OPENTEXT™

SHA-2 证书迁移事宜

常见问题解答

如何使用本文档？

此“常见问题解答”针对我们的 SHA-1 向 SHA-2 证书转换计划回答了客户最关心的问题。此文档位于 http://www.opentext.com/campaigns/sha2。

什么是 SHA-2？

SHA-2 是一种加密散列算法，最初于 2001 年由美国国家安全局发布。SHA 是英文 Secure Hash Algorithm（安全散列算法）的缩写。SHA 散列函数应用于在安全应用程序和协议中（如 TLS 和 SSL），并结合公共密钥算法用于数据加密和数字签名。

OpenText™ 为何将 SHA-1 转换成 SHA-2 证书？

近期密码攻击活动日益猖獗，网络安全专家为此发出了警告：使用 SHA-1 证书可能方便攻击者实施内容欺骗、钓鱼攻击或“中间人”攻击等。虽然这一潜在漏洞与 OpenText™ Trading Grid™、OpenText Information Exchange, OpenText EasyLink GMS 或 OpenText EasyLink ICC.Net 无关，我们还是决定迁移到 SHA-2 证书，努力确保最高级别的数据完整性和客户安全性。

相比 SHA-1，SHA-2 中所用的加密散列功能更强且不会产生类似的漏洞。

要了解自己的内部系统是否支持 SHA-2，请访问 http://www.digicert.com/sha-2-compatibility.htm

OpenText 正在采取哪些措施来实施 SHA-2 迁移？

OpenText 将在当前证书过期时将所有证书更新为 SHA-2。我们计划在 **2017 年 1 月 1 日**之前将 SHA-1 证书全部转换成 SHA-2 证书，此日期也是 Microsoft 宣布停止对 SHA-1 证书提供支持的日期。SHA-2 证书将由当前证书颁发机构 Comodo 发布。

注意：*我们保留在预生产环境证书过期前对其升级的权利，这样可为客户留出与贸易合作伙伴进行测试的时间。*

迁移对我有何影响？

如果您或您的贸易合作伙伴仍在使用 FTPS、AS2、RosettaNet、OFTP、MQ、AS3 或其他协议与 Trading Grid™、Information Exchange, EasyLink GMS 或 EasyLink ICC.Net 建立数字签名或加密的消息交换连接，OpenText 强烈建议您做好准备，将 SHA-1 证书替换为 SHA-2 证书，提高自己的安全保护级别。

我需要做什么？

为应对这一变化并确保证书顺利更新，请采取以下措施：

1. 咨询您的服务或软件提供商，确保所用的通信软件支持由 Comodo 颁发的 SHA-2 证书。

   a. 如果支持，您就可以在当前的 OpenText 公钥证书到期时与我们协商转换成安全性更高的 SHA-2 证书。
   b. 如果不支持，且当前的通信软件提供商无法为您提供支持，请联系 OpenText 客户经理商讨后续的措施。
2. 联系您的贸易合作伙伴，请他们与自己的通信软件提供商进行相同的验证，确保所用的通信软件支持由我们当前的证书颁发机构 Comodo 颁发的 SHA-2 证书。

证书更新流程是否有变化？

证书更新流程没有任何变化。不过，OpenText 可能会在证书到期之前即更新为 SHA-2 以确保 2017 年 1 月 1 日截止时间之前的合规性。

如果我当前的 OpenText 公钥证书在 2016 年 12 月 31 日之后到期该怎么办？

OpenText 会主动联系当前 OpenText 公钥 SHA-1 证书的用户，帮助他们在 2017 年 1 月 1 日截止时间之前转换成 SHA-2 证书。

此次调整会影响哪些服务？

此次调整会影响到所有 SSL 浏览器证书以及部分通信协议。如果您使用新版的 Web 浏览器连接到 OpenText，就不会受证书升级影响。

注意：*此次调整目前不会影响 SSH、PGP 或 GPG 加密密钥。*

此次调整会影响哪些协议？

以下协议会受到 SHA-2 证书转换的影响：

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

OpenText 目前支持哪些 SHA-2 散列函数？

OpenText 目前支持由以下 SHA-2 版本签名的证书：

- SHA256
- SHA384
- SHA512

OpenText 计划未来支持更多其他类型的 SHA-2 证书。我们会适时通报更多详情。

我的通信软件无法支持 SHA-2 证书。该怎么办？

尽管 OpenText 建议转换成 SHA-2 证书是保持数据完整性和安全性的最有效方式，但是我们也知道，并非所有客户都支持 SHA-2 证书。

如果您的软件不支持 SHA-2 或自签名证书，证书交换团队将与您合作提供最长一年的备用方案。2015 年 12 月 31 日之后，OpenText 将不再提供任何证书颁发备用方案。自 2016 年起，证书交换团队将禁用所有 SHA-1 证书颁发选项，从而让客户迁移到 SHA-2 或自签名证书。如果届时您仍无法支持 SHA-2 证书，证书交换团队将与您合作采用自签名的 SHA-1 证书。

证书交换团队

电子邮件：CertificateExchange@opentext.com
联系电话：1-800-334-2255x2378 (CERT)

什么是 Comodo？

Comodo 是 OpenText 的主要证书颁发机构。证书颁发机构是颁发和管理数字证书的组织。欲了解更多信息，请访问 Comodo 的网站：www.comodo.com。

OpenText 为何选择 Comodo？

OpenText 选择 Comodo 是因为后者可提供全套当前加密性能最强的数字证书，其技术能力和应用灵活性可满足企业的各种需求。作为一家 WebTrust 证书颁发机构 (CA)，Comodo 通过严格独立的资格审计，达到了最高标准的保密性、系统可靠性和相关业务实践要求。

转换成 Comodo 对我的服务有何影响？

转换成 Comodo 颁发的证书对新版文件交换产品影响不大。由于 Comodo 是一家新兴的证书颁发机构，使用旧版文件交换产品（10 年以上）的客户可能会在根证书和中间证书加载到证书存储区时遇到问题。欲了解更多信息，请访问 Comodo 的网站：www.comodo.com。

注意：*拥有旧版文件交换产品或自主软件的客户应加载所有链式证书（.p7b）。如果使用的是 .cer 版本，请确保所有三个 Comodo 证书都加载到了证书存储区。*

如果需要更多信息，应与谁联系？

有关更多信息，OpenText Trading Grid/Information Exchange 的客户可以联系云支持服务部门。

OpenText EasyLink GMS 和 ICC.Net 的客户可以联系 OpenText EasyLink 客户支持部门。

仅针对 Sterling Connect:Direct 用户

如何了解自己的 Sterling Connect:Direct 软件版本是否兼容 SHA-2？

欲了解更多 Sterling Connect:Direct 的 SHA-2 支持信息，请参阅 IBM 网站上的 SHA-2 支持指南。您可以访问以下链接来查看指南：

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

请参阅《***表 2.SHA-2 兼容软件***》，了解您的 Connect:Direct 版本是否支持 SHA-2。如果发现自己的版本不兼容 SHA-2，您可以采取多种措施，其中包括：

1. 将自己的 Connect:Direct 软件升级到支持 SHA-2 的版本。
2. 联系 OpenText 代表安装/配置其他数据传输协议。

注意：如果只通过 OpenText 发送**入站**文件，那么可能不会遇到任何问题。然而，如果您的系统不支持 SHA-2 证书，OpenText 将无法向您发送任何数据文件。

使用 Connect:Direct 连接到 OpenText 时有何标准的前提条件？

标准的前提条件包括：

- OpenText 仅将客户的根证书颁发机构和/或中间证书安装/添加到我们的受信任存储区。
- 发送到 OpenText 的证书不得是自签名的。OpenText 不接受自签名证书
- 应关闭客户端身份验证
- OpenText 更希望证书采用 Base64 编码格式
- 应将所有密码套件添加到 Secure+ 设置中
- OpenText 仅配置用于 TLSv1

需要在 Connect:Direct 系统中安装什么证书才能与 OpenText 建立连接？

客户需要以独立文件形式安装以下新证书：

- 公用证书（应包含链中的证书）
- 中间证书（应只包含根 CA 的链）
- 根 CA 证书

对新证书应如何处理？

客户应将证书相应地安装/添加到 OpenText Connect:Direct 节点的 Secure+ 设置中或咨询内部技术联系人和/或 IBM 技术支持部门。

是否要删除以前的证书？

是否需要删除以前的证书要取决于具体的 Connect:Direct Secure+ 设置。请咨询内部技术联系人和/或 IBM 技术支持部门。

是否需要任何其他的 Secure+ 设置来支持 SHA-2 证书？

否。但客户可以根据自己情况选择进行以下更改。

- 将所有密码套件添加到 Secure+ 设置中
- 删除强度弱或已被破解的密码套件

是否需要使用 SHA-2 证书进行测试？

OpenText 建议客户对新证书进行测试以确保证书正常工作。如遇任何问题，客户应向云支持服务部门提交产品服务请求。

我的证书过期了该怎么办？

证书过期通常意味着公用证书过期，但中间 CA 或根 CA 并没有过期。在许多情况下，您无需对实际证书进行任何操作，因为中间 CA 和/或根 CA 并没有改变。如果中间 CA 和/或根 CA 是新的，请将其添加到受信任的存储区。

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