切换 TLS（SSL）提供商

揭开程序的神秘面纱并设定期望值

目录

介绍

将 TLS 证书切换到新的证书颁发机构听起来像是一项艰巨的任务，但其实并没有想象中那么复杂。成功的关键在于对当前环境有充分的了解，并与利益相关者就所涉及的资源和成本设定预期。本白皮书介绍了切换到新 CA 的整个过程，从调查当前环境的初始步骤到确定需要完成的工作和估算成本。

我们还提供了有关监控、报告和管理证书财产以应对潜在迁移的建议。同样的建议也应被视为最佳实践标准，以确保您的所有证书都是安全、有效和正确配置的。

步骤 1 – 调查您所拥有的一切

在考虑更换 TLS 服务提供商时，第一步是调查环境中现有的 TLS 使用情况。您需要了解当前的情况，以便做出决策，并对转换所需的成本和时间设定合理的预期。

准备证书迁移的第一步需要识别所有已签发的证书。这通常可以通过从当前 CA 导出所有证书的记录来实现。该记录提供了以前购买证书的完整清单，使您可以创建一份核对表，避免在迁移过程中依赖旧账户。有些企业可能会使用多个 CA，这通常是由于合并、收购或不同部门从不同供应商处购买证书造成的。如果您的企业使用多个 CA，请对每个 CA 重复导出过程，以确保所有证书都有记录。

虽然这些导出的列表可以很好地充当核对表，并告诉我们已经签发了哪些证书，但它们并不能告诉我们证书安装在哪里或如何使用。大型企业的环境中通常有许多有效的 TLS 证书。如果在过渡期间没有找到所有证书，它们可能会过期，导致覆盖范围失效、中断和合规性问题。

幸运的是，您可以利用 Atlas Discovery 等证书发现工具来索引您的网络并找到所有现有证书，无论其签发者是谁。这样，在迁移到新 CA 时，就有了一份完整的清单可供参考。证书发现还提供了识别不合规证书的机会，如使用弱密钥或自签名证书的证书，这些都可以在迁移过程中进行补救。

确定管理员

确定管理新账户的团队成员，并为他们提供有关新平台的培训。将培训时间纳入过渡时间表。理想情况下，负责人员必须具备适当水平的 TLS 证书知识，以及使用、管理证书的基本原因和服务证书过期/遗失的潜在风险。

确定服务和应用程序

使用证书发现结果，评估已安装证书的服务器和应用程序的数量和类型，以确定迁移阶段需要做哪些工作。例如，根据服务器的类型，可能需要手动更新根证书和中间证书。此外，谨慎的做法是，不要简单地依赖现有证书作为基准，还要将此报告与已知服务进行比较，以确保没有需要考虑的不安全服务器或应用程序。

步骤 2 - 确定需要做什么

了解您的工作情况后，请评估切换背后的后勤工作。由于对流程时间和复杂性的误解，企业往往不愿意从现有的 CA 进行转换。但是，当您确定了所需的确切范围和可用的工具后，您可能会发现过程非常简单。

学习新的 CA 平台

您需要将培训时间纳入迁移时间表，包括考虑用户数量及其角色和职责。与严格负责下订单的用户相比，账户管理员可能需要更多的培训。

决定更新战略

在更换 TLS 提供商之前，你应该制定一个处理证书更新的攻击计划。在选择新的 CA 时，应询问其证书更换政策。它们应能满足以下两种方法的要求。

- **过渡模式**
  一种方法是逐个进行证书更新，在每个证书到期时进行更换。确保提供准确的证书报告，并将管理证书更新的责任交给相应的团队成员。采用这种模式，在初始切换过程中安装证书所需的时间较少，但在更新新管理账户下的所有证书之前，必须努力监控到期日期。
- **新起点模式**
  您也可以一次性更换所有 TLS 证书。这种方法需要投入初始时间和资源，一次性更换所有现有证书。不过，这样就无需在旧证书的剩余生命周期内对其进行监控，也无需依赖多个管理平台。

识别内部使用与外部使用

证书功能和安全级别因 CA 而异。查看新 CA 提供的证书，确定哪些产品能满足您的使用要求：

- 对于面向公众的网站，TLS 证书可向网站访问者证明网站的合法性和可信度。使用知名品牌的高质量证书可确保这些网站的安全。
- 对于通常只需要加密功能的内部网站，可以使用更基本的证书。

整合范围

如果您与当前 CA 使用 API 集成，则需要与新 CA 创建类似的集成。

您首选的 CA 应具备充足的 API 文档，并在整个入职过程中提供支持和指导。请务必在项目时间表中留出配置和测试新 API 的时间。

消除误解

由于对所涉及的复杂性存在误解，各组织往往不敢更换 CA。这些是最常见的误解：

- **根 CA 破坏过于困难**
  保留当前 CA 的一个常见理由是，你不想经历分发新 CA 根的繁琐过程。对于公众信任的证书，如果您选择的 CA 具有很强的根普遍性，则通常不需要这一过程。根普遍性强的 CA 会将其根 CA 嵌入流行的根存储中，覆盖所有主要浏览器、设备和操作系统。

如果新 CA 用于私人信任并需要发布新的根证书，则可通过组策略或其他配置管理软件自动执行此过程。

在配置网络服务器时，CA 一般会在交付最终实体证书时附上相关的根证书和中间证书，以提供完整的信任链。由于 TLS 证书基于通用标准（如 X.509 v3），因此不同供应商申请和安装证书链组件的流程完全相同。如果新的 CA 支持ACME协议，就可以利用 ACME 客户端自动签发、安装和配置 TLS 证书。

- **重新验证域名过于耗时**

  另一个阻碍 CA 迁移的因素是，为每个域名进行域名验证过程将是一场后勤噩梦。几年前，情况可能是这样。如今，这一过程可以简化并实现自动化。

  ACME 客户端与受支持的 CA 配合使用时，可通过 HTTP、DNS 或其他方法实现域名验证过程的完全自动化。对于管理许多子域的企业来说，这可以进一步简化。有些 CA 允许父域的验证适用于任何子域。例如，example.com 的成功域名验证可重复用于 sub.example.com、sub.sub.exam-ple.com 等。

步骤 3 - 估算成本

一旦您了解了更换供应商所涉及的问题，您就可以确定成本范围。

资本支出

一次性资本支出可能包括证书发现工具、证书管理服务和 API 集成工作。

- **证书发现工具**
  无论您目前使用的是一个还是多个 CA，您都可能希望使用证书发现工具来清点证书使用情况。这项服务通常与下面讨论的证书生命周期管理 (CLM) 服务捆绑在一起，不收取额外费用。

- **证书生命周期管理服务**
  您首选的 CA 应提供基于 SaaS 的证书生命周期管理平台，使客户经理能够订购、更新和签发证书，并执行其他管理功能，如计费和报告。

如果贵组织需要处理大量证书，采用多供应商策略，使用自签名证书，或希望在管理 TLS 证书时增加便利性和自动化，则可能需要投资额外的现场软件，用于密钥管理和自动化证书管理。这些服务将清单功能与提供证书的能力相结合，使用预先配置的 “连接器” 直接与主要 CA 的 API 相连接。您可以在一个平台上管理您的证书生命周期（如证书签发和更换），而无需登录每个 CA 的管理系统。

这些服务还可以通过扫描网络上的所有证书，检查密钥大小和散列算法等密码学最佳实践，帮助实现合规性。它们可以提醒您注意任何不符合安全标准的证书，并让您在服务内轻松更换。它还可以通过提供预定的可信报告来显示证书是否符合最佳实践，从而协助合规部门进行审计。

- **现有应用程序接口集成**
  如果您在现有 CA 中使用 API，请将更新代码以集成新 CA 的 API 所需的开发成本考虑在内。

- **新的应用程序接口集成**
  许多 CA 都提供 API 集成，您可以用它来自动管理证书，包括：
  - 自动签发证书
  - 通过内部门户订购
  - 维护详细的使用报告

如果您想实现这些功能的自动化，请与新 CA 讨论您所需的工作流程和功能。将任何内部开发时间和资源计入第一年的成本。

业务支出

从持续运营的角度来看，您需要考虑账户用户熟悉新管理平台所需的时间，包括设置报告、委派职责等。培训时间因个人职责不同而异。

年度证书费用

在评估不同的 CA 时，应考虑单个产品的成本以及它们在特性和功能方面提供的价值，包括：

- 重新签发或在多个服务器上安装证书的任何额外费用
- 与证书捆绑的任何附加服务，如恶意软件和网络钓鱼监控
- 证书本身的性质（例如，由 4096 位根证书签发）

每个 CA 的证书产品都不尽相同。请查看产品系列，确保证书满足您的需求，并且不包括不必要的高级附加功能。

步骤 4 - 考虑转用 GlobalSign

在比较 TLS 托管服务提供商时，一定要记住："您选择的是业务合作伙伴，而不是产品。这是一种超越交付收缩包装产品的关系。在他们签发证书后的很长一段时间内，你都将依赖于他们 "4

除了提供安全性最高、功能丰富的 TLS 证书外，CA 提供商还应能够：

- 为您提供定制环境
- 就安全措施向您提供建议
- 提出建议以满足您的业务需求
- 提供工具来验证网络服务器配置是否经过优化，以实现最高安全性
- 提供各种证书生命周期管理和自动化解决方案，以满足您的特定需求

各组织之所以选择 GlobalSign，是因为 GlobalSign 致力于提供领先的数字证书解决方案，是值得信赖的合作伙伴。作为以企业为重点的最大证书颁发机构之一，GlobalSign 在全球各地拥有专家团队为客户提供支持。其解决方案围绕客户需求和行业最佳实践而构建。

GlobalSign 的优势

GlobalSign 一直致力于开发更安全、更方便用户使用的 TLS 证书。

- 自 1998 年起使用 2048 位根，早于最佳实践建议的提出时间
- 在业界率先在 IPv6 中引入证书吊销服务
- 不断改进我们的证书签发平台，提高可靠性、性能和灵活性
- 通过支持工具和产品加强我们的证书组合，为客户提供完整的证书解决方案
- GlobalSign 是首家获得四项 ISO 认证的 CA。获得 ISO 认证证明了 GlobalSign 对国际标准的承诺，展示了我们对质量、安全和隐私的重视。
- 为什么选择GlobalSign
  - —无与伦比的客户支持和响应
  - —全球影响力和基础设施
  - —全面灵活的产品组合
  - —具有竞争力的定价和财务灵活性
  - —强大的安全性和信任
  - —易于使用和高效管理
  - —持续创新和适应性

我们将继续更新我们的管理平台并发展重要的合作伙伴关系。
与其他 CA 相比，这些创新和合作伙伴关系为 GlobalSign 带来了重要优势。

页面加载速度更快

每当浏览器连接到一个安全网站时，网站的 TLS 证书状态都需要与签发 CA 进行验证。这个过程（OCSP 响应或 CRL 传递）需要多长时间，取决于 CA 基础设施的效率和用户与 CA 之间的位置关系。

GlobalSign 与 CloudFlare 和 Fastly 等网络性能专家合作，利用其全球基础设施提供快速可靠的证书状态请求。这将 OCSP/CRL 响应速度加快了 6-10 倍。更快的页面加载速度有助于留住访客，并在提高搜索引擎优化方面发挥作用。

增强可用性

如果撤销基础架构脱机，您可能会遇到严重的中断。外部访问者将收到安全警告，内部设备将无法通信。GlobalSign 利用多个 CDN 分布我们的撤销基础架构并消除单点故障。我们坚持超越操作安全的最佳实践，包括严格遵守 GDPR，我们的基础设施和操作每年都由合格的外部审计员进行审计。我们的认证服务通过强大的 PKI 基础设施提供，该基础设施包括全球数据中心、灾难恢复、冗余、高可用性和保护网络的世界级仪器。

网站的持续安全性

GlobalSign TLS 不仅仅是挂锁。它能全天候保护您网站的安全。在线SSL配置检查器可测试您的域是否存在三十多个最常见的 TLS 配置问题和漏洞，并提供可行的补救指导。

企业证书管理

GlobalSign 基于 SaaS 的PKI托管服务可管理整个组织的证书。 托管 PKI 平台旨在帮助企业大幅降低与使用 TLS 相关的预算、时间和管理成本。只需一次性审核，管理员便可按需全天候签发全系列 TLS 证书，从经济高效的加密证书到用于公共站点的高保证 EV 证书。

根据贵组织的需求定制服务，提供灵活的业务条款，例如：

- 无限制证书颁发许可证
- 大量存款
- 可无限添加用户、域和配置文件
- 强大的报告和管理工具，确保可靠性、性能和灵活性

通过 GlobalSign 的企业自动化解决方案-- 证书自动化管理器，您可以将 PKI 托管服务与 Microsoft Windows 环境集成，从而受益于使用 Active Directory 和 Entra ID 进行自动证书供应和管理的便利性。该集成支持自动注册和静默安装，是运行成本高昂、劳动密集型内部 CA 的安全、经济的替代方案。

专职账户管理

GlobalSign 的每位客户都有一位专门的客户经理，在需要帮助时随时可以联系到他。通过电话、网络和电子邮件，客户经理可以帮助客户选择产品，为证书生命周期问题提供支持，并讨论贵组织即将实施的安全计划。

运行安全

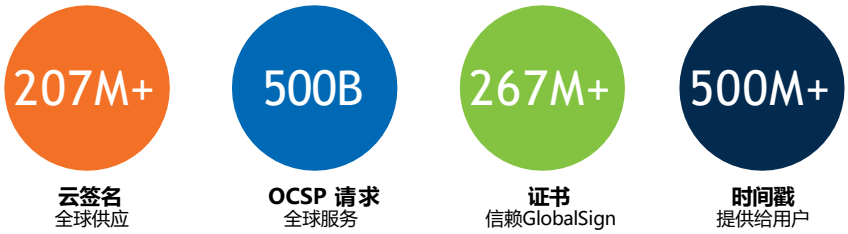
您需要依靠 TLS 证书来提升品牌声誉、增强最终用户的信任度并保护您的组织和网站访问者的敏感信息。GlobalSign 赢得了业界的认可和信任：

- GlobalSign 是最早使用 ICA 并维护离线根 CA 的 CA 之一，目的是最大限度地降低根 CA 遭受攻击的风险。现在，这已成为一种既定的安全最佳实践
- WebTrust 是针对签发公共证书的 CA 的审核标准。自 2001 年以来，GlobalSign 每年都会对 WebTrust 合规性进行审核
- GlobalSign 是 CA/B 论坛和 CA 安全理事会的创始成员
- 它是在线信任联盟和反网络钓鱼工作组的成员
- GlobalSign 是首批颁发合格数字证书的 CA 之一

除了遵守行业最佳实践外，GlobalSign 还根据第三方安全顾问的建议，使用适当的安全工具监控和保护自己的基础设施。

切换核对表

以下是切换 CA 时的注意事项汇编：

考虑因素	GlobalSign 如何提供帮助
学习新平台	GlobalSign 提供在线用户指南和教程。所有客户都有一名专门的客户经理，如有任何问题，都可以联系他们。
更新方法	GlobalSign 可采用逐步过渡和全新启动两种迁移方法。对于使用新启动方法的组织，GlobalSign 会将现有证书的剩余时间添加到替换证书中，但不超过行业允许的最大值，因此您不会损失证书的有效期。 使用过渡方法的机构将受益于域名预先审查，因此当需要更换 CA 时，您可以立即签发证书。
内部使用与外部使用	作为提供 TLS 安全性的全球 CA，GlobalSign 久负盛名，值得信赖。GlobalSign 不仅在公共网站上拥有良好的品牌声誉，还为内部使用提供了经济高效的选择。 
年度证书费用	GlobalSign 提供多种 TLS 证书，可满足各种使用情况。所有公开信任的 TLS 证书最小位数为 2048 位，可安装在无限台服务器上，并可免费补发。您只需支付使用费用，无需购买令牌或证书基金。
应用程序接口集成	无论您是在当前的 CA 中使用 API，还是有意首次集成 API，GlobalSign 专家都将与您密切合作，确保集成功能完全符合您的需求。
证书管理系统	我们的证书自动化管理器解决方案可自动提供证书，支持您的 Active Directory 或 Entra ID 环境，并提供全面的管理和报告功能。

结论

转换 TLS 提供商不仅仅是一次技术升级，更是一项影响企业安全和运营效率的战略决策。通过遵循本白皮书中概述的结构化方法，您可以确保无缝过渡到新的 CA，增强您的安全态势并简化证书管理。

立即联系 GlobalSign，了解我们如何帮助您

从现有的 TLS 提供商高效、安全地切换到我们的服务 - 请访问
https://www.globalsign.cn/company/contact

关于 GMO GlobalSign

作为世界上根基最牢固的证书颁发机构之一，GlobalSign 是可信身份和安全解决方案的领先提供商，可帮助全球组织、大型企业、基于云的服务提供商和物联网创新者进行安全的在线通信、管理数以百万计的经过验证的数字身份并自动进行身份验证和加密。该公司的大规模 PKI 和身份解决方案为物联网中的数十亿服务、设备、人和物提供支持。GMO GlobalSign 是日本 GMO Cloud KK 和 GMO Internet Group 的子公司，在美洲、欧洲和亚洲设有办事处。欲了解更多信息，请访问 https://www.globalsign.cn。