

發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※ 申請案號：96124187

※ 申請日期：96 年 7 月 3 日

※IPC 分類：

一、發明名稱：(中文/英文)

智慧卡終端資料及管理框架

SMART CARD TERMINAL SIDE DATA AND MANAGEMENT
FRAMEWORK

G06F 17/00 (2006.01)

G06F 9/44 (2006.01)

H04B 7/26 (2006.01)

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

美商·微軟公司

Microsoft Corporation

代表人：(中文/英文)

艾華那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

住居所或營業所地址：(中文/英文)

美國華盛頓州列德蒙微軟路 1 號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, U.S.A.

國 籍：(中文/英文)

美國/USA

三、發明人：(共 1 人)

姓 名：(中文/英文)

麥首爾許法倫 H

MYSORE, SHIVARAM H.

國 籍：(中文/英文)

印度/India

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

美國；2006 年 7 月 14 日；11/486,578

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

智慧卡 (smart card) 係一種包括記憶體以及一處理器之電子卡，類似於一台電腦，用來儲存、接收以及傳輸資料。除了其較小的體積外，智慧卡更理想之處在於其能防竄改 (tamper resistant) 並使用一安全模型，從而使涉及機密之個人資料可以被安全承載與保存。因此其經常被用於身份識別、金融交易以及安全存取應用。其他的一些應用，如需要或可藉由安全處理以及資料儲存使其功能得以增強，也可以應用智慧卡。

智慧卡終端係一種裝置，其接收並閱讀智慧卡上包含之資料並由此得以進入智慧卡所儲存之應用。舉例言之，在一台金融智慧卡終端處使用一貨幣智慧卡，可允許將錢轉移到該智慧卡使用者之帳戶中，而將一身份證明智慧卡插入位於某一設備處之一台智慧卡終端中，可以使持該身份證明智慧卡之使用者存取此設備。

目前，對於包含有一或多種應用之智慧卡，終端對其應用進行識別時存在一些困難。終端可無法分辨出智慧卡應用所提供的介面和協定。識別問題為終端上應用造成困難。此外，智慧卡之安全模型在終端上沒有得以執行。因此，在終端上執行一智慧卡之安全模型，同時進一步允許終端可以獲取在運行智慧卡之應用時所需之訊息係有必要的。智慧卡以及智慧卡終端更需加強之處包括錯誤和使用管理之控制。

【發明內容】

智慧卡與智慧卡終端獲取該智慧卡上一種應用之相互操作係由資料及管理框架提供的。一種應用程式介面（API）可會被寫入資料及管理框架中，係智慧卡終端基礎設施之一部分。智慧卡終端之基礎設施能存取、處理並執行智慧卡上所包含之應用。API向終端提供與智慧卡應用相關之必要資料從而使終端產生相應之應用。接著，相應之終端應用可合併終端與智慧卡應用之間的相互操作、識別以及安全等資料。與智慧卡相關之安全模型與政策可以由智慧卡終端執行。

本「發明內容」意在以一種簡單形式介紹一些概念，這些概念將在「實施方式」中進一步描述。本「發明內容」並非為了指出申請專利範圍之標的物之重要特徵或必要特徵，也不是為了對申請專利範圍之標的物之範圍作出限制。

【實施方式】

根據第1圖，實現本發明之典型系統包括一採用電腦110之形式的通用計算裝置。電腦110之組件可包括，但不僅限於，一處理單元120，一系統記憶體130；以及一系統匯流排121，其用來將包括系統記憶體在內之不同組件與處理單元120連接起來。系統匯流排121可為幾種匯流排結構類型中任一匯流排結構，包括記憶體匯流排或記憶體控制器，一周邊匯流排以及一使用不同匯流排結構之區域匯流排。舉例而言，但不限於，這些結構包括工業標準

架構 (ISA) 匯流排，微通道架構 (MCA) 匯流排，增強工業標準架構 (EISA) 匯流排，視訊電子標準協會 (VESA) 區域匯流排，以及周邊組件設備互連 (PCI) 匯流排 (也被稱為 Mezzanine 匯流排)

電腦 110 一般包括多種電腦可讀媒體。電腦可讀媒體可包括電腦 110 可讀取之任何可用媒體，包括揮發性媒體與非揮發性媒體，可移動媒體與不可移動媒體。舉例而言，但並非僅限於，電腦可讀媒體可組成了電腦儲存媒體與通信媒體。電腦儲存媒體包括揮發性與非揮發性媒體，可移動與不可移動媒體，其以任意方式或技術儲存資料，這些資料包括電腦可讀指令，資料結構，程式模組或其他資料。電腦儲存媒體包括，但不僅限於，隨機存取記憶體、唯讀記憶體、可抹除可程式化唯讀記憶體、快閃記憶體或其他儲存技術、唯讀光碟、數位多功能光碟 (DVD) 或其他光學磁碟記憶體、磁性卡匣、磁帶、磁碟儲存或其他磁性儲存裝置，或其他可以儲存所需訊息並可以由電腦 110 讀取之任何媒體。通信媒體一般包括電腦可讀指令，資料結構，電腦程式模組或其他包含在一調變數位信號中之資料，例如，一載波或其他傳輸裝置，其還包括任何資料傳輸媒體。「調變資料訊號」是指一信號，其具有以此一方式被設定或改變的一或更多特徵，從而在信號中將資料編碼。舉例而言，但不僅限於，通信媒體包括有線媒體，例如有線網路或直接有線連接，其還包括無線媒體，例如聲學、無線電射頻 (RF)、紅外線以及其他無線媒體。上述之任意組合

也應包括在電腦可讀媒體之範圍內。

系統記憶體 130 包括揮發性及/或非揮發性電腦儲存媒體，例如唯讀記憶體 131 和隨機存取記憶體 132。在唯讀記憶體 131 中存在一基本輸入輸出系統 133 (BIOS)，其包括基本例式，例如，在啟動期間，幫助在電腦 110 組件範圍內傳輸資訊。隨機存取記憶體 132 一般包括資料及/或程式模組，其可以實時由處理單元 120 讀取及/或馬上由處理單元 120 進行操作。舉例而言，但不僅限於，第 1 圖描述了一作業系統 134，應用程式 135，其他程式模組 136 以及程式資料 137。

電腦 110 亦可包括其他可移動/不可移動，揮發性/非揮發性電腦儲存媒體。僅舉例而言，第 1 圖描述了一硬式磁碟機 141，其讀寫非移動、非揮發性之磁性媒體，一磁碟機 151，其讀寫一可移動、非揮發性磁碟 152，以及一光碟機 155，其讀寫一可移動、非揮發性光碟 156，例如唯讀光碟或其他光學媒體。其他可用於該實施例中操作環境之可移動/不可移動，揮發性/非揮發性電腦儲存媒體包括，但不僅限於，磁性卡帶匣，快閃記憶體，數位化多功能光碟，數位化視訊帶，固態隨機存取記憶體，固態唯讀記憶體等。硬式磁碟機 141 一般藉由一不可移動記憶體介面，例如介面 140，連接至系統匯流排 121，而磁碟機 151 與光碟機 155 一般藉由一可移動記憶體介面，例如介面 150，連接至系統匯流排 121。

在上述討論中提及與在第 1 圖中描述之驅動器以及其

他相關之電腦儲存媒體，為電腦 110 提供電腦可讀指令，資料結構，組件，程式模組以及其他資料。在第 1 圖中，例如，硬式磁碟機 141 被描述為儲存作業系統 144，應用程式 145，其他程式模組 146，以及程式資料 147。需要注意的是，這些組件與作業系統 134，應用程式 135，其他程式模組 136 以及程式資料 137 或相同或不同。作業系統 144，應用程式 145，其他程式模組 146，以及其他程式資料 147 都被給與不同編號，以用來表明他們至少是不同副本。使用者可以藉由輸入裝置例如鍵盤 162 以及指示裝置 161，一般為滑鼠、軌跡球或觸控板。其他輸入裝置（沒有展示）可包括麥克風，操縱桿，遊戲手把，衛星天線，掃描器等。上述及其他一些輸入裝置一般藉由使用者輸入介面 160 接入處理單元 120，該介面與系統匯流排連接，但可是由其他介面或匯流排結構連接的，例如並行埠，遊戲埠或通用串列匯流排架構(USB)。一監視器 191 或其他類型之顯示器也藉由一介面，例如視訊介面 190，連接在系統匯流排 121 上。除監視器外，電腦也可以包括其他一些輸出裝置，例如麥克風 197 和印表機 196，它們也可以藉由周邊輸出介面 195 連接。

電腦 110 也可以在網路環境中操作，使用邏輯連接與一或多個遠端電腦連接，例如一遠端電腦 180。遠端電腦 180 可是一個人電腦，一伺服器，一路由器，一網路個人電腦，一點對點裝置或其他常見網路節點，其一般包含多數或所有上面所描述之電腦 110 所包含之組件，儘管在第

1 圖中對其描述僅包含有一記憶體儲存裝置 181。所描述之邏輯連接包括區域網路 (LAN) 171, 廣域網路 (WAN) 173, 但也可包含其他網路。這些網路環境在辦公室、企業範圍電腦網路、企業內部網路以及網際網絡中是很常見的。

當在區域網路環境中使用時, 電腦 110 藉由一網路介面或配接器 170 與區域網路 171 連接。當在廣域網路環境中使用時, 電腦 110 一般包括一數據機 172 或其他方式與廣域網路 173 建立聯繫, 例如網際網路。數據機 172, 可為內置或外置, 其可以藉由使用者輸入介面 160 或其他適當之機械裝置與系統匯流排 121 連接。在網路環境中, 與電腦 110 相對應之程式模組或其一部分將被儲存在遠端記憶體儲存裝置中。舉例而言, 但不僅限於, 第 1 圖描述了在儲存於記憶體裝置 181 中之遠端應用程式 185。需要引起重視的是, 所描述之網路連接是作為例證, 其他在電腦之間建立通信之連接也可以被應用。

所有或部分在此處描述之方法可以作為硬體、軟體或二者兼有之實施例。當軟體方面具體實施時, 這些方法或其中的一方面或一部分, 在被電腦系統執行時以編碼之方式實現。這一程式編碼可以被儲存在上述提到之任何電腦可讀媒體中。

一智慧卡終端係一裝置, 其讀取並處理儲存在一智慧卡上之應用, 而智慧卡係一電子卡, 其包含有記憶體與處理器。智慧卡可與電腦類似, 其執行儲存、處理、接收以及傳輸資料等功能。一智慧卡可包含一種或多種應用, 這

些應用可以被智慧卡終端讀取進行處理。

在第 2 圖中描述一智慧卡終端 200 實施例。智慧卡終端 200 可包括一電腦，例如電腦 110，一監視器 191 或其他類型之顯示裝置，以及一智慧卡讀卡機 210。讀卡機 210 作為電腦 110 與智慧卡（例如第 2 圖中所示之智慧卡 220）間之介面，因此，電腦可以讀取並處理智慧卡 220 之應用 230。

智慧卡讀卡機 210 可為一感應或無須接觸 (contact-less) 的智慧卡讀卡機 210，智慧卡讀卡機在讀取智慧卡 220 時，無須與智慧卡 220 有任何直接接觸。舉例而言，當智慧卡 220 被放置於感應智慧卡讀卡機附近時，感應智慧卡讀卡機 210 可以讀取智慧卡 220。在一實施例中，ISO14443 標準可以被用來明確規定感應智慧卡 220 以及感應智慧卡讀卡機 210 與其他符合 ISO14442 標準之卡 220 以及讀卡機 210 之相容性。根據該標準，感應智慧卡讀卡機 210 係一射頻識別 (RFID) 讀卡機，其包括一嵌入式微控制器以及一磁性迴路天線，用來讀取智慧卡 220。磁性迴路天線的使用頻率為 13.56MHz。如果智慧卡距離讀卡機在四英吋範圍內，感應智慧卡讀卡機 210 可以讀取感應智慧卡 210。此外，ISO14443 標準包括四個部分：(i) 物理特性；(ii) 射頻頻率功率以及信號介面；(iii) 初始化與防撞擊；以及 (iv) 傳輸協定。

替代地，智慧卡讀卡機 210 也可係一可插入式智慧卡讀卡機 210。如果智慧卡讀卡機 210 係可插入式之一種，

那麼當智慧卡 220 或智慧卡 220 的一部分插入智慧卡讀卡機 210 後，智慧卡讀卡機 210 可以讀取智慧卡 220 上之應用 230。ISO7816 係一已制定標準，其與接觸型智慧卡相關，例如可插入式智慧卡 220。可插入式智慧卡 220 可是根據 ISO7816 標準設計的，該 ISO7816 標準包含與在智慧卡 220 以及讀卡機 210 之間傳輸訊息、命令、回應有關的準則；存取智慧卡 220 中之檔案與內容之方法；以及安全通信之方法等。其他類型智慧卡讀卡機 210 也可以被使用，對感應智慧卡讀卡機或可插入型智慧卡讀卡機沒有限制。

智慧卡 220 可包含一種或多種應用 230。舉例言之，如第 2 圖所示，智慧卡 220 包含四種應用 230：EMV (Europay, MasterCard, VISA)，GSCIS/PIV，入侵監測以及帳戶管理中心。其他應用 230 以及應用 230 之數目都是存在可性的。此外，智慧卡 220 可包括不相關之應用 230 及/或取而代之，包括同一應用 230 之多種變化。應用 230 之任意組合都有可包含在智慧卡 220 內。

根據一實施例之智慧卡終端基礎設施 300 在第 3 圖中顯示。智慧卡終端基礎設施 300 運作以存取、處理以及執行智慧卡 220 之應用 230。此外，基礎設施 300 有慮及錯誤狀況及使用模型之管理。

智慧卡終端基礎設施 300 可包括多種方式，裝置，軟體，及/或硬體來執行功能，包括終端應用 305；一資料與控制框架 310；一加密之安全組件 320；一額外加密之安全

組件 325；一以智慧卡為基礎之加密伺服器設備 330；一智慧卡金鑰記憶體設備 335；一或多個智慧卡模式 340（例如所示 340a-d 智慧卡模式）；一智慧卡資源管理器 345；一 PC/SC-winscard.h 350；及一或多個讀卡機驅動器 355（例如讀卡機驅動器 355a 以及 355b）。

加密之安全組件 320 允許開發者對應用（例如終端應用 305）添加加密安全。加密之安全組件 320 允許在安全環境中在非安全媒體中，例如網際網路中，建立及交換檔案以及其他資料。額外之安全組件 325 可以提供與加密安全組件 320 類似但經過加強之功能。在一典型並無限制之實施例中，加密安全組件 320 可為一加密應用程式介面。在另一典型並無限制之實施例中，加密安全起見 325 可為 CNG，或下一代加密應用程式介面。

以智慧卡為基礎之加密伺服器設備 330 可以通過智慧卡模組 340 與個別智慧卡，例如智慧卡 220，進行通信操作。以智慧卡為基礎之加密伺服器設備 330 可包括加密標準及演算法之執行以保證加密安全。以智慧卡為基礎之伺服器設備 330 可包括一動態連結程式庫（DLL），其可在作業系統以及以智慧卡為基礎之加密伺服器設備 330 之間作為通信設備執行功能與服務。

智慧卡模組 340 藉由通過智慧卡資源管理器 345 與該等智慧卡通信之方式，將智慧卡之特性轉化成一用於智慧卡終端介面基礎設施 300 之統一介面。智慧卡模組 340 可實作成一動態連結程式庫（DLL）。應智慧卡終端資料基礎

設施 300 之要求，智慧卡金鑰記憶體設備 335 可執行金鑰儲存操作。

智慧卡資源管理器 345 可負責執行管理對智慧卡讀卡機 210 以及智慧卡 220 進行存取之任務。一些需要執行之功能可包括識別並追蹤資源；將資源與讀卡機跨越不同的應用進行配置；及交易基元(transaction primitives)之支援以存取在一給定智慧卡 220 上可用之服務。智慧卡資源管理器 345 可以直接被資源管理器 API 或智慧卡服務設備讀取。資源管理器 API 有一功能集合，其可提供對智慧卡管理器 345 之服務的直接存取。

智慧卡終端基礎設施 300 之資料與管理框架 310 協助開發與建立終端應用 305。終端應用 305 對智慧卡應用 230 做出回應。資料與管理框架 310 也可以管理在智慧卡終端 200 與智慧卡 220 之間通信時發生之錯誤狀況和使用模型。此外，資料與管理框架 310 也可為一應用程式介面(API)及，在一實施例中，可負責錯誤訊息對終端應用 305 之傳遞。根據一實施例之資料與管理框架 310 係如第 4 圖所示。

典型之資料與管理框架 310 包括多種構件、裝置、軟體及/或硬體來執行功能，其包括一介面組件 410、一錯誤狀況管理組件 420、一使用管理組件 430、一通信組件 440、一連接組件 450、及一終端政策組件 460。

介面組件 410 藉由獲得與智慧卡應用 230 相關之訊息，從而如一從智慧卡終端 200 到智慧卡應用 230 間之鏈

結般運作。與應用 230 相關之訊息可包括一介面及/或應用 230 之協定，其可協助終端 200 恰當地識別和存取智慧卡 220 之應用 230。此外，藉由讓終端 200 意識到該政策之存在與需求，此訊息可以用來執行智慧卡 220 之一政策。

一對應於智慧卡應用 230 之相應 API，可由例如智慧卡應用 230 之販賣者或開發者所建立，而且相應之 API 可由販賣者或開發者寫入到資料與管理框架 310。介面組件 410 可使用此相應之 API 來建立對應於智慧卡應用 230 之終端應用 305。

錯誤狀況管理組件 420 用來探測與智慧卡 220 使用之相關錯誤並在探測到錯誤之後，轉遞出一相應之錯誤訊息。錯誤訊息可會轉遞給通信組件 440。在智慧卡終端 200 嘗試存取智慧卡終端 220 上之資料時，可發生各種錯誤。舉例言之，智慧卡 220 可被不正確地插入智慧卡終端讀卡機 210。如果這個錯誤被錯誤狀況管理組件 420 探測到，錯誤會因此被轉遞給通信組件 440。在智慧卡終端 200 嘗試存取智慧卡 220 上所不包含之應用時。再次，錯誤狀況管理組件 420 可會探測到這個錯誤，並將在探測到錯誤後轉遞一恰當之錯誤訊息給通信組件 440。

使用管理組件 430 可執行與智慧卡 220 相關之使用政策。在一實施例中，智慧卡 220 之使用政策係安全模型。使用政策可被包含在與智慧卡應用相關之訊息內，並可因此被併入相應之 API 寫入資料與管理框架 310。舉例而言，使用政策可依賴於群組政策設定、本地機器政策設定或應

用政策設定。使用政策可由使用管理組件 430 執行，其可以獲得使用政策並監督智慧卡 220 及其應用 230 之使用狀況。如所定義之使用政策被違背，那麼使用管理組件會拒絕正在進行之嘗試來執行政策。此外，使用管理組件 430 在探測到與智慧卡 220 相關之違背使用政策訊息時，可會轉遞使用訊息給通信組件 440，該訊息有可是一違背訊息。

通信組件 440，用來在智慧卡 220 與智慧卡終端 200 之間進行通信，其可為一資料與管理框架 310 之進一步特徵。正如前述，錯誤狀況管理組件 420 與使用管理組件 430 都可向通信組件 440 轉遞訊息。接受到之訊息可包括一錯誤探測、一使用政策違背或另一種類型之通信。如果錯誤狀況管理組件 420 探測到與智慧卡 220 使用有關之錯誤並向通信組件 440 發出該錯誤之指示，通信組件 440 可將錯誤訊息顯示在智慧卡終端 200 之監視器 191 上。錯誤訊息可包括給智慧卡 220 以及終端 200 使用者之指令。通信組件 440 可進一步顯示由使用管理組件 430 報告之與智慧卡相關之違背使用政策之指示。這項指示也可被顯示在監視器 191 上。

通信組件 440 在接受到錯誤狀況或使用違例之指示後，可建立一錯誤或違例日誌入口。舉例言之，通信組件 440 可發送一訊息給一應用，以便對該應用提供錯誤狀況或使用違例之指示。被發送給該應用之訊息可，舉例言之，發出一種聲音或音調來當作提示訊息已經發出的警示。

在一實施例中，資料與管理框架 310 可也包括連接組

件 450，在沒有錯誤被探測到及/或使用政策得到執行情況下，其作為智慧卡應用 230 與相應終端應用 350 之間的通道。所建立之通道在終端 200 與智慧卡 220 之間可為一安全通道。

為了在處理智慧卡應用 230 時將額外之政策及/或限制併入，終端政策組件 460 可被包含在資料與管理框架 310 中。舉例言之，終端應用 305 之開發者可希望建立在終端 200 使用上對於一特定應用 230 之一時間限制。額外之政策及/或限制可被併入。

第 5 圖描述了一實施例，即在智慧卡終端應用 305 與智慧卡 220 上之智慧卡應用 230 之間相互操作方法。該相互操作方法可由一智慧卡終端應用開發者實行，以便讓該終端應用 305 能與位於智慧卡 220(其插入於智慧卡終端讀卡機 210 中)上的智慧卡應用 230 無縫地操作。

在 505 中，獲取一寫入智慧卡終端 200 資料與管理框架之 API。API 對智慧卡應用 230 做出回應。為了建立相應之終端應用 305，則使用與智慧卡應用 230 相關之資料。在 510 中，該資料從 API 獲得。與智慧卡應用相關資料可包含，但不僅限於，該智慧卡應用 230 之一介面、由該智慧卡應用 230 所使用之一協定，及該智慧卡應用 230 之一安全模型。在 515 中，所獲得與智慧卡應用 230 有關之資料，舉例而言，由資料與管理框架 310 之介面組件 410 將其併入至該對應於智慧卡應用 230 之終端應用 305 中。在藉由與智慧卡應用 230 相關之資料併入而使終端應用 305

得以建立後，各種補充的與可選的資料與管理操作可由該資料與管理框架 310 所實行。

在 520 中，智慧卡 220 之安全模型可被執行，該安全模型可作為與智慧卡應用 230 相關資料之一部分所獲取。在 525 中，執行操作可進一步在終端 200 上監視智慧卡 220 之使用情況。監視操作可與智慧卡 220 之安全模型或使用政策分析同步進行。在 530 中，藉由例如使用管理組件 430 執行一判斷，其目的在於確定該所監視到之使用是否違背安全模型。在 535 中，如果安全模型被違背，那麼一違背訊息將被轉遞。違背訊息可藉由在一顯示裝置顯示一訊息來轉遞，例如在監視器 191 上藉由建立一違背日誌入口或舉例言之，藉由對一應用傳輸訊息。舉例言之，轉遞給應用之訊息可製造一聲音或音調來當作告知訊息已發送之通知。轉遞錯誤訊息之任意組合都可被執行。

在違背訊息被轉遞之後，該方法可會回到 525 進一步監視智慧卡 220 之使用。如果，正如 530 處所判斷，模式沒有被違背，將會進行進一步的判斷以確定安全模型是否會在較遲之時間被違背。

在 540 處，在 520 及/或 530 後，如果智慧卡 220 沒有違背安全模型，在智慧卡 220 與智慧卡終端 200 之間可建立一安全通道。通道可在智慧卡 220 之安全模型被執行之後及/或在判斷安全模型沒有被違背之後建立，其目的是為了使智慧卡 220 與終端 200 之間安全通信並執行智慧卡 220 之功能。舉例言之，在資料與管理框架 310 判斷先前

定義之安全模型沒有被違背之後，安全通信通道藉由，例如連接組件 450，被建立。

在 545 中，智慧卡終端應用可被設定為進一步定義終端政策及/或終端限制。終端政策組件 460 可執行該設定，用來在智慧卡 220 及/或處理智慧卡應用 230 之過程中建立並併入額外政策及/或限制。如果判斷智慧卡 220 之安全模型尚未被違背，該設定可在 520，530 及/或 540 之後進行。

第 6 圖描述了一實施例，即在一智慧卡終端 200 上執行一智慧卡 220 之安全模型。在 610 中，從終端基礎設施 300 之資料與管理框架 310 中獲取智慧卡 220 之安全模型。從資料與管理框架 310 中獲取安全模型之步驟可包括讀取一被應用於或被寫入到資料與管理框架 310 中之 API。智慧卡終端基礎設施 300 之資料與管理框架 310 可協助終端應用 305 之開發與建立。終端應用 305 對應於一智慧卡應用 230。

在 615 中，安全模型被併入智慧卡終端應用 305 中，後者被開發的目的是對應於該智慧卡應用 230。在 620 中，執行一項判斷來確定是否有錯誤狀況被探測到，該錯誤狀況可是由安全模型定義的。這一探測可被週期性地或連續性地被執行以發現錯誤狀況。在 625 中，在探測到錯誤狀況 620 後，一對應於所探測到之錯誤狀況的錯誤訊息被傳輸。錯誤狀況管理組件 420 可執行錯誤狀況之探測，而且可在探測到錯誤時，傳輸通知給通信組件 440。舉例言之，通信組件 440 可藉由在一顯示裝置(像是監視器 191)上顯

示訊息、建立一錯誤日誌入口或藉由對一應用傳輸訊息之方式來轉遞該錯誤訊息。舉例言之，轉遞給應用之訊息可製造一聲音或音調來當作告知訊息已發送之通知。轉遞錯誤訊息之任意組合都可被執行。

需要理解的是，所描述之實施例可在一或多個電腦系統或裝置中作為一個整體或一部分被執行。第 1 圖描述的是一可被實現或實踐之具體實施例，其為一電腦系統 100 之功能性組件。如這裡所使用到的，術語“計算系統”，“電腦系統”以及“電腦”指由一可執行或可處理程式編碼或資料之處理器組成之任何機器、系統或裝置。計算系統之典型例包括，但不僅限於，個人電腦（PCs）、微電腦、大型電腦、精簡型電腦、網路個人電腦、伺服器、工作站、膝上型電腦、手持型電腦、可程式化消費性電子產品、多媒體平台、遊戲平台、衛星接收器、機上盒、自動對講機、大型電玩、行動電話、個人數位助理（PDAs）以及任何其他以處理器為基礎之系統或機器。術語“程式編碼”或“編碼”是指被執行或被處理器處理之任意指令之組合。程式編碼及/或資料可以由執行特定功能之例式、程式、物件、模組、資料結構等形式來執行。

需要注意的是，前述之實施例意在提供解釋說明，絕不能被認為是限制。由於在描述本發明的過程中用到各種具體實施例，因此需要瞭解的是這裡所用到的詞彙僅是為了描述與例證，而並非為限制性詞彙。此外，儘管這裡所描述之實施例是關於特定的構件、材料以及範例，但這些

具體實施例並非只侷限於這裡所提到的；更確切地說，具體實施例延伸到隨附之申請專利範圍內所有功能上相當之結構、方法以及用途。

【圖式簡單說明】

與隨附圖式結合起來，前述之概述以及後述之具體描述可以更好地被理解。在隨附圖式中展示了典型實施例，但是需要理解的是實施例並不侷限於這裡所描述之方法與手段。在這些圖式中：

第 1 圖係一結構圖，其代表一典型電腦裝置；

第 2 圖係一結構圖，其代表一典型智慧卡終端；

第 3 圖係一結構圖，其代表一典型智慧卡終端基礎設施；

第 4 圖係一結構圖，其代表一資料及管理框架；

第 5 圖係一流程圖，其描述了一實施例，即在一智慧卡終端應用與於智慧卡上之應用之間的相互操作性方法；以及

第 6 圖係一流程圖，其描述了一實施例，即在智慧卡終端上執行一智慧卡之安全模型的方法。

【主要元件符號說明】

100 計算環境

110 電腦

120 處理單元

121 系統匯流排

130 系統記憶體

- 131 唯讀記憶體
- 132 隨機存取記憶體
- 133 基本輸入輸出系統
- 134 作業系統
- 135 應用程式
- 136 其他程式模組
- 137 程式資料
- 140 不可移動非揮發性記憶體介面
- 141 硬式磁碟機
- 144 作業系統
- 145 應用程式
- 146 其他程式模組
- 147 程式資料
- 150 可移動非揮發性記憶體介面
- 151 磁碟機
- 152 可移動非揮發性磁碟
- 155 光碟機
- 156 可移動非揮發性光碟
- 160 使用者輸入介面
- 161 滑鼠
- 162 鍵盤
- 170 網路介面
- 171 區域網路
- 172 數據機

173	廣域網路
180	遠端電腦
181	記憶體儲存裝置
185	遠端應用程式
190	視訊介面
191	監視器
195	周邊輸出介面
196	印表機
197	揚聲器
200	智慧卡終端
210	智慧卡讀卡機
220	智慧卡
230	應用
300	智慧卡終端基礎設施
305	終端應用
310	資料與管理框架
320	加密安全組件
325	額外加密安全組件
330	基於智慧卡之加密服務設備
335	智慧卡金鑰儲存設備
340a	卡片模組
340b	卡片模組
340c	卡片模組
340d	卡片模組

345 智慧卡資源管理器

350 PC/SC-winscard.h

355a 個人電腦/智慧卡讀卡機驅動

355b 個人電腦/智慧卡讀卡機驅動

310 資料與管理框架

410 介面組件

420 錯誤狀況管理組件

430 使用管理組件

440 通信組件

450 連接組件

460 終端政策組件

五、中文發明摘要：

茲提供一智慧卡終端功能之一資料與管理框架，其係提供智慧卡終端與智慧卡之間的相互操作性，尤其是終端應用與智慧卡應用之間。一應用程式介面（API）被寫入至該資料與管理框架，該資料與管理框架係智慧卡終端基礎設施之一部分，其可由智慧卡終端所讀取並處理在智慧卡上所包含之應用。API向終端提供與智慧卡應用相關之資料，其目的在於允許一相應終端應用以整合該訊息，從而使這兩種應用進行通信。此外，一與智慧卡相關之安全模型與政策可由智慧卡終端執行。

六、英文發明摘要：

A data and management framework of a smart card terminal functions to provide interoperability between the smart card terminal and a smart card, and in particular between applications of the terminal and the card. An application program interface (API) is written to the data and management framework, which is part of a smart card terminal infrastructure that accesses and processes, by the smart card terminal, a smart card application contained on the smart card. The API provides information related to the smart card application to the terminal in order to allow a corresponding terminal application to incorporate the information for communication between the two applications. Additionally, a security model and policies related to the smart card may be enforced by the smart card terminal.

十、申請專利範圍：

1. 一種用於智慧卡終端之智慧卡終端基礎設施，該智慧卡終端基礎設施包括：

一資料與管理框架，其中該框架包括：

一介面組件，用來獲取一智慧卡上與一智慧卡應用相關之資料；

一錯誤狀況管理組件，用來探測智慧卡之一錯誤；

一使用管理組件，用來執行一與智慧卡相關之使用政策；及

一通信組件，用來在智慧卡與智慧卡終端之間進行通信。

2. 如申請專利範圍第1項所述之智慧卡終端基礎設施，其中該資料與管理框架係一應用程式介面（API）。

3. 如申請專利範圍第1項所述之智慧卡終端基礎設施，其中該智慧卡上與智慧卡應用相關之資料至少包括（i）該智慧卡應用之一介面；（ii）由該智慧卡應用所使用之一政策；及（iii）該智慧卡之一安全模型。

4. 如申請專利範圍第1項所述之智慧卡終端基礎設施，更包括：

一智慧卡模組，用來對該資料與管理框架提供該智慧卡上與智慧卡應用有關之資料。

5. 如申請專利範圍第4項所述之智慧卡終端基礎設施，更包括：

一終端應用，其對應於該智慧卡應用並係從智慧卡上

與智慧卡應用相關之資料中所建立。

6. 如申請專利範圍第 1 項所述之智慧卡終端基礎設施，其中該錯誤狀況管理組件在探測到錯誤後進一步操作以轉遞 (relay) 一錯誤訊息給通信組件。

7. 如申請專利範圍第 6 項所述之智慧卡終端基礎設施，其中該通信組件藉由以下至少一種方式來轉遞該智慧卡終端之錯誤訊息：(i) 在一顯示裝置上顯示該錯誤訊息；(ii) 建立一對應於該錯誤訊息之日誌入口；及 (iii) 發送該錯誤訊息給一項應用。

8. 如申請專利範圍第 1 項所述之智慧卡終端基礎設施，其中該使用管理組件在探測到違背與智慧卡相關之使用政策後進一步運作以轉遞使用資料給通信組件。

9. 如申請專利範圍第 8 項所述之智慧卡終端基礎設施，其中該通信組件藉由以下至少一種方式來轉遞一違背與智慧卡相關使用政策之指示：(i) 在一顯示裝置上顯示該違背指示訊息；(ii) 建立一對應於該違背之日誌入口；及 (iii) 發送該違背指示給一應用。

10. 如申請專利範圍第 1 項所述之智慧卡終端基礎設施，其中該資料與管理框架更包括：

一連接組件，在沒有探測到錯誤或執行該使用政策之情況下，其用來在該智慧卡應用與一相應終端應用之間建立一通道。

11. 如申請專利範圍第 1 項所述之智慧卡終端基礎設施，其中該資料與管理框架更包括：

一終端政策組件，用來將與該智慧卡應用處理相關之終端政策或限制予以合併。

12.一種在智慧卡終端應用與智慧卡之間相互操作之方法，該方法包括以下步驟：

獲取一應用程式介面（API），其被寫入至一智慧卡終端之一框架；

從該 API 獲取與該智慧卡應用相關之資料；及

將與該智慧卡終端應用相關之資料寫入該智慧卡終端應用中。

13.如申請專利範圍第 12 項所述之相互操作方法，其中從該 API 獲取與該智慧卡應用相關之訊息包括獲取至少一種（i）該智慧卡應用之一介面；（ii）該智慧卡應用所使用之一協定；及（iii）一智慧卡安全模型。

14.如申請專利範圍第 12 項所述之相互操作方法，更包括以下步驟：

在該智慧卡終端處執行該智慧卡之安全模型。

15.如申請專利範圍第 14 項所述之相互操作方法，其中執行智慧卡安全模型包括：

監視該智慧卡之使用情況；及

依據該所監視使用情況違背安全模型時的判斷，顯示一違背訊息。

16.如申請專利範圍第 12 項所述之相互操作方法，更包括：

在該智慧卡與該智慧卡終端之間建立一安全通道。

17.如申請專利範圍第 12 項所述之相互操作方法，更包括

以下步驟：

設定該智慧卡終端應用，以進一步定義一終端政策或一限制。

18. 一種在一智慧卡終端上執行一智慧卡安全模型之方法，其包括：

從該智慧卡終端之一資料與管理框架中獲取該智慧卡安全模型；及

將該安全模型併入至一對應於該智慧卡之智慧卡終端應用。

19. 如申請專利範圍第 18 項所述之方法，其中從該智慧卡終端之一資料與管理框架中獲取該智慧卡安全模型的步驟包括讀取一應用於該資料與管理框架之應用程式介面（API）。

20. 如申請專利範圍第 18 項所述之方法，更包括以下步驟：

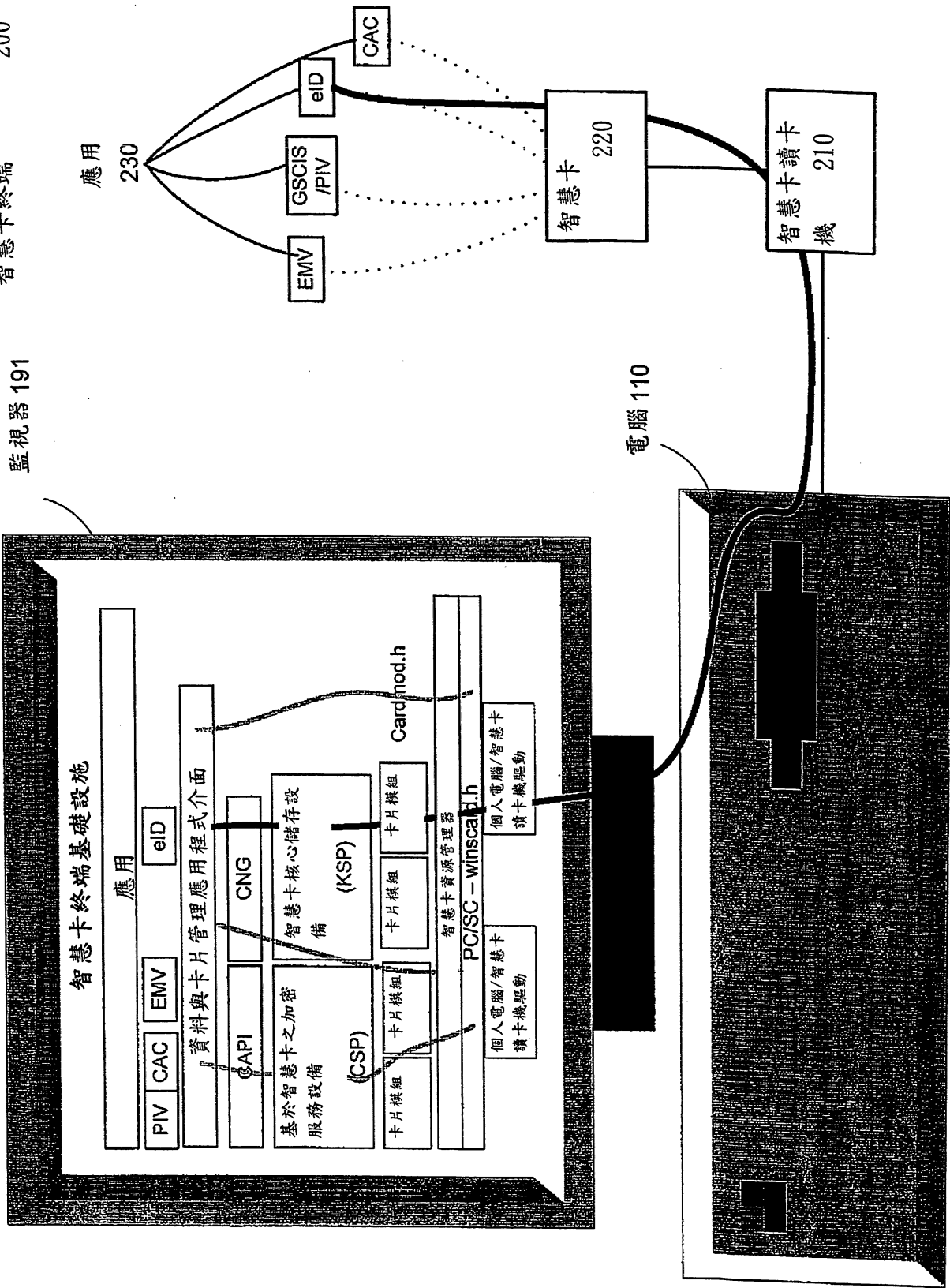
探測一由該安全模型所定義之錯誤狀況；及

在探測到該錯誤狀況後，傳送一對應於該錯誤狀況之錯誤訊息。

200

智慧卡終端

監視器 191



電腦 110

智慧卡 220

智慧卡讀卡機 210

應用 230

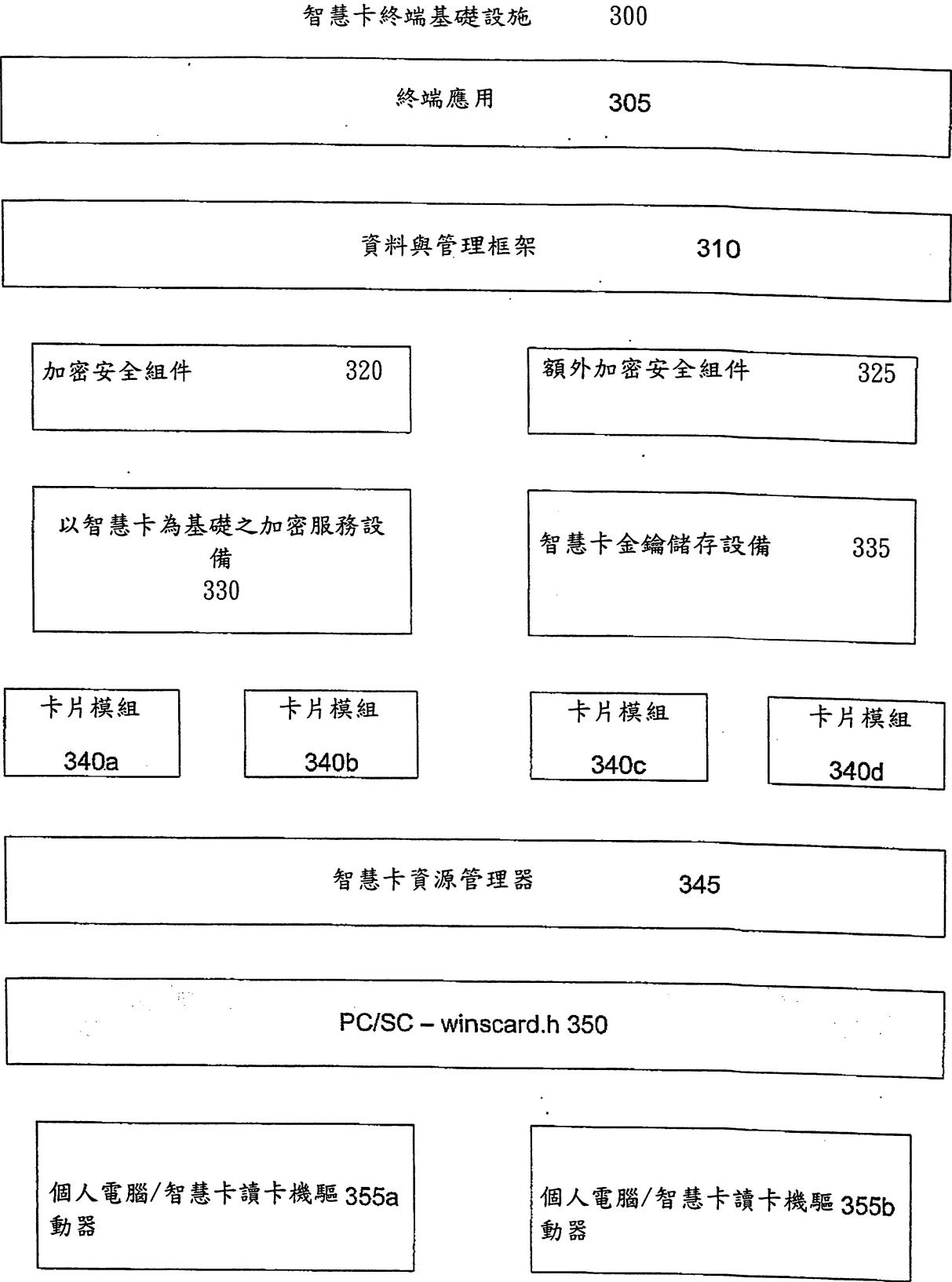
EMV

GSCIS /PIV

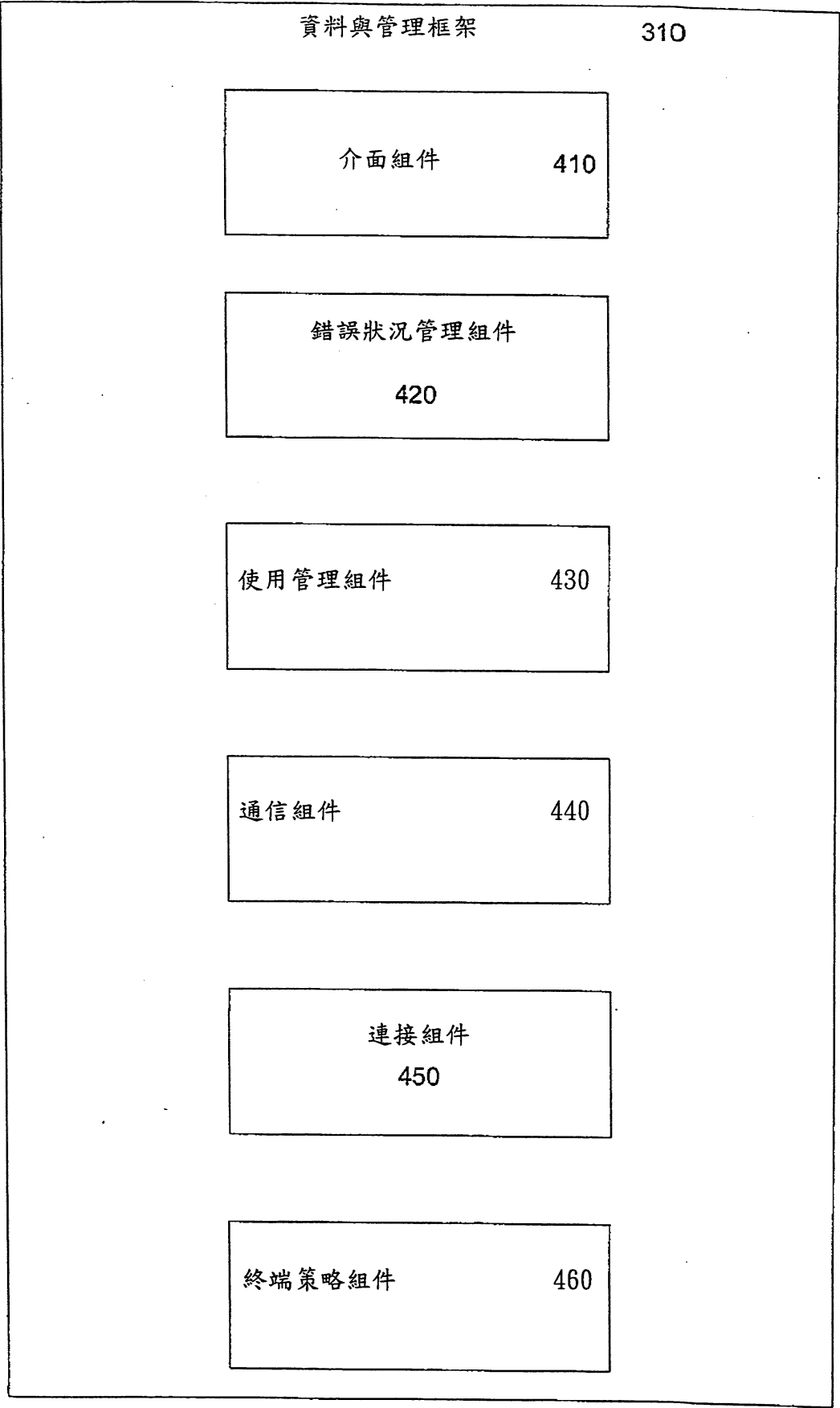
eID

CAC

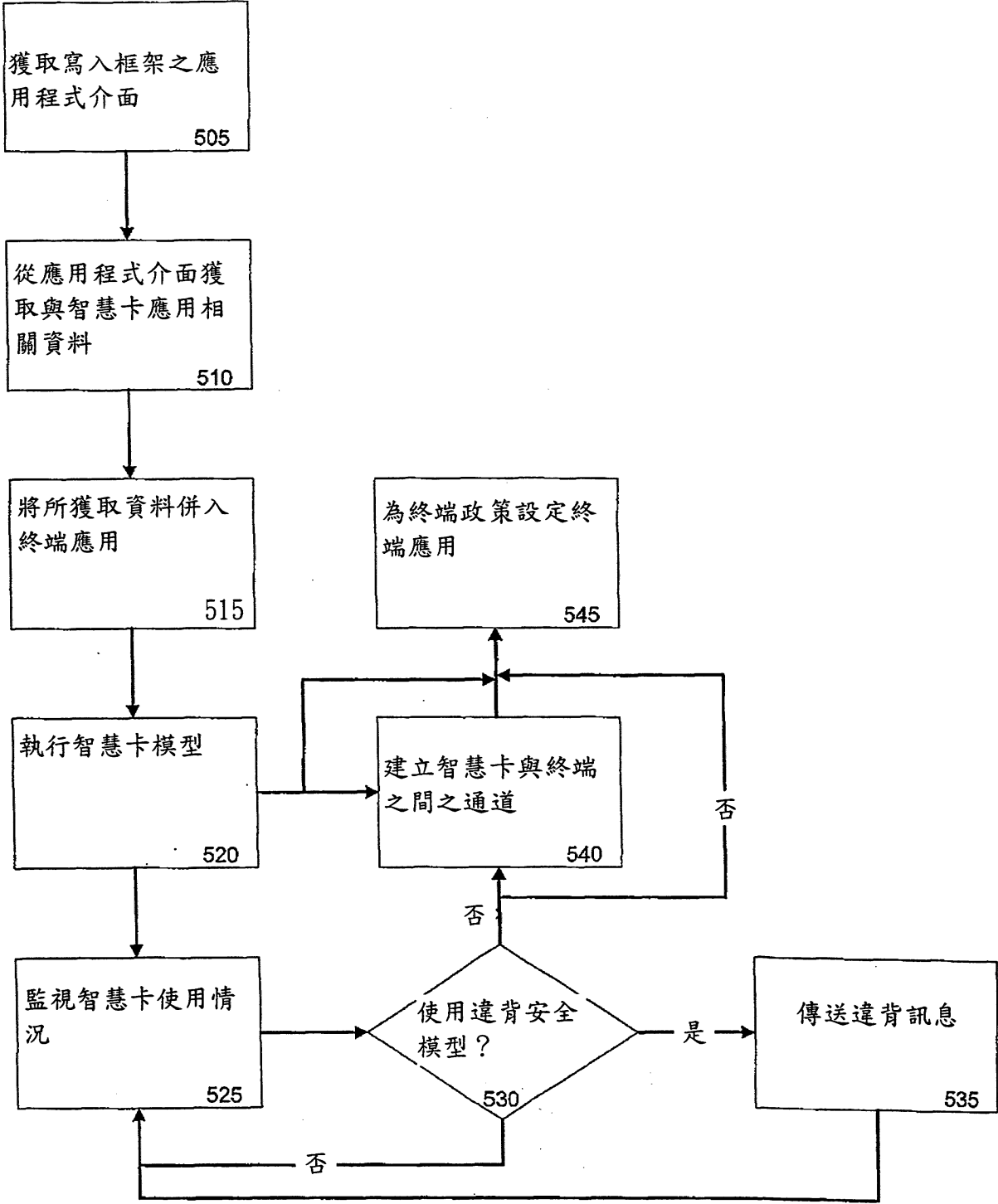
第 2 圖



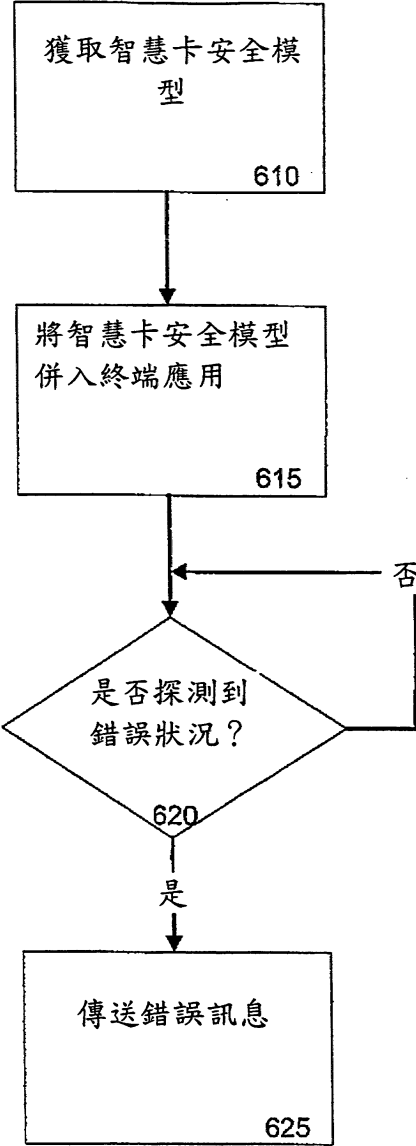
第 3 圖



第 4 圖



第 5 圖



第 6 圖

七、指定代表圖：

(一)、本案指定代表圖為：第(2)圖。

(二)、本代表圖之元件代表符號簡單說明：

110 電腦

191 監視器

200 智慧卡終端

210 智慧卡讀卡機

220 智慧卡

230 應用

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無