GlobalSign by GMO

# 信任 PKI

安全系统的基础

# 目录



# 简介

信任至关重要。随着在线交易、通信和数据交换的快速增长，确保这些互动的安全性和真实性至关重要。公钥基础设施（PKI）和数字证书是建立这种信任的基础，为验证身份、保护数据和维护数字交互的完整性提供了一种手段。本电子书将探讨 PKI 和数字证书的基本组成部分，强调它们在数字环境中建立信任的作用。

## 什么是 PKI?

公钥基础设施（PKI）是一种通过管理数字证书和加密密钥实现安全数字通信的框架。PKI 使用可信的证书颁发机构（CA）颁发数字证书，将公共密钥与经过验证的实体联系起来。该系统可确保数据的私密性和不被篡改，对用户和设备进行身份验证，并支持网站加密（SSL/TLS）、数字签名和用户身份验证等安全应用。PKI 的结构化 “信任链” 模式可验证身份，为依赖安全数据交换的行业建立在线互动的信心。

# 信任的基础

## 了解公共证书颁发机构 (CA)

证书颁发机构(CA)在创建数字环境信任基础方面发挥着关键作用。作为受信任的第三方，CA 颁发数字证书来验证网站、组织和个人的身份。当 CA 的根证书受到广泛信任时，其签发的证书也会自动受到浏览器和设备的信任，从而确保安全可信的交互。

### 根的普遍性作用

根普遍性是指 CA 的根证书出现在各种设备、操作系统和浏览器的可信根存储中。具有广泛根普遍性的 CA 可确保其证书被绝大多数平台接受和信任，从而实现顺畅安全的在线通信。

### 使用可信 CA 的主要优势

- **身份验证:** CA 验证实体身份，确保用户与合法网站或服务进行交互。
- **加密:** CA 可为在线交换的数据加密提供便利，保护敏感信息免遭未经授权的访问。
- **数据完整性:** CA 颁发的数字证书有助于维护数据的完整性，确保数据在传输过程中没有被篡改。

## 如何建立信任

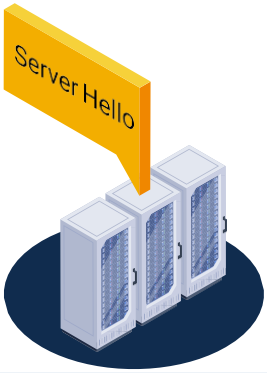
通过充当 “守门员” ，CA 可确保在线互动的合法性，从而为营造安全的数字环境做出贡献。

# 信任的基础(续)

## PKI 技术术语表

TLS 握手和证书验证
传输层安全（TLS）握手是在客户端（如网络浏览器）和服务器（如网站）之间建立安全通信通道的关键过程。 在这一握手过程中，服务器会出示其数字证书，客户端则对其进行验证，以确保其真实性。


1 **客户您好**
客户端通过向服务器发送“ClientHello”信息来启动握手，该信息包括超级加密算法（密码套件）、TLS 版本和随机生成的号码。




2 **服务器你好**
服务器响应 “ServerHello”信息，选择加密算法，提供自己的随机数和数字证书。


3 **证书验证**
客户端根据其信任的证书颁发机构（CA）列表检查服务器的证书。它验证证书的签名，检查证书的有效期，并确保证书未被吊销。


4 **密钥交换**
客户端和服务器使用非对称加密技术交换预主密钥，然后双方使用该密钥生成会话的对称加密密钥。


5 **完成信息**
双方发送用会话密钥加密的“完成”信息，确认握手完成并建立加密通信通道。

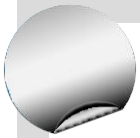
# 信任的基础(续)

## PKI 中的非对称和对称加密

了解非对称加密和对称加密的区别对于掌握 PKI 的工作原理至关重要。

### 非对称加密

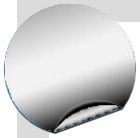
在非对称加密中，使用两个密钥--用于加密的公钥和用于解密的私钥。公钥公开共享，私钥保密。在 PKI 中，非对称加密在 TLS 握手过程中用于安全交换对称加密密钥。



当您使用 HTTPS 访问网站时，您的浏览器会使用网站的公共密钥加密预主密钥，然后使用该密钥生成会话的对称密钥。

### 对称加密

对称加密使用单个共享密钥进行加密和解密，因此比非对称加密快得多。在 PKI 中，一旦完成 TLS 握手，客户端和服务器之间交换的所有数据都将使用对称加密进行加密，从而确保高效安全的通信。



在 TLS 握手后，就会建立一个安全会话，浏览器和网站之间交换的数据会进行对称加密。

## 最佳实践

始终使用可信的证书颁发机构 (CA) 颁发的证书，并保持更新，以防止出现可能危及安全通信的验证错误。

# CA/B论坛在维护信任方面的作用

CA/B论坛在制定指导数字证书签发和管理的标准和政策方面发挥着举足轻重的作用。这个由证书颁发机构和浏览器供应商组成的联盟致力于确保颁发的证书安全、可信，并符合行业最佳实践。

## CA/B论坛的职能

- **制定标准:** 制定签发和管理数字证书的准则，确保一致的安全水平。
- **推广最佳做法:** 鼓励 CA 遵守证书管理和签发方面的最佳做法，从而提高数字通信的信任度。
- **促进交流:** 充当 CA、浏览器供应商和利益相关者就数字安全相关问题进行合作的平台。

## 如何建立信任

通过执行标准和防止欺诈性证书签发，CA/B论坛在维护互联网安全基础设施的完整性方面发挥着至关重要的作用。

# X.509证书

## 数字安全的基础

X.509 证书是安全数字交互的基础。这些证书作为数字护照，可验证参与在线通信的实体的身份。

### X.509 证书的主要组成部分

- **公钥**: 用于加密数据和验证数字签名。
- **身份信息**: 包含证书持有者的姓名、组织和其他身份信息。
- **签发者信息**: 提供有关颁发证书的证书颁发机构的信息。
- **公钥**: 用于加密数据和验证数字签名。
- **有效期**: 指定证书的有效期。
- **数字签名**: 由 CA 生成的签名，以确保证书的真实性和完整性。

### X.509 证书的应用

- **安全网站(HTTPS):** 基于 X.509 的 SSL/TLS 证书可确保网络浏览器和服务器之间的加密数据传输。
- **电子邮件安全(S/MIME):** 用于对电子邮件进行数字签名和加密，确保电子邮件通信的真实性和保密性。
- **代码签名:** 通过确保代码来自可信来源，验证软件的完整性并防止篡改。


## 如何建立信任

X.509 证书可确保只有经过验证的真实实体才能进行交易，从而实现安全通信。

# 信任链

## 确保安全的在线互动

信任链是一个验证数字证书真实性的层次结构，确保数字证书来自可信来源。

### 信任链如何运作 X.509 证书的主要组成部分

- **根证书颁发机构(CA)**: 顶级证书，由浏览器、操作系统和应用程序自行签名和信任。
- **中间 CA**: 中级 CA 由根 CA 签发，提供额外的安全层，可向最终用户签发证书。
- **终端实体证书**: 签发给网站、设备或用户的最终证书，用于建立安全通信。


## 如何建立信任

在出示证书时，会对整个证书链进行检查，以确保证书来自受信任的根，从而确认交互的真实性。

# 证书吊销

## CRL、OCSP 和 OCSP 附页吊销检查

证书吊销是 PKI 的一个重要方面，可确保不再信任受损或无效的证书。

### 吊销检查方法

- **证书吊销列表(CRL)**: 由 CA 发布的证书吊销列表。浏览器和系统会检查这些列表，以确保证书仍然有效。

  优点: 全面，因为它提供了 CA 签发的所有废止证书的完整列表。

  缺点: CRL 可能会变得很大，从而减慢验证过程，尤其是在客户端必须下载完整列表的情况下。

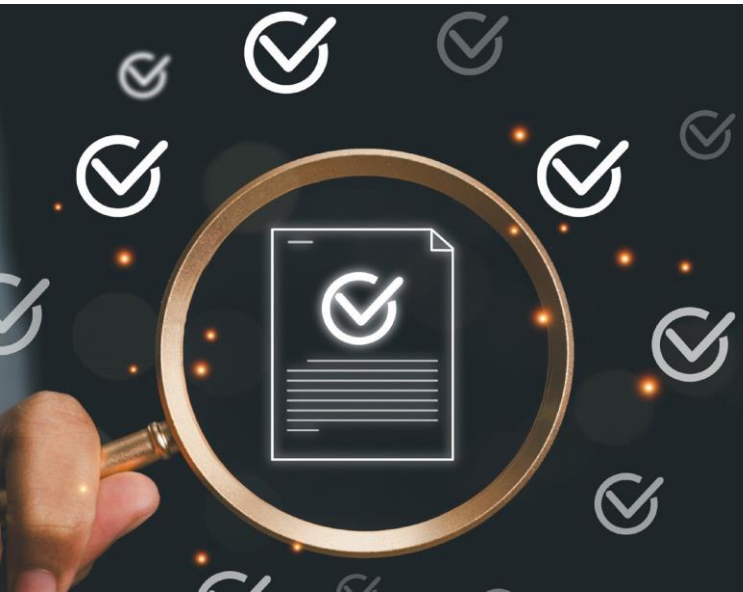
想象一下，一家企业在解雇一名员工时吊销了他的数字证书。该证书出现在 CRL 上，使该员工无法访问敏感资源。

- **在线证书状态协议(OCSP)**: 提供证书有效性的实时状态检查，减少下载整个 CRL 的需要。

  优点: 比 CRL 更有效，因为它只检查所请求证书的状态。

  缺点: 如果 OCSP 应答器速度较慢，就会造成延迟；如果它不可用，客户端就会出现延迟。

- **OCSP 装订**: 允许服务器获取 OCSP 响应并将其纳入 TLS 握手过程，从而提高效率和性能。



## 如何建立信任

吊销机制可确保及时识别不再有效的证书，从而保持证书的可信度。

# PKI 为何对有效风险管理至关重要

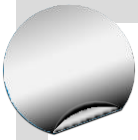
PKI 对于企业降低在线交易风险、确保通信安全和保护敏感数据至关重要。通过建立信任体系，PKI 可帮助企业维护数字互动的完整性、保密性和真实性。

## PKI 在风险管理中的主要优势

- **身份验证**: PKI 可确保只有经过授权的个人、设备或服务器才能访问敏感信息。它通过数字证书验证身份，消除了冒名顶替或未经授权访问的风险。


在登录安全的企业网络时，员工可以使用数字证书来证明自己的身份，从而降低网络钓鱼攻击的风险。

- **数据完整性**: 数字证书可确保数据在传输过程中不被篡改。即使是最轻微的改动也会导致证书失效，从而提醒接收者可能存在篡改行为。



在电子商务中，PKI 可以防止黑客拦截和篡改交易，确保支付细节完好无损。

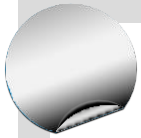
# PKI 为何对有效风险管理至关重要

## 续

- **保密性**: 通过加密，PKI 可确保只有指定的接收者才能访问敏感数据。即使数据在传输过程中被截获，这种加密也能防止未经授权的访问。

金融机构使用 PKI 加密敏感的客户数据，确保账户信息免受网络威胁。

- **不可抵赖性**: PKI 可证明信息或交易的来源和真实性，防止实体否认其参与。



合同协议中使用的数字签名可提供法律保证，使签署方无法否认已签署该文件。

## 实际应用场景

- **医疗保健**: 保护病人记录，确保只有经过授权的医疗保健专业人员才能访问敏感信息。
- **金融服务**: 安全验证交易，确保数据完整性，并实现客户与银行之间的加密通信。
- **政府**: 保障政府机构之间的通信，确保政府签发文件的真实性。

# PKI 的实施和最佳做法

公钥基础设施的实施需要精心规划并遵循最佳做法，以确保其有效性和可扩展性。

## 证书生命周期管理

有效的证书生命周期管理对于防止中断和维护安全至关重要。

- **签发**：只有经过严格的身份验证后才能颁发证书。
- **更新**：各组织应建立更新流程，避免证书过期导致服务中断。
- **吊销**：使用证书吊销列表 (CRL) 或在线证书状态协议 (OCSP)，在 24 小时内为受损或过期证书制定明确的吊销程序，以尽量减少安全风险和服务中断。

### 专家建议

自动进行证书管理，以监控到期日期、更新证书并及时撤销受损证书。

## 证书管理自动化

自动化有助于降低人为错误的风险并确保效率。它包括：

- 使用应用程序接口自动签发、更新和撤销证书。
- 部署证书管理系统 (CMS)，以监控和管理整个组织的证书生命周期。

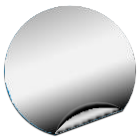
企业必须具备加密灵活性，这意味着它们必须做好准备，以快速应对加密威胁或漏洞。一旦发生事故，企业必须有能力在严格的时限内（通常是 24 小时内）撤销和重新颁发证书，以最大限度地降低安全风险和服务中断。

# PKI 的实施和最佳做法

## 续

### 证书管理责任

作为买方，重要的是要了解证书管理不仅仅是最初的实施，还包括持续的监督和迅速行动的能力。这包括制定战略，确保证书得到适当监控，并在需要时立即执行撤销程序。企业对其证书拥有所有权和责任，必须保持积极主动的态度，以确保其基础设施的安全。



CMS 可以为智能工厂中的数百台物联网设备自动更新证书，从而最大限度地降低证书过期影响运营的风险。通过采用自动化和加密灵活性，企业可以有效应对新出现的威胁，确保稳健和适应性强的安全实践。

# PKI 的新趋势和未来

PKI 在不断发展，以应对新出现的威胁、技术进步和不断变化的网络安全环境。紧跟这些趋势对于确保您的 PKI 实施保持稳健、可扩展和面向未来至关重要。

## 抗量子 PKI

量子计算的兴起是对传统加密算法的最大威胁之一。量子计算机利用量子力学原理，以经典计算机无法想象的速度解决问题，给 RSA 和 ECC 等广泛使用的加密方法带来了潜在风险。

- **重要原因**: 传统加密方法依赖于对大数进行因式分解或解决离散对数问题的难度，而量子计算机理论上可以快速解决这些问题，从而打破当前的加密标准。
- **持续努力**: 美国国家标准与技术研究院（NIST）等机构正在积极研究和开发抗量子加密算法。这些后量子算法旨在确保 PKI 能够承受未来量子机器的计算能力。
- **最佳实践**: 企业应开始评估其密码资产、清点证书并评估量子攻击可能对其产生的影响。与供应商合作并关注 NIST 的发展，为过渡到抗量子算法做好准备，这对长期安全至关重要。


如果保护客户敏感交易数据的金融机构不采用抗量子算法，就有可能在未来解密这些数据，从而损害客户的信任和监管合规性。

## 物联网和工业 4.0 中的 PKI

物联网（IoT）设备的激增为 PKI 带来了一个新领域，因为数以百万计的联网设备需要安全、可扩展的身份验证和通信。

- **挑战**: 物联网设备的计算资源通常有限，这使得传统的 PKI 实施具有挑战性。此外，由于设备数量庞大，如果不实现自动化，大规模的证书管理将不堪重负。

# PKI 的新趋势和未来(续)

## 物联网和工业 4.0 中的 PKI（续）

- **PKI 解决方案**: 轻量级证书和自动证书管理系统有助于克服这些挑战。PKI 为设备认证提供了一个框架，确保设备和网络之间交换的数据安全可信。

- **行业用例**: 在智能工厂中，PKI 可对传感器、机器和中央控制系统之间的通信进行验证和加密。这可以防止未经授权的访问或篡改，确保工业运行的完整性。

### 专家建议

部署一个能够管理大量设备证书的强大证书管理系统（CMS），可以大大提高物联网部署的安全性。

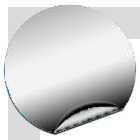
## PKI 与区块链集成

区块链技术提供了一种去中心化的信任和身份验证方法，使其成为与 PKI 相结合的一个令人兴奋的领域。

- **优势**: 区块链的去中心化特性可以补充 PKI 的中心化信任模式，提供更高的安全性和透明度。例如，在区块链上存储证书撤销信息可以提供不可更改和防篡改的记录，使证书验证更加可靠。

# PKI 的新趋势和未来(续)

- **使用案例**: 数字身份管理是区块链和 PKI 的一个交叉领域。将区块链的透明度与 PKI 的身份验证功能相结合，可以提供更安全的数字身份解决方案，减少电子商务、金融和医疗保健领域的欺诈行为。
- **挑战**: 将 PKI 与区块链整合会带来一些复杂问题，如确保互操作性和管理区块链网络的可扩展性。尽管如此，将这些技术结合在一起可能会带来重新定义数字信任的创新解决方案。

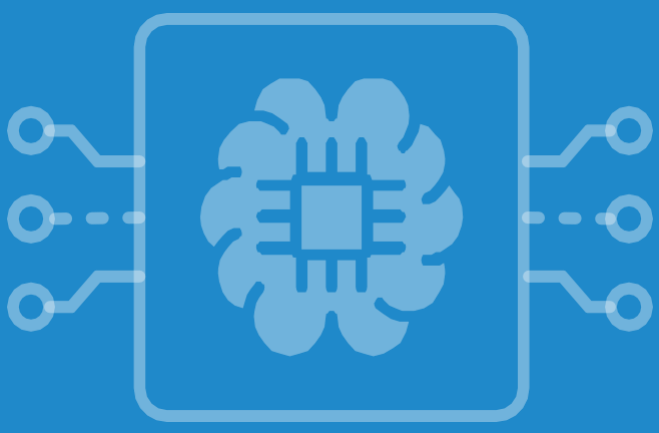


供应链管理可以从这种整合中受益。以区块链为基础、由公钥基础设施（PKI）保护的分类账可以提供透明的产品来源记录，确保真实性并防止假冒。

## 增强安全性的人工智能和 PKI

人工智能（AI）正被越来越多地用于管理 PKI 运行和加强安全措施。

- **证书管理中的人工智能**: 人工智能算法可以监控证书使用模式并预测更新需求，从而最大限度地降低过期证书导致服务中断的风险。此外，人工智能驱动的工具还能识别证书签发和使用中的潜在漏洞或异常情况，防止潜在攻击。
- **机器学习威胁检测**: 机器学习模型可以分析大量 PKI 数据，检测异常活动，如试图签发欺诈性证书或在网络钓鱼攻击中滥用合法证书。



## 专家建议

采用人工智能驱动的证书管理平台可以提供预测分析和实时洞察，从而对 PKI 环境进行主动管理。

# 合规性和监管考虑因素

遵守监管要求至关重要。PKI 在确保企业符合这些标准方面发挥着至关重要的作用，为安全可信的通信提供了一个框架。

## 《通用数据保护条例》（GDPR）

GDPR 是世界上最全面的数据保护法规之一，旨在确保欧盟（EU）公民个人数据的隐私和安全。它适用于任何处理个人数据的组织，无论其位于何处。

- **PKI 如何提供帮助**: PKI 通过对传输中和静止的数据进行加密，确保个人数据的机密性、完整性和真实性。这意味着未经授权的各方无法截获或访问敏感信息。
- **设计数据保护**: GDPR 要求企业在设计和默认情况下实施数据保护措施。PKI 提供了一种结构化的方法，用于对大量 PKI 数据进行数据化处理，以检测异常活动，如试图签发欺诈性证书或在网络钓鱼攻击中滥用合法证书。
- **最佳做法**: 使用 PKI 对包含个人数据的电子邮件进行加密，并为所有客户互动部署安全、加密的通信渠道。

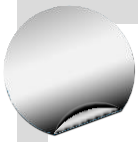
欧盟的医疗机构在与其他医疗机构共享医疗记录时，必须保护患者数据。使用基于 PKI 的加密和数字签名可确保这些记录既保密又防篡改，从而符合 GDPR 的要求。

# 合规性和监管考虑因素(续)

## eIDAS 法规

eIDAS（电子身份识别、认证和信任服务）法规是欧盟内部管理电子交易的重要框架，可确保交易安全、法律认可和可信。它为各种数字信任服务设定了标准，包括电子签名、印章和时间戳。

- **合格电子签名（QES）**: eIDAS 承认各种级别的电子签名，其中 QES 为最高级别，在法律上等同于手写签名。QES 要求使用 PKI，确保签名者的身份得到验证，文件的完整性得到维护。
- **远程签名**: eIDAS 具有远程签名功能，签名者无需实体令牌即可创建 QES。这是通过基于 PKI 的安全基础设施实现的，既方便又合规。
- **最佳做法**: 实施公钥基础设施解决方案，使其能够支持符合 eIDAS 标准的 QES，用于具有法律约束力的交易，尤其是在欧盟市场开展业务时。



一家房地产代理公司使用 QES 签订电子合同，允许客户远程签署具有完全法律效力的文件，加快了交易流程，同时确保符合 eIDAS 标准。

# 合规性和监管考虑因素(续)

## 特定行业的标准和法规

不同行业都有独特的监管要求，PKI 在确保合规方面发挥着至关重要的作用。以下是一些重要实例：

### 医疗

#### 《健康保险可携性与责任法案》（HIPAA）

HIPAA 为保护美国病人信息制定了严格的标准。

- **PKI 的作用**: PKI 可确保电子健康记录 (EHR) 经过加密，只有经过授权的人员才能访问，从而维护病人数据的保密性和完整性。
- **数字签名**: 基于 PKI 的数字签名可确保医疗记录、处方和其他敏感文件的真实性，为合规性提供清晰的审计跟踪。

**最佳做法:** 采用 PKI 对电子病历进行加密，并对电子处方使用数字签名，以保持 HIPAA 合规性并保护患者隐私。

### 金融

#### 支付卡行业数据安全标准(PCI-DSS)

PCI-DSS 适用于任何管理支付卡数据的组织，对保护持卡人信息有严格的要求。

- **PKI 的作用**: PKI 用于在传输过程中对支付卡数据进行加密，确保敏感信息的安全，防止未经授权的访问。
- **身份验证**: 基于 PKI 的双因素身份验证（2FA）有助于验证访问支付卡系统人员的身份，降低欺诈风险。

**最佳做法**: 实施 PKI，对传输中和静态的持卡人数据进行加密，并使用数字证书对支付终端和设备进行验证，确保符合 PCI-DSS 要求。

# 合规性和监管考虑因素(续)

## 政府

### 联邦信息安全管理法(FISMA)

FISMA 要求美国政府机构保护信息和系统免遭未经授权的访问

- **PKI 的作用**: PKI 为敏感的政府数据提供加密、安全访问控制和数字签名，确保符合 FISMA 的要求。
- **公共信任服务**: 政府颁发的数字证书可用于确保网站、电子邮件通信和内部系统的安全，从而增强整体安全态势。

**最佳做法**: 对所有政府系统实施基于 PKI 的访问控制，并使用数字证书保证通信渠道的安全，确保所有数据交换符合 FISMA 标准。

## 定期审计和合规维护

保持合规性是一个持续的过程，需要对 PKI 实施情况进行定期审计和审查。

- **进行内部审计**: 定期评估 PKI 基础设施，找出潜在漏洞、错误配置或不合规做法。及时处理任何问题，以保持合规性。
- **外部合规性审计**: 与第三方审计人员合作，验证您的 PKI 实施是否符合监管要求。这种独立验证有助于向监管机构和利益相关者证明合规性。
- **文档**: 保存有关 PKI 政策、程序和实践的详细文档。这包括证书签发、更新和撤销流程，以及处理受损证书的事件响应计划。

# 合规性和监管考虑因素(续)

## PKI 合规性最佳实践

- **加密和数据保护**: 使用支持 PKI 的解决方案，确保对所有敏感数据进行加密，无论是静态数据还是传输中的数据。
- **身份验证**: 使用基于 PKI 的数字证书来验证员工、客户和设备的身份，确保只有经过授权的实体才能访问敏感信息。
- **证书管理**: 实施自动证书生命周期管理，防止过期或受损证书危及合规性。
- **培训和提高认识**: 教育员工了解 PKI、数字证书和监管要求的重要性，在组织内培养合规文化。

### 专家建议

实施自动工具，监控和记录所有 PKI 相关活动，如证书的签发和撤销，为合规报告提供清晰的审计跟踪。

# PKI 的常见挑战和解决方案

PKI 为数字安全和信任提供了一个强大的框架，但同时也带来了一系列挑战。了解这些挑战并实施有效的解决方案，对于维护安全高效的 PKI 基础设施至关重要。

## 管理过期证书

证书过期会导致服务中断、信任缺失和安全漏洞。如果证书过期，可能会导致网站中断、应用程序出错甚至安全漏洞。

### 挑战

**停机**: 当证书意外过期时，关键服务可能会脱机，从而中断业务运营。

**失去信任**: 用户收到安全警告，会损害企业声誉，削弱客户信任。

**安全风险**: 过期证书可能会导致漏洞被攻击者利用，攻击者可能会冒充服务或拦截敏感数据。

### 解决方案

**自动证书管理**: 采用自动化工具监控证书到期日期，并在证书到期前进行更新。证书管理系统（CMS）可防止过期或受损证书危及合规性。

**使用短期证书**: 考虑使用自动更新的短期证书（如有效期 90 天）。这样可以降低忘记续费的风险，并最大限度地减少证书泄露的风险。

**设置警报**: 配置电子邮件或短信提醒，在证书到期日之前提前通知管理员，以便有充足的时间进行更新。

### 最佳实践

实施强有力的证书生命周期管理策略，包括定期审核、自动更新流程和主动监控，以避免证书过期的风险。

# PKI 的常见挑战和解决方案(续)

## 为大型机构扩展

随着组织规模的扩大，需要管理的证书和密钥数量也随之增加，这给保持控制和可见性带来了挑战。

### 挑战

**证书蔓延:** 企业通常会有成千上万的证书分布在各种设备、应用程序和服务中，导致难以跟踪和管理这些证书。

**政策不一致:** 跨多个部门、团队和系统管理证书会导致证书策略不一致，从而削弱安全性。

**人为错误:** 人工管理证书会增加出错的可能性，如签发参数不正确的证书或未能撤销受损证书。

### 解决方案

实施集中式证书管理系统 (CMS)，以获得组织内所有证书的可见性和控制权。这样就能实现统一的策略执行、轻松跟踪和高效的证书生命周期管理。

使用自动化工具管理证书发放、更新和撤销流程。这样可以减轻管理负担，最大限度地降低人为错误的风险。

通过根 CA 和中间 CA 创建定义明确的 CA 层次结构，以便在不同部门或地区之间划分和下放证书管理职责，提高可扩展性和安全性。

定期审核证书库存，找出未使用或重复的证书，并利用自动化来保持整个 PKI 基础设施的一致性。

# 结论

在日益数字化的世界里，信任是所有在线互动的基础。公钥基础设施（PKI）是这种信任的无形守护者，确保身份得到验证、数据保持机密、交易安全。正如我们在本指南中所探讨的，PKI 不仅仅是一种技术解决方案，它还是在每一次数字互动中建立信任的战略推动者。

实施强大的 PKI 框架可以让企业保护其资产、保护其客户，并在不断变化的网络安全威胁面前保持领先。为了保持这种安全级别，企业还必须具备加密敏捷性--做好迅速适应新威胁和加密漏洞的准备，包括在需要时快速撤销和重新颁发证书的能力。无论您是要确保电子商务平台的安全、管理物联网设备、确保监管合规性，还是要保护敏感的政府通信，PKI 都是实现安全可信数字环境的可靠途径。

## 主要收获：

- **信任的基础:** PKI 建立了一个可信任的框架，用于验证身份和确保通信安全，是在线安全的支柱。
- **多样性和适应性:** 从使用 SSL/TLS 证书确保网站安全到确保数字签名的真实性，PKI 在各行各业都有广泛的应用。
- **领先于威胁:** 技术在发展，威胁也在发展。通过拥抱抗量子算法、物联网集成和人工智能增强型 PKI 管理等新兴趋势，企业可以使其数字安全战略面向未来。
- **合规与监管:** PKI 是满足监管要求和保持合规性的重要工具，可确保组织在不断变化的法律环境中放心运作。

# 向前迈进

采用 PKI 不仅仅是部署证书或实施加密协议，而是要在整个组织内培养一种安全和信任的文化。要有效利用 PKI，请考虑以下步骤：

1. 评估 PKI 如何加强现有的安全措施，并确定可以整合或改进的领域。

2. 随着企业的发展，人工证书管理可能会成为一项重大挑战。采用自动化可降低人为错误的风险，防止服务中断，并保持对 PKI 环境的控制。

3. 数字安全领域不断变化。随时了解新出现的威胁、新标准和技术进步，确保您的 PKI 实施保持有效和安全。通过优先考虑加密灵活性，您可以确保您的组织随时准备好对任何与证书相关的事件做出快速反应，从而最大限度地降低风险并维护信任。

4. 与 GlobalSign 等经验丰富的证书颁发机构和 PKI 解决方案提供商合作，可确保您的实施不仅安全，而且具有可扩展性、高效性和合规性。

## 打造数字信任的未来

如果您准备加强组织的数字信任基础设施，请考虑如何将 PKI 整合到您的安全战略中。与值得信赖的专家合作，探索自动证书管理解决方案，并随时了解新兴趋势，以确保您的 PKI 实施既有弹性又面向未来。

## 今天就与 GlobalSign 联系！

# 与当地团队取得联系 - 访问

https://www.globalsign.cn/company/contact

## 关于 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、云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。