



(21)申請案號：106102794

(22)申請日：中華民國 106 (2017) 年 01 月 25 日

(51)Int. Cl. : **G06Q20/22 (2012.01)**
G06Q20/38 (2012.01)

G06Q20/08 (2012.01)

(30)優先權：2016/02/01	美國	62/289,656
2016/02/21	美國	62/297,923
2016/06/12	美國	62/348,960
2016/06/12	美國	62/348,979
2016/09/23	美國	15/275,122

(71)申請人：蘋果公司 (美國) APPLE INC. (US)
 美國

(72)發明人：卡爾森 卡爾 安德列斯 CARLSSON, KARL ANDERS (US)；迪德里奇 安東
 K DIEDERICH, ANTON K. (US)；夏普 克里斯多弗 SHARP, CHRISTOPHER
 (US)；法索利 吉恩波羅 FASOLI, GIANPAOLO (US)；史達裘維克 瑪西耶
 STACHOWIAK, MACIEJ (US)；拜尹通 馬修 C BYINGTON, MATTHEW C.
 (US)；席爾 尼可拉斯 J SHEARER, NICHOLAS J. (GB)；維寧 山穆爾 M
 WEINIG, SAMUEL M. (US)

(74)代理人：陳長文

申請實體審查：有 申請專利範圍項數：21 項 圖式數：9 共 173 頁

(54)名稱

驗證對安全裝置功能性之線上存取

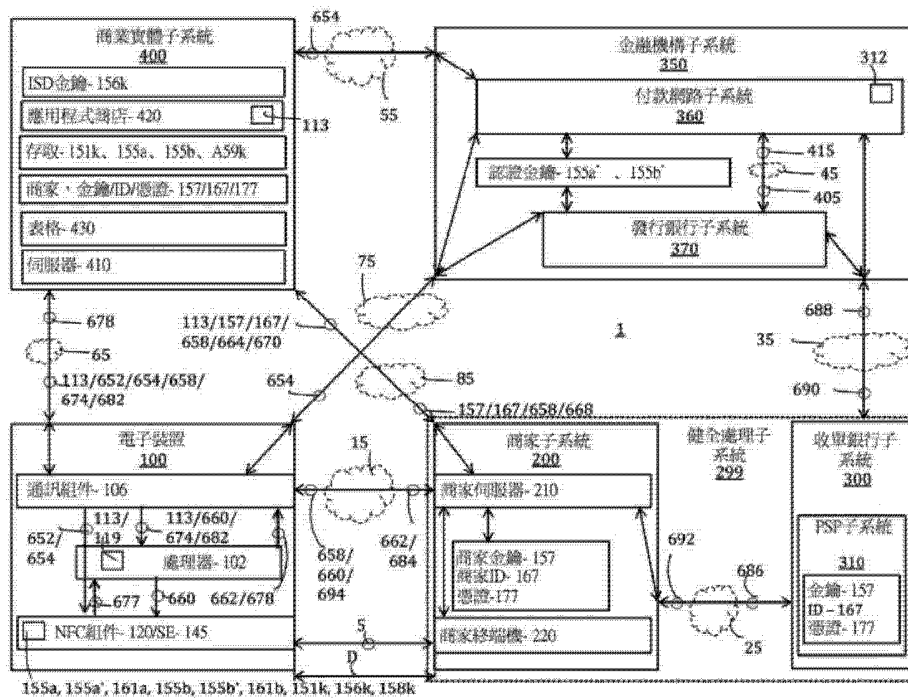
VALIDATING ONLINE ACCESS TO SECURE DEVICE FUNCTIONALITY

(57)摘要

提供用於驗證對安全裝置功能性之線上存取之系統、方法及電腦可讀取媒體，其可使用介於不同子系統之間的共用祕密與有限用途之驗證資料。

Systems, methods, and computer-readable media for validating online access to secure device functionality are provided that may use shared secrets between different subsystems and limited use validation data.

指定代表圖：



符號簡單說明：

1 . . . 系統

5 . . . 非接觸式之以
接近性為基礎之通
訊；通訊

25 . . . 通訊路徑；
路徑

35 . . . 通訊路徑；
路徑

45 . . . 通訊路徑；
路徑

55 . . . 通訊路徑；
路徑

65 . . . 通訊路徑；
路徑

75 . . . 通訊路徑；
路徑

85 . . . 通訊路徑；
路徑

100 · · · 電子裝置

102 . . . 處理器；處
理器組件

106 · · · 通訊組件

113 · · · 線上資源或
商家應用程式；第三
方商家應用程式；網
際網路應用程式；PSP
線上資源；網站商家
線上資源；商家資
源；商家線上資源應
用程式

119 · · · 裝置識別資
訊或裝置識別符

120 · · · 近場通訊 (NFC) 組件

145 · · · 安全元件

151k · · · CRS 存取
金鑰

155a . . . 存取金

鑰；金鑰；存取資訊

155a' . . . 認證金鑰
155b . . . 存取金
鑰；金鑰
155b' . . . 認證金鑰
156k . . . 發行方安
全性網域(ISD)金鑰
157 . . . 商家金鑰；
私密金鑰；商家私密
金鑰；公開及私密商
家金鑰
158k . . . CASD 存
取套件
161a . . . 認證資
訊；資訊
161b . . . 認證資
訊；資訊
167 . . . 唯一商家識
別符；商家識別符
(ID)；第一商家識別
符；第二商家識別符
177 . . . 憑證
200 . . . 商家(或處
理)子系統
210 . . . 商家伺服器
220 . . . 商家終端
機；商家付款終端機
299 . . . 健全處理子
系統
300 . . . 收單銀行
(或收單方)子系統；收
單銀行
310 . . . 第三方前端
PSP 子系統；PSP 子
系統；商家-合作夥伴
PSP 子系統
312 . . . 虛擬連結表
格
350 . . . 金融機構
(或交易或發行方)子系

統；使用者金融子系統

360 . . . 付款網路子系統；付款網路

370 . . . 發行銀行子系統；發行銀行

400 . . . 商業(或控管)實體子系統；商業實體

405 . . . 資料

410 . . . 伺服器

415 . . . 授權回應資料或交易狀態資料

420 . . . 商店組件；應用程式商店

430 . . . 表格

652 . . . 存取資料

654 . . . 認證資料

658 . . . 商家的資源；商家的線上資源

660 . . . 潛在交易資料；交易資料

662 . . . 商家線上資源驗證工作階段起始資料

664 . . . 查問請求資料

668 . . . 查問資料

670 . . . 查問回應資料

674 . . . 驗證回應資料

677 . . . 安全裝置資料

678 . . . 裝置交易資料

682 . . . 經保護安全之交易資料

684 . . . 以線上為基礎之通訊；經保護安全之交易資料

686 . . . 付款資料

688 . . . 授權請求資料

690 . . . 授權回應交易狀態資料

692 . . . 授權回應交易狀態資料

694 . . . 經確認之交易狀態資料

【發明說明書】

【中文發明名稱】 驗證對安全裝置功能性之線上存取

【英文發明名稱】 VALIDATING ONLINE ACCESS TO SECURE DEVICE
FUNCTIONALITY

【技術領域】

【0001】 相關申請案之交互參照

【0002】 本申請案主張於2016年2月1日申請之先前申請的美國專利臨時申請案第62/289,656號、於2016年2月21日申請之先前申請的美國專利臨時申請案第62/297,923號、於2016年6月12日申請之先前申請的美國專利臨時申請案第62/348,960號及於2016年6月12日申請之先前申請的美國專利臨時申請案第62/348,979號的優先權，該等案之各者之全文以引用方式併入本文中。

【0003】 本揭露係關於驗證對安全裝置功能性之線上存取，且更具體而言，係關於驗證一第三方子系統，用於實現由該第三方子系統線上存取一電子裝置之安全功能性。

【先前技術】

【0004】 攜帶型電子裝置（例如，蜂巢式電話(cellular telephone)）可具備近場通訊(「NFC」)組件，用於實現與另一實體（例如，一商家）進行非接觸式之以接近性為基礎之敏感性資料通訊，諸如需要電子裝置以與其他實體產生、存取及/或共用一原生付款認證（諸如一信用卡認證(credit card credential)）的資

料交易。然而，電子裝置在其他類型的通訊（例如，線上交易）中安全使用此一原生付款認證經常無效率。

【發明內容】

【0005】 此文件描述用於驗證對安全裝置功能性之線上存取之系統、方法及電腦可讀取媒體。

【0006】 舉一實例，可提供一種用於使用一商業實體子系統以進行經由一商家線上資源之介於一商家子系統與通訊地耦接至該商家子系統之一電子裝置之間的一安全交易之方法。該方法可包括：在該商業實體子系統處，自該商家子系統接收對於該商家線上資源的一驗證請求；使用該驗證請求及註冊資料來驗證該商家線上資源，在一開始於該接收之前已使該註冊資料可供該商業實體子系統使用；在該驗證之後，產生與該驗證請求之至少一部分相關聯的驗證資料；傳達該驗證資料至該電子裝置；接收來自該電子裝置之裝置交易資料；判定該裝置交易資料包含該驗證資料；及在該判定之後，基於該裝置交易資料來產生安全交易資料以供該商家子系統使用。

【0007】 舉另一實例，可提供一種用於使用一控管實體子系統以進行經由在一電子裝置上執行的一線上資源之介於一處理子系統與通訊地耦接至該處理子系統之該電子裝置之間的一安全交易之方法。該方法可包括：在該控管實體子系統處，接收對於該線上資源之一驗證請求，其中該驗證請求包括驗證請求資料；使用該驗證請求資料及註冊資料來驗證該線上資源，其中在一開始於接收該驗證請求之前已使該註冊資料可供該控管實體子系統使用；使驗證回應資料與該驗證請求資料之至少一部分相關聯；在已驗證該線上資源之後，傳達該

驗證回應資料至該電子裝置；在傳達該驗證回應資料至該電子裝置之後，接收來自該電子裝置之裝置交易資料；使用該驗證回應資料來驗證該裝置交易資料；及在已驗證該裝置交易資料之後，基於該裝置交易資料來產生安全交易資料以供該處理子系統使用。

【0008】 舉再另一實例，可提供一種用於使用一控管實體子系統以實現經由在一電子裝置上執行的一線上資源之介於一處理子系統與通訊地耦接至該處理子系統之該電子裝置之間的一安全交易之方法。該方法可包括：在該控管實體子系統處，註冊該線上資源，其中該註冊包括建置介於該控管實體子系統與該處理子系統之間的一處理共用祕密；接收對於該線上資源之一驗證請求，其中該驗證請求包括指示該線上資源之一處理識別符，且其中該驗證請求進一步包括經由該線上資源之介於該電子裝置與該處理子系統之間的一潛在交易所獨有的一驗證工作階段識別符；及使用該驗證工作階段識別符及該處理共用祕密來驗證由該處理識別符所指示之該線上資源。

【0009】 舉再另一實例，可提供一種用於使用一控管實體子系統以進行經由在一電子裝置上執行的一線上資源之介於一處理子系統與通訊地耦接至該處理子系統之該電子裝置之間的一安全交易之方法。該方法可包括：在該控管實體子系統處，接收對於該線上資源之一驗證請求，其中該驗證請求包括驗證請求資料，且其中該驗證請求資料包括潛在交易識別資訊，該潛在交易識別資訊指示經由該線上資源之介於該電子裝置與該處理子系統之間的一潛在交易；使用該驗證請求資料之至少一部分來驗證該線上資源；使驗證回應資料與至少該潛在交易識別資訊相關聯；在已驗證該線上資源之後，傳達該驗證回應資料至該電子裝置；在傳達該驗證回應資料至該電子裝置之後，接收來自該電子裝置

之裝置交易資料；使用該驗證回應資料及該潛在交易識別資訊來驗證該裝置交易資料；及在已驗證該裝置交易資料之後，基於該裝置交易資料來產生安全交易資料以供該處理子系統使用。

【0010】 本〔發明內容〕僅係供用於概括一些實例實施例，以提供對本文件所描述之標的物之一些態樣的基本瞭解。據此，應理解，本〔發明內容〕所描述之特徵僅係實例且不應理解為依任何方式限縮本文件所描述之標的物之精神與範疇。除非另有陳述，一個實例之內容脈絡中所描述之特徵可搭配一或多個其他實例之內容脈絡中所描述之特徵組合或使用。從下文的〔實施方式〕、〔附圖〕及〔申請專利範圍〕，本文件所描述之標的物之其他特徵、態樣及優點將顯而易見。

【圖式簡單說明】

【0011】 下文之論述參考下列圖式，圖中相似的元件符號可係指整個圖式中的相似部件，且其中：

〔圖1〕係用於驗證對安全裝置功能性之線上存取之一闡釋性系統的示意圖；

〔圖1A〕係圖1之系統的另一更詳細示意圖；

〔圖2〕係圖1及圖1A之系統之實例電子裝置的更詳細示意圖；

〔圖2A〕係圖1至圖2之實例電子裝置的另一更詳細示意圖；

〔圖3〕係圖1至圖2A之實例電子裝置的前視圖；

〔圖3A至圖3D〕係圖1至圖3之一或多者之實例電子裝置之圖形使用者介面之畫面的前視圖，繪示用於驗證對安全裝置功能性之線上存取之程序；

〔圖4〕係圖1及圖1A之系統之實例商業實體子系統的更詳細示意圖；以及

〔圖5至圖9〕係用於驗證對安全裝置功能性之線上存取之闡釋性程序的流程圖。

【實施方式】

【0012】 在使用一處理（或商家）子系統（含或不含一合作夥伴付款服務提供者（「PSP」）內嵌付款形式）之一線上資源（例如，一原生應用程式或網站）安全接收來自一使用者電子裝置之敏感性資料（例如，安全元件付款認證資料）之前，可藉由一受信任的控管（或商業）實體子系統來驗證處理子系統（含或不含PSP）。另外，除在該線上資源可操作以呈現與該處理子系統在一交易中共用敏感性資料的一選項給該使用者裝置之前驗證該線上資源外，亦可回應於選擇此一選項而實行一額外工作階段驗證程序，以重新授權該線上資源以供在實現該特定交易中使用。

【0013】 圖1及圖1A展示一系統1，其中可自一金融機構（或交易或發行方(issuer)）子系統350結合一商業（或控管）實體子系統400來佈建一或多個認證至一電子裝置100上，且其中可由電子裝置100使用此類認證來與一商家（或處理）子系統200及一相關聯之收單銀行（或收單方(acquirer)）子系統300（例如，電子裝置100之一安全裝置功能性）進行一交易（例如，一金融交易或任何其他合適的安全資料交易）；而圖2至圖3展示關於系統1之電子裝置100之特定實施例的進一步細節；圖3A至圖3D展示可代表在此一交易期間系統1之電子裝置100之圖形使用者界面的實例畫面190a至190d；圖4展示關於系統1之商業實體子系統400之特定實施例的進一步細節；及圖5至圖9係用於驗證對安全裝置功能性之線上存取之闡釋性程序（例如，進行此一金融交易）的流程圖。

圖1之說明

【0014】 圖1係一闡釋性系統1的示意圖，該系統可允許驗證一第三方子系統以用於實現由該第三方子系統線上存取一電子裝置之安全功能性，諸如驗證一商家（或處理）子系統，用於實現在與該商家子系統之一交易（例如，一線上付款或一非接觸式之以接近性為基礎之付款）中安全使用一電子裝置上的一認證。例如，如圖1中所展示，系統1可包括一電子裝置100以及一商業（或控管）實體子系統400及一金融機構（或交易或發行方）子系統350，用於安全地佈建一或多個認證於電子裝置100上。另外，如圖1中所展示，系統1亦可包括一商家（或處理）子系統200，藉此可由電子裝置100使用此一經佈建認證，用於與商家子系統200進行一交易（例如，一金融交易或任何其他合適的安全資料交易）。例如，回應於接收來自商家子系統200之潛在交易資料，電子裝置100可與商家子系統200共用該經佈建認證之安全裝置資料作為一非接觸式之以接近性為基礎之通訊5（例如，一近場通訊或一BlueTooth™通訊）及/或作為一以線上為基礎之通訊684（例如，一網路電信或以其他方式），用於提供與商家子系統200之該特定金融交易的資金。系統1亦可包括一收單銀行（或收單方）子系統300，其可利用此類非接觸式之以接近性為基礎之通訊5及/或此類以線上為基礎之通訊684，用於完成與金融機構子系統350之該交易。

【0015】 系統1可包括：一通訊路徑15，其用於實現介於電子裝置100與商家子系統200之間之通訊；一通訊路徑25，其用於實現介於商家子系統200與收單銀行子系統300之間之通訊；一通訊路徑35，其用於實現介於收單銀行子系統300與金融機構子系統350之間之通訊；一通訊路徑45，其用於實現介於金融機構子系統350之一付款網路子系統360與金融機構子系統350之一發行銀行子系

統370之間之通訊；一通訊路徑55，其用於實現介於金融機構子系統350與商業實體子系統400之間之通訊；一通訊路徑65，其用於實現介於商業實體子系統400與電子裝置100之間之通訊；一通訊路徑75，其用於實現介於金融機構子系統350與電子裝置100之間之通訊；及一通訊路徑85，其用於實現介於商業實體子系統400與商家子系統200之間之通訊。路徑15、25、35、45、55、65、75及85之一或多者可至少部分地由一或多個受信任服務管理員(「TSM」)管理。可操作以建立一通訊網路的任何合適電路系統、裝置、系統，或其等之組合(例如一有線及/或無線通訊基礎結構，其可包括一或多個通訊塔、電信伺服器、或類似者)可用來提供路徑15、25、35、45、55、65、75及85之一或多者，其可能夠使用任何合適的有線或無線通訊協定來提供通訊。例如，路徑15、25、35、45、55、65、75及85之一或多者可支援Wi-Fi(例如，802.11協定)、ZigBee(例如，802.15.4協定)、WiDi™、乙太網路、Bluetooth™、BLE、高頻系統(例如，900 MHz、2.4 GHz、及5.6 GHz通訊系統)、紅外線、TCP/IP、SCTP、DHCP、HTTP、BitTorrent™、FTP、RTP、RTSP、RTCP、RAOP、RDTP、UDP、SSH、WDS橋接、可由無線及蜂巢式電話與個人電子郵件裝置使用的任何通訊協定(例如，GSM、GSM plus EDGE、CDMA、OFDMA、HSPA、多頻帶等)、可由低功率無線個人區域網路(「6LoWPAN」)模組使用的任何通訊協定、任何其他通訊協定、或其任何組合。

圖1A之說明

【0016】 現在參考圖1A，圖1A展示上文關於圖1所描述之系統1的更詳細視圖。如圖1A中所展示，例如，電子裝置100可包括一處理器102、一通訊組件

106、及/或一近場通訊(「NFC」)組件120。NFC組件120可包括或以其他方式提供一安全元件145，該安全元件可經組態以提供一防篡改平台（例如，作為單一晶片或多晶片安全微控制器），其可能夠根據可由一組經妥善識別之受信任授權單位(authority)（例如，一金融機構子系統之一授權單位及/或一產業標準，諸如GlobalPlatform）所提出的規則及安全性要求來安全地寄存(hosting)應用程式及其等之機密及密碼編譯資料（例如，認證小程式(credential applet)及相關聯之認證金鑰，諸如一認證金鑰155a'、及一存取金鑰155a、及/或一發行方安全性網域(「ISD」)金鑰156k，如圖1A中所展示）。如下文更詳細描述，在裝置100之（例如，NFC組件120之）安全元件145上之一認證小程式或一付款應用程式可經組態以提供付款認證資料作為含用於識別一資金帳戶或其他金融工具(financial instrument)或信用來源（例如，在金融機構子系統350處）之充分細節的交易資料，其中在與商家子系統200及/或商業實體子系統400之一或多個通訊中，可由裝置100使用此類付款認證資料來用於促進一金融交易。NFC組件120可經組態以傳達此類主機付款認證資料作為與商家子系統200（例如，與商家子系統200之一商家終端機220，其可定位在一實體商店(brick and mortar store)或任何實體地點(physical location)，在該處，裝置100之使用者可使用儲存在裝置100上之一認證以經由一非接觸式之以接近性為基礎之通訊來與一接近定位之商家終端機220進行一金融交易）的一非接觸式之以接近性為基礎之通訊5（例如，近場通訊）。替代地或此外，可提供通訊組件106以允許裝置100使用任何合適的有線或無線協定（例如，經由通訊路徑15、65、及/或75之一或多者）來與一或多個其他電子裝置或伺服器或子系統（例如，系統1之一或多個子系統或其他組件，諸如經由任何合適的線上通訊來與商家子系統200之商家伺服器210）通訊任何

合適的付款認證資料（例如，作為一以線上為基礎之通訊684）。裝置100之處理器102可包括可操作以控制裝置100之一或多個組件之操作及效能的任何處理電路系統。例如，處理器102可經組態以在裝置100上執行一或多個應用程式（例如，一應用程式103及/或一線上資源或商家應用程式113），其可至少部分規定其中資料（例如，交易資料之付款認證資料）可由裝置100傳達以用於為與商家子系統200之一金融交易提供資金的方式。另外，如圖1A中所展示，裝置100可包括裝置100之處理器102或任何其他合適部分可存取的任何合適的裝置識別資訊或裝置識別符119。可由商業實體子系統400及/或商家子系統200及/或金融機構子系統350利用裝置識別資訊119來唯一地識別裝置100，以促進與商家子系統200的一交易及/或實現與裝置100的任何合適之安全通訊。僅舉一實例，裝置識別資訊119可係一電話號碼或電子郵件地址或可與裝置100相關聯的任何唯一識別符。

【0017】 商家子系統200可包括任何合適的商家伺服器210，如圖1A中所展示，其可包括任何合適組件或子系統，該組件或子系統可經組態以經由任何合適的通訊協定（例如，Wi-Fi、Bluetooth™、蜂巢式電話通訊(cellular)、有線網路協定等）來與下列者通訊任何合適資料：商業實體子系統400之一通訊組件（例如，經由通訊路徑85）；及/或收單銀行300之一通訊組件（例如，經由通訊路徑25）；及/或裝置100之一通訊組件（例如，經由通訊路徑15）。例如，商家伺服器210可操作以在任何合適的線上內容脈絡內與裝置100之通訊組件106進行潛在交易資料660通訊，諸如當裝置100之使用者經由可在裝置100上執行的任何合適商家線上資源113與商家伺服器210通訊以進行一交易時，商家線上資源113係諸如在裝置100上執行之一第三方商家應用程式113，其可由商家伺服器210管理

(例如，一原生應用程式)，或商家線上資源113係在裝置100上執行之一網際網路應用程式113(例如，Apple Inc.提供的Safari™)，其可指向可由商家伺服器210管理其目標或Web資源的一統一資源定位器(「URL」)(例如，一商家網站、使用導向至一商家網站之一Web檢視之一商家應用程式(例如，同捆(bundled)在一商家應用程式內的一網際網路瀏覽器，從而產生可稱為一混合式應用程式(hybrid app)者，其可實現使用Web技術(例如，HTML、JavaScript、CSS等)來建置此一應用程式，但仍可實現將此一應用程式封裝為一原生應用程式)、及/或使用導向至一商家網站之一Web檢視的一非商家應用程式)。據此，應注意，介於商家伺服器210與裝置100之間之通訊可無線地發生及/或經由有線路徑(例如，透過網際網路)發生。可由商家子系統200之一商家提供商家伺服器210(例如，作為代管網站資料及/或管理第三方應用程式資料之一Web伺服器)。此外或替代地，如圖1A中所展示，商家子系統200可包括任何合適的商家終端機220(例如，一商家付款終端機)，其可包括可經組態以與裝置100之一非接觸式之以接近性為基礎之通訊組件(例如，裝置100之NFC組件120的一非接觸式之以接近性為基礎之通訊5)通訊任何合適資料的任何合適組件或子系統。另外，如圖1A中所展示，商家子系統200可包括一商家金鑰157及/或一商家識別符(「ID」)167。雖然未展示，商家子系統200亦可包括：一商家處理器組件，其可相同於或相似於圖1A及圖2之電子裝置100之一處理器組件102；一商家通訊組件，其可相同於或相似於圖1A及圖2之電子裝置100之一通訊組件106(例如，作為伺服器210之一部分)；一商家I/O介面，其可相同於或相似於圖2之電子裝置100之一I/O介面114；一商家匯流排，其可相同於或相似於圖2之電子裝置100之一匯流排118；一商家記憶體組件，其可相同於或相似於圖2之電子裝置100之一

記憶體組件104，及/或一商家電源供應器組件，其可相同於或相似於圖2之電子裝置100之一電源供應器組件108。

【0018】 金融機構子系統350可包括一付款網路子系統360（例如，一付款卡聯盟或一信用卡聯盟）及/或一發行銀行子系統370。例如，發行銀行子系統370可係一金融機構，其可為一消費者清償憑藉一特定認證而引致之債務的能力承擔主要責任。裝置100之NFC組件120之各特定認證小程序可與一特定付款卡相關聯，該特定付款卡可依電子方式連結至一特定使用者之一或多個帳戶。各種類型付款卡可係合適的，包括信用卡、轉帳卡(debit card)、簽帳卡(charge card)、儲值卡、汽油特惠卡(fleet card)、禮品卡及類似物。可由發行銀行子系統370將一特定付款卡之商務認證佈建在裝置100上（例如，作為NFC組件120之一認證補充安全性網域之一認證，如下文所描述），以供在與商家子系統200（例如，直接或經由商業實體子系統400）的一商務認證資料通訊（例如，一非接觸式之以接近性為基礎之通訊及/或一以線上為基礎之通訊）中使用。各認證可係由一付款網路子系統360定品牌的一特定品牌付款卡。付款網路子系統360可係可處理一特定品牌付款卡之使用（例如，商務認證）的各種發行銀行370及/或各種收單銀行300之一網路。

【0019】 為使金融交易發生於系統1內，至少一商務認證必須安全地佈建在電子裝置100之一安全元件上。例如，此一商務認證可直接自金融機構子系統350至少部分佈建在裝置100之安全元件145上（例如，作為認證資料654，其係經由介於金融機構子系統350與裝置100之間之通訊路徑75，可經由通訊組件106將其傳遞至安全元件145）。此外或替代地，此一商務認證可經由商業實體子系統400自金融機構子系統350至少部分佈建在裝置100之安全元件145上（例如，

作為認證資料654，其係經由介於金融機構子系統350與商業實體子系統400之間之通訊路徑55，其可經由介於商業實體子系統400之一伺服器410與裝置100之通訊組件106之間之通訊路徑65作為認證資料654傳遞至裝置100，接著可自通訊組件106將其傳遞至安全元件145）。認證資料654經由路徑75及/或經由路徑55/65可經佈建在裝置100之安全元件145上，作為該安全元件之一認證補充安全性網域之至少一部分或全部，且可包括含認證資訊及/或一認證金鑰之一認證小程序，諸如含認證資訊161a及認證金鑰155a'之認證小程序153a或付款應用程式。如圖1A中所展示，例如，金融機構子系統350亦可存取認證金鑰155a'（例如，用於解密由裝置100使用認證金鑰155a'所加密之資料）。金融機構子系統350可負責管理認證金鑰155a'，其可包括產生、交換、儲存、使用及替換此一金鑰。金融機構子系統350可儲存其認證金鑰155a'之版本於金融機構子系統350之一安全元件中。應理解，裝置100及金融機構子系統350之認證金鑰155a'可係電子裝置100之安全元件及金融機構子系統350兩者皆可使用的任何合適之共用祕密（例如，一密碼(password)、密碼短語(passphrase)、隨機選取之位元組陣列、一或多個對稱式金鑰、公開-私密金鑰（例如，非對稱式金鑰）等），電子裝置100之安全元件及金融機構子系統350兩者可操作以實現由電子裝置100及金融機構子系統350獨立地產生任何合適的密碼編譯資料（例如，一編譯密碼(cryptogram)）或任何其他合適的資料（例如，用於驗證用於一金融交易之付款資料），諸如藉由使用任何合適的密碼編譯演算法或加密法(cipher)，可至少部分地藉由該共用祕密判定密碼編譯演算法或加密法之功能輸出，其中可由金融機構子系統350將此一共用祕密佈建在裝置100上。金融機構子系統350與裝置100之間可事前共用一共用祕密（例如，在由金融機構子系統350在裝置100上佈建一認證期間），

在此情況中，此一共用祕密可稱為一預先共用金鑰，或可藉由使用一金鑰協議協定(key agreement protocol)（例如：使用公開金鑰密碼編譯法(public-key cryptography)，諸如Diffie-Hellman；或使用對稱式金鑰密碼編譯法(ymmetric-key cryptography)，諸如Kerberos）在一共用祕密用於一特定金融交易之前建立該共用祕密。裝置100之安全元件可存取該共用祕密及可至少部分藉由該共用祕密判定其之功能輸出的任何合適之密碼編譯演算法或加密法。

【0020】 商業實體子系統400可經提供作為介於金融機構子系統350與裝置100之間之一中介(intermediary)，其中商業實體子系統400可經組態以當一認證經佈建在裝置100之一安全元件上時及/或當此一經佈建認證用作為介於裝置100與商家子系統200之間之一商務認證資料通訊之部分時，提供一新安全性層及/或提供一更順暢使用者體驗。可由一特定商業實體提供商業實體子系統400，該特定商業實體可經由彼商業實體之使用者特定帳戶的使用者特定登入資訊（例如，經由使用者特定之識別及密碼組合）來提供各種服務給裝置100之使用者。僅舉一實例，可由Apple Inc. (Cupertino, CA)提供商業實體子系統400，其亦可係提供各種服務給裝置100之使用者的一提供者（例如，用於銷售/租借待由裝置100播放之媒體的iTunes™商店、用於銷售/租借供在裝置100上使用之應用程式的Apple App Store™、用於儲存來自裝置100之資料及/或使多個使用者裝置及/或多個使用者設定檔彼此相關聯的Apple iCloud™服務、用於線上購買各種Apple產品之Apple線上商店、用於在裝置之間傳達媒體訊息的Apple iMessage™服務等），且其亦可係裝置100本身及/或裝置100之一作業系統（例如，裝置應用程式103）之提供者、製造商及/或開發商（例如，當裝置100係iPod™、iPad™、Phone™或類似物時）。可提供商業實體子系統400的商業實體（例如，Apple Inc.）可相異於

且獨立於金融機構子系統350之任何金融實體。例如，可提供商業實體子系統400的商業實體可相異於及/或獨立於可供給及/或管理待佈建於終端使用者裝置100上之任何信用卡或任何其他商務認證的任何付款網路子系統360或發行銀行子系統370。此外或替代地，可提供商業實體子系統400的商業實體（例如，Apple Inc.）可相異於且獨立於商家子系統200之任何商家。例如，可提供商業實體子系統400的商業實體可相異於及/或獨立於可提供用於非接觸式之以接近性為基礎之通訊的一商家終端機、用於線上通訊的一第三方應用程式或線上資源113、及/或商家子系統200之任何其他態樣的商家子系統200之任何商家。此一商業實體可充分利用其組態或控制裝置100之各種組件（例如，裝置100之軟體及/或硬體組件，諸如當彼商業實體可至少部分生產或管理裝置100時）的潛在能力，以在裝置100之使用者想要在裝置100上佈建由金融機構子系統350提供之認證時及/或在此一經佈建之認證正用作與商家子系統200的商務認證資料通訊之部分以提供一金融交易之資金時，為裝置100之使用者提供更順暢之使用者體驗。例如，在一些實施例中，裝置100可經組態以對裝置100之使用者而言順暢且透通的方式來與商業實體子系統400通訊（例如，經由通訊路徑65），以用於共用或接收可實現較高安全性等級之某些資料（例如，在介於裝置100與商家子系統200之間之一以線上為基礎之安全資料通訊期間）。雖然未展示，商業實體子系統400亦可包括：一處理器組件，其可相同於或相似於圖1A及圖2之電子裝置100之處理器組件102；一通訊組件，其可相同於或相似於圖1A及圖2之電子裝置100之通訊組件106；一I/O介面，其可相同於或相似於圖2之電子裝置100之I/O介面114；一匯流排，其可相同於或相似於圖2之電子裝置100之匯流排118；一記憶體組件，其可相同於或相似於圖2之電子裝置100之記憶體組件104，及/或一電源

供應器組件，其可相同於或相似於圖2之電子裝置100之電源供應器組件108，可至少部分地由伺服器410提供其等之一者、一些或全部。

【0021】 除至少一商務認證經佈建在裝置100之一安全元件上（例如，作為含認證金鑰155a'及認證資訊161a之一認證SSD之一部分）外，含一存取金鑰155b之至少一存取SSD亦可佈建在裝置100之安全元件上，以使裝置100能以更安全的方式與商家子系統200進行一金融交易。例如，可直接自商業實體子系統400將一存取SSD至少部分地佈建在裝置100之一安全元件上（例如，作為存取資料652，經由介於商業實體子系統400之伺服器410與裝置100之通訊組件106之間之通訊路徑65，接著可自通訊組件106傳遞存取資料652至安全元件145）。存取資料652經由路徑65可經佈建在裝置100之一安全元件上作為一存取SSD之至少一部分或全部，且可包括含一存取金鑰155b之一存取小程序153b。如圖1A中所展示，商業實體子系統400亦可存取存取金鑰155b（例如，用於使用存取金鑰155b來解密由裝置100所加密之資料）。商業實體子系統400可負責管理存取金鑰155b，其可包括產生、交換、儲存、使用及替換此一金鑰。商業實體子系統400可儲存其存取金鑰155b之版本於商業實體子系統400之一安全元件中。含存取金鑰155b之裝置100之一存取SSD可經組態以判定裝置100之使用者之意圖及本端鑑認（例如，經由裝置100之一或多個輸入組件110，諸如一生物特徵輸入組件），且回應於此一判定，可經組態以啟用另一特定SSD，用於進行一付款交易（例如，運用裝置100之一認證SSD之一認證）。藉由儲存此一存取SSD於裝置100之一安全元件內，可增加可靠地判定使用者對一金融交易之意圖及鑑認的能力。另外，可充分利用裝置100之此一存取SSD之存取金鑰155b以為可傳達至裝置100之安全元件之外的交易資料提供增強的加密。此外或替代地，如下文所描述，存取

資料652可包括用於電子裝置100之安全元件之一ISD的一發行方安全性網域(「ISD」)金鑰156k，其亦可由商業實體子系統400維護，且可除使用存取金鑰155b外亦使用ISD金鑰156k，或使用ISD金鑰156k作為存取金鑰155b之一替代，如下文所描述。

【0022】 可由裝置100存取一商家應用程式或線上資源113，以實現裝置100與商家子系統200之間之待促成的一線上金融交易，或實現由商家子系統200線上存取裝置100之任何其他合適的安全裝置功能性。首先，在可由裝置100有效利用應用程式113前，可由商業實體子系統400核准或註冊或以其他方式啟用一應用程式113。例如，商業實體子系統400之一應用程式商店420（例如，Apple App Store™）可經由通訊路徑85接收來自商家子系統200的代表應用程式113之至少一些資料。另外，在一些實施例中，商業實體子系統400可產生或以其他方式指派用於應用程式113之一商家金鑰157，且可提供此一商家金鑰157至商家子系統200（例如，經由路徑85）。替代地，商家子系統200可產生或以其他方式指派用於應用程式113之一商家金鑰157，且可提供此一商家金鑰157至商業實體子系統400（例如，經由路徑85）。商家子系統200或商業實體子系統400可負責管理商家金鑰157，其可包括產生、交換、儲存、使用及替換此一金鑰。無論此一商家金鑰157可如何產生及管理或在何處產生及管理，商家子系統200及商業實體子系統400兩者可儲存商家金鑰157之一版本（例如，於商家子系統200及商業實體子系統400之各別安全元件中，其中，在一些實施例中，由商家子系統200所儲存之商家金鑰157可係一私密金鑰，且由商業實體子系統400所儲存之商家金鑰157可係一相對應之公開金鑰（例如，用以在非對稱式金鑰加密/解密程序中使用））。在一些實施例中，此一商家金鑰157可具體地與商家應用程式113相

關聯，而在其他實施例中，商家金鑰157可具體地與商家子系統200之一商家相關聯，使得商家金鑰157可與由商家子系統200之同一商家操作的多個第三方應用程式或Web資源相關聯。可由商業實體子系統400及/或由商家子系統200產生一唯一商家識別符167及/或以其他方式指派該唯一商家識別符給應用程式113或使該唯一商家識別符與應用程式113相關聯。例如，一商家識別符167可係一文數字串、一網域（例如，用於一Web資源類型線上資源應用程式113之一URL或其他）、或可唯一識別一商家及/或一特定商家線上資源的任何其他合適識別符（例如，如此對商業實體子系統400唯一地識別）。可提供一表格430或可供商業實體子系統400存取的任何其他合適資料結構或資訊來源，用於使一特定商家金鑰157與一商家應用程式113之一特定商家識別符167或商家實體相關聯。可使一商家線上資源與一特定商家識別符167及一特定商家金鑰157相關聯，可於商家子系統200與商業實體子系統400之間安全地共用特定商家識別符167及特定商家金鑰157之各者。表格430可使商業實體子系統400能夠判定及利用一適當的商家金鑰157，用於提供一安全性層給經傳達至商家子系統200的任何安全裝置資料（例如商務認證資料，其可包括裝置100原生之付款認證資料），以用於可涉及裝置100經由與金鑰157及商家識別符167相關聯之商家應用程式113而與商家子系統200介接的一交易。裝置100可經組態以存取應用程式113（例如，經由通訊路徑65自應用程式商店420存取應用程式）並執行應用程式113（例如，以處理器102執行應用程式）。替代地或此外，一商家金鑰157及商家識別符167可與一商家網站（例如，一或多個URL或網域，其在本文中可稱為一商家線上資源，或在一些實施例中，稱為商家應用程式）相關聯，或大致上與商家相關聯，而非與一商家之第三方原生應用程式相關聯或亦與一商家之第三方原生應用程

式相關聯。例如，商家子系統200之一商家可與商業實體子系統400合作以在表格430內使一特定商家網站或商家大致上與一特定商家金鑰157及商家識別符167相關聯，其可使商業實體子系統400能夠判定及利用一適當的商家金鑰157，以用於針對一交易提供一安全性層給經傳達至商家子系統200的任何安全裝置資料（例如，可包括裝置100原生之付款認證資料的商務認證資料），其可涉及裝置100與商家伺服器210介接以經由在裝置100上執行之一網際網路應用程式或Web瀏覽器進行一交易，網際網路應用程式或Web瀏覽器可指向一URL或網域，該URL或網域之目標或Web資源可與彼商家金鑰157及商家識別符167相關聯（例如，彼Web資源之唯一網域（例如，store.merchant.com））。裝置100可經組態以例如經由通訊路徑15自商家伺服器210存取此一URL（例如，使用裝置100上之一網際網路應用程式113，當目標係此一商家Web資源時，其可視為一商家線上資源）。在其他實施例中，一應用程式113可未與一特定商家、商家子系統200、商家金鑰157及/或商家識別符167相關聯，反而可係裝置100運用定目標至此一商家Web資源的一Web檢視而可取得的一獨立應用程式，從而作為一商家線上資源。可依任何合適方式來實行藉由商業實體子系統400之商家線上資源之此一註冊（例如，安全且經驗證地共用商家金鑰157及商家識別符167於商家子系統200與商業實體子系統400之間（例如，以供儲存在表格430中）），以使商業實體子系統400確保商家子系統200係線上資源之一有效擁有者。如所提及，一商家線上資源（例如，原生應用程式、網域/URL、或任何其他合適的Web資源，或甚至可能是一商家終端機）可與一特定商家識別符167及一特定商家金鑰157相關聯（例如，在圖5之步驟501及/或在圖6之步驟606的註冊期間），可依任何合適方式於商家子系統200與商業實體子系統400之間安全地共用特定商家識別

符167及特定商家金鑰157之各者，並且此一關聯性可供商業實體子系統400存取（例如，在表格430中）。

圖2之說明

【0023】 現在參考圖2，圖2展示上文關於圖1及圖1A所描述之系統1的電子裝置100之更詳細視圖。如圖2中所展示，電子裝置100可例如包括一處理器102、記憶體104、通訊組件106、電源供應器108、輸入組件110、輸出組件112、天線116、及近場通訊(「NFC」)組件120。電子裝置100亦可包括一匯流排118，該匯流排可提供一或多個有線或無線通訊鏈路或路徑以用於傳送資料及/或電力至裝置100之各種其他組件、自該各種其他組件傳送資料及/或電力、或在該各種其他組件之間傳送資料及/或電力。電子裝置100亦可具備一外殼101，該外殼可至少部分地圍封裝置100的組件中之一或多者以用於保護免受裝置100外部之碎屑及其他降級力影響。在一些實施例中，可組合或省略電子裝置100之一或多個組件。另外，電子裝置100可包括圖2中未組合或未包括之其他組件。例如，電子裝置100可包括任何其他合適的組件或圖2中展示的組件之若干例項。為簡單起見，圖2中展示該等組件中之各者之僅一者。可提供一或多個輸入組件110以准許使用者與裝置100互動或介接，及/或可提供一或多個輸出組件112以呈現資訊（例如，圖像、聽覺及/或觸覺資訊）給裝置100之使用者。應注意，一或多個輸入組件及一或多個輸出組件有時候在本文中可統稱為一輸入/輸出(「I/O」)組件或I/O介面114（例如，輸入組件110及輸出組件112統稱為I/O組件或I/O介面114）。例如，輸入組件110及輸出組件112有時候可係一單一I/O組件114（諸如一觸控螢幕），其可透過使用者對顯示螢幕之觸摸來接收輸入資訊且亦可經由

彼同一顯示螢幕提供視覺資訊給使用者。電子裝置100之處理器102可包括可操作以控制電子裝置100之一或多個組件之操作及效能的任何處理電路系統。例如，處理器102可接收來自輸入組件110之輸入信號及/或透過輸出組件112驅動輸出信號。如圖2中所展示，處理器102可用以執行一或多個應用程式，諸如一應用程式103及/或一應用程式113。舉一實例，應用程式103可係一作業系統應用程式，而應用程式113可係一第三方應用程式或任何其他合適的線上資源（例如，與商家子系統200之商家相關聯的一應用程式）。另外，如所展示，處理器102可存取裝置識別資訊119，可由裝置100之使用者及/或商業實體子系統400利用裝置識別資訊119以用於提供裝置100之識別。

【0024】 NFC組件120可係任何合適的以接近性為基礎之通訊機構，該以接近性為基礎之通訊機構可實現介於電子裝置100與商家子系統200之一商家終端機（例如，商家付款終端機220）之間的非接觸式之以接近性為基礎之交易或通訊。NFC組件120可包括用於實現介於電子裝置100與此一商家終端機之間的非接觸式之以接近性為基礎之通訊的任何合適模組。如圖2中所展示，NFC組件120可例如包括一NFC裝置模組130、一NFC控制器模組140、及/或一NFC記憶體模組150。NFC裝置模組130可包括一NFC資料模組132、一NFC天線134、及一NFC加強器136。NFC資料模組132可經組態以含有、路由、或以其他方式提供任何合適的資料，該資料可由NFC組件120傳輸至商家終端機作為一非接觸式之以接近性為基礎之通訊之部分或NFC通訊之部分。此外或替代地，NFC資料模組132可經組態以含有、路由或以其他方式接收任何合適的資料，該資料可由NFC組件120自商家終端機予以接收而作為一非接觸式之以接近性為基礎之通訊之部分。NFC控制器模組140可包括至少一NFC處理器模組142。NFC處理器模組142

可結合NFC裝置模組130操作以啟用、啟動、允許及/或以其他方式控制NFC組件120，以用於傳達介於電子裝置100與一商家終端機之間之一NFC通訊。NFC控制器模組140可包括至少一NFC處理器模組142，NFC處理器模組142可用以執行一或多個應用程式，諸如可幫助規定NFC組件120之功能的一NFC低功率模式或錢包應用程式143。NFC記憶體模組150可結合NFC裝置模組130及/或NFC控制器模組140操作以允許介於電子裝置100與商家子系統200之間之NFC通訊。NFC記憶體模組150可防篡改且可提供一安全元件145之至少一部分（例如，參見圖2A）。例如，此一安全元件可經組態以提供一防篡改平台（例如，作為單一晶片或多晶片安全微控制器），其可能夠根據可由一組經妥善識別之受信任授權單位（例如，一金融機構子系統之一授權單位及/或一產業標準，諸如GlobalPlatform）所提出的規則及安全性要求來安全地寄存應用程式及其等之機密及密碼編譯資料（例如，小程序153及金鑰155）。

【0025】 如圖2中所展示，NFC記憶體模組150可例如包括一發行方安全性網域（「ISD」）152及一補充安全性網域（「SSD」）154之一或多者（例如，一服務提供者安全性網域（「SPSD」）、一受信任服務管理員安全性網域（「TMSD」）等），該等安全性網域可由NFC規格標準（例如，GlobalPlatform）定義及管理。例如，ISD 152可係NFC記憶體模組150之一部分，其中一受信任服務管理員（「TSM」）或發行金融機構（例如，金融機構子系統350）可儲存金鑰及/或其他合適的資訊以用於在電子裝置100上（例如，經由通訊組件106）建立或以其他方式佈建一或多個認證（例如，與各種信用卡、銀行卡、禮品卡、通行卡（access card）、交通票證（transit pass）等相關聯的認證），以用於認證內容管理，及/或安全性網域管理。一認證可包括可指派給一使用者/消費者且可安全地儲存於電子

裝置100上的認證資料（例如，認證資訊161a），諸如一信用卡付款號碼（例如，一裝置主要帳戶號碼（「DPAN」）、DPAN到期日期、CVV等（例如，作為一符記(token)或其他））。NFC記憶體模組150可包括至少兩個SSD 154（例如，至少一第一SSD 154a及一第二SSD 154b）。例如，第一SSD 154a（例如，一認證SSD 154a）可與可提供特定特殊權限或付款權給電子裝置100的一特定認證（例如，由金融機構子系統350佈建的一特定信用卡認證或一特定公共交通卡(public transit card)認證）相關聯，而第二SSD 154b（例如，一存取SSD 154b）可與可控制裝置100對另一SSD之一特定認證（例如，第一SSD 154a）之存取的一商業實體（例如，商業實體子系統400之一商業實體，其可係針對裝置100之一控制實體）相關聯，以例如提供特定特殊權限或付款權給電子裝置100。替代地，第一SSD 154a及第二SSD 154b之各者可與可提供特定特殊權限或付款權給電子裝置100的一各別特定認證（例如，由金融機構子系統350佈建的一特定信用卡認證或一特定公共交通卡認證）相關聯。各SSD 154可包括至少一小程式153及/或與至少一小程式153相關聯（例如，SSD 154a與小程式153a相關聯及SSD 154b與小程式153b相關聯）。例如，一SSD 154之一小程式153可係可在NFC組件120之一安全元件上執行的一應用程式（例如，在GlobalPlatform環境中）。一認證小程式153可包括認證資訊161或與認證資訊161相關聯（例如，小程式153a之資訊161a及/或小程式153b之資訊161b）。各SSD 154及/或小程式153亦可包括自己的金鑰155之至少一者及/或與自己的金鑰155之至少一者相關聯（例如，小程式153a與至少一金鑰155a相關聯及小程式153b與至少一金鑰155b相關聯）。

【0026】 一SSD 154之一金鑰155可係可判定一密碼編譯演算法或加密法之一功能輸出的一筆資訊。例如，在加密中，一金鑰可指定明文(plaintext)到密

文(ciphertext)之具體變換，或在解密期間反過來指定由密文到明文之具體變換。金鑰亦可用於其他密碼編譯演算法中，諸如數位簽章方案及訊息鑑認碼。一SSD之一金鑰可提供與另一實體的任何合適共用祕密。各金鑰及小程式可由一TSM或一經授權代理程式(agent)載入於裝置100之安全元件上，或當首次提供於裝置100上時預先載入於安全元件上。舉一實例，雖然認證SSD 154a可與一特定信用卡認證相關聯，但彼特定認證可僅當彼認證SSD 154a之小程式153a已經啟用或以其他方式啟動或解鎖以用於金融交易時作為商務認證資料通訊而自裝置100之安全元件（例如，自NFC組件120）傳達至商家子系統200以用於此類用途。

【0027】 可提供安全性特徵以使得能夠使用NFC組件120，其在將機密付款資訊（諸如，認證之信用卡資訊或銀行帳戶資訊）自電子裝置100傳輸至商家子系統200時可係特別實用的。此類安全性特徵亦可包括可具有受限制之存取的一安全儲存區域。例如，可能需要提供經由個人識別號碼（「PIN」）輸入項或經由使用者與生物特徵感測器之互動的使用者鑑認，以存取安全儲存區域。舉一實例，一存取SSD 154b可充分利用小程式153b以判定在允許其他SSD 154（例如，認證SSD 154a）被用於傳達其認證資訊161a之前是否已發生此類鑑認。在某些實施例中，安全性特徵之一些或全部可儲存在NFC記憶體模組150內。進一步，用於與商家子系統200通訊商務認證資料的安全性資訊（諸如一鑑認金鑰）可儲存在NFC記憶體模組150內。在某些實施例中，NFC記憶體模組150可包括內嵌在電子裝置100內之一微控制器。僅舉一實例，存取SSD 154b之小程式153b可經組態以判定裝置100之使用者之意圖及本端鑑認（例如，經由一或多個輸入組件110，諸如一生物特徵輸入組件），且回應於此一判定，可經組態以啟用另一特定SSD，用於進行一付款交易（例如，運用一認證SSD 154a之一認證）。

圖2A之說明

【0028】 現在參考圖2A，圖2A展示上文關於圖1至圖2所描述之系統1之電子裝置100之一部分的另一詳細視圖。如圖2A中所展示，例如，裝置100之一安全元件145可包括：SSD 154a，其可包括小程序153a、認證資訊161a、存取金鑰155a及/或認證金鑰155a'，或與小程序153a、認證資訊161a、存取金鑰155a及/或認證金鑰155a'相關聯；及SSD 154b，其可包括小程序153b、認證資訊161b、存取金鑰155b及/或認證金鑰155b'或與小程序153b、認證資訊161b、存取金鑰155b及/或認證金鑰155b'相關聯。在一些實施例中，一特定補充安全性網域（「SSD」）154（例如，SSD 154a及154b之一者）可與可提供特定特殊權限或付款權給電子裝置100的一特定TSM及至少一特定商務認證（例如，一特定信用卡認證或一特定公共交通卡認證）相關聯。各SSD 154可具有自己的管理員金鑰155（例如，金鑰155ak及155bk之一各別者），可能需要啟動管理員金鑰155以啟用彼SSD 154之功能以供NFC裝置模組130使用。此外或替代地，各SSD 154可包括與一特定商務認證相關聯的自己的認證應用程式或認證小程序（例如，一Java卡(Java card)小程序例項）之至少一者，及/或與該至少一者相關聯（例如，SSD 154a之認證小程序153a可與第一商務認證相關聯及/或SSD 154b之認證小程序153b可與第二商務認證相關聯），其中一認證小程序可具有自己的存取金鑰（例如，用於認證小程序153a之存取金鑰155a、及/或用於認證小程序153b之存取金鑰155b）、及/或自己的認證金鑰（例如，用於認證小程序153a之認證金鑰155a'及/或用於認證小程序153b之認證金鑰155b'），且其中可能需要啟動認證小程序以啟用其相關聯之商務認證以供NFC裝置模組130使用作為一NFC通訊（例如，

與商家終端機220之NFC通訊)及/或作為一基於線上之介於電子裝置100與商家子系統200之間之通訊(例如,經由商業實體子系統400)。在一些實施例中,一認證小程序之一認證金鑰(例如,用於認證小程序153a之認證金鑰155a',及/或用於認證小程序153b之認證金鑰155b')可由可負責此一認證之金融機構子系統350產生,且可由彼金融機構子系統350存取(例如,如圖1A中所展示),以用於實現於安全元件145與金融機構子系統350之間安全傳輸彼小程序之彼認證資訊(例如,經由商家子系統200)。此外或替代地,一認證小程序之一存取金鑰(例如,用於認證小程序153a之存取金鑰155a及/或用於認證小程序153b之存取金鑰155b)可由商業實體子系統400產生且可由商業實體子系統400存取(例如,如圖1A中所展示),用於實現於安全元件145與商業實體子系統400之間安全傳輸彼小程序之彼認證資訊。此外或替代地,如所展示,各小程序可包括自己的唯一應用程式識別符(「AID」),諸如小程序153a之AID 155aa及/或小程序153b之AID 155ba。例如,一AID可識別一特定卡方案及產品、程序或網路(例如,MasterCard Cirrus、Visa PLUS、Interac等),其中一AID不僅可包括一經註冊應用程式提供者識別符(「RID」)(其可用以識別與該AID相關聯之認證的一付款系統(例如,卡方案)或網路(例如,MasterCard、Visa、Interac等)),而且亦可包括一專屬應用程式識別符延伸(「PIX」)(其可用以區別由與該AID相關聯之認證的一提供者或付款系統所提供的產品、程式或應用程式)。可操作以統轄安全元件145之韌體的任何合適規格(例如,一Java Card規格)可操作以確保或以其他方式強制在安全元件145上之各AID之唯一性(例如,在安全元件145上之各認證例項可與自己的唯一AID相關聯)。

【0029】 此外或替代地，如圖2A中所展示，安全元件145可包括ISD 152，ISD 152可包括ISD金鑰156k，其亦可係與彼安全性網域相關聯之一受信任服務管理員（例如，商業實體子系統400，如圖1A中所展示）所已知的。相似於及/或替代存取金鑰155a及/或存取金鑰155b，可由商業實體子系統400及電子裝置100充分利用ISD金鑰156k，用於實現介於商業實體子系統400與電子裝置100之安全元件145之間之安全傳輸。另外，如圖2A中所展示，可於處理器102及與安全元件145之間進行各種資料通訊。例如，裝置100之處理器102可經組態以執行一裝置應用程式103，其可與處理器102之一商家應用程式113以及安全元件145、一I/O介面組件114a（例如，用於接收I/O輸入資料115i及/或用於傳輸I/O輸出資料115o）、及/或通訊組件106進行資訊通訊。另外，如所展示，處理器102可存取裝置識別資訊119，可利用裝置識別資訊119用於實現介於裝置100與遠端實體之間之安全通訊。

【0030】 此外或替代地，如圖2A中所展示，安全元件145可包括一控制授權單位安全性網域(「CASD」)158，其可係可經組態以作為一第三方元件上信任根(third-party on-element root of trust)的一特殊用途安全性網域。CASD 158之一相關聯應用程式可經組態以提供元件上機密金鑰產生(on-element confidential key generation)作為一全域服務給其他應用程式及/或給一特定管理層（例如，一GlobalPlatform管理層）。可在CASD 158內使用的機密金鑰材料可經組態使得機密金鑰材料不會被任何實體(包括安全元件145之發行方)調查或修改。CASD 158可經組態以包括及/或可經組態以產生及/或以其他方式包括CASD存取套件158k（例如，CASD私密金鑰(「CASD-SK」)、CASD公開金鑰(「CASD-PK」)、CASD憑證(「CASD-憑證」)、及/或CASD-簽署模組)。例如，CASD 158可經組態

以先在安全元件145上簽署某些資料（例如，使用CASD存取套件158k），之後才提供此類資料至裝置100之另一部分（例如，通訊組件106，以供與系統1之其他子系統共用）。舉一實例，CASD 158可經組態以簽署由安全元件145提供之任何資料，使得其他子系統（例如，商業實體子系統400）可能夠確認此類經簽署資料係由安全元件145所簽署（例如，在商業實體子系統400處使用一相關聯之CASD套件158k）。

【0031】 此外或替代地，如圖2A中所展示，安全元件145可包括一非接觸式登錄服務(「CRS」)小程序或應用程式151，其可經組態以提供本端功能性給電子裝置100，以用於修改某些安全性網域元件之生命週期狀態（例如，經啟動、經撤銷啟動、經鎖定等）及與裝置100之使用者共用關於處於某些生命週期狀態之某些安全性網域元件的某些輸出資訊115o（例如，經由一使用者I/O介面114a）。例如，CRS應用程式151可包括可維持在安全元件145上之各安全性網域元件之目前生命週期狀態清單的一CRS清單151t（例如，可包括SSD 154a之認證小程序153a及/或SSD 154b之認證小程序153b之一者、一些或全部之生命週期狀態的清單），其中CRS應用程式151可經組態以與裝置100之應用程式共用安全元件145之一或多個安全性網域元件之生命週期狀態（例如，與諸如精靈的任何合適的應用程式類型共用生命週期狀態，諸如卡管理精靈(「CMD」)應用程式103a，其可執行作為一作業系統應用程式103及/或一卡管理應用程式103b（例如，Apple Inc.提供的Passbook™或Wallet™應用程式）及/或一商家應用程式113（例如，可與商家金鑰157及商家識別符167相關聯之商家線上資源）及/或一識別服務(「IDS」)應用程式103c內的背景程序，但非必然受控於裝置100之互動使用者），CRS應用程式151繼而可經由I/O介面114a及一使用者介面(「UI」)應用程式（例

如，卡管理應用程式103b之一UI) 來提供某些生命週期狀態資訊給裝置100之使用者作為輸出資訊115o，UI應用程式令使用者能夠變更安全性網域元件之生命週期狀態(例如，更新一CRS清單151t及安全性網域元件之生命週期狀態，諸如，用於實現特定認證小程序之商務認證以供在一金融交易中使用)。此外或替代地，CR151可包括一CRS存取金鑰151k，其亦可係與CRS 151相關聯之一受信任服務管理員(例如，商業實體子系統400，如圖1A中所展示)所已知的。相似於及/或替代存取金鑰155a及/或存取金鑰155b，可由商業實體子系統400及電子裝置100充分利用CRS存取金鑰151k，用於實現介於商業實體子系統400與電子裝置100之安全元件145之間之安全傳輸。

【0032】 IDS應用程式103c可係任何合適的應用程式類型，諸如一精靈，其可執行作為作業系統應用程式103及/或卡管理應用程式103b內的背景程序，及/或可由CMD應用程式103a提供，且可操作為傾聽並回應IDS訊息的IDS管理員，可透過任何合適的IDS服務(其可相似於任何合適的訊息傳送服務，諸如Apple Inc.提供的iMessage™，或類似物(例如，Apple Inc.提供的FaceTime™或Continuity™))發送IDS訊息，IDS服務可實現介於主機裝置100之IDS應用程式103c與另一裝置(例如，一用戶端裝置)之相似IDS應用程式之間的訊息之唯一端對端加密。可使用用於通訊中裝置之一或兩者的唯一識別符及/或用於通訊中裝置之特定使用者之一或兩者的唯一識別符來將此類訊息加密。此類訊息可經傳達作為一本端連結或一真實裝置對裝置(例如，同級間(peer to peer))通訊，或可經由商業實體子系統400(例如，經由識別管理系統組件470)傳達。可實現此類訊息傳送作為一低延時解決方案，其可允許依結構化格式(例如，協定緩衝區(protocol buffer))及/或非結構化格式進行資料交換。若在接收到一IDS訊

息時未正在執行IDS應用程式103c，可自動喚醒IDS應用程式103c。IDS應用程式103c可操作以呈現適當的使用者介面及指引經接收之IDS通訊所請求的資料回傳至正在請求之裝置。主機裝置之IDS應用程式103c可操作以當偵測到來自用戶端裝置的初始請求時喚醒卡管理應用程式103b之卡管理精靈應用程式103a，其可允許主機裝置在低功率「睡眠」模式中操作。此外或替代地，IDS應用程式103c可操作以管理用於此一請求的「逾時」，使得若來自用戶端裝置之一付款請求在主機裝置上無動作達一段時期（例如，60秒，歸因於無回應於此一請求的主動主機裝置使用者互動）時，接著IDS應用程式103c可操作以判定終止該請求，這會導致主機裝置產生並遞送「取消」狀態回到用戶端裝置，其會顯示一適當的訊息（例如，顯示「逾時錯誤」給用戶端裝置之使用者）。

圖3及圖3A至圖3D之說明

【0033】 如圖3中所展示，且如下文所更詳細描述，電子裝置100之一特定實例可係一手持式電子裝置，諸如一iPhone™，其中外殼101可允許存取各種輸入組件110a至110i、各種輸出組件112a至112c、及各種I/O組件114a至114d，裝置100及使用者及/或周邊環境可透過該等組件彼此介接。例如，一觸控螢幕I/O組件114a可包括一顯示輸出組件112a及一相關聯之觸控輸入組件110f，其中可使用顯示輸出組件112a以顯示可允許一使用者與電子裝置100互動的一視覺或圖形使用者介面（「GUI」）180。GUI 180可包括可顯示在顯示輸出組件112a之所有或一些區域中的目前執行中應用程式（例如，應用程式103及/或應用程式113及/或應用程式143）之各種層、視窗、畫面、範本、元件、選單、及/或其他組件。例如，如圖3中所展示，GUI 180可經組態以顯示具有GUI 180之一或多個圖形元素或圖

示182的第一畫面190。選擇特定圖示182時，裝置100可經組態以開啟與彼圖示182相關聯之新應用程式，並顯示與彼應用程式相關聯的GUI 180之相對應畫面，諸如一商家線上資源應用程式。例如，當裝置100之使用者選擇標記有「商家應用程式」文字指示符181（即，特定圖示183）之特定圖示182時，裝置100可啟動或以其他方式存取一特定第三方商家應用程式（例如，一原生應用程式或混合式應用程式）。舉另一實例，當裝置100之使用者選擇標記有「網際網路」文字指示符（即，特定圖示184）之特定圖示182時，裝置100可啟動或以其他方式存取一網際網路瀏覽器應用程式，其可導向至一特定第三方商家之一Web資源之一URL，用於提供另一類型商家線上資源給裝置100。當存取任何合適的商家線上資源時，裝置100可操作以顯示特定使用者介面之畫面，其可包括用於以特定方式使用裝置100來與彼商家線上資源互動之一或多個工具或特徵（例如，請參見圖3A至圖3D，圖中展示在使用任何合適的應用程式（例如，一商家線上資源113）期間，GUI 180之此類顯示之特定實例），裝置使用者可使用該一或多個工具或特徵來實行裝置100之任何安全功能性（例如，使用裝置100之NFC組件120之認證（例如，認證SSD 154a之認證）來付款給商家子系統200））。對於各應用程式，畫面可顯示在顯示輸出組件112a上，且可包括各種使用者介面元素。此外或替代地，對於各應用程式，可經由裝置100之各種其他輸出組件112提供各種其他類型之非視覺資訊給使用者。例如，在一些實施例中，裝置100可不包括操作以提供GUI之使用者介面組件，而是可提供音訊輸出組件及機械或其他合適的使用者輸入組件，用於選擇及鑑認一付款認證之使用，以用於提供一交易之資金或用於實行裝置之任何其他合適的安全功能性。

圖4之說明

【0034】 現在參考圖4，圖4展示關於系統1之商業實體子系統400之特定實施例的進一步細節。如圖4中所展示，商業實體子系統400可係一安全平台系統，且可包括一安全行動平台(「SMP」)代理人組件440、一SMP受信任服務管理員(「TSM」)組件450、一SMP密碼編譯服務組件460、一識別管理系統(「IDMS」)組件470、一詐騙系統組件480、一硬體安全性模組(「HSM」)組件490、商店組件420、及/或一或多個伺服器410。可使用下列各者來實施商業實體子系統400之一組件、一些組件或全部組件：一或多個處理器組件，其可相同於或相似於裝置100之處理器組件102；一或多個記憶體組件，其可相同於或相似於裝置100之記憶體組件104；及/或一或多個通訊組件，其可相同於或相似於裝置100之通訊組件106。可相異於且獨立於金融機構子系統350及/或商家子系統200之一單一商業實體(例如，Apple Inc.)可管理、擁有、至少部分控制及/或以其他方式提供商業實體子系統400之一組件、一些組件或全部組件。商業實體子系統400之組件可彼此互動且與金融機構子系統350及/或電子裝置100及/或商家子系統200共同地用於提供新安全性層及/或用於提供更順暢的使用者體驗。

【0035】 商業實體子系統400之SMP代理人組件440可經組態以使用商業實體使用者帳戶來管理使用者鑑認。SMP代理人組件440亦可經組態以管理在裝置100上之認證之生命週期及佈建。SMP代理人組件440可係可控制裝置100上之使用者介面元素(例如，GUI 180之元素)之主要端點。終端使用者裝置之作業系統或其他應用程式(例如，裝置100之應用程式103、應用程式113及/或應用程式143)可經組態以呼叫特定應用程式設計介面(「API」)，且SMP代理人440可經組態以處理彼等API之請求並回應可導出裝置100之使用者介面的資料及/或回

應可與安全元件145通訊（例如，經由介於商業實體子系統400與電子裝置100之間之一通訊路徑65）的應用程式協定資料單元（「APDU」）。可由商業實體子系統400經由系統1之受信任服務管理員（「TSM」）（例如，商業實體子系統400與金融機構子系統350之間的通訊路徑55之TSM）自金融機構子系統350接收此類APDU。商業實體子系統400之SMP TSM組件450可經組態以提供以GlobalPlatform為基礎之服務或可用以自金融機構子系統350實行在裝置100上之認證佈建操作的任何其他合適的服務。GlobalPlatform或任何其他合適安全頻道協定可使此SMP TSM組件450能夠恰當地於裝置100之安全元件145與一TSM之間傳達及/或佈建敏感性帳戶資料，用於介於商業實體子系統400與金融機構子系統350之間之安全資料通訊。

【0036】 SMP TSM組件450可經組態以使用HSM組件490來保護其金鑰及產生新金鑰。商業實體子系統400之SMP密碼編譯服務組件460可經組態以提供可提供用於使用者鑑認及/或系統1之各種組件之間之機密資料傳輸的金鑰管理及密碼編譯法操作。SMP密碼編譯服務組件460可利用HSM組件490，用於安全金鑰儲存及/或不透明密碼編譯操作。SMP密碼編譯服務組件460之付款密碼編譯服務可經組態以與IDMS組件470互動，以擷取與檔案上信用卡相關聯的資訊或與商業實體之使用者帳戶（例如，Apple iCloud™帳戶）相關聯的其他類型商務認證。此一付款密碼編譯服務可經組態為商業實體子系統400之唯一組件，該組件可在記憶體中具有描述其使用者帳戶之商務認證（例如，信用卡號碼）的純文字(clear text)（例如，非雜湊）資訊。IDMS組件470可經組態以實現及/或管理介於裝置100與另一裝置之間的任何合適通訊，諸如識別服務（「IDS」）傳輸（例如，使用商業實體特定服務（例如，Apple Inc.提供的iMessage™）。例如，某些

裝置可自動地或手動地註冊此一服務（例如，商業實體400之生態系統中的所有裝置可自動地註冊該服務）。此一服務可提供一端對端加密機構，在可使用該服務（例如，使用裝置100之IDS應用程式103c）發送訊息之前，該機構會需要主動註冊。商業實體子系統400之IDMS組件470及/或任何其他合適的伺服器或部分可操作以識別或以其他方式查詢經佈建在與給定使用者帳戶或其他者相關聯的任何電子裝置上之任何認證之狀態，使得商業實體子系統400可操作以有效率且有效地識別一或多個非原生付款認證，非原生付款認證可供與特定使用者帳戶相關聯的特定用戶端裝置（例如，商業實體子系統400之家庭帳戶之多個裝置）使用。商業實體子系統400之商業實體詐騙系統組件480可經組態以基於商業實體已知的有關商務認證及/或使用之資料（例如，基於與隨商業實體之使用者帳戶相關聯之資料（例如，商務認證資訊）、及/或可受控於商業實體的任何其他合適的資料、及/或可不受控於金融機構子系統350之任何其他合適的資料）對商務認證執行商業實體詐騙檢查。商業實體詐騙系統組件480可經組態以基於各種因素或臨限判定針對認證的商業實體詐騙計分。此外或替代地，商業實體子系統400可包括商店420，其可係提供各種服務給裝置100之使用者的提供者（例如，用於銷售/租借待由裝置100播放之媒體的iTunes™商店、用於銷售/租借供在裝置100上使用之應用程式的Apple App Store™、用於儲存來自裝置100之資料及/或使多個使用者裝置及/或多個使用者設定檔彼此相關聯的Apple iCloud™服務、用於線上購買各種Apple產品之Apple線上商店等）。僅舉一實例，商店420可經組態以管理及提供應用程式113至裝置100（例如，經由通訊路徑65），其中應用程式113可係任何合適的應用程式，諸如銀行業務應用程式、商業商家應用程式、電子郵件應用程式、文字訊息傳送應用程式、網際網路應用程式、卡管理

應用程式、或任何其他合適的通訊應用程式。可由商業實體子系統400使用任何合適的通訊協定或通訊協定之組合，以在商業實體子系統400之各種組件之間進行資料通訊（例如，經由圖4之至少一通訊路徑495）及/或於系統1之商業實體子系統400與其他組件之間進行資料通訊（例如，於商業實體子系統400與金融機構子系統350之間經由圖1之通訊路徑55，及/或於商業實體子系統400與電子裝置100之間經由圖1之通訊路徑65）。

圖5之說明

【0037】 圖5係用於驗證對安全裝置功能性之線上存取之闡釋性程序500的流程圖。程序500係展示為由電子裝置100、商業實體子系統400及商家子系統200實施。然而，應理解，可使用任何其他合適的組件或子系統實施程序500。程序500可提供一順暢的使用者體驗：用於安全地且有效率地驗證一第三方商家子系統200，用以實現由商家子系統200線上存取電子裝置100之安全功能性，諸如由商業實體子系統400驗證商家子系統200，以用於實現在與商家子系統200的交易（例如，線上付款或非接觸式之以接近性為基礎之付款）中安全地使用電子裝置100上的認證，或用以實現由商家子系統200自電子裝置100安全存取任何其他合適的資料（例如，地點資料、健康資料、或不宜與尚未有效驗證之第三方子系統共用的任何其他私人資料或其他者）。雖然可利用用語「商家」來描述商家子系統200及/或其任何特徵，諸如商家線上資源或金鑰或伺服器或終端機或識別符，然而應理解，子系統200可係由任何合適的第三方實體操作的任何合適子系統（例如，處理子系統（例如，資料處理子系統）），第三方實體可相異於電子裝置100之擁有者或使用者及/或相異於商業（或控管）實體子系統400。

例如，商家子系統200可係任何合適的第三方子系統，其可嘗試存取或以其他方式接收電子裝置100之安全裝置功能性或與電子裝置100之安全裝置功能性互動（例如，使用商家線上資源載入資料至裝置100上（例如，佈建付款認證於裝置100上）、接收來自裝置100之資料（例如，自裝置100存取付款認證資料或健保資料或地點資料或連絡人資料或私密媒體資料）、及/或類似者）。程序500可操作以於裝置100與任何合適商家子系統之任何合適Web資源之間實現任何合適資料的更安全且更受信任之通訊。程序500可操作以驗證任何合適的Web資源或其他線上資源，以在啟用此類資料通訊之前，確保彼資源具有與商業實體子系統400的一受信任關係。

【0038】 在程序500之步驟501，商家子系統200可向商業實體子系統400註冊。如所提及，商家子系統200之商家線上資源113（例如，原生應用程式、網域/URL、或任何其他合適的Web資源，或甚至可能是一商家終端機）可與特定商家識別符167及特定商家金鑰157相關聯，可依任何合適方式於商家子系統200與商業實體子系統400之間安全地共用特定商家識別符167及特定商家金鑰157之各者，並且此一關聯性可供商業實體子系統400存取（例如，在表格430中）。在一些實施例中，一原生應用程式（例如，一原生應用程式商家線上資源113）之一開發商可使用一權利(entitlement)系統，以允許該應用程式存取正在執行該應用程式的電子裝置100之安全裝置功能性（例如，推送訊息傳送(push messaging)、雲端儲存、安全元件認證付款等），其中該等權利可經簽署至該應用程式的二進位中作為一代碼簽署(code signing)程序之部分，可需要代碼簽署程序以實現由商業實體子系統400註冊該應用程式（例如，用於部署於應用程式商店420中，及/或用於在表格430中安全地使該應用程式之商家金鑰157與商家識

別符167相關聯)，其中商家識別符167可例如形成該應用程式之權利之一部分。不同於此一原生應用程式，Web資源（例如，網站商家線上資源113）可不具有代碼簽署或不具有可提供（例如，由商業實體子系統400）給可操作以在電子裝置100上執行的原生應用程式的相似保護。而是，可在可註冊Web資源之前先實證彼Web資源之網域之擁有權。對於註冊由商家子系統200擁有或以其他方式控制的網站商家線上資源113，在商業實體子系統400註冊彼商家線上資源113之前（例如，在使特定商家識別符167及特定商家金鑰157與彼商家線上資源113相關聯且於商家子系統200與商業實體子系統400之間共用以供未來由商業實體子系統400存取（例如，在表格430中）之前），必須向商業實體子系統400經實證此類擁有權。例如，為了向商業實體子系統400實證待註冊之商家線上資源113之網域之擁有權，可提供該網域之識別至商業實體子系統400，商業實體子系統400可提供任何合適的檔案（例如，靜態檔案，諸如JSON檔案）至商家子系統200，商家子系統200可簽署彼檔案（例如，運用共用之商家金鑰157）及寄存彼檔案於待註冊之該網域上的熟知路徑處，且接著商業實體子系統400可自該網域存取彼經簽署檔案及移除該檔案之簽署（例如，運用共用之商家金鑰157）以確認所存取之檔案符合與商家子系統200共用之檔案。用於註冊Web資源之一些例示性程序可描述於美國專利申請案公開案第2015/0350106號、標題為「Sharing Account Data Between Different Interfaces To A Service」中，該案之全文以引用方式併入本文中。在步驟502可利用任何合適的一或多個程序，用於向商業實體子系統400安全地註冊商家子系統200之任何合適類型商家線上資源113之有效性（例如，待由電子裝置利用的任何原生應用程式、混合式應用程式、Web資源、或甚至商家之商家終端機，無論是否在該裝置本端執行、或遠端寄存於伺服器

上、或經定位接近該裝置），藉此與商家線上資源113相關聯的至少一商家識別符167及至少一商家金鑰157（例如，對稱式或非對稱式金鑰對）可與商家線上資源113相關聯且可供商家子系統200及商業實體子系統400兩者存取（例如，在表格430中）以供未來使用，及可依任何合適方式在任何此類程序期間於商家子系統200與商業實體子系統400之間進行任何合適資料通訊（例如，使用任何合適的通訊協定經由通訊路徑85傳達應用程式113、金鑰157、識別符167及/或任何其他合適的資料）。一或多個商家識別符可與一特定商家線上資源113相關聯，諸如一第一商家識別符167唯一地與特定商家線上資源113相關聯，且/或一第二商家識別符167與特定商家子系統200之各商家線上資源113相關聯。此外或替代地，一或多個商家金鑰可與一特定商家識別符相關聯或與一特定商家線上資源113相關聯。在步驟501之一或多個例項，所有此類商家金鑰與商家識別符之關聯性可由商業實體子系統400予以儲存，或以其他方式可供商業實體子系統400存取（例如，在一或多個表格430中）。

【0039】 在程序500之步驟502，可使用經註冊商家線上資源於商家子系統200與電子裝置100之間進行潛在交易資料通訊。例如，在使用者與執行或以其他方式存取商家線上資源應用程式113的裝置100互動期間之一些時間點（例如，當使用者正在線上購買商家之貨物或服務時，或當使用者使用者正在與醫療專業人員通訊時），可自商家子系統200或自任何其他合適的實體傳達潛在交易資料至裝置100，其可指示相關於可發生於裝置100與商家（或處理）子系統200之商家（或處理器）之間之潛在安全資料交易的任何合適資料，包括但不限於：(i)特定商家資訊，諸如商家線上資源應用程式113之至少一或各商家識別符167；(ii)特定交易資訊，諸如待於裝置100與商家子系統200之間共用之特定類型

安全資料之識別（例如，用於金融交易的貨幣及數額(value amount)及付款類型（例如，使用經佈建在裝置100上之Visa付款認證付款5美元）、用於健康交易的健保資料之類型及總額（例如，如由裝置100所偵測或以其他方式獲得之特定使用者最近3天的心跳率資料），及/或類似物）；及/或(iii)一唯一之以商家為基礎之交易識別符（例如，任何合適的資料元素，諸如一多字元文數字串，其可由商家子系統200隨機或唯一地產生以供與正在進行中的交易相關聯）。此類潛在交易資料可包括可為必要或至少用於完成安全資料交易的任何合適數目個及類型之資料欄位（含或不合相關聯之資料），諸如進行購買之客戶的連絡人資訊欄位（例如，電話號碼、電子郵件地址、郵寄地址），其中一些欄位可經填入且被包括作為此類潛在交易資料之部分，及/或其中一些欄位可未經填入作為此類潛在交易資料之部分，但可在程序500之稍後部分期間開放及等待填入。在本文中，步驟502之此類潛在交易資料可稱為PKDataRequest或PKPaymentRequest（例如，用於金融交易）。在一些實施例中，使用者可不主動與裝置100互動，以在步驟502使與商家子系統200相關聯的潛在交易資料可供裝置100使用。而是，舉一實例，裝置100可經組態以判定一特定產品宜購買並與一或多個商家互動，以自彼特定產品的至少一特定商家獲得相關聯之交易資料（例如，裝置100可係一家用電器，其可經組態以判定必須購買的電器用產品（例如，偵測洗衣機需要更多洗衣清潔劑，或偵測由使用者預設要在特定日期買更多清潔劑的行事曆事件），並可自動識別提供彼產品之最佳優惠的一特定商家，且可自動使用商家線上資源來與彼商家互動以自彼商家獲得用於購買彼產品的交易資料），全部皆自動化且無需由裝置100之使用者進行任何主動互動。步驟502之潛在交易資料可包括必要的所有資料以供裝置100安全地產生及/或提供安全裝

置資料（例如，適當的付款認證資料）至商家子系統200，以用於完成與潛在交易資料相關聯的安全資料交易（例如，為金融交易提供資金）。在步驟502，可依任何合適方式由商家子系統200傳達此類潛在交易資料至裝置100（例如，可使用任何合適的通訊協定經由通訊路徑15，或使用任何合適的通訊協定經由介於終端機220與NFC組件120之間的非接觸式之以接近性為基礎之通訊頻道，自商家子系統200之伺服器210傳輸此類潛在交易資料至裝置100之通訊組件106）。

【0040】 在程序500之步驟504，可起始一商家線上資源驗證工作階段。此可回應於電子裝置100指示安全資料交易（例如，由步驟502之潛在交易資料所識別的安全資料交易）應發生（例如，回應於裝置100之使用者選擇商家線上資源之一GUI元素（例如，選項按鈕(radio button)），用以傳達使用者想要進行由步驟502之商家線上資源之潛在交易資料所識別的安全資料交易，或自動地基於經滿足的任何合適需求（例如，簡單地回應於步驟502之潛在交易資料傳達至裝置100））而發生。當判定運用一商家線上資源實行一特定安全資料交易的此類意圖時，在裝置100上之商家線上資源113可操作以產生及發送一資料交易請求至卡管理應用程式或在裝置100上之任何其他合適的裝置應用程式，且在步驟504，彼裝置應用程式103b可操作以產生及傳達商家驗證工作階段起始資料至商家子系統200。在步驟504，可由電子裝置100產生及/或傳達任何合適的資料至商家子系統200而作為商家驗證工作階段起始資料，用於起始用於待實行之一特定安全資料交易的一商家線上資源驗證工作階段。例如，在步驟504，可由電子裝置100產生一驗證工作階段識別符並且傳達至商家子系統200來作為商家驗證工作階段起始資料之至少一部分，其中此一驗證工作階段識別符可係可唯一識別目前正在起始之商家線上資源驗證工作階段的任何合適之文數字串或任何其他

合適之識別符（例如，唯一識別對商家子系統200及/或對商業實體子系統400的此類工作階段至少達一定時期）。當由電子裝置100產生一驗證工作階段識別符時，該驗證工作階段識別符關於商業實體子系統400可係唯一的，此係藉由利用裝置100之一唯一識別符（例如，裝置識別符119或裝置100之安全元件145之一唯一安全元件識別符，其可係裝置100獨有的（例如，關於商業實體子系統400））來幫助產生該驗證工作階段識別符。此外或替代地，在步驟504，一查問請求目標識別符（例如，一查問請求URL）可自裝置100傳達至商家子系統200作為商家驗證工作階段起始資料之至少一部分，其中此一查問請求目標識別符可識別商家子系統200待與其通訊以驗證該商家之一實體（例如，識別商業實體子系統400之伺服器410之一URL，其可與商家子系統200合作，用以驗證用於待實行之特定安全資料交易的商家線上資源）。一裝置應用程式（例如，卡管理應用程式103b（例如，一錢包應用程式））可具有經程式化之此一查問請求目標識別符（作為任何合適的作業系統或應用程式更新之部分），其可受控於商業實體子系統400，使得可由商業實體子系統400在任何合適的時間更新裝置100上之查問請求目標識別符。此外或替代地，此類商家驗證工作階段起始資料可包括任何其他合適的資料，諸如：指示對商家驗證其自身之一請求的任何合適資料；指示裝置100的任何合適資料（例如，裝置識別符119）；及/或指示待實行之特定安全資料交易的任何合適資料（例如，來自步驟502之潛在交易資料的任何合適資料，諸如特定商家資訊（例如，商家識別符167）、特定交易資訊（例如，用於金融交易的貨幣及數額及付款類型或用於健康交易的健保資料之類型及總額）、及/或一唯一之以商家為基礎之交易識別符）。在步驟504，可依任何合適方式由裝置100傳達任何合適的商家驗證工作階段起始資料至商家子系統200

（例如，可使用任何合適的通訊協定經由通訊路徑15，或使用任何合適的通訊協定經由介於NFC組件120與終端機220之間之一非接觸式之以接近性為基礎之通訊頻道，自裝置100之通訊組件106傳輸此類商家驗證工作階段起始資料至商家子系統200之伺服器210）。

【0041】 在程序500之步驟506，回應於在步驟504商家子系統200接收來自裝置100的任何合適商家驗證工作階段起始資料以用於起始一驗證工作階段，商家子系統200可操作以與商業實體子系統400通訊以驗證商家線上資源。在一些實施例中，其中步驟504之商家驗證工作階段起始資料不包括一驗證工作階段識別符，商家子系統200可操作以產生可唯一識別經起始之當前商家線上資源驗證工作階段的此一驗證工作階段識別符。當由商家子系統200產生一驗證工作階段識別符時，該驗證工作階段識別符關於商業實體子系統400可係唯一的，此係藉由商家子系統200確保至少關於相同商業實體子系統及/或關於相同商家識別符及/或在足以確保工作階段識別符對於在一商業實體子系統處的任何特定程序非係擱置中的一定時期內，不使用相同驗證工作階段識別符兩次。步驟506可包括任何合適數目個子程序，該等子程序可使商業實體子系統400能夠驗證用於待實行之特定安全資料交易的商家線上資源（例如，如在步驟502及504所識別）。如關於在圖6之程序600之步驟614至622所詳細描述，步驟506之驗證可包括商家子系統200傳達下列項目至商業實體子系統400（例如，如可藉由在步驟504來自裝置100之商家驗證工作階段起始資料所識別）：一查問請求，其可包括與待驗證之商家線上資源相關聯的一商家識別符（例如，如在步驟501所註冊之商家識別符167，其可係一商家線上Web資源之一網域）；一驗證工作階段識別符（例如，如在步驟504由電子裝置100所產生者，或在步驟506由商家子系統200所產

生者)；及任何其他合適的資料(例如，識別裝置100的資料及/或識別待實行之特定安全資料交易的資料)。可由商家子系統200使用與查問請求之商家識別符相關聯之一商家金鑰(例如，如在步驟501連同商家識別符167一起註冊之商家金鑰157(例如，用於待驗證之商家線上資源113))來簽署此一查問請求(例如，在一HTTP標頭中或以其他方式)。商業實體子系統400可操作以接收此一查問請求，驗證由查問請求之商家識別符167所識別的商家線上資源113(例如，以確認已在步驟501註冊商家線上資源113(例如，藉由在表格430中識別彼商家識別符167)且其仍然有效)，且接著驗證該查問請求之簽章(例如，使用在表格430中與彼經識別商家識別符167相關聯的商家金鑰157)。回應於驗證查問請求之元件，商業實體子系統400可：產生查問資料(例如，經由熵(entropy)的任何合適隨機資料)；依任何合適的資料結構(例如，表格430或以其他方式)對照識別符資料(例如，查問請求之驗證工作階段識別符及商家之商家識別符之一或兩者)來儲存該查問資料；使用可由商業實體子系統400存取之一商家金鑰157來加密該查問資料(例如，來自表格430的用以驗證該查問請求之簽章之商家金鑰)；及接著傳達查問資料至商家子系統200，該查問請求可包括經加密查問資料連同任何其他合適的資料，諸如用以加密該查問資料的該商家金鑰之一雜湊(例如，表格430之一公開商家金鑰157之一雜湊版本，其可由商家子系統200用來識別恰當的商家金鑰157(例如，用於解密該查問資料的商家子系統200之私密金鑰157))，可提供雜湊版本以輔助可具有多個經註冊商家線上資源及/或多個商家金鑰的商家)；該查問請求之驗證工作階段識別符；及/或類似物。回應於接收此類查問資料，商家子系統200可操作以使用適當的商家金鑰157來解密經加密查問資料(例如，在商家子系統200處的一私密商家金鑰157，如可

已在步驟501註冊），並接著傳達查問回應資料（包括經解密之查問資料連同任何其他合適的資料，諸如查問請求之驗證工作階段識別符及適當的商家識別符）至商業實體子系統400，其中可由商家子系統200使用與查問請求之商家識別符相關聯之一商家金鑰（例如，如在步驟501所註冊之商家金鑰157與商家識別符167（例如，用於待驗證之商家線上資源113））來簽署彼查問回應（例如，在一HTTP標頭中或以其他方式）。回應於接收此類查問回應資料，商業實體子系統400可操作以驗證該查問回應之簽章（例如，使用在表格430中與所識別商家識別符167相關聯之商家金鑰157），並確認該查問回應之經解密查問資料係對照該查問回應之驗證工作階段識別符及/或對照商家之一識別符經儲存（例如，在表格430中）。在一些實施例中，介於該查問資料與驗證工作階段識別符及商家識別符之一或兩者之間的此一儲存連結可在自動清除該連結之前維持達僅一段有限時間量，使得商家子系統200會受限於必須在一定持續時間內接收查問資料並接著發送適當的查問回應資料至商業實體子系統400，用以驗證針對特定驗證工作階段的商家線上資源（例如，商業實體子系統400可操作以在一定時期之後移除在商業實體子系統400處之介於該查問資料與驗證工作階段識別符及/或商家識別符之間的此一關聯性（例如，在建立該連結後不超過10分鐘（或任何其他合適的時期）即自表格430移除該連結），其可增加交易安全性。因此，可使用在商業實體子系統400處之介於商家金鑰與商家識別符之間的關聯性（例如，如在步驟501所註冊者）來完成在步驟506之用於待實行之特定安全資料交易（例如，如在步驟502及504所識別）的商家線上資源之驗證。在步驟506可依任何合適方式於商家子系統與商業實體子系統400之間進行任何合適的資料通

訊（例如，可使用任何合適的通訊協定經由通訊路徑85，於商家子系統200之伺服器210與商業實體子系統400之伺服器410之間傳輸此類資料）。

【0042】 在步驟508，回應於在步驟506基於在步驟504起始之驗證工作階段來驗證商家線上資源，商業實體子系統400可產生驗證資料並對照識別符資料（諸如該驗證工作階段之該驗證工作階段識別符及/或商家識別符）來儲存該驗證資料。例如，回應於驗證該查問回應之簽章及回應於確認在商業實體子系統400處（例如，在表格430中）亦恰當地連結該查問回應之查問資料及驗證工作階段識別符及/或商家識別符，在步驟508，商業實體子系統400可：耗用彼連結（例如，移除在商業實體子系統400處之介於查問資料與驗證工作階段識別符及/或商家識別符之間的此一關聯性（例如，自表格430移除該連結））；產生驗證資料（例如，任何合適的隨機資料（例如，一密碼編譯臨時值(*nonce*)（例如，經由熵的任何合適隨機資料）））；並接著對照查問請求之驗證工作階段識別符及/或查問回應之驗證工作階段識別符來儲存該驗證資料，或以其他方式使該驗證資料與查問請求之驗證工作階段識別符及/或查問回應之驗證工作階段識別符相關聯，及/或對照商家之商家識別符來儲存該驗證資料（例如，依任何合適的資料結構（諸如表格430）或以其他方式）。

【0043】 在步驟510，回應於在步驟506驗證一商家線上資源並接著在步驟508對照一驗證工作階段識別符及/或商家識別符來儲存任何合適的驗證資料，商業實體子系統400可傳達驗證回應資料至電子裝置100，其中此類驗證回應資料可包括任何合適的資料，包括但不限於：步驟508之驗證資料；步驟508之驗證工作階段識別符；識別在步驟506所驗證之商家線上資源的資料（例如，商家識別符167）；及/或任何其他合適的資料。在一些實施例中，如圖5中所展示，可

自商業實體子系統400直接傳達此類驗證回應資料至電子裝置100（例如，使用任何合適的通訊協定經由通訊路徑65），其中識別電子裝置100的資料（例如，裝置識別符119）可與驗證工作階段識別符相關聯（例如，在步驟502或以其他方式）且藉由步驟506之驗證而相關聯，使得商業實體子系統400可傳達該驗證回應資料至恰當的電子裝置100。替代地，在一些實施例中，可經由商家子系統200自商業實體子系統400傳達此類驗證回應資料至電子裝置100，藉此商家子系統200可接收來自商業實體子系統400之驗證回應資料（例如，使用任何合適的通訊協定經由通訊路徑85）並接著傳遞該驗證回應資料之至少一部分至電子裝置100上（例如，使用任何合適的通訊協定經由通訊路徑15或作為一非接觸式之以接近性為基礎之通訊）。可由商業實體子系統400使用與商業實體子系統400相關聯的一存取金鑰（例如，存取金鑰155a、存取金鑰155b、CRS 151k、及/或安全元件145之ISD金鑰156k，或一裝置應用程式（例如，卡管理應用程式103b）可已知的任何金鑰）來簽署此類驗證資料（例如，在一HTTP標頭中或以其他方式），電子裝置100亦可存取該存取金鑰，使得裝置100可在接收到該經簽署驗證資料後驗證簽章，以確認商業實體子系統400產生該驗證資料，而非不受電子裝置100信任的另一實體子系統產生該驗證資料。

【0044】 在程序500之步驟512，安全裝置資料可至少部分由裝置100產生或存取，且接著在步驟514，此類安全裝置資料連同在步驟510所接收之驗證回應資料之至少一部分及步驟502之潛在交易資料之至少一部分可由裝置100傳達至商業實體子系統400作為裝置交易資料。例如，回應於在步驟510接收驗證回應資料（其可指示被用於步驟502之潛在交易資料的商家線上資源之有效性），裝置100可操作以在步驟512獲得或以其他方式識別待與商家子系統200共用之

安全資料以用於實行特定安全資料交易（例如，產生付款認證資料以供在一金融交易中使用，或收集待在一健康交易中共用的特定健康資料）。接著，在步驟514，裝置100可傳達步驟512之彼安全資料連同步驟510之驗證回應資料之驗證資料及驗證工作階段識別符及商家識別符及/或連同與待實行之潛在安全資料交易相關的任何合適資料（例如，如可由步驟502之潛在交易資料提供至裝置100者，諸如特定商家資訊（例如，商家識別符167）、特定交易資訊（例如，用於金融交易的貨幣及數額及付款類型，或用於健康交易的健保資料之類型及總額）、及/或一唯一基於商家之交易識別符）作為至商業實體子系統400之裝置交易資料。因此，在步驟514自裝置100傳達至商業實體子系統400之裝置交易資料可包括步驟502之潛在交易資料以及步驟512之安全裝置資料以及步驟510之驗證回應資料之一些或全部。

【0045】 在步驟514傳達裝置交易資料至商業實體子系統400之前，裝置100可運用一商業實體金鑰來加密步驟514之裝置交易資料之全部或至少一部分（例如，步驟512之安全裝置資料）。例如，裝置100可運用存取金鑰155a、存取金鑰155b、CRS 151k、CASD 158k、及/或安全元件145之ISD金鑰156k或裝置100可存取之任何其他金鑰來加密裝置交易資料之至少一部分（例如，自任何裝置應用程式103至處理器102或以其他方式），商業實體子系統400亦可存取該等金鑰（例如，介於裝置100與商業實體子系統400之間的任何共用祕密）。在一些實施例中，此一商業實體金鑰或存取金鑰可係與商業實體子系統400之一方案相關聯的一商業實體公開金鑰且其之商業實體子系統400可存取一相關聯之商業實體私密金鑰。商業實體子系統400可依任何合適方式來提供此一商業實體公開金鑰至裝置100。在步驟514可由裝置100依任何合適方式來傳達裝置交易資料

（無論是否藉由任何合適的商業實體金鑰來至少部分加密及/或簽署）至商業實體子系統400（例如，可使用任何合適的通訊協定經由通訊路徑65，自裝置100之通訊組件106傳輸此類裝置交易資料至商業實體子系統400之伺服器410）。

【0046】 接下來，在接收在步驟514傳達之裝置交易資料之後，程序500之步驟516可包括商業實體子系統400驗證在步驟514接收之所接收的裝置交易資料之驗證資料。例如，回應於接收此類裝置交易資料，在步驟516，商業實體子系統400可操作以識別來自彼裝置交易資料之驗證回應資料，並確認彼所接收之驗證回應資料之驗證資料係對照所接收之裝置交易資料之一驗證工作階段識別符（例如，驗證回應資料）及/或對照所接收之裝置交易資料之一商家識別符（例如，驗證回應資料）經儲存（例如，在表格430中）。在一些實施例中，介於該驗證資料與驗證工作階段識別符及商家識別符之一或兩者之間的此一所儲存連結可在自動清除該連結之前維持達僅一段有限時間量，使得電子裝置100會受限於必須在一定持續時間內在步驟510接收驗證回應資料並接著在步驟514發送裝置交易資料至商業實體子系統400，用於實現由商業實體子系統400保護彼裝置交易資料之安全裝置資料的安全，以用於運用經驗證商家線上資源實行特定安全資料交易（例如，商業實體子系統400可操作以在一定時期之後移除在商業實體子系統400處之介於驗證資料與驗證工作階段識別符及/或商家識別符之間的此一關聯性（例如，在建立該連結之後不超過10分鐘（或任何其他合適的時期）即自表格430移除該連結），其可增加交易安全性。此外或替代地，在步驟508亦可使介於該驗證資料與驗證工作階段識別符及商家識別符之一或兩者之間的一所儲存連結與任何合適的特定交易資訊（在步驟506期間可藉由商家子系統200使彼特定交易資訊可供商業實體子系統400使用）相關聯（例如，作為

一查問請求之一部分），諸如待共用於裝置100與商家子系統200之間的一特定類型安全資料之識別（例如，用於金融交易的貨幣及數額及付款類型（例如，使用經佈建在裝置100上之Visa付款認證付款5美元）、用於健康交易的健保資料之類型及總額（例如，由裝置100所偵測或以其他方式獲得之特定使用者最近3天的心跳率資料），及/或類似物），及亦可藉由電子裝置100使相似特定交易資訊可供商業實體子系統400使用作為步驟514之裝置交易資料之一部分，使得步驟516亦可包括商業實體子系統400確認目前對照在步驟514所接收之驗證資料所儲存之特定交易資訊（例如，如在步驟508儲存在表格430中者）在一特定程度上至少相似於在步驟514所接收之特定交易資訊，其可增加交易安全性。例如，如果在步驟508對照與指示5美元金融交易之潛在交易相關聯的特定交易資訊來儲存特定驗證資料，但是接著在步驟514由商業實體子系統400連同彼特定驗證資料一起接收的特定交易資訊指示2,000美元之金融交易，則歸因於介於5美元與2,000美元之間之差異量值大於一特定臨限（例如，超過一5%差值），商業實體子系統400可操作以不驗證該裝置交易資料之該驗證資料。因此，即使在商業實體子系統400處確認在步驟514所接收之裝置交易資料之驗證資料及驗證工作階段識別符及/或商家識別符為經主動連結（例如，在表格430中），如果該裝置交易資料未滿足可與彼連結相關聯之其他資料，則該驗證資料仍可不被驗證（例如，如果在驗證步驟506期間識別的安全資料交易之任何合適特性與步驟514之裝置交易資料中所識別之任何合適特性相差達任何合適的量（例如，相差超過一金融交易貨幣值之10%、相差超過健康資料之時間框架之10%、健康資料之類型係不同等））。

【0047】 在程序500之步驟518，回應於在步驟516驗證該裝置交易資料之該驗證資料，商業實體子系統400可藉由使用與商家子系統200的一共用祕密至少加密在步驟514所接收之裝置交易資料之安全裝置資料來進一步保護裝置交易資料之安全裝置資料的安全，使得商家子系統200以外之任何實體無法接收及利用該安全裝置資料。例如，回應於在步驟516藉由確認裝置交易資料之驗證資料及驗證工作階段識別符及/或商家識別符亦在商業實體子系統400處恰當地連結（例如，在表格430中）而驗證裝置交易資料之驗證資料，商業實體子系統400可耗用彼連結（例如，移除在商業實體子系統400處之介於驗證資料與驗證工作階段識別符及/或商家識別符之間的此一關聯性（例如，自表格430移除該連結））並進行至步驟518以用於進一步保護裝置交易資料之安全裝置資料的安全。如果步驟514之裝置交易資料經用任何商業實體金鑰予以加密，則在步驟518，商業實體子系統400可操作以解密此類資料（例如，商業實體子系統400之伺服器410可接收裝置交易資料並接著解密/移除簽署彼裝置交易資料（例如，用存取金鑰155a、存取金鑰155b、CRS 151k、CASD 158k，及/或商業實體子系統400之ISD金鑰156k））。藉由依已使用裝置100及商業實體子系統400兩者已知之一商業實體金鑰加密/簽署的形式來於裝置100與商業實體子系統400之間進行裝置交易資料通訊，程序500可抑制彼裝置交易資料之通訊被不具有商業實體金鑰之存取權的一實體攔截及使用。另外，在步驟518，商業實體子系統400可操作以用一商家金鑰（例如，一商家金鑰157，其可與正在提供該特定交易之資金所針對的商家子系統200相關聯）來加密或以其他方式重新格式化裝置交易資料之至少一部分。商業實體子系統400可經由表格430來判定及存取此一商家金鑰（例如，藉由識別與步驟514之裝置交易資料之一商家識別符相關聯之一商家金鑰）。在

步驟518，可由商業實體子系統400接收及利用該商家識別符以識別可由商業實體子系統400存取之許多商家金鑰之一特定者（例如，商家金鑰157，透過充分利用商業實體子系統400之表格430），且接著商業實體子系統400可使用彼經識別之商家金鑰來用於加密該裝置交易資料之至少一部分（例如，至少裝置交易資料之安全裝置資料）。藉由用此一商家金鑰（例如，可係商業實體子系統400及商家子系統200已知之一金鑰，而非電子裝置100或系統1之任何其他子系統已知之一金鑰）來加密此類安全裝置資料，使得此類安全裝置資料之安全可受到保護而可自商業實體子系統400安全地傳達至商家子系統200，而不會被另一實體攔截而用於非預定用途。在步驟518由商業實體子系統400利用來至少加密裝置交易資料之安全裝置資料的商家金鑰可係與在步驟506驗證商家線上資源期間由商業實體子系統400用來加密該查問資料的商家金鑰相同的金鑰（例如，非可供裝置100或除商業實體子系統400及商家子系統200外之任何子系統使用之一金鑰）。因此，商業實體子系統400可操作以使用最近在安全資料交易特定之一商家驗證工作階段期間已藉由商業實體子系統400驗證之一商家線上資源促進介於裝置100與商家子系統200之間之一安全資料交易（例如，步驟504及506之驗證工作階段以及步驟516及518之安全資料交易可使用主動或以其他方式啟用達一段有限時間量的相同驗證工作階段識別符（例如，介於驗證工作階段識別符與查問資料之間之一連結及/或介於驗證工作階段識別符與驗證資料之間之一連結可在商業實體子系統400處有效達一段有限時間量（例如，任何合適的時間量，諸如介於30秒與10分鐘之間）），其可增加交易安全性）。

【0048】 接下來，在步驟520，程序500可包括商業實體子系統400傳達步驟518之經保護安全之安全裝置資料至裝置100來作為經保護安全之交易資料。

例如，在步驟520，可使用任何合適的通訊協定經由通訊路徑65，將裝置交易資料的此類經商家金鑰加密之安全裝置資料作為經保護安全之交易資料之至少一部分，自商業實體子系統400傳輸至裝置100。此類經保護安全之交易資料除包括該經商家金鑰加密之安全裝置資料外，亦可包括任何合適的資料，諸如與交易相關聯的步驟502之任何合適的資料，包括但不限於：(i)特定商家資訊，諸如一商家識別符之識別，其可識別提供步驟502之潛在交易資料的特定商家子系統200；(ii)特定交易資訊，諸如用以支付一金融交易的一特定貨幣或金額之識別；(iii)一唯一之以商家為基礎之交易識別符（例如，如由商家子系統200產生以供與正在進行中的交易相關聯）；(iv)一唯一之以裝置為基礎之交易識別符（例如，如由電子裝置100所產生以供與正在進行中的交易相關聯）；(v)該驗證工作階段識別符，及/或類似物。因此，在步驟520自商業實體子系統400傳達至裝置100的經保護安全之交易資料可包括步驟502之潛在交易資料之一些或全部以及經保護安全之安全裝置資料。

【0049】 接下來，在程序500之步驟522，裝置100可接收在步驟520自商業實體子系統400傳達的經保護安全之交易資料且可依任何合適方式來與商家子系統200共用彼經保護安全之交易資料。例如，可使用任何合適的通訊協定經由通訊路徑15及/或作為介於NFC組件120與商家終端機220之間的一非接觸式之以接近性為基礎之通訊，自裝置100之通訊組件106傳輸此類經保護安全之交易資料至商家子系統200之伺服器210。在步驟522可由裝置100傳達至商家子系統200的經保護安全之交易資料（例如，使用商家線上資源113（例如，相同於在步驟502使用的資源））除包括步驟520之經商家金鑰加密之安全裝置資料外，亦可包括任何合適的資料，諸如與交易相關聯之任何合適的資料，包括但不限於：(i)

特定商家資訊，諸如一商家識別符之識別，其可識別提供步驟502之潛在交易資料的特定商家子系統200；(ii)特定交易資訊，諸如用以支付一金融交易的一特定貨幣或金額之識別；(iii)一唯一之以商家為基礎之交易識別符（例如，如由商家子系統200產生以供與正在進行中的交易相關聯）；(iv)一唯一之以裝置為基礎之交易識別符（例如，如由電子裝置100所產生以供與正在進行中的交易相關聯）；(v)該驗證工作階段識別符，及/或類似物。因此，在步驟522與商家子系統200共用的經保護安全之交易資料可包括步驟502之潛在交易資料之一些或全部以及步驟518之至少該經商家金鑰加密之安全裝置資料。藉由在步驟522傳達經保護安全之交易資料的經商家金鑰加密之安全裝置資料，程序500可實現此類經商家金鑰加密之安全裝置資料至商家子系統200之通訊以用於促進特定安全資料交易，同時防止在步驟512由裝置100所產生或以其他方式識別的安全裝置資料被不具有該商家金鑰之存取權的一商家（或處理器）實體（例如，除系統1之商家子系統200外的一商家子系統或任何其他子系統）使用。替代地，雖然未展示，可依任何合適方式（例如，使用任何合適的通訊協定經由通訊路徑85）來自商業實體子系統400直接傳達此類經保護安全之交易資料至商家子系統200（而非在步驟520及522經由裝置100進行傳達），其中商業實體子系統400可充分利用步驟514之裝置交易資料之任何商家識別符來識別目標商家子系統200。在已由商家子系統200接收經保護安全之交易資料的經商家金鑰加密之安全裝置資料之後，程序500可包括商家子系統200利用彼經商家金鑰加密之安全裝置資料以用於任何合適的用途（例如，任何合適的安全裝置資料處理或處置）。

【0050】 應理解，圖5之程序500中展示之步驟僅係闡釋性，且可修改或省略現有步驟、可新增額外步驟、並且可改變某些步驟之順序。應理解，如果程

序500之任何驗證步驟失敗，此類失敗可傳達至一或多個合適的實體。例如，如果在步驟506一商家線上資源之驗證失敗及/或如果在步驟516驗證資料之驗證失敗，可由商業實體子系統400與電子裝置100共用此類失敗，使得裝置100可取消與商家子系統200的潛在交易且有可能自裝置100移除商家線上資源。在裝置100之使用者可選取某些安全資料以用於在步驟512之一安全資料交易之後，程序500之其餘步驟可對彼使用者透通地發生（例如，步驟514至522可發生而無需任何與裝置100的進一步使用者互動且對裝置100之使用者而言如同瞬時）。在步驟512之後，程序500對裝置100之使用者而言看來像是安全裝置資料係自動且瞬間地發送至商家子系統200並且可對裝置100確認交易狀態（例如，藉由商家子系統200及/或商業實體子系統400）。此外或替代地，一商家線上資源之驗證可對裝置100透通地發生（例如，步驟506至510（若未亦含步驟504）可發生而無需任何與裝置100的使用者互動，且步驟502之後對裝置100之使用者而言如同瞬時）。替代地，在一些實施例中，程序500可對裝置100之使用者完全透通地發生（例如，其中裝置100可經組態以自動判定何時宜發生一安全裝置交易及自動接收驗證回應資料、及/或自動發送裝置交易資料、及/或自動接收及/或發送經保護安全之交易資料以用於一安全裝置交易，而無需與裝置100的任何主動使用者互動）。

圖6之說明

【0051】 圖6係用於驗證對安全裝置功能性之線上存取之闡釋性程序600的流程圖，用於進行一金融交易。程序600係展示為由電子裝置100、商家子系統200、收單銀行子系統300、商業實體子系統400、及金融機構子系統350實施。

然而，應理解，可使用任何其他合適的組件或子系統實施程序600。程序600可提供一順暢使用者體驗，用於使用來自裝置100之一付款認證安全地且有效率且進行與商家子系統200之一金融交易。為了有助於下文關於用於根據圖6之程序600進行金融交易之系統1之操作的論述，參考圖1至圖4之示意圖之系統1之各種組件，及參考圖3至圖3D之畫面190至190d的前視圖，其可代表在此一交易期間裝置100之一圖形使用者介面（例如，如可由裝置100之商家線上資源113或任何合適的應用程式提供的一GUI）。可使用廣泛多樣的圖形元素及視覺方案來達成所描述之操作。因此，圖3至圖3D之實施例非意欲受限於本文採用之精確使用者介面慣例。而是，實施例可包括廣泛多樣的使用者介面樣式。雖然至少部分地在驗證商家子系統200以用於實現由商家子系統200存取電子裝置100之安全付款功能性的內容脈絡中來描述程序600之步驟，然而應理解，可利用程序600之許多（若非全部）部分以用於驗證任何合適的第三方子系統，用以實現由彼第三方子系統存取裝置100之任何安全功能性（例如，地點資料、健康資料、或不宜與尚未有效地經驗證之第三方子系統共用或自尚未有效地經驗證之第三方子系統接收之任何其他私人資料或其他）。

【0052】 程序600可開始於步驟602，在此步驟可由商業實體子系統400在裝置100上佈建存取資料652（例如，圖1A之存取資料652）。例如，可自商業實體子系統400之伺服器410將一存取SSD（例如，SSD 154b）佈建在裝置100之安全元件145上作為存取資料652，以更安全地使裝置100能夠與商家子系統200進行一交易。如所提及，可直接自商業實體子系統400將存取SSD 154b至少部分地佈建在裝置100之安全元件145上（例如，作為經由介於商業實體子系統400之伺服器410與裝置100之通訊組件106之間之通訊路徑65的存取資料652，其接著可

自通訊組件106傳遞至安全元件145（例如，經由匯流排118））。存取資料652經由路徑65可經佈建在裝置100之安全元件145上作為一存取SSD154b之至少一部分或全部，且可包括存取小程序153b及/或存取金鑰155b。可在最初組態裝置100時至少部分地實行步驟602（例如，在裝置100出售給一使用者之前，由商業實體子系統400實行）。替代地或此外，可回應於裝置100之使用者一開始設定NFC組件120之安全元件145而至少部分實行步驟602。此外或替代地，存取資料652可包括用於安全元件145之ISD 152的ISD金鑰156k，且可除使用存取金鑰155b外或作為金鑰155之替代而使用ISD金鑰156k，用以實現介於商業實體子系統400與裝置100之間之安全傳輸。此外或替代地，存取資料652可包括裝置100之安全元件145的CRS 151之CRS 151k及/或CASD 158之CASD 158k，並可除使用存取金鑰155b及/或存取金鑰155a及/或ISD金鑰156k外或作為存取金鑰155b及/或存取金鑰155a及/或ISD金鑰156k之替代而使用，用以實現介於商業實體子系統400與裝置100之間之安全傳輸（例如，用作為介於商業實體子系統400與裝置100之間之任何合適的商業實體金鑰或共用祕密）。替代地或此外，存取資料652可包括介於商業實體子系統400與裝置100之間之任何其他合適的商業實體金鑰或共用祕密，其可未儲存於裝置100之一安全元件上，而是可供裝置100之其他部分（諸如處理器102）經由記憶體104存取。

【0053】 在程序600之步驟604，金融（或發行方或交易）機構子系統350可在裝置100上佈建認證資料654（例如，圖1A之認證資料654），在一些實施例中係經由商業實體子系統400。例如，此類認證資料654可直接自金融機構子系統350至少部分佈建在裝置100之安全元件145上（例如，經由介於金融機構子系統350與裝置100之間之圖1A之通訊路徑75，其可經由通訊組件106傳遞至安全元

件145)。此外或替代地，此類認證資料654可自金融機構子系統350經由商業實體子系統400至少部分地佈建在裝置100之安全元件145上（例如，經由介於金融機構子系統350與商業實體子系統400之間之圖1A之通訊路徑55，其可經由介於商業實體子系統400之伺服器410與裝置100之通訊組件106之間之圖1A之通訊路徑65傳遞至裝置100而作為認證資料654，其接著可自通訊組件106傳遞至安全元件145（例如，經由匯流排118））。認證資料654經由路徑75及/或經由路徑65可經佈建在裝置100之安全元件145上作為認證SSD 154a之至少一部分或全部，且可包括含認證資訊161a及/或認證金鑰155a'及/或金鑰155ak之認證小程序153a。可在裝置100之使用者選擇待佈建在裝置100上之一特定認證時至少部分地實行步驟604。在一些實施例中，認證資料654亦可包括存取金鑰155a，其可於最初自商業實體子系統400提供至金融機構子系統350及/或可由商業實體子系統400新增。在一些實施例中，此類認證資料654可包括：主要帳戶號碼，其作為經佈建之付款認證之認證資訊之至少一部分（例如，小程序153a之認證資訊161a）；一AID（例如，經佈建在SSD 154a處之付款認證之資料之小程序153a之AID 155aa）；一SSD識別符；及/或一SSD計數器。

【0054】 經佈建在裝置100上之認證資料可包括用彼認證進行付款所必須的所有資料（當彼認證係一金融或付款認證時），例如，諸如一主要帳戶號碼（「PAN」）、一卡安全性碼（例如，一卡驗證碼（「CVV」））、PAN到期日期、與該認證相關聯之名稱、及類似者，以及可供裝置100操作以產生適當之密碼編譯資料的其他資料（例如，任何合適的共用祕密及可至少部分藉由該共用祕密判定其之功能輸出的任何合適之密碼編譯演算法或加密法）。一「虛擬」認證或虛擬PAN或裝置PAN（「D-PAN」）可佈建在裝置100上，而非使用者的「實際」

認證或實際PAN或資金PAN(「F-PAN」)。例如，一旦判定一認證待佈建在裝置100上，則可(例如，由金融機構子系統350、由商業實體子系統400、及/或由裝置100之使用者)請求一虛擬認證(而非實際認證)被產生、連結至該實際認證、及佈建在裝置100上。與一實際認證之一虛擬認證的此類建立及連結可由金融機構子系統350之任何合適的組件來執行。例如，一付款網路子系統360(例如，可與該實際認證之品牌相關聯的一特定付款網路子系統360)可定義及儲存可建立介於該實際認證與一虛擬認證之間之關聯性的一虛擬連結表格312(例如，如圖1A中所展示)，使得在由裝置100利用一虛擬認證來用於與商家子系統200之一金融交易(例如，經佈建在裝置100上之後)的任何時間，付款網路子系統360可接收一授權或驗證請求或以其他方式嘗試驗證任何所接收之指示彼虛擬認證的資料(例如，在步驟640回應於在步驟638接收資料688)並可按照如藉由表格312所判定之與該虛擬認證相關聯的該實際認證來分析彼驗證嘗試請求。替代地，可由一適當的發行銀行子系統370或可由金融機構子系統350可存取之任何其他合適的子系統來存取及/或同樣地充分利用此一表格。藉由在裝置100上佈建一虛擬認證(而非一實際認證)，金融機構子系統350可經組態以限制當虛擬認證被未經授權使用者攔截時可導致的詐騙活動，此係因為付款網路子系統360可僅經組態以在某些交易期間利用用於連結該虛擬認證至該實際認證的表格312。

【0055】 在程序600之步驟606，商業實體子系統400可註冊商家子系統200。例如，如關於在程序500之步驟501所描述，在步驟606，商家子系統200之一商家線上資源113(例如，原生應用程式、網域/URL、或任何其他合適的Web資源，或甚至可能是一商家終端機)可與至少一特定商家識別符167及至少一特定商家金鑰157相關聯，可依任何合適方式於商家子系統200與商業實體子系統

400之間安全地共用至少一特定商家識別符167及至少一特定商家金鑰157之各者，並且此一關聯性可供商業實體子系統400存取（例如，在表格430中），使得可向商業實體子系統400註冊商家線上資源113。在一些實施例中，為了參與一線上資源付款計劃，會要求一商家註冊作為由商業實體子系統400之商業實體執行之一計劃的一成員及/或獲得一商家憑證。在沒有一憑證或其他合適的註冊證明的情況中，商家無法接收付款資料。無論如何或在何處，可產生及/或管理此類（一或多個）商家金鑰及/或（一或多個）商家識別符，商家子系統200及商業實體子系統400兩者可儲存任何商家金鑰對之一商家金鑰之一版本（例如，儲存在商家子系統200及商業實體子系統400之一各自的安全元件中）。此可實現介於商業實體子系統400與商家子系統200之間之一共用祕密，用於在彼等之間安全地傳達資料。在一些實施例中，裝置100可具備此一商家金鑰以用於運用在裝置100上之彼金鑰安全地加密付款資料。

【0056】 在程序600之步驟608，裝置100可存取一商家的線上資源658（例如，圖1A之一商家線上資源113（例如，如在步驟606所註冊者））。如圖1A中所展示，一商家的資源應用程式113可自商業實體子系統400（例如，自應用程式商店420）載入至裝置100上。例如，如圖3中所展示，裝置100之使用者可使用I/O組件114a之觸控螢幕輸入組件110f來選擇GUI 180之一特定畫面190之一「商家應用程式」圖示183，且可由裝置100辨識此選擇作為一起始事件，用於提供該使用者與一商家第三方應用程式113（例如，至少部分地在裝置100上執行之一原生應用程式，如可已由裝置100經由商業實體子系統400所存取者（例如，作為應用程式商店420之一經註冊商家線上資源））互動的能力。替代地或此外，可由裝置100直接自商家子系統200存取此一商家的資源658（例如，經由

伺服器210或終端機220)。回應於一商家應用程式圖示之此一選擇，一GUI可提供一互動式畫面，其中裝置100可令使用者能夠與應用程式113互動（例如，以細閱可自該商家購得的品項以進行購買，或判定要與該商家共用的某些健康資料或地點資料或其他）。替代地，步驟608可包括裝置100使用下列者自商家子系統200存取作為一商家Web資源的一商家的資源658（例如，經由商家伺服器210或至少部分受控於一商家實體之任何伺服器）：裝置100之網際網路應用程式（其亦可藉由一「網際網路」圖示（例如，圖3之GUI 180之特定畫面190之圖示184）來選擇）、或具有Web檢視之一混合式應用程式（用於提供該使用者與一商家的網頁或其他Web資源互動的能力，而非與一商家的第三方原生應用程式互動）。替代地，步驟608可包括在沒有主動使用者輸入的情況下對作為商家線上資源113的資源658之任何合適的自動存取（例如，裝置100可操作以回應於偵測任何合適的事件而自動與資源658互動，諸如一自主式家用電器裝置100偵測其正在一特定供應為低的情況下執行（例如，一洗衣機裝置100回應於偵測到低的洗衣清潔劑供應））。

【0057】 接下來，在步驟610，裝置100可接收來自所存取之商家資源的潛在交易資料660（例如，如關於在程序500之步驟502所描述）。例如，如圖1A中所展示，當裝置100正在與商家的資源113（例如，商家之第三方應用程式或網站或任何其他合適的線上資源（例如，資源658））互動時，潛在交易資料660可自商家子系統200（例如，自商家伺服器210）提供至裝置100。替代地或此外，可由裝置100經由裝置100本端之應用程式113本端地存取潛在交易資料660之至少一部分（例如，當應用程式113儲存於一記憶體組件中或正由裝置100之處理器102執行時），而非在步驟610自商家伺服器210主動發送資料至裝置100。例

如，當應用程式113可最初儲存在裝置100上時（例如，在步驟608，作為商家的資源658（例如，自應用程式商店420載入）），潛在交易資料660之至少一些可由最初儲存之應用程式113予以產生而無由商家子系統200提供至裝置100的任何額外資訊。潛在交易資料660可包括指示發生於裝置100之使用者與商家子系統200之一商家之間之一潛在金融交易的任何合適特性的任何合適資料，包括但不限於：(i)特定商家資訊，諸如一唯一商家識別符（例如，一收單銀行商家識別符及/或一商業實體商家識別符（例如，商家識別符167，如可在步驟610註冊者））及/或使用中之特定商家資源（例如，特定商家應用程式113）之識別；(ii)特定交易資訊，諸如用於交易之支付之一特定貨幣之識別（例如，日元、英鎊、美元等）、及/或交易之待支付之一貨幣之一特定總額之識別、及/或待購買或租借或以其他方式支付之特定產品或服務之識別、及/或待使用之一預設或初始運送地址之識別；(iii)指示商家可接受用於交易之一或多種類型付款方法的資訊（例如，可用於購買的付款卡清單（例如，MasterCard，而非Visa））；及/或(iv)一唯一之以商家為基礎之交易識別符（例如，任何合適的資料元素，諸如一3或4字元文數字串，其可由商家子系統200隨機或唯一地產生以供與正在進行中的交易相關聯）。此類潛在交易資料660可包括可為必要或至少用於完成金融交易的任何合適數目個及類型之資料欄位（含或不含相關聯之資料），諸如進行購買之客戶的連絡人資訊欄位（例如，電話號碼、電子郵件地址、郵寄地址），其中一些欄位可經填入且被包括作為此類潛在交易資料660之部分，及/或其中一些欄位可未經填入作為此類潛在交易資料660之部分，但可在程序600期間開放及等待填入。在本文中，步驟610之此類潛在交易資料660可稱為一PKDataRequest或一PKPaymentRequest（例如，用於金融交易）。替代地，如所提及，使用者

可不主動與裝置100互動，以在步驟610使與商家子系統200相關聯的潛在交易資料660可供裝置100使用。

【0058】 對於安全付款資料之通訊，潛在交易資料660可包括針對裝置100產生用於購買產品及/或服務之一付款符記的一商家資源的請求，且可封裝關於潛在交易的任何合適資訊，包括例如關於該商家的付款處理能力、支付總額、及貨幣代碼等資訊。潛在交易資料660亦可包括商家可支援的一或多個付款網路（例如，（一或多個）付款網路360）之一清單，使得裝置100可經組態以判定此類所列出一或多個付款網路之任何者是否具有一經授權付款認證在裝置100上或作為一用戶端的裝置100可使用的任何合適主機裝置上。在一些實施例中，一旦此類潛在交易資料660可由裝置100存取，如圖3A中所展示，例如，裝置100之一GUI可提供畫面190a，其中一商家的資源可使用交易資料660來展示與潛在交易相關聯的任何合適資訊給裝置100之使用者，諸如用資訊307a展示商家之名稱（例如，「商家A」）、用資訊307b展示產品之名稱（例如，「產品B」）、用資訊307c展示價格（例如，「價格C」）及/或用資訊307d展示初始運送資料（例如，「地址D」）。可由商家子系統200提供至裝置100之潛在交易資料660可指示此類資訊307a、307b、307c、及/或307d。裝置100之使用者可與裝置100及畫面190a互動以調整此類資訊之某些部分（例如，運送地址等），其會需要待由商家子系統200產生及共用的經更新之潛在交易資料（例如，在步驟610之另一例項）。亦如圖3A所展示及如下文更詳細描述，畫面190a亦可包括一安全支付提示309。潛在交易資料660之至少一部分可經由圖1A之通訊路徑15自商家子系統200提供至裝置100且可由裝置100之通訊組件106予以接收。通訊組件106可傳遞此潛在交易資料660至處理器102上（例如，用於顯示在畫面190a上作為在裝置

100上之一使用者介面之部分（例如，用於資訊307a至307d及309））及/或至安全元件145。例如，安全元件145可利用此類潛在交易資料660之至少一部分，用以安全地實現介於裝置100與商家子系統200之間之一金融交易。在一些實施例中，潛在交易資料660可稱為商家付款請求資料及/或一統一資源定位器(「URL」)或任何其他合適的參考字元字串及/或查詢字串。

【0059】 在程序600之步驟612，可起始一商家線上資源驗證工作階段。如關於在程序500之步驟504所提及，步驟612可回應於電子裝置100指示安全資料交易（例如，由步驟610之潛在交易資料660所識別的安全資料交易（例如，金融交易））應發生而發生。此指示可回應於裝置100之使用者選擇商家線上資源之一GUI元素（例如，選項按鈕）而發生，諸如圖3A之安全支付提示309，用以傳達該使用者想要進行由步驟610之商家線上資源之潛在交易資料660所識別的安全資料交易。替代地，此指示可基於任何合適需求被滿足而自動發生（例如，單純回應於步驟610之潛在交易資料660被傳達至裝置100）。例如，當此指示發生時，商家線上資源113（例如，用於Web資源之Web套件）可操作以發送一安全資料交易請求至卡管理應用程式103b（例如，用於付款安全資料交易之通行套件(pass kit)），且接著裝置100（例如，裝置100之卡管理應用程式103b或任何其他合適的應用程式）可操作以接收及處理此一安全資料交易請求，且作為回應，在步驟612，接著可操作以產生及傳達商家線上資源驗證工作階段起始資料662至商家子系統200。

【0060】 在步驟612，可由電子裝置100產生及/或傳達任何合適的資料至商家子系統200作為商家線上資源驗證工作階段起始資料662，用以起始用於待實行之一特定安全資料交易的一商家線上資源驗證工作階段（例如，由資料660

及/或圖3A之畫面190a所識別的金融交易)。例如，在步驟612，可由電子裝置100產生一驗證工作階段識別符並且傳達至商家子系統200來作為商家線上資源驗證工作階段起始資料662之至少一部分，其中此一驗證工作階段識別符可係可唯一識別目前正在起始之商家線上資源驗證工作階段的任何合適之文數字串或任何其他合適之識別符(例如，唯一識別對商家子系統200及/或對商業實體子系統400的此類工作階段至少達一定時期)。此外或替代地，在步驟612，一查問請求目標識別符(例如，一查問請求URL)可自裝置100傳達至商家子系統200作為商家線上資源驗證工作階段起始資料662之至少一部分，其中此一查問請求目標識別符可識別商家子系統200待與其通訊以驗證該商家之一實體(例如，識別商業實體子系統400之伺服器410之一URL，其待與商家子系統200合作，用以驗證用於待實行之特定安全資料交易的商家線上資源)。一裝置應用程式(例如，卡管理應用程式103b)可具有經程式化之此一查問請求目標識別符(作為任何合適的作業系統或應用程式更新之部分)，其可受控於商業實體子系統400，使得可由商業實體子系統400在任何合適的時間更新裝置100上之查問請求目標識別符。此外或替代地，此類商家線上資源驗證工作階段起始資料662可包括任何其他合適的資料，諸如：指示對商家之一請求以驗證其自身的任何合適資料；及/或在步驟608所存取且在步驟610被利用以用於接收潛在交易資料660的特定商家線上資源；指示裝置100的任何合適資料(例如，裝置識別符119)；及/或指示待實行之特定安全資料交易的任何合適資料(例如，來自步驟610之潛在交易資料660的任何合適資料，諸如特定商家資訊(例如，商家線上資源之一商家識別符167)、特定交易資訊(例如，用於該金融交易的貨幣及數額及付款類型)、及/或一唯一之以商家為基礎之交易識別符)。在步驟612，可依任何合

適方式由裝置100傳達任何合適的商家線上資源驗證工作階段起始資料662至商家子系統200（例如，可使用任何合適的通訊協定經由通訊路徑15，或使用任何合適的通訊協定經由介於終端機220與NFC組件120之間的一非接觸式之以接近性為基礎之通訊頻道，自裝置100之通訊組件106傳輸此類商家線上資源驗證工作階段起始資料662至商家子系統200之伺服器210）。

【0061】 在程序600之步驟614，回應於在步驟612商家子系統200接收來自裝置100的任何合適商家線上資源驗證工作階段起始資料662以用於起始商家線上資源113之一驗證工作階段，商家子系統200可操作以傳達任何合適的查問請求資料664至商業實體子系統400，用以驗證用於待實行之特定安全資料交易（例如，如在步驟610及/或步驟612所識別之金融付款交易）的商家線上資源。在步驟614自商家子系統200傳達至商業實體子系統400之查問請求資料664可包括用於嘗試向商業實體子系統400實證商家子系統200（例如，商家資源113）之有效性的任何合適資料，包括但不限於：與待驗證之商家線上資源相關聯的一商家識別符（例如，如在步驟606所註冊之至少一商家識別符167，其可係一商家線上Web資源之一網域）；一驗證工作階段識別符（例如，如在步驟504由電子裝置100所產生者，或在步驟506由商家子系統200所產生者）；及任何其他合適的資料（例如，識別裝置100的資料及/或識別待實行之特定安全資料交易的資料）。例如，查問請求資料664之一商家識別符可係與在步驟610所使用之商家線上資源（其起始目前商家線上資源驗證工作階段）相關聯的任何合適商家識別符167。當步驟612之商家線上資源驗證工作階段起始資料662包括一驗證工作階段識別符（例如，如由電子裝置100所產生者）時，接著在步驟614，可由商家子系統提供彼驗證工作階段識別符作為查問請求資料664之至少一部分。然而，當

步驟612之商家線上資源驗證工作階段起始資料662不包括一驗證工作階段識別符時，或當可由商家子系統200自動起始一商家線上資源驗證工作階段（例如，回應於傳達步驟610之潛在交易資料660）而非回應於任何步驟612之任何商家線上資源驗證工作階段起始資料662時，商家子系統200可操作以產生可唯一識別目前正在起始之商家線上資源驗證工作階段的此一驗證工作階段識別符，並接著在步驟614可操作以包括彼驗證工作階段識別符作為查問請求資料664之至少一部分。在一些實施例中，在步驟614，可提供可係待實行之安全資料交易（例如，如在步驟610及/或步驟612所識別之金融付款交易）特定的任何合適額外資訊作為查問請求資料664之至少一部分，包括但不限於指示下列各項之資訊：潛在交易資料之資訊307b之「產品B」、潛在交易資料之資訊307c之「價格C」、潛在交易資料之資訊307d之運送資料「地址D」、潛在交易資料之付款認證識別「認證X」資訊313、及/或與待實行之安全資料交易相關聯的任何其他合適資訊，其可適合與商業實體子系統400共用（例如，按照關於該資料之任意者之任何隱私權考量），諸如「來自最近三天的心跳率資訊」，而非實際心跳率資訊（如果待實行之安全資料交易係一健康資料交易）。可在程序600之任何合適部分期間使用可係安全資料交易特定之此類資訊（在本文中可稱為潛在交易識別資訊），用於提供（一或多個）任何額外安全性層至目前資料交易程序，及/或用於提供任何額外安全性（例如，詐騙偵測）服務以供未來資料交易。可由商家子系統200使用商家子系統200可使用且與查問請求之商家識別符相關聯的一商家金鑰（例如，如在步驟606與商家識別符167一起註冊之一商家金鑰157（例如，用於待驗證之商家線上資源113））來簽署查問請求資料664（例如，在一HTTP標頭中或以其他方式），使得可由商業實體子系統400有效地利用查問請

求資料664以用於驗證商家線上資源113。在步驟614可依任何合適方式由商家子系統200傳達任何合適的查問請求資料664至商業實體子系統400（例如，可使用任何合適的通訊協定經由通訊路徑85，自商家子系統200之伺服器210傳輸此類查問請求資料664至商業實體子系統400之伺服器410）。查問請求資料664之此類通訊可基於一查問請求目標識別符（例如，一查問請求URL）而恰當地定址至商業實體子系統400，該查問請求目標識別符可在步驟612自裝置100傳達至商家子系統200作為商家線上資源驗證工作階段起始資料662之至少一部分。替代地或此外，查問請求資料664之此類通訊可基於一查問請求目標識別符（例如，一查問請求URL）而恰當地定址至商業實體子系統400，該查問請求目標識別符可供商家子系統200取用並與步驟610之潛在交易資料660相關聯（例如，識別商業實體子系統400之一識別符可與任何代碼（例如，用於Web資源之java腳本代碼）相關聯或與可供商家子系統200使用以在一商家線上資源中提供任何合適的「安全交易」提示（例如，圖3A之安全支付提示309））之其他者相關聯。

【0062】 在程序600之步驟616，回應於在步驟614商業實體子系統400接收來自商家子系統200的任何合適查問請求資料664，商業實體子系統400可操作以驗證由查問請求之商家識別符167所識別的商家線上資源113。例如，在步驟616，商業實體子系統400可操作以嘗試確認在商業實體子系統400處由所接收之查問請求資料664之一商家識別符167所識別的商家線上資源113係一有效且經註冊之商家線上資源，其可藉由下列方式而確認：在表格430中識別彼商家識別符167（例如，以判定商家識別符167已經向商業實體子系統400註冊（例如，在步驟606），且判定此類註冊仍然有效（例如，彼商業實體子系統400並未自表格430移除商家識別符167或並未在表格430中將商家識別符167旗標為可疑或以

其他方式不再受信任，及/或判定與商家識別符167相關聯之一憑證（例如，在表格430中）仍然有效））；及/或藉由識別與彼商家識別符167相關聯或由彼商家識別符167所識別的一網域，並藉由重新驗證可寄存在彼網域上之一檔案來重新驗證彼網域（例如，如關於步驟501及/或步驟606所描述），其中替代地或此外，可由商業實體子系統400在任何合適的時間（例如，定期地或以其他方式）實行此類重新驗證，且非必然在步驟616回應於接收資料664而實行此類重新驗證。此外或替代地，在步驟616，商業實體子系統400可操作以嘗試驗證所接收之查問請求資料664之簽章，其可藉由以下來完成：識別一商家金鑰157（商家金鑰157可與所接收之查問請求資料664之一商家識別符167相關聯（在商業實體子系統400處的表格430中或以其他方式在商業實體子系統400處（例如，可已在步驟606之註冊期間建立之一關聯性））），並接著利用彼經識別之商家金鑰157以驗證所接收之查問請求資料664之簽章（例如，以確認商業實體子系統400可存取之商家金鑰157係連同商家子系統200可存取之商家金鑰157之一經配對金鑰組之一者，在步驟614傳達查問請求資料664至商業實體子系統400之前，可已由商家子系統200使用商家金鑰157來簽署查問請求資料664（例如，該等金鑰之一者可係一公開金鑰且另一者可係經配對之金鑰組的一私密金鑰）），其可確保由商家子系統200持有可需要在在程序600之（一或多個）較後部分中由商家子系統200使用的商家金鑰157（例如，在步驟636，在此步驟商家子系統200可解密先前由商業實體子系統400所加密的資料）。在由商業實體子系統400對所接收之查問請求資料664進行任何合適的驗證之後（例如，在驗證所接收之查問請求資料664之一商家識別符及/或簽章之後），在步驟616，商業實體子系統400亦可操作以產生任何合適的查問資料並對照所接收之查問請求資料664的任何

合適識別符資料來儲存彼查問資料。例如，在對所接收之查問請求資料664進行任何合適的驗證之後，商業實體子系統400可操作以產生任何合適的查問資料（例如，經由熵的任何合適隨機資料），並接著依商業實體子系統400可存取之任何合適的資料結構（例如，在表格430中或以其他方式）對照查問請求資料664之驗證工作階段識別符及查問請求資料664之一商家識別符之一或兩者來儲存彼查問資料。介於此類查問資料與驗證工作階段之識別符資料（例如，查問請求資料664之驗證工作階段識別符及/或商家識別符）之間之此一儲存連結或關聯性可稍後由商業實體子系統400使用以進一步驗證驗證工作階段之商家線上資源（例如，在步驟622）及/或進一步保護待實行之安全資料交易的安全（例如，在步驟630）。另外，在一些實施例中，查問請求資料664之潛在交易識別資訊之任何者或全部亦可對照查問資料及識別符資料予以儲存或以其他方式與查問資料及識別符資料相關聯。

【0063】 在程序600之步驟618，回應於在步驟616商業實體子系統400驗證所接收之查問請求資料664及對照驗證工作階段之識別符資料來產生查問資料，商業實體子系統400可操作以使用任何合適的金鑰或以其他方式加密步驟616之查問資料並接著可操作以傳達彼經加密查問資料連同任何其他合適的資料作為至商家子系統200的查問資料668。例如，商業實體子系統400可使用供商業實體子系統400存取且與所接收之查問請求資料664之一商家識別符167相關聯（例如，在商業實體子系統400處的表格430中或以其他方式在商業實體子系統400處（例如，可已在步驟606之註冊期間建立之一關聯性））的任何合適商家金鑰157來加密該查問資料，其中在步驟618由商業實體子系統400用於加密該查問資料的此一商家金鑰157可相同於或不同於在步驟616可已由商業實體子系

統400用來驗證查問請求資料664的商家金鑰157。除此類經加密查問資料外，可包括任何其他合適的資料作為在步驟618由商業實體子系統400傳達至商家子系統200的查問資料668之一部分，包括但不限於：由商業實體子系統400用來加密該查問資料的商家金鑰157之一雜湊（例如，表格430之一公開商家金鑰157之一雜湊版本，其可由商家子系統200接收並使用以識別恰當的商家金鑰157（例如，用於解密該查問資料的商家子系統200之私密金鑰157），可提供雜湊版本以輔助可具有多個經註冊商家線上資源及/或多個商家金鑰的商家）；查問請求資料664之驗證工作階段識別符；查問請求資料664之商家識別符；在商業實體子系統400處（例如，在表格430中）與由商業實體子系統400用來加密該查問資料之商家金鑰157相關聯之商家識別符；及/或類似物。在步驟618可依任何合適方式由商業實體子系統400傳達任何合適的查問資料668至商家子系統200（例如，可使用任何合適的通訊協定經由通訊路徑85，自商業實體子系統400之伺服器410傳輸此類查問資料668至商家子系統200之伺服器210）。

【0064】 在程序600之步驟620，回應於在步驟618商家子系統200接收此類查問資料668，商家子系統200可操作以處理所接收之查問資料668並接著產生及傳達查問回應資料670至商業實體子系統400，以供在目前驗證工作階段期間進一步驗證商家子系統200。例如，在步驟620，商家子系統200可操作以使用商家子系統200可使用之任何合適的商家金鑰157（例如，如在步驟606與一商家識別符167一起註冊之一商家金鑰157（例如，用於在目前驗證工作階段期間被驗證的商家線上資源113））來解密所接收之查問資料668之經加密查問資料。可由商家子系統200使用下列者來識別在步驟620由商家子系統200用來解密經加密查問資料之此一商家金鑰157：查問資料668之任何雜湊金鑰資訊；及/或查問資

料668之任何商家識別符；及/或藉由使用查問請求資料664之任何商家識別符（例如，如可與資料664及資料668之一共同工作階段識別符相關聯）。在步驟620由商家子系統200用來解密經加密查問資料之此一商家金鑰157可相同於或不同於在步驟614可已由商家子系統200用來簽署查問請求資料664的商家金鑰157。在解密所接收之查問資料668之經加密查問資料之後，在步驟620，商家子系統200亦可操作以自商家子系統200產生並傳達查問回應資料670至商業實體子系統400，其中查問回應資料670可包括如由商家子系統200所解密之查問資料（以供進一步嘗試向商業實體子系統400實證商家子系統200（例如，商家資源113）之有效性）連同任何其他合適的資料，包括但不限於：目前驗證工作階段之驗證工作階段識別符（例如，查問請求資料664之有效工作階段識別符，及/或所接收之查問資料668之有效工作階段識別符）；與藉由目前驗證工作階段所驗證之商家線上資源相關聯的一商家識別符（例如，查問請求資料664之商家識別符、在商業實體子系統400處（例如，在表格430中）與由商業實體子系統400用於加密該查問資料之商家金鑰157相關聯之商家識別符，及/或類似物）；用於待實行之安全資料交易的任何或所有合適潛在交易識別資訊，其可已包括或不包括於步驟614之查問請求資料664中；及/或類似物。可由商家子系統200使用商家子系統200可使用的一商家金鑰（例如，如在步驟606與商家識別符167一起註冊之一商家金鑰157（例如，用於目前正被驗證之商家線上資源113））來簽署查問回應資料670（例如，在一HTTP標頭中或以其他方式），使得可由商業實體子系統400有效地利用查問回應資料670，以供進一步驗證商家線上資源113。在步驟620可由商家子系統200用來簽署查問回應資料670之此一商家金鑰157可相同於或不同於在步驟614可已由商家子系統200用來簽署查問請求資料664的商家金

鑰157。此外或替代地，在步驟620可由商家子系統200用來簽署查問回應資料670之此一商家金鑰157可相同於或不同於在步驟620可已由商家子系統200用來解密經加密查問資料的商家金鑰157。在步驟620可依任何合適方式由商家子系統200傳達任何合適的查問回應資料670至商業實體子系統400（例如，可使用任何合適的通訊協定經由通訊路徑85，自商家子系統200之伺服器210傳輸此類查問回應資料670至商業實體子系統400之伺服器410）。

【0065】 在程序600之步驟622，回應於在步驟620商業實體子系統400接收來自商家子系統200的任何合適查問回應資料670，商業實體子系統400可操作以進一步驗證商家子系統200及在目前驗證工作階段中其所關注之商家線上資源。例如，在步驟622，商業實體子系統400可操作以嘗試驗證所接收之查問回應資料670之簽章，其可藉由以下來完成：識別一商家金鑰157（在表格430中，商家金鑰157可與所接收之查問回應資料670之一驗證工作階段識別符相關聯，或在商業實體子系統400處的表格430中或以其他方式在商業實體子系統400處，商家金鑰157可與所接收之查問回應資料670之一商家識別符167相關聯（例如，可已在步驟606之註冊期間建立之一關聯性）），並接著利用彼經識別之商家金鑰157以驗證所接收之查問回應資料670之簽章（例如，以確認商業實體子系統400可存取之商家金鑰157係連同商家子系統200可存取之商家金鑰157之一經配對金鑰組之一者，在步驟620傳達查問回應資料670至商業實體子系統400之前，可已由商家子系統200使用商家金鑰157來簽署查問回應資料670（例如，該等金鑰之一者可係一公開金鑰且另一者可係經配對之金鑰組的一私密金鑰）。在步驟622可由商業實體子系統400用來驗證查問回應資料670之簽章之此一商家金鑰157可相同於或不同於在步驟616可已由商業實體子系統400用來驗證查

問請求資料664之簽章的商家金鑰157，及/或在步驟622可由商業實體子系統400用來驗證查問回應資料670之簽章之此一商家金鑰157可相同於或不同於在步驟618可已由商業實體子系統400用來加密該查問資料的商家金鑰157。此外或替代地，在步驟622，商業實體子系統400可操作以嘗試確認所接收之查問回應資料670之經解密查問資料係有效查問資料。例如，商業實體子系統400可操作以嘗試確認所接收之查問回應資料670之經解密查問資料係目前經儲存或以其他方式可供商業實體子系統400獨立地存取（例如，在表格430中）。在一些實施例中，商業實體子系統400可藉由識別同一查問資料目前係經儲存在表格430中來判定所接收之查問回應資料670之經解密查問資料之有效性。替代地，商業實體子系統400可藉由識別與目前對照所接收之查問回應資料670的任何合適識別符資料（例如，對照一驗證工作階段識別符或一商家識別符）經儲存在表格430中（如在步驟616可已儲存在表格430中）相同的查問資料來判定所接收之查問回應資料670之經解密查問資料之有效性。在一些實施例中，介於該查問資料與驗證工作階段識別符及商家識別符之一或兩者之間的此一所儲存連結（或此類所儲存查問資料本身）可在自動清除該連結或所儲存資料之前由商業實體子系統400維持達僅一段有限時間量，使得商家子系統200會受限於必須在一定持續時間內接收查問資料668並接著發送適當的查問回應資料670至商業實體子系統400，用以驗證用於特定驗證工作階段的商家線上資源（例如，商業實體子系統400可操作以在一定時期之後移除在商業實體子系統400處之介於該查問資料與驗證工作階段識別符及/或商家識別符之間的此一關聯性（例如，在建立該連結或查問資料之後不超過10分鐘即自表格430移除該連結或查問資料），其可增加交易安全性）。因此，可使用在商業實體子系統400處之介於商家金鑰與商家識

別符之間之一或多個關聯性（例如，如在步驟608所註冊者）來完成在步驟614至622之任何者或全部之用於待實行之特定安全資料交易（例如，如在步驟610及/或步驟612所識別）的商家線上資源之驗證。

【0066】 在由商業實體子系統400對所接收之查問回應資料670進行任何合適的驗證之後（例如，在驗證所接收之查問回應資料670之一簽章之後及/或在驗證所接收之查問回應資料670之經解密查問資料之後），在步驟622，商業實體子系統400亦可操作以產生任何合適的驗證資料並對照所接收之查問請求資料664的任何合適識別符資料及/或所接收之查問回應資料670的任何合適識別符資料來儲存彼驗證資料。例如，在對所接收之查問請求資料664及/或所接收之查問回應資料670進行任何合適的驗證之後，商業實體子系統400可操作以產生任何合適的驗證資料（例如，經由熵的任何合適隨機資料及/或任何合適的密碼編譯臨時值(cryptographic nonce)），並接著依商業實體子系統400可存取之任何合適的資料結構（例如，在表格430中或以其他方式）對照查問請求資料664及查問回應資料670之任何一或兩者的驗證工作階段識別符及商家識別符之一或兩者來儲存彼驗證資料。介於此類驗證資料與驗證工作階段之識別符資料（例如，查問請求資料664之驗證工作階段識別符及/或一商家識別符及/或查問回應資料670之驗證工作階段識別符及/或一商家識別符）之間之此一所儲存連結或關聯性可稍後由商業實體子系統400使用以進一步保護待實行之安全資料交易的安全（例如，在步驟630）。另外，在一些實施例中，查問請求資料664之潛在交易識別資訊之任何者或全部及/或查問回應資料670之任何者或全部亦可對照該驗證資料及識別符資料予以儲存或以其他方式與該驗證資料及識別符資料相關聯。

【0067】 回應於藉由確認在商業實體子系統400處（例如，在表格430中）所接收之查問回應資料670之經解密查問資料係與識別符資訊（例如，驗證工作階段識別符及/或商家識別符資訊）連結而驗證該查問資料，在步驟622，商業實體子系統400可操作以：耗用彼連結（例如，移除在商業實體子系統400處之介於查問資料與驗證工作階段識別符及/或商家識別符之間的此一關聯性（例如，自表格430移除該連結））；產生驗證資料（例如，任何合適的隨機資料（例如，一密碼編譯臨時值（例如，經由熵的任何合適隨機資料）））；並接著在商業實體子系統400處對照任何合適的識別符資訊（例如，查問請求之驗證工作階段識別符及/或查問回應之驗證工作階段識別符，及/或對照該查問請求之一商家識別符及/或該查問回應之一商家識別符）來儲存該驗證資料或以其他方式使該驗證資料與任何合適的識別符資訊相關聯（例如，依任何合適的資料結構，諸如表格430或以其他方式）。替代地，回應於藉由確認在商業實體子系統400處（例如，在表格430中）所接收之查問回應資料670之經解密查問資料係與識別符資訊（例如，驗證工作階段識別符及/或商家識別符資訊）連結而驗證該查問資料，在步驟622，商業實體子系統400可操作以在商業實體子系統400處維持彼連結或以其他方式更新彼連結（例如，在商業實體子系統400處（例如，在表格430中）重設可與彼連結相關聯之任何計時器，或新增任何額外潛在交易識別資訊以供與該連結相關聯），並接著利用彼連結之查問資料（例如，如在步驟616所產生）作為在其他狀況下可在步驟622產生之驗證資料。在一些實施例中，查問資料及驗證資料可關於大小或任何其他合適的一或多個屬性而不同，此係因為在步驟618至622使用之查問資料可不同於在步驟624至630使用之驗證資料。

【0068】 在程序600之步驟624，回應於在步驟622商業實體子系統400驗證所接收之查問請求資料664及/或驗證所接收之查問回應資料670並產生或以其他方式對照驗證工作階段之識別符資料來定義驗證資料，商業實體子系統400可操作以產生及傳達任何合適的驗證回應資料674。例如，驗證回應資料674可包括步驟622之驗證資料連同任何其他合適的資料，包括（但不限於）：該驗證工作階段識別符（例如，查問請求資料664之驗證工作階段識別符及/或查問回應資料670之驗證工作階段識別符及/或如可依其他方式與該驗證工作階段相關聯者）；一商家識別符（例如，查問請求資料664之一商家識別符及/或查問回應資料670之一商家識別符；及/或如可依其他方式在商業實體子系統400處（例如，在表格430中）與在驗證工作階段期間正被驗證之商家線上資源相關聯者）；及/或類似物。在一些實施例中，如圖6中所展示，此類驗證回應資料674可自商業實體子系統400直接傳達至電子裝置100（例如，使用任何合適的通訊協定經由通訊路徑65），其中識別電子裝置100的資料（例如，裝置識別符119）可與驗證工作階段起始資料662及/或查問請求資料664及/或查問回應資料670或其他相關聯或以其他方式被包括在驗證工作階段起始資料662及/或查問請求資料664及/或查問回應資料670或其他中，使得商業實體子系統400可傳達驗證回應資料674至恰當的電子裝置100。替代地，在一些實施例中，可經由商家子系統200自商業實體子系統400傳達驗證回應資料674至電子裝置100，藉此商家子系統200可接收來自商業實體子系統400之驗證回應資料674（例如，使用任何合適的通訊協定經由通訊路徑85）並接著傳遞驗證回應資料674之至少一部分至電子裝置100上（例如，使用任何合適的通訊協定經由通訊路徑15或作為一非接觸式之以接近性為基礎之通訊），使得商業實體子系統400可不必在步驟624直接與裝置100的

建置一安全通訊頻道。可由商業實體子系統400使用與商業實體子系統400相關聯的一存取金鑰（例如，存取金鑰155a、存取金鑰155b、CRS 151k、及/或安全元件145之ISD金鑰156k，或一裝置應用程式（例如，卡管理應用程式103b）可已知的任何金鑰）來簽署驗證回應資料674（例如，在一HTTP標頭中或以其他方式），電子裝置100亦可存取該存取金鑰，使得裝置100可在接收到該經簽署驗證資料後驗證簽章，以確認商業實體子系統400產生驗證回應資料674而非不受電子裝置100信任的另一實體子系統產生驗證回應資料，及/或使得該經簽署驗證資料不會被不具有此一存取金鑰之存取權的一實體利用（例如，商家子系統200，其可用以自商業實體子系統400傳遞該經簽署驗證資料至裝置100）。

【0069】 如所提及，裝置100之使用者可選擇商家線上資源之一GUI元素（例如，選項按鈕），諸如圖3A之安全支付提示309，用於傳達使用者想要進行由步驟610之商家線上資源之潛在交易資料660所識別的安全資料交易。如圖3B中所展示，裝置100及/或商家線上資源113可經組態以提供畫面190b，該提供畫面190b係單獨回應於接收對圖3A之畫面190a之安全支付提示309的選擇或除此之外亦回應於在步驟624裝置100接收驗證回應資料674（其可指示無驗證工作階段失敗），及/或回應於裝置100驗證介於在步驟612可已由電子裝置100所產生作為驗證工作階段起始資料662之一部分的一工作階段識別符與可提供作為所接收之驗證回應資料674之一部分的一工作階段識別符之間之一致性（例如，在步驟625），其可使裝置100能夠確認回應資料674與作為在程序600之相同驗證工作階段之部分的驗證工作階段起始資料662相關聯（例如，裝置100可與商家子系統200之一商家識別符組合地儲存驗證工作階段起始資料662之一工作階段識別符（例如，在步驟612），並可接著在允許程序600之其餘者之前，可比較所

儲存資料組合與驗證回應資料674之工作階段識別符及商家識別符（例如，在步驟625）以確保一恰當的匹配，其中裝置100可操作以確保在步驟612由電子裝置100所產生之任何工作階段識別符在步驟612起始之工作階段期間係待驗證之特定商家子系統或商家線上資源所獨有的）。在任何情況中，如圖3B中所展示，畫面190b可提示使用者依一或多種方式與裝置100互動以選取可供裝置100使用之一特定付款來源或認證以進行購買。例如，如所展示，畫面190b可包括一付款來源選擇提示311，其可令使用者能夠選擇可供裝置100使用的潛在之多個付款來源之一者。付款來源選擇提示311可僅包括含與由該商家所支援之付款網路相關聯的認證之付款來源（例如，如可藉由潛在交易資料660所判定，如上文所提及），或可展示裝置100可使用之所有付款來源，但可使得只有與可接受付款之網路相關聯者能夠由使用者選擇。付款來源選擇提示311可包括任何合適的付款來源（例如：使用「認證X」之一付款方法，如可由提示311之付款選項識別符311a所指示；使用「認證Y」之一付款方法，如可由提示311之付款選項識別符311b所指示等），包括但不限於：裝置100之一安全元件原生的任何合適付款認證及/或裝置100可存取之任何可用付款來源的任何合適非原生付款認證（例如，可作為裝置100（作為一用戶端裝置）之一主機裝置的另一裝置）。僅舉一特定實例，如圖3C中所展示，裝置100可經組態以回應於接收使用者對圖3B之付款來源選擇提示311的識別符311a之「認證X」的選擇而提供畫面190c。圖3C之畫面190c可用認證識別符資訊313識別經選擇之認證或自動經識別之預設認證，並且可提示裝置100之使用者依一或多種方式與裝置100互動以鑑認該使用者及其利用該所選擇認證之意圖。此可包括提示使用者（例如，用圖3C之一鑑認提示315）經由個人識別號碼（「PIN」）輸入項鍵入使用者鑑認或經由與一生物

特徵感測器之使用者互動，以存取裝置100之安全元件，且因此存取待用於購買之認證。可基於任何合適的事件（諸如回應於潛在交易資料660被傳達、及/或回應於畫面190a被呈現、及/或回應於使用者選擇圖3A之畫面190a之安全支付提示309、及/或回應於使用者選擇圖3B之付款來源選擇提示311之一特定認證、及/或回應於呈現圖3C之畫面190c），而起始一商家線上資源驗證工作階段（例如，在步驟612及/或步驟614）。可在任何合適的時刻呈現圖3B之付款來源選擇提示311，諸如回應於使用者選擇圖3A之畫面190a之安全支付提示309而不論任何驗證工作階段之狀態（其可發生在步驟612至624（例如，在步驟612至614之任何者之前或在期間或之後）），及/或不僅回應於使用者選擇圖3A之畫面190a之安全支付提示309而且亦回應於在步驟624接收驗證回應資料674（其可指示無驗證工作階段失敗）。可在任何合適的時刻呈現圖3C之鑑認提示315，諸如回應於接收使用者對付款來源選擇提示311之一付款識別符的選擇而不論任何驗證工作階段之狀態（其可發生在步驟612至624（例如，在步驟612至614之任何者之前或在期間或之後）），及/或不僅回應於接收使用者對付款來源選擇提示311之一付款識別符的選擇而且亦回應於在步驟624接收驗證回應資料674（其可指示無驗證工作階段失敗），及/或可在步驟624接收驗證回應資料674之前呈現畫面190c，但是圖3C之鑑認提示315可未經啟用以供使用，直到在步驟624接收驗證回應資料674之後。

【0070】 如果裝置100之使用者願意且能夠回應於在步驟610所接收之潛在交易資料660（例如，付款請求資料）而選擇或確認一特定付款認證以用在為潛在交易提供資金，且在步驟624已由電子裝置100接收驗證回應資料674（例如，可指示步驟612至622之商家線上資源驗證工作階段成功的資料），則程序

600可進行至步驟625，在此步驟，程序600可包括：在已識別任何工作階段識別符一致性之後（例如上文所提及，於步驟625），接收裝置100之使用者對於利用一特定認證來實行針對基於潛在交易資料660之一特定商家、產品、價格及運送目的地的潛在交易之意圖及鑑認（例如，透過使用者選擇圖3C之鑑認提示315）。存取SSD 154b可充分利用裝置100之小程序153b以判定在允許使用其他SSD 154（例如，認證SSD 154a）被用於在一商務認證資料通訊中啟用其認證資訊之前是否已發生此類鑑認。僅舉步驟625之一實例，存取SSD 154b之小程序153b可經組態以判定裝置100之使用者之意圖及本端鑑認（例如，經由一或多個輸入組件110，諸如圖3之一生物特徵輸入組件110i，如可由與裝置100之任何應用程式（例如，裝置100之商家資源113及/或卡管理應用程式103b）互動的使用者所使用），且回應於此一判定，可經組態以啟用另一特定SSD，用於進行一付款交易（例如，運用認證SSD 154a之一認證）。在一些實施例中，在此一判定之後，但是在此類啟用之前，裝置100之一GUI可經組態以提供另一畫面（圖中未展示），該畫面可提示裝置100之使用者（例如，以相似於圖3C之提示315的一提示）依一或多種方式與裝置100互動以最終使用經選擇且經鑑認之認證起始付款。在步驟625，裝置100之使用者可提供意圖及鑑認以供使用裝置100原生的一特定付款認證來為由步驟610之潛在交易資料660所識別的一潛在交易提供資金（例如，針對畫面190a至190c之「商家A」及「產品B」及「價格C」及「運送D」）。然而，替代地，程序600可使裝置100之使用者能夠在可於步驟625提供任何意圖及鑑認之前調整潛在交易之一或多個特性（例如，可更新在畫面190a及/或190b上的運送地址資訊或以其他方式透過商家子系統200與裝置100之間傳達之額外經更新之潛在交易資料660）。

【0071】 接下來，一旦回應於接收潛在交易資料660之特定付款請求資料而在步驟625已接收針對一特定付款認證的意圖及鑑認，在程序600之步驟626至628可包括裝置100產生、加密、及傳輸裝置交易資料678以供商業實體子系統400使用（例如，如關於在程序500之步驟512及514所描述）。一旦已選擇、鑑認、及/或啟用在裝置100之安全元件145上的認證SSD 154a之認證以供在一金融交易中使用（例如，在步驟625），裝置100之安全元件145（例如，NFC組件120之處理器模組142）可產生及加密彼經選擇之認證之某些認證資料以供商業實體子系統400使用。例如，在步驟626，認證SSD 154a之裝置付款認證資料675（例如，SSD 154a之付款卡資料（例如，如可與所選擇之「認證X」相關聯）），諸如符記資料及密碼編譯資料，可經產生及/或至少部分地用認證金鑰155a'予以加密，作為裝置付款認證資料676以包括至少符記資料及密碼編譯資料，使得此類經加密裝置付款認證資料676可僅由可存取彼認證金鑰155a'之一實體予以解密（例如，金融機構子系統350）以用於存取裝置付款認證資料675。此類付款認證資料675可包括可操作以安全地實證裝置100之特定安全元件認證之恰當擁有權的任何合適資料（例如，SSD 154a之認證），包括但不限於：(i) 符記資料（例如，SSD 154a之認證資訊161a之DPAN、DPAN到期日期、及/或CVV）；及(ii)密碼編譯資料（例如，一編譯密碼，其可由安全元件145使用SSD 154a與金融機構子系統350之一共用祕密（例如，金鑰155a'）予以產生，及可供裝置100使用且亦經使得可供金融機構子系統350使用以用於使用該共用祕密來獨立產生該密碼編譯資料的任何其他合適資訊（例如，符記資料之一些或全部、識別裝置100之資訊、識別步驟610之潛在交易資料660之一些或全部之資訊，諸如費用及/或貨幣、任何合適的計數器值、臨時值（例如，驗證回應資料674之驗證資料之一臨

時值)等))。因此,付款認證資料675可包括用彼認證進行付款所必須的所有資料,例如,諸如一主要帳戶號碼(例如,一實際F-PAN或一虛擬D-PAN)、一卡安全性碼(例如,一卡驗證碼(「CVV」))、到期日期、與該認證相關聯之名稱、相關聯之密碼編譯資料(例如,使用介於安全元件145與金融機構子系統350之間之一共用祕密所產生的一編譯密碼,及任何其他合適的資訊),及/或類似物。在一些實施例中,一旦在步驟626已經用認證金鑰155a'加密認證SSD 154a之彼付款認證資料675之一些或全部作為經加密付款認證資料676,旋即在步驟627,可藉由存取資訊(例如,藉由SSD 154a之存取金鑰155a、存取SSD 154b之存取金鑰155b、ISD金鑰156k、及/或CRS 151k及/或由CASD 158k所簽署)將以下加密作為安全裝置資料677:彼經加密付款認證資料676(單獨地或連同適用之潛在交易資料660之至少一第一部分(若非全部))(例如,潛在交易資料660之一部分或全部,其可包括商家之識別、價格總額之識別、貨幣及/或運送及/或產品之識別、及/或唯一之以商家為基礎之交易識別符、及/或唯一之以使用者裝置為基礎之交易識別符,及/或類似物)、驗證回應資料674之一些或全部、及/或任何其他合適的資訊(例如,識別裝置100本身之任何資訊(例如,裝置識別符119)、任何特定以裝置為基礎之交易識別符,及/或類似物)。例如,裝置100之安全元件145(例如,NFC組件120之處理器模組142)可使用存取資訊以不僅將來自資料660及/或資料674的一商家之識別(例如,商家之識別或其正用於購買之資源,諸如應用程式113)加密至安全裝置資料677中,而且亦將來自資料660的購買總額及/或貨幣代碼之識別以及SSD 154a之經加密付款認證資料675(例如,經加密付款認證資料676)加密至安全裝置資料677中。在一些實施例中,可產生認證SSD 154a之付款認證資料675(例如,SSD 154a之付款卡資料,

諸如符記資料及密碼編譯資料），但是在運用一商業實體金鑰或存取金鑰予以加密（例如，在步驟627，作為資料677）之前，未經用一認證金鑰予以加密（例如，在步驟626，作為資料676），且替代地，可運用一商業實體金鑰或存取金鑰來加密此類付款認證資料675（例如，在步驟627，作為資料677），藉此在此等實施例中，任何未來對資料676之參考亦可係對未經用任何認證金鑰加密之資料675之參考。在一些實施例中，此一商業實體金鑰或存取金鑰可係與商業實體子系統400之一方案相關聯的一商業實體公開金鑰且其之商業實體子系統400可存取一相關聯之商業實體私密金鑰。商業實體子系統400可提供此一商業實體公開金鑰至金融機構子系統350，且接著金融機構子系統350可與裝置100共用彼商業實體公開金鑰（例如，當佈建認證資料於裝置100上時（例如，在程序600之步驟654））。

【0072】 接下來，在步驟628，安全裝置資料677連同任何額外資訊（諸如潛在交易資料660或潛在交易識別資訊之至少一些（例如，商家之識別、價格總額之識別、貨幣之識別、一唯一之以商家為基礎之交易識別符、產品/服務之識別，及/或類似物））、及/或驗證回應資料674之至少一部分或全部、及/或任何其他合適的資訊（例如，識別裝置100本身之任何資訊、一唯一之以裝置為基礎之交易識別符，及/或類似物）可一起作為裝置交易資料678自裝置100傳輸至商業實體子系統400（例如，如關於在程序500之步驟514所描述）。因此，裝置交易資料678之至少部分（例如，含或不含驗證回應資料674之安全裝置資料677）可僅由可存取用於加密的彼存取資訊（例如，存取金鑰155a、存取金鑰155b、ISD金鑰156k、CRS 151k、及/或CASD 158k）之一實體（例如，商業實體子系統400）予以解密，該加密產生裝置交易資料678之安全裝置資料677。此類裝置交易資

料678可在步驟626至628予以產生及接著在步驟628傳輸至商業實體子系統400

（例如，經由通訊組件106及通訊路徑65，自安全元件145或以其他方式傳輸）。步驟626、627及628可確保自裝置100之安全元件145所產生及傳輸的任何認證資料（作為裝置交易資料678之部分）已經先依不可被裝置100之另一部分解密（例如，被處理器102解密）之方式予以加密。即，可用可未暴露於裝置100之在其安全元件外的任何部分或不可由該任何部分存取的一認證金鑰155a'來加密裝置交易資料678之付款認證資料675作為經加密裝置付款認證資料676。另外，可用可未暴露於裝置100之在其安全元件外的任何部分或不可由該任何部分存取的一存取金鑰（例如，存取金鑰155a、155b、156k、151k、及/或158k（例如，本文中稱為「存取資訊」））來加密交易資料678之此類裝置付款認證資料676作為安全裝置資料677。

【0073】 接下來，在步驟629，程序600可包括商業實體子系統400接收及解密裝置交易資料678之至少一部分。例如，商業實體子系統400可接收裝置交易資料678並可接著使用如可在商業實體子系統400處可用的存取資訊（例如，155a、155b、156k、151k、及/或158k）來解密裝置交易資料678之安全裝置資料677。此可使商業實體子系統400能夠判定一未經加密之商家之識別（例如，自經解密安全裝置資料677），同時亦維持付款認證資料675處於一經加密狀態（例如，作為經加密裝置付款認證資料676），此係因為商業實體子系統400可不具有認證金鑰155a'之存取權，在步驟626，此類裝置付款認證資料675可已由裝置100之安全元件145予以加密作為經加密裝置付款認證資料676。此外或替代地，可由可已連同安全裝置資料677一起包括於裝置交易資料678中的額外資料來識別商家。裝置交易資料678可包括識別裝置100或至少其安全元件之資訊，使得

當由商業實體子系統400接收裝置交易資料678時，商業實體子系統400可知道要在步驟629使用哪一個存取資訊（例如，存取資訊155a、155b、156k、151k、及/或158k之哪一者）。例如，商業實體子系統400可存取多個存取金鑰155a/155b及/或多個ISD金鑰156k，該等金鑰之各者可係一特定裝置100特定之金鑰或一特定安全元件特定之金鑰。

【0074】 另外，在步驟629之前或之後，在接收在步驟628所傳達的裝置交易資料678之後，程序600之步驟629可包括商業實體子系統400驗證可已被裝置100包括在裝置交易資料678中的驗證回應資料674之驗證資料。例如，回應於接收此類裝置交易資料678，在步驟630（例如，相似於在程序500之步驟516），商業實體子系統400可操作以識別來自彼裝置交易資料678之驗證回應資料674之至少一部分或全部並確認彼所接收之裝置交易資料678之驗證資料目前係經儲存在商業實體子系統400處，或更具體而言，在一些實施例中，確認彼所接收之裝置交易資料678之驗證資料目前係在商業實體子系統400處對照所接收之裝置交易資料678之一驗證工作階段識別符及/或對照所接收之裝置交易資料678之一商家識別符經儲存（例如，在表格430中）。在一些實施例中，介於該驗證資料與驗證工作階段識別符及商家識別符之一或兩者之間的此一儲存連結可在自動清除該連結之前維持達僅一段有限時間量，使得電子裝置100會受限於必須在一定持續時間內在步驟624接收驗證回應資料674並接著在步驟628發送裝置交易資料678至商業實體子系統400，用於實現由商業實體子系統400保護裝置交易資料678之安全裝置資料677的安全，以用於運用經驗證商家線上資源實行特定安全資料交易（例如，商業實體子系統400可操作以在一定時期之後移除在商業實體子系統400處之介於驗證資料與驗證工作階段識別符及/或商家識別符之

間的此一關聯性（例如，在建立該連結之後不超過10分鐘即自表格430移除該連結），其可增加交易安全性）。此外或替代地，在步驟622，亦可使介於該驗證資料與驗證工作階段識別符及商家識別符之一或兩者之間的一所儲存連結與任何合適的特定潛在交易識別資訊（在步驟614及620之一或多者期間，可由商家子系統200使潛在交易識別資訊可供商業實體子系統400使用）相關聯（例如，作為查問請求資料664之一部分及/或查問回應資料670之一部分），諸如待共用於裝置100與商家子系統200之間的一特定類型安全資料之識別（例如，用於金融交易的貨幣及數額及付款類型），及亦可由電子裝置100使相似特定潛在交易識別資訊可供商業實體子系統400使用，作為步驟628之裝置交易資料678之一部分，使得步驟630亦可包括商業實體子系統400確認目前對照在步驟614及/或步驟620所接收之驗證資料所儲存的特定潛在交易識別資訊（例如，如在步驟616及/或步驟622儲存在表格430中者）至少相似於在步驟628所接收之特定潛在交易識別資訊。例如，如果在步驟622對照與指示5美元金融交易之潛在交易相關聯的特定潛在交易識別資訊來儲存特定驗證資料，但是接著在步驟628由商業實體子系統400連同彼特定驗證資料一起接收的特定潛在交易識別資訊指示2,000美元之金融交易，則歸因於介於\$5與\$2,000之間之差異量值，商業實體子系統400可操作以不驗證裝置交易資料678之驗證資料。因此，即使在步驟628所接收的裝置交易資料678之驗證資料及驗證工作階段識別符及/或商家識別符可在商業實體子系統400處確認為經主動連結（例如，在表格430中），如果裝置交易資料678未滿足可與彼連結相關聯之其他資料，則該驗證資料仍會不被驗證（例如，如果在步驟616至622期間所識別的安全資料交易之任何合適特性與步驟628之裝置交易資料678中所識別之任何合適特性相差達任何合適的量（例如，一特定

資料類型之百分比變異(percentage variance)，諸如相差超過一金融交易貨幣值之10%，或相差超過健康資料之時間框架之10%）；或一特定類型不同（例如，所識別資料之類型不同，諸如所識別資料之兩個例項之間之健康資料類型不同（例如，心跳率資料對行走哩程數資料，或生物特徵資料對付款資料等）；及/或所識別資料之兩個例項之間之正用於交易的貨幣類型不同（例如，美元對日元等）；及/或用於遞送貨物之付款交易之運送地址之地點））。資料比較可係介於針對一特定交易實際接收之資料與針對一特定商家之彙總過去資料之間，以偵測與預期範數(norm)偏差的某些例項（例如，由一商家測偵生活史資料(biodata)之第一交易直到那時僅已交易付款認證資料等），其中可由商家使用潛在交易識別資訊以驗證或偵測詐騙且非必然關於該使用者裝置（例如，在某些例項中，可追蹤商家（而非裝置）的彙總資料，以尊重終端使用者之隱私權問題）。

【0075】 接下來，在步驟631，程序600可包括商業實體子系統400識別可已藉由付款請求資料610及/或驗證工作階段（且因此，藉由裝置交易資料678）所識別的商家相關聯之一商家金鑰（例如，商家金鑰157），並接著使用彼商家金鑰來重新加密裝置交易資料678之至少一部分。即，在步驟629使用合適的存取資訊來解密裝置交易資料678之至少一部分之後（例如，在解密安全裝置資料677以具現化(realize)裝置付款認證資料676及可已在安全裝置資料677中加密之任何其他資訊（例如，驗證回應資料674）之後），接著在步驟631，商業實體子系統400可用一適當的商家金鑰（其可與在裝置交易資料678中所識別之商家資訊相關聯，或可與在表格430中識別為與在步驟630經驗證之經連結驗證資料相關聯者）來重新加密裝置交易資料678之至少一部分（例如，裝置付款認證資料676之符記資料及/或密碼編譯資料）。例如，可藉由比較使用裝置交易資料678

所識別之商業實體商家資訊與在圖1A之表格430中的資料來判定此一商家金鑰（例如，商家金鑰157）。運用此經判定之適當的商家金鑰，商業實體子系統400可用彼商家金鑰（例如，商家金鑰157）來重新加密裝置交易資料678之至少一部分（例如，裝置付款認證資料676之符記資料及/或密碼編譯資料）作為經加密商家認證資料681。例如，經加密商家認證資料681可至少包括來自裝置交易資料678之經加密裝置付款認證資料676以及任何合適的交易資料，諸如來自或基於裝置交易資料678及/或潛在交易資料660的購買總額資料或其他合適的交易資料。來自裝置交易資料678之商家識別資訊可不需要被包括在經加密商家認證資料681中，此係因為可已使用彼商家識別來判定在步驟631可用來加密經加密商家認證資料681的商家金鑰。可由商業實體子系統400來簽署經加密商家認證資料681使得當由商家子系統200接收時，商家子系統200可確立商業實體子系統400為此類經加密商家認證資料681之建立者並且/或者可使商家子系統200能夠確保此類經加密商家認證資料681在經簽署之後未經修改。在步驟631可產生此類經加密商家認證資料681，並且接著在步驟632傳輸此類經加密商家認證資料681連同任何其他合適的資料至裝置100，作為經保護安全之交易資料682（例如，經由圖1A之路徑65自商業實體子系統400之伺服器410傳輸至裝置100之通訊組件106）。

【0076】 步驟631及632可操作以確保自商業實體子系統400經傳輸作為圖1A之經保護安全之交易資料682之部分的認證資料（例如，經加密商家認證資料681之符記資料及/或密碼編譯資料）可經加密使得裝置100除安全元件145外無一部分可解密該認證資料。即，可用可未暴露於裝置100之任何部分（在一些實施例中，包括安全元件145）或以其他方式不可由該任何部分存取的一商家金鑰（例

如，商家金鑰157）來加密經保護安全之交易資料682之認證資料（例如，經加密商家認證資料681之符記資料及/或密碼編譯資料）。另外，可用可未暴露於裝置100之安全元件145之外之任何部分或以其他方式不可由該任何部分存取的一認證金鑰155a'來加密經保護安全之交易資料682之認證資料（例如，經加密商家認證資料681之符記資料及/或密碼編譯資料）（例如，在步驟626）。

【0077】 接著，在步驟634，經保護安全之交易資料682可轉遞至商家子系統200上作為經保護安全之交易資料684（例如，經由通訊路徑15或作為一非接觸式之以接近性為基礎之通訊5）。替代地，商家認證資料681可自商業實體子系統400傳達至商家子系統200，而無需經由裝置100予以傳達（圖中未展示）。可透過裝置100及/或商業實體子系統400載送潛在交易資料660之一者、一些或所有部分至經保護安全之交易資料682及/或至經保護安全之交易資料684，使得在程序600期間可由實體之各者來識別潛在交易之某些識別符，包括但不限於：(i) 特定商家資訊，諸如商家之唯一商家識別符（即，「商家A」），及/或使用中之特定商家資源之識別（例如，特定商家應用程式113'）；(ii) 特定交易資訊，諸如用以支付交易之一特定貨幣之識別（例如，日元、英鎊、美元等），及/或用於交易之待支付之一貨幣之一特定總額之識別（即，「價格C」），及/或待購買或租借或以其他方式支付之特定產品或服務之識別（即，「產品B」），及/或待使用之一預設或初始運送地址之識別（即，「運送D」）；(iii) 指示商家可接受用於交易之一或多種類型付款方法的資訊（例如，可用於購買的付款卡清單（例如，MasterCard，而非Visa））或由裝置100所選擇（即，「認證X」）；(iv) 一唯一之以商家為基礎之交易識別符（例如，任何合適的資料元素，諸如一3或4字元文數字串，其可由商家子系統200隨機或唯一地產生以供與正在進行中

的交易相關聯)；(v)一唯一之以使用者裝置為基礎之交易識別符(例如，任何合適的資料元素，諸如一3或4字元文數字串，其可由裝置100隨機或唯一地產生以供與正在進行中的交易相關聯)；(vi)一唯一商家線上資源驗證工作階段識別符)，及/或類似物。

【0078】 一旦由商家子系統200接收包括付款認證資料675/676的商家認證資料681(例如，作為經保護安全之交易資料684，在步驟634)，程序600亦可包括步驟636，在此步驟，商家子系統200可經組態以產生並傳輸付款資料686至收單銀行子系統300(例如，經由圖1A之介於商家子系統200與收單銀行子系統300之間之通訊路徑25)，其中資料686可包括付款資訊及一授權請求，其可指示裝置100之經保護安全之裝置付款認證資料及針對產品或服務的商家購買價格(例如，如可被包括在經保護安全之交易資料684中或以其他方式與經保護安全之交易資料684相關聯，或如可以其他方式與如由商家子系統200已知之交易相關聯(例如，藉由潛在交易資料660(例如，基於一唯一交易識別符)))。例如，在步驟636，商家子系統200可充分利用其之已知之商家金鑰157以至少部分解密經保護安全之交易資料684之商家認證資料681，使得付款資料686可包括經用其認證金鑰155a'(而非用不可供金融機構子系統350使用之一金鑰)加密的認證SSD 154a之經保護安全之付款認證資料(例如，資料676)。

【0079】 如果在步驟636傳輸付款資料686至收單銀行子系統300，則接著，在步驟638，收單銀行子系統300可轉遞來自付款資料686之授權請求資訊至金融機構子系統350而作為授權請求資料688(例如，經由圖1A之介於收單銀行子系統300與金融機構子系統350之間之通訊路徑35)。接下來，在步驟640，當金融機構子系統350之發行銀行子系統370接收一授權請求(例如，在步驟640，

直接接收來自收單銀行子系統300之授權請求，作為資料688，或間接經由付款網路子系統360接收授權請求，作為資料405）、付款資訊（例如，如由裝置100之安全元件145藉由認證金鑰155a'所加密的裝置100之付款認證資料675（例如，資料676））及購買總額時，授權請求、付款資訊及購買總額之各者：可被包括在授權請求資料688中，以及被包括在資料682、684及/或686中；可經解密（例如，在金融機構子系統350處使用認證金鑰155a'）及經分析以判定與該商務認證相關聯的帳戶是否具有足以履行該購買總額的信用。如果不存在足夠資金，發行銀行子系統370可藉由傳輸一否定授權回應至收單銀行子系統300而拒絕所請求之交易。然而，如果存在足夠資金，發行銀行子系統370可藉由傳輸一肯定授權回應至收單銀行子系統300而核准所請求之交易，而可完成金融交易。在程序600之步驟640，可由使用者金融子系統350提供任一類型授權回應至收單銀行子系統300作為授權回應交易狀態資料690（例如，經由通訊路徑35自發行銀行子系統370直接提供至收單銀行子系統300，或基於可經由圖1A之通訊路徑45自發行銀行子系統370提供至付款網路子系統360的授權回應資料415，自付款網路子系統360提供至收單銀行子系統300）。接下來，回應於在步驟640接收授權回應交易狀態資料690，在步驟642，程序600亦可包括收單銀行子系統300或任何其他合適的子系統與商家子系統200共用此類授權回應交易狀態資料作為授權回應交易狀態資料692，其接著在步驟644可與裝置100共用（例如，使用商家資源或以其他方式）作為經確認之交易狀態資料694。此類經確認之交易狀態資料可經組態以提供任何合適的確認資料至裝置100，諸如圖3D之畫面190d之確認資料317。如果交易成功，在步驟644，經確認之交易狀態資料可操作以在裝置100關閉交易。此外或替代地，如果交易不成功，則經確認之交易狀態資料可操作或

可不操作以關閉交易（例如，如果無可用的有效資金或如果裝置識別為詐騙，則關閉交易，但若是判定一非有效運送地址則保持開放並允許更新）。任何非交易終止交易狀態資料可允許付款程序繼續，直到由一應用程式取消該程序、由一使用者取消該程序、或程序完成。

【0080】 因此，商家子系統200可經組態以依任何合適的方式處理經保護安全之交易資料684或商家認證資料681之任何其他載體(carrier)。例如，為了自商家認證資料681獲得裝置付款認證資料，商家子系統200可驗證所接收之商家認證資料681之一簽章屬性係有效且彼商業實體子系統400係彼簽章之簽署者。商家子系統200可使用任何合適的技術以判定可已由商業實體子系統400使用哪一商家金鑰（例如，哪一商家公開金鑰157）來建構商家認證資料681。接著，商家子系統200可擷取相對應之商家私密金鑰（例如，在商家子系統200處之一商家私密金鑰157）並使用彼經擷取之金鑰以解封裝及/或解密經加密商家認證資料681，以復原經加密資料676。接著此類資料676可提供至適當的付款網路360，其可充分利用金融機構子系統350之適當的認證金鑰155a'，以解封裝及/或解密經加密裝置付款認證資料676，以復原裝置付款認證資料675（例如，復原裝置付款認證資料675之符記資料及/或密碼編譯資料，用以驗證裝置付款認證資料675（例如，以基於所接收之裝置付款認證資料675之符記資料來獨立產生密碼編譯資料、比較所產生之密碼編譯資料與所接收之裝置付款認證資料675之密碼編譯資料、並基於該比較而驗證或拒絕交易））。

【0081】 應理解，圖6之程序600中展示之步驟僅係闡釋性，且可修改或省略現有步驟、可新增額外步驟、並且可改變某些步驟之順序。雖然未展示，經保護安全之交易資料可自商業實體子系統400直接傳達至商家子系統200（例

如，在步驟632及634，經由通訊路徑85而非經由裝置100），或直接傳達至金融機構子系統350（例如，在步驟632至638，經由通訊路徑55而非經由裝置100及/或非經由商家子系統200及/或非經由收單銀行300）。此外或替代地，雖然未展示，經保護安全之交易資料可自裝置100直接傳達至金融機構子系統350（例如，未經由商家子系統200）。應理解，如果程序600之任何驗證步驟失敗，此類失敗可傳達至一或多個合適的實體。例如，如果在步驟616驗證查問請求資料664失敗，及/或如果在步驟622驗證查問回應資料670失敗，及/或如果在步驟630驗證裝置交易資料678之驗證回應資料674之驗證資料失敗，則可由商業實體子系統400與商家子系統200及/或電子裝置100共用此類失敗，使得裝置100可取消與商家子系統200的潛在交易且有可能自裝置100移除商家線上資源。在步驟625裝置100之使用者可選取某安全資料以用於一安全資料交易之後（例如，一特定付款認證之某付款認證資料），在程序600之其餘步驟可對彼使用者透通地發生（例如，步驟626至644可發生而無需任何與裝置100的進一步使用者互動且對裝置100之使用者而言如同瞬時）。在步驟625之後，程序600對裝置100之使用者而言看來像是安全裝置資料係自動且瞬間地發送至商家子系統200並且可對裝置100確認交易狀態（例如，藉由商家子系統200及/或商業實體子系統400）。此外或替代地，一商家線上資源之驗證可對裝置100透通地發生（例如，步驟614至624（若未亦含步驟612）可發生而無需任何與裝置100的使用者互動且步驟610之後對裝置100之使用者而言如同瞬時）。替代地，在一些實施例中，程序600可對裝置100之使用者完全透通地發生（例如，其中裝置100可經組態以自動判定何時宜發生一安全裝置交易及自動接收驗證回應資料，及/或自動發送裝置交易資料，及/或自動接收及/或發送經保護安全之交易資料以用於一安全裝置交

易，而無需與裝置100的任何主動使用者互動，同時商家線上資源仍然可在一驗證工作階段經起始並經實行期間被驗證以用於彼特定安全裝置交易）。例如，如所提及，裝置100可經組態以判定一特定產品宜購買並與一或多個商家互動，以自彼特定產品的至少一特定商家獲得相關聯之潛在交易資料（例如，裝置100可係一家用電器，其可經組態以判定必須購買的電器用產品（例如，偵測洗衣機需要更多洗衣清潔劑，或偵測由使用者預設要在特定日期買更多清潔劑的行事曆事件），並可自動識別提供彼產品之最佳優惠的一特定商家，且可自動與彼商家互動以自彼商家獲得用於購買彼產品的潛在交易資料），全部皆自動化且無需由裝置100之使用者進行任何主動互動。其後，裝置100及/或特定商家可操作以自動起始步驟612之驗證工作階段。

【0082】 在一些實施例中，在步驟616已驗證一查問請求之後可略過步驟618至622，且替代地，在步驟616可產生及儲存驗證資料，而非查問資料。因此，在一些實施例中，步驟614及616可足以驗證用於一特定驗證工作階段之一商家線上資源。在一些實施例中，在步驟616所產生之查問資料可不同於在步驟622所產生之驗證資料。例如，查問資料可足夠長（例如，合適長度的資料字串，諸如10或更多個字元）以提供足夠的隨機性，以用於用查問資料668實現對商家子系統200的顯著健全查問，然而驗證資料可比查問資料更短（例如，驗證資料可係長度比查問資料之長度更短的資料字串，諸如6個字元）以提供足夠的隨機性，以用於用驗證回應資料674實現工作階段驗證之證明及/或滿足任何合適的標準（例如，滿足Europay MasterCard Visa(「EMV」)標準的資料長度需求）。替代地，查問資料及驗證資料可相同且在步驟616及步驟622兩者重複使用。在步驟624，可基於商家子系統200之查問之成功驗證而非僅僅基於介於裝置100與商

家之間將發生付款交易的判定，由商業實體子系統400產生及提供驗證回應資料674之驗證資料（例如，臨時值）至裝置100。當裝置100可經由在裝置100上之一原生應用程式（其可係商家特定之應用程式）來與商家子系統200通訊時，則可由此一應用程式提供商家應用程式113。然而，當裝置100可經由一網際網路瀏覽器應用程式或混合式應用程式（其可係或可不係商家特定之應用程式，但是，其可經指向至由一商家管理之網站（例如，在受控於商家之伺服器上））來與商家子系統200通訊時，則商家應用程式113可係一版面配置引擎(layout engine)軟體組件（例如，WebKit），版面配置引擎軟體組件可轉遞通訊至商家之網站上（例如，經由通訊組件106）。例如，裝置100之此一應用程式113可係用於待提供至商家子系統200之任何裝置交易資料的一管道。

【0083】 現在可關於不同商家組態來描述程序600之某部分之替代實施例。商家子系統200可經配備以運用變化之控制程度來處置程序600之安全交易。在一第一商家組態中，其中商家子系統200可保持控制整個程序，商家子系統200可操作以不僅處置商家線上資源之驗證（例如，在步驟614及616及/或在步驟618及620，商家子系統200本身可與商業實體子系統400通訊以驗證該商家線上資源），而且亦可處置由商業實體子系統400所加密之安全資料之解密（例如，在步驟636，商家子系統200可充分利用一商家金鑰157以至少部分解密經保護安全之交易資料684之商家認證資料681）。在此一第一商家組態中，商家子系統200可作為自己的付款服務提供者（「PSP」）且可係與商業實體子系統400通訊（以在程序600中註冊及驗證一線上資源）的唯一子系統，如對高交易量之大型商家而言可係典型的（例如，Amazon.com）。替代地，在一第二商家組態中，商家子系統200可交出付款解密責任給任何合適的商家-合作夥伴子系統，諸如一PSP

子系統310，其在圖1A及圖6可展示為收單銀行300之一部分。在此一第二商家組態中，商家子系統200可操作以處置商家線上資源之驗證（例如，在步驟614及/或在步驟618及620，商家子系統200本身可與商業實體子系統400通訊以驗證該商家線上資源），但是PSP子系統310可操作以處置由商業實體子系統400所加密之安全資料之解密（例如，在步驟638，PSP子系統310可充分利用一商家金鑰157以至少部分解密付款資料686之商家認證資料681）。在此一第二商家組態中，商家子系統200可使用一相異第三方後端PSP用於其付款解密，使得商家子系統200及PSP子系統310兩者可與商業實體子系統400通訊以用於在程序600中註冊一線上資源，如對可利用一付款服務提供者之較小型商家而言可係典型的（例如，一收單銀行（例如，Chase Paymentech）或較小型PSP（例如，Stripe，Braintree，First Data等），其可操作以與多個收單銀行、卡及付款網路通訊，及/或代表商家子系統200管理與外部網路及銀行帳戶的此類技術連接及關係，從而使商家子系統200較不依賴於金融機構）。此一第二商家組態之PSP子系統310可對裝置100之使用者隱藏，使用者可僅介接商家子系統200之線上資源（例如，在圖3A至圖3D之畫面190a至190d）。替代地，在一第三商家組態中，商家子系統200可交出線上資源驗證責任及付款解密責任給任何合適的商家-合作夥伴子系統，諸如一PSP子系統310。在此一第三商家組態中，PSP子系統310可操作以不僅處置商家線上資源之驗證（例如，在步驟614，PSP子系統310本身可與商業實體子系統400進行查問請求資料664之傳達以驗證該商家線上資源（例如，回應於PSP子系統310接收來自商家子系統200之工作階段起始資料662）），而且亦可處置由商業實體子系統400所加密之安全資料之解密（例如，在步驟638，PSP子系統310可充分利用一商家金鑰157以至少部分解密付款資料686之商家認證資料681）。在

此一第三商家組態中，商家子系統200可使用一相異第三方前端PSP用於驗證及付款解密，使得商家子系統200及PSP子系統310兩者可與商業實體子系統400通訊以在程序600中註冊及驗證一線上資源，如對「長尾型(long tail)」商家而言可係典型的，長尾型商家會依賴一第三方付款服務提供者來代表其等實行整個檢查及付款程序（例如，可由Stripe Inc.之PSP提供Stripe Checkout）。一相異第三方前端PSP子系統310可針對桌上型電腦、平板電腦及行動裝置提供一可內嵌的付款形式（例如，如可寄存於PSP子系統310之一伺服器上，諸如內嵌至商家子系統200之一商家資源中之PSP子系統310之一Java腳本），桌上型電腦、平板電腦及行動裝置可在商家子系統200之Web資源內運作以供客戶經由PSP子系統310之彼付款形式進行付款，而無需將客戶（例如，裝置100之使用者）重新導向離開商家子系統200之Web資源以完成交易或客戶可被重新導向離開商家子系統200之Web資源至PSP子系統310之Web資源以完成程序（例如，PayPal.com）。此一第三商家組態之PSP子系統310可操作以管理及操作一PSP線上資源，PSP線上資源可相似於商家線上資源，但是可由本身不具備處理付款能力的商家線上資源利用PSP線上資源，例如，其中網站商家線上資源113可將與彼網站商家線上資源113介接的裝置100之使用者導向至網站PSP線上資源113之介面（其可內嵌在網站商家線上資源113之任何部分內），或可自網站商家線上資源113之任何合適部分將使用者重新導向（例如，可由網站PSP線上資源（而非由網站商家線上資源）提供圖3A至圖3D之畫面190a至190d之一或多者之任何合適部分）。因此，取決於系統1之組態及商家子系統200之能力，商家子系統200及PSP子系統310（例如，收單方子系統300）可一起提供系統1之單一健全處理子系統299或可用作為系統1之相異實體。

【0084】 向商業實體子系統400註冊一商家線上資源可包括商家子系統200單獨地或與PSP子系統310組合(例如,取決於採用該三種商家組態之哪一者)向商業實體子系統400登記,以操作地向商業實體子系統400驗證線上資源並且亦解密如由商業實體子系統400所加密之認證資料。例如,步驟606可不僅包括關於與一線上資源相關聯之一或多個商家識別符167而於商業實體子系統400與商家子系統200或PSP子系統310之間共用的商家金鑰157,其中在商業實體子系統400處可使用此類金鑰157來加密資料(例如,在步驟631)並在商家子系統200或PSP子系統310處使用此類金鑰157來解密彼資料(例如,在步驟636或步驟638),而且亦可包括關於與該線上資源相關聯之一或多個商家識別符167而於商業實體子系統400與商家子系統200或PSP子系統310之間共用之一憑證177,其中憑證177可於驗證該線上資源(例如,在步驟614及步驟616)。

【0085】 僅舉一實例,在步驟606,用於一線上資源(例如,一網站商家線上資源113)之共用金鑰之一第一憑證簽署請求(「CSR」)可經產生並傳達至商業實體子系統400。用於共用金鑰之此第一CSR可包括:與該線上資源相關聯之至少一商家識別符167,諸如該線上資源之一完全合格網域名稱(「FQDN」)(例如,可指定其確切地點之一Web網域,包括根及子網域(例如,DNS主機名稱));及/或任何其他合適的商家識別符,其可連結至該線上資源之該網域;及/或任何合適的商家-合作夥伴之任何其他合適的識別符,其可與該線上資源相關聯(例如,一PSP識別符(如果商家子系統200可使用一PSP以解密由商業實體子系統400所加密之認證資料))。在步驟606,商業實體子系統400可回應用於共用金鑰之該第一CSR,而促進一金鑰對(例如,公開及私密商家金鑰157)作為於商業實體子系統400與商家子系統200或PSP子系統310之間之一共用祕密

（其可與該第一CSR之商家識別符167之一或多者相關聯）。例如，該金鑰對之一第一商家金鑰157可對照用於該商家線上資源之該第一CSR之商家識別符之一者、一些或各者而儲存在商業實體子系統400之表格430中，或以其他方式使該金鑰對之一第一商家金鑰157與用於該商家線上資源之該第一CSR之商家識別符之一者、一些或各者相關聯，而該金鑰對之一第二商家金鑰157可對照用於該商家線上資源之該第一CSR之商家識別符之一者、一些或各者而儲存在商家子系統200及/或在一PSP子系統310處，或以其他方式使該金鑰對之一第二商家金鑰157與用於該商家線上資源之該第一CSR之商家識別符之一者、一些或各者相關聯。一或多個商家識別符可與一特定商家線上資源113相關聯，諸如一第一商家識別符167唯一地與該特定商家線上資源113相關聯（例如，一FQDB（若為一Web資源商家線上資源113）），及/或一第二商家識別符167與一特定商家子系統200之各商家線上資源113相關聯。此外或替代地，一或多個商家金鑰可與一特定商家識別符相關聯或與一特定商家線上資源113相關聯。在步驟606之一或多個例項，所有此類商家金鑰與商家識別符之關聯性可由商業實體子系統400予以儲存，或以其他方式可供商業實體子系統400存取（例如，在一或多個表格430中）。在第一商家組態中，商家子系統200可產生並提供此一第一CSR至商業實體子系統400，且商家子系統200可對照用於該線上資源之該第一CSR之商家識別符167之一者、一些或各者來儲存商家金鑰157，或以其他方式使商家金鑰157與用於該線上資源之該第一CSR之商家識別符167之一者、一些或各者相關聯。在第二商家組態及第三商家組態中，PSP子系統310或商家子系統200可產生此一第一CSR，而PSP子系統310或商家子系統200之任一者可提供此一第一CSR至商業實體子系統400，且PSP子系統310可接收來自商業實體子系統400（例如，直接或

經由商家子系統200)之商家金鑰157，並對照用於該線上資源之該第一CSR之商家識別符167之一者、一些或各者來儲存商家金鑰157，或以其他方式使商家金鑰157與用於該線上資源之該第一CSR之商家識別符167之一者、一些或各者相關聯。

【0086】 此外，在步驟606，用於該線上資源之一憑證之一第二CSR（例如，一網站商家線上資源113）可經產生並傳達至商業實體子系統400。用於一憑證之此第二CSR可包括：與該線上資源相關聯之至少一商家識別符167，諸如該第一CSR之至少一商家識別符167或其他（例如，線上資源之FQDN或任何其他合適的商家識別符，其可連結至該線上資源之該網域），及/或任何合適的商家-合作夥伴之任何其他合適的識別符，其可與該線上資源相關聯（例如，一PSP識別符（如果商家子系統200可使用一PSP子系統以驗證該線上資源））。在步驟606，商業實體子系統400可回應於用於一憑證之該第二CSR，而促進憑證177被產生且於商業實體子系統400與商家子系統200或PSP子系統310之間共用，其中憑證177可包括該第二CSR之商家識別符167之一者、一些或全部，且可使用用於該商家線上資源之該第一CSR之一商家金鑰（例如，如可由第二CSR之商家識別符之一或多者所識別）來產生（例如，由商業實體子系統400）憑證177。例如，用於該第二CSR之線上資源之憑證177可對照用於該線上資源之該第二CSR之商家識別符之一者、一些或各者來儲存在商業實體子系統400之表格430中，或以其他方式使憑證177與用於該線上資源之該第二CSR之商家識別符之一者、一些或各者相關聯，而憑證177亦可對照用於該線上資源之該第二CSR之商家識別符之一者、一些或各者來儲存於商家子系統200處及/或儲存在其一PSP子系統310處，或以其他方式使憑證177與用於該線上資源之該第二CSR之商家識別符之

一者、一些或各者相關聯。憑證177可係任何合適的數位憑證，諸如一傳輸層安全性(「TLS」)憑證或一安全通訊端層(「SSL」)憑證。在第一商家組態及第二商家組態兩者中，商家子系統200可產生並提供此一第二CSR至商業實體子系統400，且商家子系統200可對照用於該線上資源之該第二CSR之商家識別符167之一者、一些或各者來儲存憑證177，或以其他方式使憑證177與該線上資源之該第二CSR之商家識別符167之一者、一些或各者相關聯。在第三商家組態中，PSP子系統310及/或商家子系統200可產生此一第二CSR且可提供此一第二CSR至商業實體子系統400，且PSP子系統310可對照用於該線上資源之該第二CSR之商家識別符167之一者、一些或各者來儲存憑證177，或以其他方式使憑證177與用於該線上資源之該第二CSR之商家識別符167之一者、一些或各者相關聯，其中用於提供憑證177給PSP子系統310之此程序可完成而無關於商家子系統200且可在商家子系統200與PSP子系統310形成一合作關係之前完成(例如，商家子系統200與PSP子系統310形成一合作關係用於提供一前端PSP模型之前，PSP子系統310可係商業實體子系統400之一受信任PSP且具備憑證177，其中經由PSP子系統310及PSP子系統310之一網域發生一付款)。商家子系統200可提供一PSP所提供之網域至商業實體子系統400，並向商業實體子系統400請求確認彼PSP子系統310係受信任且具有彼網域之一憑證177。

【0087】 此外，在步驟606，在處置該第一CSR及該第二CSR之任一者或兩者之前、期間或之後，可已向商業實體子系統400驗證或以其他方式實證由商家子系統200或由商家-合作夥伴PSP子系統310擁有權該網站線上資源之一網域(例如，FQDN)(例如，如關於步驟501所描述)。當註冊一線上資源時，用於金鑰之該第一CSR、用於憑證之該第二CSR及該網域驗證中之任何一者可發生

在用於金鑰之該第一CSR、用於憑證之該第二CSR及該網域驗證中之任何其他者之前或之後。然而，在一些實施例中，在處理用於憑證之一第二CSR之前驗證一網域可實現更容易且/或更有效率之註冊程序。在第一商家組態及第二商家組態兩者中，商家子系統200可共用向商業實體子系統400登記之一網站商家線上資源之FQDN，商業實體子系統400可提供任何合適的檔案（例如，諸如一JSON檔案）至商家子系統200，商家子系統200可簽署彼檔案（例如，運用共用之商家金鑰157）並在FQDN上寄存彼檔案，且接著商業實體子系統400可自該FQDN存取彼經簽署檔案並移除該檔案之簽署（例如，運用共用之商家金鑰157）以確認所存取之檔案匹配與商家子系統200共用之該檔案，且任何相關聯之臨限值已符合（例如，持續時間等）。在第三商家組態中，PSP子系統310可與商業實體子系統400共用經登記之一網站線上資源之FQDN（例如，PSP之一網站線上資源），商業實體子系統400可提供任何合適的檔案（例如，諸如一JSON檔案）至PSP子系統310，PSP子系統310可簽署彼檔案（例如，運用共用之商家金鑰157）並在FQDN上寄存彼檔案，且接著商業實體子系統400可自該FQDN存取彼經簽署檔案並移除該檔案之簽署（例如，運用共用之商家金鑰157）以確認所存取之檔案匹配與PSP子系統310共用之該檔案，且任何相關聯之臨限值已符合（例如，持續時間等）。在第三商家組態中，商家子系統200可操作以傳達指示介於商家子系統200與PSP子系統310之間之合作關係的資料至商業實體子系統400，使得商業實體子系統400可操作以向商家子系統200確認PSP子系統310之有效性並儲存介於商家子系統200之一商家識別符167與PSP子系統310之FQDN及/或憑證177之間之一關聯性（例如，在表格430中），以供在程序600之其他部分期間的任何合適使用。在一些實施例中，針對第二商家組態及第三商家組態，提供至PSP

子系統310之（一或多個）商家金鑰157可由PSP子系統310全域使用，用以解密關於任何合作夥伴商家子系統200之資料。替代地，針對第二商家組態及第三商家組態，提供至PSP子系統310之（一或多個）商家金鑰157可特定於一特定合作夥伴商家子系統200，藉此商家子系統200可與商業實體子系統400通訊（例如，運用用於金鑰之該第一CSR），且接著可使PSP子系統310能夠接收彼商家子系統200特定之此類（一或多個）商家金鑰157（例如，直接來自商業實體子系統400或來自商家子系統200），其中在商業實體子系統400處（例如，在表格430中）及/或在PSP子系統310處，此類（一或多個）商家金鑰157可與商家子系統200之任何合適的商家識別符167一起儲存或以其他方式使此類（一或多個）商家金鑰157與商家子系統200之任何合適的商家識別符167相關聯。此可在商業實體子系統400不再信任一特定商家子系統時能夠在商業實體子系統400處使一商家特定商家金鑰157無效化，同時仍然使得能夠關於其他商家子系統使用PSP子系統310之其他商家特定金鑰。在一些實施例中，可提供一或多個API，用於實現PSP子系統310直接介接商業實體子系統400，用於允許PSP子系統310與商業實體子系統400共用任何商家金鑰157及/或憑證177（其可特定於PSP子系統310之一特定合作夥伴商家子系統200），而無需要求商家子系統200直接涉及彼程序（例如，使得PSP子系統310可向商業實體子系統400上架(onboard)一商家，作為彼商家之一代理(proxy)）。憑證177亦可對於PSP子系統310係全域的或係特定於一特定合作夥伴商家子系統200。

【0088】 因此，步驟606及/或步驟501可不僅包括已由商業實體子系統400驗證一線上資源之一網域，而且亦可包括在商業實體子系統400處及在商家子系統200處及/或在商家-合作夥伴PSP子系統310處對照一商家金鑰157及一憑證177

兩者來儲存與該線上資源之彼網域相關聯或相同之一商家識別符167，用於在商業實體子系統400處登記該線上資源。因此，在商業實體子系統400處及在商家子系統200處及/或在PSP子系統310處，可對照一商家金鑰157及一憑證177來儲存一線上資源之一已驗證FQDN及/或任何其他合適的商家識別符167（例如，在程序600之步驟606及/或在程序500之步驟501），用於不僅實現在一驗證工作階段期間驗證線上資源之FQDN（例如，在程序600之步驟614及616及/或在程序500之步驟506），而且亦用於實現由商業實體子系統400加密安全資料（例如，在程序600之步驟631及/或在程序500之步驟518），及由商家子系統200或PSP子系統310來對應地解密彼經加密安全資料（例如，在程序600之步驟636或步驟638及/或在程序500之步驟522之後）。例如，在第一商家組態及第二商家組態兩者中，回應於在步驟612商家子系統200接收來自裝置100的任何合適商家線上資源驗證工作階段起始資料662以用於起始一商家線上資源113之一驗證工作階段（其中此類驗證工作階段起始資料662可包括該線上資源之一識別符，例如，由裝置100存取的商家線上資源之FQDN），在步驟614商家子系統200可操作以傳達任何合適的查問請求資料664（包括在步驟606由商家子系統200所接收並對照驗證工作階段起始資料662之彼FQDN儲存之憑證177）至商業實體子系統400，用以驗證用於待實行之特定安全資料交易的商家線上資源（例如，如在步驟610及/或步驟612所識別之金融付款交易）。替代地，在第三商家組態中，回應於在步驟612 PSP子系統310接收來自裝置100的任何合適線上資源驗證工作階段起始資料662以用於起始一PSP線上資源113之一驗證工作階段（其中此類驗證工作階段起始資料662可包括該線上資源之一識別符，例如，由裝置100存取的PSP線上資源之FQDN），在步驟614PSP子系統310可操作以傳達任何合適的查問請求資

料664（包括在步驟606由PSP子系統310所接收並對照驗證工作階段起始資料662之彼FQDN所儲存之憑證177）至商業實體子系統400，用以驗證用於待實行之特定安全資料交易的PSP線上資源（例如，如在步驟610及/或步驟612所識別之金融付款交易）。在步驟614自商家子系統200或PSP子系統310傳達至商業實體子系統400之此類查問請求資料664可包括用於嘗試向商業實體子系統400實證線上資源之有效性的任何合適資料，包括但不限於：憑證177，其可包括與線上資源相關聯之FQDN及/或任何其他合適的識別符，如在步驟606由商業實體子系統400產生者；及任何其他合適的資料（例如，識別裝置100的資料，及/或識別待實行之特定安全資料交易的資料（例如，如在步驟610及/或步驟612所識別之金融付款交易，其在本文中可稱為潛在交易識別資訊，且其可在程序600之任何合適部分期間使用，用於提供（一或多個）任何額外安全性層至目前資料交易程序，及/或用於提供任何額外安全性（例如，詐騙偵測）服務以供未來資料交易）。

【0089】 在程序600之步驟616，回應於在步驟614商業實體子系統400接收來自商家子系統200或PSP子系統310的任何合適的含憑證177之查問請求資料664，商業實體子系統400可操作以驗證由查問請求之一商家識別符167所識別的線上資源113。例如，在第一商家組態及第二商家組態兩者中，回應於在步驟614商業實體子系統400接收來自商家子系統200的任何合適的含憑證177之查問請求資料664，商業實體子系統400可操作以驗證並檢查所接收之查問請求資料664之憑證177，以透過（一或多個）任何合適的程序確保其信任仍然有效且尚未過期（例如，可由商業實體子系統400在資料664中接收憑證177，且接著商業實體子系統400可操作以判定彼憑證177是否係商業實體子系統400已知（例如，儲存在表格430中）、及彼憑證177是否仍然受信任、及/或彼憑證177是否尚未過期）。

接下來，如果已驗證所接收之憑證177，則可自所接收之憑證177擷取一FQDN及/或另一商家識別符167並與儲存在商業實體子系統400之表格430中的任何FQDN及憑證177關聯性進行交叉檢查，以確保所接收之憑證177之FQDN係經註冊。例如，在步驟616，商業實體子系統400可操作以嘗試確認在商業實體子系統400處由所接收之查問請求資料664之一商家識別符167所識別的線上資源113係一有效且經註冊之線上資源，其可藉由下列方式而確認：在表格430中識別彼商家識別符167（例如，以判商家識別符167已經向商業實體子系統400註冊（例如，在步驟606），且此類註冊仍然有效（例如，彼商業實體子系統400並未自表格430移除商家識別符167，或並未在表格430中將商家識別符167旗標為可疑或以其他方式不再受信任））。同樣地，在第三商家組態中，回應於在步驟614商業實體子系統400接收來自PSP子系統310的任何合適的含憑證177之查問請求資料664，商業實體子系統400可操作以驗證並檢查所接收之查問請求資料664之憑證177，以確保其信任仍然有效且尚未過期，且如果所接收之憑證177經驗證，則可自所接收之憑證177擷取一FQDN及另一商家識別符167及一PSP識別符，使得接著可判定所識別之PSP是否經授權以代表所識別之商家進行交易以及在商業實體子系統400處所擷取之FQDN是否經註冊至其他所擷取之商家識別符，以完全驗證步驟614之請求。一商家識別符167可係用於一特定商家子系統200之一全域商家識別符（例如，可使用單一商家識別符167以識別商家子系統200之一原生應用程式商家線上資源及一網站商家線上資源，及/或單一FQDN可與多個商家子系統相關聯（例如，可由多個商家子系統使用一PSP之一FQDN））。一FQDN及至少一其他識別符（諸如一特定商家子系統200之一唯一識別符及/或一特定PSP子系統310之一唯一識別符）兩者可擷取自一憑證177並在商業實體子系

統400處（例如，在表格430中）確認該兩者已彼此相關聯，如可已在步驟606完成。在由商業實體子系統400對所接收之查問請求資料664進行任何合適的驗證之後（例如，在驗證所接收之憑證177、及/或驗證所接收之憑證177之一FQDN、及/或確認介於一經識別PSP與所接收之憑證177之一經識別商家之間之經授權關係之後），在步驟616，商業實體子系統400亦可操作以產生任何合適的驗證資料並對照所接收之查問請求資料664的任何合適識別符資料來儲存彼驗證資料。例如，在步驟616對所接收之查問請求資料664進行任何合適的驗證之後，在步驟616，商業實體子系統400亦可操作以產生任何合適的驗證資料（例如，經由熵的任何合適隨機資料及/或任何合適的密碼編譯臨時值（例如，相似於上文所描述之步驟622之驗證資料））及一驗證工作階段識別符（例如，任何合適的文數字串或可唯一地對商業實體子系統400識別目前線上資源驗證工作階段的任何其他合適識別符（例如，如在步驟612可由電子裝置100所產生者，或在步驟614可由商家子系統200或PSP子系統310所產生者，或在步驟616可由商業實體子系統400所產生者）），且接著在步驟616，商業實體子系統400可依商業實體子系統400可存取之任何合適的資料結構（例如，在表格430中或以其他方式）對照查問請求資料664之驗證工作階段識別符及商家識別符之一或兩者來儲存彼驗證資料。因此，在某些實施例中，可由商業實體子系統400產生一驗證工作階段識別符，使得商業實體子系統400可確保（至少關於一特定商家識別符）該驗證工作階段識別符係正在由商業實體子系統400實行之一特定驗證程序所獨有的。然而，如果由商家子系統200或PSP子系統310產生一驗證工作階段識別符，則在使彼驗證工作階段識別符能夠用於彼特定驗證工作階段之前，商業實體子系統400可確認此一驗證工作階段識別符係該驗證工作階段之一商家識別

符獨有的。否則，商業實體子系統400可拒絕該驗證工作階段識別符並請求由商家子系統200或PSP子系統310產生一新驗證工作階段識別符。介於此類驗證資料與驗證工作階段之識別符資料之間之此一經儲存連結或關聯性（例如，查問請求資料664之該驗證工作階段識別符及/或一商家識別符）可稍後由商業實體子系統400使用以進一步保護待實行之安全資料交易的安全（例如，在步驟630）。另外，在一些實施例中，在步驟616，查問請求資料664之潛在交易識別資訊之任何者或全部亦可對照該驗證資料及識別符資料予以儲存或以其他方式與該驗證資料及識別符資料相關聯。

【0090】 在第一商家組態、第二商家組態及第三商家組態中之任何一者中，在此一步驟616之後，可略過步驟618、620及622，此係因為在單一組步驟614及616中該線上資源可經驗證，並且接著程序600可包括步驟624，在此步驟商業實體子系統400可操作以產生及傳達任何合適的驗證回應資料674。例如，驗證回應資料674可係一工作階段物件，其可包括步驟616之驗證資料連同任何其他合適的資料，包括但不限於：驗證工作階段識別符（例如，在步驟616所產生之驗證工作階段識別符）；一或多個商家識別符（例如，查問請求資料664之任何或各商家識別符（例如，FQDN、其他商家識別符、PSP識別符等），及/或如可依其他方式在商業實體子系統400處（例如，在表格430中）與在驗證工作階段期間經驗證之線上資源相關聯者）；查問請求資料664之憑證177；及/或類似物。在一些實施例中，如圖6中所展示，此類驗證回應資料674可自商業實體子系統400直接傳達至電子裝置100（例如，使用任何合適的通訊協定經由通訊路徑65），其中識別電子裝置100的資料（例如，裝置識別符119）可與驗證工作階段起始資料662及/或查問請求資料664或其他相關聯或以其他方式被包括

在驗證工作階段起始資料662及/或查問請求資料664或其他中，使得商業實體子系統400可傳達驗證回應資料674至恰當的電子裝置100。替代地，在一些實施例中（圖中未展示），可經由商家子系統200（例如，在第一商家組態及第二商家組態中）及/或經由PSP子系統310（例如，在第三商家組態中）自商業實體子系統400傳達驗證回應資料674至電子裝置100，藉此商家子系統200及/或PSP子系統310可接收來自商業實體子系統400之驗證回應資料674並接著傳遞驗證回應資料674之至少一部分至電子裝置100上。可由商業實體子系統400使用與商業實體子系統400相關聯且電子裝置100亦可存取的一存取金鑰（例如，存取金鑰155a、存取金鑰155b、CRS 151k、及/或安全元件145之ISD金鑰156k，或一裝置應用程式（例如，卡管理應用程式103b）可已知的任何金鑰）來簽署驗證回應資料674之工作階段物件（例如，在一HTTP標頭中或以其他方式），使得裝置100可在接收到該經簽署驗證資料後驗證簽章，以確認商業實體子系統400產生驗證回應資料674而非不受電子裝置100信任的另一實體子系統產生驗證回應資料，並且/或者防止無此一存取金鑰之存取權的另一實體（例如，商家子系統200及/或PSP子系統310）使用該經簽署驗證資料，同時仍然使其他實體能夠接收並轉遞此類經簽署驗證資料至裝置100上。

【0091】 在第一商家組態、第二商家組態及第三商家組態之任何一者中，如果裝置100之使用者願意且能夠回應於在步驟610所接收之潛在交易資料660（例如，付款請求資料）而選擇或確認一特定付款認證以用在為潛在交易提供資金，且在步驟624已由電子裝置100接收驗證回應資料674（例如，可指示步驟612至616之商家線上資源驗證工作階段成功的資料），則程序600可進行至步驟625，在此步驟，程序600可包括：在已識別任何工作階段識別符一致性之後（例

如上文所提及，於步驟625），接收裝置100之使用者對於利用一特定認證來實行針對基於潛在交易資料660之一特定商家、產品、價格及運送目的地的潛在交易之意圖及鑑認（例如，透過使用者選擇圖3C之鑑認提示315）。在一些實施例中，除步驟625包括在此類意圖及鑑認之前驗證工作階段識別符一致性外或作為一替代，步驟625可包括在此類意圖及鑑認之前驗證網域一致性。例如，回應於在步驟624裝置100接收驗證回應資料674，裝置100可操作以比較此類驗證回應資料674之一網域識別符（例如，驗證回應資料674之一FQDN）與目前在裝置100之一線上資源之一網址列中的一網域識別符。例如，裝置100之一Web套件（例如，線上資源應用程式113）可接收驗證回應資料674並轉送(relay)彼驗證回應資料674連同目前由該Web套件定目標之一網域識別符（例如，一FQDN）至裝置100之一通行證套件（例如，卡管理應用程式103b）。接著，該通行證套件可驗證所接收之驗證回應資料674之簽章（若有）（例如，使用裝置100之一存取金鑰）、自驗證回應資料674擷取一網域識別符（例如，FQDN）、並接著比較所擷取之網域識別符與由Web套件所識別且自Web套件所提供的網域識別符（例如，目前由裝置100之Web套件寄存的java腳本之FQDN（例如，在第一商家組態及第二商家組態中，一商家線上資源之FQDN，及在第三商家組態中，一PSP線上資源之FQDN）），其可使裝置100能夠確認回應資料674與裝置100目前存取之相同線上資源相關聯（例如，以避免一重新執行攻擊(replay attack)）。在步驟625已驗證任何合適的工作階段識別符一致性及/或任何合適的網域識別符一致性之後，可在步驟625接收針對一特定付款認證之意圖及鑑認。接著，對於第一商家組態、第二商家組態及第三商家組態中之各者，步驟626至629可如上文所描述發生，其中驗證回應資料674之任何或所有合適的部分（例如，工作階段識

別符，驗證資料（例如，臨時值）、FQDN、及/或任何其他合適的商家識別符或PSP識別符、及/或任何其他資料（例如，憑證177之至少一部分））可連同安全裝置資料677及交易資料660被包括作為裝置交易資料678。

【0092】 在第一商家組態、第二商家組態及第三商家組態中之任何一者中，在步驟630，商業實體子系統400可操作以驗證裝置100可已包括在裝置交易資料678中的驗證回應資料674之驗證資料。例如，回應於接收此類裝置交易資料678，在步驟630（例如，相似於在程序500之步驟516），商業實體子系統400可操作以識別來自彼裝置交易資料678之驗證回應資料674之至少一部分或全部並確認彼所接收之裝置交易資料678之驗證資料目前係經儲存在商業實體子系統400處，或更具體而言，在一些實施例中，確認彼所接收之裝置交易資料678之驗證資料目前係在商業實體子系統400處對照所接收之裝置交易資料678之一驗證工作階段識別符及/或對照所接收之裝置交易資料678之一商家識別符（例如，FQDN）經儲存（例如，在表格430中）。介於該驗證資料與驗證工作階段識別符及商家識別符之一或兩者之間的此一儲存連結可在自動清除該連結之前維持達僅一段有限時間量，使得電子裝置100會受限於必須在一定持續時間內在步驟624接收驗證回應資料674並接著在步驟628發送裝置交易資料678至商業實體子系統400，用於實現由商業實體子系統400保護裝置交易資料678之安全裝置資料677的安全，以用於運用經驗證商家線上資源實行特定安全資料交易（例如，商業實體子系統400可操作以在一定時期之後移除在商業實體子系統400處之介於驗證資料與驗證工作階段識別符及/或商家識別符之間的此一關聯性（例如，建立該連結之後不超過10分鐘即自表格430移除該連結），其可增加交易安全性）。此外或替代地，在步驟622，介於該驗證資料與驗證工作階段識別符及

商家識別符之一或兩者之間的一所儲存連結亦可與任何合適的特定潛在交易識別資訊（在步驟614，可由商家子系統200或PSP子系統310使潛在交易識別資訊可供商業實體子系統400使用）相關聯（例如，作為查問請求資料664之一部分），諸如待共用於裝置100與商家子系統200或PSP子系統310之間的一特定類型安全資料之識別（例如，用於金融交易的貨幣及數額及付款類型），及亦可由電子裝置100使相似特定潛在交易識別資訊可供商業實體子系統400使用，作為步驟628之裝置交易資料678之一部分，使得步驟630亦可包括商業實體子系統400確認目前對照在步驟614所接收之驗證資料所儲存的特定潛在交易識別資訊（例如，如在步驟616儲存在表格430中者）至少相似於在步驟628所接收之特定潛在交易識別資訊。

【0093】 接下來，在步驟631，程序600可包括商業實體子系統400識別與商家子系統200或PSP子系統310相關聯之一商家金鑰（例如，商家金鑰157）（例如，在步驟606，該子系統可已產生用於金鑰之該第一CSR，以用於驗證工作階段之線上資源）。即，在步驟629使用合適的存取資訊來解密裝置交易資料678之至少一部分之後（例如，在解密安全裝置資料677以具現化裝置付款認證資料676及可已在安全裝置資料677中加密之任何其他資訊之後），接著，在步驟631，商業實體子系統400可用商家子系統200之一適當的商家金鑰157（例如，對於第一商家組態）或用PSP子系統310之一適當的商家金鑰157（例如，對於第二商家組態及第三商家組態）來重新加密裝置交易資料678之至少一部分（例如，裝置付款認證資料676之符記資料及/或密碼編譯資料）作為經加密商家認證資料681，其中可在商業實體子系統400處使用可包括在資料678中的驗證資料之任何合適的識別符資料及使用與彼識別符資料相關聯之任何預先儲存關聯性（例

如，在表格430中，如可在步驟606期間定義）來識別彼適當的商家金鑰157。例如，經加密商家認證資料681可至少包括來自裝置交易資料678之經加密裝置付款認證資料676以及任何合適的交易資料，諸如來自或基於裝置交易資料678及/或潛在交易資料660的購買總額資料或其他合適的交易資料。可由商業實體子系統400來簽署經加密商家認證資料681使得當由商家子系統200或PSP子系統310接收時，彼子系統可確立商業實體子系統400為此類經加密商家認證資料681之建立者並且/或者可使彼子系統能夠確保此類經加密商家認證資料681在經簽署之後未經修改。在步驟631可產生此類經加密商家認證資料681，並且接著在步驟632傳輸此類經加密商家認證資料681連同任何其他合適的資料至裝置100，作為經保護安全之交易資料682（例如，經由圖1A之路徑65自商業實體子系統400之伺服器410傳輸至裝置100之通訊組件106）。

【0094】 步驟631及632可操作以確保自商業實體子系統400經傳輸作為圖1A之經保護安全之交易資料682之部分的認證資料（例如，經加密商家認證資料681之符記資料及/或密碼編譯資料）可經加密使得裝置100除安全元件145外無一部分可解密該認證資料。即，可用可未暴露於裝置100之任何部分（在一些實施例中，包括安全元件145）或以其他方式不可由該任何部分存取的一商家金鑰（例如，商家金鑰157）來加密經保護安全之交易資料682之認證資料（例如，經加密商家認證資料681之符記資料及/或密碼編譯資料）。另外，可用可未暴露於裝置100之安全元件145之外之任何部分或以其他方式不可由該任何部分存取的一認證金鑰155a'來加密經保護安全之交易資料682之認證資料（例如，經加密商家認證資料681之符記資料及/或密碼編譯資料）。

【0095】 在第一商家組態及第二商家組態中，在步驟634可接著由裝置100轉遞經保護安全之交易資料682至商家子系統200作為經保護安全之交易資料684（例如，經由通訊路徑15或作為一非接觸式之以接近性為基礎之通訊5），或替代地，商家認證資料681可自商業實體子系統400傳達至商家子系統200而無需經由裝置100予以傳達（圖中未展示）。可透過裝置100及/或商業實體子系統400載送潛在交易資料660之一部分、一些部分或所有部分至經保護安全之交易資料682及/或至經保護安全之交易資料684，使得在程序600期間可由實體之各者來識別潛在交易之某些識別符。

【0096】 一旦由商家子系統200接收包括付款認證資料675/676的商家認證資料681（例如，作為經保護安全之交易資料684，在步驟634），程序600亦可包括步驟636，在此步驟，商家子系統200可經組態以產生並傳輸付款資料686。在第一商家組態中，例如，在步驟636，商家子系統200可充分利用其已知之商家金鑰157以至少部分解密經保護安全之交易資料684之商家認證資料681，使得付款資料686可包括經用其認證金鑰155a'（而非用不可供金融機構子系統350使用之一金鑰）加密的認證SSD 154a之經保護安全之付款認證資料（例如，資料676），並且接著可由商家子系統200傳達此類資料686至任何合適的子系統（例如，收單銀行子系統300及/或PSP子系統310）。替代地，在第二商家組態中，例如，在步驟636，商家子系統200可轉遞經保護安全之交易資料684之經重新加密商家認證資料681至PSP子系統310而作為付款資料686，且接著PSP子系統310可充分利用其已知之商家金鑰157以至少部分解密付款資料686之彼經重新加密商家認證資料681。替代地，在第三商家組態中，可由裝置100轉遞經保護安全之交易資料682至PSP子系統310（例如，使用目前可由裝置100存取

之PSP線上資源），且接著PSP子系統310可充分利用其已知之商家金鑰157以至少部分解密彼經轉遞之經保護安全之交易資料的經重新加密商家認證資料681。可如上文關於步驟638至644所描述進程序600之其餘者，其中根據適用之商家組態，商家子系統200及PSP子系統310之一或多個適當者與裝置100進行資料通訊。

圖7之說明

【0097】 圖7係用於使用一控管實體子系統以進行經由在一電子裝置上執行的一線上資源之介於一處理子系統與通訊耦接至該處理子系統之該電子裝置之間的一安全交易之闡釋性程序700之步驟的流程圖。在程序700之步驟702，該控管實體子系統可接收對於該線上資源之一驗證請求，其中該驗證請求可包括驗證請求資料（例如，在程序600之步驟614，商業實體子系統400可接收查問請求資料664，及/或在步驟620，商業實體子系統400可接收查問回應資料670）。在程序700之步驟704，該控管實體子系統可使用該驗證請求資料及註冊資料來驗證該線上資源，其中在一開始於接收該驗證請求之前已使該註冊資料可供該控管實體子系統使用（例如，在程序600之步驟616，商業實體子系統400可使用來自步驟606之查問請求資料664及註冊資料來驗證一線上資源113，及/或在程序600之步驟622，商業實體子系統400可使用來自步驟606之查問回應資料670及註冊資料來驗證一線上資源113）。在程序700之步驟706，該控管實體子系統可使驗證回應資料與該驗證請求資料之至少一部分相關聯（例如，在程序600之步驟616及/或在步驟622，商業實體子系統400可使驗證資料與識別符資料相關聯）。在程序700之步驟708，該控管實體子系統可傳達該驗證回應資料至該電子裝置

（例如，在程序600之步驟624，商業實體子系統400可傳達驗證資料（作為驗證回應資料674之一部分）至電子裝置100）。在程序700之步驟710，該控管實體子系統可接收來自該電子裝置之裝置交易資料（例如，在程序600之步驟628，商業實體子系統400可接收來自電子裝置100之裝置交易資料678）。在程序700之步驟712，該控管實體子系統可使用該驗證回應資料來驗證該裝置交易資料（例如，在程序600之步驟630，商業實體子系統400可使用驗證回應資料674來驗證裝置交易資料678之驗證資料）。在程序700之步驟714，在已驗證該裝置交易資料之後，該控管實體子系統可基於該裝置交易資料來產生安全交易資料以供該處理子系統使用（例如，在程序600之步驟631，商業實體子系統400可基於裝置交易資料678來產生商家認證資料681）。

【0098】 應理解，圖7之程序700中展示之步驟僅係闡釋性，且可修改或省略現有步驟、可新增額外步驟、並且可改變某些步驟之順序。

圖8之說明

【0099】 圖8係用於使用一控管實體子系統以實現經由在一電子裝置上執行的一線上資源之介於一處理子系統與通訊耦接至該處理子系統之該電子裝置之間的一安全交易之闡釋性程序800之步驟的流程圖。在程序800之步驟802，該控管實體子系統可藉由建置介於該控管實體子系統與該處理子系統之間的一處理共用祕密來註冊該線上資源（例如，在程序600之步驟606，商業實體子系統400可藉由建置與商家子系統200之一共用祕密來註冊線上資源113）。在程序800之步驟804，該控管實體子系統可接收對於該線上資源之一驗證請求，其中該驗證請求可包括指示該線上資源之一處理識別符，且其中該驗證請求可進一步包

括經由該線上資源之介於該電子裝置與該處理子系統之間的一潛在交易所獨有的一驗證工作階段識別符（例如，在程序600之步驟614，商業實體子系統400可接收含一商家識別符及一工作階段識別符之查問請求資料664，及/或在程序600之步驟620，商業實體子系統400可接收含一商家識別符及一工作階段識別符之查問回應資料670）。在程序800之步驟806，該控管實體子系統可使用該驗證工作階段識別符及該處理共用祕密來驗證由該處理識別符所指示之該線上資源（例如，在程序600之步驟616，商業實體子系統400可使用來自步驟606之查問請求資料664及註冊資料來驗證線上資源113，及/或在程序600之步驟622，商業實體子系統400可使用來自步驟606之查問回應資料670及註冊資料來驗證線上資源113）。

【0100】 應理解，圖8之程序800中展示之步驟僅係闡釋性，且可修改或省略現有步驟、可新增額外步驟、並且可改變某些步驟之順序。

圖9之說明

【0101】 圖9係用於使用一控管實體子系統以進行經由在一電子裝置上執行的一線上資源之介於一處理子系統與通訊耦接至該處理子系統之該電子裝置之間的一安全交易之闡釋性程序900之步驟的流程圖。在程序900之步驟902，該控管實體子系統可接收對於該線上資源之一驗證請求，其中該驗證請求可包括驗證請求資料，且其中該驗證請求資料可包括潛在交易識別資訊，該潛在交易識別資訊指示經由該線上資源之介於該電子裝置與該處理子系統之間的一潛在交易（例如，在程序600之步驟614，商業實體子系統400可接收查問請求資料664，及/或在步驟620，商業實體子系統400可接收查問回應資料670）。在程序

900之步驟904，該控管實體子系統可使用該驗證請求資料之至少一部分來驗證該線上資源（例如，在程序600之步驟616，商業實體子系統400可使用查問請求資料664來驗證一線上資源113，及/或在程序600之步驟622，商業實體子系統400可使用查問回應資料670來驗證線上資源113）。在程序900之步驟906，該控管實體子系統可使驗證回應資料與至少該潛在交易識別資訊相關聯（例如，在程序600之步驟616及/或步驟622，商業實體子系統400可使驗證資料與潛在交易識別資訊相關聯）。在程序900之步驟908，該控管實體子系統可傳達該驗證回應資料至該電子裝置（例如，在程序600之步驟624，商業實體子系統400可傳達驗證資料（作為驗證回應資料674之一部分）至電子裝置100）。在程序900之步驟910，該控管實體子系統可接收來自該電子裝置之裝置交易資料（例如，在程序600之步驟628，商業實體子系統400可接收來自電子裝置100之裝置交易資料678）。在程序900之步驟912，該控管實體子系統可使用該驗證回應資料及該潛在交易識別資訊來驗證該裝置交易資料（例如，在程序600之步驟630，商業實體子系統400可使用驗證回應資料674及潛在交易識別資訊來驗證裝置交易資料678之驗證資料）。在程序900之步驟914，在已驗證該裝置交易資料之後，該控管實體子系統可基於該裝置交易資料來產生安全交易資料以供該處理子系統使用（例如，在程序600之步驟631，商業實體子系統400可基於裝置交易資料678來產生商家認證資料681）。

【0102】 應理解，圖9之程序900中展示之步驟僅係闡釋性，且可修改或省略現有步驟、可新增額外步驟、並且可改變某些步驟之順序。

實施例之進一步描述

【0103】 當適當啟用裝置100之安全元件之認證（例如，與認證SSD 154a之經啟用小程序153a相關聯的商務認證資料）以提供作為交易資料之付款認證資料（例如，作為至商家終端機220的非接觸式之以接近性為基礎之通訊及/或作為至商家伺服器210的以線上為基礎之通訊）時，收單銀行子系統300可利用此類付款認證資料用以完成與金融機構子系統350之金融交易。例如，在電子裝置100之使用者已選擇所要購買之產品且已適當地啟用待用於付款的裝置100之特定認證後，商家子系統200可接收付款認證資料，其指示用於該特定認證之付款認證資料。可由商家子系統200之任何合適的商家或商家代理來提供商家伺服器210及/或商家終端機220，其可回應於裝置100提供付款認證資料而提供產品或服務給終端使用者電子裝置之使用者。基於此類所接收之付款認證資料（例如，作為資料684），商家子系統200可經組態以產生及傳輸資料686至收單銀行子系統300（例如，經由介於商家子系統200與收單銀行子系統300之間之通訊路徑25），其中資料686可包括付款認證資料及一授權請求，其可指示針對產品或服務的裝置付款認證及商家的購買價格。亦名為一付款處理器或收單方的收單銀行子系統300可係與商家子系統200相關聯之商家的銀行業務合作夥伴，且收單銀行子系統300可經組態以與金融機構子系統350合作以用付款認證資料來核准及結清(settle)嘗試由裝置100提供資金的認證交易。接著，收單銀行子系統300可轉遞來自付款資料686之授權請求至金融機構子系統350而作為授權請求資料688（例如，經由介於收單銀行子系統300與金融機構子系統350之間之通訊路徑35）。

【0104】 付款網路子系統360及發行銀行子系統370可係單一實體或分開之實體。例如，American Express可係一付款網路子系統360及一發行銀行子系統

370兩者。相比而言，Visa及MasterCard可係付款網路360且可與發行銀行370（諸如Chase、Wells Fargo、Bank of America及類似者）合作。金融機構子系統350亦可包括一或多個收單銀行，諸如收單銀行子系統300。例如，收單銀行子系統300可係與發行銀行子系統370相同的實體。可使用下列各者來實施收單銀行子系統300之一組件、一些組件或全部組件：一或多個處理器組件，其可相同於或相似於裝置100之處理器組件102；一或多個記憶體組件，其可相同於或相似於裝置100之記憶體組件104；及/或一或多個通訊組件，其可相同於或相似於裝置100之通訊組件106。可使用下列各者來實施付款網路子系統360之一組件、一些組件或全部組件：一或多個處理器組件，其可相同於或相似於裝置100之處理器組件102；一或多個記憶體組件，其可相同於或相似於裝置100之記憶體組件104；及/或一或多個通訊組件，其可相同於或相似於裝置100之通訊組件106。可使用下列各者來實施發行銀行子系統370之一組件、一些組件或全部組件：一或多個處理器組件，其可相同於或相似於裝置100之處理器組件102；一或多個記憶體組件，其可相同於或相似於裝置100之記憶體組件104；及/或一或多個通訊組件，其可相同於或相似於裝置100之通訊組件106。在付款網路子系統360及發行銀行子系統370係分開之實體之情況中，付款網路子系統360可接收來自收單銀行子系統300之資料690及接著可轉遞一請求至發行銀行子系統370，作為資料405（例如，經由介於付款網路子系統360與發行銀行子系統370之間之通訊路徑45）。在付款網路子系統360及發行銀行子系統370係同一實體之情況中，收單銀行子系統300可直接提交資料690至發行銀行子系統370。此外，付款網路子系統360可代表發行銀行子系統370來回應收單銀行子系統300（例如，根據付款網路子系統360與發行銀行子系統370之間達成協議之條件）。藉由於收單銀行子

系統300與發行銀行子系統370之間介接，付款網路子系統360可減少各收單銀行子系統300及各發行銀行子系統370可能必須直接與之互動的實體之數目。即，為了使金融機構子系統350之直接整合點減至最少，付款網路子系統360可作為各種發行銀行370及/或各種收單銀行300之聚集者(aggregator)。金融機構子系統350亦可包括一或多個收單銀行，諸如收單銀行子系統300。例如，收單銀行子系統300可係與發行銀行子系統370相同的實體。

【0105】 當發行銀行子系統370接收一授權請求時（例如，直接自收單銀行子系統300接收而作為資料688，或間接經由付款網路子系統360接收而作為資料405），可分析包括在授權請求中之付款資訊（例如，資訊裝置100之商務認證）及購買量，以判定與商務認證相關聯的帳戶是否具有足以履行該購買量的信用。如果不存在足夠資金，發行銀行子系統370可藉由傳輸一否定授權回應至收單銀行子系統300而拒絕所請求之交易。然而，如果存在足夠資金，發行銀行子系統370可藉由傳輸一肯定授權回應至收單銀行子系統300而核准所請求之交易，而可完成金融交易。可由使用者金融子系統350提供任何類型授權回應至收單銀行子系統300作為授權回應資料或交易狀態資料690（例如，可經由通訊路徑35自發行銀行子系統370直接提供交易狀態資料690至收單銀行子系統300，或基於可經由通訊路徑45自發行銀行子系統370提供至付款網路子系統360的授權回應資料或交易狀態資料415，自付款網路子系統360提供交易狀態資料690至收單銀行子系統300）。

【0106】 如所提及，及如圖2中所展示，電子裝置100可包括但不限於：音樂播放器（例如，可購自Apple Inc.(Cupertino, California)的iPod™）、視訊播放器、靜態影像播放器、遊戲機、其他媒體播放器、音樂記錄器、電影或視訊攝影機

或記錄器、靜態相機、其他媒體記錄器、無線電、醫療設備、家用或商用器具、運輸載具儀器、樂器、計算器、蜂巢式電話（例如，可購自Apple Inc.的iPhone™）、其他無線通訊裝置、個人數位助理、遙控器、傳呼機、電腦（例如，桌上型電腦、膝上型電腦、平板電腦（例如，可購自Apple Inc.的iPad™）、伺服器）、監視器、電視、立體音響設備、數位視訊轉換盒(set up box)、機上盒、數據機、路由器、印表機或其任何組合。在一些實施例中，電子裝置100可執行單一功能（例如，專用以進行安全資料交易之裝置），及在其他實施例中，電子裝置100可執行多種功能（例如，進行安全資料交易、播放音樂及撥接電話通話的裝置）。電子裝置100可係可經組態成無論使用者身在何處皆可進行金融交易的任何攜帶型、行動型、手持型或微型電子裝置。一些微型電子裝置可具有小於手持型電子裝置（諸如，iPod™）之形狀因子的形狀因子。闡釋性微型電子裝置可整合至各種物件中，該等物件可包括但不限於：腕錶（例如，Apple Inc.的Apple Watch™）、戒指、項鍊、皮帶、皮帶配件、耳機、鞋之配件、虛擬實境裝置、眼鏡、其他可佩帶之電子器件、運動設備之配件、健身設備之配件、鑰匙鏈或其任何組合。替代地，電子裝置100可完全非攜帶型，反而可係大致上固定的。

【0107】 如圖2中所展示，電子裝置100可例如包括一處理器102、記憶體104、通訊組件106、電源供應器108、輸入組件110、輸出組件112、天線116、及近場通訊(「NFC」)組件120。電子裝置100亦可包括一匯流排118，該匯流排可提供一或多個有線或無線通訊鏈路或路徑以用於傳送資料及/或電力至裝置100之各種其他組件、自該各種其他組件傳送資料及/或電力、或在該各種其他組件之間傳送資料及/或電力。在一些實施例中，可組合或省略電子裝置100之一或多個組件。另外，電子裝置100可包括圖2中未組合或未包括之其他組件。例如，

電子裝置100可包括任何其他合適的組件或圖2中展示的組件之若干例項。為簡單起見，圖2中展示該等組件中之各者之僅一者。

【0108】 記憶體104可包括一或多個儲存媒體，例如包括硬碟機、快閃記憶體、諸如唯讀記憶體(「ROM」)之永久性記憶體、諸如隨機存取記憶體(「RAM」)之半永久性記憶體、任何其他合適類型之儲存組件，或其任何組合。記憶體104可包括快取記憶體，其可係用於暫時儲存電子裝置應用程式之資料的一或多種不同類型記憶體。記憶體104可固定地內嵌於電子裝置100內或可併入於可被重複地插入至電子裝置100中及自電子裝置100移除的一或多種合適類型之卡（例如，用戶識別模組(「SIM」)卡或安全數位(「SD」)記憶卡）上。記憶體104可儲存媒體資料（例如，音樂及影像檔案）、軟體（例如，用於實施裝置100上之功能）、韌體、偏好資訊（例如，媒體播放偏好）、生活型態資訊（例如，食物偏好）、運動資訊（例如，由運動監控設備獲得之資訊）、交易資訊（例如，諸如信用卡資訊之資訊）、無線連接資訊（例如，可使裝置100能夠建立無線連接之資訊）、訂閱資訊（例如，追蹤使用者所訂閱之播客(podcast)或電視節目或其他媒體的資訊）、連絡人資訊（例如，電話號碼及電子郵件地址）、行事曆資訊、任何其他合適資料或其任何組合。

【0109】 可提供通訊組件106以允許裝置100使用任何合適的通訊協定來與一或多個其他電子裝置或伺服器或子系統（例如，系統1之一或多個子系統或其他組件）通訊。例如，通訊組件106可支援Wi-Fi（例如，802.11協定）、ZigBee（例如，802.15.4協定）、WiDi™、乙太網路、Bluetooth™、Bluetooth™低能量(Bluetooth™ Low Energy；「BLE」)、高頻系統（例如，900 MHz、2.4 GHz、及5.6 GHz通訊系統）、紅外線、傳輸控制協定/網際網路協定(「TCP/IP」)（例如，

於TCP/IP層中之各者中使用的協定中之任一者)、串流控制傳輸協定(「SCTP」)、動態主機組態協定(「DHCP」)、超文字傳送協定(「HTTP」)、BitTorrent™、檔案傳送協定(「FTP」)、即時輸送協定(「RTP」)、即時串流協定(「RTSP」)、即時控制協定(「RTCP」)、遠端音訊輸出協定(「RAOP」)、實資料輸送協定™(「RDTP」)、使用者資料包協定(「UDP」)、安全殼層協定(「SSH」)、無線分佈系統(「WDS」)橋接、可由無線及蜂巢式電話與個人電子郵件裝置使用的任何通訊協定(例如,全球行動通訊系統(「GSM」)、GSM+增強型資料速率GSM演進(「EDGE」)、分碼多重存取(「CDMA」)、正交分頻多重存取(「OFDMA」)、高速封包存取(「HSPA」)、多頻帶等)、可由一低功率無線個人區域網路(「6LoWPAN」)模組使用的任何通訊協定、任何其他通訊協定、或其任何組合。通訊組件106亦可包括或電耦接至可使裝置100能夠通訊地耦接至另一裝置(例如,主機電腦或配件裝置)且與彼另一裝置無線地或經由有線連接(例如,使用連接器埠)通訊的任何合適之收發器電路系統(例如,經由匯流排118之收發器電路系統或天線116)。通訊組件106當操作以傳達任何合適的資料至任何遠端伺服器或其他合適的實體(例如,至任何合適的網際網路連接)時可稱為線上通訊組件。通訊組件106可經組態以判定電子裝置100之地理位置。例如,通訊組件106通訊組件106可利用全球定位系統(「GPS」)或區域性或站點範圍定位系統,其可使用小區塔定位技術或Wi Fi技術。

【0110】 電源供應器108可包括用於接收及/或產生電力及用於將此電力提供至電子裝置100之其他組件其中之一或多者的任何合適電路系統。例如,電源供應器108可耦接至電網(例如,當裝置100不作為攜帶型裝置時或當裝置之電池係在具有由發電廠產生之電力的電插座處充電時)。舉另一實例,電源供應

器108可經組態以自天然來源產生電力（例如，使用太陽能電池自太陽能產生電力）。舉另一實例，電源供應器108可包括用於提供電力之一或多個電池（例如，當裝置100作為攜帶型裝置時）。例如，電源供應器108可包括以下各者中之一或多者：電池（例如，凝膠體、鎳金屬氫化物、鎳鎘、鎳氫、鉛酸或鋰離子電池）；不間斷或連續電源供應器（「UPS」或「CPS」）；及用於處理自電力產生源接收之電力（例如，由發電廠產生且經由電插座或以其他方式而被遞送至使用者的電力）的電路系統。可由電源供應器108提供電力為交流電或直流電，且電力可經處理以變換電力或使接收之電力限於特定特性。例如，電力可變換至直流電或可變換自直流電，且被約束至下列之一或多個值：平均功率、有效功率、峰值功率、每脈衝能量、電壓、電流（以安培量測）或所接收之電力的任何其他特性。電源供應器108可操作以（例如）基於電子裝置100或可耦接至電子裝置100之周邊裝置的需要或需求而在不同時間請求或提供特定電力量（例如，在正對電池充電時請求多於在電池已充好電時的功率）。

【0111】 可提供一或多個輸入組件110以准許使用者與裝置100互動或介接。例如，輸入組件110可採用多種形式，包括但不限於：觸控板、撥號件、點選輪、滾輪、觸控螢幕、一或多個按鈕（例如，鍵盤）、滑鼠、操縱桿、軌跡球、麥克風、攝影機、掃描器（例如，條碼掃描器或可自諸如條碼、QR代碼或相似者之代碼獲得產品識別資訊之任何其他合適的掃描器）、鄰近性感測器、光偵測器、運動感測器、生物特徵感測器（例如，指紋讀取器或其他特徵辨識感測器，其可結合電子裝置100可存取的特徵處理應用程式來操作以用於鑑認使用者）、及其組合。各輸入組件110可經組態以提供用於進行選擇或發出命令（與操作裝置100相關聯）的一或多個專用控制功能。

【0112】 電子裝置100亦可包括一或多個輸出組件112，輸出組件可呈現資訊（例如，圖形、聽覺及/或觸覺資訊）給裝置100之使用者。例如，電子裝置100之輸出組件112可採取各種形式，包括但不限於：音訊揚聲器、頭戴式耳機、音訊線輸出、視覺顯示、天線、紅外線埠、觸感輸出組件（例如，低頻警報器（rumbler）、振動器等）或其組合。

【0113】 舉一具體實例，電子裝置100可包括一顯示輸出組件作為輸出組件112。此一顯示輸出組件可包括用於向使用者呈現視覺資料的任何合適類型之顯示器或介面。一顯示輸出組件可包括可包括內嵌於裝置100中或耦接至裝置100的顯示器（例如，可移除式顯示器）。一顯示輸出組件可包括（例如）液晶顯示器（「LCD」）、發光二極體（「LED」）顯示器、有機發光二極體（「OLED」）顯示器、表面傳導電子發射器顯示器（「SED」）、碳奈米管顯示器、奈米晶體顯示器、任何其他合適之顯示器類型或其組合。替代地，顯示輸出組件可包括可移動顯示器或用於在距電子裝置100遙遠之表面上提供內容之顯示的投影系統（例如，諸如視訊投影儀、抬頭式顯示器或三維（例如，全像）顯示器）。舉另一實例，顯示輸出組件可包括數位或機械取景器，諸如在小型數位相機、反射式相機或任何其他合適之靜態相機或視訊攝影機中找到之取景器類型。顯示輸出組件可包括顯示驅動器電路系統、用於驅動顯示驅動器之電路系統或兩者，且此一顯示輸出組件可操作以顯示可在處理器102之指導下的內容（例如，媒體播放資訊、用於實施於電子裝置100上之應用程式的應用程式畫面、關於正在進行之通訊操作的資訊、關於傳入之通訊請求的資訊、裝置操作畫面等）。

【0114】 應注意，一或多個輸入組件及一或多個輸出組件有時候在本文中可統稱為輸入/輸出（「I/O」）組件或I/O介面（例如，輸入組件110及輸出組件112

統稱為I/O組件或I/O介面114)。例如，輸入組件110及輸出組件112有時候可係一單一I/O組件114(諸如一觸控螢幕)，其可透過使用者對顯示螢幕之觸摸來接收輸入資訊且亦可經由彼同一顯示螢幕提供視覺資訊給使用者。

【0115】 電子裝置100之處理器102可包括可操作以控制電子裝置100之一或多個組件之操作及效能的任何處理電路系統。例如，處理器102可接收來自輸入組件110之輸入信號及/或透過輸出組件112驅動輸出信號。如圖2中所展示，處理器102可用以執行一或多個應用程式，諸如一應用程式103、一應用程式113及/或一應用程式143。各應用程式103/113/143可包括但不限於：一或多個作業系統應用程式、韌體應用程式、媒體播放應用程式、媒體編輯應用程式、NFC低功率模式應用程式、生物特徵處理應用程式或任何其他合適之應用程式。例如，處理器102可載入應用程式103/113/143作為使用者介面程式，以判定經由輸入組件110或裝置100之其他組件所接收的指令或資料可如何操縱可儲存資訊及/或經由輸出組件112將資訊提供至使用者的方式。可由處理器102自任何合適來源(諸如，自記憶體104(例如，經由匯流排118)或自另一裝置或伺服器(例如，經由通訊組件106))來存取應用程式103/113/143。處理器102可包括單一處理器或多個處理器。例如，處理器102可包括可包括至少一個「一般用途」微處理器、一般用途微處理器及特殊用途微處理器之組合、指令集處理器、圖形處理器、視訊處理器及/或相關晶片組，及/或特殊用途微處理器。處理器102亦可包括用於快取用途之板上(on board)記憶體。

【0116】 電子裝置100亦可包括近場通訊(「NFC」)組件120。NFC組件120可係任何合適的基於接近性之通訊機構，該以接近性為基礎之通訊機構可實現介於電子裝置100與商家子系統200(例如，商家付款終端機220)之間之非接觸

式之以接近性為基礎之交易或通訊。NFC組件120可允許以相對低資料速率（例如，424 kbps）進行近距離通訊，且可遵照任何合適標準，諸如ISO/IEC 7816、ISO/IEC 18092、ECMA-340、ISO/IEC 21481、ECMA-352、ISO 14443、及/或ISO 15693。替代地或此外，NFC組件120可允許以相對高資料速率（例如，370 Mbps）進行近距離通訊，且可遵照任何合適標準，諸如TransferJet™協定。介於NFC組件120與商家子系統200之間之通訊可發生在介於NFC組件與商家子系統200之間的任何合適的近距離（例如，參見圖1及圖1A之介於NFC組件120與商家付款終端機220之間之距離D）內（諸如，近似2至4公分之範圍），且可在任何合適之頻率（例如，13.56 MHz）下操作。例如，NFC組件120之此近距離通訊可經由磁場感應而發生，磁場感應可允許該NFC組件與其他NFC裝置通訊及/或自具有射頻識別（「RFID」）電路系統之標籤擷取資訊。此一NFC組件可提供獲取商品資訊、傳送付款資訊及以其他方式與一外部裝置通訊（例如，介於NFC組件120與商家終端機220之間之通訊）之方式。

【0117】 NFC組件120可包括用於實現介於電子裝置100與商家子系統200之間之非接觸式之以接近性為基礎之通訊的任何合適模組。如圖2中所展示，NFC組件120可例如包括一NFC裝置模組130、一NFC控制器模組140、及一NFC記憶體模組150。

【0118】 NFC裝置模組130可包括一NFC資料模組132、一NFC天線134、及一NFC加強器136。NFC資料模組132可經組態以含有、路由或以其他方式提供任何合適的資料，該資料可由NFC組件120傳輸至商家子系統200而作為一非接觸式之以接近性為基礎或NFC通訊5之部分。此外或替代地，NFC資料模組132可經組態以含有、路由或以其他方式接收任何合適的資料，該資料可由NFC組

件120接收自商家子系統200而作為非接觸式之以接近性為基礎之通訊之部分（例如，NFC組件120與商家終端機220之間之通訊5）。

【0119】 NFC收發器或NFC天線134可係大致上實現將通訊自NFC資料模組132傳達至商家子系統200及/或自商家子系統200傳達至NFC資料模組132的任何合適天線或其他合適的收發器電路系統。因此，可提供NFC天線134（例如，環形天線）以具體地用於實現NFC組件120之非接觸式之以接近性為基礎之通訊能力。

【0120】 替代地或此外，NFC組件120可利用電子裝置100之另一通訊組件（例如，通訊組件106）可利用之同一收發器電路系統或天線（例如，天線116）。例如，通訊組件106可充分利用天線116以實現電子裝置100與另一遠端實體之間的Wi-Fi、Bluetooth™、蜂巢式或GPS通訊，而NFC組件120可充分利用天線116以實現NFC裝置模組130之NFC資料模組132與另一實體（例如，商家子系統200）之間的非接觸式之以接近性為基礎之通訊或NFC通訊。在此等實施例中，NFC裝置模組130可包括NFC加強器136，NFC加強器可經組態以提供針對NFC組件120之資料（例如，NFC資料模組132內之資料）的適當信號放大，使得可藉由共用天線116將此資料適當地作為通訊而傳輸至子系統200。例如，在可恰當地啟用天線116（例如，一非環形天線）以在電子裝置100與商家子系統200之間傳達非接觸式之以接近性為基礎之通訊或NFC通訊之前，共用天線116可能需要來自加強器136之放大（例如，使用天線116來傳輸NFC資料所需的功率可能多於使用天線116來傳輸其他類型之資料所需的功率）。

【0121】 NFC控制器模組140可包括至少一NFC處理器模組142。NFC處理器模組142可結合NFC裝置模組130操作以啟用、啟動、允許及/或以其他方式控

制NFC組件120，以用於傳達介於電子裝置100與商家子系統200之間之一NFC通訊。NFC處理器模組142可存在作為一分開之組件、可整合至另一晶片組中，或可與處理器102整合（例如）以作為系統單晶片（「SoC」）之一部分。如圖2中所展示，NFC控制器模組140之NFC處理器模組142可用以執行一或多個應用程式，諸如可幫助規定NFC組件120之功能的一NFC低功率模式或錢包應用程式143。應用程式143可包括但不限於：一或多個作業系統應用程式、韌體應用程式、NFC低功率應用程式、或可供NFC組件120存取的任何其他合適應用程式（例如，應用程式103/113）。NFC控制器模組140可包括一或多個協定，諸如近場通訊介面及協定（「NFCIP-1」），以用於與另一NFC裝置（例如，商家子系統200）通訊。可使用該等協定來調適通訊速度並將所連接裝置中之一者指定為控制近場通訊之起始者裝置。

【0122】 NFC控制器模組140可控制NFC組件120之近場通訊模式。例如，NFC處理器模組142可經組態以在下列模式之間切換NFC裝置模組130：用於將資訊（例如，通訊5）自NFC標籤（例如，自商家子系統200）讀取至NFC資料模組132的讀取器/寫入器模式；用於與另一NFC啟用裝置（例如，商家子系統200）交換資料（例如，通訊5）的同級間模式；及用於允許另一NFC啟用裝置（例如，商家子系統200）自NFC資料模組132讀取資訊（例如，通訊5）的卡模擬模式。NFC控制器模組140亦可經組態以使NFC組件120於主動模式與被動模式之間切換。例如，NFC處理器模組142可經組態以使NFC裝置模組130（例如，結合NFC天線134或共用天線116）在主動模式（其中NFC裝置模組130可產生其自身之RF場）與被動模式（其中NFC裝置模組130可使用負載調變以將資料傳送至產生RF場之另一裝置（例如，商家子系統200））之間切換。與處於此主動模式之操作

相比，處於此被動模式之操作可延長電子裝置100之電池壽命。可基於使用者之偏好及/或基於裝置100之製造商的偏好來控制NFC裝置模組130之模式，可由在裝置100上之執行應用程式（例如，應用程式103及/或應用程式143）來定義或以其他方式規定該等偏好。

【0123】 NFC記憶體模組150可結合NFC裝置模組130及/或NFC控制器模組140操作以允許介於電子裝置100與商家子系統200之間之NFC通訊。NFC記憶體模組150可內嵌在NFC裝置硬體內或在一NFC積體電路(「IC」)內。NFC記憶體模組150可防篡改且可提供一安全元件之至少一部分。例如，NFC記憶體模組150可儲存與NFC通訊有關且可由NFC控制器模組140存取的一或多個應用程式（例如，應用程式143）。例如，此類應用程式可包括可經加密的金融付款應用程式、安全存取系統應用程式、會員卡(loyalty card)應用程式及其他應用程式。在一些實施例中，NFC控制器模組140及NFC記憶體模組150可獨立地或組合地提供一專用微處理器系統，該專用微處理器系統可含有意欲被用來在電子裝置100上儲存及執行敏感應用程式的作業系統、記憶體、應用程式環境及安全性協定。NFC控制器模組140及NFC記憶體模組150可獨立地或組合地提供可防篡改之安全元件145之至少一部分。例如，此一安全元件145可經組態以提供一防篡改平台（例如，作為單一晶片或多晶片安全微控制器），其可能夠根據可由一組經妥善識別之受信任授權單位（例如，一金融機構子系統之一授權單位及/或一產業標準，諸如GlobalPlatform）所提出的規則及安全性要求來安全地寄存應用程式及其等之機密及密碼編譯資料（例如，小程序153及金鑰155）。NFC記憶體模組150可係記憶體104之一部分或NFC組件120特定之至少一專用晶片。NFC記憶體模組150可駐留於SIM上、電子裝置100之主機板上的一專用晶片上、或作為

一外部插入式記憶卡。NFC記憶體模組150可完全獨立於NFC控制器模組140且可由裝置100之不同組件來提供及/或由不同之可移除式子系統而被提供至電子裝置100。安全元件145可係一晶片內之高度安全的防篡改硬體組件，該組件可用於在電子裝置100上儲存敏感性資料或應用程式。可在諸如通用積體電路卡(「UICC」)或用戶識別模組(「SIM」)卡之可移除式電路卡中提供安全元件145之至少一部分，可於與全球行動通訊系統(「GSM」)網路、通用行動電信系統(「UMTS」)及/或長期演進(「LTE」)標準網路相容之電子裝置100中使用該可移除式電路卡。替代地或此外，安全元件145之至少一部分可提供於可在裝置100之製造期間內嵌至電子裝置100中的積體電路中。替代地或此外，安全元件145之至少一部分可提供於可插塞至、插入至或以其他方式耦接至電子裝置100之周邊裝置(諸如，微安全數位(「SD」)記憶卡)中。

【0124】 如圖2中所展示，NFC記憶體模組150可包括一發行方安全性網域(「ISD」)152及一補充安全性網域(「SSD」)154之一或多者(例如，一服務提供者安全性網域(「SPSD」)、一受信任服務管理員安全性網域(「TSMSPD」)等)，該等安全性網域可由NFC規格標準(例如，GlobalPlatform)定義及管理。例如，ISD 152可係NFC記憶體模組150之一部分，其中一受信任服務管理員(「TSM」)或發行金融機構(例如，商業實體子系統400及/或金融機構子系統350)可儲存金鑰及/或其他合適的資訊以用於在電子裝置100上(例如，經由通訊組件106)建立或以其他方式佈建一或多個認證(例如，與各種信用卡、銀行卡、禮品卡、通行卡、交通票證、數位貨幣(例如，比特幣(bitcoin))及相關聯之付款網路)等相關聯的商務認證)，以用於認證內容管理，及/或用於安全性網域管理。一特定補充安全性網域(「SSD」)154(例如，SSD 154a)可與可提供特定特殊權限

或付款權給電子裝置100的一特定TSM及至少一特定商務認證（例如，一特定信用卡認證或一特定公共交通卡認證）相關聯。例如，第一付款網路子系統360（例如，Visa）可為用於第一SSD 154a之TSM，且第一SSD 154a之小程序153a可與由第一付款網路子系統360管理之商務認證相關聯，而第二付款網路子系統360（例如，MasterCard）可為用於另一SSD 154之TSM。

【0125】 可提供安全性特徵以使得能夠使用NFC組件120（例如，用於實現啟動經佈建在裝置100上之商務認證），此在將機密付款資訊（諸如，認證之信用卡資訊或銀行帳戶資訊）自電子裝置100傳輸至商家子系統200時可係特別實用。此類安全性特徵亦可包括可具有受限制之存取的一安全儲存區域。例如，可能需要提供經由個人識別號碼（「PIN」）輸入項或經由使用者與生物特徵感測器之互動的使用者鑑認，以存取安全儲存區域（例如，以供使用者更改安全元件之安全性網域元件的生命週期狀態）。在某些實施例中，安全性特徵之一些或全部可儲存在NFC記憶體模組150內。進一步，用以與子系統200通訊之安全性資訊（諸如鑑認金鑰）可儲存在NFC記憶體模組150內。在某些實施例中，NFC記憶體模組150可包括內嵌在電子裝置100內之微控制器。

【0126】 圖1A之商家子系統200之商家終端機220可包括用於偵測、讀取或以其他方式接收來自電子裝置100之NFC通訊（例如，當電子裝置100在此商家終端機220之某一距離內或附近時的通訊5）的一讀取器。據此，應注意，此一商家終端機與電子裝置100之間的NFC通訊可以無線方式發生，且因而，可能不需要在各別裝置之間的無障礙「視線(line of sight)」。如所提及，NFC裝置模組130可係被動式或主動式。當NFC裝置模組130係被動式時，NFC裝置模組130可僅在處於此一商家終端機之合適讀取器之回應範圍內時啟動。舉例而言，此

商家終端機之讀取器可發射相對低功率無線電波場，該相對低功率無線電波場可用以對由NFC裝置模組130所利用之天線（例如，共用天線116或NFC特定天線134）供電，且藉此，使彼天線能夠將合適的NFC通訊資訊（例如，信用卡認證資訊）自NFC資料模組132經由天線116或天線134傳輸至此商家終端機作為NFC通訊。當NFC裝置模組130係主動式時，NFC裝置模組130可併有或以其他方式存取在電子裝置100本端之電源（例如，電力供應器108），其可使共用天線116或NFC特定天線134能夠主動地將NFC通訊資訊（例如，信用卡認證資訊）自NFC資料模組132經由天線116或天線134傳輸至此商家終端機220作為NFC通訊，而非反射射頻信號，如在被動式NFC裝置模組130之情況中。可由商家子系統200之一商家提供商家終端機220（例如，在商家之商店中，用於向在該商店處的裝置100之使用者直接銷售產品或服務）。雖然已關於近場通訊描述NFC組件120，但應理解，組件120可經組態以在電子裝置100與此一商家終端機之間提供任何合適的非接觸式之以接近性為基礎之行動付款或任何其他合適類型之非接觸式之以接近性為基礎之通訊。例如，NFC組件120可經組態以提供任何合適的短程通訊，諸如，涉及電磁/靜電耦合技術之短程通訊。

【0127】 雖然已關於近場通訊描述NFC組件120，但應理解，組件120可經組態以在電子裝置100與商家子系統200之間提供任何合適的非接觸式之以接近性為基礎之行動付款或任何其他合適類型之非接觸式之以接近性為基礎之通訊。例如，NFC組件120可經組態以提供任何合適的短程通訊，諸如，涉及電磁/靜電耦合技術之短程通訊。替代地，在一些實施例中，裝置100之NFC組件120可經組態以包括任何合適的組件，用於使可供處理器102或裝置100之任何其他部件使用的資料能夠被傳達作為介於裝置100之NFC組件120與商家子系統200

之商家終端機220之間任何合適的非接觸式之以接近性為基礎之通訊，但是NFC組件120可或可不包括可操作以安全地儲存認證小程序的一安全元件，用於在裝置100上產生安全認證資料以供安全地為一金融交易提供資金，如同程序600之認證資料。

【0128】 電子裝置100亦可具備一外殼101，該外殼可至少部分地圍封裝置100的組件中之之一或多者以用於保護免受裝置100外部之碎屑及其他降級力影響。在一些實施例中，該等組件中之之一或多者可提供於其自身外殼內（例如，輸入組件110可為在其自身外殼內之獨立鍵盤或滑鼠，該獨立鍵盤或滑鼠可以無線方式或經由電線來與可提供於其自身外殼內之處理器102通訊）。應理解，任何裝置100可經提供為彼此結合運作的兩個或更多裝置之組合（例如，經由任何合適的接近式通訊協定（例如，BlueTooth™）通訊耦接的蜂巢式電話及智慧錶）。

【0129】 如所提及，且如圖3中所展示，電子裝置100之一特定實例可係一手持式電子裝置，諸如一iPhone™，其中外殼101可允許存取各種輸入組件110a至110i、各種輸出組件112a至112c、及各種I/O組件114a至114d，裝置100及使用者及/或周邊環境可透過該等組件彼此介接。輸入組件110a可包括一按鈕，當該按鈕經按壓時，可使裝置100顯示當前執行之應用程式的「首頁(home)」畫面或選單。輸入組件110b可係用於在睡眠模式與喚醒模式之間或在任何其他合適模式之間切換電子裝置100之按鈕。輸入組件110c可包括雙位置式滑動器，在電子裝置100之某些模式中，該滑動器可停用一或多個輸出組件112。輸入組件110d及110e可包括用於增加或減少電子裝置100之輸出組件112的音量輸出(volume output)或任何其他特性輸出之按鈕。輸入組件110a至110e之各者可係機械輸入組

件，諸如，由半球形開關支撐之按鈕、滑動開關、控制墊、鍵、旋鈕、滾輪或任何其他合適形式。

【0130】 輸出組件112a可係一顯示器(其可用以顯示一視覺或圖形使用者介面(「GUI」)180，其可允許一使用者與電子裝置100互動。GUI 180可包括可顯示在顯示輸出組件112a之所有或一些區域中的目前執行中應用程式(例如，應用程式103及/或應用程式113及/或應用程式143)之各種層、視窗、畫面、範本、元件、選單、及/或其他組件。例如，如圖3中所展示，GUI 180可經組態以顯示一第一畫面190。使用者輸入組件110a至110i之一或多者可用以導覽GUI 180。例如，一使用者輸入組件110可包括滾輪，該滾輪可允許使用者選擇GUI 180之一或多個圖形元素或圖示182。圖示182亦可經由可包括顯示輸出組件112a及相關聯之觸控輸入組件110f的觸控螢幕I/O組件114a來選擇。此一觸控螢幕I/O組件114a可採用任何合適類型之觸控螢幕輸入技術，諸如(但不限於)：電阻式、電容式、紅外線、表面聲波、電磁或近場成像。此外，觸控螢幕I/O組件114a可採用單點或多點(例如，多點觸控)輸入感測。

【0131】 圖示182可表示在由使用者選擇後即可顯示於顯示組件112a之區域中之一些或全部中的各種圖層、視窗、畫面、範本、元件、及/或其他組件。此外，特定圖示182之選擇可導致階層式導覽程序。例如，特定圖示182之選擇可導致GUI 180之新畫面，其可包括同一應用程式或與彼圖示182相關聯之新應用程式的一或多個額外圖示或其他GUI元素。文字指示符181可顯示於每一圖示182上或附近以幫助使用者解讀每一圖形元素圖示182。應理解，GUI 180可包括按階層式及/或非階層式結構配置之各種組件。選擇特定圖示182時，裝置100可經組態以開啟與彼圖示182相關聯之新應用程式，並顯示GUI 180之與彼應用程

式相關聯的相對應之畫面。例如，當選擇標記有「商家應用程式」文字指示符181（即，特定圖示183）之特定圖示182時，裝置100可啟動或以其他方式存取一特定商家應用程式且可顯示特定使用者介面之畫面，該使用者介面可包括用於以特定方式與裝置100互動之一或多個工具或特徵。對於各應用程式，畫面可顯示在顯示輸出組件112a上，且可包括各種使用者介面元素（例如，圖3A至圖3D之畫面190a至190d）。此外或替代地，對於各應用程式，可經由裝置100之各種其他輸出組件112提供各種其他類型之非視覺資訊給使用者。可使用廣泛多樣的圖形元素及視覺方案來達成關於各種GUI 180所描述之操作。因此，所描述之實施例非意欲受限於本文採用之精確使用者介面慣例。而是，實施例可包括廣泛多樣的使用者介面樣式。

【0132】 電子裝置100亦可包括可允許裝置100與其他裝置之間的通訊之各種其他I/O組件114。I/O組件114b可係一連接埠，其可經組態用於自遠端資料源傳輸及接收資料檔案（諸如，媒體檔案或客戶訂單檔案），及/或自外部電源傳輸及接收電力。例如，I/O組件114b可係專屬埠，諸如來自Apple Inc. (Cupertino, California)的Lightning™ 連接器或30針基座(30-pin dock)連接器。I/O組件114c可係用於收納SIM卡或任何其他類型之可移除式組件的連接槽。I/O組件114d可係用於連接可或可不包括麥克風組件之音訊頭戴式耳機的頭戴式耳機插口。電子裝置100亦可包括諸如麥克風之至少一音訊輸入組件110g及諸如音訊揚聲器之至少一音訊輸出組件112b。

【0133】 電子裝置100亦可包括至少一觸感或觸覺輸出組件112c（例如，低頻警報器）、攝影機及/或掃描器輸入組件110h（例如，視訊或靜態相機，及/或條碼掃描器或可自諸如條碼、QR碼或相似者獲得產品識別資訊之任何其他合

適掃描器)及生物特徵輸入組件110i(例如,指紋讀取器或可結合可由電子裝置100存取之特徵處理應用程式來操作以用於鑑認使用者的其他特徵辨識感測器)。如圖3中所展示,生物特徵輸入組件110i之至少一部分可併入至輸入組件110a或裝置100之任何其他合適輸入組件110內或以其他方式與輸入組件110a或裝置100之任何其他合適輸入組件110組合。例如,生物特徵輸入組件110i可係指紋讀取器,其可經組態以當使用者藉由用使用者之手指按壓輸入組件110a而與機械輸入組件110a互動時掃描彼手指之指紋。舉另一實例,生物特徵輸入組件110i可係指紋讀取器,其可與觸控螢幕I/O組件114a之觸控輸入組件110f組合,使得生物特徵輸入組件110i可經組態以當使用者藉由用使用者之手指按壓觸控螢幕輸入組件110f或沿著觸控螢幕輸入組件110f滑動而與觸控螢幕輸入組件110f互動時掃描彼手指之指紋。另外,如所提及,電子裝置100可進一步包括NFC組件120,其可由子系統200經由天線116及/或天線134(圖3中未展示)以通訊方式存取。NFC組件120可至少部分位於外殼101內,且可將標記或符號121提供於外殼101之外部上,該標記或符號121可識別與NFC組件120相關聯的天線中之一或多者之大致定位(例如,天線116及/或天線134之大致定位)。

【0134】 關於圖1至圖9所描述的程序之一者、一些或全部可各由軟體實施,但亦可實施於硬體、韌體或軟體、硬體與韌體之任何組合內。亦可將用於執行此等程序之指令體現為記錄於機器或電腦可讀取媒體上之機器或電腦可讀取程式碼。在一些實施例中,該電腦可讀取媒體可係非暫時性電腦可讀取媒體。此一非暫時性電腦可讀取媒體之實例包括但不限於:唯讀記憶體、隨機存取記憶體、快閃記憶體、CD-ROM、DVD、磁帶、可移除式記憶卡及資料儲存裝置(例如,圖2之記憶體104及/或記憶體模組150)。在其他實施例中,該電腦可讀

取媒體可係暫時性電腦可讀取媒體。在此等實施例中，暫時性電腦可讀取媒體可分佈於網路耦接式電腦系統上，以使得以分散式方式儲存及執行電腦可讀取程式碼。例如，可使用任何合適的通訊協定將此一暫時性電腦可讀取媒體自一電子裝置傳達至另一電子裝置（例如，可經由通訊組件106（例如，作為應用程式103之至少一部分及/或作為應用程式113之至少一部分及/或作為應用程式143之至少一部分）將電腦可讀取媒體傳達至電子裝置100）。此一暫時性電腦可讀取媒體可以將電腦可讀程式碼、指令、資料結構、程式模組或其他資料體現於經調變之資料信號（諸如，載波或其他輸送機制）中，且可包括任何資訊遞送媒體。經調變之資料信號可係具有其特性集之一或多者的信號或以將資訊編碼於信號中之方式經變化的信號。

【0135】 應理解，系統1之任何、每一或至少一模組或組件或子系統可提供為軟體建構、韌體建構、一或多個硬體組件或其組合。例如，可於可由一或多個電腦或其他裝置執行的電腦可執行指令（諸如，程式模組）之大致內容脈絡中描述系統1之任何、每一或至少一模組或組件或子系統。大致上而言，一程式模組可包括可執行一或多個特定任務或可實施一或多個特定抽象資料類型之一或多個常式、程式、物件、組件、及/或資料結構。亦應理解，系統1之模組及組件及子系統的數目、組態、功能性及互連僅為闡釋性，且可修改或省略現有模組、組件及/或子系統的數目、組態、功能性及互連，可新增額外模組、組件及/或子系統，且可更改某些模組、組件及/或子系統之互連。

【0136】 系統1之模組或組件或子系統中之一或多者的至少一部分可依任何合適方式儲存於系統1之實體中或以其他方式可為系統1之實體所存取（例如，在裝置100之記憶體104中（例如，作為應用程式應用程式103之至少一部分

及/或作為應用程式113之至少一部分及/或作為應用程式143之至少一部分））。例如，NFC組件120之任何或各模組可使用任何合適的技術來實施（例如，作為一或多個積體電路裝置），且不同模組在結構、能力及操作上可相同或可不相同。系統1之模組或其他組件中之任何者或全部可安裝於一擴充卡上，直接安裝於一系統主機板上，或整合至一系統晶片組組件中（例如，至「北橋」晶片中）。

【0137】 系統1之任何或每一模組或組件（例如，NFC組件120之任何或每一模組）可係使用經調適用於各種匯流排標準之一或多個擴充卡所實施的專用系統。例如，所有模組可安裝於不同的互連擴充卡上，或所有模組可安裝於一擴充卡上。關於NFC組件120，僅舉實例，可透過擴充槽（例如，周邊組件互連（「PCI」）槽或 快速周邊組件互連(PCI Express)槽）使NFC組件120之模組與裝置100之主機板或處理器102介接。替代地，NFC組件120無需為可移除式，而是可包括一或多個專用模組，該一或多個專用模組可包括專用於模組之利用的記憶體（例如，RAM）。在其他實施例中，NFC組件120可整合至裝置100中。例如，NFC組件120之模組可利用裝置100之裝置記憶體104的一部分。系統1之任何或每一模組或組件（例如，NFC組件120之任何或每一模組）可包括自己的處理電路系統及/或記憶體。替代地，系統1之任何或每一模組或組件（例如，NFC組件120之任何或每一模組）可與NFC組件120之任何其他模組及/或裝置100之處理器102及/或記憶體104共用處理電路系統及/或記憶體。

【0138】 本揭露認知到，在本技術中，此類個人資訊資料之使用可用來對使用者有益。例如，可使用個人資訊資料來遞送使用者較關注的經定目標內容。據此，使用此類個人資訊資料實現所遞送之內容的經計算控制。進一步，本揭露亦設想有益於使用者的個人資訊資料之其他用途。

【0139】 本揭露進一步設想，負責此類個人資訊資料之收集、分析、揭露、傳送、儲存、或其他使用的實體將遵循經妥善制定之隱私權政策及/或隱私權作法。具體而言，此類實體應實施及一致地使用一般認知為符合或超過產業或政府對維持個人資訊資料隱私及安全之要求的隱私權政策及隱私權作法。例如，應收集來自使用者的個人資訊以供實體合法且合理使用且不分享或出售而超過彼等合法使用。進一步，此類收集應僅發生在接收到使用者的知情同意(informed consent)之後。此外，此類實體將採取任何必要步驟來保障並保護存取此類個人資訊資料的安全，並且確保可存取個人資訊資料的其他者遵守其等之隱私權政策及程序。進一步，可由第三方評鑑此類實體本身，以認證該等實體遵守廣泛接受之隱私權政策及隱私權作法。

【0140】 儘管有前述內文，本揭露亦設想其中使用者選擇性封鎖對個人資訊資料之使用或存取的實施例。即，本揭露設想，可提供硬體及/或軟體元件以防止或封鎖對此類個人資訊資料之存取。例如，在廣告遞送服務之情況中，本技術可經組態以允許使用者在註冊服務期間選擇「加入」或「退出」參與個人資訊資料之收集。在另一實例中，使用者可選擇不對經定目標之內容遞送服務提供地點資訊。在又另一實例中，使用者可選擇不提供精確地點資訊，但是准許傳送定位區(location zone)資訊。

所描述概念之進一步應用

【0141】 雖然已描述用於驗證對安全裝置功能性之線上存取之系統、方法及電腦可讀取媒體，但應理解，可在不背離本文中所描述之標的之精神及範疇的情況下以任何方式在其中作出許多改變。明確設想如由所屬技術領域中具有

通常知識者所見、現在已知或之後設計的對所主張標的物之非實質改變等效地屬於申請專利範圍之範疇內。因此，所屬技術領域中具有通常知識者現在已知或之後已知的明顯替代案係界定為屬於所定義元件之範疇內。

【0142】 因此，所屬技術領域中具有通常知識者應理解，本發明可藉由不同於所描述實施例之實施例實踐，所描述實施例出於說明而非限制之目的而呈現。

【符號說明】

【0143】

- 1 系統
- 5 非接觸式之以接近性為基礎之通訊；通訊
- 15 通訊路徑；路徑
- 25 通訊路徑；路徑
- 35 通訊路徑；路徑
- 45 通訊路徑；路徑
- 55 通訊路徑；路徑
- 65 通訊路徑；路徑
- 75 通訊路徑；路徑
- 85 通訊路徑；路徑
- 100 電子裝置
- 101 外殼
- 102 處理器；處理器組件

- 103 應用程式；作業系統應用程式；裝置應用程式
- 103a 卡管理精靈(「CMD」)應用程式
- 103b 卡管理應用程式；裝置應用程式
- 103c 識別服務(「IDS」)應用程式
- 104 記憶體組件；記憶體
- 106 通訊組件
- 108 電源供應器組件；電源供應器
- 110 輸入組件
- 110a 輸入組件；使用者輸入組件；機械輸入組件
- 110b 輸入組件；使用者輸入組件
- 110c 輸入組件；使用者輸入組件
- 110d 輸入組件；使用者輸入組件
- 110e 輸入組件；使用者輸入組件
- 110f 輸入組件；使用者輸入組件；觸控輸入組件；觸控螢幕輸入組件；
- 110g 輸入組件；音訊輸入組件；使用者輸入組件
- 110h 輸入組件；攝影機及/或掃描器輸入組件；使用者輸入組件
- 110i 輸入組件；生物特徵輸入組件；使用者輸入組件
- 112 輸出組件
- 112a 輸出組件；顯示輸出組件
- 112b 輸出組件；音訊輸出組件
- 112c 輸出組件；觸感或觸覺輸出組件

- 113 線上資源或商家應用程式；第三方商家應用程式；網際網路應用程式；
PSP線上資源；網站商家線上資源；商家資源；商家線上資源應用程式
- 114 I/O介面；I/O組件
- 114a 觸控螢幕I/O組件；I/O介面組件；I/O介面；使用者I/O介面；I/O組件
- 114b I/O組件
- 114c I/O組件
- 114d I/O組件
- 115i I/O輸入資料
- 115o I/O輸出資料
- 116 天線
- 118 匯流排
- 119 裝置識別資訊或裝置識別符
- 120 近場通訊(NFC)組件
- 121 標記或符號
- 130 NFC裝置模組
- 132 NFC資料模組
- 134 NFC天線；NFC收發器
- 136 NFC加強器
- 140 NFC控制器模組
- 142 NFC處理器模組
- 143 NFC低功率模式或錢包應用程式
- 145 安全元件

- 150 NFC記憶體模組
- 151 非接觸式登錄服務(「CRS」)小程式或應用程式
 - 151k CRS存取金鑰
 - 151t CRS清單
- 152 發行方安全性網域(「ISD」)
- 153 小程式；認證小程式
 - 153a 認證小程式；小程式
 - 153b 存取小程式；小程式
- 154 補充安全性網域(「SSD」)
 - 154a 第一SSD；認證SSD
 - 154b 第二SSD；存取SSD
- 155 金鑰；管理員金鑰
 - 155a 存取金鑰；金鑰；存取資訊
 - 155a' 認證金鑰
 - 155aa 應用程式識別符(「AID」)
 - 155ak 金鑰
 - 155b 存取金鑰；金鑰
 - 155b' 認證金鑰
 - 155ba 應用程式識別符(「AID」)
 - 155bk 金鑰
- 156k 發行方安全性網域(ISD)金鑰
- 157 商家金鑰；私密金鑰；商家私密金鑰；公開及私密商家金鑰

- 158 控制授權單位安全性網域(「CASD」)
- 158k CASD存取套件
- 161a 認證資訊；資訊
- 161b 認證資訊；資訊
- 167 唯一商家識別符；商家識別符(ID)；第一商家識別符；第二商家識別符
- 177 憑證
- 180 視覺或圖形使用者介面(「GUI」)
- 181 標記有「商家應用程式」文字指示符；文字指示符
- 182 圖形元素或圖示
- 183 圖示
- 184 圖示
- 190 第一畫面；畫面
- 190a 圖形使用者介面的實例畫面；畫面
- 190b 圖形使用者介面的實例畫面；畫面
- 190c 圖形使用者介面的實例畫面；畫面
- 190d 圖形使用者介面的實例畫面；畫面
- 200 商家（或處理）子系統
- 210 商家伺服器
- 220 商家終端機；商家付款終端機
- 299 健全處理子系統
- 300 收單銀行（或收單方）子系統；收單銀行
- 307a 資訊

- 307b 資訊
- 307c 資訊
- 307d 資訊
- 309 安全支付提示
- 310 第三方前端PSP子系統；PSP子系統；商家-合作夥伴PSP子系統
- 311 付款來源選擇提示
- 311a 付款選項識別符
- 311b 付款選項識別符
- 312 虛擬連結表格
- 313 付款認證識別「認證X」資訊；認證識別符資訊
- 315 鑑認提示
- 317 確認資料
- 350 金融機構（或交易或發行方）子系統；使用者金融子系統
- 360 付款網路子系統；付款網路
- 370 發行銀行子系統；發行銀行
- 400 商業（或控管）實體子系統；商業實體
- 405 資料
- 410 伺服器
- 415 授權回應資料或交易狀態資料
- 420 商店組件；應用程式商店
- 430 表格
- 440 安全行動平台（「SMP」）代理人組件

- 450 SMP受信任服務管理員(「TSM」)組件
- 460 SMP密碼編譯服務組件
- 470 識別管理系統(「IDMS」)組件
- 480 詐騙系統組件；商業實體詐騙系統組件
- 490 硬體安全性模組(「HSM」)組件
- 495 通訊路徑
- 500 程序
- 501 步驟
- 502 步驟
- 504 步驟
- 506 步驟
- 508 步驟
- 510 步驟
- 512 步驟
- 514 步驟
- 516 步驟
- 518 步驟
- 520 步驟
- 522 步驟
- 600 程序
- 602 步驟
- 604 步驟

606 步驟

608 步驟

610 步驟

612 步驟

614 步驟

616 步驟

618 步驟

620 步驟

622 步驟

624 步驟

625 步驟

626 步驟

627 步驟

628 步驟

629 步驟

630 步驟

631 步驟

632 步驟

634 步驟

636 步驟

638 步驟

640 步驟

- 642 步驟
- 644 步驟
- 652 存取資料
- 654 認證資料
- 658 商家的資源；商家的線上資源
- 660 潛在交易資料；交易資料
- 662 商家線上資源驗證工作階段起始資料
- 664 查問請求資料
- 668 查問資料
- 670 查問回應資料
- 674 驗證回應資料
- 675 裝置付款認證資料
- 676 經加密裝置付款認證資料；裝置付款認證資料
- 677 安全裝置資料
- 678 裝置交易資料
- 681 經加密商家認證資料；商家認證資料
- 682 經保護安全之交易資料
- 684 以線上為基礎之通訊；經保護安全之交易資料
- 686 付款資料
- 688 授權請求資料
- 690 授權回應交易狀態資料
- 692 授權回應交易狀態資料

694 經確認之交易狀態資料

700 程序

702 步驟

704 步驟

706 步驟

708 步驟

710 步驟

712 步驟

714 步驟

800 程序

802 步驟

804 步驟

806 步驟

900 程序

902 步驟

904 步驟

906 步驟

908 步驟

910 步驟

912 步驟

914 步驟

D 距離



201732701

201732701

申請日：106/01/25

IPC分類：G06Q 20/22 (2012.01)
G06Q 20/08 (2012.01)
G06Q 20/38 (2012.01)

【發明摘要】

【中文發明名稱】 驗證對安全裝置功能性之線上存取

【英文發明名稱】 VALIDATING ONLINE ACCESS TO SECURE DEVICE
FUNCTIONALITY

【中文】

提供用於驗證對安全裝置功能性之線上存取之系統、方法及電腦可讀取媒體，其可使用介於不同子系統之間的共用祕密與有限用途之驗證資料。

【英文】

Systems, methods, and computer-readable media for validating online access to secure device functionality are provided that may use shared secrets between different subsystems and limited use validation data.

【指定代表圖】 第1A圖

【代表圖之符號簡單說明】

- 1 系統
- 5 非接觸式之以接近性為基礎之通訊；通訊
- 25 通訊路徑；路徑
- 35 通訊路徑；路徑
- 45 通訊路徑；路徑
- 55 通訊路徑；路徑
- 65 通訊路徑；路徑
- 75 通訊路徑；路徑

85 通訊路徑；路徑

100 電子裝置

102 處理器；處理器組件

106 通訊組件

113 線上資源或商家應用程式；第三方商家應用程式；網際網路應用程式；PSP

線上資源；網站商家線上資源；商家資源；商家線上資源應用程式

119 裝置識別資訊或裝置識別符

120 近場通訊(NFC)組件

145 安全元件

151k CRS存取金鑰

155a 存取金鑰；金鑰；存取資訊

155a' 認證金鑰

155b 存取金鑰；金鑰

155b' 認證金鑰

156k 發行方安全性網域(ISD)金鑰

157 商家金鑰；私密金鑰；商家私密金鑰；公開及私密商家金鑰

158k CASD存取套件

161a 認證資訊；資訊

161b 認證資訊；資訊

167 唯一商家識別符；商家識別符(ID)；第一商家識別符；第二商家識別符

177 憑證

200 商家（或處理）子系統

210 商家伺服器

220 商家終端機；商家付款終端機

- 299 健全處理子系統
- 300 收單銀行（或收單方）子系統；收單銀行
- 310 第三方前端PSP子系統；PSP子系統；商家-合作夥伴PSP子系統
- 312 虛擬連結表格
- 350 金融機構（或交易或發行方）子系統；使用者金融子系統
- 360 付款網路子系統；付款網路
- 370 發行銀行子系統；發行銀行
- 400 商業（或控管）實體子系統；商業實體
- 405 資料
- 410 伺服器
- 415 授權回應資料或交易狀態資料
- 420 商店組件；應用程式商店
- 430 表格
- 652 存取資料
- 654 認證資料
- 658 商家的資源；商家的線上資源
- 660 潛在交易資料；交易資料
- 662 商家線上資源驗證工作階段起始資料
- 664 查問請求資料
- 668 查問資料
- 670 查問回應資料
- 674 驗證回應資料
- 677 安全裝置資料
- 678 裝置交易資料

682 經保護安全之交易資料

684 以線上為基礎之通訊；經保護安全之交易資料

686 付款資料

688 授權請求資料

690 授權回應交易狀態資料

692 授權回應交易狀態資料

694 經確認之交易狀態資料

【發明申請專利範圍】

【第1項】 一種用於使用一控管實體子系統以進行經由在一電子裝置上執行的一線上資源之介於一處理子系統與通訊耦接至該處理子系統之該電子裝置之間的一安全交易之方法，該方法包含：

在該控管實體子系統處：

接收對於該線上資源之一驗證請求，其中該驗證請求包含驗證請求資料；

使用該驗證請求資料及註冊資料來驗證該線上資源，其中在一開始於接收該驗證請求之前已使該註冊資料可供該控管實體子系統使用；

使驗證回應資料與該驗證請求資料之至少一部分相關聯；

在已驗證該線上資源之後，傳達該驗證回應資料至該電子裝置；

在傳達該驗證回應資料至該電子裝置之後，接收來自該電子裝置之裝置交易資料；

使用該驗證回應資料來驗證該裝置交易資料；及

在已驗證該裝置交易資料之後，基於該裝置交易資料來產生安全交易資料以供該處理子系統使用。

【第2項】 如請求項 1 之方法，其中：

該驗證請求資料包含一驗證工作階段識別符；且

該驗證回應資料及該驗證請求資料之該至少一部分之至少一者包含該驗證工作階段識別符。

【第3項】如請求項 2 之方法，其中該驗證工作階段識別符包含由該電子裝置產生之資料。

【第4項】如請求項 3 之方法，其中在該控管實體子系統處接收來自該處理子系統之該驗證請求。

【第5項】如請求項 2 之方法，其中該驗證工作階段識別符包含由該處理子系統產生之資料。

【第6項】如請求項 1 之方法，其中：

該驗證請求資料包含指示該線上資源之一處理識別符；

該註冊資料包含該處理識別符及介於該控管實體子系統與該處理子系統之間的一處理共用祕密；且

該驗證該線上資源包含使用該處理共用祕密自該驗證請求資料存取該處理識別符。

【第7項】如請求項 1 之方法，其中：

該驗證請求資料包含指示該線上資源之一處理識別符；

該驗證回應資料包含隨機資料；且

該使相關聯包含在該控管實體子系統處對照該處理識別符來儲存該隨機資料。

【第8項】如請求項 7 之方法，其中：

該註冊資料包含該處理識別符及介於該控管實體子系統與該處理子系統之間的一處理共用祕密；且

該產生該安全交易資料包含使用該處理共用祕密來加密該裝置交易資料之一部分。

【第9項】如請求項 7 之方法，其中該處理識別符包含經由該線上資源之介於該電子裝置與該處理子系統之間的一潛在交易所獨有的一驗證工作階段識別符。

【第10項】如請求項 7 之方法，其中該傳達該驗證回應資料至該電子裝置包含：

在該控管實體子系統處，運用介於該控管實體子系統與該電子裝置之間的一共用祕密來簽署該隨機資料；及

與該電子裝置共用經簽署的該隨機資料。

【第11項】如請求項 10 之方法，其中該驗證該裝置交易資料包含：判定該裝置交易資料包含該隨機資料。

【第12項】如請求項 7 之方法，其中：

該傳達該驗證回應資料至該電子裝置包含與該電子裝置共用該隨機資料及該處理識別符；且

該驗證該裝置交易資料包含判定該裝置交易資料之至少一部分係在該控管實體子系統處對照該處理識別符經儲存。

【第13項】如請求項 12 之方法，其中該對照該處理識別符來儲存該隨機資料包含：保持在該控管實體子系統處對照該處理識別符所儲存的該隨機資料達不超過一特定時間長度。

【第14項】如請求項 1 之方法，其中：

該驗證請求資料包含潛在交易識別資訊，該潛在交易識別資訊指示經由該線上資源之介於該電子裝置與該處理子系統之間的一潛在交易；

該驗證回應資料包含隨機資料；

該使相關聯包含在該控管實體子系統處對照該潛在交易識別資訊來儲存該隨機資料；

該傳達該驗證回應資料至該電子裝置包含與該電子裝置共用該隨機資料；

該裝置交易資料包含裝置交易識別資訊；且

該驗證該裝置交易資料包含：

判定該裝置交易資料包含該隨機資料；且

判定該裝置交易資料之該裝置交易識別資訊係在該潛在交易識別資訊之一臨限內。

【第15項】一種用於使用一控管實體子系統以實現經由在一電子裝置上執行的一線上資源之介於一處理子系統與通訊耦接至該處理子系統之該電子裝置之間的一安全交易之方法，該方法包含：

在該控管實體子系統處：

註冊該線上資源，其中該註冊包含建置介於該控管實體子系統與該處理子系統之間的一處理共用祕密；

接收對於該線上資源之一驗證請求，其中該驗證請求包含指示該線上資源之一處理識別符，且其中該驗證請求進一步包含經由該線上資源之介於該電子裝置與該處理子系統之間的一潛在交易所獨有的一驗證工作階段識別符；及

使用該驗證工作階段識別符及該處理共用祕密來驗證由該處理識別符所指示之該線上資源。

【第16項】 如請求項 15 之方法，其中該驗證包含：

產生隨機資料；

對照該驗證工作階段識別符來儲存該隨機資料；

使用該處理共用祕密來加密該隨機資料；

傳達經加密之該隨機資料至該處理子系統；

在傳達經加密之該隨機資料至該處理子系統之後，接收來自該處理子系統之查問回應資料；及

判定所接收之該查問回應資料之至少一部分係對照該驗證工作階段識別符經儲存。

【第17項】 如請求項 15 之方法，其中該驗證包含：

產生隨機資料；

使用該處理共用祕密來加密該隨機資料；

傳達經加密之該隨機資料至該處理子系統；

在傳達經加密之該隨機資料至該處理子系統之後，接收來自該處理子系統之查問回應資料；及

偵測所接收之該查問回應資料包含該隨機資料。

【第18項】 如請求項 17 之方法，其中該驗證進一步包含：在傳達該經加密隨機資料之前判定該線上資源之該註冊係有效的。

【第19項】 一種用於使用一控管實體子系統以進行經由在一電子裝置上執行的一線上資源之介於一處理子系統與通訊耦接至該處理子系統之該電子裝置之間的一安全交易之方法，該方法包含：

在該控管實體子系統處：

接收對於該線上資源之一驗證請求，其中該驗證請求包含驗證請求資料，且其中該驗證請求資料包含潛在交易識別資訊，該潛在交易識別資訊指示經由該線上資源之介於該電子裝置與該處理子系統之間的一潛在交易；

使用該驗證請求資料之至少一部分來驗證該線上資源；

使驗證回應資料與至少該潛在交易識別資訊相關聯；

在已驗證該線上資源之後，傳達該驗證回應資料至該電子裝置；

在傳達該驗證回應資料至該電子裝置之後，接收來自該電子裝置之裝置交易資料；

使用該驗證回應資料及該潛在交易識別資訊來驗證該裝置交易資料；及

在已驗證該裝置交易資料之後，基於該裝置交易資料來產生安全交易資料以供該處理子系統使用。

【第20項】 如請求項 19 之方法，其中：

該驗證回應資料包含隨機資料；

該使相關聯包含在該控管實體子系統處對照該潛在交易識別資訊來儲存該隨機資料；

該傳達該驗證回應資料至該電子裝置包含與該電子裝置共用該隨機資料；

該裝置交易資料包含裝置交易識別資訊；且

該驗證該裝置交易資料包含：

判定該裝置交易資料包含該隨機資料；且

判定該裝置交易資料之該裝置交易識別資訊係在該潛在交易識別資訊之一臨限內。

【第21項】 如請求項 19 之方法，其中：

該驗證該線上資源包含使用該驗證請求資料之該至少一部分及註冊資料；

在一開始於接收該驗證請求之前已使該註冊資料可供該控管實體子系統使用；

該註冊資料包含介於該控管實體子系統與該處理子系統之間的一處理共用祕密；且

該產生該安全交易資料包含使用該處理共用祕密來加密該裝置交易資料之一部分。

