I596547

(19)中華民國智慧財產局

(12)發明說明書公告本　(11)證書號數：TW I596547 B

(45)公告日： 中華民國 106 (2017) 年 08 月 21 日

(21)申請案號：105137566　(22)申請日： 中華民國 105 (2016) 年 11 月 17 日

(51)Int. Cl.：　*G06K19/08 (2006.01)*　*G06F21/32 (2013.01)*

G06F21/60 (2013.01)

(71)申請人：中華電信股份有限公司 (中華民國)　(TW)

桃園市楊梅區電研路 99 號

(72)發明人：謝秉諺 HSIEH, PING YEN (TW)；洪丞甫 HUNG, CHENG FU (TW)；王傳陞 WANG, CHUAN SHENG (TW)；張本毅 CHANG, PEN YI (TW)；羅志賢 LO, CHIH HSIEN (TW)

(74)代理人：葉璟宗；卓俊傑

(56)參考文獻：

TW	200502840A	TW	200949765A
TW	201101778A1	TW	201512888A
TW	201541924A	CN	102064944B
US	2008/0005567A1	US	2012/0198548A1

審查人員：張發祥

申請專利範圍項數：4 項　圖式數：5　共 20 頁

(54)名稱

基於多卡合一之卡片應用服務防偽寫入系統與方法

(57)摘要

本發明係揭露一種基於多卡合一之卡片應用服務防偽寫入系統與方法，提供卡片應用服務之驗證技術，利用數位簽章技術可以有效的驗證欲寫入資料之不可否認性以及完整性，避免有心人士圖謀不當利益，刻意將偽造的卡片應用服務寫入卡片，提高多卡合一應用服務之安全性。

指定代表圖：

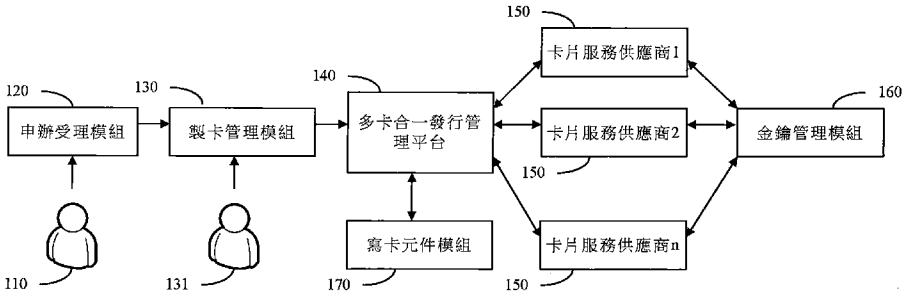

圖 1

符號簡單說明：

110・・・使用者

120・・・申辦受理模組

130・・・製卡管理模組

131・・・操作人員

140・・・多卡合一發行管理平台

150・・・卡片服務供應商

160・・・金鑰管理模組

170・・・寫卡元件模組

180・・・智慧卡模組

公告本

發明摘要

※ 申請案號：105137566

※ 申請日：105/11/17　　※IPC 分類：**G06K 19/08** (2006.01)
G06F 21/32 (2013.01)
G06F 21/60 (2013.01)

【發明名稱】(中文/英文)

基於多卡合一之卡片應用服務防偽寫入系統與方法

【中文】

本發明係揭露一種基於多卡合一之卡片應用服務防偽寫入系統與方法，提供卡片應用服務之驗證技術，利用數位簽章技術可以有效的驗證欲寫入資料之不可否認性以及完整性，避免有心人士圖謀不當利益，刻意將偽造的卡片應用服務寫入卡片，提高多卡合一應用服務之安全性。

【英文】

【代表圖】

【本案指定代表圖】：圖 1。

【本代表圖之符號簡單說明】：

110 使用者

120 申辦受理模組

130 製卡管理模組

131 操作人員

140 多卡合一發行管理平台

150 卡片服務供應商

160 金鑰管理模組

170 寫卡元件模組

180 智慧卡模組

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】（中文/英文）

基於多卡合一之卡片應用服務防偽寫入系統與方法

【技術領域】

【0001】本發明屬於一種基於多卡合一之卡片應用服務防偽寫入系統與方法，尤指一種基於多卡合一之卡片應用服務防偽寫入系統與方法，以降低偽造的多卡合一智慧卡於市面流通之數量。

【先前技術】

【0002】智慧卡即是一晶片卡，是在一可攜式塑膠卡片上內嵌一積體電路晶片。卡片包含了微處理器、I/O介面以及記憶體，可儲存各式卡片資訊，並依其儲存資訊之用途不同，可區分為身分證、健保卡、駕照、信用卡、電子票證、交通票證等。由於卡片種類眾多，造成攜帶之不便，故多卡合一便應運而生。

【0003】如台灣公開號 TW 200502840「具備多應用程式之智慧卡與終端機間的資料處理方法」，其智慧卡具有複數應用程式，為多卡合一之原型，其中透過一終端機向應用程式傳遞參數並取得狀態回應訊息，唯此一方法並未進行安全性上的驗證；又如台灣公開號 TW 201610858「多卡合一裝置、系統和卡資訊載入方法」，其通過多卡合一裝置在輸入單元接收使用者發出的一指令並透過記憶體讀取對應之卡片資訊，此一方法僅提供了讀卡時的安全性驗證，並未於發卡階段進行安

全性的處理；又如美國公開號 US 20080005567 A1「Method and system for personalizing smart cards using asymmetric key cryptography」，其使用複數個密鑰加密個人化指令，並以應用程式提供者私鑰進行簽章，傳送至卡片並透過應用程式進行驗證與解密，以達到發卡時之安全性處理，唯以應用程式提供者私鑰簽章之狀況下，無法保護獲取之卡片應用服務隸屬於同一使用者。

【0004】另如美國公開號 US 7380125 B2「Smart card data transaction system and methods for providing high levels of storage and transmission security」，其揭露一智慧卡儲存與傳輸安全之方法，唯其未針對驗證之行為進行說明，且其未將此一安全機制擴展至多卡合一上。

【0005】本案發明人鑑於上述習用方式所衍生的各項缺點，乃亟思加以改良創新，並經多年苦心孤詣潛心研究後，終於成功研發完成本基於多卡合一之卡片應用服務防偽寫入系統與方法。

【發明內容】

【0006】為達上述目的，本發明提出提供一種基於多卡合一之卡片應用服務防偽寫入系統與方法，於多卡合一架構下，若欲進行一多卡合一之晶片卡發卡流程，需包含一使用者之要求、一申辦受理模組、一製卡管理模組、一多卡合一發行管理平台、一寫卡元件模組、各式提供該卡片資訊的卡片服務供應商、以及一金鑰管理模組；其中由製卡管理系統提供使用者資訊與需求予多卡合一發行管理平台，然若此一流程經由人為操縱製卡管理系統，竄改其中任一卡片應用服務之使用者

資訊為他人並發出需求，則此惡意攻擊者即可獲得未授權寫入之卡片應用服務，進而使同一實體證件內的卡片應用服務不隸屬於同一使用者。因此，現有的多卡合一架構有安全性上的疑慮。

【0007】本發明為一種基於多卡合一之卡片應用服務防偽寫入系統與方法，其主要目的在於設計一多卡合一架構下，縱使製卡流程中製卡管理系統被操縱，竄改任一卡片應用服務之使用者資訊，亦無法於寫卡階段將未取得授權之卡片應用服務寫入卡片之方法。

【0008】一種基於多卡合一之卡片應用服務防偽寫入系統，其主要包括：

一製卡管理模組，是以啟動製卡程序，傳遞使用者資訊與一或複數個需求至一多卡合一發行管理平台；

多卡合一發行管理平台，是將使用者資訊與需求傳遞至指定之卡片服務供應商，再將回傳之個人化資料與簽章傳送至寫卡元件模組；

寫卡元件模組，是將個人化資料與簽章傳送給卡片內指定之應用程式；

一金鑰管理模組，是具有卡片唯一金鑰對，並得以儲存私鑰，以及將公鑰寫入智慧卡，同時得以紀錄使用者資訊與其金鑰對的配對關是，並產製個人化資料的簽章值。

【0009】其中卡片內指定之應用程式，是得以驗證簽章並判定是否寫入個人化資料。

【0010】一種基於多卡合一之卡片應用服務防偽寫入方法，包括：

獲得使用者資訊或需求；

多卡合一發行管理平台提出個人化資料要求；

卡片服務供應商完成個人化資料產製；

卡片服務供應商提出簽章要求；

金鑰管理模組完成簽章動作；

金鑰管理模組回傳簽章資料；

卡片服務供應商回傳個人化資料與對應簽章；

多卡合一發行管理平台提出寫卡要求；

寫卡元件模組進行寫卡動作。

【0011】其中寫卡動作之流程，是包含：

寫卡元件模組接收多卡合一發行管理平台之個人化資料與簽章；

寫卡元件模組將個人化資料與簽章輸入智慧卡模組之卡片服務供應商所屬之應用程式；

智慧卡模組卡片公開金鑰存放區驗證卡片服務供應商所屬之應用程式之個人化資料與簽章。

【0012】其中驗證之流程，是包含：

應用程式執行碼模組之個人化資料簽章驗證單元向卡片公開金鑰存放區接收公開金鑰；

應用程式執行碼模組之正常應用程式處裡單元接收驗證成功之個人化資料；

卡片應用程式模組之應用程式區接收由正常應用程式處裡單元接收之驗證成功之個人化資料。

【0013】本發明所提供一種基於多卡合一之卡片應用服務防偽寫入系統與方法，與其他習用技術相互比較時，更具備下列優點：

1. 本發明在一多卡合一架構下提供卡片應用服務之驗

證技術，防範偽造的卡片應用服務之寫入，當有心人士或駭客取得製卡管理系統的權限後，縱使刻意竄改使用者資料，亦無法將未取得授權之卡片應用服務寫入卡片。

【圖式簡單說明】

【0014】請參閱有關本發明之詳細說明及其附圖，將可進一步瞭解本發明之技術內容及其目的功效；有關附圖為：

圖 1 為本發明基於多卡合一之卡片應用服務防偽寫入系統與方法之架構示意圖；

圖 2 為本發明基於多卡合一之卡片應用服務防偽寫入系統與方法之初始化示意圖；

圖 3 為本發明基於多卡合一之卡片應用服務防偽寫入系統與方法之發卡流程圖；

圖 4 為本發明基於多卡合一之卡片應用服務防偽寫入系統與方法之寫卡動作流程圖；

圖 5 為本發明基於多卡合一之卡片應用服務防偽寫入系統與方法之驗證流程圖。

【實施方式】

【0015】為了使本發明的目的、技術方案及優點更加清楚明白，下面結合附圖及實施例，對本發明進行進一步詳細說明。應當理解，此處所描述的具體實施例僅用以解釋本發明，但並不用於限定本發明。

【0016】以下，結合附圖對本發明進一步說明：

【0017】請參閱圖 1 所示，為本發明基於多卡合一之卡片應用服務防偽寫入系統與方法之架構示意圖，其包括：

一製卡管理模組 130，是以啟動製卡程序，傳遞使用者資訊與一或複數個需求至一多卡合一發行管理平台 140；

多卡合一發行管理平台 140，是將使用者資訊與需求傳遞至指定之卡片服務供應商 150，再將回傳之個人化資料與簽章傳送至寫卡元件模組 170；

寫卡元件模組 170，是將個人化資料與簽章傳送給卡片內指定之應用程式；

一金鑰管理模組 160，是具有卡片唯一金鑰對，並得以儲存私鑰，以及將公鑰寫入智慧卡，同時得以紀錄使用者資訊與其金鑰對的配對關是，並產製個人化資料的簽章值。

【0018】由上述步驟可以得知，進入發卡流程前，卡片需經過金鑰管理模組以完成初始化動作；發卡流程開始後，使用者 110 向申辦受理模組 120 提出製卡之要求，由申辦受理模組 120 傳遞此要求至製卡管理模組 130，製卡管理模組 130 操作人員 131 操作模組，依序傳遞使用者資訊與需求 1 到 n 至多卡合一發行管理平台 140，由多卡合一發行管理平台 140 將對應之使用者資訊與需求傳遞至對應之卡片服務供應商 140，卡片服務供應商 150 至金鑰管理模組 160 取得簽章後，將個人化資料與對應之簽章回傳至多卡合一發行管理平台 140，由多卡合一發行管理平台 140 要求寫卡元件模組 170 進行寫卡動作，寫卡時，卡片之應用程式會針對各卡片應用服務之個人化資料與對應之簽章進行驗證，若驗證成功，則可進行寫入之動作，反之則拒絕寫入。

【0019】藉由上述之流程與方法，縱使製卡管理模組操縱人員 131 竄改任一卡片應用服務之使用者資訊，亦無法製造

出卡片應用服務不隸屬於同一使用者的實體證件，提升了多卡合一架構下製卡流程的安全性。

【0020】請參閱圖 2 所示，為本發明基於多卡合一之卡片應用服務防偽寫入系統與方法之初始化示意圖，在進入發卡流程之前，所有卡片皆須經過初始化動作，而初始化過程主要則是包括規劃卡片資料空間、applet 預先載入以及產製金鑰 161 等。由圖 2 中可以看到，金鑰管理模組 160 將於初始化過程中產製專屬於每張卡片之唯一金鑰對，並將私密金鑰存放於金鑰管理模組 160 中，並寫入公開金鑰 181 於智慧卡模組 180 中預先規劃之公開金鑰存放區；其中，金鑰對的產製動作亦可利用硬體保密器來協助進行，則私密金鑰可直接存放於硬體保密器之中。

【0021】在產製此金鑰對之目的在於後續進行寫卡動作時，卡片本身將利用公開金鑰進行簽章之驗證動作，用以判斷欲寫入之資料是否確定由同一金鑰對之私密金鑰所進行簽署；由於當使用者申辦多卡合一證件時，使用者資訊及配發之卡片金鑰間的配對關係將紀錄於金鑰管理模組中，因此根據卡片驗證簽章之結果，即可判斷出欲寫入之資料是否確為所屬使用者之個人化產製資料，唯有驗證簽章正確時，方可進行寫卡動作。金鑰產製的方法是由金鑰管理模組產製，並從外部將公開金鑰寫入卡片，此舉與直接從卡片內部產製金鑰之方法有所不同，其原因在於卡片內部產製金鑰之目的主要是利用卡片內之私密金鑰進行簽章，而上述所提及透過金鑰管理模組產製金鑰對，並將公開金鑰寫入卡片之中，此舉之目的是要利用卡片上之公開金鑰來驗證簽章，意即利用卡片上之公開金鑰來驗證欲寫入之資料確定為該使用者之私密金鑰所簽署，

等同於使用卡片本身來檢驗欲寫入資料之合法性，針對個人化資料而言，如同達到「身分識別」之效果，此目的與過去直接使用卡片進行簽章之應用場景有所差異，可避免發出具不同使用者資料的多卡合一智慧卡，達降低偽卡數量的功效。

【0022】請參閱圖 3 所示，為本發明基於多卡合一之卡片應用服務防偽寫入系統與方法之發卡流程圖，包括：

S310 獲得使用者資訊或需求；

多卡合一發行管理平台 S320 提出個人化資料要求；

卡片服務供應商 S303 完成個人化資料產製；

卡片服務供應商 S304 提出簽章要求；

金鑰管理模組 S305 完成簽章動作；

金鑰管理模組 S306 回傳簽章資料；

卡片服務供應商 S307 回傳個人化資料與對應簽章；

多卡合一發行管理平台 S308 提出寫卡要求；

寫卡元件模組 S309 進行寫卡動作。

【0023】由上述得知，多卡合一發行管理平台須根據所收到的使用者資訊，以及該使用者所要求之卡片應用服務，向相對應之卡片服務供應商要求該使用者之個人化資料，此時多卡合一發行管理平台須告知卡片服務供應商所需之使用者資訊，例如：使用者之唯一識別代碼(如：帳號、識別碼等)。當卡片服務供應商獲得使用者之識別資訊後，首先會針對該使用者進行個人化資料產製，產製完成後則根據使用者識別資訊向金鑰管理模組提出簽章要求，而簽章要求中須提供給金鑰管理模組之必要資訊至少需要包含使用者識別資訊，以及個人化資料雜湊值等兩項主要資訊。當金鑰管理模組收到簽章要求之後，則根據簽章要求中的使用者識別資訊，以該使用

者之私密金鑰，對此使用者之個人化資料雜湊值進行簽章動作，完成簽章後再回傳至卡片服務供應商。卡片服務供應商收到金鑰管理模組回傳之簽章資料後，才將個人化資料與簽章一併回傳至多卡合一發行管理平台，多卡合一發行管理平台則會將個人化資料與簽章傳送至寫卡元件模組，由寫卡元件模組開始進行寫卡動作。

【0024】請參閱圖 4 所示，為本發明基於多卡合一之卡片應用服務防偽寫入系統與方法之寫卡動作流程圖，是包含：

S401 個人化資料與對應簽章；

寫卡元件模組 S402 接收多卡合一發行管理平台之個人化資料與簽章；

寫卡元件模組 S403 將個人化資料與簽章輸入智慧卡模組之 S404 卡片服務供應商所屬之應用程式；

智慧卡模組 S405 卡片公開金鑰存放區驗證卡片服務供應商所屬之應用程式之個人化資料與簽章。

【0025】由上述得知，寫卡元件模組與智慧卡模組進行通訊，並選擇特定卡片服務供應商所屬之應用程式以嘗試進行個人化資料寫入。寫卡元件模組對智慧卡模組建立連線通道，並將接收到的個人化資料與簽章傳遞給智慧卡模組，而在本實施例中智慧卡模組中之卡片服務供應商所屬之應用程式是以 applet 的形式存在，而寫卡元件模組是為國際標準 ISO 7816，再將欲寫入之個人化資料與簽章傳送給對應之卡片服務供應商所屬之應用程式，卡片服務供應商所屬之應用程式將由金鑰存放區取得公開金鑰進行簽章驗證，並依驗證結果決定是否寫入收到的個人化資料。

【0026】請參閱圖 5 所示，為本發明基於多卡合一之卡片

應用服務防偽寫入系統與方法之驗證流程圖，是包含：

S501 個人化資料與簽章輸入應用程式執行碼模組

應用程式執行碼模組之 S502 個人化資料簽章驗證單元向 S503 卡片公開金鑰存放區接收公開金鑰；

應用程式執行碼模組之 S504 正常應用程式處裡單元接收驗證成功之個人化資料；

卡片應用程式模組之 S505 應用程式區接收由正常應用程式處裡單元接收之驗證成功之個人化資料。

【0027】由上述得知，卡片初始化過程中會產生專屬於每張卡片之唯一金鑰對，其私鑰存放於金鑰管理模組，而對應之公鑰則寫入卡片之公開金鑰存放區內。卡片內之應用程式取得個人化資料與簽章後，將經由應用程式可執行碼執行驗證簽章程序。應用程式可執行碼以 Java Card 應用程式介面向卡片公開金鑰存放區取得卡片公開金鑰，並以此公鑰驗證個人化資料對應之簽章。若個人化資料經過竄改、替換為非原卡片使用者之資料，則於金鑰管理模組會使用非原卡片使用者之私密金鑰簽章，此驗簽程序將會失敗，應用程式可執行碼將回覆存取失敗而拒絕寫入。若驗簽程序成功，則代表此個人化資料是由金鑰管理模組認證為原卡片使用者對應的個人化資料，應用程式可執行碼將會把驗證成功之個人化資料寫入應用程式資料區。如此即完成一種基於多卡合一之卡片應用服務防偽寫入系統與方法。

【0028】上列詳細說明乃針對本發明之一可行實施例進行具體說明，惟該實施例並非用以限制本發明之專利範圍，凡未脫離本發明技藝精神所為之等效實施或變更，均應包含於本案之專利範圍中。

【0029】綜上所述，本案不僅於技術思想上確屬創新，並具備習用之傳統方法所不及之上述多項功效，已充分符合新穎性及進步性之法定發明專利要件，爰依法提出申請，懇請　貴局核准本件發明專利申請案，以勵發明，至感德便。

【符號說明】

【0030】

110 使用者

120 申辦受理模組

130 製卡管理模組

131 操作人員

140 多卡合一發行管理平台

150 卡片服務供應商

160 金鑰管理模組

161 產製金鑰

170 寫卡元件模組

180 智慧卡模組

181 寫入公開金鑰

S301~S309 發卡流程

S401~S405 寫卡動作流程

S501~S505 驗證流程

106年06月07日修正替換頁

申請專利範圍

1. 一種基於多卡合一之卡片應用服務防偽寫入系統，其主要包括：

一製卡管理模組，係以啟動製卡程序，傳遞使用者資訊與一或複數個需求至一多卡合一發行管理平台；

該多卡合一發行管理平台，係將使用者資訊與需求傳遞至指定之卡片服務供應商，再將產製個人化資料的簽章值傳送至寫卡元件模組；

該寫卡元件模組，係將個人化資料與簽章傳送給卡片內指定之應用程式；

一金鑰管理模組，係具有卡片唯一金鑰對，並得以儲存私鑰，以及將公鑰寫入智慧卡，同時得以紀錄使用者資訊與其該金鑰對的配對關係，並產製個人化資料的簽章值。

2. 如申請專利範圍第1項所述之基於多卡合一之卡片應用服務防偽寫入系統，其中該卡片內指定之應用程式，係得以驗證簽章並判定是否寫入個人化資料。

3. 一種基於多卡合一之卡片應用服務防偽寫入方法，包括：

獲得使用者資訊或需求；

多卡合一發行管理平台提出個人化資料要求；

卡片服務供應商完成個人化資料產製；

卡片服務供應商提出簽章要求；

金鑰管理模組完成簽章動作；

金鑰管理模組回傳簽章資料；

卡片服務供應商回傳個人化資料與對應簽章；

多卡合一發行管理平台提出寫卡要求；

寫卡元件模組進行寫卡動作。

4. 如申請專利範圍第3項所述之基於多卡合一之卡片應用服務防偽寫入方法，其中該寫卡動作之流程，係包含：

寫卡元件模組接收多卡合一發行管理平台之個人化資料與簽章；

寫卡元件模組將個人化資料與簽章輸入智慧卡模組之卡片服務供應商所屬之應用程式；

智慧卡模組卡片公開金鑰存放區驗證卡片服務供應商所屬之應用程式之個人化資料與簽章，其中該卡片公開金鑰存放區驗證之流程，係包含：

應用程式執行碼模組之個人化資料簽章驗證單元向卡片公開金鑰存放區接收公開金鑰；

應用程式執行碼模組之正常應用程式處裡單元接收驗證成功之個人化資料；

卡片應用程式模組之應用程式區接收由正常應用程式處裡單元接收之驗證成功之個人化資料。

圖式

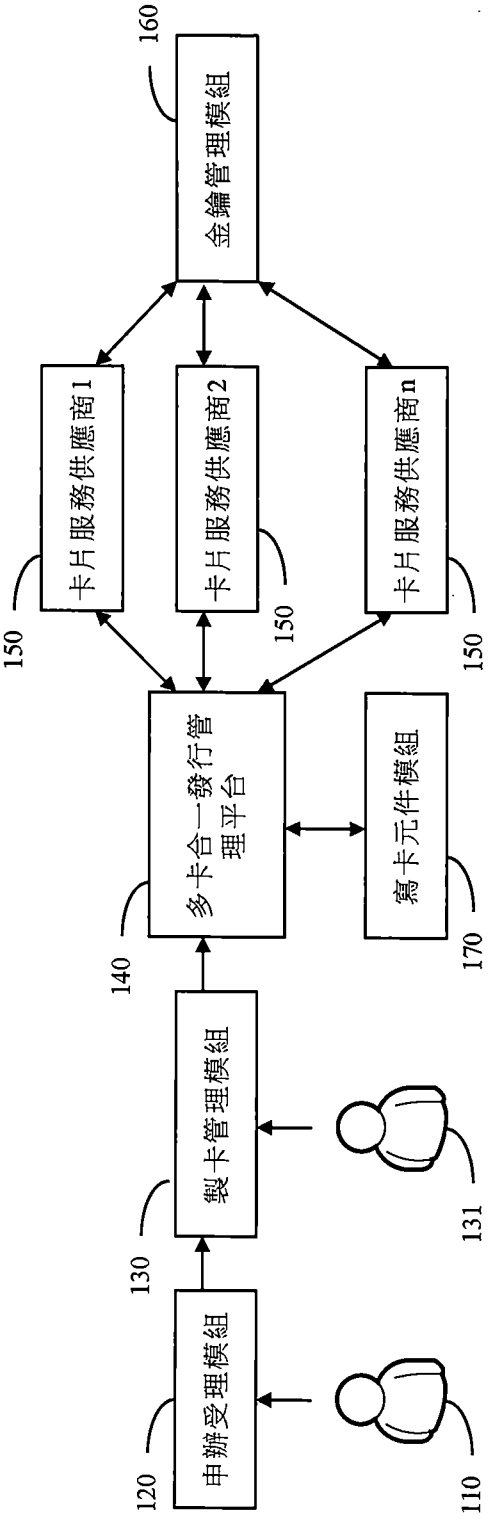
160
金鑰管理模組
卡片服務供應商1
卡片服務供應商2
卡片服務供應商n
150
150
150
多卡合一發行管理平台
寫卡元件模組
140
170
製卡管理模組
130
131
申辦受理模組
120
110

圖 1

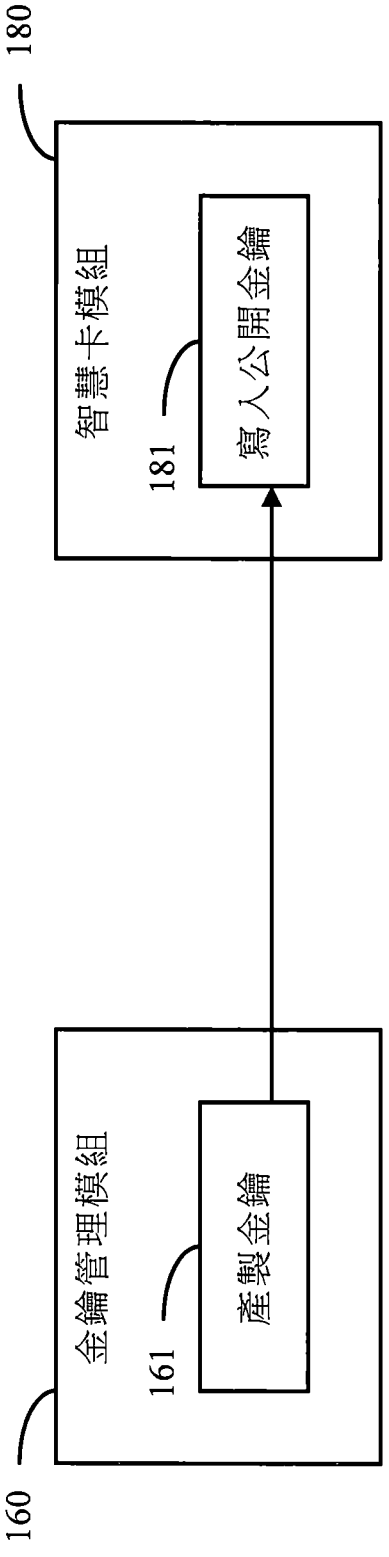

圖 2

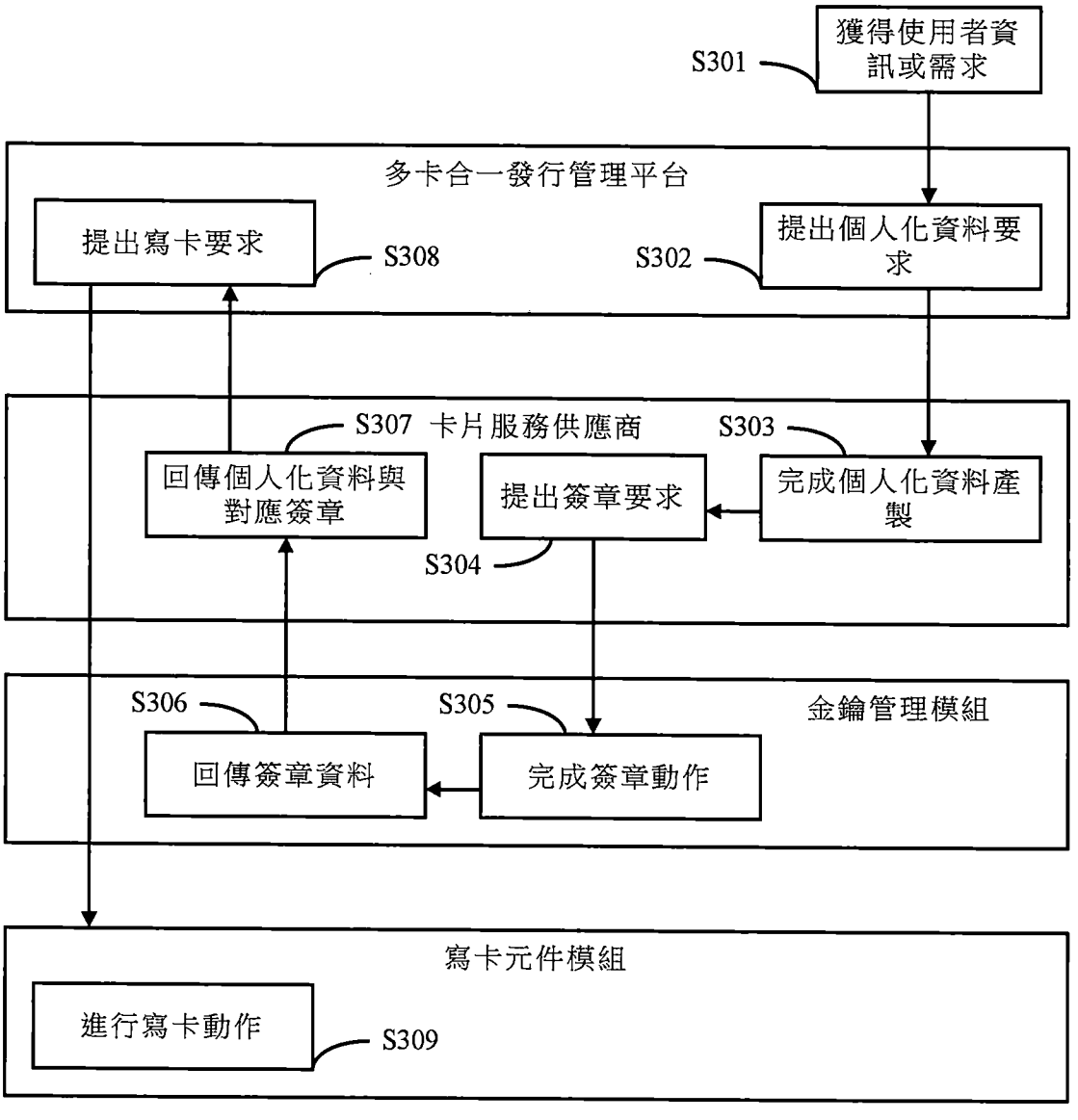
S301
獲得使用者資訊或需求
多卡合一發行管理平台
提出寫卡要求
S308
S302
提出個人化資料要求
S307 卡片服務供應商
S303
回傳個人化資料與對應簽章
提出簽章要求
完成個人化資料產製
S304
S306
S305
金鑰管理模組
回傳簽章資料
完成簽章動作
寫卡元件模組
進行寫卡動作
S309

圖 3

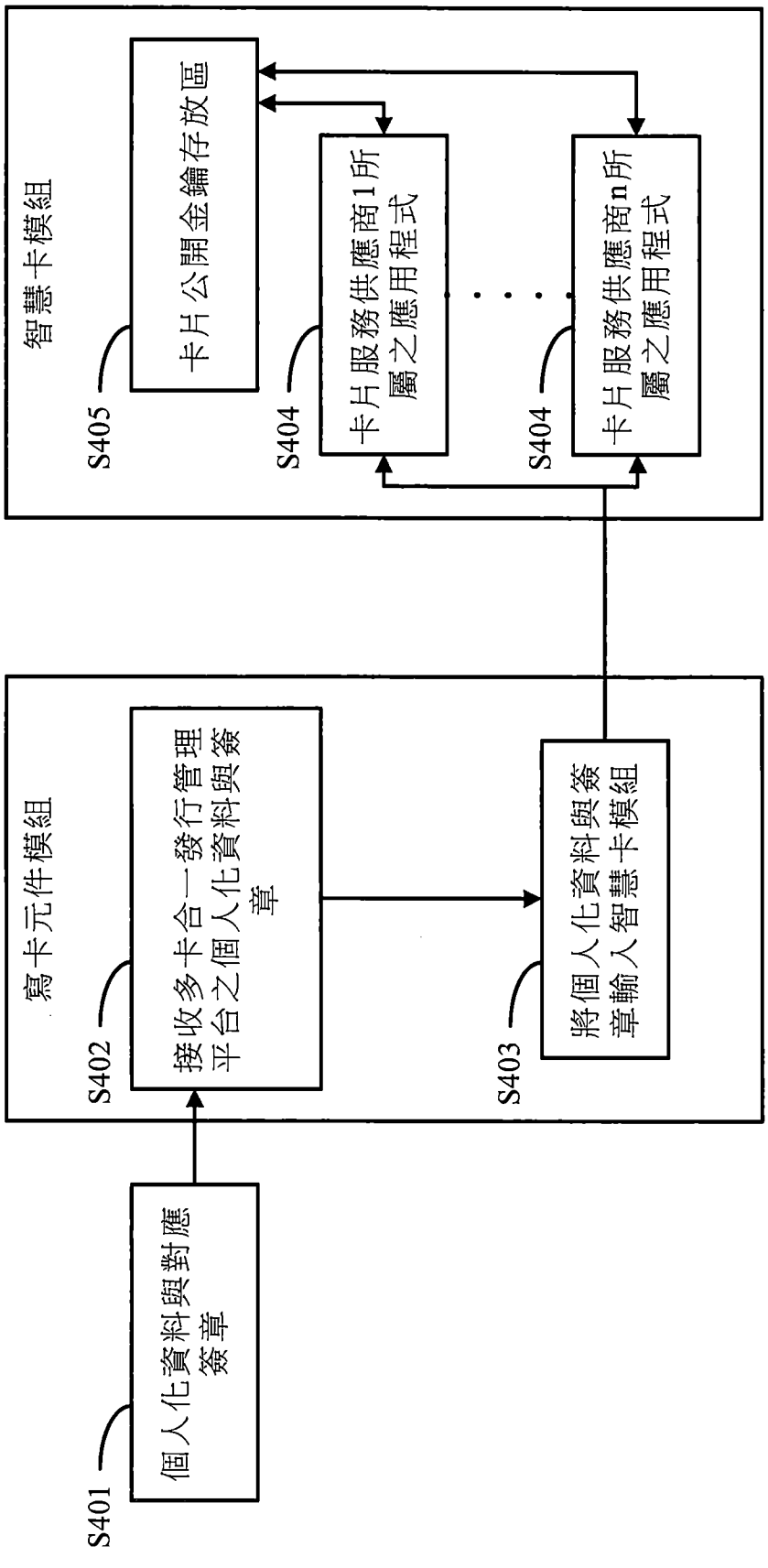
個人化資料與對應簽章
S401
寫卡元件模組
接收多卡合一發行管理平台之個人化資料與簽章
S402
將個人化資料與簽章輸入智慧卡模組
S403
智慧卡模組
卡片公開金鑰存放區
S405
卡片服務供應商1所屬之應用程式
S404
卡片服務供應商n所屬之應用程式
S404

圖 4

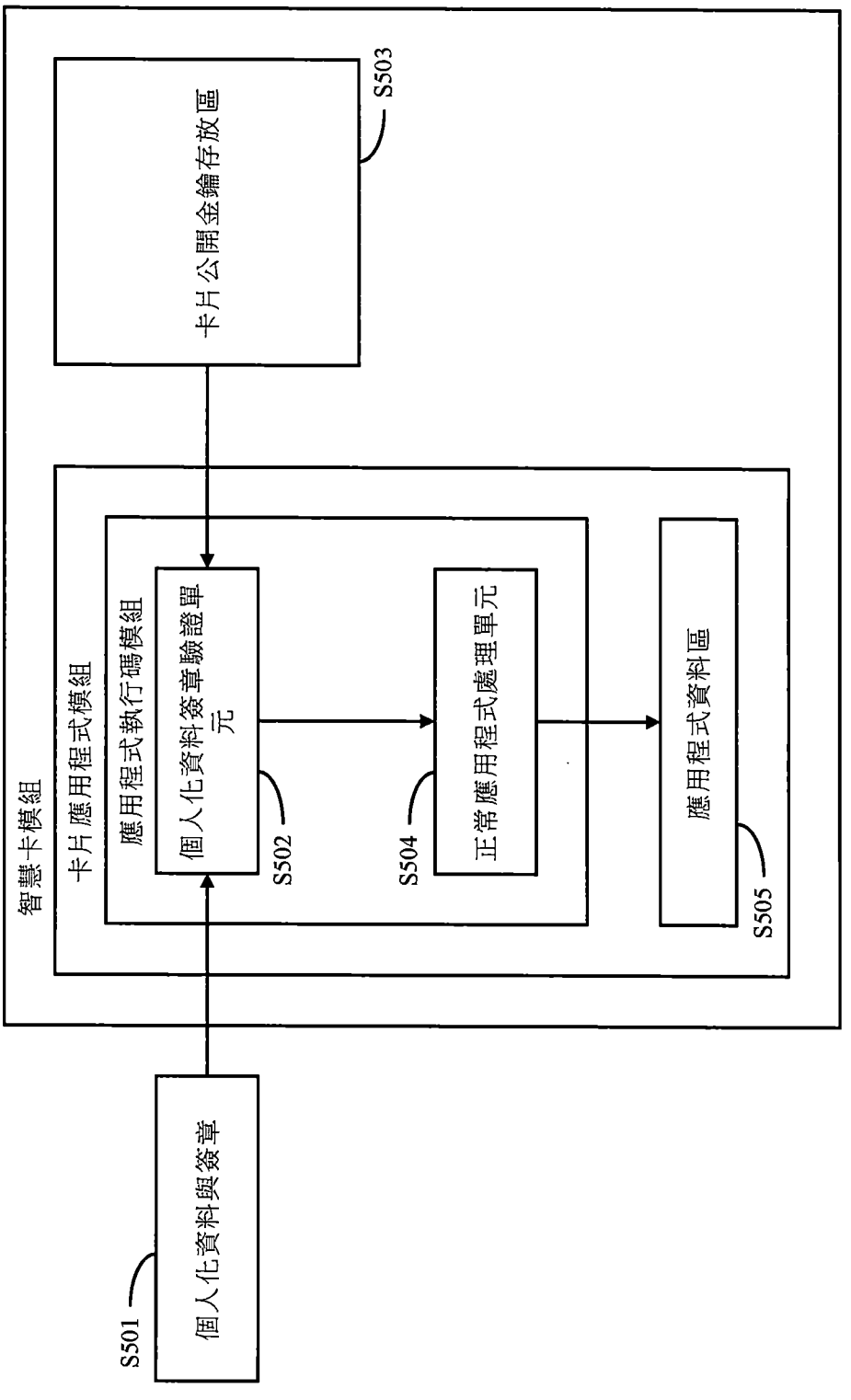
智慧卡模組
卡片應用程式模組
應用程式執行碼模組
個人化資料簽章驗證單元
正常應用程式處理單元
應用程式資料區
卡片公開金鑰存放區
個人化資料與簽章
S501
S502
S503
S504
S505

圖 5