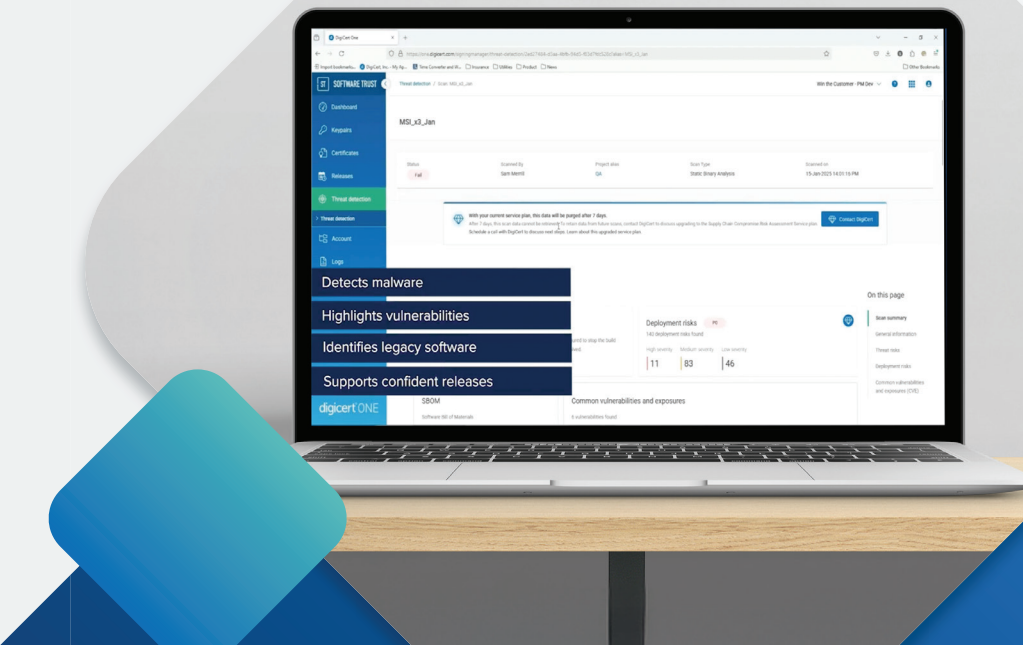
digicert®

佳能引入了更强的安全性和对代码签名的严格控制



Case Study

佳能引入了更强的安全性和对代码签名的严格控制

概述

公司名称：佳能公司
业务领域：数字印刷业务部
https://global.canon/

行业：电气设备
总部：东京都大田区

主要业务要求:

- 对应用程序、打印机驱动程序等进行代码签名
- 按照 CA/浏览器论坛的要求管理私钥保护的代码签名系统
- 合规控制

解决方案:

- DigiCert Software Trust Manager

主要功能:

- 全面了解和控制所有代码签署操作，以便快速检测和应对潜在威胁
- 基于角色的访问管理将签名和管理任务分开，减少了工作量，最大限度地降低了人为错误和安全漏洞的风险
- 自动工作流程和直观工具可将签署代码、简化流程和授权的时间减半，无论用户的技术专长如何
- 集中和严格的控制可确保遵守企业安全政策和法规，并对公司的安全系统一目了然

要求

用供应商系统取代内部代码签名系统，以快速满足私钥保护的基本要求

佳能公司是全球领先的数码影像解决方案提供商，需要加强其代码签名流程的安全性。 印刷部门约占公司销售额的 50%，为各行各业生产打印机和多功能外围设备 (MFP)。内部开发的打印机设备应用程序、打印机驱动程序必须安全可靠，以确保连接设备的安全性以及与现代操作系统的兼容性。直到最近，佳能一直在使用为自己开发的代码签名系统，但不断变化的安全要求使其有必要考虑进行修改。其一，从 2023 年 6 月起，CA/浏览器论坛将要求提供安全的私人密钥保护。

与此同时，全球软件供应链受到的攻击急剧增加，这就需要一种能够集中管理代码签名流程并在整个组织内发挥作用的解决方案。如果不对自己的系统进行重大改进，佳能就无法继续使用该系统，经过比较，佳能决定使用 DigiCert 提供的基于云的 DigiCert Software Trust Manager。 这就实现了严格的密钥管理，以及业务部门内签署流程的可视化和内部合规控制。

“我们能够将工作流程缩减到签约成员单次签约工作量的一半左右。”

在多个地点进行代码开发

印刷部门是佳能的核心业务之一，负责开发从个人和企业印刷到印刷业、制造业和食品业的各种印刷相关产品。应用程序和固件在其中发挥着非常重要的作用。其应用程序的安全要求很高，传统上使用代码签名证书和代码签名系统。这可以保护所连接的计算机和其他设备的安全，并确保它们能与最新、最多样化的操作系统配合使用。

应该指出的是，开发和签批这些应用程序和固件的成员目前分散在佳能的各个地点。

CA/浏览器论坛基线要求(BASELINE REQUIREMENT)更新和内部流程变更

2022 年 11 月，在全球频繁发生代码签名证书及其私钥被泄露事件的背景下，CA/浏览器论坛决定修改代码签名证书在私钥生成和保护要求方面的基线要求。 会议决定，OV 代码签名证书的私钥应与 EV 代码签名证书一样，存储在具有 FIPS 140-2 2 级或 Common Criteria EAL 4+ 或更高版本的安全 HSM 中。尽管佳能正在考虑转向 EV 代码签名证书，因为 EV 代码签名证书具有更严格的安全要求，但保护私钥的要求将迫使业务部门的运营发生重大变化。

因此，出现了一个新问题，即是否继续使用已使用一段时间的签名，以及是否对系统进行修改以符合新标准。

解决方案

代码签署操作的可见性和基于角色的访问管理

在此背景下，佳能在对修改和运行内部签名系统的成本与供应商自制系统的成本以及通过密钥管理和签名过程可视化实现内部合规控制的优势进行综合比较后，决定引入 DigiCert DigiCert Software Trust Manager。

Software Trust Manager 为 佳能 提供可视性和控制能力，以跟踪和监控整个组织的所有代码签名操作。这种全公司范围的监控使公司的安全团队能够掌握它。：

- 何时以及在哪个系统中进行代码签名?
- 谁履行了签署职责?
- 使用了哪些证书和私钥?

这种细粒度的可视性使安全团队能够比以往更快地发现和应对异常情况和潜在威胁。

此外，Software Trust Manager 还提供了基于角色的访问控制，使佳能能够大幅减少开发人员的责任。开发人员不再需要担心证书和密钥的管理问题，只需关注代码的签名行为。这种职责分离不仅减少了开发人员的工作量，还最大限度地降低了人为错误和潜在安全漏洞的风险。

SoftwareTrust Manager 管理员评论说：”SoftwareTrust Manager 将签名成员从繁琐的密钥管理和其他任务中解放出来，使签名成员单次签名的工作流程减少了一半左右。此外，对所有代码签名任务的管理和控制也大大减少了业务部门内部管理代码签名任务的时间”。

针对不同软件开发环境和开发人员偏好的签名

佳能选择软件信任管理器的另一个主要原因是为了简化签名工作流程。使用Software Trust Manager进行签名有多种方法，具体取决于签名工具和平台。

特别是，Microsoft的 SignTool 签名方法包括命令行调用和名为 “DigiCert Click-to-Sign “的右键签名方法，后者如果事先进行设置，可以很容易地签名。特别是后者，如果事先进行设置，可以很容易地进行签名，因此可以大大减少工作量。

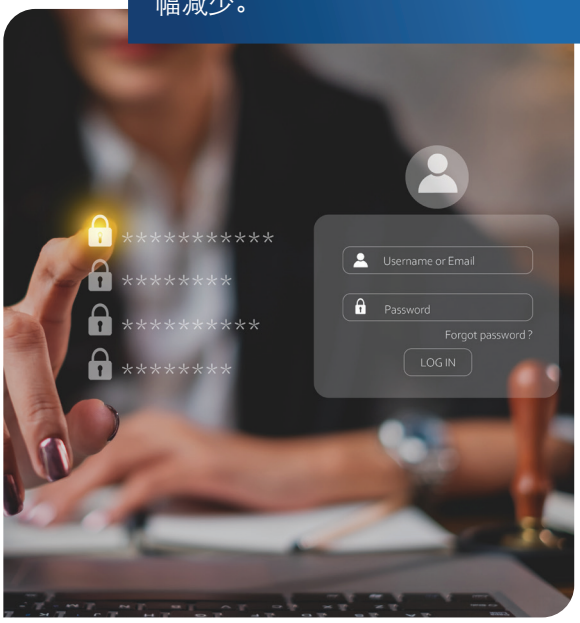
据判断，这将得到广大用户的支持，因为它可以像正常的 PC 操作一样进行。

事实上，用户评论说，与从命令行签名的方法相比，现在用右键单击执行签名更容易，而且无论信息技术知识水平如何，各种人都可以执行签名。

此外，与将应用程序上传到签名系统、执行签名、然后从签名系统下载的传统方法相比，“Click-to-Sign”将签名所需的时间缩短了一半。此外，由于签名成员只需签名即可自动留下日志，因此无需将历史记录输入管理系统，这从签名管理的角度提高了效率和数据完整性。

DigiCert Click-to-sign

“业务部门管理代码签署操作的时间大幅减少。”



尽管“Click-to-Sign”已经节省了大量时间，但仍提出了一些支持佳能开发的请求。DigiCert 采用敏捷开发方式，根据客户利益和要求在短时间内进行更新，因此这可能会带来效率的进一步提升。

佳能代码数字信任计划的展望

SoftwareTrust Manager 的推出是由签名密钥的管理和现有管理系统的替换引发的，但安全软件开发框架涵盖的范围非常广泛。对软件进行签名并不意味着其安全，但对安全创建的软件进行签名才是安全的。此外，最近的软件是通过组合许多库和组件来构建的。

如果在这些组件之一中发现漏洞，则需要采取措施使该组件无法使用，并且需要不断地管理所使用组件的漏洞。

Software Trust Manager实现了各种集成和协作功能来支持这些软件开发框架。它具有对代码执行二进制扫描以查找漏洞和秘密信息的威胁检测功能、根据扫描结果生成 SBOM 的功能以及执行文档签名以防止篡改所创建的 SBOM 的功能。因此，在可用的各种功能中，我们询问他们希望在不久的将来使用哪些功能。

“由于用户无权访问用于代码签名的私钥，因此已经实现了安全的软件签名和密钥管理。但是，如果在使用的库或组件中发现漏洞。通过轮换每个签名的私钥，可以仅撤销具有我对此功能感兴趣的特定签名的软件。Software Trust Manager管理员说道。

为未来做好准备

未来，软件代码的安全标准不仅在日本国内，而且在海外以及由各种行业组织正在制定。对付他们需要付出很大的努力。

此外，还有不少报道称，生成式人工智能的发展将加速量子计算机的实现。虽然人们期望量子计算机将提高各种发明和预测的准确性，但人们也认为目前使用的代码很容易被破解。代码签名也是如此，被解密和篡改的风险是一个问题。

为了解决这些问题，我们需要维护证书、签名以及它们使用的加密强度算法的清单，准确了解每个标准的遵守情况，确定它们的优先级，并实施对策计划，这一点很重要。届时，使用SoftwareTrust Manager进行集中库存管理和严格控制的系统将为未来做好有力的准备。

”通过轮换每个签名的私钥，可以只撤销具有特定签名的应用程序。”