Migração para certificados SHA-2

Perguntas frequentes

Como devo utilizar este documento?

Esse documento fornece respostas para algumas das perguntas mais frequentes feitas pelos nossos clientes sobre nossos planos de transição de certificados SHA-1 para SHA-2. Esse documento ficará hospedado no site http://www.opentext.com/campaigns/sha2.

O que é SHA-2?

SHA-2 é um algoritmo de hash criptográfico publicado pela primeira vez pela Agência de Segurança Nacional dos EUA em 2001. SHA significa algoritmo de hash seguro. As funções de hash SHA são usadas em aplicativos e protocolos de segurança como TLS e SSL e com algoritmos de chave pública para assinaturas digitais e de criptografia.

Por que a OpenText está realizando transição de certificados SHA-1 para SHA-2?

Com os últimos avanços em ataques de criptografia, os especialistas em segurança de rede informaram que usar certificado SHA-1 pode permitir que um invasor falsifique conteúdo, execute ataques de phishing ou ataques a intermediários. Apesar dessa potencial vulnerabilidade não existir com relação ao OpenText™ Trading Grid™, OpenText Information Exchange, OpenText EasyLink GMS ou OpenText EasyLink ICC.Net, estamos mudando para certificados SHA-2 como parte do nosso esforço contínuo de manter os níveis mais altos de integridade e segurança de dados para os nossos clientes.

O hash de criptografia utilizado no SHA-2 é consideravelmente mais forte e não está sujeito às mesmas vulnerabilidades como o SHA-1.

Para saber se os seus sistemas internos são compatíveis com SHA-2, acesse o site https://www.digicert.com/sha-2-compatibility.htm

O que a OpenText está fazendo para realizar a transição para SHA-2?

A OpenText começará a renovação de todos os certificados como SHA-2 assim que o certificado atual vencer. Planejamos concluir a transição de certificados SHA-1 para SHA-2 até **1º de janeiro de 2017**, data que a Microsoft® anunciou que não terá mais compatibilidade com certificados SHA-1. Os certificados SHA-2 serão emitidos pela nossa autoridade certificadora atual, Comodo.

Observação: *Reservamos o direito de atualizar certificados de ambiente de pré-produção antes do vencimento, para permitir que os clientes tenham tempo para realizar testes com seus parceiros comerciais.*

Como isso me afeta?

Se você ou seu parceiro comercial utiliza FTPS, AS2, RosettaNet, OFTP, MQ, AS3 ou outro protocolo para estabelecer uma conexão de troca de mensagem digitalmente assinada ou criptografada com

Trading Grid™, Information Exchange, EasyLink GMS ou EasyLink ICC.Net, a OpenText recomenda que você comece a se preparar para substituir seus certificados SHA-1 por certificados SHA-2 para aprimorar suas proteções de segurança.

O que devo fazer?

Para preparar sua empresa para essa alteração e ajudar a garantir um processo de renovação de certificado adequado:

1. Verifique com o seu provedor de software ou serviços para garantir que seu software de comunicação seja compatível com os certificados SHA-2 emitidos pela Comodo.
    a. Se sim, sua empresa estará pronta para coordenar sua transição para o certificado SHA-2 mais seguro quando seu certificado de chave pública da OpenText expirar.
    b. Do contrário, e se o seu provedor de software de comunicação não puder ajudar, entre em contato com o seu Gerente de Cliente da OpenText para conversar sobre quais opções estão disponíveis para você.
2. Entre em contato com os seus parceiros comerciais e peça que façam a mesma verificação com os respectivos provedores de software comunicação para garantir que o respectivo software de comunicação de cada parceiro seja compatível com os certificados SHA-2 emitidos pela Comodo, nossa autoridade certificadora atual.

Haverá alguma alteração no processo de renovação de certificado?

Não haverá alterações nos processos de renovação de certificado. Entretanto, a OpenText pode renovar os certificados para SHA-2 antes da data de vencimento para garantir conformidade antes do prazo final de 1º de janeiro de 2017.

O que ocorre se o meu certificado de chave pública atual da OpenText expirar antes de 31 de dezembro de 2016?

A OpenText entrará em contato de maneira proativa com os clientes que tenham certificados SHA-1 de chave pública da OpenText para ajudar na transição para certificados SHA-2 antes do prazo final de 1º de janeiro de 2017.

Quais serviços são afetados por essa alteração?

Essa alteração afeta todos os certificados SSL de navegador e alguns protocolos de comunicação. Se a sua conexão à OpenText for realizada usando um navegador moderno, você não será afetado pela atualização do certificado.

Observação: *isso não afeta atualmente chaves de criptografia SSH, PGP ou GPG.*

Quais protocolos são afetados por essa alteração?

Os seguintes protocolos são afetados pela transição para certificados SHA-2:

- AS2
- AS3
- HTTPs
- SSL-FTP (FTPs)
- RosettaNet
- MQ
- Sterling/IBM – Connect:Direct Secure Plus

Com quais funções de hash SHA-2 os sistemas da OpenText são compatíveis atualmente?

Os sistemas da OpenText atualmente são compatíveis com certificados assinados pelas seguintes versões de SHA-2:

- SHA256
- SHA384
- SHA512

Futuramente, a OpenText planeja que seus sistemas sejam compatíveis com outros tipos de certificados SHA-2. Detalhes adicionais serão comunicados assim que forem disponibilizados.

Meu software de comunicação não é compatível com certificados SHA-2. O que devo fazer?

Embora a OpenText recomende realizar a transição para certificados SHA-2 como a maneira mais eficaz para ajudar a manter a integridade e a segurança dos dados, entendemos que nem todos os sistemas dos clientes podem ser compatíveis com certificados SHA-2.

Se o seu software não for compatível com certificados SHA-2 ou certificados autoassinados, a Equipe de Troca de Certificados trabalhará com a sua empresa para encontrar uma alternativa por até um ano. Depois de 31 de dezembro de 2015, a OpenText deixará de oferecer outras opções de emissão de certificados. A partir de 2016, a Equipe de Troca de Certificados desabilitará todas as opções de emissão de certificados SHA-1, fazendo com que seja necessário que os clientes mudem para um certificado autoassinado ou SHA-2. Se os sistemas da sua empresa ainda não forem compatíveis com certificados SHA-2 quando chegar a hora, a Equipe de Troca de Certificados trabalhará com você para implementar um certificado SHA-1 autoassinado.

Equipe de Troca de Certificados

Email: CertificateExchange@opentext.com
Telefone: 1-800-334-2255 ramal 2378 (CERT)

O que é Comodo?

Comodo é a principal autoridade certificadora da OpenText. Autoridade certificadoras são organizações que emitem e gerenciam certificados digitais. Para obter informações adicionais, acesse o site da Comodo em www.comodo.com.

Por que a OpenText mudou para a Comodo?

A OpenText escolheu a Comodo porque a empresa oferece uma gama completa de certificados digitais com a criptografia mais forte disponível, além da flexibilidade e capacidade técnica para atender as necessidades empresariais. Como uma Autoridade Certificadora WebTrust (CA), a Comodo atende as mais elevadas normas de confidencialidade, confiabilidade de sistema e práticas empresariais pertinentes por meio de auditorias independentes qualificadas.

A mudança para a Comodo pode afetar os meus serviços?

Mudar para um certificado emitido pela Comodo praticamente não deve afetar produtos mais recentes de troca de arquivo. Como a Comodo é uma autoridade certificadora relativamente nova, os clientes com produtos de troca de arquivo mais antigos (com mais de 10 anos) podem ter alguns problemas ao carregar os certificados intermediários e raiz em seus respectivos repositórios de certificados. Para obter informações adicionais, acesse o site da Comodo em www.comodo.com.

***Observação**: Clientes com produtos de troca de arquivo mais antigos ou softwares desenvolvidos internamente devem carregar todos os certificados de cadeia (.p7b). Se você usar as versões .cer, todos os três certificados Comodo precisam ser carregados no seu repositório de certificados.*

Com quem devo falar para obter informações adicionais?

Para obter informações adicionais, os clientes OpenText Trading Grid ou Information Exchange podem entrar em contato com os Serviços de assistência de nuvem.

Clientes OpenText EasyLink GMS e ICC.Net podem entrar em contato com o Atendimento ao cliente OpenText EasyLink.

Apenas para usuários Sterling Connect:Direct

Como posso saber se a versão do meu software Sterling Connect:Direct é compatível com SHA-2?

Para obter informações adicionais sobre a compatibilidade do Sterling Connect:Direct com SHA-2, consulte o manual de assistência de SHA-2 no site da IBM. O manual está disponível através do link abaixo:

ftp://ftp.software.ibm.com/software/commerce/doc/mft/cdcommon/secplus_SHA2SupportForCD_Book.pdf

Consulte a ***Tabela 2***. ***Software compatível com SHA-2*** para ver se a sua versão do Connect:Direct é compatível com SHA-2. Se a sua versão não for compatível com SHA-2, existem diversas opções disponíveis. São elas:

1. Atualizar o seu software Connect:Direct para uma versão compatível com SHA-2.
2. Entrar em contato com seu representante OpenText para instalar/configurar outro protocolo para transmissão de dados.

Observação: Se apenas estiver enviando arquivos **recebidos** pela OpenText, é bem provável que seu sistema não seja afetado. Entretanto, a menos que o seu sistema seja compatível com certificados SHA-2, a OpenText não poderá lhe enviar arquivos de dados.

Quais são os pré-requisitos padrão para realizar conexão com a OpenText usando Connect:Direct?

Os pré-requisitos padrão incluem:

- A OpenText apenas instala / adiciona certificados de Autoridades Certificadoras Raiz (AC raiz) e/ou Intermediários do cliente em nosso repositório confiável
- Os certificados enviados para a OpenText não devem ser autoassinados. A OpenText não aceitará um certificado autoassinado
- A autenticação do cliente deve estar desativada
- A OpenText prefere que os certificados estejam em formato codificado em Base64
- Todos os pacotes de codificação devem ser adicionados à configuração Secure+
- A OpenText está configurada para TLS

Quais certificados eu precisarei instalar no meu sistema Connect:Direct para habilitar uma conexão com a OpenText?

Os clientes precisarão instalar os seguintes novos certificados como arquivos separados:

- Certificado público (deve conter os certificados na cadeia)
- Certificado intermediário (deve conter a cadeia apenas com a Autoridade Certificadora Raiz)
- Certificado da Autoridade Certificadora Raiz

O que devo fazer com os novos certificados?

Os clientes devem instalar/adicionar os certificados aplicáveis na respectiva configuração Secure+ para o nó do Connect:Direct da OpenText ou discutir com o respectivo contato técnico interno e/ou Suporte da IBM.

Devo remover os certificados anteriores?

O requisito de remoção dos certificados anteriores depende de cada configuração do Secure+ do Connect:Direct. Converse com o respectivo contato técnico interno e/ou Suporte da IBM.

Existem alguma outra configuração do Secure+ exigida para alcançar compatibilidade com certificados SHA-2?

Não. Entretanto, os clientes podem fazer as seguintes alterações, a seu critério.

- Adicionar todos os pacotes de codificação à respectiva configuração do Secure+
- Remover pacotes de codificação fracos ou comprometidos

Preciso testar a utilização do certificado SHA-2?

A OpenText recomenda que os clientes testem os novos certificados para garantir que funcionem conforme o esperado. Se houver algum problema, os clientes devem abrir uma solicitação de serviço do produto junto aos Serviços de assistência de nuvem.

O que ocorre se o meu certificado expirar?

Um certificado expirado normalmente significa que o certificado público expirou, mas não o certificado de AC raiz ou Intermediário. Em muitos casos, não é necessário fazer nada com os certificados atuais, porque o certificado de AC raiz e/ou Intermediário não foi alterado. Se o certificado de AC raiz e/ou Intermediário for novo, adicione ao repositório confiável.

About OpenText

OpenText enables the digital world by simplifying, transforming, and accelerating enterprise information needs, on premises or in the cloud. For more information about OpenText Cloud Services (NASDAQ: OTEX, TSX: OTC) visit www.gxs.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn | Facebook

www.gxs.com/support | www.easylink.com/support

NORTH AMERICA +800 334 2255 • UNITED STATES +1 301 251 65100

OTHER LOCATIONS http://techsupport.gxs.com/regional-directories