fazer...

Siga estas diretrizes para migrar dos certificados SSL que utilizam o algoritmo de assinatura SHA-1 para o algoritmo de assinatura SHA-256, mais robusto:

1. **Examine seu ambiente.** Certifique-se de que seu ambiente ofereça suporte para certificados SHA-256.

   - Consulte recursos online, como o Guia de compatibilidade com SHA-2 da DigiCert e a Lista de servidores e navegadores com suporte da Symantec para obter uma lista dos hardwares e softwares suportados.
   - Se partes do seu ambiente não oferecem suporte ao SHA-256, você deve substituir ou fazer upgrade dessas partes antes de implementar os novos certificados.
   - O Windows 2000 Server e algumas versões do Windows XP podem ser incompatíveis com o SHA-2. Este blog de KPI do Windows sobre a compatibilidade entre o SHA-2 e o Windows pode oferecer correções e recomendações para ajudá-lo a fazer o upgrade de seu ambiente.

2. **Verifique seus certificados.** Se seu ambiente oferecer suporte ao SHA-256, certifique-se de que você tenha o Certificado Raiz G5 da VeriSign em seu repositório principal.

Dúvidas?

Para obter detalhes adicionais e ter acesso às perguntas frequentes, consulte o 2015-2016 SSL Certificate Change Microsite.

Obrigado!

Agradecemos sua compreensão e solicitamos que você siga nossas instruções imediatamente. Sabemos que essas medidas, apesar de necessárias, podem ocasionar problemas de compatibilidade. Ainda assim, não podemos deixar de ressaltar que se trata de um problema de curto prazo e que essas medidas estão a serviço de algo muito mais importante: nosso compromisso em manter protegidas as contas e informações financeiras de nossos clientes.