# DigiCert PKI Platform
# 服務描述

## 服務概述

DigiCert PKI Platform（「PKI Platform」或「Platform」）為整個憑證生命週期管理提供了靈活的 PKI 平台，以頒發新憑證、續購現有憑證及撤銷不可信賴的憑證。此外，DigiCert PKI Platform 為用來加密電子郵件、檔案系統或其他資料的憑證私密金鑰提供交付和復原功能，以及各種驗證憑證當前狀態的驗證服務，以確保只以可信賴的憑證執行資料加密、文件數位簽署或網路驗證等動作。

**本服務描述（以及任何以參照方式所包含的附件）是任何將此服務描述以參照文件方式併入的協議（統稱為「協議」）之一部分，協議中適用的服務如本服務描述所述並由 DigiCert 提供。**

# 目錄



© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

## 技術/商業功能與性能

### 服務特色

DigiCert PKI Platform 是一種委外管理服務，可大幅降低與內部 PKI 相關的成本。舉例來說，以內部 PKI 部署頒發第一個憑證前，客戶必須取得密碼加密和應用程式伺服器硬體、購買伺服器與用戶端授權，並進行員工培訓。客戶必須建立自己的憑證政策 (CP) 以作為管理 PKI 階層的主要政策聲明，並需建立憑證實務作業基準 (CPS)，對憑證流程與程序及可信任角色和責任加以定義。DigiCert PKI Platform 以頂尖密碼加密與應用程式伺服器硬體為基礎，採用多用戶、高可用性環境設計。此環境由受過專業訓練並通過安全背景加強檢查的工作人員進行全天候監控，並定期接受審核以維持 WebTrust 和 SOC-2 認證。

- DigiCert PKI Platform 可建立和管理**憑證授權中心 (CA)** 階層。
  - DigiCert PKI Platform 適用以下標準 CA 階層：
    - DigiCert Trust Network– 參閱***附錄 A***
    - 私人憑證授權中心 – 參閱***附錄 B***
    - Adobe® 文件簽署服務 – 參閱***附錄 C***
    - LTE 憑證服務 – 參閱***附錄 D***
    - 製造商憑證 – 參閱***附錄 E***
  - 在每個服務帳戶中，每個所選 CA 階層都至少會有一個 CA 憑證。指定數量的額外 CA 憑證可於日後進行購買。任何 DigiCert 系統與服務的 CA 憑證摘錄和/或相關金鑰組皆需遵守雙方協議。
- DigiCert PKI Platform 提供雲端型與混合型兩 (2) 種部署模式，以**管理憑證生命週期**。
  - 雲端型部署模式將帳戶、憑證與金鑰管理工具託管在 DigiCert 的資料中心；
  - 混合型部署模式也將所有帳戶、憑證與金鑰管理工具託管在 DigiCert 資料中心，但此模式另外會在客戶資料中心安裝憑證註冊中心 (RA) 和目錄整合工具。
  - 部署模式並非專有，可依各種 PKI 專業需求採用不同部署模式組合。兩種部署模式都可與電腦中介軟體 PKI Client 搭配運作，大幅改善憑證生命週期使用者體驗。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

- DigiCert PKI Platform 提供以下管理工具：
  - **PKI Manager** – PKI Manager 是託管在 DigiCert 資料中心的入口網站，讓 PKI 管理者能夠執行與帳戶、使用者、憑證和金鑰管理相關之任務。
    - **帳戶管理：**PKI Manager 讓 PKI 管理員能夠查看憑證授權中心 (CA)、基座數和帳戶相關報告。PKI Manager 也允許 PKI 管理員建立和指派責任給其他 PKI 管理員。
    - **使用者管理：**PKI Manager 允許 PKI 管理員新增使用者、撤銷使用者、為每個使用者產生獨特註冊代碼，並自訂發送給使用者的電子郵件通知。PKI Manager 也能夠為使用者提供文件與影音指示來進行協力廠商應用程式設定，以和新頒發的憑證搭配運作。
    - **憑證管理：**PKI Manager 讓 PKI 管理員能夠為帳戶中不同的 CA 設定憑證設定檔。PKI 管理員可設定金鑰大小、金鑰用途和簽署演算法等參數，這些參數屬於憑證設定檔的一部份。PKI 管理員也可選擇使用者體驗 (透過 OS/瀏覽器或 PKI 用戶端註冊) 和安全保護等級。PKI 管理員決定是否要委付憑證的私密金鑰。除了設定憑證設定檔外，PKI Manager 也讓 PKI 管理員可針對因使用者不再需要憑證 (例如使用者離開公司) 或私密金鑰遭到洩漏 (例如使用者遺失筆記型電腦) 而不可信賴的憑證進行撤銷。
    - **金鑰管理：**PKI Manager 可提供 PKI 管理員加密憑證私密金鑰的復原功能。
  - **PKI 憑證服務** – PKI 憑證服務將憑證註冊網頁託管在 DigiCert 資料中心，供使用者 (也稱為訂閱者) 請求憑證。這些網頁會逐步導引使用者完成請求憑證的必要步驟。此外，網頁可能會顯示 PKI 管理員提供的指令，以進行協力廠商產品設定。
  - **憑證頒發中心** – 憑證頒發中心是託管在 DigiCert 資料中心的憑證引擎。此憑證引擎會根據由 PKI 憑證服務送出、PKI 企業閘道接收，或是透過網頁服務傳送的憑證簽署請求來建立憑證。此憑證引擎會透過頒發憑證授權中心 (CA) 簽署憑證。
  - **PKI 企業閘道** – PKI 企業閘道是視需要安裝於客戶資料中心的憑證註冊中心 (RA) 授權應用程序。此應用程序會與輕量型目錄存取通訊協定 (LDAP) 源 (例如 Microsoft® Active Directory®) 緊密整合，自動核准憑證請求並將憑證資料發佈回 LDAP 源。
  - **PKI Client** – PKI Client 是一種端點中介軟體，設計目的為大幅改善憑證生命週期使用者體驗。PKI Client 適用 Windows 或 MAC 作業系統電腦。在瀏覽器註冊體驗方面，用戶可使用 Microsoft Internet Explorer®、Safari®、Chrome™ 或 Mozilla® Firefox®，從憑證註冊網頁請求憑證。雖然此原生體驗並不需要任何其他軟體，但有已知的使用限制。例如 Microsoft Internet Explorer 會產生許多警告訊息彈出視窗，造成使用者混淆。在 PKI Client 體驗中，憑證生命週期經過簡化，可自動執行常用功能 (即憑證續購) 並盡可能減少使用者操作。PKI Client 也提供集中式策略管理功能 (例如 PIN 和匯出等) 以保護憑證。此外，PKI Client 也能夠對協力廠商產品 (例如無線、虛擬專用網路用戶端等) 進行自動設定，讓其可使用憑證。DigiCert PKI Platform 憑證生命週期

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

管理功能也可於行動裝置上使用，例如利用內建 iOS 空中介面 (OTA) 通訊協定功能的 iOS 裝置，讓 iOS 裝置或應用程序能透過 Apple SCEP 通訊協定進行憑證註冊請求。至於不具 iOS OTA 等效功能的 Android OS 等行動作業系統，DigiCert 提供能夠以類似方式隱藏裝置與應用程式設定複雜性的 PKI Client，來進行憑證使用。

- **PKI 網頁服務** – PKI 網頁服務託管在 DigiCert 資料中心內，可提供以程式設計方式與 DigiCert PKI Platform 進行整合的功能。協力廠商應用程式可透過 PKI 網頁服務所提供的 API，取得憑證政策並執行憑證生命週期功能，例如註冊與續購。

- DigiCert PKI Platform 提供以下幾種**驗證方式：**
  - **使用註冊代碼進行驗證** – 透過這種驗證類型，PKI 管理員可以為每個使用者產生一組獨特的註冊代碼，以自動核准憑證請求。當 PKI 管理員將內含憑證註冊網頁連結的憑證邀請送給使用者時，會連同該使用者的獨特註冊代碼一起寄出。使用者便可在憑證註冊網頁提供註冊代碼與任何其他資訊。憑證頒發中心會將此註冊代碼與 PKI Manager 中產生的資訊進行比對。如果兩者相符，憑證頒發中心就會頒發憑證。如果使用者輸入的註冊代碼與產生給該名使用者的資訊不符，憑證頒發中心會傳送錯誤訊息給使用者。
  - **自動驗證** – 自動驗證根據 LDAP 源 (即 Microsoft Active Directory) 中的資料來核准憑證請求。客戶資料中心必須安裝 PKI 企業閘道，並且需與 LDAP 源整合。當使用者透過用戶 PKI 憑證服務提交憑證請求時，PKI 企業閘道會將憑證請求中的資料與 LDAP 源進行比較。如果資料相符，PKI 企業閘道會核准憑證請求，並以憑證註冊中心 (RA) 憑證，簽署憑證請求，再將簽署完畢的憑證請求傳送到憑證頒發中心。否則 PKI 企業閘道會拒絕憑證請求。
- DigiCert PKI Platform 提供以下**憑證驗證工具：**
  - **憑證撤銷清單 (CRL)** – 許多協力廠商產品都能夠透過憑證撤銷清單 (CRL) 來檢查憑證當下狀態 (例如使用中、撤銷等)。CRL 是尚未到期就被撤銷的憑證黑名單。可設定此類產品來定期下載和檢查最新 CRL。如果憑證在 CRL 中出現，這類產品便會拒絕存取 (例如不會進行網路驗證、數位簽署文件等)。DigiCert 至少每 24 小時就會產生新的 CRL。
  - **線上憑證狀態協定 (OCSP)** – 許多協力廠商產品都可透過線上憑證狀態協定 (OCSP) 確認憑證當前的狀態 (例如使用中、撤銷等)。雖然所有經撤銷的憑證都會顯示在 CRL 中，但在憑證撤銷和產生下一次 CRL 間會有時間延遲，以標準 CRL 來說最長可達 24 小時。DigiCert 會在任何改變 (例如撤銷、停用等) 發生後立即更新憑證狀態，並近乎即時的反應在 DigiCert 的 OCSP 工具 Trusted Global Validation (TGV) 中。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

- DigiCert 提供以下**硬體選項**讓 DigiCert PKI Platform 更加完整：
  - **SafeNet® PKI Tokens** – DigiCert 是 SafeNet® 硬體 USB Tokens 的授權經銷商。這些 Tokens 如儲存庫中的保固資訊補充內容所述，隨附三 (3) 年保固。這些 Tokens 符合聯邦資訊處理標準 (FIPS) 140-2 與共同準則標準。
  - **SafeNet® 硬體安全模組 (HSM)** – DigiCert 是 SafeNet® Luna® 硬體安全模組 (HSM) 的授權經銷商，內容包含 Luna® PCI 卡、Luna® SA 網路設備與 Luna® PCM tokens。這些 HSM 也包括韌體或相關軟體 (例如 SafeNet Authentication Client)。這類 HSM 提供一 (1) 年基本保固，另外 DigiCert 也轉售 SafeNet 選配延伸保固計劃，需額外付費。這類 HSM 也符合 FIPS 140-2 Level 2 和共同準則標準。
    - 任何售出 HSM 的所有權將於 DigiCert 出貨後移轉至客戶或由客戶指定的任何一方。所有物品交貨皆採 Ex Works (EXW) DigiCert 起運點 – 國貿條約 Incoterms 2010。前述物品於 DigiCert 運輸點交付給運送人時，HSM 交貨作業即告完成。運費條款必須為運費到付或第三方。
    - 若客戶選擇透過 DigiCert 購買 HSM (「客戶 HSM」)，並將這類客戶 HSM 儲存在 DigiCert 的資料中心，客戶 HSM 便會以與 DigiCert 自身 HSM 相同的方式進行儲存和保護。提供給客戶的 DigiCert 可用服務到期或終止後，DigiCert 會應客戶要求，循業界最佳作法將客戶 HSM 移轉給客戶。客戶不需負擔移轉客戶 HSM 費用，但若客戶要求提供客戶 HSM 移轉之相關技術支援，DigiCert 將根據另外協調並取得雙方共同協議的工作說明書，提供移轉支援。
- DigiCert 透過 DigiCert PKI Platform 提供以下類型**憑證**或**基座**：
  - **使用者基座：**頒發給人類訂閱者的憑證，驗證訂閱者可以使用者身份透過 VPN/WiFi 存取專用網路。在這種*「使用者基座」*下頒發的憑證，允許發行多個及多種類型使用者憑證 (來自使用者基座庫的 VPN、WiFi、SMIME 等) 給使用者。一個*使用者基座*可指頒發給單一專門使用者的多個憑證。
  - **裝置基座：**頒發憑證給裝置 (例如筆記型電腦、電腦、LTE 設備等) 為訂閱者，允許這類設備存取專用網路。與*使用者基座*不同，*裝置基座*是指頒發給一個裝置並且只能在一 (1) 個實體裝置上使用的憑證。
  - **伺服器基座**：頒發給組織內部伺服器訂閱者的憑證，於使用者或裝置要求存取託管在伺服器的內部網路網頁時，確保伺服器的身分。DigiCert PKI Platform 會在此解決方案中頒發私有階層伺服器憑證。每個實體或虛擬伺服器都需要伺服器基座。
  - **組織憑證：**頒發給組織或實體訂閱者的憑證，允許身份認證 (例如在專用代碼簽署憑證的情況下) 以及數位簽章 (如在組織層級進行 Word 或 PDF 簽章)。以下為*組織憑證*的限制。在下列情況下，客戶不得使用代碼簽章或任何其他*組織憑證：* (i) 為或代表客戶組織以外的任何組織；(ii) 執行與提交憑證申請上客戶以外任何網域及 / 或組織名稱相關之私密或公開金鑰操作；(iii) 發佈任何惡意或有害內容，包括但不限於會對內容接收者造成不便的內容；或 (iv) 採用會將憑證公開金鑰之相對應的私密金鑰控制移轉至客戶授權員工以外任何人，或允許其存取的方式 (前述任何移轉都必須採用安全的方式，以保護私密金鑰)。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

## DIGICERT 義務

- 完成必要安裝後，DigiCert 將為客戶提供此服務描述中闡述之服務。
- DigiCert 將根據客戶與其 PKI Platform 管理員所提供的指示頒發、管理、撤銷和/或續購憑證。
- 客戶核准憑證申請後，DigiCert 將：(1) 有權仰賴每個此類核准憑證申請中的資訊準確性；並 (2) 為提交此類憑證申請的憑證申請者頒發憑證。
- 根據本服務描述所頒發或授權的憑證 (包括管理員憑證)，最長使用期限為各憑證頒發日期起十二 (12) 個月。
- 於單一 CA 金鑰產生事件中，DigiCert 將為客戶產生 CA 金鑰組，用來簽署 DigiCert 在 DigiCert Trust Network 或其他客戶選擇之階層中代表客戶頒發的憑證。
- 每個金鑰組的客戶 CA 私密金鑰將會儲存在一個或多個硬體安全模組中。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

## 客戶責任

只有在客戶提供所需資訊或執行所需行動的情況下，DigiCert 才能執行服務。若客戶未能提供/執行以下責任，DigiCert 的服務性能可能會受到延遲、影響或無法使用，如下所述。

- 設定啟用：客戶必須提供 DigiCert 開始提供服務所需的資訊。
- 適當客戶人員：客戶必須依 DigiCert 的合理要求，提供足夠人員協助 DigiCert 提供服務。
- 客戶必須確保：
  - 由或代表客戶所驗證之所有頒發憑證資訊內容均真實無誤。
  - 客戶的憑證申請核可不會導致錯誤頒發；
  - 客戶的憑證撤銷符合 DigiCert Trust Network CPS 或 Adobe CPS（如果適用或視具體狀況而定）；
  - 客戶實際上遵守 DigiCert Trust Network CPS 或 Adobe CPS（如適用或視具體狀況而定）；
  - 客戶實際上遵循 RA 要求（如適用）；
  - 提供給 DigiCert 的憑證資訊不會侵犯任何第三方的智慧財產權（例如網域搶註）；
  - 憑證申請（包含電子郵件信箱）中的資訊未曾用過，也不會用於任何非法用途；
    - 客戶的 PKI Platform 管理員一直是（自建立管理員憑證起），並且仍會是唯一擁有管理員憑證私密金鑰，以及任何保護私密金鑰的查問片語、PIN、軟體或硬體機制之人員，不曾有也不會有未經授權人員存取前述內容或資訊；
    - 客戶僅會將管理員憑證用在與本服務描述一致之授權且合法用途；
    - 客戶不會對 DigiCert 系統或軟體的技術執行進行監控、干擾或逆向工程，也不會故意損害 DigiCert 系統或軟體的安全性。

### 協助與技術支援

DigiCert 的支援和維護承諾於適用之服務層級協議加以說明，可於儲存庫中取得。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

## 服務特定條款

### 不提供自動續購

即使有任何與協議相反之情事，NSL 服務均不會自動續購。客戶必須在 NSL 服務到期之前，聯繫 DigiCert 或其通路經銷商合作夥伴進行續購。

### 服務條件

- **管理員憑證：**客戶提交管理員憑證申請且 DigiCert 完成管理員憑證所需驗證程序後，DigiCert 將處理憑證申請。DigiCert 將通知客戶其管理員憑證申請是否經核准或拒絕。PKI Platform 管理員使用 DigiCert 的 PIN 取得管理員憑證，或是安裝/使用管理員憑證，等同 PKI Platform 管理員接受管理員憑證。PKI Platform 管理員取得或安裝管理員憑證後，PKI Platform 管理員必須在使用前檢視其中資訊，並立即通知 DigiCert 任何錯誤。收到前述通知後，DigiCert 可撤銷管理員憑證並頒發經修正的管理員憑證。
- **有效性：**除本協議中闡明之終止條款外，本服務描述的撤銷與安全要求及任何適用的 CPS 也會在協議或適用訂單文件終止後仍然有效，直到本協議頒發的所有憑證使用期間結束為止。
- **當地法律遵循：**客戶有責任確保客戶對 DigiCert 依本服務描述產生的公開金鑰與私密金鑰之取得、使用或接受方式符合當地適用法律、規則和規範 – 包含但不限於客戶取得、使用、接受或接收前述金鑰組之管轄機關出口和進口法律、規則與規範。
- **審查權利：**DigiCert 每年可對客戶程序進行一次以下審查，以確保符合本服務描述之條款。此類審查將在向客戶發出合理書面通知後於營業時間內執行，並且不會以不合理方式干擾客戶業務活動。客戶必須合理配合 DigiCert 此類審查相關作業。如果審查顯示客戶違反本服務描述條款與條件之任何一項條款：(1) 客戶將支付 DigiCert 執行審查的合理費用，(2) 即使有前述每年一次的審查限制，DigiCert 仍可於其認為合理必要時執行進一步審查，以確保符合本協議條款。例行年度審查可僅涵蓋前一年的活動。
- **使用限制：**任何不符合適用憑證要求之依賴方可能無法整合或安裝頒發給訂閱者的憑證。每個憑證僅可依憑證所指類型用於其預期用途。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

- 請參閱以下 CA 階層特定附加條件：
  - DigiCert Trust Network– 參閱***附錄 A***
  - 私人憑證授權中心 – 參閱***附錄 B***
  - Adobe® 文件簽署服務 – 參閱***附錄 C***
  - LTE 憑證服務 – 參閱***附錄 D***
  - 製造商憑證 – 參閱***附錄 E***
- 以軟體形式使用任何服務元件應受軟體隨附之授權協議約束。如果服務元件未附帶 EULA，則應受儲存庫內 b-hosted-service-component-eula-eng.pdf 之條款與條件約束。其他使用此服務元件之任何相關權利和義務應如本服務描述所述。
- 除非服務描述中另有說明，否則服務（包括隨其提供的任何託管服務軟體元件）可以使用其他授權之開放原始碼與其他協力廠商素材。如果適用，請參閱適用之協力廠商聲明，位置在 https://www.websecurity.symantec.com/legal/repository#managed-pki-service。
- DigiCert 可以隨時更新服務，以維持服務有效性。
- 服務可於全世界進行存取與使用，並需依據當時 DigiCert 標準，遵守適用出口法規限制與技術限制。

**評估授權**

若客戶因評估目的而存取此服務，則適用以下條款和條件。

- **使用權利。**授予客戶的授權僅限依內部、非商業、非生產評估和服務互通性測試之目的使用。客戶不得將本服務用於任何其他目的。
- **評估期。**授予客戶的授權有時間限制，會持續至客戶註冊評估授權時指定之試用結束日期（「評估期」）。除非客戶購買服務的商業授權，否則授予客戶的授權將於評估期滿後終止。
- **終止之後。**客戶必須於終止後停止使用本服務。任何終止都不會解除任何一方在終止日前已產生之任何義務。條款本身性質為於終止、取消或到期後繼續生效者，將持續有效。
- **責任限制。**在任何情況下，即使被告知損害的可能性，DIGICERT 對任何損害（包括但不限於任何收入損失、利潤損失或衍生性損害）概不負責。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

- **免責聲明。**如果服務包含 DIGICERT 尚未公開宣布其一般可用性的技術，服務可能無法達到最終提供產品水準。服務可能無法正常運作，並可能在首次正式發表前進行大幅修改 (若有)。雙方承認根據且為評估目的提供予客戶之服務或軟體係「依現狀」提供，不附帶任何責任保證。DIGICERT 免除任何明示、默示或法定保證，包括但不限於任何適銷性、適於特定用途或不侵犯第三方權利之默示擔保。雙方進一步承認本服務描述僅作描述服務目的之用，DIGICERT 特此聲明對任何陳述、保證、服務等級承諾或其他 DIGICERT 承諾、義務或責任概不負責。未授權任何 DIGICERT 代理人或員工對本擔保進行任何修改、延伸或補充。
- **優先順序。**本節與本協議任何條款如有任何抵觸，將以本節為準並取代與服務相關之其他規定，同時提供評估目的。

## 使用 MICROSOFT AUTO ENROLLMENT

如果您使用 PKI Platform 的 Microsoft Auto Enrollment 元件，則適用以下 MICROSOFT 要求增補義務：

(a) **保證免責聲明。**MICROSOFT 與其附屬機構對依本協議提供之伺服器軟體 (「伺服器軟體」) 不做任何明示、默示或法定保證，並對其性能或無法執行概不負責。對 MICROSOFT 而言，伺服器軟體係依「現狀」及現有故障提供，MICROSOFT 與其附屬機構特此豁免所有明示、默示或法定之其他保證、責任與條件，包括但不限於任何 ( 若有 ) 與伺服器軟體相關之適銷性、適於特定用途、可靠性或可用性之默示擔保與條件。此外，MICROSOFT 與其附屬機構對與伺服器軟體相關之所有權、平靜受益權、與描述一致性或無侵權不作任何相關擔保和條件。

(b) **特定損害之排除。**在適用法律允許的最大範圍內，MICROSOFT 對因使用或無法使用伺服器軟體、透過伺服器軟體提供或不提供支援或其他服務、資訊、軟體與相關內容，而產生或以任何方式相關，或因使用伺服器軟體而產生，或在本服務描述中之任何條款與條件下或相關之任何特殊性、附帶性、懲罰性、間接性或結果性損害 [ 包括但不限於利潤損失或機密或其他因業務中斷、個人傷害、隱私損失、未盡責任 ( 包括善意或合理照顧、過失以及任何其他金錢或其他損失 )] 概不予負責，即使當發生故障、侵權 ( 包括過失行為 )、嚴格責任、違反合約或違反 MICROSOFT 保固，甚至當 MICROSOFT 已被告知該損害之可能性時亦同。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

(c) **伺服器軟體要求。**如本軟體隨附文件說明，客戶僅可使用於本協議條件下提供之一 (1) 個伺服器軟體複本 ( 除非於適用服務指示或工作說明書中另有說明 )，並僅可與原生 Microsoft Windows 2000 Professional、Windows XP Home 或 Professional 或 Vista client 作業系統 ( 或任何後續版本 ) 相互操作或溝通。任何情況下客戶均不得於個人電腦使用伺服器軟體。前述之**「個人電腦」**係指任何經過設定，主要目的為每次供單一個人使用，並使用視訊顯示器與鍵盤之電腦。

(d) **受益第三人。**即使協議中條款有任何不一致，客戶在此同意 Microsoft Corporation 為伺服器軟體中智慧財產之授權人，並為本服務描述條款和條件之受益第三者，有權對任何影響 Microsoft 智慧財產或與本協議條款相關之其他 Microsoft 利益強制執行本協議中之任何條款。

(e) **伺服器類別 2。**若客戶選擇伺服器類別 2，客戶可於符合以下條件之伺服器上使用伺服器軟體：(a) 包含四 (4) 個以下處理器，其中每個處理器最多搭載三十二 (32) 位元和四 (4) GBRAM，且 (b) 無法在伺服器不需重新開機的情況下新增、更改或刪除記憶體 (「**熱插拔功能**」)。客戶不得將伺服器軟體與任何支援**熱插拔功能**或叢集功能之軟體搭配使用，「叢集功能」係指允許伺服器群組透過群組中伺服器節點間的應用程式容錯移轉，而以單一高可用性平台方式執行應用程式的功能。

(f) **審查權利。**DigiCert 可在給予不少於十四 (14) 天通知的情況下，於一般營業時間至客戶機房進行客戶審查並檢查客戶的設施與程序，以驗證客戶遵循本協議中之所有條款和條件。即使本協議條款有任何不一致 ( 包括但不限於任何保密條款 )，若客戶拒絕接受此類審查，且 DigiCert 有理由相信客戶可能未遵守服務描述之條款和條件時，客戶同意 DigiCert 可向 Microsoft 揭露客戶身份以及 DigiCert 相信其違規之基礎。

(g) **多工裝置。**能夠減少直接存取或使用伺服器軟體提供服務使用者數量之硬體或軟體，無法減少被視為存取或使用伺服器軟體提供之服務使用者數。存取或使用伺服器軟體的使用者數，等於直接或透過多工裝置存取或使用由 (a) 伺服器軟體或 (b) 任何其他軟體或系統提供之服務使用者數，此類軟體或系統的認證或驗證由伺服器軟體提供 (「**其他認證系統**」)。此處使用之「**多工裝置**」係指透過較少連接數，為或代表多個其他使用者以直接或間接方式，提供或獲得存取伺服器軟體或任何其他認證系統提供服務之硬體或軟體。

(h) **Windows CAL 需求。**客戶必須為每位以直接或透過多工裝置方式，存取或使用伺服器軟體或其他認證系統提供之服務使用者，取得並使用不同 Windows CAL。**「Windows CAL」**係指 (a) 適用 Microsoft Windows Server 2003 ( 標準版、企業版或資料中心版 ) 伺服器作業系統產品 ( 或任何後續版本 ) (**Windows 伺服器** ) 之 Windows 裝置用戶端存取使用權 (「**CAL**」)，或稱 Windows 使用者 CAL，或 (b) 提供單一個人或電子裝置 Windows 伺服器存取與使用權利之 Microsoft 核心 CAL，客戶以上述 (a) 或 (b) 方式使用一個或以上 Microsoft Windows 伺服器作業系統產品或電子裝置，並以每位使用者或每個裝置為基礎進行使用。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

## 服務等級協議

DigiCert 的服務可用性承諾於適用之服務等級協議進行描述，相關服務等級協議可於儲存庫取得。

## 定義

本服務描述中使用的大寫字詞若未在協議或本服務說明中另行定義，則具以下意義：

**「管理員憑證」**是指 DigiCert 為經指定為 PKI Platform 管理員之客戶員工或其他可信人員頒發的憑證，目的僅為存取 PKI Manager 以執行管理員功能。

**[適用附錄 D – 僅限 LTE 憑證服務]：**「管理員憑證」係指 DigiCert 為客戶指定的 PKI Platform 管理員或被指定為 Managed PKI 管理員的其他可信人員所頒發之用戶端憑證，目的為存取 PKI Manager 以管理終端實體 LTE 憑證或製造商憑證。

**「附屬個人」**係指附屬於客戶之人員：(1) 在客戶組織內擔任管理人員、董事、雇員、合夥人、承包商、實習生或其他人員；或 (2) 與客戶組織保持合約關係之人員，且客戶具備能夠為此人身分提供有力保證的商業紀錄。

**「CA 憑證」**係指頒發給憑證授權中心 ( 或稱 CA) 的數位憑證。

**「憑證」**或**「數位憑證」**係指至少包含頒發 CA 名稱或身份、訂閱者、訂閱者的公開金鑰、憑證使用期間、憑證序號及頒發 CA 數位簽章的數位記錄。

**「憑證申請者」**係指請求 CA 頒發憑證的個人或組織。

**「憑證申請」**係指憑證申請者 ( 或授權代理人 ) 向 CA 提出頒發憑證之請求。

**「憑證授權中心」**或**「CA」**係指經授權頒發、停用或撤銷憑證之個人或實體。

**「憑證管理協定」**或**「CMP」**係指 LTE 或製造商憑證自動註冊與生命週期管理之協定。裝置將透過 CMP 與 DigiCert PKI 系統直接連接。允許裝置向 CMP 發送 DigiCert PKI 系統請求前，必須由 PKI Platform 管理員對裝置進行預授權。

**「憑證實務作業基準」**或**「CPS」**係指經不時修訂，能夠代表 CA 或 RA 頒發憑證實務作業基準之文件。DigiCert Trust Network CPS 與 Adobe CPS 皆發佈於 DigiCert 網站的儲存庫。

**「客戶」**係指使用服務的實體。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

**「錯誤頒發」**係指 (a) 頒發與適用 CPS 所需程序實質上不一致的憑證；(b) 將憑證頒發給與憑證主體名稱不同之個人、實體或物件；或 (c) 未取得與憑證主體名稱相同之個人、實體或物件授權而頒發憑證。

**「使用者授權合約」**或**「EULA」**係指軟體隨附的條款及條件。

**「金鑰產生」**係指透過可靠過程正確產生客戶 CA 公開金鑰與私密金鑰，並儲存本協議私密金鑰和文件的 DigiCert 程序。

**「LTE 憑證」**係指將儲存於裝置中的訊息，包括名稱、頒發 CA 或營運者網路中的網路元素。網路元素可為營運者基地台或安全閘道或其他類似裝置。在所有情況下，LTE 憑證都包含網路元素的公開金鑰、憑證使用期間、憑證序號與頒發 CA 之數位簽章。

**「PKI Platform 管理員」**係指經授權執行 RA 任務之憑證註冊中心員工或其他可信人員。

**[ 適用附錄 D – 僅限 LTE 憑證服務 ]**「PKI Platform 管理員」係指客戶或關係企業中，被指定執行服務描述中所述特定憑證相關管理功能之可信人員。

**「製造商」**係指製造裝置以進行經銷與銷售之商業實體。

**「製造商憑證」**係指頒發給裝置並於製造時嵌入裝置的憑證，生命週期通常可長達 35-40 年，且不需撤銷機制。

**「使用期間」**係指從憑證頒發日期與時間（或於憑證中闡明之較晚日期和時間）開始，至憑證到期日期和時間結束（或因撤銷提早）的期間。

**[ 適用附錄 D – 僅限 LTE 憑證服務 ]**「使用期間」係指自憑證頒發日期和時間開始，至憑證到期日期和時間結束之期間。

**「營運者」**係指客戶附屬機構的商業實體，通常來自其他國家或地區，並由 DigiCert 視為客戶的子帳戶。

**「私用階層」**係指憑證授權中心以 DigiCert Trust Network 外之階層頒發憑證，以及包含一系列 CA 的網域，並根據客戶實務作業，透過一個以上 CA 以鏈狀方式自客戶根 CA 頒發憑證給訂閱者。於私有階層下頒發之憑證旨在滿足組織對頒發進行授權的需求，而非於組織和/或個人間透過公開通道進行互動。

**「私密金鑰」**係指用來建立數位簽章的數學金鑰（由持有者保密），並根據演算法，以相對應的公開金鑰對訊息或加密檔案（提供機密性）進行解密。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

**「公開金鑰」**係指可公開使用之數學金鑰，用來驗證對應私密金鑰建立之簽章。依演算法不同，公開金鑰也可用於加密訊息或檔案，這些訊息或檔案可再由相對應的私密金鑰進行解密。

**「憑證註冊中心」**或**「RA」**係指執行憑證申請者身份驗證與認證、啟動或傳遞憑證撤銷請求，或核准憑證續購或金鑰更新申請之實體。RA 並非憑證申請者的代理人。除了將權力授與 RA 的授權 PKI Platform 管理員外，RA 可不授與核准憑證申請的權力。

**「依賴方」**係指依賴憑證和/或數位簽章之個人、實體或物件。依賴方可以是，也可不是訂閱者。

**「儲存庫」**係指位於 https://www.websecurity.symantec.com/legal/repository 之所有文件，以符合任何適用 CPS 規範為目的進行維護。

**「根 CA」**係指信賴階層網域中最上層實體，並由「根憑證」辨識根 CA。

**「基座」**係指服務授權終端使用者之單一訂閱者，不考慮實際頒發給該訂閱者之憑證數量。

**「服務元件」**係指每台客戶電腦因服務所需而必須安裝之軟體，以便接收服務。服務元件包括由 DigiCert 單獨提供的軟體和相關文檔，以作為服務的一部分。

**「軟體」**係指每個採用物件碼格式的 DigiCert 或授權者軟體程式，由 DigiCert 授權給客戶並受隨附之 EULA 條款或本服務描述（若適用）約束，包含但不限於本協議提供之新版本或更新。

**「訂閱者」**係指為憑證主體，並經頒發憑證之人員、實體或物件，可使用且經授權使用相關憑證所列出與公開金鑰相對應的私密金鑰。

**「訂閱者協議」**係指於訂閱者與 CA 或 DigiCert 間執行，且與指定憑證相關服務條款有關，並規定訂閱者憑證相關權利與義務之協議。DigiCert Trust Network 訂閱者協議於 DigiCert 網站儲存庫中公佈。

**「訂閱方式」**係指下列一個或以上適用文件，這些文件對客戶服務相關權利和義務進行進一步定義：伴隨服務或在服務前後之 DigiCert 憑證或由 DigiCert 發佈之類似文件，或是客戶與 DigiCert 間之書面協議。

**「DigiCert Trust Network」**係指由 DigiCert Trust Network CPS 管理之憑證式公開金鑰基礎架構，允許 DigiCert 與其附屬單位，以及其個別客戶、訂閱者和依賴方，進行全球部署或憑證使用。

**「可信人員」**係指負責管理客戶結構性信賴度、其產品、服務、設施和/或實務作業之客戶員工、承包商或顧問。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

# 附錄

## *附錄 A：DigiCert Trust Network*

DigiCert PKI Platform 為客戶提供自 DigiCert Trust Network 頒發憑證之功能。DigiCert 與軟硬體廠商合作，將 DigiCert Trust Network 主要憑證授權中心 (PCA) 嵌入最常用的網頁瀏覽器、電子郵件應用程式、作業系統與網路設備中。因此，應用程式將自動信任串鏈至這些 PCA 之一的憑證。這些憑證可於組織間用於一般用途，管理員或使用者不需進行任何特別準備。舉例來說，許多客戶採用安全電子郵件 DigiCert Trust Network 憑證來進行數位簽章和/或加密電子郵件。

選擇 DigiCert Trust Network 作為憑證授權中心 (CA) 的客戶在帳戶設定中會自動配置到 Class 2 PCA 的頒發 CA 串鏈。客戶若想要其他商標名稱或更改 CA 中的任何預設值，可以購買選項來建立額外 CA。

註：客戶與使用者必須遵守 DigiCert Trust Network 憑證實務作業基準 (CPS)，以頒發、管理和使用這些憑證。

**其他服務條件 – 僅適用於 DigiCert Trust Network**

**指派。**DigiCert 根據 DigiCert Trust Network CPS，特此指派客戶為 DigiCert Trust Network 中之非 DigiCert CA，客戶亦接受此指派。

**DigiCert Trust Network CPS。**除了在此服務描述下外包給 DigiCert 的功能外，客戶必須滿足定期修訂之 DigiCert Trust Network 對 CA和/或RA 的所有要求並執行所有義務，包括但不限於 DigiCert Trust Network CPS。若有修訂，DigiCert 將以張貼資訊至 PKI Manager 的方式，通知客戶指派之 PKI Platform 管理員。

**指派。**客戶必須將一個或以上的授權客戶員工或可信人員，指派為 PKI Platform 管理員。PKI Platform 管理員必須具備代表客戶指派額外 PKI Platform 管理員的權力。客戶必須要求接收憑證之 PKI Platform 管理員遵守適用訂閱者協議之條款。

**管理者功能。**客戶必須使用 DigiCert 指定的硬體和軟體，遵循定期修訂之 DigiCert Trust Network CPS 所述要求，包括但不限於憑證申請、核准或拒絕憑證申請及撤銷憑證的資訊驗證要求。客戶必須以稱職、專業且熟練的方式執行此任務。只有當憑證申請者為客戶的附屬個人時，客戶才能核准憑證申請。如果已取得客戶頒發憑證的訂閱者停止與客戶的附屬個人關係，客戶必須立即透過 PKI Manager 請求撤銷該訂閱者的憑證。若 PKI Platform 管理員代表客戶擔任 PKI Platform 管理員的權力已終止，客戶必須立即請求撤銷該 PKI Platform 管理員的管理員憑證。

**客戶的訂閱者。**客戶必須要求接收本協議中憑證之訂閱者遵守適用訂閱者協議之條款，訂閱者必須同意以作為註冊憑證之條件。客戶應確保訂閱者協議條款對 CA 的保護不得少於 DigiCert Trust Network CPS。

DigiCert 的保證。DigiCert 保證：(i) 憑證資訊中沒有因建立憑證時 DigiCert 未合理注意而造成之錯誤；(ii) 憑證之頒發在

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

所有重大方面皆遵循 DigiCert Trust Network CPS；且 (iii) 撤銷服務與儲存庫之使用在所有重大方面皆符合 DigiCert Trust Network CPS。

### *附錄 B：私人憑證授權中心*

DigiCert PKI Platform 為客戶提供私人憑證授權中心 (CA) 頒發憑證的功能。DigiCert 採用正式、安全的程序來為此 CA 建立私密/公開金鑰，稱為金鑰儀式。這些憑證通常用來控制組織資源的存取。舉例來說，許多客戶只信任其私人 CA 存取其專用網路 (透過 VPN 或 WiFi)，以防止未經授權之網路存取。

每位客戶的帳號設定都會自動配置私人憑證授權中心 (CA)。此 CA 根據提供給 DigiCert 且經審核之客戶法人名稱來進行帳號設定。客戶如欲在組織中使用其他名稱商標 (例如品牌名稱與法人名稱) 或更改 CA 中的任何預設值，客戶可以購買選項來建立額外 CA。

註：客戶應負責定義與遵守自己的憑證實務作業基準 (CPS)，以對適用私人 CA 之憑證頒發、管理和使用加以約束。

**其他服務條件 – 僅適用於私人憑證授權中心**

**指派。**客戶必須將一個或以上的授權客戶員工或可信人員，指派為 PKI Platform 管理員。PKI Platform 管理員必須具備代表客戶指派額外 PKI Platform 管理員的權力。客戶必須要求接收憑證之 PKI Platform 管理員遵守適用訂閱者協議之條款。

**管理者功能。**客戶必須使用 DigiCert 指定的硬體和軟體，透過其 PKI Platform 管理員驗證憑證申請中的資訊、核准或拒絕憑證申請，並指示 DigiCert 頒發、續購和撤銷憑證。若 PKI Platform 管理員代表客戶擔任 PKI Platform 管理員的權力已終止，

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

客戶必須立即請求撤銷該 PKI Platform 管理員的管理員憑證。

**DigiCert 的保證。**DigiCert 保證憑證資訊中沒有因建立憑證時 DigiCert 未合理注意而造成之錯誤。

## *附錄 C：Adobe® 文件簽署服務*

DigiCert PKI Platform 提供客戶透過 Adobe® 文件簽署服務頒發憑證的功能。DigiCert 與 Adobe 合作，提供自動受 Adobe Acrobat®、Reader® 和 LiveCycle® 產品信任的憑證頒發功能。此類憑證可在這些產品中用來進行可攜式文件格式 (PDF) 之數位簽署。

選擇 Adobe 作為憑證授權中心 (CA) 的客戶，帳號設定中會自動將 Adobe 文件簽署服務，配置到賽門鐵克中繼 CA 之頒發 CA 串鏈。此 CA 根據提供給 DigiCert 且經審核之客戶法人名稱來進行帳號設定。客戶如欲在組織中使用其他名稱商標 (例如品牌名稱與法人名稱) 或更改 CA 中的任何預設值，客戶可以購買選項來建立額外 CA。

註：客戶和使用者必須遵守 Adobe CDS 憑證實務作業基準 (CPS) 或 Adobe ATL CPS (如果適用)，以頒發、管理和使用這些憑證。

針對 AATL，客戶可選擇 SHA256 或 ECC。

### 其他服務條件 – 僅適用於 Adobe® 文件簽署服務

**指派。**客戶必須將一個或以上的授權客戶員工或可信人員，指派為 PKI Platform 管理員。PKI Platform 管理員必須具備代表客戶指派額外 PKI Platform 管理員的權力。客戶必須要求接收憑證之 PKI Platform 管理員遵守適用訂閱者協議及 CPS 相關條款。

**管理者功能。**客戶必須使用 DigiCert 指定的硬體和軟體，透過其 PKI Platform 管理員驗證憑證申請中的資訊、核准或拒絕憑證申請，並根據發佈在 PKI Manager 且不時修訂之 CPS，指示 DigiCert 頒發、續購和撤銷憑證。若 PKI Platform 管理員代表客戶擔任 PKI Platform 管理員的權力已終止，客戶必須立即請求撤銷該 PKI Platform 管理員的管理員憑證。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

**客戶的訂閱者。**客戶必須要求接收本協議中憑證之訂閱者遵守適用訂閱者協議之條款，訂閱者必須同意以作為註冊憑證之條件。客戶應確保訂閱者協議條款對 CA 的保護不得少於 CPS。

**DigiCert 的保證。**DigiCert 保證憑證資訊中沒有因建立憑證時 DigiCert 未合理注意而造成之錯誤。

## *附錄 D：LTE 憑證服務*

DigiCert LTE Base Station 服務（「LTES」或「服務」）提供客戶在私有階層下取得裝置憑證的功能，以整合至營運者 LTE 設備。客戶或其營運者透過憑證管理協定 (CMP) 等程式設計介面，向 DigiCert 提交 LTES 請求。

### 其他服務條件 – 僅適用於 LTE 憑證服務

**指派。**客戶必須將一個或以上的授權客戶員工或可信人員，指派為 PKI Platform 管理員。客戶必須要求接收管理員憑證之 PKI Platform 管理員遵守與該憑證相關之適用訂閱者協議條款，並僅將 PKI Platform 管理員憑證用於符合本服務描述之授權且合法用途。若訂閱者已終止擔任授權 PKI Platform 管理員，客戶必須立即請求撤銷適用的管理員憑證。

**管理員功能。**客戶和/或其營運者 (如適用) 必須透過指定的 PKI Platform 管理員，負責下列事項：

1. 建立營運者子帳號；
2. 建立憑證設定檔；
3. 提供製造商 CA 憑證；
4. 提供驗證用 IP 位址區塊；
5. 註冊新裝置並為未來請求設定預先核准；並
6. 將 CMP 回應程式 URL 設定在網路元件上。

**帳號認證與憑證頒發。**若任何營運者經授權可接收依此協議頒發之 LTE 憑證，客戶必須向 DigiCert 提供事前書面授權，內容

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

包括營運者聯絡資訊、被指派為營運者 PKI Platform 管理員之個人身份證明（包含註冊資訊）及各營運者被授權之 LTE 憑證與站點數量。客戶必須確保並要求其營運者確認每個 PKI Platform 管理員一直是（自適用 PKI Platform 管理員憑證建立時間起算），並仍會是處理這類憑證私密金鑰、任何 PIN、保護私密金鑰之軟體或硬體機制的唯一人員，不曾有也不會有未經授權人員存取前述內容或資訊。

PKI Platform 管理員透過 PKI Manager 提交憑證請求後（請求之憑證數量已依前述經過客戶授權），DigiCert 有權 (i) 仰賴每個此類核准憑證請求中的資訊準確性；並 (2) 頒發與提供憑證給提出請求之 PKI Platform 管理員。根據本服務描述頒發或授權的憑證有效期間為憑證頒發日起一 (1)、二 (2) 或三 (3) 年。DigiCert 將依接收順序履行所有訂單並滿足所有前述要求。即使本服務描述中有任何條款不一致，可請求憑證的營運者數量，以及可透過其請求憑證之生產站點與 PKI Platform 管理員數量，都會受適用訂單文件中所指定的數量嚴格限制。

**製造商分包流程義務。**客戶不得對 DigiCert 系統或軟體的技術執行進行監控、干擾或逆向工程，也不得故意損害任何 DigiCert 系統或軟體的安全性，並且必須對其指定的製造商施以相同限制。

**CA 憑證。**即使有任何與本服務協議相反之情事，DigiCert 將根據賽門鐵克的標準 PKI 實務作業與政策建立並託管兩 (2) 個客戶根憑證，並可選擇在每個根憑證下頒發最多兩 (2) 個 CA 憑證，CA 憑證則僅作為提供客戶服務之用。其他 CA 憑證可以單獨購買。DigiCert 會根據客戶請求，依照標準 PKI 實務作業與政策讓營運者上線並為其建立子帳號。

**IP 位址設定。**新營運者的上線程序之一，是必須提供 DigiCert 一系列有效的 IP 位址。DigiCert 的系統僅會回應來自有效 IP 位址的 CMP 請求，其他非來自設定 IP 位址的請求都將被拒絕。此設定必須由營運者執行。

**帳號啟用。**若為事前購買，DigiCert 會盡商業上合理之努力，於十 (10) 個工作天內啟用美國境內子帳號，美國境外的子帳號則會在滿足以下要求後，於商業合理期間內完成啟用：(i) 完成必要註冊程序；(ii) 營運者與其 PKI Platform 管理員認證。在此期間必須能夠與 PKI Platform 管理員取得聯繫，以利 DigiCert 及時執行身份認證。

**DigiCert 的保證。**DigiCert 保證頒發之憑證中沒有因建立憑證時 DigiCert 未合理注意而造成之錯誤。

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

## *附錄 E：製造商憑證*

DigiCert PKI Platform 為客戶提供在私有階層下頒發製造商憑證的功能，以整合至製造商生態系統中的特定裝置。製造商憑證的用途包含裝置驗證或對裝置傳送的訊息加密。客戶使用批次介面來向 DigiCert PKI 服務請求製造商憑證。

**其他服務條件 – 僅適用於製造商憑證**

**指派。**客戶必須將一個或以上的授權客戶員工或可信人員，指派為 PKI Platform 管理員。客戶必須要求接收管理員憑證之 PKI Platform 管理員遵守與該憑證相關之適用訂閱者協議條款，並僅將管理員憑證用於符合本服務描述之授權且合法用途。若訂閱者已終止擔任授權服務管理員，客戶必須立即請求撤銷適用的管理員憑證。

**管理員功能。**客戶和/或其營運者 (如適用) 必須透過指定的 PKI Platform 管理員，負責下列事項：

1. 建立子帳號；
2. 建立憑證設定檔；
3. 提供製造商 CA 憑證；並
4. 提交憑證頒發批次要求。

**製造商分包流程義務。**客戶不得對 DigiCert 系統或軟體的技術執行進行監控、干擾或逆向工程，也不得故意損害任何 DigiCert 系統或軟體的安全性，並且必須對其指定的製造商施以相同限制。

**憑證頒發。**服務管理員透過 PKI Manager 提交批次憑證要求後，DigiCert 有權 (i) 仰賴每個此類憑證要求中的資訊準確性；並 (2) 頒發與提供憑證給提出請求之 PKI Platform 管理員。DigiCert 將依接收順序履行所有訂單並滿足所有前述要求。即使本服務描述中有任何條款不一致，可請求的憑證數量會受適用訂單文件中所指定的數量嚴格限制。

**帳號啟用。**若為事前購買，DigiCert 會盡商業上合理之努力，於十 (10) 個工作天內啟用美國境內帳號，美國境外的帳號則會在滿足以下要求後，於商業合理期間內完成啟用：(i) 完成必要註冊程序；(ii) 客戶與其 PKI Platform 管理員認證。在此期間必須能夠與 PKI Platform 管理員取得聯繫，以利 DigiCert 及時執行身份認證。

**DigiCert 的保證。**DigiCert 保證頒發之憑證中沒有因建立憑證時 DigiCert 未合理注意而造成之錯誤。

**私有根 CA 的必要條款。**由於製造商憑證在根 CA 的私有階層中執行，若根 CA 為客戶以外的第三方 (例如產業協會或標準制

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

定機構），DigiCert 對製造商憑證的提供便取決於客戶是否滿足根 CA 所要求的所有條件，以作為 DigiCert 託管並於根憑證下頒發之製造商憑證接收先決條件，另外此類製造商憑證僅限於該根 CA 管理的生態系統中使用。先決條件可能包括但不限於執行根 CA 指定之任何其他文件。**根 CA 對其生態系統之製造商憑證頒發具有絕對權力，並保留指示 DigiCert 不頒發憑證給客戶的權利。DigiCert 免於承擔與根 CA 採取行動相關之任何和所有責任。根 CA 保留其在生態系統每個製造商憑證中所擁有的所有專有權和智慧財產權。根 CA 擁有的此類權利係根據根 CA 所指定的文件授權給客戶。客戶確認並同意，根據根 CA 要求，DigiCert 可能需要報告客戶的身份與所有憑證銷售情況。**

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。

## 更多資訊

DIGICERT, INC.

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

© 2018 DigiCert, Inc. 保留所有權利。DigiCert 是 DigiCert, Inc. 在美國和
其他地區的註冊商標。所有其他商標及註冊商標均為其各自持有者之財產。