DigiCert PKI Platform 服务说明

服务概述

DigiCert PKI Platform（“PKI Platform” 或 “Platform”）提供一个灵活的 PKI 平台，用于管理完整的证书生命周期、颁发新证书、续订原有证书，并撤销不可靠的证书。此外，DigiCert PKI Platform 还能够加密和恢复证书私钥，用于加密电子邮件、文件系统或其他数据，以及很多验证服务，可验证证书的当前状态，确保只有可靠的证书能进行加密数据、文档数字签名或网络认证等操作。

本服务说明，及其中包含的引用附件，是本服务说明中通过引用包含的任何协议的一部分（合称 “协议”），用于本服务说明中所述之 DigiCert 提供的服务。

目录

技术 / 业务功能和性能

服务特性

作为一项托管服务,DigiCert PKI Platform 能够显著减少与内部 PKI 有关的成本。例如，客户希望获取密码和应用服务器硬件，购买服务器和客户端许可，以及在通过内部 PKI 部署颁发第一个证书之前培训员工。客户必须创建自己的证书政策 (CP)，作为管控 PKI 层级的主要政策声明，以及证书实施说明 (CPS)，后者定义证书流程和程序以及受信任的角色和职责。基于业界最佳的密码和应用服务器硬件，DigiCert PKI Platform 被设计为多租户、高可用性的环境。该环境由经过专业培训、通过增强安全背景检验的员工，进行 24x7x365 不间断监测并定期审计，从而维持 WebTrust 和 SOC-2 资格认证。

- DigiCert PKI Platform 创建并管理**证书颁发机构 (CA)** 层级。
  - DigiCert PKI Platform 采用以下标准 CA 层级：
    - DigiCert Trust Network – 参见***附录 A***
    - 私营证书颁发机构 – 参见***附录 B***
    - Adobe® 文档签名服务 – 参见***附录 C***
    - LTE 证书服务 – 参见***附录 D***
    - 制造商证书 – 参见***附录 E***
  - 每个服务账户至少包括一个您为每个 CA 层级选择的 CA 证书。如需特定容量的更多 CA 证书，需要稍后购买。从 DigiCert 系统和服务中提取任何 CA 证书和 / 或对应的密钥对需要双方协商达成一致。
- DigiCert PKI Platform 提供两 (2) 种部署模式，即云模式和混合模式，用于**管理证书生命周期**。
  - 云部署模式将账户、证书和密玥管理工具托管在 DigiCert 的数据中心。
  - 混合部署模式也将所有账户、证书和密玥管理工具托管在 DigiCert 的数据中心，但这种模式也同时在客户的数据中心安装注册机构 (RA) 和目录集成工具。
  - 部署模式并不是独占的，可以根据各种 PKI 项目的需要使用部署模式的组合。这两种部署模式都配合桌面中间件、PKI 客户端使用，旨在通过证书生命周期大幅改进用户体验。

- DigiCert PKI Platform 提供以下管理工具：
  - **PKI Manager** – PKI Manager 是托管在 DigiCert 数据中心的网站门户，可由 PKI 管理员用来执行与账户、用户、证书和密钥管理相关的任务。
    - **账户管理:** PKI Manager 允许 PKI 管理员查看证书颁发机构 (CA)、座席数量，以及与其账户有关的报告。PKI Manager 还允许 PKI 管理员为其他 PKI 管理员创建和分配责任。
    - **用户管理:** PKI Manager 允许 PKI 管理员添加用户、撤销用户、为每个用户生成唯一的注册码，并定制发送到用户的电子邮件通知。PKI Manager 还能够为用户提供文档和视频形式的第三方应用配置说明，从而使新颁发的证书生效。
    - **证书管理:** PKI Manager 允许 PKI 管理员在其账户中配置不同 CA 的证书配置文件。作为证书配置文件的一部分，PKI 管理员设置的参数包括密钥大小、密钥用途和签名算法。PKI 管理员还选择用户体验（通过操作系统/浏览器或 PKI 客户端登记）和安全保护等级。PKI 管理员决定是否加密证书的私钥。除了配置证书配置文件，PKI Manager 还让 PKI 管理员撤销不再可信的证书，因为用户不再需要证书（比如，用户离开公司）或私钥受到威胁（比如，用户丢失了笔记本电脑）。
    - **密钥管理:** PKI Manager 让 PKI 管理员能够恢复加密证书的私钥。
  - **PKI 证书服务** – PKI 证书服务将证书登记网页托管在 DigiCert 数据中心，供用户申请证书。这些网页通过必要的步骤引导用户申请证书。此外，这些网页可以显示 PKI 管理员提供的用于配置第三方产品的说明。
  - **证书颁发中心** – 证书颁发中心是托管在 DigiCert 数据中心的证书引擎。该证书引擎根据 PKI 证书服务提交的，从 PKI 企业网关收到的，或通过 Web 服务发送的证书签名申请创建证书。该证书引擎可将证书登记到颁发证书的证书颁发机构 (CA)。
  - **PKI 企业网关** –PKI 企业网关是在需要时安装在客户数据中心的注册证书机构 (RA) 应用。该应用紧密集成轻量目录访问协议 (LDAP) 源（即，Microsoft® Active Directory®），从而自动审批证书申请并将证书数据发布回 LDAP 源。
  - **PKI 客户端** – PKI 客户端是一个端点中间件，旨在通过证书生命周期大幅改进用户体验。PKI Client 可用于采用 Windows 的笔记本电脑以及 MAC 操作系统。在浏览器登记体验中，用户使用 Microsoft Internet Explorer®、Safari®、Chrome™ 或 Mozilla® Firefox® 向证书登记网页申请证书。尽管本地体验不需要任何额外的软件，本地体验也具有已知的可用局限性。例如，Microsoft Internet Explorer 会产生很多包含警告消息的弹出窗口，经常让用户感到困惑。在 PKI 客户端体验中，证书生命周期简化实现常用功能（比如证书续约）的自动化，从而最小化用户参与度。PKI 客户端还提供集中化策略管理功能（比如 PIN、导出等），可用于保护证书。另外，PKI 客户端还能够自动配置第三方产品（比如无线、虚拟私有网络客户端等），以使用证书。DigiCert PKI

Platform 证书生命周期管理功能还可用于采用内置 iOS 无线 (OTA) 协议功能的移动设备，比如 iOS。这允许 iOS 设备或应用通过 Apple 的 SCEP 协议进行证书登记申请。对于不具备 iOS OTA 等效功能的移动操作系统，比如 Android OS，DigiCert 提供一个 PKI 客户端，同样能够隐藏配置设备和应用以便使用证书的复杂性。

- **PKI Web 服务** – 托管在 DigiCert 数据中心的 PKI Web 服务提供以编程方式与 DigiCert PKI Platform 集成的功能。第三方应用可以通过 PKI Web 服务提供的 API 获取证书策略，并执行登记和续订等证书生命周期功能。

- DigiCert PKI Platform 提供以下**认证方式：**
  - **使用登记代码进行认证** – 通过这种认证，PKI 管理员可以为每个用户生成唯一的登记代码，从而自动审批证书申请。当 PKI 管理员通过证书登记网页链接发送证书邀请到用户时，PKI 管理员包括该用户的唯一登记代码。然后用户在证书登记网页上包含其登记代码以及其他信息。证书颁发中心将比较登记代码与 PKI Manager 生成的信息。如果匹配，证书颁发中心就会颁发证书。如果用户输入的登记代码与为用户生成的代码不匹配，证书颁发中心会向用户显示错误消息。
  - **自动化认证** – 自动化认证根据 LDAP 源 (比如 Microsoft Active Directory) 中数据审批证书申请。PKI 企业网关必须安装在客户的数据中心，并与 LDAP 源集成。当用户通过 PKI 证书服务提交证书申请时，PKI 企业网关将证书申请中的数据与 LDAP 源比较。如果数据匹配，PKI 企业网关会批准证书申请，在证书申请上签署证书注册机构 (RA) 证书，然后将签署后的证书申请发送到证书颁发中心。或者，PKI 企业网关拒绝证书申请。
- DigiCert PKI Platform 提供以下**证书验证工具：**
  - **证书撤销列表 (CRL)** – 很多第三方产品都能够通过证书撤销列表 (CRL) 查看证书的当前状态 (比如，有效、撤销等)。CRL 是尚未过期的已撤销证书的黑名单。可以配置这些产品，从而定期下载和查看最近的 CRL。如果证书出现在 CRL 上，这些产品拒绝访问(比如不会认证到网络上、数字签名文档等)。DigiCert 至少每 24 小时就会产生一个 CRL。
  - **在线证书状态协议 (OCSP) –** 很多第三方产品通过在线证书状态协议 (OCSP) 验证证书的当前状态 (比如：有效、撤销等)。尽管撤销的所有证书都会显示在 CRL 上，在证书的撤销与下一次 CRL 运行之间存在一个时延，对于标准 CRL 来说最多为 24 小时。DigiCert 会在发生任何更改 (比如:撤销、暂停等) 时更新证书的状态，这会以接近实时的方式反映在 DigiCert 的 OCSP 工具内，即值得信赖的全球验证 (TGV)。

- DigiCert 提供以下**硬件选项**，用于补充 DigiCert PKI Platform：
  - **SafeNet® PKI 令牌 –** DigiCert 是 SafeNet® 硬件 USB 令牌的授权分销商。此外，这些令牌还有三 (3) 年的保修期，请参见知识库中的保修信息补充。这些令牌满足联邦信息处理标准 (FIPS) 140-2 和通用标准。
  - **SafeNet® 硬件安全模块 (HSM)** – DigiCert 是 SafeNet® Luna® 硬件安全模块 (HSM) 的授权分销商，模块包括 Luna® PCI 卡、Luna® SA 网络设备和 Luna® PCM 令牌。这些 HSM 还包括固件或相关的软件（比如 SafeNet 认证客户端）。尽管这些 HSM 包括一 (1) 年的基本保修期，DigiCert 也提供付费延长 SafeNet 保修期的选择。这些 HSM 还满足 FIPS 140-2 2 级和通用标准。
    - 销售的任何 HSM 的所有权在从 DigiCert 发货时转移给客户或由客户指定的任何一方。所有货品的交付都是工厂交货 (EXW) DigiCert 的交货点 – Incoterms 2010。当 HSM 在 DigiCert 的交货点被交付给承运商时，HSM 即完成交付。运费条款必须是运费到付或第三方代收。
    - 如果客户选择通过 DigiCert 购买 SHM（“客户 HSM”）并且将客户 HSM 存储在 DigiCert 的数据中心，那么客户 HSM 将按照与 DigiCert 自己的 HSM 相同的方式给予保存并受到保护。若 DigiCert 提供给客户的适用服务到期或结束，在客户的请求下，DigiCert 将根据业界最佳实践将客户 HSM 转交给客户。客户 HSM 的转交不会收取客户费用，但是如果客户申请与客户 HSM 转交有关的技术支持，DigiCert 将根据双方达成一致的单独工作说明书提供转移支持。
- DigiCert 通过 DigiCert PKI Platform 提供以下类型的**证书**或**座席**：
  - **用户座席：**颁发给人类订阅者的证书，当用户通过 VPN/WiFi 访问专用网络时对用户进行认证。在此类*“用户座席”*下颁发的证书，允许向用户颁发多种数量和不同类型的用户证书（用户座席池中的 VPN、WiFi、SMIME 等）。一个*用户座席*意味着颁发给一个唯一的用户多个数量的证书。
  - **设备座席：**作为订阅者颁发给设备（如笔记本电脑、电脑、LTE 设备等），允许此类设备访问专用网络。与*用户座席*不同，*设备座席*是指颁发给设备的证书，仅用于一 (1) 台物理设备。
  - **服务器座席：**作为订阅者颁发给企业内部服务器的证书，向请求访问服务器上托管的内部网站的用户或设备验证此类服务器的身份。DigiCert PKI Platform 颁发私有层级服务器证书作为该解决方案的一部分。每个物理或虚拟化服务器都需要一个服务器座席。
  - **组织证书：**作为订阅者颁发给组织或实体的证书，允许身份验证（如在私有代码签名证书情况下）和数字签名（如在组织级 Word 或 PDF 签名情况下）。下面是对*组织证书*的限制。客户不得使用代码签名，或任何其他*组织证书：*(i) 针对或代表除客户组织以外的任何组织；(ii) 进行与证书申请书中提交的客户以外的任何域和 / 或组织名称有关的私钥或公钥操作；(iii) 传播任意类型的恶意或有害内容，包括但不限于会给此类内容接收者造成不便的内容；或 (iv) 将证书公钥对应的私钥控制权或访问权转交给客户授权员工以外的人员（此类转交采用安全的方式，从而保护私钥的安全）。

DIGICERT 的义务

- 在完成必要的安装后，DigiCert 将为客户提供本服务说明中指定的服务。
- DigiCert 将根据客户及其 PKI Platform 管理员提供的说明颁发、管理、撤销和/或续订证书。
- 当客户批准证书申请后，DigiCert：(1) 有权依赖于每份经过批准的证书申请书中的信息准确性；且 (2) 为每个提交证书申请的证书申请者颁发证书。
- 根据本服务说明颁发或授权的证书，包括管理员证书，自颁发之日起将具有最长十二 (12) 个月的操作期。
- 在单次 CA 密钥生成事件中，DigiCert 会为客户生成 CA 密钥对，用于签署在 DigiCert Trust Network 或客户选择的其他层级中代表客户签署 DigiCert 颁发的证书。
- 每个密钥对的客户 CA 私钥将存储在一个或多个硬件安全模块中。

客户责任

只有当客户提供必要的信息或执行必要的操作，DigiCert 才能履行服务。如果客户不能提供/履行以下责任，DigiCert 履行服务可能会被延迟、受到阻碍或阻止，详见下文介绍。

- 设置启用：客户必须提供必要的信息，DigiCert 才能开始提供服务。
- 充足的客户人员：当 DigiCert 提出合理的请求时，客户必须提供足够的人员，协助 DigiCert 提供服务。
- 客户必须确保：
  - 所有对于颁发证书非常重要、经由客户验证或以客户的名义验证的信息，在所有实质性方面都必须真实准确。
  - 客户批准证书申请不会导致错误颁发；
  - 客户撤销证书符合 DigiCert Trust Network CPS 或 Adobe CPS 的要求（如适用）；
  - 客户已大致遵守 DigiCert Trust Network CPS 或 Adobe CPS 的要求（如适用）；
  - 客户已大致遵守 RA 要求（如适用）；
  - 提供给 DigiCert 的证书信息不会侵犯任何第三方的知识产权（如域名抢注）；
  - 证书申请中的信息（包括电子邮件地址）未用于且将来不会用于任何非法用途；
    - 客户的 PKI Platform 管理员已经（自创建管理员证书时起）且将一直是拥有管理员证书私钥、保护私钥的任何管理密码、PIN、软件或硬件机制的唯一人员，并且未授权人员没有或者将来不会有访问此类资料或信息的权限；
    - 客户将根据本服务说明将管理员证书专用于授权和合法用途；且
    - 客户将不会监控、干涉或反向还原 DigiCert 系统或软件的技术实现，否则视为故意威胁 DigiCert 系统或软件的安全。

帮助和技术支持

DigiCert 的支持和维护承诺请参见知识库中适用的《服务等级协议》。

服务特定条款

无自动续订

虽然与协议内容相反，但 NSL 服务不会自动续订。在 NSL 服务到期前，客户必须联系 DigiCert 或其渠道分销商合作伙伴进行续订。

服务条件

- **管理员证书：**当客户提交管理员证书的证书申请，且 DigiCert 完成管理员证书所需的认证程序后，DigiCert 将处理证书申请。DigiCert 将通知客户准或还是拒绝其管理员证书的证书申请。PKI Platform 管理员使用 DigiCert 提供的 PIN 获取管理员证书，或者通过安装或使用管理员证书表明 PKI Platform 管理员接受管理员证书。当 PKI Platform 管理员获取或安装管理员证书后，PKI Platform 管理员在使用前必须检查其中的信息，如有任何错误，请及时通知 DigiCert。收到此类通知后，DigiCert 可撤销管理员证书并颁发正确的管理员证书。
- **存续：**除了协议中规定的终止条款外，本服务说明和任何适用的 CPS 中的撤销和安全要求在协议或适用的订单文件结束后仍适用，直到颁发的所有证书操作期结束。
- **遵守当地法律：**客户负责确保其在购买、使用或验收 DigiCert 根据本服务说明生成的公钥和私钥对时，遵守客户购买、使用、验收或接收此类密钥对所在司法辖区内适用的当地法律、规则和法规 – 包括但不限于出口和进口法律、规则和法规。
- **审计权：**DigiCert 可以每年最多对客户的程序进行一次审计，从而确保符合本服务说明中的条款。此类审计将在向客户发送合理的书面通知后在工作时间进行，不会对客户的业务活动造成不合理的干涉。客户必须合理地配合 DigiCert 进行此类审计。若审计显示客户违反了服务说明条款条件中的任意条款，则：(1) 客户将支付 DigiCert 进行审计的合理成本；且 (2) 尽管按照上述说明每年仅限一次审计，DigiCert 可以在认为有必要时进行进一步审计，从而确保符合本服务说明中的条款。例行年度审计可以只涵盖上一年进行的活动。
- **使用限制：**颁发给用户的证书不得集成或安装到与适用的证书请求不对应的任何依赖方。每个证书必须只用于此证书类型指定的用途。

- 请参考以下针对具体 CA 层级的其他条件：
  - DigiCert Trust Network– 参见***附录 A***
  - 私营证书颁发机构 – 参见***附录 B***
  - Adobe® 文档签名服务 – 参见***附录 C***
  - LTE 证书服务 – 参见***附录 D***
  - 制造商证书 – 参见***附录 E***
- 任何以软件形式使用的服务组件都须受到软件随附许可协议的制约。如果服务组件没有随附 EULA，则该服务组件须受到知识库中 b-hosted-service-component-eula-eng.pdf 中的条款和条件的制约。针对此类服务组件使用的其他权利和义务应在该服务说明中规定。
- 除非服务说明中明确说明，本服务（包括本文中提供的任何托管服务软件组件）可以使用开源和其他采用单独许可证的第三方资料。请访问以下网址参见适用的第三方通知（如果适用）https://www.websecurity.symantec.com/legal/repository#managed-pki-service。
- DigiCert 可随时更新本服务，以便保持服务的有效性。
- 本服务可以在全球范围内访问和使用，须根据当时最新的 DigiCert 标准遵守适用的出口合规性限制和技术限制。

评估许可证

如果客户出于评估目的访问本服务，则这些条款和条件适用。

- **使用权利。**授予客户的许可仅限于内部、非商业、非生产评估和服务的互操作性测试用途。客户不得将该服务用于其他目的。
- **评估期。**授予客户的许可证有时间限制，持续到客户登记评估许可证时指定的试用结束日期（“评估期”）。除非客户购买本服务的商用许可证，否则授予客户的许可证在评估期到期时终止。
- **终止后。**客户必须在到期时停止使用本服务。终止使用并不能解除任何一方在终止日期前产生的任何义务。根据性质在终止、取消或到期时仍存续的条款仍将适用。
- **责任范围。**在任何情况下，DIGICERT 都不承担任何损害赔偿，包括但不限于，任何财政收入损失、利润损失或间接损害（即使是已经就其可能性提供了建议）。

- **免责声明。**如果本服务包含 DIGICERT 尚未公开宣布其通用适用性的技术，本服务可能无法达到最终通用产品所能实现的水平。在发布第一个商用版本前（如有），本服务可能无法正确运行，且有可能进行重大修改。双方确认根据且出于评估目的提供给客户的服务或软件“按原样”提供，且不包含任何保修服务。DIGICERT 拒绝承担任何明示、暗示或法定的保证，包括但不限于任何暗示的商品性能保证、对于特定用途的适用性，或不侵犯第三方权利。双方进一步确认本服务说明仅用于说明本服务和任何声明、保证、服务等级承诺等的目的。DIGICERT 特此公布对此类承诺、义务或责任的免责声明。DIGICERT 代理或员工均无权修改、扩展该保证条款或向其中增加内容。
- **优先顺序。**在用于评估目的时，若本部分内容与协议中的任何条款存在冲突，应以本部分为准，并将取代与本服务相关的此类其他条款。

MICROSOFT AUTO ENROLLMENT 的使用

如果您使用 DigiCert PKI Platform 的 Microsoft Auto Enrollment 组件，那么下列 MICROSOFT 必要的补充义务将适用：

(a) **免责条款。**MICROSOFT 及其附属机构未作出与此处提供的服务软件（“服务软件”）有关的任何明示、暗示或法定的保证，且不对其性能或性能故障承担责任。对于 MICROSOFT，服务器软件按包含所有缺陷的原样提供，MICROSOFT 及其附属机构特此声明，不作任何其他明示、暗示或法定的保证、责任和条件，包括但不限于所有与服务器软件有关的任何（若有）暗示保证、适销性条件、特定用途的适用性、可靠性或可用性。此外，MICROSOFT 及其附属机构不作出与服务软件有关的任何保证或权利条件、保密权、描述一致性或不侵权的保证。

(b) **特定损害赔偿除外。**在适用法律允许的最大范围内，MICROSOFT 在任何情况下均不对任何特殊、偶然、惩罚性、非直接或间接的损害赔偿承担责任（包括但不限于利润损失或机密或其他信息的损害赔偿，对于业务中断、个人伤害、隐私损失，未能履行任何义务，包括良好的信誉、合理注意义务，对于疏忽，以及任何其他应罚款或任何其他损失（由此引起或与之相关的任何其他方式）使用或无法使用服务器软件，提供或未能通过服务器软件提供支持或其他服务、信息、软件和相关内容，或者原因是使用服务器软件或与使用任何服务说明条款和条件相关，即使在出现故障、侵权行为（包括疏忽）、严格赔偿责任、违反合同或违反微软保修期的情况下，即使是 MICROSOFT 已被告知此类损害的可能性时也是如此。

(c) **服务器软件要求。**客户只能使用本软件随附文档中指定的服务器软件的一 (1) 份副本（除非在适用的服务订单或工作说明书中另有规定），并且只能与本机 Microsoft Windows 2000 Professional、Windows XP Home 或 Professional，或 Vista 客户端操作系统（或其任何后续版本）进行互操作或通信。客户不得在任何情况下在个人电脑上使用服务器软件。鉴于上述目的，**“个人电脑”** 是指配置的任何电脑，主要用途是一次由一个人使用并使用视频显示器和键盘。

(d) **第三方受益人。**尽管协议中可能存在不一致的条款，客户特此同意 Microsoft Corporation，作为服务器软件中包含的知识产权的许可方，是此类服务说明条款和条件的第三方受益人，有权执行影响 Microsoft 知识产权或其他 Microsoft 利益相关的条款。

(e) **服务器 2 级。**如果客户选择了服务器 2 级，则可选择在具备以下条件的服务器上使用服务器软件 (a) 包含不超过四 (4) 个处理器，其中每个处理器最多为三十二 (32) 位和四 (4) 千兆字节的 RAM，及 (b) 无法添加、更改或移除内存，无需重新启动运行所在的服务器（“**热插拔功能**”）。客户不能将服务器软件与支持**热插拔功能**或集群功能的任何软件配合使用，其中“集群功能”是指能够允许一组服务器用作一个高可用性平台，从而利用组中服务器节点之间的应用失效转移运行应用。

(f) **审计权。**DigiCert 可在至少提前十四 (14) 天通知客户的情况下，在客户场所的正常工作时间内对客户进行审核并检查客户的设施和程序，以验证客户是否遵守了本协议的所有条款和条件。尽管本协议可能存在不一致的条款（包括但不限于任何保密条款），如果客户拒绝接受此类审核且 DigiCert 有理由相信客户可能不遵守服务说明的条款和条件，则客户同意 DigiCert 可能会向 Microsoft 透露客户的身份以及 DigiCert 认为其不合规的基本信息。

(g) **多工设备。**减少直接访问用户数量或使用服务器软件所提供服务用户数量的软硬件，不会减少视为访问的用户数量或使用服务器软件所提供服务的用户数量。访问或使用服务器软件的用户数量等于直接访问或通过多工设备访问或使用 (a) 服务器软件或 (b) 任何其他软件或系统提供的服务的用户数量。此类软件或系统通过服务器软件（“**其他经过认证的系统**”）进行身份验证或授权。本文所用 “**多工设备**” 是指具有以下功能的任何软硬件：通过更少数量的连接直接或间接提供或获取，服务器软件所提供服务的访问权限，或任何其他认证系统提供或代表多个其他用户所提供服务的访问权限。

(h) **Windows CAL 要求。**针对直接访问或使用、通过多工设备访问或使用服务器软件或任何其他认证系统所提供服务的每个用户，客户必须获取并指定单独的 Windows CAL。“**Windows CAL**”是指 (a) a Windows 设备客户端访问许可（“**CAL**”）或 Windows 用户 CAL，均适用于 Microsoft Windows Server 2003（标准版、企业版、或数据中心版）服务器操作系统产品（或任何更新版本）（“**Windows 服务器**”）；或者 (b) 为个人或电子设备提供访问和使用 Windows Server 权限的 Microsoft Core CAL，在上述 (a) 或 (b) 情况下，客户均已获取一个或多个此类 Microsoft Windows 服务器操作系统或电子设备，以单个用户或单个设备的形式使用。

服务等级协议。

DigiCert 的服务可用性承诺请参阅知识库中适用的《服务等级协议》。

定义

本服务说明中使用的大写术语，以及未在协议或本服务说明中定义的术语具有以下意义：

“管理员证书” 是指由 DigiCert 颁发给客户员工或指定为 PKI Platform 管理员的此类其他受信任人员的证书，仅用于访问 PKI Manager 以履行管理员职能的用途。

[对于附录 D – 仅限 LTE 证书服务] “管理员证书” 是指由 DigiCert 颁发给客户任命的 PKI Platform 管理员或指定为 PKI Platform 管理员的此类其他受信任人员的客户端证书，用于访问 PKI Manager 以管理终端实体 LTE 证书或制造商证书的用途。

“附属个体” 是指附属于客户的个人：(1) 作为客户组织内的官员、主管、员工、合作伙伴、分包商、实习生或其他个人；(2) 作为维持与客户组织合同关系的个人，其中客户有提供此人的有力身份保证的商业记录。

“CA 证书” 是指颁发给证书颁发机构 (CA) 的数字证书。

“证书” 或 **“数字证书”** 是指至少包括颁发证书的 CA 的名称或身份、用户、用户的公钥、证书的操作期、证书序列号以及颁发证书的 CA 的数字签名的数字记录。

“证书申请人” 是指申请 CA 颁发证书的个人或组织。

“证书申请” 是指证书申请人 (或授权代理) 向 CA 申请颁发证书。

“证书颁发机构” 或 **“CA”** 是指授权颁发、暂停或取消证书的个人或实体。“证书管理协议” 或 “CMP” 是指 LTE 或制造商证书自动登记和生命周期管理的协议。设备通过 CMP 直接与 DigiCert PKI 系统连接。允许设备向 DigiCert PKI 系统发送 CMP 请求之前，必须由 PKI Platform 管理员对设备进行预授权。

“认证操作规范” 或 **“CPS”** 是指不时进行修订的文档，表示 CA 或 RA 在颁发证书时所采用的操作规范。DigiCert Trust Network CPS 和 Adobe CPS 发布在 DigiCert 网站的知识库中。

“客户” 是指使用服务的实体。

“错误颁发” 是指 (a) 证书的颁发很大程度上不符合适用的 CPS 要求的程序; (b) 向除证书主体以外的其他个人、实体或对象颁发证书；或 (c) 在命名为证书主体的个人、实体或对象没有授权的情况下颁发证书。

“终端用户许可协议” 或 **“EULA”** 是指软件随附的条款条件。

“密钥生成” 是指 DigiCert 通过值得信赖的流程正常生成客户 CA 公钥和私钥，并存储私钥和相关文件的程序。

“LTE 证书” 是指存储在设备中的消息，包括名称、颁发证书的 CA，或运营商网络中的网元。网元可能是运营商基站或安全网关或其他类似设备。在任何情况下，LTE 证书都包含网元的公钥、证书的操作期、证书序列号，以及颁发证书 CA 的数字签名。

“PKI Platform 管理员” 是指注册证书机构的员工或授权执行 RA 工作的其他受信任个人。

[对于附录 D – 仅限 LTE 证书服务] “PKI Platform 管理员” 是指履行《服务说明》中所述某些证书相关管理职能的客户或附属机构的受信任员工。

“制造商” 是指进行设备分销和销售的商务实体。

“制造商证书” 是指颁发在制造时颁发给或嵌入到设备上的证书，通常有 35-40 年的长使用寿命，并且不需要撤销机制。

“操作期” 是指从颁发证书的日期和时间开始 (或者如果证书中明确说明，则可能是稍后的日期和时间) 到证书到期的日期和时间 (或者提前撤销时间) 结束。

[对于附录 D – 仅限 LTE 证书服务] “操作期” 是指从颁发证书的日期和时间开始，到证书到期的日期和时间结束。

“运营商” 是指客户子公司商务实体 (通常是位于另一个国家或地区) 并被 DigiCert 视为该客户的子账户。

“私有层级” 是指证书颁发机构颁发证书是在 DigiCert Trust Network 以外的其他层级，以及由一个 CA 系统组成的域中。这个 CA 系统根据客户的实践在一个链中颁发证书，从客户的根 CA 经过一个或多个 CA，再到用户。在私有层级颁发的证书旨在满足授权颁发证书之企业的需求，并适不用于通过公共渠道进行企业和 / 或个人之间的交互。

“私钥” 是指用于创建数字签名，并根据算法，通过相应的公钥来解密经加密的 (为确保机密性) 消息或文件的数学密钥 (由持有者保持机密性)。

“公钥” 是指可以公开的数学密钥，用于验证通过相应私钥创建的签名。根据算法，公钥也可以用于加密消息或文件，然后通过相应的私钥解密。

“注册证书机构” 或 **“RA”** 是指执行证书申请人的身份验证和认证，启动或传输证书撤销请求，或审批证书续约或密钥更新申请的实体。RA 不是证书申请人的代理。RA 不会委托机构审批提交给除 RA 授权 PKI Platform 管理员以外的证书申请。

“依赖方” 是指依赖证书和 / 或数字签名的个人、实体或对象。依赖方可以是或者不是用户。

“知识库” 是指在 https://www.websecurity.symantec.com/legal/repository 上维护的一系列文档，用于遵守适用的 CPS。

“根 CA” 是指受信任层级域中的顶级实体，根 CA 可用 “根证书” 标识。

“座席” 是指为服务的授权终端用户的单个用户，与实际颁发给该用户的证书数量无关。

“服务组件” 是指软件，按照服务的要求，必须安装在每个客户计算机上，以便接收服务。服务组件包括可能被 DigiCert 作为服务的一部分单独提供的软件和相关文档。

“软件” 是指每个 DigiCert 或许可颁发方软件程序，由 DigiCert 通过对象代码的形式授权给客户，并受随附 EULA 条款或《服务说明》(如适用) 的制约，包括但不限于本文提供的新版本或更新。

“用户” 是指已经颁发证书的主体的个人、实体或对象，用户能够使用且被授权使用颁发时证书中列出的公钥对应的私钥。

“用户协议” 是指用户与 CA 或 DigiCert 之间执行的协议，协议是关于与指定证书相关服务的条款，管控用户与证书相关的权利和义务。DigiCert Trust Network 用户协议发布在 DigiCert 网站的知识库中。

“订阅工具” 是以下一份或多份适用的文档，其进一步定义与本服务有关的客户权利和义务：Digicert 颁发的 DigiCert 证书或类似文档，或客户与 DigiCert 之间的书面协议，随服务一起交付，或在服务之前或之后交付。

“DigiCert Trust Network” 是指受 DigiCert Trust Network CPS 管控的基于证书的公钥基础架构，支持在全球由 DigiCert 及其附属机构，以及对应的客户、用户和依赖方部署和使用证书。

“受信任的个人” 是指负责管理客户、其产品、服务、设施和/或实践做法的基础架构信赖度的员工、分包商或客户顾问。

附录

附录 A: DigiCert Trust Network (DigiCert Trust Network)

DigiCert PKI Platform 为客户提供从 DigiCert Trust Network 颁发证书的能力。DigiCert 已经与各个硬件和软件供应商合作，将 DigiCert Trust Network 主要证书颁发机构 (PCA) 嵌入到最受欢迎的网络浏览器、电子邮件应用、操作系统以及网络设备。因此，一个 PCA 中的证书自动受到这些应用的信任。这些证书通常用于组织之间，无需管理员或用户进行任何特殊的准备。例如，很多客户使用 DigiCert Trust Network 证书确保电子邮件的安全，它可用于对电子邮件进行数字签名和/或加密。

选择 DigiCert Trust Network 作为证书颁发机构 (CA) 的客户被自动分配一个属于 2 级 PCA 的颁发证书 CA，作为账户设置的一部分。如果客户希望采用另一个注册商标名称或更改 CA 中的任何默认值，该客户可以购买选件，从而创建更多 CA。

说明：客户和用户必须遵循 DigiCert Trust Network 证书操作规范 (CPS) 来颁发、管理和使用这些证书。

更多服务条件 – 仅适用于 DigiCert Trust Network

任命。DigiCert 特此根据 DigiCert Trust Network CPS 委派客户作为 DigiCert Trust Network 内的非 DigiCert CA，并且客户接受此任命。

DigiCert Trust Network CPS。除了根据本服务说明外包给 DigiCert 的功能，客户必须满足 DigiCert Trust Network 内的所有要求并且履行强加于 CA和/或RA 的所有义务，包括但不限于 DigiCert Trust Network CPS（会定期修订）。DigiCert 将通过张贴信息给 PKI Manager，通知客户任命的 PKI Platform 管理员有关任何修订。

任命。客户必须任命一个或多个授权客户员工或受信任的个人作为 PKI Platform 管理员。此类 PKI Platform 管理员必须有权代表客户任命更多的 PKI Platform 管理员。客户必须引导 PKI Platform 管理员接收相应的证书，以遵守适用用户协议的条款。

管理员职能。客户必须遵守 DigiCert Trust Network CPS（会定期修订）中说明的要求，包括但不限于，使用 DigiCert 指定的硬件和软件验证证书申请中的信息、批准或拒绝此类证书申请，以及撤销证书的要求。客户必须以合格、专业、技巧熟练的方式执行此类任务。只有当证书申请人是客户的附属个人时，客户才能批准证书申请。如果某个订阅者已经获得由客户颁发的证书，停止作为客户的附属个人，那么客户必须通过 PKI Manager 及时申请撤销此用户的证书。如果某个 PKI Platform 管理员不再被授权作为代表客户的 PKI Platform 管理员，那么客户必须及时申请撤销该 PKI Platform 管理员的管理员证书。

客户的用户。客户必须终止让用户接收证书，以便遵守适用用户协议的条款，他们必须同意后者作为登记证书的条件。客户将确保此类用户协议必须是保护度不低于 DigiCert Trust Network CPS 中 CA 的 CA。

DigiCert 的保证。DigiCert 保证：(i) 证书信息中不存在因为 DigiCert 在创建证书时的疏忽而造成的错误；(ii) 其证书颁发在

所有重要方面都符合 DigiCert Trust Network CPS；且 (iii) 其撤销服务和知识库的使用在所有重要方面都符合 DigiCert Trust Network CPS。

附录 B：私有证书颁发机构

DigiCert PKI Platform 为客户提供从私有证书颁发机构 (CA) 颁发证书的能力。DigiCert 执行正式、安全的程序，为该 CA 创建私钥 / 公钥，称为密钥仪式。这些证书通常用于控制组织资源的访问权。例如，很多客户仅信任其私有 CA 可访问其专用网络（通过 VPN 或 WiFi），以便阻止对其网络的非授权访问。

每个客户被自动分配一个私有证书颁发机构 (CA)，作为账户设置的一部分。该客户是基于提供给 DigiCert 的经过审查的客户法律实体名称，用于设置账户。如果客户希望采用该组织注册的另一个商标名称（比如品牌名称与法律实体名称）或更改 CA 中的任何默认值，客户可以狗哦买选件，从而创建更多 CA。

说明：客户负责定义和遵守其自己的证书操作规范 (CPS)，后者管控适用的私有 CA 对证书的颁发、管理和使用。

更多服务条件 - 仅适用于私有证书颁发机构

任命。客户必须任命一个或多个授权客户员工或受信任的个人作为 PKI Platform 管理员。此类 PKI Platform 管理员必须有权代表客户任命更多的 PKI Platform 管理员。客户必须引导 PKI Platform 管理员接收相应的证书，以遵守适用用户协议的条款。

管理员职能。客户必须通过其 PKI Platform 管理员使用 DigiCert 指定的硬件和软件，验证证书申请中的信息、批准或拒绝此类证书申请，并指导 DigiCert 颁发、续订和撤销证书。如果某个 PKI Platform 管理员不再被授权作为代表客户的 PKI Platform 管理员，那么客户必须及时申请撤销该 PKI Platform 管理员的管理员证书。

DigiCert 的保证。DigiCert 保证证书信息中不存在因为 DigiCert 在创建证书时的疏忽而造成的错误。

附录 C: Adobe® 文档签名服务

DigiCert PKI Platform 让客户能够从 Adobe® 文档签名服务颁发证书。DigiCert 已经与 Adobe 合作，能够自动颁发受 Adobe Acrobat®、Reader® 和 LiveCycle® 产品信任的证书。这些证书用于在产品中对可移植文档格式 (PDF) 进行数字签名。

选择 Adobe 为证书颁发机构 (CA) 的客户被自动分配一个属于赛门铁克用于 Adobe 文档签名服务的中级证书颁发机构，作为账户设置的一部分。该客户是基于提供给 DigiCert 的经过审查的客户法律实体名称，用于设置账户。如果客户希望采用该组织注册的另一个商标名称（比如品牌名称与法律实体名称）或更改 CA 中的任何默认值，客户可以狗哦买选件，从而创建更多 CA。

说明：客户和用户必须遵循 Adobe CDS 证书操作规范 (CPS) 或 Adobe ATL CPS（如适用）来颁发、管理和使用这些证书。

对于 AATL，客户可以在 SHA256 与 ECC 之间选择。

更多服务条件 – 仅适用于 Adobe® 文档签名服务

任命。客户必须任命一个或多个授权客户员工或受信任的个人作为 PKI Platform 管理员。此类 PKI Platform 管理员必须有权代表客户任命更多的 PKI Platform 管理员。客户必须引导 PKI Platform 管理员接收相应的证书，以遵守适用用户协议和 CPS 的条款。

管理员职能。客户必须，通过其 PKI Platform 管理员使用 DigiCert 指定的硬件和软件，验证证书申请中的信息、批准或拒绝此类证书申请，并指导 DigiCert 根据 CPS 颁发、续订和撤销证书，发布在 PKI Manager 并会不时修订。如果某个 PKI Platform 管理员不再被授权作为代表客户的 PKI Platform 管理员，那么客户必须及时申请撤销该 PKI Platform 管理员的管理员证书。

客户的用户。客户必须终止让用户接收证书，以便遵守适用用户协议的条款，他们必须同意后者作为登记证书的条件。客户将确保此类用户协议必须是保护度不低于 CPS 中 CA 的 CA。

DigiCert 的保证。DigiCert 保证证书信息中不存在因为 DigiCert 在创建证书时的疏忽而造成的错误。

附录 D: LTE 证书服务

DigiCert LTE Base Station 服务（“LTES” 或 “服务”）让客户能够获取私有层级中设备证书，从而集成到运营商 LTE 设备。客户或其运营商通过编程接口比如证书管理协议 (CMP) 向 DigiCert 提交 LTES 申请。

更多服务条件 – 仅适用于 LTE 证书服务

任命。客户必须任命一个或多个授权客户和/或运营商员工作为聘用此类人员实体的 PKI Platform 管理员。客户必须要求 PKI Platform 管理员接收相应的管理员证书，以遵守与此类证书相关的适用用户协议的条款，并根据本服务说明，将 PKI Platform 管理员证书专用于授权和合法目的。如果某个用户不再被授权作为 PKI Platform 管理员，那么客户必须及时申请撤销适用管理员证书。

管理员职能。客户和/或其运营商，如适用，必须通过任命的 PKI Platform 管理员负责：

1. 创建运营商子账户；
2. 创建证书配置文件；
3. 提供制造商 CA 证书；
4. 提供 IP 地址块进行验证；
5. 注册新设备并为未来的请求设置预先批准；和
6. 在网元上配置 CMP 应答器 URL。

账户授权和证书颁发。客户必须向 DigiCert 预先提任何运营商的书面授权，从而接收颁发的 LTE 证书，包括此运营商的联系信息、指定为该运营商 PKI Platform 管理员的个人的身份信息（包括登记信息），以及 LTE 证书数量和每个运营商授权的网站。客户必须要确保并要求其运营商确保每个 PKI Platform 管理员已经（自适用的 PKI Platform 管理员证书创建之时起）并且将一直是拥有此证书私钥、保护私钥的任何 PIN、软件或硬件机制的唯一人员，并且未授权人员没有或者将来不会有访问上述资料或信息的权限。

当 PKI Platform 管理员通过 PKI Manager 提交证书申请后（申请的证书数量由上述客户授权），DigiCert 有权 (i) 依赖每个证书请求中信息的准确性，且 (ii) 向申请的 PKI Platform 管理员颁发和提供此类证书。根据本服务说明颁发或授权的设备证书具有自证书颁发之日起一 (1)、二 (2) 或 三 (3) 年的有效期。DigiCert 将履行所有满足已收到订单中所有限制要求的订单。尽管条款可能存在不同，但可以申请证书的运营商数量，以及借以申请证书的生产网站和 PKI Platform 管理员数量都必须严格限制为适用订单文档中规定的数量。

制造商细分义务。客户不得监控、干涉或反向还原任何 DigiCert 系统或软件的技术实现，否则视为故意威胁 DigiCert 系统或软件的安全，而且必须对其任命的制造商施加相同的限制。

CA 证书。尽管与本服务说明的内容相悖，DigiCert 仍将根据 DigiCert 的标准 PKI 实践和策略，创建和托管两 (2) 个客户根证书，并且可以在每个根证书下选择最多颁发两 (2) 个 CA 证书，而 CA 证书仅用于为相应客户提供服务。如果需要更多 CA 证书，需要单独购买。DigiCert 将根据标准的 PKI 实践和策略，登记运营商并根据客户的请求为他们创建子账户。

IP 地址配置。作为新运营商登记的一部分，必须向 DigiCert 提供一系列有效的 IP 地址。DigiCert 的系统只会响应有效 IP 地址的 CMP 请求，非已配置 IP 地址的任何其他请求都会被拒绝。该配置必须由运营商执行。

账户激活。在提前购买后，DigiCert 将尽合理的商业化努力，在满足以下要求时，在十 (10) 个工作日内激活美国境内的子账户，在合理的商业时段内激活美国以外的账户：(i) 完成必要的登记流程；且 (ii) 完成运营商及其 PKI Platform 管理员的认证。此类 PKI Platform 管理员必须在这一时间段内可以联系到，以便允许 DigiCert 及时进行认证。

DigiCert 的保证。DigiCert 保证颁发的证书中不存在因为 DigiCert 在创建证书时的疏忽而造成的错误。

附录 E：制造商证书

DigiCert PKI Platform 为客户提供颁发私有层级制造商证书的能力，从而集成到制造商的具体的生态系统设备中。制造商证书用于设备认证或用于加密从设备发送的消息。客户使用批量接口，向 DigiCert PKI Platform 申请制造商证书。

更多服务条件 – 仅适用于制造商证书

任命。客户必须任命一个或多个授权客户员工，作为聘用此类人员实体的 PKI Platform 管理员。客户必须要求 PKI Platform 管理员接收相应的管理员证书，以遵守与此类证书相关的适用用户协议的条款，并根据本服务说明，将管理员证书专用于授权和合法目的。如果某个用户不再被授权作为服务管理员，那么客户必须及时申请撤销适用管理员证书。

管理员职能。客户和/或其运营商，如适用，必须通过任命的 PKI Platform 管理员负责：

1. 创建子账户；
2. 创建证书配置文件；
3. 提供制造商 CA 证书；且
4. 批量提交证书颁发请求。

制造商细分义务。客户不得监控、干涉或反向还原任何 DigiCert 系统或软件的技术实现，否则视为故意威胁 DigiCert 系统或软件的安全，而且必须对其任命的制造商施加相同的限制。

证书颁发。在服务管理员通过 PKI Manager 提交一批证书请求后，DigiCert 有权 (i) 依赖每个证书请求中信息的准确性，且 (ii) 向申请的 PKI Platform 管理员颁发和提供此类证书。DigiCert 将履行所有满足已收到订单中所有限制要求的订单。尽管条款可能存在不同，但可以申请的证书数量将严格限制为适用订单文档中规定的数量。

账户激活若提前购买，DigiCert 将尽合理的商业化努力，在满足以下要求时，在十 (10) 个工作日内激活美国境内的账户，在合理的商业时段内激活美国以外的账户：(i) 完成必要的登记流程；且 (ii) 完成客户及其 PKI Platform 管理员的认证。此类 PKI Platform 管理员必须在这一时间段内可以联系到，以便 DigiCert 及时进行认证。

DigiCert 的保证。DigiCert 保证颁发的证书中不存在因为 DigiCert 在创建证书时的疏忽而造成的错误。

私有根 CA 的必要条款。由于制造商证书在根 CA 的私有层级运行，如果根 CA 是第三方，而不是客户，比如产业联盟或标准设定机构，则 DigiCert 的制造商证书条款可以调整，但客户需要满足根 CA 要求的所有条件，作为接收由 DigiCert 托管的根证书下颁发的制造商证书的前提条件，并且此类制造商证书仅限于在此根 CA 管控的生态系统内使用。此前提条件可以包括，但不限于执行根 CA 指定的任何其他文档。**根 CA 对其生态系统中制造商证书的颁发拥有绝对权威，并且保留指示 DigiCert 不向客户颁发证书的权利。DigiCert 不承担与根 CA 采取行动有关的任何责任。根 CA 保留其在生态系统的每个制造商证书中拥有的所有专有和知识产权。根 CA 拥有的此类权利根据根 CA 指定的文件授权给客户。客户承认并同意，若根 CA 提出请求，DigiCert 需要报告客户的身份和证书的所有销量。**

更多信息

DIGICERT, INC.

2801 Thanksgiving Way, Suite 500
Lehi, Utah 84043
United States
https://www.digicert.com/