白皮书

digicert

实现 PKI 现代化，提高安全性、效率和灵活性

PKI 技术以一种随意的方式进入企业，造成了一种缺乏灵活性、效率低下的局面，具有讽刺意味的是，还造成了不安全性。现代 PKI 可以将整个生态系统置于控制之下，从而解决这些问题，而无需改造和替换现有技术。

即使尽可能更新，它们也缺乏灵活性，无法支持新的使用案例，也无法在不影响业务的情况下快速部署保护措施。许多现有的 PKI 系统根本无法实现充分的现代化，以支持企业在过去十年中采用的技术措施或不断变化的行业法规和标准。

在本文中，我们将介绍问题和解决方案。我们举例说明了哪些公司实现了 PKI 系统的现代化，使其处于支持业务和阻止下一代攻击的最佳位置。

当今 PKI 的现状

PKI 的目的是在我们的网络中，甚至在单个系统内，建立起无处不在的信任。我们对 PKI 系统的依赖不断增加，但我们管理这些系统的能力却没有跟上。

这个问题最常见于 “PKI 孤岛 “的开发，即在同一公司内实施不同的 PKI。这些孤岛可能是在合并或收购过程中获得的，也可能是为某个特定项目而建立的，当时没有考虑或不愿意集中 化PKI 管理的选择。在最好的情况下，这样做的结果是增加了管理成本：必须分别管理这些 “筒仓”，可能要使用不同的工具，也可能要由不同的团队来管理。如果管理不协调，政策、治理和实施可能会发生冲突。

我们在整个企业和多种软件中使用加密操作。在软件堆栈的许多步骤中，PKI 可用于验证各方身份或交换密钥和其他资源，以达到应用通信和保护隐私的目的。

这些交易在我们的系统和网络中不断发生，企业的安全取决于它们的正确执行。

全企业范围的 PKI 管理是一个相对较新的现象。在采用 PKI 之前，实施 PKI 的应用程序往往包含自己的工具和安全策略，从而导致企业中出现 PKI 孤岛。

PKI 在企业中的作用

公钥/私钥加密是互联网上或企业内部各方建立信任的机制。我们用它来证明用户的真实身份、服务器或其他设备的真实性，以及交换加密密钥以确保数据安全。PKI 或公钥基础设施是一套可信协议、库和标准，允许用户和设备在保护隐私、安全和高效的情况下交换信息。

进一步了解 PKI 的作用。

常见的例子有很多：

- VPN 系统从本质上讲是实施独立的网络并颁发证书，以支持其身份识别和加密功能。
- 微服务环境通常会创建自己的 PKI，用于识别容器和执行加密。
- 许多 UEM（unified endpoint management）系统都会为身份验证颁发证书。
- 物联网设备管理平台通常采用专门的 PKI 设置，管理软件通过 PKI 识别和控制设备。

此外，与其他软件一样，兼并和收购往往会将不同的 PKI 系统引入企业。

杂乱无章的 PKI

在现代企业中，技术的采用和发展往往是杂乱无章的。技术的获取可能不是正式计划的一部分，而是通过企业收购或员工倡议。依赖于 PKI 的重要基础设施功能，如移动设备、云计算和 DevOps，往往被作为既成事实呈现给已经投入运行的 IT 部门。

在这些例子和其他例子中，PKI 功能可能只是为此目的而提供的，并没有集成到受管理的基础设施中。因此，PKI 管理任务必须由多个人员使用多种不同的工具来完成，而且往往实时进行。即便如此，典型大型企业的许多系统仍未使用 PKI 实施强大的加密和身份验证。

数字证书和 PKI

PKI 身份验证使用的主要资源是数字证书。它能识别需要验证的对象，可以是用户、程序、手机或其他任何运行软件的东西。因此，管理的证书数量大幅增长，并将继续增长。Ponemon 研究所 2021 年的一项研究表明，典型企业管理的证书数量超过 50,000 份。现在这个数字无疑要大得多。

证书有明确的有效期。例如，公众信任的 TLS 证书的最长寿命为 398 天，约为 13 个月，而用于云工作负载等内部用途的证书的寿命则短得多。证书更新自动化的必要性是显而易见的，尤其是随着证书数量的增加和寿命的缩短。

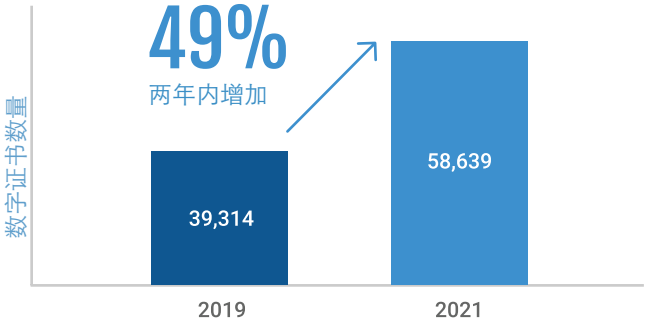
证书生命周期管理的难点之一是管理证书废止。目前有两种方法，即 CRL（Certificate Revocation Lists）和 OCSP（Online Certificate Status Protocol），这两种方法都很难有效地大规模实施。

对于短期证书，我们的想法是不去管撤销的问题，而是直接让证书过期。证书吊销和证书更新是经常需要在多个系统和流程之间协调的证书操作的两个例子。

持续的服务中断

证书过期只是 PKI 管理不善导致故障和治理、风险与合规（GRC）失败的原因之一，但却是最常见的原因。与证书总量一样，它们的数量也可能会增加。

即使取得了这些进展，人工更新的证书数量仍然很大。出现中断不仅仅是因为必须手动更新证书。在复杂的大型企业中，负责人甚至可能不知道自己拥有哪些证书。在这种无序的情况下，制定技术或预算计划就变得不可能了。

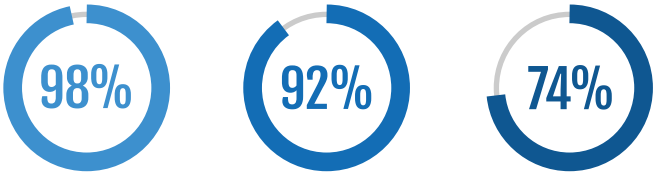


2021 年 Ponemon研究所 IoT 和 PKI 趋势

即使系统管理得再好，也有可能发生故障，因此现代 PKI 必须能够正常运行，并在发生故障时迅速恢复。

利旧系统的货币化成本

从本质上讲，每增加一个 PKI 系统，都会增加维护和管理成本。每个系统都需要由具备足够专业知识的人员来管理（这一点越来越难找到），而且软件本身可能需要持续的许可证和维护费用。这可能会导致大量的运行开销，尤其是在处理多个系统时。不同的系统和孤立的操作也会给可见性和管理带来挑战，增加中断和安全漏洞的风险。



DigiCert 2024 数字信任状况调查报告

定义现代 PKI 平台

发现、清点和所有权

要使杂乱无章的企业 PKI 井然有序，首先要有一个发现过程。现代 PKI 可以扫描网络的所有可到达部分，从其他系统中获取有关现有证书的数据，并创建一份清单（最好作为资产跟踪系统的一部分），以便 IT 部门进行规划。一个好的发现程序应能识别多种类型的证书，包括公共证书和私人证书--无论签发证书的机构是谁--并很可能发现多个 PKI 孤岛。

这些都是独立的系统，用于从内部或公共 CA 签发数字证书。他们都是从哪里来的？它们很可能是为支持特定应用程序而设置的，或者是作为合并或内部整合的一部分而添加的。原因有很多，在当时可能都是合理的。

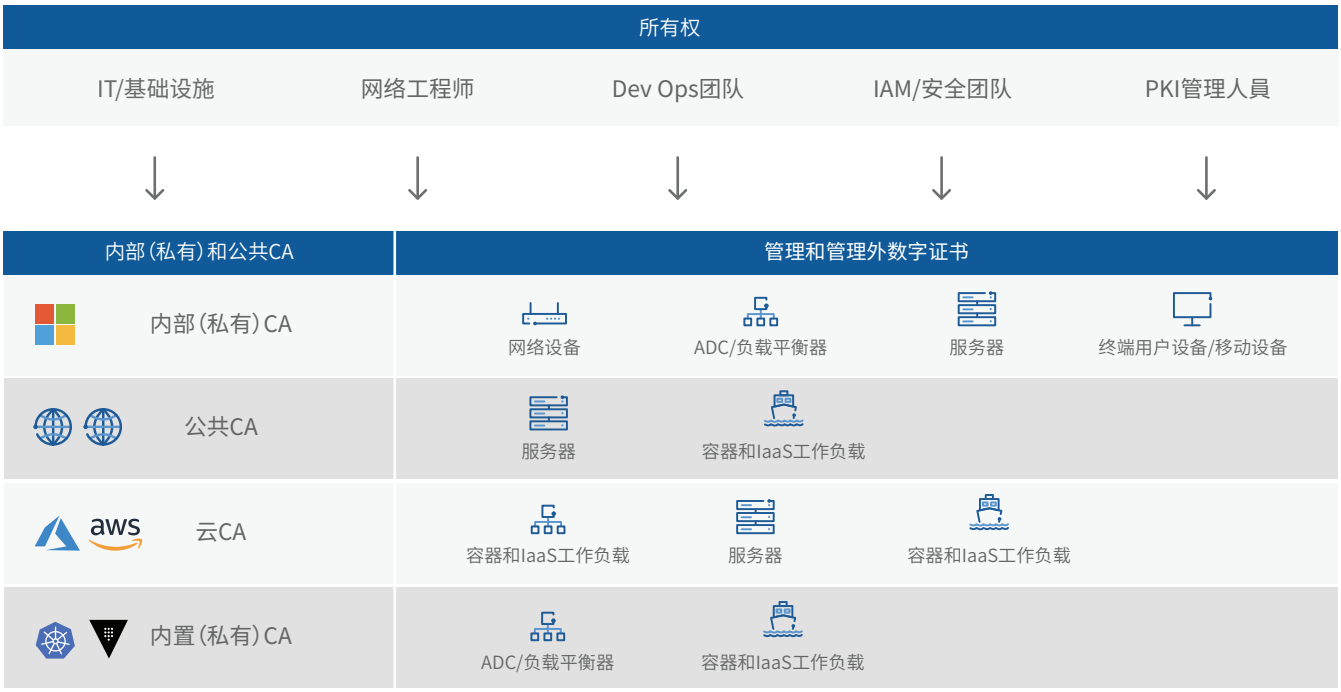
原因有很多，在当时可能都是合理的。同时，还可以建立使用 PKI 的应用程序的清单和所有权。

什么是 “PKI”？ 什么是 “网络 PKI”？ “P” 代表什么？

公钥密码学涉及公钥和私钥，PKI 是实现这些操作的系统和服务的术语。虽然可以说是 “公钥/私钥基础设施”，但只有一个 “P”，而且第一个用到的词就是 “公共”。也许这是因为私钥是私人的，而基础设施是公共的。

企业内部的私有 PKI 也很常见。这些系统可能是专门为服务特定应用而设置的，如大型 Enterprise Java Beans 系统或 Kubernetes 集群。他们也可能是不法 “影子 IT “行动的一部分。你可能只能通过发现来了解它们。

你还会听到 “PKI “和 “网络 PKI “等说法。网络 PKI “指的是公共 PKI，即面向互联网的 PKI，DigiCert 等公共 CA 就是其中的一部分。” PKI” 也可以指它，但在专门讨论私有PKI 时，也可以指它。



集中管理、分散使用

现代 PKI 平台通过分布式证书使用和生命周期管理提供集中管理和监督。这意味着整个企业的团队都可以根据公司政策管理自己的证书获取和使用。与大多数云软件一样，现代 PKI 在提供一定程度的自助服务时效果最佳。

在这种情况下，什么是自助服务？PKI 系统是证书生命周期管理系统CLM）的一部分，对许多功能进行集中控制，包括系统使用政策和基础设施管理。但组织内的团队和个人应该能够根据政策执行许多常见的 证书生命周期管理CLM 操作。

为此，CLM 应提供一个可访问的门户网站或专用应用程序，用户可通过它们申请和获取证书，并在需要中央 PKI 团队协助的更复杂操作方面获得协助。现代 PKI 系统还必须通过标准协议、应用程序接口和集成，支持系统和设备的自动交付和安装。

在可能的情况下，集中管理可以将 PKI 系统交到最有专业知识的管理员手中，并释放出专门用于传统 PKI 系统的人员和预算。

公共和内部（私有）使用案例

要整合不同的 PKI，需要支持任何证书颁发机构以及各种云、内部部署和混合企业架构。有些是公共证书颁发机构，如 DigiCert，但内部私有 CA 也适合某些应用。它们应该受到同样的管理。虽然行业标准提供了公共证书颁发机构之间证书的互操作性，但私人证书颁发机构却没有这样的标准。现代 PKI 应兼顾这两方面，但要有防范私有CA危险做法的智能。

你为什么要运营一个私有 CA？某些应用程序，如基于容器的大容量应用程序，会在短期任务中使用大量证书。专用 PKI 提供的身份验证和加密功能对于确保这些工作负载和环境的安全非常重要。性能最高的解决方案是本地私有 CA，它可以快速响应证书请求并记录所有操作。

即使在这些情况下，应用程序在逻辑上是孤立的，最好的做法也是使用全局 PKI 政策来管理专用 CA。提供这种管理方式的托管 PKI 是大多数组织的理想选择。

开箱即用，支持多种工作负载

现代 PKI 系统可适应任何工作负载，包括终端用户设备、服务器、服务、应用程序、容器、虚拟机和其他设备上的负载。由于开放标准由来已久，任何 PKI 系统一般都能与其他系统互操作。通过标准接口和供应商联盟，现代系统可以与任何其他系统或应用程序协同工作。正如本文后面所述，必须具备与企业架构无缝互操作和集成的能力。

灵活的部署模式

混合型企业尤其棘手和重要。一个逻辑应用程序可能在内部系统和多个云中都有组件。它还可以管理嵌入到专有设备中的客户和供应商证书。复杂的企业可能拥有在不同司法管辖区独立运营的单位，这些单位具有不同的法律要求，需要灵活地进行适当管理。

现代 PKI 系统应能在这种情况下合理地管理证书，即使并不容易。这包括与传统 IT 基础架构的内部目录服务集成，与云提供商证书服务的兼容性，以及跨混合设置管理证书的能力。通过在这些环境中提供一致的管理工具和自动化功能，企业可以简化证书生命周期流程并避免安全风险。

工作流程和自动化

现代 PKI 系统将关键程序和工作流程正规化，例如证书撤销等事件所需的审批以及所有事件（或至少客户希望保留的所有事件）的记录保存。

它应自动处理日常和特殊用例，以改善用户体验，降低管理开销，并减少导致中断和安全事件的错误配置机会。

PKI 生态系统

报告、分析和通知

它还应提供许多默认报告，并能对其进行定制。例子包括：

- 库存报告
- 报告过期和即将过期的证书
- 报告已撤销的证书
- 报告证书如何符合企业的安全策略、行业标准和相关政府法规

现代 PKI 系统应提供分析功能，以显示重要问题，如哪些证书仍在使用较弱的加密算法或密钥长度。它还可以进行成本分析，并提出优化成本的建议。它甚至可以进行与证书管理不善或监管合规有关的风险评估。

在主动方面，现代 PKI 应提醒用户注意许多事件，并允许事件升级和配置。最明显的是证书即将过期的警告。在大多数情况下，最好将证书设置为自动更新，并在提示中说明何时更新。证书吊销、违反政策、在系统外发现证书以及许多其他事件（包括正常事件和其他事件）都必须通知正确的用户。当然，警报应根据组织现有的服务管理和安全操作实践进行流程。

生态系统支持的重要性

最后，它应使用标准和专有接口与企业生态系统中的相关软件集成。PKI 生态系统广泛而复杂，互操作性尚未完全标准化。优秀的现代 PKI 将直接与亚马逊网络服务和 HashiCorp 等主要云服务和 DevOps 基础设施提供商集成，以简化发现流程并建立中央管理。

由于 PKI 在企业中的应用范围不断扩大，许多大公司的产品都依赖于 PKI。Microsoft Windows和其他操作系统依靠 PKI 进行联网和身份验证。Office 和 Exchange Server 等 Microsoft 应用平台广泛使用 PKI 进行联网、身份验证和加密。 出于同样的原因，Apple和 Google的产品也依赖于 PKI。Adobe Acrobat 和其他 PDF 工具可以使用数字证书对 PDF 文件进行数字签名，以证明其创建者的身份。例如，顾问编写的定制应用程序可能依赖 PKI 来确保数字交易和通信的安全性和可验证性，以满足合规要求。有了现代 PKI，它们都能更好地工作，而且更加安全。

该领域的主要特例是 Windows 和 Azure 上的 Microsoft Active Directory（AD）。AD 在1990 年代设计时可能是现代和先进的，但如今，它已成为一座技术孤岛。Microsoft正通过 Azure Active Directory（现为 Microsoft Entra Domain Services）向现代标准迈进，该目录使用 SAML、OAuth 和 OpenID Connect 等协议，而不是 NTLM 和 Kerberos。Azure AD 具有多因素身份验证、条件访问和单点登录等核心功能。

DigiCert Trust Lifecycle Manager

企业可能会高度依赖 Active Directory 进行用户、服务器和域管理，但也需要通过其他方式管理移动设备、互联网服务和其他资源。他们还有许多其他需要 PKI 的应用程序，现代 PKI 应尽可能多地与这些应用程序无缝集成。开发人员使用的 DevOps 工具如果有强大的 PKI 支持，就会最安全。网络服务器、负载平衡器和其他应用平台都有核心 PKI 需求。防火墙和路由器等网络设备使用 PKI 实现安全通信。 Mobile Device Management 广泛使用 PKI。这样的例子不胜枚举。

现代 PKI 将所有这些要素整合到一个系统中，使企业能够对它们进行逻辑管理，并与其他 PKI 系统协同工作。

现代 PKI 在行动

现代 PKI 解决方案并非抽象概念。它今天依然存在，但通常与现代化项目或历程联系在一起。
以下是三个客户案例，重点介绍现代化历程和相关效益。

发现节约和安全

这家大型金融服务集团依赖于众多难以管理的孤岛式公钥基础设施（PKI）系统。过时的 PKI 环境经常因证书过期而导致中断。由于证书的可见度有限，有时使用证书的系统的 IT 管理员又缺乏 PKI 方面的专业知识，这种情况就更加严重了；有一次，他们不得不联系一名前雇员来帮助恢复运行。

该公司利用 DigiCert Trust Lifecycle Manager 启动了 PKI 现代化之旅，首先是全面发现所有证书并分配所有权。结果发现，与不活动系统相关联的未使用证书数量惊人，这些证书仍被各自为政地管理着。

DigiCert Trust Lifecycle Manager 提供的发现、清查和所有权流程使他们能够：

- 降低成本，提高效率：DigiCert 推动了不必要证书和系统的退役，节省了预算并简化了 IT 操作。
- 加强安全态势：加强对公钥基础设施环境的了解有助于发现漏洞，并通过停用未使用的系统来减少攻击面。
- 简化管理：DigiCert 将证书管理整合到 IT 团队的直接权限范围内，实现了主动管理并减少了中断。

通过自动化实现简化

一家技术公司运营着复杂的 IT 基础设施，在多个数据中心拥有数千台虚拟机，但由于证书数量不断增加，而调配和安装又需要人工操作，该公司在管理证书方面举步维艰。

网站可靠性团队在耗时且容易出错的人工证书管理流程中苦苦挣扎。配置和安装一个证书可能需要几个小时。缺乏对证书库存和生命周期的可视性，增加了因证书过期或配置错误而导致中断的风险。

DigiCert Trust Lifecycle Manager 实现了证书生命周期管理的自动化和简化，显著提高了效率，降低了中断风险。

主要优势包括:

- 简化自动注册：配置模板和自动化将证书配置时间从数小时缩短到数分钟。
- 增强可见性：自动发现和清点证书可提供更好的监督。
- 提高安全性：撤销和替换受损证书的自动工作流程增强了安全态势。
- 提高效率：与各种工作负载的无缝集成和日常任务的自动化减轻了 IT 负担。

克服并购中的 PKI 盲点

这家大型企业常常对因合并或收购而产生的与 IT 运营相关的证书管理挑战感到惊讶。这种复杂的环境包括内部部署和基于云的基础设施，证书由多个 CA 签发，并采用不同的政策和流程进行管理。

由于存在多个 CA、政策不一致以及缺乏集中管理等问题，证书盲点阻碍了高效的证书管理。合并和收购引入了新的证书库存、政策和系统，加剧了这些挑战。这就增加了因证书过期或受损而导致中断、漏洞和业务中断的风险。

该组织与 DigiCert 合作进行 PKI 现代化。他们利用 Trust Lifecycle Manager 提供的服务来应对这些挑战：

- 全面发现：在多个 CA 和环境中识别和清点证书。
- 集中管理：整合证书政策和流程，实现高效管理。
- 自动化：简化证书发放、更新和吊销流程。
- 集成：与现有证书管理系统无缝集成。

加密灵活性和 PKI 格局

PKI 是进攻性和防御性安全研究的一个丰富领域，因为它是所有领域安全的核心。多年来，针对公钥基础设施中实施的标准中存在的弱点，已经通过了许多修改。

在一个杂乱无章的公钥基础设施中实施这些更改充其量也就是困难重重，而且不太可能在可接受的时间范围内取得成功，并将对业务的干扰降到最低。

这样的例子有很多，钥匙长度就是其中之一。随着计算能力的逐年提高，攻击者越来越能破解更短、更弱的密钥。
现代 PKI 系统可以告诉你是否有弱密钥，然后为你更换强密钥提供方便。

随着时间的推移，研究人员发现了一些加密算法的弱点。这种情况不止一次发生在哈希算法上，流行的 MD5 和 SHA1 哈希算法就有明显的弱点。拥有现代 PKI 系统的企业更有能力确保不使用弱算法。

但最大的问题还在后面。量子计算有可能成功攻击许多广泛使用的加密算法。NIST 多年来一直致力于解决这一问题，并发布了第一套后量子标准。有些算法使用较大的密钥是 “量子安全 “的，但有些算法必须完全替换。

与哈希算法一样，如果没有现代 PKI，对这一过程的管理也不可能成功。现代 PKI 系统已经开始支持新的 NIST 后量子算法。而且，算法领域可能出现的问题还不止这些；假设需要多次尝试才能获得量子安全密码学的正确性，这并不夸张。

建议

采用现代 PKI 并不是 “翻新和替换”。它能让您更安全、更高效地使用现有加密资产。通往现代 PKI 的道路可能会很复杂，而且需要一些时间，但幸运的是，它的起点总是相同的：

1. 发现和评估：首先评估当前的 PKI 系统。 即使没有进一步的进展，在执行发现程序后也会更好。这将让你了解你拥有哪些证书，以及 PKI 在企业中的普及程度。如果您和大多数企业一样，会在发现报告中看到许多意外情况，并得出结论：您需要为混乱的局面带来一些秩序。确定 PKI 系统的优势、劣势和需要改进的地方。评估 PKI 与业务目标和监管要求的一致性。这项评估将为您的现代化之旅奠定坚实的基础。

2. 这项评估将为您的现代化之旅奠定坚实的基础。首先关注这些高度优先领域的 PKI 现代化。这种方法将带来最显著的效益和投资回报。

3. 集中政策和管理：将 PKI 集中到单个系统或层次结构中可能对某些组织有效，但对于更复杂的组织或部署而言，将重点放在集中策略和治理上，并结合通过发现实现的可视性，可使现代 PKI 灵活地根据整个企业的特定用例进行微调。

4. 整合公共和私有：将公共和私有 PKI 用例整合到一个统一的平台上是 PKI 现代化的一个常见举措。这样做可以简化管理、降低成本并提高安全性。评估与整合相关的潜在优势和挑战，并选择符合您特定要求的平台。

缺乏现代 PKI 的企业很容易发生故障，而通过现代 PKI 实现流程自动化，就可以避免这些故障。它们还需要额外的管理资源来管理杂乱无章的加密基础设施和不必要的证书，从而浪费了大量资金。

最适合您的解决方案是能够帮助您消除这些浪费、与现有生态系统互操作、在不中断业务的情况下进行更改和升级的解决方案。

关于 DigiCert

在 DigiCert，我们一直在寻找更好的互联网安全方法。这就是为什么我们的 PQC、TLS、PKI 和 IoT 解决方案无处不在，每天被全球各地的人们和公司信任数百万次。这就是为什么我们的客户一直将我们评为五星级服务最多的原因。正因如此，我们将继续引领未来的量子安全之路，为现实世界提供数字信任。

了解 Trust Lifecycle Manager 如何助力您的 PKI 现代化之旅。