



(19) 中華民國智慧財產局

(12) 發明說明書公開本

(11) 公開編號：TW 201606560 A

(43) 公開日：中華民國 105 (2016) 年 02 月 16 日

(21) 申請案號：104112472

(22) 申請日：中華民國 104 (2015) 年 04 月 17 日

(51) Int. Cl. :

*G06F21/60 (2013.01)**G06F21/62 (2013.01)**G06F21/72 (2013.01)**H04W12/06 (2009.01)*

(30) 優先權：2014/05/07

美國

61/990,044

2014/05/07

美國

61/990,050

2014/05/07

美國

61/989,993

2014/11/06

美國

14/535,194

(71) 申請人：密碼研究公司 (美國) CRYPTOGRAPHY RESEARCH, INC. (US)

美國

(72) 發明人：漢伯格 麥可 HAMBURG, MICHAEL (US)；詹 哲明 JUN, BENJAMIN CHE-

MING (US)；柯契爾 保羅 C KOCHER, PAUL C. (US)；歐洛夫林 丹尼爾

O'LOUGHLIN, DANIEL (US)；波薛夫 丹尼斯 亞歷山卓維屈 POCHUEV, DENIS

ALEXANDROVICH (US)

(74) 代理人：陳長文

申請實體審查：無 申請專利範圍項數：20 項 圖式數：17 共 102 頁

(54) 名稱

用以安全地提供資產至目標裝置之模組

MODULES TO SECURELY PROVISION AN ASSET TO A TARGET DEVICE

(57) 摘要

本文中所描述之實施例描述用於模組管理之技術，其包含在一密碼編譯管理器(CM)環境中於一目標裝置之一製造生命週期之一操作階段中的模組建立及至該目標裝置的模組部署。一項實施方案包含一根授權機構(RA)裝置，該 RA 裝置接收用以建立一模組之一命令；及回應於該命令，執行一模組範本以產生該模組。該模組經部署至一器具裝置。該模組之一指令集在由該器具裝置執行時導致一操作序列之一安全建構安全地提供一資料資產至該目標裝置。該器具裝置經組態以將該資料資產分發至該目標裝置之一密碼編譯管理器(CM)核心。

The embodiments described herein describe technologies for Module management, including Module creation and Module deployment to a target device in an operation phase of a manufacturing lifecycle of the target device in a cryptographic manager (CM) environment. One implementation includes a Root Authority (RA) device that receives a command to create a Module and executes a Module Template to generate the Module in response to the command. The Module is deployed to an Appliance device. A set of instructions of the Module, when executed by the Appliance device, results in a secure construction of a sequence of operations to securely provision a data asset to the target device. The Appliance device is configured to distribute the data asset to a cryptographic manager (CM) core of the target device.

指定代表圖：

符號簡單說明：

100 . . . 密碼編譯管理
器(CM)系統

102 . . . 根裝置

103 . . . 網路

104 . . . 服務裝置

105 . . . 企業網路

106 . . . 目標裝置

107 . . . 服務

108 . . . 委派器具裝
置/安全器具裝置

109 . . . 器具叢集

110 . . . 提供裝置/
Cryptography Research
Inc.系統提供(CRISP)
裝置111 . . . 硬體安全性
模組(HSM)

112 . . . 測試器裝置

114 . . . 用戶端庫

130 . . . 高產量製造
場址/遠端製造場址/
製造設施場址

140 . . . 資料中心

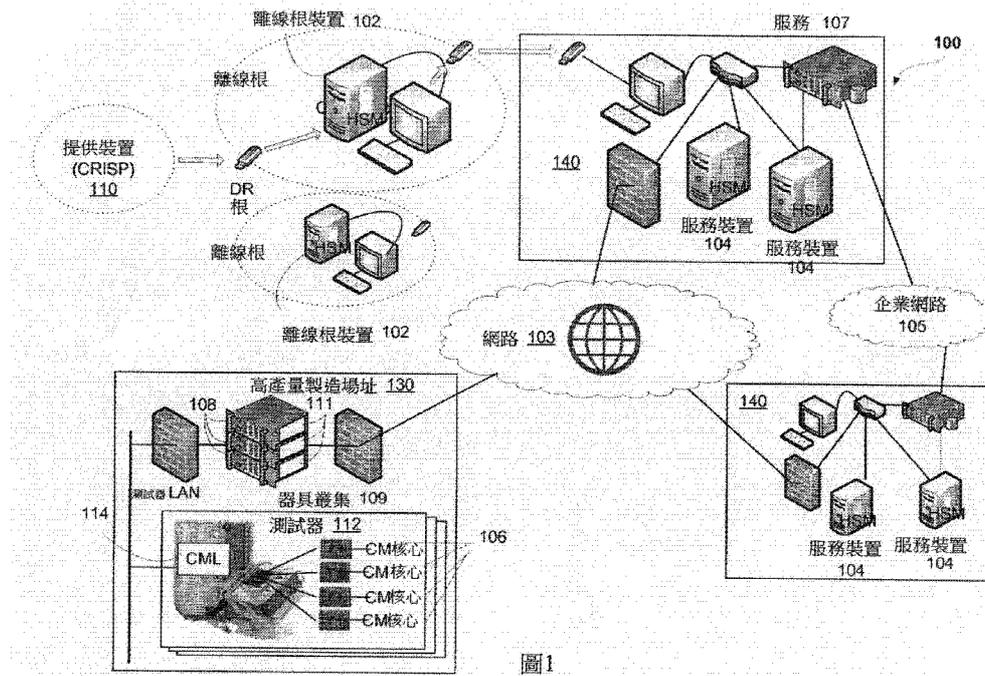


圖1

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】

用以安全地提供資產至目標裝置之模組

MODULES TO SECURELY PROVISION AN ASSET TO A
TARGET DEVICE

相關申請案

本申請案主張2014年5月7日申請之第61/990,004號美國臨時申請案、2014年5月7日申請之第61/990,050號美國臨時申請案及2014年5月7日申請之第61/989,993號美國臨時申請案之權益，該等案之全部內容以引用的方式併入本文中。本申請案係關於以下申請案：與其同時申請、標題為「產生預先計算資料資產並將其分發至目標裝置 (GENERATING AND DISTRIBUTING PRE-COMPUTED DATA (PCD) ASSETS TO A TARGET DEVICE)」之代理人案號27170.109 (L0092) 之同在申請中申請案；及與其同時申請、標題為「在分散式安全資產管理基礎架構中之稽核及權限提供機制 (AUDITING AND PERMISSION PROVISIONING MECHANISMS IN A DISTRIBUTED SECURE ASSET-MANAGEMENT INFRASTRUCTURE)」之代理人案號27170.110 (L0093)之同在申請中申請案。

【先前技術】

目前，系統單晶片 (SoC) 廠商可銷售相同「積體電路 (亦稱為「晶片」或「IC」)」之諸多不同品種，其中每個品種經組態用於一特定應用。IC組態通常藉由在IC上熔斷一或多根保險絲或以其他方式程式化一單次可程式化記憶體而發生。此類型之IC組態通常為一單向程序且無法復原。一種規避組態程序之永久性之方法為在單次可程式化記

憶體內新增可經組合以修改一先前設定(例如，藉由一起互斥或運算多個位元以產生最終組態設定)之冗餘或備用位元。然而，此類型之冗餘性具有受限靈活度，且需要額外保險絲，從而在IC上佔據額外面積(real estate)。此外，使多根保險絲在一設定之後不會移除對執行多個程式化步驟以組態IC之需要，但會增加成本。同樣地，組態現今繼續由IC廠商(或其經銷商)執行，其等接著維持具有多種保險絲組態之IC之庫存。

相同IC之不同品種之儲備通常不足。例如，若經組態用於一特定應用之儲備IC過度生產或若客戶之IC組態需要變更，則其等可能被浪費。此外，在一些情況下，若經組態IC之庫存不足以滿足需求，則訂單履行可能延遲。此外，IC廠商之目前組態模型可限制IC廠商與下游客戶之間的業務關係及實際營收源流(revenue stream)之範圍。例如，目前模型可限制在IC初始銷售之後從其重新組態產生未來營收之能力。若一下游客戶希望獲得超越經組態特徵集之特徵，則當前IC通常缺乏對此功能性解鎖之手段且因此沒有機會將下游特徵啟用用作一營收源流。

此外，安全系統及應用之需要在遞增。目前，據稱，通常在廠區中運用安全金鑰程式化安全IC。可按各種方式使用安全金鑰，舉例而言，諸如以保護經儲存資料，控制對數位內容之存取，或加密/鑑認用於交易之資料。現今，此等金鑰可儲存於一單次可程式化記憶體中，其可直接保存金鑰或保存結合導出各種功能金鑰之加密編譯功能使用之一基底金鑰。通常，藉由在一安全設施中執行金鑰載入程序來提供安全性。

【圖式簡單說明】

在隨附圖式之圖中，藉由實例的方式且非限制的方式繪示本發明。

圖1繪示根據一項實施例之一密碼編譯管理器(CM)系統之一網路圖。

圖2為繪示根據一項實施例之圖1之CM系統之裝置之間的訊息之一圖。

圖3為繪示根據一項實施例之一模組生命週期之一流程圖。

圖4為根據一項實施例之建立一模組並將其部署至一器具裝置之一方法之一流程圖。

圖5為根據一項實施例之部署一模組至一測試器裝置之一CM程式庫之一方法之一流程圖。

圖6為繪示根據一項實施例之用於預先計算資料(PCD)部署授權之圖1之CM系統之裝置之間的訊息之一圖。

圖7為繪示根據一項實施例之在產生及匯入時之一個循序PCD檔案及在重新分塊之後的兩個循序PCD檔案之一流程圖。

圖8為繪示根據一項實施例之在產生及匯入時之兩個非循序PCD檔案及在合併之後的一個非循序PCD檔案之一流程圖。

圖9為繪示根據一項實施例之模組、PCD與票證(ticket)關係之一圖。

圖10為根據一項實施例之一PCD產生程序之一流程圖。

圖11為繪示根據一項實施例之一高頻寬數位內容保護(HDCP)匯入程序之一網路圖。

圖12為根據一項實施例之在一HDCP生命週期中之一傳入HDCP資產之一匯入程序之一流程圖。

圖13為根據一項實施例之在一CM系統中產生並封裝一PCD資產用於安全部署之一方法之一流程圖。

圖14為根據一項實施例之一加票證(Ticketing)及HSM互動常駐程式(THID)組件之一方塊圖。

圖15為根據一項實施例之加票證於一模組以安全地提供一資料資產至一目標裝置之一方法之一流程圖。

圖16為根據一項實施例之一電腦系統之一項實施例之一圖，包含一處理器及連接至一可抽取式儲存裝置之一可抽取式儲存裝置介面。

圖17為根據一項實施例之一域劃分(domain partition)之一圖。

【實施方式】

本文中所描述之實施例描述用於在目標裝置之製造生命週期之一或多個階段中提供安全資產至目標裝置之一安全資產管理基礎架構之技術。該安全資產管理基礎架構(亦稱為CM生態系統)包含經設計以履行提供安全晶片製造之使用案例之硬體及軟體之一多裝置密碼編譯管理器(CM)系統(下文中亦稱為「CM系統」)。該CM系統包含旨在安全地產生、處理並遞送有效負載(序列)之一安全裝置製造之各種授權、客製化及測試子系統以及其他程序。該CM系統安全地產生、處理並遞送有效負載(序列)。該CM系統通常包含一CM根裝置(本文中稱為「根裝置」或「CM根裝置」)、一或多個CM服務器具裝置(本文中稱為「服務裝置」或「CM服務裝置」)、數個CM器具裝置(本文中稱為「器具裝置」或「CM器具裝置」)、測試器裝置、及數個CM核心及相關軟體。在此CM生態系統中，一CM器具為安全地產生、處理並遞送有效負載(亦稱為序列或模組序列)至一目標裝置一CM核心之一產品。該CM核心為能夠執行一命令集之一硬體核心，該等命令為用於將功能性遞送至該目標裝置(亦稱為產品)之建置組塊。此等命令之執行結果為該CM系統之目的。序列可進行數位簽署及/或實行有效性之其他密碼編譯示範(例如，一MAC)，該CM核心可驗證其以確認序列之保持原樣及有效性。此提供對該CM核心將接受何種資料(及將由該CM核心執行哪些操作)之控制，即使用以遞送序列之通信頻道不受信任。在一項實施例中，該等CM核心為

CryptoManager™核心。CryptoManager™核心為提供對特徵啟動、組態管理及安全金鑰管理之密碼編譯控制之一硬體核心。CryptoManager™核心整合至系統單晶片(SoC)設計中且經由定位於SoC主匯流排上之一暫存器介面進行存取。該模組為含有指令及資料兩者之一程式，其執行導致一序列之一安全建構。該序列可為由在一委派器具裝置內之一HSM上運行之一模組所產生且由該CM核心消耗之二進位資料。由一CM核心安全執行一序列為該CM系統之主目的。一模組之確切指令集可定義為該CM系統設計之一部分。

含有電子組件(諸如微控制器、感測器、處理器等)之電子裝置及其他裝置之製造及組裝已隨此等硬體裝置之使用遞增而遞增。為了降低製造成本，諸多公司已將製程之態樣外包給第三方公司。此等第三方公司之一些可在海外且可在其中企業安全性不如其他管轄區強大之管轄區中。

在某些裝置之製造中，軟體、程式碼、金鑰及其他重要資產可嵌入或安裝於硬體裝置中。當前，此等資產可在一儲存媒體上從客戶輸送至一製造場址，諸如儲存於一光碟上。此等資產之管理可對安全性及客戶營收重要，此係因為其並非在所有方面盡如人意。本文中所描述之實施例提供安全資產管理系統及技術，以在不受信任環境中安全地提供資產至此等硬體裝置。該安全資產管理系統包含共同協作以允許一客戶在由第三方製造商執行之製程期間監測並控制此等資產之接收及消耗之諸多組件。該系統包含安裝於第三方製造商處之遠端組件及被客戶用以與此等遠端組件通信並控制其等之組件。一資產可為數位資料(諸如一金鑰或金鑰集)、一憑證、一唯一裝置識別符等，其需要在該裝置準備好銷售給一消費者之前安全地傳送至消耗裝置。

圖1繪示根據一項實施例之一CM系統100之一網路圖。CM系統100通常包含各種密碼編譯管理器(CM)裝置。CM系統100可提供安全

交易處理及資料報告基礎架構，其經設計以透過一網路服務介面提供安全金鑰及資產管理能力給一目標裝置106 (例如，行動裝置)。CM系統100之使用者或客戶可為生產行動裝置之晶片組之無晶圓廠半導體廠商、製造行動網際網路連接裝置之系統整合商(OEM)、及在其無線網路上部署此等裝置之行動網路運營商(MNO)等。此等客戶可將其裝置或組件製造之一些發包給操作遠端製造設施之第三方製造商，諸如一高產量製造場址130。作為客戶之製造及通信系統之一任務關鍵部分，CM系統100之設計重點為高可用性及完整性。

CM系統100包含充當裝置及模組之一初始提供設施之一提供裝置110，其可為CM系統100之部分或在CM系統100中用以裝置之初始身分識別及認證。一裝置102接收由提供裝置110簽署之資料，諸如圖2中所繪示。根裝置102為授權CM系統100之安裝、組態及操作之一實體。根裝置102可保護主控金鑰且授權在任何給定場址(諸如製造場址130)中進行CM系統100之組件之設置、安裝、組態及操作。出於安全考慮，在一些實施例中，提供裝置110可不具有至CM系統100之其餘部分之一永久性連接。即，根裝置102可被視為授權CM系統操作中之設置及主要組態參數之一離線根。通常，藉由一可抽取式儲存裝置(諸如一通用串列匯流排(USB)快閃隨身碟等)往返根裝置102傳送資料。電腦系統在安全性與便利性之間進行權衡。假定根授權機構之主任務為保護鞏固一整個CM部署之安全性之主控金鑰，則依據安全需要來設計根授權機構。此係為何根授權機構可為氣隙式之原因(即，不連接至任何電腦網路)。此外，一HSM可用以保護由根授權機構儲存之最重要金鑰。由於根授權機構離線，故假定其不可連續使用。因此，根授權機構可提前授權一許可動作範圍，使得在需要採取一動作時不必要地涉及根授權機構。根授權機構之授權提供至服務裝置，其中作出關於實際上將使用哪些授權之決定。

一服務107 (下文中稱為「服務」)(包含一或多個服務裝置104)提供用以集中控制及監測CM系統100之操作之一方式，並且提供資料至一器具叢集109 (一或多個器具裝置之一集合)。服務裝置104為用以促進CM系統100之中央管理且提供資料至一器具叢集109之一硬體器具。此外，服務裝置104 (經由委派器具裝置108)分發目的地為目標裝置106之模組、資料及安全性參數。一目標裝置106為單片積體電路，其通常包含一CM核心。服務107之服務裝置104可駐留於客戶之實體安全企業資料中心140中且可提供一轉鑰(turn-key)安全性服務至公司，以在一遠端製造場址130中管理其資產。在另一實施例中，服務107可在透過一企業網路105連接之多個資料中心140處包含多個服務裝置104，如圖1中所繪示。一資產為一數位資料檔案，諸如一HDCP裝置金鑰集，其需要安全地傳送至一目標消耗裝置(例如，CM核心)。一資產為任何敏感資料，諸如透過CM系統安全地管理且在從製造供應鏈至終端使用者之各個生命週期階段提供至裝置之金鑰、序號及韌體。資產通常為裝置特有。例如，perso1、perso2及裝置序列化記錄為資產。Digital Content Protection, LLC (DCP)為建立並銷售HDCP金鑰之一組織。例如，一客戶從DCP購買金鑰，且接著將HDCP金鑰匯入至CM服務中。該匯入程序將金鑰檔案重新格式化為一預先計算(PCD)檔案並加密其使得僅合適授權器具裝置可存取該PCD。器具叢集109負責在於製造場址130處製造目標裝置106之程序期間本端地代管敏感資料以傳送至目標裝置106 (例如，CM核心)。

可由一網路服務介面提供管理器具叢集109之分發網路及跨安全器具裝置108之一網路103提供PCD資產、票證授權、簽署序列及模組之能力給CM系統100之使用者。在半導體裝置測試及/或製造之程序期間，器具叢集109可負責於製造設施場址130本端安全地儲存敏感資料且負責使該資料以一低延時方式高效地用於一目標裝置106，諸如

一系統單晶片 (SoC) 或此一 SoC 上之一子組件。目標裝置 106 可在 SoC 之設計階段期間整合至 SoC 設計中以提供對 SoC 特徵啟動、組態管理及安全金鑰管理之密碼編譯控制。在一些實施例中，目標裝置 106 各包含一 CM 核心。該 CM 核心為能夠執行一命令集之一硬體核心，該等命令為用於將功能性遞送至一產品 (目標裝置 106) 之建置組塊。此等命令之執行結果為 CM 系統 100 之最終目的。一委派為根裝置 102 對其授予 CM 核心程式化能力之一子集從而允許將根裝置 102 未知之資料併入至目的地為目標裝置 106 (例如，CM 核心) 之序列中之一實體。一器具裝置 108 為經設計以提供安全計算、數位簽署及至目標裝置 106 (例如，CM 核心) 之序列分發且併入由委派實體提供之資料之一實體。器具裝置 108 各含有一硬體安全性模組 (HSM) 111，其用作一保存庫防護敏感資料及用於執行一模組之一平台兩者。此外，器具裝置 108 經由服務 107 產生、收集、保護、數位地簽署並發送各種記載 (logging) 資訊至客戶。器具叢集 109 (亦稱為委派叢集) 為增大由一委派器具裝置 108 提供之服務之可用性之委派器具裝置 108 之一群組。若一特定器具裝置 108 無法履行一請求，則一測試器裝置 112 可連接至相同器具叢集 109 中之任何其他器具裝置 108 以繼續服務而不受主要干擾。測試器裝置 112 為在半導體裝置製造中用以測試裝置是否正確執行之一機器。CM 系統使用測試器裝置 112 以在晶圓測試 (wafer sort) 及封裝測試期間程式化資料。一測試器裝置 112 通常為定位於製造商場址 130 處、用以將序列遞送至特定目標裝置 106 (例如，CM 核心) 之一不受信任裝置。測試器裝置 112 為經設計以執行驗核、特性化及高產量製造測試之一裝置。測試器裝置 112 運行一系列半導體測試，其中之一或若干者將為 CM 系統操作之一部分。測試器裝置 112 能夠起始與委派器具叢集 109 之通信且提供記載資訊。一序列為二進位資料，其由在一委派器具裝置 108 內之一 HSM 111 上運行之一模組予以產生且由該 CM 核心消

耗。由一CM核心安全執行一序列為CM系統100之主目的。測試器裝置112可存取一用戶端庫114。用戶端庫114可為與測試器裝置112之一主要應用程式整合之一軟體組件。用戶端庫114可為由Cryptography Research Inc.提供之用戶端庫。本文中描述由含有CM核心之一CM系統100中之一測試器裝置112起始之典型互動。在其他實施例中，在一非CM核心系統中，由測試器裝置112進行之互動可稍微不同。在一測試器裝置112運行一「CRI」測試時，測試器裝置112可調用一指令碼，以將一請求發送至器具裝置108之一者。作為回應，器具裝置108執行本文中所描述之一協定，其中導致安全地遞送一序列至一或多個CM核心進行一給定測試。

為了使資料可用於目標裝置106，器具叢集109可透過一網路103(諸如公共網際網路、一私人網路、及/或其組合)連接至資產管理服務(稱為服務107)。器具叢集109可駐留於外包製造設施場址130之一資料中心中且可充當服務107之一代理。在製造期間，器具叢集109以一低延時方式使用強鑑認及存取控制以使PCD資產及票證授權之一安全且高可用的本端庫存可用於目標裝置106(例如：行動裝置及晶片組)。

一資產至一裝置之提供及/或安裝可稱為資產管理交易。可由一模組管理資產管理交易。一單一器具叢集109可運行諸多模組且各模組可經設計以提供一單一類型之交易至CM核心啟用之目標裝置。在一HSM 111上執行該模組所需之安全性敏感計算。一模組連同防篡改HSM 111可消耗來自由服務107提供至器具裝置108或器具叢集109之一批量授權檔案之一目標裝置特有授權或票證。一模組為含有指令及資料兩者之一程式，其執行導致一序列之一安全建構。一模組之確切指令集定義為CM系統設計之一部分。一模組範本為定義該模組之指令集之一程式。模組範本由根裝置102匯入且其執行導致建立一模組。模組範本提供用於CM系統擴充性之一機制。如本文中所描述，

PCD為由委派器具裝置分發、通常離線計算、批量地發送至一委派器具裝置、藉由一索引加索引且傳送為一序列之一部分之資料。該索引可獨立於目標裝置之序號或其他識別符。一PCD範本為如何格式化PCD之一描述，PCD變成用於一特定類型模組之一輸入。一PCD類型為基於一特定PCD範本、具有一特定性質(property)(諸如唯一性、序列化等)之一PCD集。例如，PCD包含CM根產生之金鑰、序號等，其等經安全封裝使得僅一裝置上之CM核心IP可提供該資料。舉另一實例，PCD包含來自各種廠商、從CM服務至目標裝置之安全地管理之金鑰(例如，HDCP金鑰)。金鑰資料在載入至服務中時變換成PCD。

藉由具有相同票證名稱之票證加索引於一給定PCD類型內之所有資產。一票證為使能夠強制執行CM核心參數之使用計數限制及唯一性/循序發佈之資料。票證由服務操作者授權且由CM模組消耗。下文更詳細描述模組、PCD資產及票證。

大體言之，CM裝置(例如，102、104及108)必須受信任以便代表CRI客戶(或一根授權機構實體之客戶)提供管理、分發及程式化有價值電子資產所需之安全基礎。跨CM系統100建置可用於鑑認所有裝置之一受信任根為CM基礎架構之整個安全性模型之中心環節。為了解決安全地建置及提供安全識別符及認證之問題，可使用一提供裝置110，亦稱為CRISP或CRISP裝置。可在任何CM裝置之一生命週期中之一開始點使用CRISP。在CRISP可提供任何新CM裝置之前，CRISP首先自行建立認證，且向提供資產之一實體(例如，Cryptography Research Inc.)及將該等資產分發至製造中之CM裝置之客戶兩者確立本身為一受信任第三方。CRISP提供將CM系統100從使用CRI發佈之金鑰(例如，由Cryptography Research Inc.提供之金鑰)切換至使用通常由一根授權機構(RA)產生之客戶特有金鑰來操作之能力。

應注意，本發明描述之各個部分提及CM系統100之組件，諸如作

為邏輯實體之根、服務或器具。有時，一邏輯實體之內部結構係重要的。例如，一服務實體通常包含兩個伺服器、一公用檔案系統、一公用資料庫等。在其中服務107之內部係重要的且此等伺服器之各者被視為一邏輯實體之內容脈絡中，其各者稱為服務裝置，以區別其與服務實體(其表示服務裝置以及共用資源)。類似地，一根裝置102為實施根授權機構之功能性之一伺服器；一器具裝置為一單一伺服器(通常為器具裝置108之器具叢集109之一成員)。一目標裝置106 (通常為該目標裝置之一CM核心)為CM系統100之功能性之消費者。根裝置102、服務裝置104及器具裝置108各包含一主運算裝置(例如，處理器等)以及一嵌入式HSM 111。一些ID及金鑰將儲存於HSM 111內，而其他ID及金鑰將儲存於裝置之硬碟機上。ID或金鑰之確切位置基於其敏感性及實施細節來判定，如本文中所描述。ID用以識別CM系統100內之組件。該等組件之一些為實體(例如，服務107)，而其他組件為裝置(例如，服務裝置104)。此外，如本文中所使用，晶片系列指代在CM核心內共用相同安全性參數之一產品集(例如，共用一共同屬性(attribute)集(例如RsbSigningKey)之一產品集)。此概念亦藉由根授權機構之資料模型來反映。各安全性參數集囊封於根授權機構上之不同ChipSeries資料集中。ChipSeriesID為一ChipSeries之一識別符。ChipSeriesName或alias為由一客戶對一Chipseries使用之一碼名稱(code-name)。一產品為共用一共同屬性集之一裝置集合，例如deviceID空間。DeviceID為一目標裝置之一識別符。Product Name或product alias可為由一客戶對一產品使用之一碼名稱。ChipID為一產品之一ID，而非一晶片、核心或裝置之一識別符。

一提供系統(諸如Cryptography Research Inc. (CRI系統提供)CRISP實體)可包含一或多個提供裝置110 (在圖1中標示為CRISP裝置110)。CRISP裝置110充當CM系統100中之所有裝置及模組之一初始金

鑰提供授權機構，其提供該等裝置之啟動身分識別及認證。特定言之，根裝置102接收由提供裝置110簽署之資料，諸如圖2中所繪示：器具定義檔案，其等指定器具裝置及其HSM 111之屬性；服務定義檔案，其等指定服務裝置及其HSM之屬性；模組範本；PCD範本；ChipSeries範本等。

關於CM系統100之所有裝置之資訊(具體言之，其ID及金鑰)將由CRISP裝置110傳遞至根授權機構(根裝置102)。此資料用作根授權機構進行授權之一基礎。例如，在啟動一新服務107時，一根操作者從根授權機構已知之所有服務裝置104之清單挑選服務裝置104以建置一新服務。應注意，在某些情況下，根授權機構可能匯入CRISP裝置110未授權之裝置資料、模組資料或其他資料。儘管CM系統100可按一有意義方式運作，但此匯入可引入不受信任元素且可導致嚴重安全性及可靠性後果。

圖2為繪示根據一項實施例之圖1之CM系統100之裝置之間的訊息之一圖。圖2繪示CM系統傳訊200之一高階概述圖。此等訊息在CM系統100中提供一視覺訊息表示。此等訊息在邏輯上可劃分成以下功能性群組：定義；啟動；模組分發；PCD分發；及票證分發，其等大致上對應於上文所描述之CM生態系統生命週期階段。操作亦可細分成若干特定階段：模組；PCD；及票證分發。應注意，各編號訊息實際上可表示若干訊息，但已大體上經表示以表示訊息交換。此外，圖2中所描繪之訊息可含有若干部分。本文中描述訊息及產生並處理各訊息所需之相關聯功能性。

訊息劃分歸因於兩個因素：以裝置106及HSM 111為目標之訊息之編碼需求以及檔案簽名。對於以HSM為目標之檔案，HSM通常處理以二進位格式編碼之輸入資料。因此，以HSM 111為目標之資料應按該方式進行編碼。對於以裝置為目標之檔案，待由服務裝置或器具

裝置處理之資料可使用JSON來編碼以使處理簡化。為了避免HSM 111解析JSON物件，訊息可分割成此兩種類型：二進位或JSON。HSM 111之特徵之一者為備份還原機制，其使用主控備份金鑰(MBK)。此外，為了操作，一HSM 111必須將一MBK儲存於其中。在根裝置、服務裝置及器具裝置上不同地處理MBK。在根裝置102上，MBK根據計畫用於備份/還原操作。在服務裝置104及器具裝置108上，可不使用MBK且可產生MBK並將其儲存於HSM 111上。

如上文所描述，為了定義，CRISP裝置110之角色為提供裝置身分識別及認證之初始鑑認。CRISP裝置110建立並分發認證，其等用於在啟動服務裝置104及器具裝置108之前在其間建置互相鑑認之安全殼層(SSH)隧道。此外，CRISP裝置110用作一分發器，其分發關於裝置之鑑認公共資訊至根授權機構及其他裝置。例如，ApplianceActivationConn金鑰對提供器具認證用於SSH鑑認。此金鑰對在一器具裝置108上予以產生且其公開金鑰在於一器具定義訊息202中進行定義期間發送至CRISP裝置110。作為器具定義之一部分，根裝置102接收來自CRISP 110之一器具定義訊息202中之此公開金鑰(連同此種類之其他公開金鑰及其他種類之公開金鑰)。此公開金鑰分發至服務裝置104，服務裝置104可使用該等公開金鑰以與器具裝置108安全地通信。額外定義訊息可用於定義其他裝置。例如，可由CRISP裝置110接收來自服務裝置104之一服務定義訊息204。作為服務定義之部分，根裝置102接收來自CRISP之一服務定義訊息208中之此公開金鑰(連同此種類之其他公開金鑰及其他種類之公開金鑰)。此外，作為根定義之部分，根裝置102可接收來自CRISP裝置110之一根定義訊息210。

該定義之另一重要部分為提供根裝置102與裝置(服務裝置104及器具裝置108兩者)之各者之間共用之裝置臨時亂數 nonce)、單次密

碼，其允許在啟動期間鑑認啟動訊息及遞送加密資料。更廣泛言之，定義為在該等裝置之各者與CRISP裝置110之間交換資料、將實體近接度用於其安全性、在啟動期間用於啟動程式(bootstrap)安全性之一程序。

根授權機構之主功能之一者為提供授權至CM系統100之其餘部分。為了啟動，CM系統100之裝置可經由啟動訊息交換啟動檔案。此可藉由使用可抽取式儲存裝置(例如，USB快閃隨身碟)傳送簽署檔案來完成。各授權包含若干檔案，其中一些成對地出現：一個內容檔案及一個簽名或雜湊檔案。在授權需要遞送至裝置本身(而非HSM 111)時，通常以JSON格式表達訊息內容，而二進位格式用於以HSM 111為目標之授權。所有一切意謂著一典型授權為含有若干檔案之一TAR檔案。如圖2中所繪示，服務裝置104接收來自根裝置102之一服務啟動訊息212及器具啟動訊息214。器具裝置108可接收來自服務裝置104之器具啟動訊息216。

基礎架構組態包含由根裝置102以一系列簽署檔案之一形式提供至服務裝置之一授權集。此等檔案由服務裝置104處理且其中一些進一步發送至器具裝置108。例如，在一器具裝置108可執行任何有用功能作為CM系統100之一部分(除升級外)之前，需要啟動器具裝置108。為此，根裝置102建立並簽署器具啟動訊息214並將其發送至服務裝置104。此訊息之傳送造成啟動授權。從根裝置之觀點，已發佈此器具啟動，但可能長時間未在器具裝置108本身上生效。僅在服務操作者決定按照提供之授權採取行動及轉遞所接收之授權時，可能有機會生效。在接收到來自服務裝置104之此器具啟動訊息216之後，器具裝置108驗證其上之簽名並應用啟動授權，接著其可達到作用中狀態。應注意，器具啟動授權之一部分可由服務裝置104本身處理。例如，此為服務裝置104在啟動其時如何接收需要用以連接至器具裝置

108之SSH認證。如上文所描述，根授權機構可提前授權一許可動作範圍，使得在需要採取一動作時不必要地涉及根授權機構。根授權機構之授權(214、216)提供至服務裝置104，其中作出關於實際上將使用哪些授權之決定。

如圖2中所繪示，訊息用以在CM系統中之裝置之間安全地交換關於模組、PCD及票證之資訊。例如，根裝置102接收一模組範本匯入訊息220以將一模組範本匯入至根裝置102中，且接收一PCD範本匯入訊息230以將一PCD範本匯入至根裝置102中。下文更詳細描述模組、模組範本及PCD範本。服務裝置104接收一模組匯入訊息222以將一模組匯入至服務裝置104中且接收一模組部署訊息224以將一模組部署至一器具裝置108。服務裝置104接收一PCD匯入訊息232以將一PCD匯入至服務裝置104中且接收一PCD部署訊息234以將一PCD部署至一器具裝置108。器具裝置108接收一模組匯入訊息226以將一模組匯入至器具裝置108中且接收一模組部署訊息228以將一模組部署至一目標裝置106。器具裝置108接收一PCD匯入訊息236以將一PCD匯入至器具裝置108中。可結合部署至目標裝置106之模組將PCD部署至目標裝置106。應注意，PCD用以提供資料輸入至模組。大體言之，存在至模組之兩個主要輸入，包含PCD及票證。例如，為了將金鑰傳送至一目標裝置106之一CM核心，以PCD之形式提供該等金鑰，該PCD在回應於來自一測試器裝置112之一請求而執行時被該模組消耗。PCD為對如本文中所描述之PCD相關資訊之一般參照。

服務裝置104及器具裝置108可交換加票證訊息240。特定言之，器具裝置108接收來自服務裝置104之票證授予訊息240。以PCD之形式之票證為在於目標裝置106上執行時至模組之一輸入。下文描述關於加票證之額外細節。

CM系統100之特徵之一者為在執行命令序列之一委派器具裝置

108上運行之命令解譯器。在一序列中主要存在兩種類型命令：由一根授權機構密碼編譯地簽署一種類型命令；由一委派(諸如服務裝置104)密碼編譯地簽署另一類型命令。此等序列提供安全且鑑認的程式化指令至目標裝置106 (例如，CM核心)。

模組

一模組為含有指令及資料之一程式，其執行導致一序列之一安全建構。繼而，一序列定義為由目標裝置106之一CM核心消耗之一模組之二進位輸出。一序列至CM核心之安全傳輸及其後續執行為CM系統100之主目的。換言之，模組囊封由CM系統100提供之一不同功能性片段。在一委派器具裝置上一模組之執行遞送由CM系統100以與最終消費類裝置(通常為一CM核心)互動之一形式提供之公用程式。

大體言之，一模組為安全地提供資料至一目標裝置之一應用程式。模組源自根授權機構，在根授權機構處模組被授權以在一特定製造場址處之一特定器具叢集上運行。一模組可將來自一器具叢集上之庫存之以PCD資產之形式之加密資產處理成一裝置獨有的不可重新執行(non-replayable)訊息。一些模組不具有PCD且一些模組不具有唯一訊息。模組使用一加票證系統來確保資產不被複製或重複消費(double-spent)。模組含有由一測試器裝置寫入至一裝置之資訊，該測試器裝置在製程期間使用用戶端庫調用一模組；例如，在晶圓測試或最終測試期間。多數模組亦將裝置交易安全地記載於器具裝置上。日誌項目包含追蹤資料，諸如deviceId及金鑰識別符。該加票證系統追蹤模組使用且可能需要一庫存來確保每當一測試器裝置寫入至一裝置時，有效負載為該裝置獨有且防止重新執行或重複消費。該器具裝置可已包含各模組之特定數目個PCD及票證之一庫存。可由服務操作者將模組部署至選定之器具叢集，但首先可能需要來自根之一授權。該服務接著以足夠層級將由各模組所需要之PCD及票證之庫存維持於各

器具叢集處，以獲得允許網路連接失敗或頻寬波動之生產率。

模組提供CM系統基礎架構之靈活性及擴充性。可在一運作中CM系統100上開發、測試及部署新模組，同時支援使用先前部署模組進行生產。模組生命週期有些複雜，其為系統需求之一反映、要求一可擴充機制來提供未知特徵至該運作中系統，而不犧牲任何系統安全性。下文描述提供在一模組生命週期期間模組管理之各項實施例。

圖3為繪示根據一項實施例之一模組生命週期300之一流程圖。在302處，一CRISP操作者建立一模組規格檔案(CM檔案)。在304處，該CRISP操作者使用一CRISP命令列介面(CLI)或其他使用者介面，以運行一命令(例如，cmCompiler命令)以建立一模組範本(CMT檔案)。該CM檔案被CM編譯器用作輸入。在306處，操作者(CRISP操作者及根操作者)根據需要使用CRISP CLI及一根CLI以產生PCD。在308處，經由拇指隨身碟(thumb drive)(或如本文中所描述之其他可抽取式儲存裝置)將模組範本及PCD範本從CRISP傳送至根。在310處，在根CLI處，根操作者運行一命令(例如，createModule命令)以建立一模組。在一項實施例中，對於一模組M1，一softHSM建立該模組且HSM簽署該模組。模組含有或使用以下項之一些或所有：PCD 305 (來自CRISP及/或根)；來自根資料庫之金鑰(經加密)；由該根操作者供應之引數；器具裝置108隨後提供之資料之「預留位置」(placeholder) 311。應注意，在此例示性實施例中，該模組不含有PCD，但該模組可需要PCD存在於該器具上。由根操作者提供至一模組之引數可為用於一特徵管理模組之一特定特徵位元。引數可包含判定所得金鑰儲存於何處之記憶體位移。在312處，經由一拇指隨身碟將具有預留位置311之模組從根裝置102傳送至服務裝置104。在314處，在根CLI處，根操作者運行一命令(createModuleDeploymentAuthorization命令)以產生一模組部署授權。在316處，經由一拇指隨身碟將模組授權檔案從根裝置102

傳送至服務104。在318處，一服務操作者上載一高頻寬數位內容保護(HDCP)金鑰檔案(來自DCP)用於HDCP模組。該服務操作者請求服務裝置104將DCP金鑰轉換至格式化為PCD檔案之HDCP加密金鑰。在320處，服務裝置104提供PCD 305及票證307至器具裝置108。服務裝置104可對器具裝置108連續地授予票證以賦予器具裝置108執行一模組之權限。服務裝置104可詢問器具裝置108以判定庫存狀態，且可在庫存下降至一組態限制以下時將PCD發送至器具裝置108。在322處，透過網路將該模組部署至器具裝置108。在此實施例中，可在該服務操作者使用使用者介面(GUI或CLI)、將一器具裝置108新增至一器具叢集109 (圖3中未繪示)及將一模組部署至新器具裝置108時觸發一部署命令(loadModule命令)。

在324處，使用測試器CLI，一測試方法開發人員建立一測試指令碼315 (例如，lot_test)並將其載入至測試器裝置112中。在326處，測試指令碼315觸發用戶端庫114至器具裝置108之通信，此觸發調用該模組。在328處，用戶端庫114將引數發送至器具裝置108，器具裝置108使用該等引數連同PCD 305以產生一模組序列313以發送至測試器裝置112。在330處，器具裝置108之HSM 111組譯PCD 305及測試器資訊、簽署委派簽署區塊(DSB)，且建立模組序列313。在332處，器具裝置108將模組序列313發送至測試器裝置112之用戶端庫114以發送至CM核心。

在一項實施例中，該根裝置接收一模組範本、PCD範本及使用者輸入，包含與多種類型之一特定交易類型相關聯之引數。一模組基於模組範本、預先計算資料及引數而產生且部署至一器具裝置。該模組在於該器具裝置上執行時導致一操作序列之一安全建構執行為關於一目標裝置(例如，CM核心)之該特定交易類型之一交易。

在一些實施例中，由根授權機構基於模組範本而產生模組。可

由CRISP裝置110透過類似於裝置定義之分發之一機制分發模組範本。模組範本基於該模組需要支援之使用案例本質上定義一模組之一類型。在相同生產階段運行為器具裝置與CM核心之間的一單一互動集之使用案例可使用組合所期望功能性集之一模組範本。基於此模組範本，將在根裝置102上建立一特定chipSeries資料集之一模組。此模組將連同模組部署訊息分發至器具叢集，以執行與CM核心進行之互動以提供組合資料至目標裝置。

模組管理可劃分成兩個不同CM功能性片段：模組匯入及模組部署。在一高層級下，模組匯入為在一器具裝置可將一模組載入至其HSM中並使用其來服務測試器裝置請求之前需要執行者。然而，若未接收並處理用於一特定模組之模組部署訊息，則將無法執行其功能。模組部署訊息遞送用以加密該模組內之敏感資訊之一模組金鑰(moduleKey)。此外，模組部署訊息將一模組繫結至一特定叢集。該模組可根據一慣例予以命名，諸如用包含對以下項之一描述之一複合描述符命名：模組功能性(與模組範本名稱相同)、一模組域、對模組範本參數之一參照、及一版本。例如，在開發模式中對一產品提供序列化、cvdak (ChipVendorDeviceAesKey) 及 padak (ProvisioningAuthorityDeviceAesKey)程式化功能性之一模組之名稱將為：srl_cvdak_padak_productname_dev_01，其中最後一個參數為該版本，其在技術上不是該名稱之一部分，但通常隨附於該名稱。模組範本參數可在模組建立期間予以提供且可被賦予一參照(控制代碼(handle))。此等參照變成該模組之名稱之部分。例如，srl_cvdak_padak模組範本需要一開發模式。模組範本編碼該需求，且根CLI提示根操作者鍵入該模式以及參照(別名)以供挑選。此參照將用以識別該模組。例如，在命名為srl_cvdak_padak_productname_dev_01之模組中，「dev」為對模組範本

參數之參照。

由根裝置102藉由將一模組範本轉變成一模組而產生模組。模組範本本身為一模組。即，模組範本為在根裝置102內之HSM解譯器上運行之一程式。模組範本執行結果為另一模組。模組範本定義將由該模組回應於來自測試器裝置112之一請求而執行之泛型功能性。例如，可建立一模組範本以執行序列化、提供序號至CM核心中等。然而，可需要關於CM核心之一些特定資訊來建構模組以執行序列化。該模組範本可由根HSM上之一解譯器運行以產生一模組。

在一項實施例中，在一TAR檔案庫303中在根裝置102、服務裝置104與器具裝置108之間傳送該模組。服務裝置104可保存一特定模組並在不同模組部署授權下再次使用其以將其部署於不同器具叢集上。模組本身為部署中立(deployment-neutral)，換言之，模組可部署於任何器具叢集上。模組部署訊息為將該模組繫結至一器具叢集之訊息，其包括提供 moduleKey，運用 clusterKey 加密，待遞送至該器具/HSM。該器具裝置驗證一模組部署訊息上之簽名，檢查該器具裝置是否屬於該訊息中指定之器具叢集並將其傳遞至該HSM，在HSM處解除包裝(unwrapped)並儲存該 moduleKey。

在一項實施例中，根裝置102包含一處理器及經組態以連接至一可抽取式儲存裝置之一可抽取式儲存裝置介面。該處理器可操作以接收用以建立一模組之一命令。回應於該命令，該處理器執行一模組範本以產生該模組。該處理器例如藉由將該模組儲存至該可抽取式儲存裝置而將該模組部署至一器具裝置。特定言之，該處理器經由該可抽取式儲存裝置介面將該模組儲存於該可抽取式儲存裝置中以將該模組傳送至一服務裝置，且該服務裝置經組態以透過一網路將該模組分發至該器具裝置。在一些實施例中，該處理器可運用來自一操作者之PCD、金鑰、輸入(例如，與一特定交易類型相關聯之一引數)或其任

何組合來產生該模組。在另一實施例中，該處理器可運用用於隨後提供之資料之一預留位置來產生該模組，如本文中所描述。該處理器可產生一模組部署授權並將該模組部署授權儲存於該可抽取式儲存裝置中，以將該模組部署授權傳送至一服務裝置，以透過一網路將該模組分發至該器具裝置。

在一項實施例中，器具裝置108包含一處理器、耦合至該處理器之一網路介面及一測試器裝置介面。該處理器透過該網路介面接收來自一服務裝置之一模組且透過該測試器裝置介面接收來自一測試器裝置之一CM用戶端庫之一通信。該CM用戶端庫為從該測試器裝置提供至CM器具叢集之一介面之一功能集。回應於該通信，該處理器基於該通信中之一引數調用該模組以產生一模組序列。在一目標裝置之一製造生命週期之一操作階段中，該處理器將該模組序列發送至該CM用戶端庫以供該測試器裝置運行，以將該模組序列遞送至該目標裝置之一CM核心。在一進一步實施例中，器具裝置108包含一HSM，其可操作以組譯測試器資訊及PCD、簽署一DSB，並運用該測試器資訊、該PCD及該DSB建立該模組序列。在另一實施例中，該測試器裝置經組態以將該模組序列遞送至該目標裝置之CM核心作為一測試指令碼之部分。

圖4為根據一項實施例之建立一模組並將其部署至一器具裝置之一方法400之一流程圖。可由可包括硬體(例如，電路、專用邏輯、可程式化邏輯、微程式碼等)、軟體、韌體或其組合之處理邏輯執行方法400。在一項實施方案中，圖1至3之根裝置102執行方法400。在其他實施方案中，本文中所描述之CM系統100之其他組件可執行方法400之操作之一些或所有。

參考圖4，方法400開始於處理邏輯接收用以建立一模組之一命令(方塊402)。該模組係在一目標裝置106 (目標裝置106之CM核心)之

一製造生命週期之一操作階段中安全地提供一資料資產至該目標裝置之一第一應用程式。回應於該命令，該處理邏輯執行一模組範本以產生該模組(方塊404)。該模組範本為定義該模組及該資料資產之一指令集之一第二應用程式。該處理邏輯將該模組部署至一器具裝置(方塊406)，且方法400結束。該模組之指令集在由該器具裝置執行時導致一操作序列之一安全建構安全地提供該資料資產至該目標裝置。該器具裝置經組態以將該資料資產分發至該目標裝置之一密碼編譯管理器核心。

在一進一步實施例中，該處理器邏輯判定是否已接收預先計算資料(PCD)(方塊408)，預先計算資料含有該資料資產(方塊408)。當在方塊408處已接收PCD時，該處理邏輯運用該PCD產生該模組(方塊410)，且返回至方塊406以將該模組部署至該器具裝置。在另一實施例中，該處理邏輯從一根資料庫擷取一金鑰且該處理邏輯運用該PCD及該金鑰產生該模組。在一進一步實施例中，該處理邏輯接收來自一根操作者之輸入，該輸入包含與一特定交易類型相關聯之引數。該處理邏輯運用該PCD及該等引數產生該模組。如本文中所描述，該處理邏輯可運用待由該器具裝置提供之資料之一預留位置來產生該模組。

如本文中所描述，該處理邏輯可藉由將該模組儲存於一可抽取式儲存裝置中以將該模組傳送至一服務裝置而將該模組部署至該器具裝置。該服務裝置經組態以透過一網路將該模組分發至該器具裝置。

在另一實施例中，該處理邏輯產生一模組部署授權，並將該模組部署授權儲存至一可抽取式儲存裝置以將該模組部署授權傳送至一服務裝置，且該服務裝置經組態以透過一網路將該模組部署授權分發至該器具裝置。在一進一步實施例中，該處理邏輯運用一根模組私密金鑰來簽署該模組。

圖5為根據一項實施例之將一模組部署至一測試器裝置之一CM程

式庫之一方法500之一流程圖。可由可包括硬體(例如，電路、專用邏輯、可程式化邏輯、微程式碼等)、軟體、韌體或其組合之處理邏輯來執行方法500。在一項實施方案中，圖1至3之器具裝置108執行方法500。在其他實施方案中，本文中所描述之CM系統100之其他組件可執行方法500之操作的一些或所有。

參考圖5，方法500開始於處理邏輯透過一網路接收來自一服務裝置之一模組(方塊502)。該處理邏輯判定是否接收來自一測試器裝置之一CM用戶端庫之一通信(方塊504)。若未接收到通信，則該處理邏輯繼續判定直至接收一通信為止。該通信包含來自該CM用戶端庫之一引數。回應於該通信，該處理邏輯基於該引數而調用該待執行模組以產生一模組序列(方塊506)。該處理邏輯將該模組序列發送至該CM用戶端庫(方塊508)，且方法500結束。在一目標裝置之一製造生命週期之一操作階段中，該測試器裝置之一測試器指令碼遞送該模組序列至該目標裝置之一CM核心。

在一進一步實施例中，該處理邏輯組譯測試器資訊及PCD，簽署一DSB，並運用該測試器資訊、該PCD及該DSB來建立該模組序列。該處理邏輯可指示各自裝置之一HSM以組譯測試器資訊及PCD，簽署該DSB並建立該模組序列。該測試器裝置經組態以將該模組序列遞送至該目標裝置之CM核心作為一測試指令碼之部分。

預先計算資料(PCD)

預先計算資料(簡稱PCD)用作至該模組之輸入。PCD產生及封裝可取決於PCD之類型而發生於該CM系統之不同部分上。具體言之，PCD可由CM根或CM服務完成。大體言之，不同類型之PCD對應於不同客戶使用案例且因此對應於不同模組。然而，此對應性並非一對一(或成映射)。一些模組無需PCD(例如，一除錯解鎖模組)，而其他模組可能需要多種類型之PCD，諸如一組合式

Serialization/Perso1/Perso2模組。多個模組亦可能消耗一單一類型之PCD。例如，可能由若干不同模組消耗格式化為PCD之HDCP金鑰。PCD資產之產生可或可不在CM系統100內發生，即，HDCP金鑰匯入至CM系統100中、非產生。在此情況下，PCD封裝為資產以一PCD形式引入至CM系統100中之一階段。對於一些類型之預先計算資料(諸如HDCP金鑰)，可由該服務執行PCD封裝。對於其他類型(諸如Perso1)，將由CM根授權機構執行PCD封裝。該CM根授權機構為授權模組、CM器具裝置及叢集並產生PCD之一受信任、離線實體。該CM根授權機構不連接至該CM系統。一第三選項為一提供授權機構(例如，CRISP裝置110)直接提供經封裝PCD至該CM服務中。該CM服務為由客戶或Cryptography Research Inc.代管之中央管理CM系統。該CM服務管理CM器具叢集之分發網路及預先計算資料(PCD)資產、票證授權、簽署序列及模組跨CM器具裝置之網路之提供。下文描述PCD部署授權之傳訊。

在一項實施例中，根裝置102包含一處理器及經組態以連接至一可抽取式儲存裝置之一可抽取式儲存裝置介面。該處理器可操作以接收用以產生一目標裝置之一PCD資產之一第一命令，該PCD資產為該目標裝置獨有。回應於該第一命令，該處理器產生該PCD資產並封裝該PCD資產以將該PCD資產安全地部署至該目標裝置且由該目標裝置獨佔使用。該處理器將該經封裝PCD資產部署於一CM系統中以識別並追蹤該目標裝置。在一進一步實施例中，該處理器進一步可操作以接收用以基於一PCD範本批量地產生一PCD資產集之一CLI命令，其中該PCD範本為該等PCD資產如何格式化為用於一特定類型模組之一輸入之一描述。該處理器產生該PCD資產作為該PCD資產集之批量產生之部分並封裝該產生PCD資產用於安全部署。該處理器透過一網路將該封裝PCD資產分發至該CM系統之一器具裝置。該器具裝置使用

該特定類型模組之一模組安全地提供該PCD資產至該目標裝置之一CM核心，該模組為在由該器具裝置執行時導致在該目標裝置之製造生命週期之一操作階段期間一操作序列之一安全建構安全地提供該PCD資產至該目標裝置之一應用程式。

在另一實施例中，服務裝置104包含一處理器及經組態以連接至一可抽取式儲存裝置之一可抽取式儲存裝置介面。該處理器可操作以接收用以封裝用於一目標裝置之一PCD資產之一第一命令。回應於該第一命令，該處理器封裝該PCD資產以將該PCD資產安全地部署至該目標裝置且由該目標裝置獨佔使用。該處理器將該經封裝PCD資產部署於一CM系統中以識別並追蹤該目標裝置。在一進一步實施例中，於該CM裝置外部產生該PCD資產。回應於該第一命令，該處理器進一步可操作以匯入該PCD資產，封裝該匯入PCD資產用於安全部署，並透過一網路將該經封裝PCD資產分發至該CM系統之一器具裝置。該器具裝置使用一模組安全地提供該PCD資產至該目標裝置之一CM核心，該模組為在由該器具裝置執行時導致在該目標裝置之製造生命週期之一操作階段期間一操作序列之一安全建構安全地提供該PCD資產至該目標裝置之一應用程式。

圖6為繪示根據一項實施例之用於PCD部署授權600之圖1之CM系統之裝置之間的訊息之一圖。對於PCD部署授權，CRISP裝置110提供含有一PCD產生器、一PCD範本及一模組範本ID之一訊息602至根裝置102。在另一實施例中，訊息602包含一PCD範本、一模組範本ID、一PCD包裝公開金鑰、一PCD包裝金鑰參照等。一額外訊息可包含由一實體簽署金鑰簽署之一PCD包裝公開金鑰。可藉由一CRISP模組金鑰簽署訊息602。該服務(包含服務裝置104 (主)及服務裝置104 (DR)以及一共用資料庫及儲存裝置)接收一訊息604以匯入一CM根封裝PCD。訊息604可包含資料(例如，AEAD_pcdinstanceKey(record))之一

標頭及一有效負載。對於CM根產生/封裝PCD，一CLI命令集可供一操作者用以基於接收自CRISP裝置110之訊息602中之一PCD範本批量地產生PCD資產。可使用一可抽取式儲存裝置(諸如一USB快閃隨身碟)將批量PCD資產從根裝置102匯出並匯入至CM服務中。服務裝置104亦可運用PCD金鑰傳送/服務封裝PCD匯入一訊息606。訊息606可包含運用一共同服務HSM金鑰(例如，E_commonServiceHSMKey(pcdinstanceKey))加密(包裝)之一PCD例項金鑰。替代地，訊息606可包含一封裝識別符、PCD類型、票證類型、記錄格式、記錄索引類型、記錄個別識別符長度、記錄大小等。訊息606可由一根授權金鑰簽署以供服務裝置140驗證。如所描繪實施例中繪示，服務裝置104及器具裝置108將各種資料儲存於其各自HSM或硬碟機或共用儲存裝置中。

在一項實施例中，於該目標裝置外部產生用於一目標裝置之一唯一敏感資料資產集。一CM裝置安全地封裝該唯一敏感資料資產集以確保該唯一敏感資料資產集由該目標裝置獨佔使用。該CM裝置將該經封裝唯一敏感資料資產集分發至該目標裝置以提供該目標裝置之後續識別及追蹤。

下文描述PCD產生及部署之各項實施例。PCD可儲存於記錄中並予以加索引。藉由一索引參照各項目(各PCD記錄)。各項目含有未加密資料、加密資料及訊息鑑認碼(MAC)(例如，一金鑰密碼編譯雜湊函數)之一或多個欄位。可能出於偵測資料複製之目的解析未加密資料。項目中之共同資訊可包含與PCD相關聯之檔案類型、票證類型、及後設資料。該後設資料可指定何處可使用該PCD。PCD記錄應為唯一且各PCD記錄可具有一全域唯一識別符。該全域唯一識別符對循序存取PCD而言係循序的。通常，該等全域唯一識別符對票證控制PCD而言係循序的。在其他實施例中，該全域唯一識別符對表查找PCD而

言係非循序的，其中該系統中之各個別PCD記錄映射至一個以上唯一票證。在一些組態中，一個票證可能應用於一個以上PCD記錄，但不可藉由一個以上票證參照一單一PCD記錄。可循序地存取PCD記錄，或使用表查找存取(隨機存取)PCD記錄。在一些實施方案中，存在大數目個PCD記錄項目且PCD檔案格式應支援大數目(2^{32})個記錄。該PCD檔案格式亦可結構化成相對較緊密而甚至無需檔案檔案壓縮。在其他實施方案中，PCD可經結構化以允許驗核PCD檔案標頭及個別PCD項目，而無需具備密碼編譯金鑰之知識。此稱為資料保護之非金鑰完整性檢查，從而允許偵測檔案損毀，而無需具備密碼編譯金鑰之知識。PCD亦經結構化以允許金鑰完整性檢查，其中擁有密碼編譯金鑰之一實體亦可能驗核整個項目。即，可在解密已加密內容之後驗核該等內容。此可避免惡意操控或金鑰管理問題。

在一些實施方案中，PCD檔案可被分塊(chunk)(分割成不同檔案)，而無需具備密碼編譯金鑰之知識且無需變更批量資料欄位。一單一加索引PCD項目可按允許對PCD項目、PCD類型及票證類型進行一完全金鑰完整性檢查之一方式傳遞至一HSM。PCD可作為一單一完全可驗核項目傳遞至HSM。此可係票證繫結之強制執行所需要的。

如本文中所描述，可由根、服務、CRISP或第三方產生或匯入PCD。模組及模組範本可參照PCD，但PCD不參照一模組。CRISP裝置110可用以建置PCD範本及檔案格式，且根裝置102可建立、追蹤並管理PCD具現化(instantiation)。一PCD具現化應落於CRSIP提供之範本規格內。然而，該根具有識別一PCD具現化、指定該PCD之參數、將票證連結至PCD及將模組連結至PCD方面之判斷力。PCD產生方應在產生PCD之前接收關於該PCD具現化之資訊。可在一PCD檔案或一PCD獨立記錄中管理及分發該PCD。該PCD檔案為用於多個PCD記錄之一儲存機構。可操控及參照PCD檔案，而無需具備密碼編譯金鑰之

知識。PCD檔案格式為用於PCD儲存及傳輸之主機制。CM服務以此形式匯入並儲存PCD。該PCD獨立記錄為提供至HSM用於解密、鑑認及票證合規性檢查之一「完整」PCD記錄，如圖7至8中所繪示。

圖7為繪示根據一項實施例之在產生及匯入時之一個循序PCD檔案702及在重新分塊(re-chunk)之後的兩個循序PCD檔案之一流程圖700。循序PCD檔案702可係循序的且含有循序地加索引之記錄。在該檔案內之索引與記錄位置之間存在一直接對應性。此等檔案通常遞送循序地消耗之資料。如圖7中所繪示，循序PCD檔案702含有一內標頭704、一外標頭706及多個PCD記錄708至712。內標頭704含有被PCD記錄708至712共用之資訊。內標頭704在產生循序PCD檔案702之後不被修改且在重新分塊循序PCD檔案702時被複製。外標頭706含有關於特定PCD檔案例項之資訊。可在重新分塊循序PCD檔案702時修改外標頭706。PCD記錄708至712為個別PCD記錄，由在該內標頭中之一recordFormat識別符指定各PCD記錄。對於儲存效率，來自內標頭及外標頭之資訊未複製於PCD記錄708至712中。圖7亦繪示在循序PCD檔案702之一重新分塊之後的一循序PCD檔案。在此情況下，新外標頭714及716經產生以含有關於在重新分塊之後的特定PCD檔案例項(PCD檔案718及PCD檔案720)之資訊。內標頭704及PCD記錄708至712保持相同，但現在在兩個單獨PCD檔案718及720中運用PCD檔案718中之PCD記錄708及709以及PCD檔案720中之PCD記錄710至712予以表示。PCD記錄708至712可為獨立記錄，如同PCD記錄708之PCD獨立記錄722。獨立記錄722可包含可藉由一索引存取之一獨立記錄標頭724。獨立記錄標頭724可傳輸有或隱含有PCD記錄708。此資料結構為可藉由其鑑認及解密一單一加索引PCD項目之手段。例如，CM器具裝置軟體以此形式將PCD獨立記錄722之資訊傳遞至HSM。在無額外PCD資訊之情況下，該HSM能夠完全地解密且鑑認PCD及票證。可

自循序PCD檔案702、718、720之任一者建立PCD獨立記錄722。建立一獨立記錄之程序無需密碼編譯金鑰。記錄708可含有一MAC、一加密資料區域、或兩者。執行此等密碼編譯操作所需要之初始化向量(IV)及相關聯資料全部存在於一獨立記錄722內。在一些實施方案中，在一PCD記錄傳輸至該HSM時，隱含且不傳輸獨立記錄標頭724。

圖8為繪示根據一項實施例之在產生及匯入時之兩個非循序PCD檔案802、820及在合併之後的一個非循序PCD檔案822之一流程圖800。PCD檔案亦可係非循序的。此等檔案含有依一非循序索引進行排序之記錄。PCD檔案802、820可係非循序的且含有依一非循序索引進行排序之記錄。運用一索引查找來參照一檔案記錄，且此等檔案有時稱為查找PCD。如圖8中所繪示，PCD檔案802含有一內標頭804、一外標頭806及多個PCD記錄808至812。內標頭804在與PCD檔案820合併之後不被修改。在排序840及合併記錄808至812之後產生PCD檔案822且複製內標頭804。外標頭806含有關於特定PCD檔案例項(PCD檔案802)之資訊。外標頭806可在合併PCD檔案802 (諸如與PCD檔案820合併)之後被修改。PCD檔案820亦包含一內標頭804及一外標頭844。內標頭804相同，但外標頭844含有關於PCD檔案820之資訊。PCD記錄808至812為個別PCD記錄，由在各自內標頭804中之一recordFormat識別符指定各PCD記錄。在此實例中，PCD檔案802包含兩個PCD記錄808、809，且PCD檔案820包含三個PCD記錄808至812。對於儲存效率，來自內標頭及外標頭之資訊未複製於PCD記錄808至812中。圖8亦繪示在其中對PCD記錄808至812進行排序840之一合併之後的一非循序PCD檔案822。產生一新外標頭846。外標頭846含有關於具有經排序之PCD記錄808至812之PCD檔案820之資訊。內標頭804及PCD記錄808至812保持相同，但現在在一個非循序PCD檔

案822中運用排序PCD記錄808至812予以表示。PCD記錄808至812可為獨立記錄，如同PCD記錄808之PCD獨立記錄826。獨立記錄826可包含可依一索引經由一查找842存取之一獨立記錄標頭824。獨立記錄標頭824可傳輸有或隱含有PCD記錄808。此資料結構為可藉由其鑑認及解密一單一加索引PCD項目之手段。例如，CM器具裝置軟體以此形式將PCD獨立記錄826之資訊傳遞至HSM。在無額外PCD資訊之情況下，該HSM能夠完全地解密且鑑認PCD及票證。可自循序PCD檔案802、820、822之任一者建立PCD獨立記錄826。建立一獨立記錄之程序無需密碼編譯金鑰。記錄808可含有一MAC、一加密資料區域、或兩者。執行此等密碼編譯操作所需要之初始化向量(IV)及相關聯資料全部存在於一獨立記錄826內。在一些實施方案中，在一PCD記錄傳輸至該HSM時，隱含且不傳輸獨立記錄標頭824。

圖9為繪示根據一項實施例之模組、PCD及票證關係之一圖。PCD定義為記錄格式902 (recordFormat)、PCD範本904及PCD類型906 (pcdType)。記錄格式902識別一特定按每記錄之資料結構。PCD範本904識別用於一特定目的之PCD資產之一類別，且每個PCD範本904參照一個記錄格式902且包含用以描述如何產生或使用PCD檔案之後設資料。應注意，模組範本908指代一特定PCD範本904。在CM根撰寫一模組910時，操作者指定對應於指定PCD範本904之PCD。PCD類型906為用於一PCD資產之一特定例項之一識別符。每個PCD類型906參照一個PCD範本904。CM根建立新PCD類型906。在PCD類型906建立時，關聯、票證繫結、金鑰及參數係固定的。操作系統將在一段時間後累積記錄格式902、PCD範本904及PCD類型906之新識別符。由於此等定義以不容易重新呼叫(recall)之方式展透(percolate)系統，故在已建置記錄格式902、PCD範本904及PCD類型906之定義之後不應變更。遷移涉及在一段時間後建立一新定義且取代舊定義。一特定PCD

類型906對應於一票證類型912。票證類型可為測試、開發、生產等。

下文實施例描述如何定位一PCD記錄。對於循序資料，基於記錄大小(在一內標頭中指定)及索引範圍(在一外標頭中指定)判定該檔案中之一記錄位置。對於非循序資料，執行一索引搜尋。記錄在一記錄之前N個位元組中儲存有如由recordIndividualIdentifierLength指定之索引。由於一單一PCD檔案可不含有完全加索引空間，故必須在判定一PCD檔案是否含有該所討論索引之前解譯由該外標頭指定之循序索引範圍。

在循序資料之一些實施例中，該循序資料加票證有必須相同地匹配循序索引之一票證索引。期望PCD元素與票證之間存在一強唯一繫結關係。另一方面，可不對非訊息資料加票證。儘管HSM模組調用受限於一票證，但一票證不可能映射至非循序索引。

在一些實施方案中，循序PCD檔案可分成更小檔案以：(1)分配不同包裹(swath)至不同CM服務或CM器具裝置；或(2)產生可在CM服務與CM器具裝置連接之間通信之更小細微度PCD。

諸多種類之recordFormat可經定義以將各種量及類型之資料儲存於PCD記錄中，用於系統程序中之各個點處。innerHeader中之recordFormat欄位之值可用於指示用於PCD之recordFormat之種類。一些例示性記錄定義可為：序列化資訊、個人化資訊、裝置識別符、各種種類之金鑰(例如，提供授權機構金鑰、HDCP金鑰、裝置金鑰等)、前述項之一組合。下文為PCD recordFormat定義之一實例：

指派至一recordFormat之各值將表示一PCD記錄之一不同種類之recordFormat。各種類之PCD記錄可儲存各種類型之資料，諸如金鑰、裝置識別符及其他資訊。此等值可經加密或未經加密，且完整性檢查值亦可包含於PCD中。

例如，可定義一系統，其中一recordFormat (在該系統中例如運

用innerHeader中之一值「2」進行表示)可儲存資料以包含於一目標裝置之提供中。此資料可包含一裝置識別符、一晶片系列識別符、及各種金鑰值。此資料可經加密或解密，且包含記錄中資料之完整性檢查值。下表中提供一獨立記錄中之RecordFormat 2之一實例(17個位元組)。

recordFormat 2之獨立記錄			
類別	欄位	位元組	描述
隱含標頭中之資料	deviceIdSequential	0	非模糊裝置識別符。全域唯一識別符由(chipSeries、devciceIdSequential)組成。 <i>隱含且不儲存索引。</i>
未加密	deviceId	8	模糊裝置識別符。 <i>[recordIndividualIdentifierLengt h=8]</i>
	deviceIdCheck	1	deviceId之完整性檢查值
完整性檢查	keyedIntegrityCheck	8	內標頭+記錄之MAC。

其他recordFormat值將指示具有不同類別、不同欄位及大小、不同描述及不同值之一不同種類之PCD記錄。另一實例為指示一HDCP金鑰之一PCD之一recordFormat值。此一PCD可保存資料，諸如循序HDCP索引、一HDCP金鑰集、一金鑰選擇向量(KSV)、及一完整性檢查值。

一recordFormat可經設定以散佈大數目個多樣化deviceId特有金鑰。該檔案可儲存成使能夠快速擷取一加密金鑰值之一形式。除非另有指定，否則PCD檔案應經管理且儲存有藉由該索引進行排序之記錄，其可為例如未加密記錄資料之前幾個位元組。

pcdTemplate定義一PCD記錄格式且提供關於如何產生/使用該等記錄之背景。在內標頭中藉由pcdTemplate識別符參照pcdTemplate。下表中展示pcdTemplate欄位之一實例。

由pcdTemplate指定之欄位之清單	
名稱	描述
recordFormat	指定記錄類型及記錄大小。
recordIndexType	指定檔案組織及加索引方案。 0 = RESERVED (保留) 1 = SEQUENTIAL。循序地加索引於記錄。 2 = NON_SEQUENTIAL。運用數字遞增索引對記錄進行排序。
recordMetadata	在內標頭及單元素標頭中載送此固定長度的後設資料欄位。 由pcdTemplate指定recordMetadata之格式及結構。 亦可由pcdTemplate指定recordMetadata中之一些欄位。

下表包含PCD產生輸入。PCD產生程序之一實例可包含以下全域動作：檢查一特定PCD類型之產生所需之值之存在；語義驗證與所討論PCD類型之域相關聯之後設資料；檢查新產生PCD之潛在重複。該PCD產生程序可包含以下預先記錄動作：導出deviceID；導出每個裝置的金鑰；及計算包含於PCD記錄中之完整性檢查。

圖10為根據一項實施例之一PCD產生程序1000之一流程圖。PCD產生程序1000涉及：(1)對於各裝置產生輸出範圍中之模糊deviceId值(方塊1002)；(2)導出相關聯基底金鑰(base key)(方塊1004)；及(3)執行一多樣化操作(1006)。在其他實施例中，可使用產生資料集之其他手

段，諸如使所有 `deviceId` 值及測試計數器之 SNE 遞增。代表小數目加密之 SNE 用於使序號隨機出現以免顯露關於生產良率之任何資訊。查找表 PCD 之產生接近相同於 `pcdTemplate 0x0001 0001` 之程序。

PCD 類型定義：`pceType` 建立於 CM 根處且參照一 `pcdTemplate`。下表中展示在建立期間由 `pceType` 指定(且在 CM 根處具現化 `pceType` 時選擇)之例示性欄位。

在 <code>pcdType</code> 建立時指定之欄位	
名稱	描述
Name / Alias	此在根文件中指定；其不是檔案格式之當前部分。
<code>pcdTemplate</code>	在 <code>recordMetadata</code> 中指定 <code>recordFormat</code> 及欄位。
<code>ticketType</code>	在一記錄之前所需要之票證類型可被一 CM 模組消耗。可藉由 (<code>ticketType</code> 、 <code>pcdRecordIndex</code>) 唯一地參照 PCD 檔案中之各記錄
<code>pcdTypeKey</code>	PCD 資料之 AES256 金鑰。此金鑰對於各 <code>pcdType</code> 產生且由根維持。
<code>recordMetadata</code>	此欄位由 <code>pcdTemplate</code> 指定。此欄位中之一些元素由 <code>pcdTemplate</code> 固定，其他元素在 <code>pcdType</code> 具現化時固定。

PCD 類型資訊從 CM 根傳達至 CM 服務 (PCD 管理)、基於服務之 PCD 產生器/匯入工具 (HDCP)、或第三方 PCD 產生器/匯入工具 (`provisioningAuthority`)。可完成 PCD 加密及完整性檢查。且由 `recordFormat` 指定密碼編譯方案。PCD 可加密。下表包含 PCD 加密金鑰。

PCD加密金鑰		
欄位	位元組	描述
pcdTypeKey	x	PCD資料之金鑰(例如, AES256)。此金鑰對於各 pcdType產生且由根維持。 其以加密形式匯出用於模組參照pcdType。其亦匯出至 PCD建立器或PCD匯入器。

對於高頻寬數位內容保護(HDCP)，匯入程序在一單一步驟中將金鑰檔案從數位內容保護LLP直接轉譯成PCD格式。HDCP在將內容傳輸為一數位資料串流以供顯示時加密並保護該內容。參與顯示鏈之任何裝置需要一HDCP金鑰來運作。HDCP由Intel®公司開發；由Intel®公司之子公司Digital Content Protection (LLC)處置HDCP技術之授權(licensing)。一HDCP金鑰包含40個56位元私密值(金鑰)、及一個非私密40位元值(金鑰選擇向量, KSV)。圖11中概述HDCP匯入程序。

圖11為繪示根據一項實施例之一HDCP匯入程序1100之一網路圖。HDCP匯入程序1100開始於(1)接收、加密並上載新HDCP金鑰至服務裝置(方塊1102)。將加密HDCP金鑰傳播至器具裝置(2)(方塊1104)，以將該等加密HDCP金鑰新增至一循序資料庫(3)(方塊1106)。根提供一根簽署區塊(RSB)及提供資料(4)(方塊1108)，以傳播至器具裝置(5)(方塊1110)。器具裝置經由測試器裝置讀取CM核心之deviceId(6)(方塊1112)且該測試器裝置傳回deviceID(7)(方塊1114)。該器具裝置基於該deviceId查找derivedKey(8)(方塊1116)。從循序DB擷取一HDCP金鑰，運用輸送金鑰解密該HDCP金鑰，且運用derivedKey包裝該HDCP金鑰(9)(方塊1118)。該器具裝置建構一序列以燒錄該包裝金鑰(10)(方塊1120)。將該序列發送至CM核心(11)(方塊1122)，該CM核

心執行該序列且經由中斷或狀態更新對器具裝置指示程序完成(方塊 1124)。

在匯入端上，HDCP金鑰被指派一唯一循序遞增的64位元PCD索引用於UID指派。該單一PCD索引用於參照目的及加票證目的兩者。一完整重複檢查可(由KSV)執行為匯入程序之部分。一特定PCD類型內之非獨立加索引HDCP記錄可具有一重複KSV。偵測到複製導致拒絕整個匯入集且需要手動干預來解決。此允許在匯入端上對重複KSV進行綜合封鎖。在其他實施方案中，可在匯入端上完成一例行性重複檢查。此可為匯入程序開始時之一快速返回重複檢查。此檢查之目的為提供快速回饋至已匯入HDCP磁碟之一使用者。該快速返回檢查無需完全綜合且可使用KSV或其他檢查機制。

在其他實施方案中，在可消耗一HDCP記錄用於票證強制執行之前，CM器具裝置需要一CM服務發佈、記錄特有、密碼編譯票證。完整CM加票證系統必須強制執行HDCP金鑰提供之單次使用且唯一本質。該CM服務裝置可追蹤所有發佈之KSV值之一歷史且若在基於日誌之檢查中偵測到複製則發佈一警報。重複檢查可基於以下項執行：

- (1) CM器具裝置參照之KSV之日誌；
- (2) 具有KSV之CM器具裝置序列之日誌；
- (3) CM器具裝置之消耗票證之日誌；
- (4) 測試器裝置日誌等。

該系統可追蹤足夠後設資料以使能夠識別一違規複製。例如，在該系統處於一健康操作模式時，可在提供動作4小時內傳回基於日誌之警報。在其他實施例中，加票證可應用於除如本文中所描述之HDCP金鑰提供外之情況。

對於資料安全，CM器具裝置僅可存取/操控HSM內之未加密HDCP金鑰。在不具備密碼編譯金鑰之知識之情況下，必須以PCD形式讀取KSV值。此使CM服務裝置及CM器具裝置能夠執行重複檢查。

圖12為根據一項實施例之在一HDCP生命週期中之一傳入HDCP

資產 1202 之一匯入程序 1200 之一流程圖。使用 PGP 金鑰及複雜密碼 (passphrase) 1204 解密 HDCP 資產 1202 (方塊 1206)。對 KSV 資料庫 1208 執行一基本完整性檢查以確認正確心 PGP 解密 (方塊 1210)。此可為一快速例行性重複檢查以確保先前未匯入相同 HDCP 金鑰檔案。此檢查之目的為提供快速回饋至已匯入 HDCP 磁碟之一使用者，其中可在該 HDCP 生命週期中之一後期階段處執行一綜合檢查。產生檔案標頭 (方塊 1212)。將一 PCD 索引指派至各記錄 (方塊 1214)。使用一 UID 計數器 1216，索引係循序的。一旦已指派一索引，則不再使用該索引。將 PCD 記錄加密 (方塊 1218) 至一 PCD 檔案 1222 中。對先前產生並儲存於重複資料儲存區 1226 (標記為 DUP 檢查資料庫) 中之所有檔案執行一完整 KSV 重複檢查 (方塊 1224)。此程序確保：(1) 一 KSV 分配至僅一單一 UID；及 (2) 一 KSV 僅出現一次。用於 KSV 比較之備用資料庫包含 PCD 索引使得可定位/追蹤複製。應注意，若對一完全形成之 PCD 檔案執行該檢查，則相同程序可用於其他非 HDCP 資料。若複製檢查失敗，則可拒絕整個 PCD。若所有檢查成功地完成，則重複資料儲存區 1226 擴增新匯入之 KSV。CM 服務可擴增其索引追蹤資料庫以覆蓋新紀錄。此程序涉及一索引唯一性檢查以確保不存在重疊索引。由該 CM 服務提交該匯入。應認為，此時 HDCP 金鑰檔案之匯入及轉譯係成功的。

下文描述內容描述 PCD 生命週期決策。一個決策為序列化 PCD 之生命週期。序列化 PCD 通稱為晶圓測試 PCD。各記錄包含裝置序列化資料且視需要包含 perso1 金鑰分割。另一 PCD 生命週期決策為分配/設置程序，其中 CM 根每當一 chipSeries 或 chipId 變更時定義一新 pcdType，且 CM 根將一 pcdType 授權/定義傳達至 CM 服務裝置。另一 PCD 生命週期決策為產生相依性類型。由 CM 根經由一 cmCoreVersion 特有產生器產生 PCD。由 CM 根管理產生所需要之所有資料/程式碼。

另一PCD生命週期決策為生產產生。CM根產生PCD以對該CM服務賦予一足夠庫存，諸如6個月以上的庫存。建議，`deviceIdSequential`值之範圍分配至生產服務及非生產服務。PCD檔案可直接地匯入至CM服務中。

PCD生命週期之一實例為p5 PCD之生命週期。提供授權機構PCD由CRISP (作為提供授權機構)產生且直接地匯入至CM服務裝置中。對於分配/設置程序，CM根每當`cmCoreVersion`變更定義一新`pcdType`且將一`pcdType`授權/定義傳達至CM服務裝置時。該CM根將`pcdType`資訊傳達至CRISP。一安全且鑑認的手段用於傳輸`pcdType`資訊(特定言之，內標頭資料及`pcdTypeKey`)。CRISP產生(或選擇重新使用)與`provisioningAuthorityDeviceAesKey`相關聯之SNE參數、主控金鑰、及其他資料。對於產生相依性，由CRISP經由將CRISP管理之秘密用於金鑰產生及SNE序號產生之一產生器而產生此PCD。PCD (標頭、加密)之封裝需要由根採購之`pcdType`資訊。對於生產產生，CRISP產生PCD以對該CM服務賦予足夠庫存(例如，6個月以上)。PCD檔案直接地匯入至CM服務中。

PCD生命週期之一實例為金鑰查找PCD之生命週期。金鑰查找PCD用以遞送一多樣化基底金鑰群組。金鑰查找PCD經設計以存取為一查找表。金鑰查找PCD用於以下項之遞送多樣化值：藉由`deviceId`加索引之`chipVendorDeviceAesKey`；及藉由`provisioningAuthorityId`加索引之`provisioningAuthorityDeviceAesKey`。對於`chipVendorDeviceAesKey`之分配/設置決定，每當(1) `chipSeries`變更；(2) `chipId`變更；或(3)委派ID變更時，CM根定義一新`pcdType`。實際上，可對於一委派ID區塊一次建立數個`pcdType`。CM根將一`pcdType`授權/定義傳達至CM服務裝置。對於`provisioningAuthorityDeviceAesKey`之分配/設置決定，每當(1)

cmCoreVersion變更；或(2) ID變更時，CM根定義一新pcdType。實際上，可對於一委派ID區塊一次建立數個pcdType。CM根將一pcdType授權/定義傳達至CM服務裝置且將pcdType資訊傳達至CRISP。一安全且鑑認的手段用於傳輸 pcdType 資訊(特定言之，內標頭資料及 pcdTypeKey)。對於 chipVendorDeviceAesKey 之相依性之產生，由CM根產生PCD。由CM根管理產生所需要之所有資料/程式碼。對於 provisioningAuthorityDeviceAesKey 之相依性之產生，由CRISP產生PCD。CRISP管理之秘密用於金鑰產生及SNE序號產生。PCD (標頭、加密)之封裝需要由根採購之 pcdType 資訊。對於生產產生，通常大量地產生查找PCD。資料檔案可為大，例如500 M記錄安裝於一24 GB PCD檔案中(recordFormat 10具有48個位元組/記錄)。在具有AES-NI加速器之CPU核心上，效能相對較高。PCD檔案直接地匯入至CM服務中。

為了執行資產分發、模組部署、日誌收集及其他基本功能，服務需要獲得器具裝置管理之當前狀態。此使用一GetState訊息及相關JSON-RPC API呼叫完成。結合兩個其他訊息(PCD移除及模組移除)使用此方法允許服務適當地處置器具裝置之狀態。使用ServiceSigningPriv 簽署源自該服務之訊息，而使用ApplianceHsmSigningPriv簽署由器具裝置提供之訊息。

本文中所描述之實施例描述在一密碼編譯管理器(CM)環境中在一目標裝置之一製造生命週期之一操作階段中之預先計算資料(PCD)資產產生及該PCD資產至該目標裝置之安全部署。一項實施方案包含一根授權機構(RA)裝置，其接收用以產生用於一目標裝置之一唯一PCD資產之一第一命令。作為回應，該RA裝置產生該PCD資產並封裝該PCD資產，以將該PCD資產安全地部署至該目標裝置且由該目標裝置獨佔使用。該RA裝置將該經封裝PCD資產部署於一CM系統中以

識別並追蹤該目標裝置。

圖13為根據一項實施例之在一CM系統中產生並封裝一PCD資產用於安全部署之一方法1300之一流程圖。可由可包括硬體(例如，電路、專用邏輯、可程式化邏輯、微程式碼等)、軟體、韌體或其組合之處理邏輯執行方法1300。在一項實施方案中，圖1至3之根裝置102執行方法1300。在其他實施方案中，本文中所描述之CM系統100之其他組件可執行方法1300之操作之一些或所有。

參考圖13，方法1300開始於處理邏輯產生或匯入用於一目標裝置之一唯一PCD資產(方塊1302)。該處理邏輯接收用以封裝該唯一PCD之一命令(方塊1304)。該處理邏輯封裝該PCD資產以將該PCD資產安全地部署至該目標裝置且由該目標裝置獨佔使用(方塊1306)。該處理邏輯將該經封裝PCD資產部署於一CM系統中以識別並追蹤該目標裝置(方塊1308)，接著方法1300結束。

在一項實施例中，該處理邏輯駐留於一根裝置中。回應於該命令，該處理邏輯產生該PCD資產並封裝該產生PCD資產用於安全部署。可由該處理邏輯部署該PCD資產以將該經封裝PCD資產儲存於一可抽取式儲存裝置中，以將PCD資產傳送至該CM系統之一服務裝置。該服務裝置經組態以透過一網路將該PCD資產分發至該CM系統之一器具裝置。該器具裝置可使用一模組安全地提供該PCD資產至該目標裝置之一CM核心且該PCD資產為至該模組之一輸入。該模組為在由該器具裝置執行時導致一操作序列之一安全建構安全地提供該資料資產至該目標裝置之一應用程式。在一項實施例中，回應於一命令列介面(CLI)命令而產生PCD資產，以基於一PCD範本批量地產生PCD資產。該PCD範本為該等PCD資產如何格式化為用於一特定類型模組之一輸入之一描述。在一進一步實施例中，該PCD範本對應於一PCD類型，該PCD類型對應於具有一唯一性或序列化之至少一者之一特定

性質之一PCD資產集。可加索引於該PCD類型之PCD資產集。

在另一實施例中，該處理邏輯駐留於一服務裝置中。回應於該命令，該服務裝置產生並封裝該PCD資產用於安全部署。在另一實施例中，於該服務裝置外部產生該PCD資產，且該服務裝置之處理邏輯匯入該PCD資產並封裝該匯入PCD資產用於安全部署。

在一項實施例中，該匯入PCD資產為一HDCP金鑰。在其他實施例中，該產生PCD資產為如本文中所描述之一個人化金鑰或一序列化金鑰。該匯入PCD資產可由一根授權私密金鑰簽署且該處理邏輯可使用一根授權公開金鑰驗證該匯入PCD資產。

如上文所描述，該PCD資產可儲存於一獨立記錄中，或作為一PCD記錄儲存於含有至少一個額外PCD記錄之一PCD檔案中。該PCD檔案可為一循序PCD檔案或一非循序PCD檔案。該循序PCD檔案可包含：1)一內標頭，其含有被該PCD記錄及該至少一額外PCD記錄共用之資訊；2)一外標頭，其含有關於在該循序PCD檔案之任何分割之前該循序PCD檔案之一例項之資訊；以及3)該PCD記錄及該至少一額外PCD記錄。該非循序PCD檔案可包含：1)一內標頭，其含有被該PCD記錄及該至少一額外PCD記錄共用之資訊；2)一外標頭，其含有關於在一第一非循序PCD檔案及一第二非循序PCD檔案之一合併之後該非循序PCD檔案之一例項之資訊；及3)該PCD記錄及該至少一額外PCD記錄。

在一項實施例中，該處理邏輯可將該循序PCD檔案分割成一第一循序PCD檔案及一第二循序PCD檔案。該處理邏輯對於該第一循序PCD檔案產生含有關於該第一循序PCD檔案之資訊之一第一外標頭，使得在分割之後該第一循序PCD檔案包含內標頭、含有關於該第一循序循序PCD檔案之資訊第一外標頭、及PCD記錄。該處理邏輯亦產生含有關於該第二循序PCD檔案之資訊之一第二外標頭，使得在分割之

後，該第二循序PCD檔案包含內標頭、含有關於該第二循序PCD檔案之資訊之第二外標頭、及至少一額外PCD記錄。

在另一實施例中，該處理邏輯將一第一非循序PCD檔案及一第二非循序PCD檔案合併成該非循序PCD檔案。該處理邏輯對該PCD記錄及該至少一額外PCD記錄進行排序並產生該外標頭。在此實施例中，該第一非循序PCD檔案可包含：1)內標頭；2)含有關於該第一非循序PCD檔案之資訊之一第一外標頭；及3) PCD記錄。該第二非循序PCD檔案可包含：1)內標頭；2)含有關於該第二循序PCD檔案之資訊之一第二外標頭；及3)至少一額外PCD記錄。

票證

一票證可用於消耗及提供資料資產，諸如PCD資產。如本文中所使用，一票證可為使能夠強制執行目標裝置參數之使用計數限制及唯一性/循序發佈之一數位檔案或資料。在製造及/或測試期間，票證可由根授權機構授權且由目標裝置消耗。一票證可提供對該目標裝置之授權以消耗一資料資產，例如一預先計算密碼編譯金鑰。該票證亦可繫結資料資產以供該目標裝置消耗並用於記錄及稽核目的且可提供對個別資料資產之一庫存追蹤機制。此資訊可透過網路從製造設施傳達至客戶。

一票證或票證授權為一模組可需要其來進行一交易之一可驗證值。票證授權可被快速產生並驗證(對稱MAC)且可由一器具裝置本身或由一器具叢集同級予以發佈。一票證授權可包含一索引值(例如，以選擇預先計算記錄、產生序號)及一票證類型及請求識別符以防止誤用或重新使用。

一給定票證授權可賦予權限給該器具裝置使得其經繫結以運行一模組達特定次數，諸如一次。該票證授權可變為一序號，其接著或隨後經加密以產生一加密序號，或用作一預先計算資料索引以便參照

預先計算資料。該票證可由建立其之器具裝置或由一器具叢集同級予以消耗且可繫結至一特定請求。

資產管理系統中之票證及其使用可使能夠分離權限管理與操作及資料。例如，選擇HDCP金鑰之一票證類型可供多個模組使用。票證可允許一叢集成員共用授權同時經連接以防止序號、HDCP金鑰及/或其他認證或資料之重新使用。若器具叢集連線性斷線，則器具裝置可滿足自行票證需求。該等票證可用於強制限制一器具裝置或器具叢集可進行之交易次數。雖然連接器具裝置108，但服務裝置104 (服務107)可將更多票證授權分配至該等器具裝置。可基於需要或使用提供該等票證授權，或可提供更大量之票證授權，使得若連接性斷線，則器具裝置可運行達一定時間，在此期間可嘗試還原連線性。此可防止製造設施之當機時間。

一器具叢集中之各器具可包含一票證發佈者，其可為在管理票證授權之設備上之處理邏輯。該票證發佈者可操作以：追蹤叢集同級之可用票證資源；接收來自模組或同級之票證請求；將請求發送至一本端HSM常駐程式；或詢問一叢集同級之票證發佈者。該HSM可循序地發佈票證授權，受制於由服務裝置授權之範圍且可運用一有效票證或一錯誤訊息作出回應。

該等票證可用於監測資產庫存並評估該等資產之一狀態。該等資產之收集狀態由金鑰、在傳輸中且儲存於服務及器具裝置兩者上之資料資產(預先計算資料)及票證授權庫存組成。此可提供該等資產之一本端狀態，該狀態在製造設施本端。在客戶已在複數個設施處承包裝置製造之情況下，此本端狀態資料可與其他本端狀態資料組合以對該客戶提供全域狀態資料。

可在一使用者介面中提供該狀態資訊連同預測對工廠處之預先計算資料及票證授權之未來需求所需之資訊至該客戶。一旦可估計該

需求，則操作者可設定庫存使得由服務107分發一適當庫存邊限至各工廠器具叢集，以在未來生產中被消耗。給定一估計工廠消耗率，則可在該器具叢集上維持預先計算資料及票證授權之一適當最小容量，以在不存在工廠連線性之情況下保證一指定生產正常執行時間。

圖14為根據一項實施例之一加票證及HSM互動常駐程式(THID)組件1400之一方塊圖。THID組件1400包含一THID外部API 1402及一HSM API 1404。可提供一THID組件1400，以(特定言之)結合票證授權來管理器具裝置108之一HSM 111。此THID組件1400可對在一器具裝置108上(或在器具叢集109上)操作之其他組件提供一介面以存取HSM 111，用於機密性或完整性計算。此等計算或操作可為快速路徑操作1401或慢速路徑操作1403。快速路徑操作1401可被理解為源自一測試器裝置112以獲取票證或調用一模組之時間關鍵操作，而慢速路徑操作1403可被理解為源自一服務佇列1408之操作，或不是快速路徑操作1401之操作。慢速路徑操作1403可為將票證從服務107新增至器具裝置108 (或器具叢集109)之操作、稽核使用達一定時間之票證或票證使用率及其他資產消耗資訊之操作、及用以移除票證之操作。THID組件1400可提供多個應用程式設計介面(API)，以促進與器具裝置108中之其他組件之通信。

THID組件1400可接受多個同時請求。該等請求接著經序列化，此係因為HSM 111一次僅可服務一個請求。THID組件1400可為至器具裝置108中之HSM 111之唯一路徑。THID組件1400包含一票證快取記憶體1406，票證快取記憶體1406保持票證名稱至票證卷(ticket roll)(具有最小及最大票證值)之資產之一映射1410，以有效地反映HSM 111之一票證狀態。票證快取記憶體1406可用以對HSM 111卸載所有票證請求(例如，GetTickets()請求)並在THID組件1400中處置該等請求。由於該票證狀態在啟動時存留於HSM 111中，故THID組件

1400可要求對HSM 111上之票證之一稽核並運用稽核或計數結果初始化票證快取記憶體1406。例如，THID組件1400呼叫HSM 111上之AuditTickets()並運用結果初始化票證快取記憶體1406。票證快取記憶體1406可額外地追蹤一單獨夥伴映射1412中之「保留」票證，其可為由一模組常駐程式1414（例如，經由GetTickets()）請求但尚未發送回至THID組件1400用於一呼叫以調用一特定模組（例如，InvokeModule()）之票證。一模組常駐程式1414解析CM模組並準備相關資料及CM模組管理。

因此，THID組件1400可提供影響快取記憶體狀態之API，而不提供其他API。例如，一外部API 1402可將命令發佈至一服務佇列1408以新增票證、稽核票證或移除票證。例如，外部API 1402之AddTicket (tickets、importCounter、hsmId、及signature)命令傳回void。舉另一實例，AddTicket (challenge)命令傳回(hsmId、tickets、importCounter)，且RemoveTicket (tickets、importCounter、hsmId、signature)傳回void。外部API 1402可將各種命令發佈至模組常駐程式1414：GetTickets (ticketNames)傳回tickets；LoadModule (Module、signature、keys)傳回moduleHandle；UnloadModule (moduleHandle)傳回void（當前未供模組常駐程式1414使用）；且InvokeModule (moduleHandle、input、tickets)傳回sequence。在其他實施例中，THID組件1400可包含提供及啟動相關API。

上述大部分資訊直接通過HSM。HSM API 1404可將票證新增至THID、稽核票證、移除票證、載入模組、卸載模組、調用模組等。HSM API 1404可包含以下動作：AddTickets (tickets、importCounter、hsmId、signature)傳回void；AddTickets (hsmId、challenge)傳回(hsmId、tickets、importCounter)；RemoveTickets (tickets、importCounter、hsmId、signature)傳回void；LoadModule

(Module、signature、keys)傳回 moduleId；UnloadModule (moduleId)傳回 void；且 InvokeModule (moduleHandle、input、tickets)傳回 sequence。

例如，影響快取記憶體狀態之API可包含：用以獲得票證之一API，其可傳回待從該快取記憶體移除並放入至保留票證映射1412中之票證；用以新增待直接地轉遞至HSM 111之票證之一API，且在HSM 111完成該操作之後，THID組件1400可呼叫一API（例如，HSM 111上之AuditTickets()）以在HSM 111上稽核該等票證。票證快取記憶體1406可被清除並設定至經稽核狀態。此可允許「新增票證」資料對THID組件1400完全不透明。

接著，從票證快取記憶體1406移除當前保留之票證以保持兩個集拆散：3) AuditTickets() - 在來自服務佇列1408之每個顯式AuditTickets()請求之後，該票證快取記憶體如對Add/RemoveTickets()所做般使票證快取記憶體1406重新同步（主要保證來自模組常駐程式1414之漂移不出現當機/調用錯誤等）。服務佇列1408可用作至CM服務之CM器具裝置108之一閘道；4) InvokeModule() - 在成功調用一模組時，認為所涉及票證被花費且從保留票證映射1412移除。在失敗之情況下，若可依賴保留票證映射1412以推斷該等票證未被花費，則可未被清除。THID組件1400可丟棄已花費票證以防止一票證或預先計算資料之重新使用。一重新同步(如上文所描述)還原THID組件1400被謹慎地丟棄、被證明未被花費的任何票證。

THID組件1400可用作至HSM 111之一閘道，以用於來自測試器裝置112及服務裝置104之交易。接著，可從票證快取記憶體1406移除當前保留之票證以保持兩個集拆散。在作出稽核票證之一請求之後，票證快取記憶體1406可經重新同步以防止可由模組常駐程式1414當機/調用錯誤等所致之漂移等。可於供該CM系統使用之一追蹤系統中使

用一票證，以強制執行可在器具裝置108上運行之模組達數次，且追蹤由一模組使用之資產。票證確保資產不被複製或重複花費。該票證包含使得能夠強制執行CM核心參數之使用計數限制及唯一性/循序發佈的資料。票證可由根授權機構授權且由CM核心消耗。

在一項實施方案中，在一當機及重新啟動時，THID組件1400將不具有任何保留票證，因此模組常駐程式1414中之任何進展中模組(即，在GetTickets()與InvokeModule()之間)將無法滿足必須保留票證之HTID要求，因而InvokeModule()將失敗。若模組常駐程式1414當機並重新啟動，或簡言之，在至THID組件1400之票證請求或模組調用之間發生錯誤，則保留票證可不發送至THID組件1400，從而允許THID組件1400中之保留票證累積。在一些實施例中，保留票證可被加時間戳記且在重新同步時，若保留票證長於一定臨限秒數，則可移除該等保留票證。此用作用以使票證作廢以阻止THID組件1400中之保留票證累積之一機制。

在一些例項中，可被服務裝置104指派至一器具裝置之模組多於可置入於HSM 111之一記憶體中之模組。THID組件1400可載入及卸載模組以管理該HSM之記憶體，經由一「最不頻繁使用」原則撤出一或多個模組。例如，模組LRU可用於管理HSM之記憶體，經由一LRU原則進行撤出。此可特別有用於其中多個客戶共用一器具叢集之資產管理系統之一部署。

票證可為關於已花費哪些預先計算資料索引之唯一授權資訊，且由於THID組件1400可具備票證之知識，故THID組件1400可執行一預先計算資料清除程序，以回收已花費預先計算資料封裝之磁碟空間。

在正常操作期間，THID組件1400為至委派器具裝置之HSM之唯一介面。THID組件1400抽象化(abstract)票證管理程序，使對HSM 111

之存取同步，且管理HSM之記憶體及其他資源。

HSM 111 (及因此其介面點、THID組件1400)具有三個主功能：1) 發佈及花費資產管理票證；2) 運行HSM位元碼；及3) 稽核。使用 `hsmInvokeModule` 呼叫運行位元碼。然而，位元碼經簽署且可含有加密組件。運行中的位元碼可分割成兩次呼叫，使得HSM 111不驗證簽名並在每次 `hsmInvokeModule` 呼叫時解密任何加密組件。`loadHsmOps` 將位元碼載入至HSM中，驗證其簽名並解密(且可能排程)其可含有之任何加密金鑰。實際上藉由 `hsmInvokeModule` 呼叫執行該位元碼。

在一項實施例中，可在三個階段中完成加票證：1) 使用 `addTickets` 呼叫將票證從服務裝置載入至THID組件1400及HSM 111中；2) THID組件1400使用 `getTickets` 呼叫分配票證；及3) 由HSM位元碼在 `hsmInvokeModule` 呼叫中花費票證。

存在兩種類型之稽核，一種稽核用於位元碼且一種稽核用於加票證。位元碼調用可含有記載呼叫。此資料通過一運行中雜湊，且亦將由THID組件1400予以記錄。可命令HSM 111匯出並簽署此雜湊。HSM 111具有有限記憶體，因此其將僅儲存該運行中的雜湊。可命令HSM 111匯出並簽署其加票證相關狀態。若此狀態之一些被THID組件1400儲存於外部(例如，資產管理票證中之低記憶體HSM提議)，則THID組件1400透過HSM 111傳遞其使得HSM 111可簽署其。THID組件1400之主目的為對在器具裝置上運行之所有其他組件提供一統一介面，以存取資產管理HSM組件用於任何機密性或完整性計算。

可存在一些例外狀況。由於此為一RPC API，故用戶端程式碼可擲回之例外狀況落於三種類別中：1) 若RPC程式庫耗盡記憶體或遭遇一程式錯誤，則其可擲回 `std::logic_error`、`std::bad_alloc` 等。不建議用戶端處置此等例外狀況(但一 `finally` 子句或等效物除外)，此係因為例外狀況通常表示其中可能無復原選項之嚴重錯誤。2) 若RPC失敗(伺

伺服器處之錯誤版本、連接中斷、RPC程式庫中之邏輯錯誤)，則RPC程式庫可擲回一CriRpc::RpcException；3)若伺服器擲回一例外狀況，則RPC程式庫將中繼其作為一CriRpc::RpcException。在新增一定數目個票證時，該等票證傳遞為結構ticketStruct之一向量。

HSM可維持其已從服務裝置接收之授權之次數之一計數，該計數亦為下一次授權之所預期計數值。HSM可檢查此計數器值，檢查簽名，將票證新增至其庫存，且接著使其計數器值遞增。此防止授權被重新執行。

存在兩種類型之稽核，一種稽核用於位元碼且一種稽核用於加票證。位元碼調用可含有記載呼叫。此資料通過一運行中雜湊，且亦將由THID組件1400予以記錄。可命令HSM 111匯出並簽署此雜湊。HSM 111具有有限記憶體，因此其將僅儲存該運行中雜湊。可命令HSM 111匯出並簽署其加票證相關狀態。若此狀態之一些被THID組件1400儲存於外部(例如，資產管理票證中之低記憶體HSM提議)，則THID組件1400透過HSM 111傳遞其使得HSM 111可簽署其。

THID組件1400之主目的為對在器具裝置上運行之所有其他組件提供一統一介面，以存取資產管理HSM組件用於任何機密性或完整性計算。由於此為一RPC API，故用戶端程式碼可擲回之例外狀況落於三種類別中：若RPC程式庫耗盡記憶體或遭遇一程式錯誤，則其可擲回std::logic_error、std::bad_alloc等。不建議用戶端處置此等例外狀況(但一finally子句或等效物除外)，此係因為例外狀況通常表示其中可能無復原選項之嚴重錯誤。若RPC失敗(伺服器處之錯誤版本、連接中斷、及RPC程式庫中之邏輯錯誤)，則RPC程式庫可擲回一CriRpc::RelayedException；若伺服器擲回一例外狀況，則RPC程式庫將中繼其作為一CriRpc::RelayedException。下表繪示根據一項實施例之THID組件API。

函式	呼叫程式	階段	注釋
void addTickets(vector<ticketRoll> tickets, uint64 counter, byteArray hsmId, byteArray signature)	服務 佇列	初期 測試 版	
tuple<ticketAuditStruct, byteArray, ticketAuditStruct, byteArray> removeTickets(vector<ticketRoll> tickets, uint64 counter, byteArray hsmId, byteArray challenge, byteArray signature)	服務 佇列	生產	此呼叫係罕見的，且可係慢速的。初期測試版(pre-alpha)無需此呼叫。
vector<uint64> getTickets(uint64 ticketName, int n=1)	模組 常駐 程式	初期 測試 版	可傳回之票證少於n。
pair<ticketAuditStruct, byteArray signature> auditTickets(byteArray challenge)	服務 佇列	生產	此函式可能需要匯出額外資訊。
int loadHsmOps(byteArray module, byteArray signature, vector<byteArray> encryptedModuleKeys)	模組 常駐 程式	初期 測試 版	
byteArray hsmInvokeModule(int moduleHandle, byteArray inputBlock, vector<pair<uint64,uint64>> tickets)	模組 常駐 程式	初期 測試 版	必須由此模組預先載入 moduleHandle引數。
logRecord	記載	初期	

commitLog(byteArray log)	常駐 程式	測試 版	
pair<logAuditStruct, byteArray> auditLogs(byteArray challenge)	記載 常駐 程式	初期 測試 版	

addTicket呼叫之一項實例如下：

```
void addTickets(vector<ticketRoll> tickets,
               uint64 counter,
               byteArray hsmId,
               byteArray signature)
```

為了將一定數目個票證新增至系統，票證被傳遞為結構 ticketStruct 之一向量。HSM 111 維持其已接收來自服務裝置之之授權之次數之一計數，該計數亦為下一次授權之所預期計數值。HSM 111 將檢查此計數器值，檢查簽名，將票證新增至其庫存，且接著使其計數器值遞增。此防止授權被重新執行。下表包含參數及對應描述。

參數	描述
ticket	新增序列化票證。
counter	必須設定為等於HSM之服務匯入計數器之當前值。
hsmId	必須設定為等於HSM之16位元組唯一ID。
signature	使用服務之票證發佈金鑰之("addTickets" hsmId counter tickets)之一RSA-PSS簽名

結構 ticketRoll 可表示為如下：

位元 組位 移	欄位名稱	類型	大小 (位元 組)	描述
0	ticketName	uint64	8	票證名稱。
8	minTicketID	uint64	8	卷開始。
16	maxTicketID	uint64	8	卷結束。卷含有編號為從minTicketID至

				maxTicketID (包含minTicketID及maxTicketID)之票證。
24	mode	modeEnum	1	票證模式。應設定至存量。
25	reserved	uint8[7]	7	保留，必須設定至0。

列舉modeEnum可表示為如下：

名稱	ID	含義
stock	0	票證授權給此HSM。
issued	1	票證授權給一些其他HSM，且已傳送至此HSM。

此函式將給定票證卷載入至HSM中。

例外狀況	描述
SignatureException	簽名未經驗證。
HsmStateException	hsmId或計數器值係錯誤的。
InvalidParameterException	參數之一些其他態樣無效，例如hsmId或簽名大小錯誤。
InternalError	發生一些其他內部錯誤，例如HSM或THID耗盡記憶體。
RpcException	常見RPC例外狀況，例如I/O錯誤。

removeTicket可表達為如下：

```
tuple<ticketAuditStruct,
      byteArray,
      ticketAuditStruct,
      byteArray>
removeTickets(vector<ticketRoll> tickets,
              uint64 counter,
              byteArray hsmId,
              byteArray challenge,
              byteArray signature)
```

此函式移除從HSM輸入之票證中所列之所有票證。下表包含參數及對應描述。

參數	描述
tickets	待移除之序列化票證。
counter	必須設定為等於HSM之服務匯入計數器之當前值。
hsmId	必須設定為等於HSM之16位元組唯一ID。
signature	使用服務之票證發佈金鑰之一RSA-PSS簽名 ("removeTickets" hsmId counter tickets)

HSM首先執行一票證稽核，從而產生一ticketAuditStruct，且簽署("responseBeforeRemoveTickets"||challenge||ticketAuditStruct)。其接著移除給定票證，執行另一稽核，且簽署("responseAfterRemoveTickets"||challenge||ticketAuditStruct)。下表包含例外狀況及對應描述：

例外狀況	描述
SignatureException	簽名未經驗證。
HsmStateException	hsmId或計數器值錯誤。
InvalidParameterException	參數之一些其他態樣無效，例如hsmId或簽名大小錯誤。
InternalError	發生一些其他內部錯誤，例如HSM或THID耗盡記憶體。
RpcException	常見RPC例外狀況，例如I/O錯誤。

getTicket呼叫可表達為如下：

```
vector<uint64> getTickets(uint64 ticketName, int n=1)
```

下表包含參數及對應描述：

參數	描述
ticketName	待新增之票證名稱。
n	請求票證之數目。
傳回值	長度至多為n之一票證號碼陣列。

此函式傳回具有給定名稱之至少為1個且至多為n個票證之一向量。其嘗試傳回n個票證，但若可快速地獲得n個以下票證，則其將快速地傳回，而非等待全部n個票證。

對於其中器具裝置用作HSM之外部記憶體之案例，票證可具有與其等相關聯之密碼編譯資料。此資料由THID組件1400持有；其並

非藉由此呼叫傳回。

藉由此呼叫傳回之票證僅可由相同用戶端使用 `hsmInvokeModule` 來花費。連接至 THID 組件之另一程序無法使用此等票證。`getTicket` 呼叫僅保留該等票證。若呼叫程式 (caller) 在花費其等之前與 THID 組件斷開，則該 THID 組件可賦予相同票證給另一用戶端。下表包含例外狀況及對應描述：

例外狀況	描述
<code>InvalidParameterException</code>	n 通行票證之值為非正。
<code>NoTicketsException</code>	不存在具有該名稱之任何票證。
<code>InternalError</code>	發生一些其他內部錯誤，例如，HSM 或 THID 耗盡記憶體。
<code>RpcException</code>	常見 RPC 例外狀況，例如 I/O 錯誤。

`auditTickets` 呼叫可表達為如下：

```
pair<ticketAuditStruct,
      byteArray signature>
auditTickets(byteArray challenge)
```

下表包含參數及對應描述：

參數	描述
<code>challenge</code>	一選用之挑戰。長度必須恰好 0 或 16 個位元組。若長度為 16 個位元組，則該挑戰應為隨機。

回應為一 `ticketAuditStruct`：

位元組位移	欄位名稱	類型	大小(位元組)	描述
0	<code>hsmId</code>	<code>uint8[16]</code>	16	HSM 之唯一 ID
16	<code>counter</code>	<code>uint64</code>	8	HSM 之服務互動計數器。
24	<code>nrolls</code>	<code>uint32</code>	4	存在之票證卷數目。
28	<code>tickets</code>	<code>ticketRoll[nrolls]</code>	$32 * nrolls$	票證卷。

該結構中之票證不按任何特定次序傳回。若指定一挑戰，則 HSM 111 將在 ("`responseAuditTickets`" || `challenge` || `ticketAuditStruct`) 上

產生一簽名。否則，該簽名將為一空的byteArray。下表包含例外狀況及對應描述。

例外狀況	描述
InternalError	發生一些內部錯誤。
InvalidParameterException	該挑戰之長度並非恰好0或16個位元組。
RpcException	常見RPC例外狀況，例如I/O錯誤。

LoadHSMOps呼叫可表達為如下：

```
int loadHsmOps(byteArray module, byteArray signature,
vector<byteArray> encryptedModuleKeys)
```

下表包含參數及對應描述。

參數	描述
Module	由編譯器/根HSM輸出封裝模組資料。在CM HSM頁上描述此位元組陣列之格式。
signature	模組資料上之簽名，如在CM HSM頁上所描述。
encryptedModuleKey	模組金鑰之封裝值加密至叢集金鑰，準備自根HSM，如在CM HSM頁上所描述。
傳回值	一模組控制代碼ID。

此函式將給定模組載入至HSM中。存在於模組本身中之任何金鑰運用encryptedModuleKeys加密；該等金鑰單獨賦予給THID組件。該HSM可能不具有足夠記憶體來儲存於系統上的每個模組之ops。在此情況下，該THID組件負責管理該HSM之記憶體，根據載入需求載入及卸載程式碼。下表包含例外狀況及對應描述。

例外狀況	描述
SignatureException	模組之簽名未經驗證。
DecryptionException	encryptedModuleKes或模組金鑰區域(key zone)之解密失敗。
InvalidParameterException	參數之一些其他態樣失效，例如簽名大小錯誤。
InternalError	發生一些其他內部錯誤，例如HSM或THID耗盡記憶體，或模組未解析為ASN.1。

RpcException	常見RPC例外狀況，例如I/O錯誤。
--------------	--------------------

hsmInvokeModule呼叫可表達為如下：

byteArray

```
hsmInvokeModule(int moduleHandle,
                byteArray inputBlock,
                vector<pair<uint64,uint64>> tickets)
```

下表包含參數及對應描述。

參數	描述
moduleHandle	由loadHsmOps傳回之一模組控制代碼ID。
inputBlock	至模組之一封裝輸入區塊。
tickets	—(ticket name, ticket number)對陣列。
傳回值	HSM之輸出。

此函式呼叫已預先載入有loadHsmOps之一模組。必須賦予從此用戶端藉由一loadHsmOps呼叫傳回之一moduleHandle給此函式。同樣地，票證引數之第二元素必須為從一getTicket呼叫傳回至此用戶端之一票證號碼(第一元素為票證名稱)。一旦HSM程式碼已運行，則其結果傳回為一位元組陣列。下表包含例外狀況及對應描述。

例外狀況	描述
NoSuchModuleException	moduleHandle無效，即，其未藉由一loadHsmOps呼叫傳回至此用戶端。
DecryptionException	模組無法解密一預先計算資料片段。
InvalidParameterException	參數之一些其他態樣無效，例如存在錯誤票證號碼或輸入之大小錯誤。
InternalError	發生一些其他內部錯誤，例如HSM或THID耗盡記憶體，或模組之位元碼無效。
RpcException	常見RPC例外狀況，例如I/O錯誤。

commitLog呼叫可表達為如下：

logRecord

commitLog(byteArray log)

將一外部日誌訊息新增至HSM之日誌鏈。下表包含例外狀況及對應描述。

例外狀況	描述
InternalError	發生一些內部錯誤。
RpcException	常見RPC例外狀況，例如I/O錯誤。

auditLogs呼叫可表達為如下：

```
pair<logRecord, byteArray>
```

```
auditLogs(byteArray challenge)
```

auditLogs使用HSM稽核金鑰簽署當前日誌之一運行雜湊。一挑戰用於放置推遲及重新執行。其應為隨機。下表包含例外狀況及對應描述。

例外狀況	描述
InternalError	發生一些內部錯誤。
RpcException	常見RPC例外狀況，例如I/O錯誤。

THID組件1400維持HSM 111之狀態之一陰影複製，減去密碼編譯金鑰。此意謂著HSM程式碼可更簡單，且亦意謂著THID組件1400無需向HSM 111詢問任何資訊，但密碼編譯資訊除外。THID組件1400亦可維持在(根據CM加票證系統規格) HSM 111外之一些密碼編譯資訊，諸如一雜湊樹。當前未預期使用此資訊。若此資訊被使用，則其為叢集金鑰之MAC，但出於記憶體原因駐留於HSM 111外。

票證名稱用以將票證類型分群組在一起。票證名稱可為64個位元。位元組具有以下含義：

MSB	6	5	4	3	2	1	LSB
廠商ID				票證類型		唯一ID	

分配以下票證類型：

票證類型	描述
0	測試
1	開發
2	生產

總言之，一票證為用以一次運行一模組之一簽署授權。票證提供模組執行控制，允許重複防護並且對此執行提供一稽核證跡(稽核日誌)。在內部，一票證可為一對64位元字串、一票證名稱及一票證ID。票證名稱表示一票證類型。若一特定票證類型與PCD類型相關聯，則票證ID識別一特定PCD記錄。於模組檔案之「輸入」區段中擷取此關聯。在內部，HSM對於其已知之票證名稱之各者維持一CurrentTickets清單。HSM亦維持用以防止重新執行攻擊之一計數器(hsmTicketCounter)。亦可簽署該票證。即使各票證可不具有一個別簽名，但一票證卷(一票證集)可具有一簽名。此簽名之驗證可用於票證驗核。存在三種類型之票證相關訊息 - 稽核、授予及移除。票證稽核搜集HSM 111之內部狀態並將其傳送其至服務。票證授予提供新票證至HSM 111，而票證移除從HSM 111移除票證。下圖描述訊息類型之各者之內容。

由於在HSM 111與服務裝置104之間發生票證通信，故該訊息之各者之內容需經ASN.1編碼。ASN.1訊息之定義如下：

```

TicketAudit ::= SEQUENCE {
    hsmID IA5String,
    hsmTicketCounter IA5String,
    currentTickets CmTickets
}

CMTickets := SEQUENCE {

```

```

    currentTicket IA5String
}

```

在此，CMTickets定義為一SEQUENCE而非一SET以保持元素次序。若服務及器具HSM同意對票證進行排序並按次序處理票證清單，此可用於搜尋該清單。

以下定義票證授予訊息之ASN.1格式。

```

TicketGrant ::= SEQUENCE {
    hsmID IA5String,
    hsmTicketCounter IA5String,
    grantedTickets CmTicketRange
}

CmTicketRange ::= SEQUENCE {
    ticketName IA5String,
    ticketRangeStart IA5String,
    ticketRangeEnd IA5String
}

```

以下表示票證移除訊息：

```

TicketRemoval ::= SEQUENCE {
    hsmID IA5String,
    hsmTicketCounter IA5String,
    grantedTickets CmTicketRange
}

```

圖15為根據一項實施例之加票證於一模組以安全地提供一資料資產至一目標裝置之一方法1500之一流程圖。可由可包括硬體(例如，電路、專用邏輯、可程式化邏輯、微程式碼等)、軟體、韌體或其組合之處理邏輯執行方法1500。在一項實施方案中，圖1至3之器具

裝置108執行方法1500。在一項實施方案中，圖14之器具裝置108或THID組件1400執行方法1500。在其他實施方案中，本文中所描述之CM系統100之其他組件可執行方法1500之操作之一些或所有。

參考圖15，方法1500開始於透過一網路接收來自CM系統之一服務裝置之一模組(方塊1502)。該模組為在一目標裝置之一製造生命週期之一操作階段期間安全地提供一資料資產至該目標裝置之一應用程式。該處理邏輯判定是否透過一網路接收來自該服務裝置之一票證(方塊1504)。在接收該票證之後，該處理邏輯驗證該票證(方塊1506)。在驗證該票證時，該處理邏輯執行該模組以安全地提供該資料資產至該目標裝置(方塊1508)，且方法1500結束。在該票證未經驗證時，該處理處理發佈一無效票證之一警報(方塊1510)且方法1500結束或方法1500返回至方塊1504以判定是否接收另一票證。

在一進一步實施例中，該票證為一簽署票證授權，其允許執行該模組一次以防止該資料資產之複製及該資料資產之重複消耗。該處理邏輯防止在使用該簽署票證授權執行該模組之後該資料資產之複製及該資料資產之重複消耗。在一進一步實施例中，該處理邏輯使用該票證建立執行該模組之一稽核日誌。

在一項實施例中，該票證包含：一對N位字串；一票證名稱，其表示與一資料資產類型相關聯之一票證類型；及一票證識別符(ID)，其識別一特定資料資產記錄。在另一實施例中，該處理邏輯結合該模組及該票證透過該網路接收一PCD資產。一模組檔案之一輸入區段(含有該模組)使一PCD類型與一票證類型相關聯。該處理邏輯藉由比較該票證之一當前票證類型與該模組檔案之輸入區段中之票證類型來驗證該票證。在該票證類型與該當前票證類型匹配時，驗證該票證。

在一項實施例中，該器具裝置之一HSM對於該器具裝置已知之票證名稱之各者維持一當前票證清單且維持用以防止重新執行攻擊之

一計數器。在一進一步實施例中，該處理邏輯接收以下票證相關訊息之至少一者：來自該服務裝置之一第一票證相關訊息，其用以獲得該HSM之一內部狀態並將該內部狀態傳送至該服務裝置；一第二票證相關訊息，其用以授予一新票證給該HSM；或一第三票證相關訊息，其用以從該HSM移除該票證。

在另一實施例中，該處理邏輯藉由比對該資料資產之一循序索引來驗證一票證索引而驗證該票證，其中該資料資產為循序資料。在一進一步實施例中，該資料資產為在一循序PCD檔案中指定一PCD類型及一票證類型之一PCD資產。該處理邏輯藉由比較該票證之一當前票證類型與該PCD資產之票證類型及比較一當前PCD類型與該PCD資產之PCD類型，而驗證該票證。在該當前票證類型與該PCD資產之票證類型匹配且該當前PCD類型與該PCD資產之PCD類型匹配時，驗證該票證。

在一項實施例中，該資料資產為含有一HDCP金鑰之一HDCP記錄且該票證為由該服務裝置發佈用於該HDCP記錄之一密碼編譯金鑰。該處理邏輯在該票證經驗證時消耗該HDCP金鑰，以強制執行HDCP金鑰提供之單次使用且唯一本質。該處理邏輯追蹤由該服務裝置發佈之一票證歷史且偵測該票證歷史中之一複製。當在該票證歷史中偵測到該複製時，該處理邏輯產生一警報。

在另一實施例中，該資料資產為含有一加密HDCP金鑰及一金鑰選擇向量(KSV)值之一HDCP記錄。該處理邏輯追蹤該KSV值之一歷史且執行該歷史之一基於日誌之檢查以偵測一違規複製。該基於日誌之檢查基於以下至少一者：1)該器具裝置之日誌，其等參照該等發佈KSV值之一相同者；2)由器具裝置執行之序列之日誌，其等具有該等發佈KSV值之一相同者；3)由器具裝置消耗之票證之日誌；或4)一測試器裝置之日誌。在偵測到該複製時，該處理邏輯發佈一警報。在一

進一步實施例中，該HDCP記錄儲存於一PCD資產中且該PCD資產中之KSV值可供該器具裝置讀取，而無需具備供該器具裝置之HSM用於解密已加密HDCP金鑰之HDCP金鑰之知識。

下文描述指示一些使用案例。下文概述用作CM系統設計之一基礎之使用案例之一核心集。

個人化

個人化為提供一唯一裝置特有金鑰至CM核心。出於安全原因，其分解成兩個步驟，稱為perso1及perso2。本質上，在各步驟處，一金鑰分割將程式化至CM核心中且在內部重組以產生一裝置特有金鑰。

裝置序列化

裝置序列化提供一唯一序號至一CM核心。此序號隨機出現以隱藏關於生產良率之資訊；然而，此序號依據循序編號而變化。此允許於裝置序列化中使用之預先計算資料之加索引且確保一特定產品內之ID唯一性。

揮發性RMA再篩選啟用

在晶片裝運至現場中時，要求安全地停用在製造期間測試晶片所需之硬體支援測試特徵，亦稱為測試特徵設計(DFT)。亦必須在透過RMA通道返回壞部件以便故障分析之後安全地啟用此等特徵。CryptoManager™提供一種用以鑑認裝置並授權按每裝置之再篩選測試啟用/停用操作之提供之方法給客戶。

非揮發性RMA再篩選啟用

與上述相同，惟無法透過電源開啟重設保持永續性除外。

HDCP金鑰管理及提供

CM系統必須支援來自一發佈授權機構之HDCP金鑰之安全批量匯入及一唯一HDCP金鑰至一特定CM核心之安全提供。亦必須提供一

種用以將各HDCP金鑰繫結至一唯一識別符且貫穿其生命週期追蹤各HDCP金鑰之機制。

提供授權機構金鑰提供

CM系統必須能夠提供金鑰至客戶未知之CM核心。此等金鑰亦必須繫結至一唯一識別符且一對此等金鑰及其識別符應能夠促進此等金鑰之使用。

圖 16 為根據一項實施例之一電腦系統 1600 之一項實施例之一圖，包含一處理器 1602 及連接至一可抽取式儲存裝置 1605 之一可抽取式儲存裝置介面 1603。可抽取式儲存裝置介面 1603 經組態以連接至可抽取式儲存裝置 1605。處理器 1602 可操作以在一 CM 裝置之一製造生命週期之一裝置定義階段中執行指令 1626 (或軟體)。指令 1626 可包含儲存於主記憶體 1604 或可抽取式儲存裝置 1605 中且供處理器 1602 執行以執行關於如本文中所描述之模組、PCD 及票證之各種操作之指令。在一項實施例中，電腦系統 1600 表示根裝置 102。在另一實施例中，電腦系統 1600 表示服務裝置 104。在另一實施例中，電腦系統 1600 表示器具裝置 108。替代地，電腦系統 1600 可表示本文中所描述之其他裝置之任一者，諸如 CRISP 裝置 110。

在一些情況下，電腦系統 1600 可連接(例如，網路連線)至一 LAN、一內部網路、一外部網路或網際網路中之其他機器。電腦系統 1600 可為一雲端、一雲端提供者系統、一雲端控制器、一伺服器、一用戶端、或任何其他機器中之一主機。電腦系統 1600 可作為一用戶端伺服器網路環境中之一伺服器或一用戶端機器操作，或操作為一同級間(或分散式)網路環境中之一同級機器。該機器可為個人電腦(PC)、平板 PC、遊戲機裝置或視訊轉換器(STB)、個人數位助理(PDA)、蜂巢式電話、網路器具、伺服器、網路路由器、交換器或橋接器、或能夠執行指定由機器採取之動作之一指令集(循序的或以其他方式)之任

何機器。此外，雖然繪示僅單一機器，但術語「機器」不應被解釋為包含個別地或共同地執行一指令集(或多個指令集)以執行本文中所論述之方法論之任何一或多者之機器(例如，電腦)之任何集合。

電腦系統1600包含彼此經由一匯流排1630通信之一處理器1602(例如，主機處理器或處理裝置)、一主記憶體1604(例如，唯讀記憶體(ROM)、快閃記憶體、動態隨機存取記憶體(DRAM)、一儲存記憶體1606(例如，快閃記憶體、靜態隨機存取記憶體(SRAM)等)、及一輔助記憶體1618(例如，以一碟機單元之形式之一資料儲存裝置，其可包含固定或可抽取式電腦可讀儲存媒體)。

處理器1602表示一或多個通用處理裝置，諸如一微處理器、中央處理單元等。更特定言之，處理器1602可為一複雜指令集運算(CISC)微處理器、精簡指令集運算(RISC)微處理器、超長指令字(VLIW)微處理器、實施其他指令集之處理器、或實施一指令集組合之處理器。處理器1602亦可為一或多個專用處理裝置，諸如一特定應用積體電路(ASIC)、一場可程式化閘陣列(FPGA)、一數位信號處理器(DSP)、網路處理器等。

在一項實施例中，處理器1602可駐留於一第一積體電路上且主記憶體1604可駐留於一第二積體電路上。例如，該積體電路可包含一主機電腦(例如，具有一或多個處理核心、L1快取記憶體、L2快取記憶體等之CPU)、一主機控制器或其他類型之處理器1602。該第二積體電路可包含耦合至該主機裝置之一記憶體裝置，且其主要功能性取決於該主機裝置，且因此可被視為擴展該主機裝置之能力，而不形成該主機裝置之核心架構之部分。該記憶體裝置可能與該主機裝置通信。例如，該記憶體裝置可為一單IC或一多IC模組，其在一共同積體電路基板上包含單IC裝置之任何組合。圖16之組件可駐留於「一共同載體基板」上，舉例而言，諸如一積體電路(「IC」)晶粒基板、一多

IC模組基板等。替代地，該記憶體裝置可駐留於一或多個印刷電路板上，舉例而言，諸如一主機板、一子板或其他類型之電路卡。在其他實施方案中，該主記憶體及處理器1602可駐留於相同或不同載體基板上。

電腦系統1600可包含一晶片組1608，其指代經設計以與處理器1602合作且控制處理器1602與外部裝置之間的通信之積體電路或晶片之一群組。例如，晶片組1608可為一主機板上之一IC集，其將處理器1602連接至超高速裝置(諸如主記憶體1604及圖形控制器)並且將該處理裝置連接至周邊裝置1610之較低速周邊匯流排(諸如USB、PCI或ISA匯流排)。在一項實施例中，可抽取式儲存裝置介面1603可在晶片組1608中實施。

電腦系統1600可進一步包含一網路介面裝置1622。電腦系統1600亦可包含一或多個周邊裝置1610，諸如透過一圖形埠及圖形晶片組連接至該電腦系統之一視訊顯示單元(例如，一液晶顯示器(LCD))、一文數字輸入裝置(例如，一鍵盤)、一游標控制裝置(例如，一滑鼠)、一信號產生裝置(例如，一揚聲器)等。積體電路裝置「程式化」可包含例如且不限於：回應於一主機指令而將一控制值載入至該裝置內之一暫存器或其他儲存電路中且因此控制該裝置之一操作態樣；透過單次程式化操作建置一裝置組態或控制該裝置之一操作態樣(例如，在裝置生產期間熔斷一組態電路內之保險絲)；及/或將該裝置之一或多個選定接腳或其他接觸結構連接至參考電壓線(亦稱為搭接(strapping))以建置一特定裝置組態或該裝置之操作態樣。術語「例示性」用以表示一實例，但並不偏好或要求表示一實例。

域

如用於CM系統之域可用以反映目標裝置106劃分成更小集，諸如以對應於一客戶對不同產品、晶片系列、原始設備製造商(OEM)等之

觀點。於一CM系統中亦可使用域以判定PCD範本及模組範本之一適用性。為了詳細說明劃分目標裝置106，一CM核心集可屬於一特定晶片系列。如上文所描述，晶片系列指代共用CM核心內之相同安全性參數之一產品集(例如，共用一共同屬性集之一產品集，例如RsbSigningKey)。例如，該CM核心集可共用代表根簽署一序列(使用RsbSigningPriv)之一密鑰對以及用以提供此等核心之一其他基底金鑰集。共用該序列之相同金鑰對之CM核心集可被視為一模組域。可基於產品(亦稱為chipID)、ChipSeries等劃分一CM核心對。一特定產品僅可屬於一單一ChipSeries。一特定ChipSeries內之任何CM核心亦可屬於某個產品。

圖17為根據一項實施例之一域劃分1700之一圖。域劃分1700為一客戶1701之目標裝置106(例如，CM核心)之一劃分。域劃分1700包含基於一晶片系列1702(chipSeries1至3)之一第一層級分群組。晶片系列1702之劃分之各者包含基於產品1704之一第二層級分群組。各產品1704包含多個目標裝置106，在此實施方案中其各者包含一CM核心1706。在一些情況下，一第三層級分群組可基於一原始設備製造商(OEM)1706。例如，在一個晶片系列1702(chipSeries2)內，一個OEM可包含具有來自一第一產品類型(product1)之CM核心1706之多個目標裝置及具有來自一不同產品類型(product2)之CM核心1706之多個目標裝置。舉另一實例，在相同晶片系列1702(chipSeries2)內，另一OEM可包含具有相同產品類型(product2)中之CM核心1706之多個目標裝置。此外，如圖17中所繪示，基於OEM 1706之分群組可覆蓋橫跨三種產品類型(Product1至3)之兩個以上產品類型，諸如OEM 1706中所繪示。替代地，可基於CM核心1706之一集內之其他共同屬性來定義域。

域可用以統一基於一特定資料集之特定資產之建立。例如，一晶片系列1702 (chipSeries1)內之模組可基於相同根簽署私密金鑰(例如，RsbSigningPriv key)。替代地，可根據其他後設資料集來劃分CM核心1706。

此外，一域內之所有CM核心1706共用一後設資料集。為了指定CM核心1706中之若干資料值及金鑰，兩個資料封裝可用於CM系統，包含CM Netlist (接線對照表)及HW CONFIG (硬體組態)。Netlist為用以產生CM核心及其互連件之部件或裝置之描述。HW CONFIG值從根予以匯出以變為硬體Netlist之一部分，且HW CONFIG值可為客戶特有值。存在被CM系統(例如，根、模組)及CM核心硬體共用之若干值(金鑰及ID)。例如，RsbSigningPub供CM核心1706用以鑑認其透過測試器裝置112從設備HSM 111接收之序列。此一金鑰之另一實例為chipVendorDeviceAesKey。此金鑰用作一基底個人化金鑰。特定言之，此金鑰用以計算驗證程式(validator)，CM核心1706檢查此金鑰以鑑認器具108。除金鑰外，亦存在需為Netlist之一部分之常數。下表含有可經匯出以變為Netlist之一部分之例示性值。

名稱/ini名稱/硬體規格名稱	描述	長位 (以位元為單位)	產生者	匯出
CoreVersion / cmCoreVersion/ cmNetlistVersion	CRI設定之Netlist發行版本。在該序列存在一定版本相依性(例如，受支援命令之變更)時，序列使用此值來確認CM是否為適當版本。MSB = 主要，LSB = 次要。	16	CRISP	CRISP -> Root -> Netlist
Build /build/cmBuild	由CRI設定之Netlist版本號碼可基於來自修訂控制之資訊自動遞增。	8	CRISP	CRISP -> Root -> Netlist

hwConfigType	識別/使用約束標誌	1	CRISP	As a part of the Module Template
chipSeries	晶片系列。0x0000值不用於生產。	16	CRISP	CRISP -> Root -> Netlist
modelSelection	用以識別EA之類型之列舉	8	CRISP	CRISP -> Root -> Netlist
chipSeriesAesKey	基底AES金鑰	256	Root	Root -> Netlist
chipSeriesAesKeyChecksum	截斷雜湊	16	Root	Root -> Netlist
chipSeriesKeyUnwrapAesKey	安全p1/p2金鑰分割組合。不是一基底金鑰。	256	Root	Root -> Netlist
chipSeriesKeyUnwrapAesKeyChecksum	截斷雜湊	16	Root	Root -> Netlist
RsbSigningKeyLsb	用以驗證RSB之公開金鑰	2048-960	Root	Root -> netlist
publicKeyMsbs	根及委派公開金鑰之MSB	960	CRISP	CRISP -> Root

對於PCD或模組，基於一範本(PCD範本或模組範本)之一特定實體之建立可表達為如下：

Template + Domain => Entity

即，為了建立一模組，可選擇一模組範本且可指定一域。不同模組範本可具有不同域類型，但應指定一域。同樣地，PCD類型建立可使用一PCD範本及一域。下文描述提供PCD類型域及模組域之進一步實例。

模組域及PCD類型域

從實務觀點，模組域及PCD類型域之概念有助於描述如何基於一

特定模組範本或PCD範本建立多少不同模組或PCD類型。為了產生一模組，一模組範本繫結至一特定模組域。例如，一模組範本可描述如何提供序列化及個人化(稱為「serial+perso12」)。提供一特定chipSeries (稱為「cs12」)之序列化及個人化之一特定模組將稱為「serial+perso.cs12」且僅可結合屬於chipSeries cs12之CM核心1706使用。類似地，PCD範本「serial+perso12」可提供晶片ID「cid123」之裝置ID資料及個人化資料。基於提供資產至「cid123」之「serial+perso12」範本之PCD類型之全識別符將為「cid123」及「serial+perso12」兩者之組合且將稱為「serial+perso12.cid123」。下表包含具有PCD類型域及模組域之例示性使用案例。

使用案例	PCD域	模組域
srl_cvdak_padak	srl_cvdak: Product	Product
	padak: ChipSeries	
HDCP	全部	ChipSeries
*debug_unlock	不適用	ChipSeries

在上文描述中，陳述諸多細節。然而，獲益於本發明之一般技術人員將明白，可在無此等特定細節之情況下實施本發明之實施例。在一些例項中，以方塊圖形式而非詳細地展示熟知結構及裝置，以免使本發明描述不清楚。

關於對一電腦記憶體內之一資料位元之操作之演算法及符號表示提出詳細描述之一些部分。此等演算法描述及表示為熟悉資料處理技術之人員用以將其工作主旨最有效地傳達給其他熟悉此項技術者之手段。在此且通常，應預想一演算法為導致一所期望結果之步驟之一自相一致序列。該等步驟為需要實體量之實體操控之步驟。通常但非必要地，此等量採取能夠經儲存、經傳送、經組合、經比較及以其他方式經操控之電信號或磁信號之形式。其被證明有時主要出於共同使

用之原因便於指代此等信號為位元、值、元件、符號、字元、術語、數字等。

然而，應牢記，所有此等及類似術語與適當實體量相關聯且僅為應用於此等量之便利標記。如從上文論述可明白，除非別處另有具體所述，否則應明白，貫穿該描述，利用術語(諸如「加密」、「解密」、「儲存」、「提供」、「導出」、「獲得」、「接收」、「鑑認」、「刪除」、「執行」、「請求」、「傳達」等)之論述指代一運算系統或類似電子運算裝置之動作及程序，其操控表示為該運算系統內之暫存器及記憶體內之實體(例如，電子)量之資料並將該資料變換成類似地表示為運算系統記憶體或暫存器或其他此類資訊儲存裝置、傳輸或顯示裝置內之實體量之其他資料。

字詞「實例」或「例示性」在本文中用以意味著用作一實例、例項或闡釋。本文中描述為「實例」或「例示性」之任何態樣或設計未必被解釋為優於其他態樣或設計。相反，單詞「實例」或「例示性」之使用意欲於以一具體方式提出概念。如本發明中所使用，術語「或」意欲於意味著一包含性「或」而非一排除性「或」。即，除非另有指定或上下文清楚指出，否則「X包含A或B」意欲於意味著任何自然包含性置換。即，若X包含A；X包含B；或X包含A及B兩者，則在前述例項之任一者下滿足「X包含A或B」。此外，除非另有指定或上下文清楚指出旨在單數形式，否則如本發明及隨附申請專利範圍中所使用之冠詞「一」及「一個」通常應被解釋為意味著「一或多個」。此外，全文「一實施例」或「一項實施例」或「一實施方案」或「一項實施方案」之使用並非意欲於意味著相同實施例或實施方案，除非如此描述。

本文中所描述之實施例亦可關於一種用於執行本文中之操作之設備。此設備可經特殊建構用於所要目的，或其可包括一通用電腦，

其由儲存於該電腦中之一電腦程式選擇性地啟動或重新組態。此一電腦程式可儲存於一非暫時性電腦可讀儲存媒體中，諸如但不限於適於儲存電子指令之任何類型之磁碟，包含軟碟、光碟、CD-ROM及磁光碟、唯讀記憶體 (ROM)、隨機存取記憶體 (RAM)、EPROM、EEPROM、磁卡或光卡、快閃記憶體、或任何類型之媒體。術語「電腦可讀儲存媒體」應被解釋為包含儲存一或多個指令集之一單一媒體或多個媒體(例如，一集中或分散式資料庫及/或相關聯快取記憶體及伺服器)。術語「電腦可讀媒體」亦應被解釋為包含能夠儲存、編碼或實行一指令集以供機器執行且致使機器執行本發明實施例之方法論之任何一或多者之任何媒體。術語「電腦可讀儲存媒體」據此應被解釋為包含但不限於能夠儲存一指令集以供機器執行且致使機器執行本發明實施例之方法論之任何一或多者之固態記憶體、光媒體、磁媒體、任何媒體。

本文中所提出之演算法及顯示器並非內在地關於任何特定電腦或其他設備。各種通用系統可結合根據本文教示之程式使用，或其可被證明便於建構一更專業設備以便執行所要方法步驟。從下文描述將明白各種此等系統之所要結構。此外，本發明實施例並未參考任何特定程式化語言進行描述。將明白，各種程式化語言可用以實施如本文中所描述之實施例之教示。

上文描述陳述諸多特定細節(諸如特定系統、組件、方法等之實例)，以便良好地理解本發明之若干實施例。然而，熟習此項技術者將明白，可在無此等特定細節之情況下實行本發明之至少一些實施例。在其他例項中，未詳細地或以簡單方塊圖格式描述熟知組件或方法以免不必要地使本發明不清楚。因此，上文所陳述之特定細節僅為例示性。特定實施方案可隨此等例示性細節而變化且仍被預期在本發明之範疇內。

應瞭解，上文描述意欲為闡釋性而非限制性。熟習此項技術者在閱讀及瞭解上文描述時將明白諸多其他實施例。因此，應參考隨附申請專利範圍連同此等請求項具備之等效物之全部範疇判定本發明之範疇。

雖然本發明已參考其特定實施例進行描述，但顯然在不背離本發明之更廣精神及範疇之情況下可對其作出各種修改及變更。例如，在可行情況下，至少可結合任何其他實施例或取代其配對特徵或態樣應用任何實施例之特徵及態樣。據此，應在一闡釋性意義而非一限制性意義上考量本發明書及隨附圖式。

【符號說明】

100	密碼編譯管理器(CM)系統
102	根裝置
103	網路
104	服務裝置
105	企業網路
106	目標裝置
107	服務
108	委派器具裝置/安全器具裝置
109	器具叢集
110	提供裝置/Cryptography Research Inc.系統提供(CRISP)裝置
111	硬體安全性模組(HSM)
112	測試器裝置
114	用戶端庫
130	高產量製造場址/遠端製造場址/製造設施場址
140	資料中心

200	密碼編譯管理器(CM)系統傳訊
202	器具定義訊息
204	服務定義訊息
208	服務定義訊息
210	根定義訊息
212	服務啟動訊息
214	器具啟動訊息
216	器具啟動訊息
220	模組範本匯入訊息
222	模組匯入訊息
224	模組部署訊息
226	模組匯入訊息
228	模組部署訊息
230	預先計算資料(PCD)範本匯入訊息
232	預先計算資料(PCD)匯入訊息
234	預先計算資料(PCD)部署訊息
236	預先計算資料(PCD)匯入訊息
240	加票證訊息/票證授予訊息
300	模組生命週期
302	流程
303	TAR檔案庫
304	流程
305	預先計算資料(PCD)
306	流程
307	票證
308	流程

310	流程
311	預留位置
312	流程
313	模組序列
314	流程
315	測試指令碼
316	流程
318	流程
320	流程
322	流程
324	流程
326	流程
328	流程
330	流程
332	流程
400	方法
402	操作
404	操作
406	操作
408	操作
410	操作
500	方法
502	操作
504	操作
506	操作
508	操作

600	預先計算資料(PCD)部署授權
602	訊息
604	訊息
606	訊息
700	流程圖
702	循序預先計算資料(PCD)檔案
704	內標頭
706	外標頭
708至712	預先計算資料(PCD)記錄
714	外標頭
716	外標頭
718	預先計算資料(PCD)檔案
720	預先計算資料(PCD)檔案
722	預先計算資料(PCD)獨立記錄
724	獨立記錄標頭
800	流程圖
802	非循序預先計算資料(PCD)檔案
804	內標頭
806	外標頭
808至812	預先計算資料(PCD)記錄
820	非循序預先計算資料(PCD)檔案
822	非循序預先計算資料(PCD)檔案
824	獨立記錄標頭
826	預先計算資料(PCD)獨立記錄
840	排序
842	查找

844	外標頭
846	外標頭
902	記錄格式
904	預先計算資料(PCD)範本
906	預先計算資料(PCD)類型
908	模組範本
910	模組
912	票證類型
1000	預先計算資料(PCD)產生程序
1002	流程
1004	流程
1006	流程
1100	高頻寬數位內容保護(HDCP)匯入程式
1102	流程
1104	流程
1106	流程
1108	流程
1110	流程
1112	流程
1114	流程
1116	流程
1118	流程
1120	流程
1122	流程
1124	流程
1200	匯入程式

- 1202 傳入高頻寬數位內容保護(HDCP)資產
- 1204 PGP金鑰及複雜密碼
- 1206 流程
- 1208 金鑰選擇向量(KSV)資料庫
- 1210 流程
- 1212 流程
- 1214 流程
- 1216 UID計數器
- 1218 流程
- 1222 預先計算資料(PCD)檔案
- 1224 流程
- 1226 重複資料儲存區
- 1300 方法
- 1302 操作
- 1304 操作
- 1306 操作
- 1308 操作
- 1400 加票證及硬體安全性模組(HSM)互動常駐程式(THID)組件
- 1401 快速路徑操作
- 1402 加票證及硬體安全性模組(HSM)互動常駐程式(THID)外部應用程式設計介面(API)
- 1403 慢速路徑操作
- 1404 硬體安全性模組(HSM)應用程式設計介面(API)
- 1406 票證快取記憶體
- 1408 服務佇列
- 1410 映射

- 1412 單獨夥伴映射
- 1414 模組常駐程式
- 1500 方法
- 1502 操作
- 1504 操作
- 1506 操作
- 1508 操作
- 1510 操作
- 1600 電腦系統
- 1602 處理器
- 1603 可抽取式儲存裝置介面
- 1604 主記憶體
- 1605 可抽取式儲存裝置
- 1606 儲存記憶體
- 1608 晶片組
- 1610 周邊裝置
- 1622 網路介面裝置
- 1626 指令
- 1630 匯流排
- 1700 域劃分
- 1701 客戶
- 1702 晶片系列
- 1704 產品
- 1706 密碼編譯管理器(CM)核心

201606560

發明摘要

※ 申請案號：104112412

※ 申請日：104.9.17

 ※IPC 分類：

G06F 21/60	(2013.01)
G06F 21/12	(2013.01)
G06F 21/92	(2013.01)
H04W 12/06	(2009.01)

【發明名稱】

用以安全地提供資產至目標裝置之模組

 MODULES TO SECURELY PROVISION AN ASSET TO A
 TARGET DEVICE

【中文】

本文中所描述之實施例描述用於模組管理之技術，其包含在一密碼編譯管理器(CM)環境中於一目標裝置之一製造生命週期之一操作階段中的模組建立及至該目標裝置的模組部署。一項實施方案包含一根授權機構(RA)裝置，該RA裝置接收用以建立一模組之一命令；及回應於該命令，執行一模組範本以產生該模組。該模組經部署至一器具裝置。該模組之一指令集在由該器具裝置執行時導致一操作序列之一安全建構安全地提供一資料資產至該目標裝置。該器具裝置經組態以將該資料資產分發至該目標裝置之一密碼編譯管理器(CM)核心。

【英文】

The embodiments described herein describe technologies for Module management, including Module creation and Module deployment to a target device in an operation phase of a manufacturing lifecycle of the target device in a cryptographic manager (CM) environment. One implementation includes a Root Authority (RA) device that receives a command to create a Module and executes a Module Template to generate the Module in response to the command. The Module is deployed to an Appliance device. A set of instructions of the Module, when executed by the Appliance device, results in a secure construction of a sequence of operations to securely provision a data asset to the target device. The Appliance device is configured to distribute the data asset to a cryptographic manager (CM) core of the target device.

【代表圖】

【本案指定代表圖】：第(1)圖。

【本代表圖之符號簡單說明】：

- 100 密碼編譯管理器(CM)系統
- 102 根裝置
- 103 網路
- 104 服務裝置
- 105 企業網路
- 106 目標裝置
- 107 服務
- 108 委派器具裝置/安全器具裝置
- 109 器具叢集
- 110 提供裝置/Cryptography Research Inc.系統提供(CRISP)裝置
- 111 硬體安全性模組(HSM)
- 112 測試器裝置
- 114 用戶端庫
- 130 高產量製造場址/遠端製造場址/製造設施場址
- 140 資料中心

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

申請專利範圍

1. 一種方法，其包括：

由一根授權機構(RA)裝置接收用以建立一模組之一命令，其中該模組為在一目標裝置之一製造生命週期之一操作階段中安全地提供一資料資產至該目標裝置之一第一應用程式；

回應於該命令，由該RA裝置執行一模組範本以產生該模組，其中該模組範本為定義該模組及該資料資產之一指令集之一第二應用程式；及

將該模組部署至一器具裝置，其中該模組之該指令集在由該器具裝置執行時導致一操作序列之一安全建構安全地提供該資料資產至該目標裝置，其中該器具裝置經組態以將該資料資產分發至該目標裝置之一密碼編譯管理器核心。

2. 如請求項1之方法，進一步包括接收含有該資料資產之一預先計算資料(PCD)資產，且其中執行該模組範本包括運用該PCD資產來產生該模組。
3. 如請求項2之方法，進一步包括從一根資料庫擷取一金鑰，且其中執行該模組範本包括運用該PCD資產及該金鑰來產生該模組。
4. 如請求項2之方法，進一步包括接收來自一RA操作者之輸入，該輸入包括與一特定交易類型相關聯之引數，且其中執行該模組範本包括運用該PCD資產及該等引數來產生該模組。
5. 如請求項4之方法，其中執行該模組範本包括：運用該PCD資產、該等引數及待由該器具裝置提供之資料之一預留位置來產生該模組。
6. 如請求項1之方法，其中部署該模組包括：藉由該RA裝置將該模組儲存於一可抽取式儲存裝置中以將該模組傳送至一服務裝

置，其中該服務裝置經組態以透過一網路將該模組分發至該器具裝置。

7. 如請求項1之方法，進一步包括：

由該RA裝置產生一模組部署授權；及

由該RA裝置將該模組部署授權儲存至一可抽取式儲存裝置，以將該模組部署授權傳送至一服務裝置，其中該服務裝置經組態以透過一網路將該模組部署授權分發至該器具裝置。

8. 如請求項1之方法，進一步包括由該RA裝置運用一根模組私密金鑰來簽署該模組。

9. 一種方法，其包括：

由一器具裝置透過一網路接收來自一服務裝置之一模組；

由該器具裝置接收來自一測試器裝置之一密碼編譯管理器(CM)用戶端庫之一通信，其中該通信包括來自該CM用戶端庫之一引數；

回應於該通信，由該器具裝置基於該引數來調用該模組以產生一模組序列；及

藉由該器具裝置將該模組序列發送至該CM用戶端庫，其中在一目標裝置之一製造生命週期之一操作階段中，該測試器裝置之一測試器指令碼對該目標裝置之一CM核心遞送該模組序列。

10. 如請求項9之方法，進一步包括：

由該器具裝置上之一硬體安全性模組(HSM)組譯測試器資訊及一預先計算資料(PCD)資產；

由該HSM簽署一委派簽署區塊(DSB)；及

由該HSM運用該測試器資訊、該PCD資產及該DSB來建立該模組序列。

11. 如請求項10之方法，其中該測試器裝置經組態以將該模組序列

遞送至該目標裝置之該CM核心作為一測試指令碼之部分。

12. 一種根授權機構(RA)裝置，其包括：

一處理器；及

一可抽取式儲存裝置介面，其經組態以連接至一可抽取式儲存裝置，其中該可抽取式儲存裝置介面經耦合至該處理器，其中該處理器可操作以：

接收用以建立一模組之一命令，其中該模組為在一目標裝置之一製造生命週期之一操作階段中安全地提供一資料資產至該目標裝置之一第一應用程式；

回應於該命令，執行一模組範本以產生該模組，其中該模組範本為定義該模組及該資料資產之一指令集之一第二應用程式；及

將該模組部署至一器具裝置，其中該模組之該指令集在由該器具裝置執行時導致一操作序列之一安全建構安全地提供該資料資產至該目標裝置，其中該器具裝置經組態以將該資料資產分發至該目標裝置之一密碼編譯管理器核心。

13. 如請求項12之RA裝置，其中該處理器進一步可操作以使用預先計算資料(PCD)來建立該模組。

14. 如請求項12之RA裝置，其中該處理器進一步可操作以使用一預先計算資料(PCD)資產或與一特定交易類型相關聯之一引數之至少一者來建立該模組。

15. 如請求項12之RA裝置，其中該處理器進一步可操作以使用待由該器具裝置提供之資料之一預留位置來建立該模組。

16. 如請求項12之RA裝置，其中該處理器進一步可操作以經由該可抽取式儲存裝置介面將該模組儲存於該可抽取式儲存裝置中，以將該模組傳送至一服務裝置，其中該服務裝置經組態以透過

一網路將該模組分發至該器具裝置。

17. 如請求項12之RA裝置，其中該處理器進一步可操作以：

產生一模組部署授權；及

經由該可抽取式儲存裝置介面，將該模組部署授權儲存至一可抽取式儲存裝置，以將該模組部署授權傳送至一服務裝置，其中該服務裝置經組態以透過一網路將該模組分發至該器具裝置。

18. 一種器具裝置，其包括：

一處理器；

一網路介面，其經耦合至該處理器；及

一測試器裝置介面，其經耦合至該處理器，其中該處理器可操作以：

透過該網路接收來自一服務裝置之一模組；

透過該測試器裝置介面接收來自一測試器裝置之一密碼編譯管理器(CM)用戶端庫之一通信，其中該通信包括來自該CM用戶端庫之一引數；

回應於該通信，基於該引數來調用該模組以產生一模組序列；及

將該模組序列發送至該CM用戶端庫以供該測試器裝置運行，以在一目標裝置之一製造生命週期之一操作階段中將該模組序列遞送至該目標裝置之一CM核心。

19. 如請求項18之器具裝置，進一步包括一硬體安全性模組(HSM)，其中該HSM可操作以：

組譯測試器資訊及一預先計算資料(PCD)資產；

簽署一委派簽署區塊(DSB)；及

運用該測試器資訊、該PCD資產及該DSB來建立該模組序列。

20. 如請求項18之器具裝置，其中該測試器裝置經組態以將該模組序列遞送至該目標裝置之該CM核心作為一測試指令碼之部分。

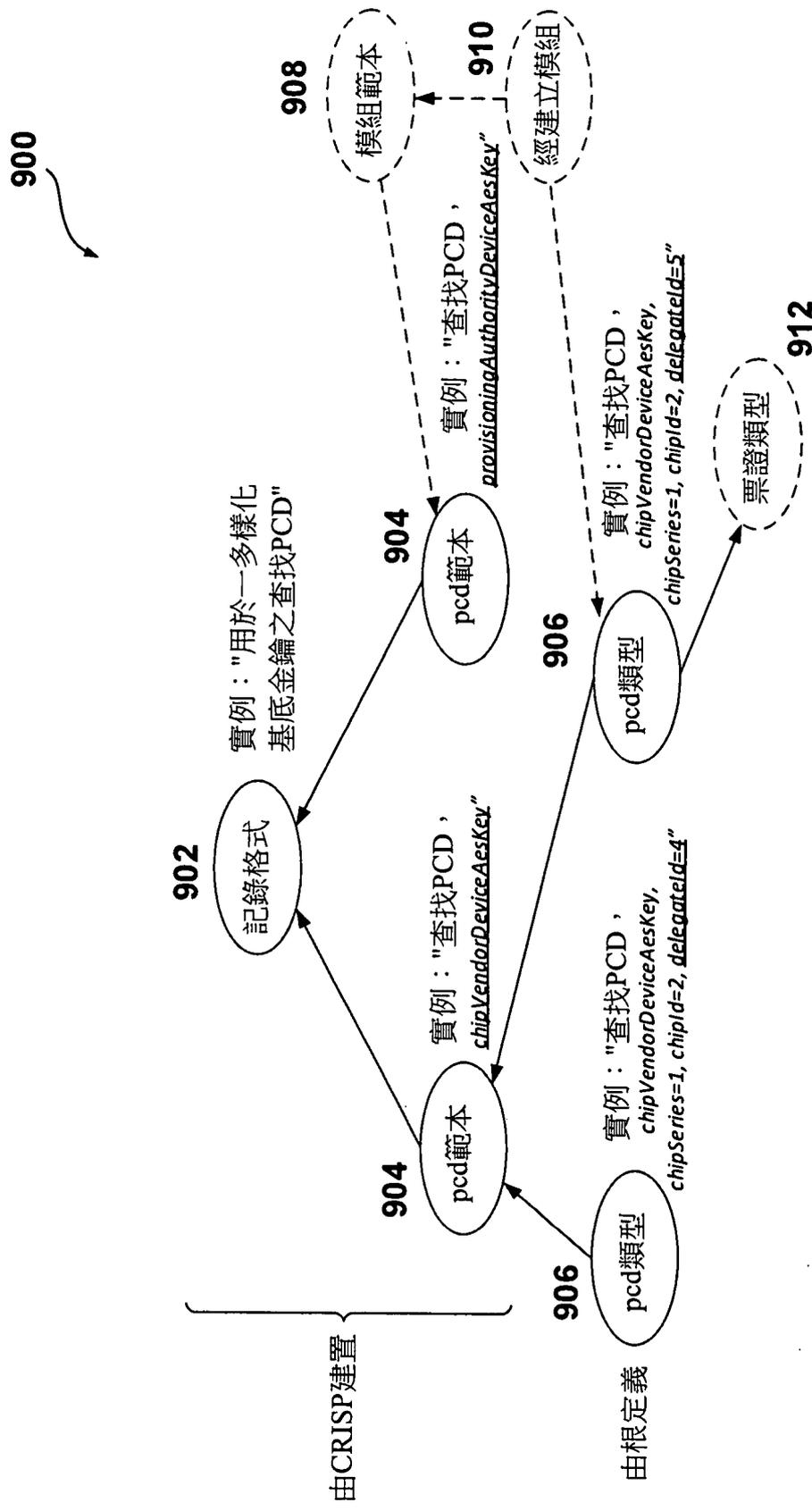


圖9

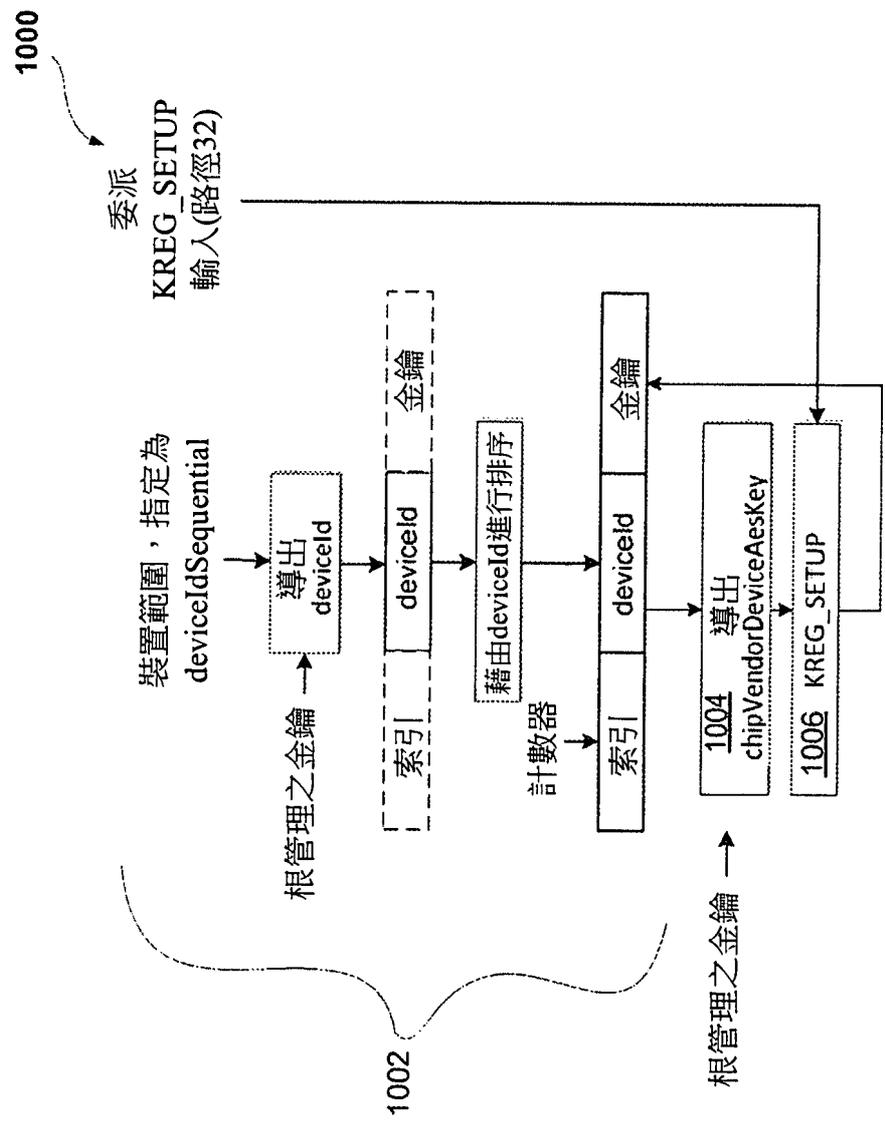


圖10

