OPENTEXT™

SHA-2 인증서로 마이그레이션

자주 묻는 질문

이 문서의 용도는 무엇입니까?

이 FAQ 에서는 SHA-1 에서 SHA-2 인증서로의 전환 계획과 관련하여 고객이 자주 묻는 질문들에 대한 답변을 제공합니다. 본 문서는 http://www.opentext.com/campaigns/sha2 에서 확인하실 수 있습니다.

SHA-2 란 무엇입니까?

SHA-2 는 암호 해시 알고리즘으로 2001 년 미국 국가안보국에 의해 처음 발표되었습니다. SHA 는 보안 해시 알고리즘을 의미합니다. SHA 해시 기능은 암호화 및 디지털 서명 모두에 대한 공개 키 알고리즘과 함께 TLS 및 SSL 와 같은 보안 애플리케이션 및 프로토콜에서 사용됩니다.

OpenText 가 인증서를 SHA-1 에서 SHA-2 로 전환하는 이유는 무엇입니까?

네트워크 보안 전문가들은 암호화 공격이 나날이 발전하면서 SHA-1 인증서 사용으로 인해 공격자가 컨텐츠를 도용하고 피싱 공격 또는 "중간자" 공격을 수행할 수도 있다고 경고했습니다. 이러한 잠재적인 취약성이 OpenText™ Trading Grid™, OpenText Information Exchange, OpenText EasyLink GMS 또는 OpenText EasyLink ICC.Net 에 존재하지는 않지만 당사는 데이터 무결성 및 고객 보안에 있어 최고 수준을 유지하려는 노력의 일환으로 인증서를 SHA-2 로 전환하고 있습니다.

SHA-2 에서 사용되는 암호화 해시는 매우 강력하며 SHA-1 에서와 같은 취약성에 영향을 받지 않습니다.

내부 시스템이 SHA-2 를 지원하는지 알아보려면 https://www.digicert.com/sha-2-compatibility.htm 을 참고하십시오.

OpenText 의 SHA-2 전환 대책은 무엇입니까?

OpenText 는 현재 인증서가 만료되면 모든 인증서를 SHA-2 로 갱신할 것입니다. Microsoft®가 발표한 SHA-1 인증서 지원 중단 날짜인 **2017 년 1 월 1 일**까지 SHA-1 에서 SHA-2 인증서로 전환을 완료할 것입니다. SHA-2 인증서는 당사의 현재 인증서 기관인 Comodo 에 의해 발급됩니다.

참고: *당사는 사전 제작 환경 인증서가 만료되기 전에 업그레이드하여 고객이 거래 파트너와 테스트할 수 있는 시간을 허용할 권리가 있습니다.*

사용자에게 미치는 영향은 무엇입니까?

사용자 또는 사용자의 거래 파트너가 FTPS, AS2, RosettaNet, OFTP, MQ, AS3 또는 다른 프로토콜을 사용하여 Trading Grid™, Information Exchange, EasyLink GMS 또는 EasyLink ICC.Net 과 디지털 서명되거나 암호화된 메시지 교환 연결을 설정한 경우 OpenText 는 보안 강화를 위해 SHA-1 인증서를 SHA-2 인증서로 교체할 것을 권장합니다.

사용자가 해야 할 일은 무엇입니까?

인증서 변경을 준비하고 원활한 인증서 갱신 절차를 수행하려면:

1. 서비스 또는 소프트웨어 제공 업체를 확인하여 통신 소프트웨어가 Comodo 에 의해 발급된 SHA-2 인증서를 지원하는지 확인합니다.
    a. 지원하는 경우 현재 OpenText 공개 키 인증서가 만료되면 보다 보안이 강력한 SHA-2 인증서로 전환할 수 있습니다.
    b. 지원하지 않는 경우 현재 통신 소프트웨어 제공 업체는 사용자를 지원할 수 없습니다. OpenText 고객 관리자에게 연락하여 사용 가능한 옵션에 대해 문의하십시오.
2. 거래 파트너에게 연락하여 통신 소프트웨어 제공 업체와 함께 동일한 확인 절차를 수행하여 통신 소프트웨어가 당사의 현재 인증서 기관인 Comodo 에 의해 발급된 SHA-2 인증서를 지원하는지 확인하십시오.

인증서 갱신 절차가 변경됩니까?

인증서 갱신 절차는 변경되지 않습니다. 그러나 OpenText 는 2017 년 1 월 1 일 이전에 절차를 완료하기 위해 만료 날짜에 앞서 SHA-2 로 인증서를 갱신할 수도 있습니다.

현재 OpenText 공개 키 인증서가 2016 년 12 월 31 일 이후에 만료되는 경우 어떻게 됩니까?

OpenText 는 현재 OpenText 공개 키 SHA-1 인증서에 대해 사전에 고객에게 연락하여 마감 기한인 2017 년 1 월 1 일 전에 SHA-2 인증서로 전환할 수 있도록 지원할 것입니다.

인증서 변경으로 인해 영향 받는 서비스는 무엇입니까?

모든 SSL 브라우저 인증서 및 특정 통신 프로토콜이 영향을 받게 됩니다. 최신 웹 브라우저를 사용하여 OpenText 에 연결하는 경우 인증서 업그레이드로 인한 영향을 받지 않습니다.

참고: *현재 SSH, PGP 또는 GPG 암호화 키에는 영향을 미치지 않습니다.*

인증서 변경으로 인해 영향 받는 프로토콜은 무엇입니까?

다음은 SHA-2 인증서 변경으로 인해 영향 받는 프로토콜입니다.

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

현재 OpenText 가 지원하는 SHA-2 해시 기능은 무엇입니까?

OpenText 는 현재 다음 SHA-2 버전에 의해 서명된 인증서를 지원합니다.

- SHA256
- SHA384
- SHA512

나아가 OpenText 는 추가 SHA-2 인증서 유형도 지원할 계획입니다. 자세한 사항은 지원이 확정되면 알려드릴 것입니다.

내 통신 소프트웨어가 SHA-2 인증서를 지원하지 않습니다. 어떻게 해야 합니까?

OpenText 는 데이터 무결성 및 보안 유지를 위한 가장 효과적인 방법으로 SHA-2 인증서로의 전환을 권장하지만 모든 고객이 SHA-2 인증서를 지원할 수 있는 것이 아니라는 것을 알고 있습니다.

사용자의 소프트웨어가 SHA-2 또는 자체 서명된 인증서를 지원하지 않는 경우 인증서 변경 팀이 최대 1 년까지 대체 인증서를 제공할 것입니다. 2015 년 12 월 31 일 이후 OpenText 는 더 이상 대체 인증서 발급 옵션을 제공하지 않을 것입니다. 2016 년부터 인증서 변경 팀은 모든 SHA-1 인증서 발급 옵션을 비활성화하고 고객에게 SHA-2 또는 자체 서명된 인증서로 변경하도록 요청할 것입니다. 그때까지 SHA-2 인증서를 지원할 수 없는 경우 인증서 지원 팀은 자체 서명된 SHA-1 인증서 사용을 지원할 것입니다.

인증서 변경 팀

이메일: CertificateExchange@opentext.com
전화번호: 1-800-334-2255 x2378(CERT)

Comodo 란 무엇입니까?

Comodo 는 OpenText 의 주 인증서 기관입니다. 인증서 기관은 디지털 인증서를 발급하고 관리하는 조직입니다. 보다 자세한 정보는 Comodo 웹사이트 www.comodo.com 을 참조하십시오.

OpenText 가 Comodo 를 선택한 이유는 무엇입니까?

OpenText 는 Comodo 를 선택한 이유는 가장 강력한 암호화를 구현하는 다양한 디지털 인증서 및 기업의 요구사항을 충족하는 기술 능력과 유연성을 제공하기 때문입니다. WebTrust 인증서 기관(CA)으로서 Comodo 는 자격을 갖춘 독립 감사를 통해 최고 수준의 기밀성, 시스템 신뢰도 및 적합한 비즈니스 관행을 인정받고 있습니다.

Comodo 로의 변경이 내 서비스에 영향을 미칩니까?

인증서 발급 기관이 Comodo 로 변경된 것은 최신 파일 변경 제품에 거의 영향을 미치지 않습니다. Comodo 는 비교적 새로운 인증 기관이므로 이전 파일 변경 제품(10 년 이상)을 가지고 있는 고객의 경우

루트 및 중간 인증서를 인증서 저장소로 로드하는 중 문제가 발생할 수도 있습니다. 보다 자세한 정보는 Comodo 웹사이트 www.comodo.com 을 참조하십시오.

***참고**: 이전 파일 변경 제품 또는 자체 개발한 소프트웨어를 가지고 있는 고객은 연결된 모든 인증서를 로드해야 합니다(.p7b). .cer 버전을 사용하는 경우 세 개의 모든 Comodo 인증서가 인증서 저장소에 로드되었는지 확인하십시오.*

더 자세한 정보를 알고 싶으면 어떻게 해야 합니까?

OpenText Trading Grid/Information Exchange 고객은 클라우드 지원 서비스에 문의하여 더 자세한 정보를 알아볼 수 있습니다.

OpenText EasyLink GMS 및 ICC.Net 고객은 OpenText EasyLink 고객 지원에 문의하십시오.

Sterling Connect:Direct 사용자의 경우만

내 Sterling Connect:Direct 버전이 SHA-2 를 지원하는지 어떻게 알 수 있습니까?

Sterling Connect:Direct 의 SHA-2 지원에 대한 자세한 정보는 IBM 웹사이트의 SHA-2 지원 가이드를 참조하십시오. 아래 링크를 방문하여 가이드에 액세스할 수 있습니다.

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

사용자의 Connect:Direct 버전이 SHA-2 를 지원하는지 알아보려면 ***표 2. SHA-2 호환 소프트웨어***를 참조하십시오. SHA-2 와 호환되지 않는 버전을 사용 중인 경우 여러 옵션을 설정할 수 있습니다. 설정 가능한 옵션:

1. Connect:Direct 소프트웨어를 SHA-2 를 지원하는 버전으로 업그레이드합니다.
2. OpenText 담당자에게 문의하여 데이터 전송을 위한 다른 프로토콜을 설치/구성합니다.

참고: OpenText 를 통해 **인바운드** 파일만 전송하는 경우 문제가 발생하지 않을 수 있습니다. 그러나 시스템이 SHA-2 인증서를 지원하지 않으면 어떤 데이터 파일도 OpenText 를 통해 사용자에게 전송되지 않습니다.

Connect:Direct 를 사용하여 OpenText 에 연결하기 위한 기본 전제 조건은 무엇입니까?

기본 전제 조건:

- OpenText 는 고객 루트 인증 기관 및/또는 중간 인증서를 신뢰하는 저장소에 설치/추가만 할 수 있습니다.
- OpenText 로 전송된 인증서는 자체 서명할 수 없습니다. OpenText 는 자체 서명된 인증서를 수락하지 않습니다.
- 클라이언트 인증서는 비활성화되어야 합니다.
- OpenText 는 Base64 형식으로 인코딩된 인증서를 권장합니다.
- 모든 암호 그룹이 Secure+ 설정에 추가되어야 합니다.
- OpenText 는 TLSv1 용으로 구성됩니다.

OpenText 와 연결하기 위해 내 Connect:Direct 시스템에 설치해야 하는 인증서는 무엇입니까?

고객은 다음 새 인증서를 개별 파일로 설치해야 합니다.

- 공용 인증서(체인에 인증서가 포함되는 경우)
- 중간 인증서(루트 CA 만을 통해 체인이 포함되는 경우)
- 루트 CA 인증서

새 인증서를 어떻게 해야 합니까?

고객은 해당 인증서를 OpenText 의 Connect:Direct 노드용 Secure+ 설정에 설치/추가하거나 내부 기술 담당자 및/또는 IBM 지원 서비스에 문의해야 합니다.

이전 인증서는 제거합니까?

특정 Connect:Direct Secure+ 설정의 경우 이전 인증서를 제거해야 합니다. 보다 자세한 사항은 내부 기술 담당자 및/또는 IBM 지원 서비스에 문의하십시오.

SHA-2 인증서 지원하기 위해 기타 Secure+ 설정이 필요합니까?

아니요. 그러나 고객은 옵션에서 다음 사항을 변경할 수 있습니다.

- 모든 암호화 그룹을 Secure+ 설정에 추가
- 취약하거나 해독된 암호 그룹 제거

SHA-2 인증서를 사용하여 테스트해야 합니까?

OpenText 는 고객이 새 인증서를 테스트하여 제대로 작동하는지 확인할 것을 권장합니다. 문제가 발생할 경우 고객은 클라우드 지원 서비스에서 제품 서비스를 요청해야 합니다.

내 인증서가 만료되면 어떻게 합니까?

일반적으로 만료된 인증서의 경우 공용 인증서는 만료되었지만 중간 또는 루트 CA 는 만료되지 않습니다. 대부분의 경우 중간 및/또는 루트 CA 가 변경되지 않았기 때문에 실제 인증서를 그냥 두면 됩니다. 중간 및/또는 루트 CA 가 새로운 인증서인 경우 신뢰하는 저장소에 추가하십시오.

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

Copyright ©2013-2014 Open Text Corporation
OpenText is a trademark or registered trademark of Open Text SA and/or Open Text ULC. The list of trademarks is not exhaustive of other trademarks, registered trademarks, product names, company names, brands and service names mentioned herein are property of Open Text SA or other respective owners. All rights reserved. For more information, visit: http://www.opentext.com/2/global/site-copyright.html SKU#