200823715

# 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： 96124596

※ 申請日期： 96.7.6 ※IPC 分類：G06F 21/00 (2006.01)

## 一、發明名稱：（中文/英文）

使用憑證廢止清單之內容控制系統及方法

CONTENT CONTROL SYSTEM AND METHOD USING CERTIFICATE REVOCATION LISTS

## 二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商桑迪士克股份有限公司

SANDISK CORPORATION

代表人：（中文/英文）

麗莎 K 托斯

TOTH, LIZA K.

住居所或營業所地址：（中文/英文）

美國加州謬佩塔斯市麥卡錫大道601號

601 MCCARTHY BOULEVARD, MILPITAS, CA 95035, U.S.A.

國 籍：（中文/英文）

美國 U.S.A.

## 三、發明人：（共 4 人）

姓　名：（中文/英文）

1. 邁可 侯茲曼
   HOLTZMAN, MICHAEL
2. 羅 巴利列
   BARZILAI, RON
3. 羅坦 席拉
   SELA, ROTEM
4. 菲布利斯 喬根得-庫倫巴
   JOGAND-COULOMB, FABRICE

國　籍：（中文/英文）

1. 以色列　ISRAEL
2. 以色列　ISRAEL
3. 以色列　ISRAEL
4. 法國　FRANCE

## 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：

1. 美國；2006年07月07日；60/819,507
2. 美國；2006年11月06日；11/557,006
3. 美國；2006年11月06日；11/557,026

☐ 無主張專利法第二十七條第一項國際優先權：

1.
2.

☐ 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】

本發明一般而言係關於記憶體系統，且尤其係關於一種具有多用途控制特徵之記憶體系統。

【先前技術】

諸如快閃記憶體卡之儲存裝置係已經變成用於儲存諸如相片之數位內容的儲存媒體之選擇。快閃記憶體卡亦可以被使用於散佈其他類型媒體內容。再者，種類增加的主機裝置(諸如電腦、數位相機、行動電話、個人數位助理及諸如MP3播放機之媒體播放機)現在係具有呈現儲存於快閃記憶體卡內的媒體內容之能力。因此，對於快閃記憶體卡以及其他類型行動儲存裝置而言，係具有很大的潛能變成用於散佈數位內容的廣泛使用傳播媒介。

數位內容之擁有者及散佈者之主要考量之一係：在該內容已經透過自諸如網際網路之網路下載或透過儲存裝置上之內容的散佈而被散佈之後，應僅一經授權當事人被允許存取該內容。一種避免未經授權存取之方式係使用一種用於在內容存取被授予給當事人之前建置該當事人之身份之系統。諸如公開密鑰基礎結構(PKI)之系統係已經被發展，以用於此目的。於一種公開密鑰基礎結構系統中，稱為憑證授權單位(Certificate Authority；CA)之受信任的授權單位發佈憑證，以證明個人及組織之身份。諸如想要建置身份之證明的組織及個人之當事人可用適當的證據向該憑證授權單位登錄，以證明其之身份。在已經向該憑證授

權單位證明當事人之身份之後，該憑證授權單位將發佈一憑證給此當事人。該憑證典型地包含：發佈該憑證之該憑證授權單位的名稱、該憑證發佈給予之當事人的名稱、該當事人的一個公開密鑰以及藉由該憑證授權單位之一私有密鑰所簽名(典型地，係藉由將該公開密鑰之一摘要加密)之當事人的公開密鑰。

憑證授權單位之私有密鑰及公開密鑰係相關的，使得使用公開密鑰加密之任何資料係可以藉由該私有密鑰予以解密，且反之亦然。因此，私有密鑰及公開密鑰形成一密鑰對。於RSA Security股份有限公司於2002年6月14日提出之"PKCS#1 v2.1:RSA Cryptography Standard"中提供用於密碼編譯之私有及公開密鑰對之解說。憑證授權單位之公開密鑰係被實施成可公開取用。因此，當一當事人想要驗證由另一個當事人所提呈之憑證是否係真實的時，該驗證當事人可以利用一解密演算法，僅使用該憑證授權單位之公開密鑰來解密該憑證內之公開密鑰之經加密摘要。典型地，亦於該憑證中識別該解密演算法。假如該憑證內之公開密鑰之經加密摘要匹配於該憑證內之未經加密公開密鑰之摘要，則根據信任該憑證授權單位及該憑證授權單位之公開密鑰之真實性，此係證明該憑證內的公開密鑰係尚未被竄改，且係真實的。

為了驗證一當事人的身份，典型地，驗證當事人將傳送一項挑戰(例如，隨機號碼)，且要求另一當事人傳送其憑證以及一對於該挑戰的回應(亦即，以另一當事人之私有

密鑰加密的隨機號碼)。當該回應及憑證被接收時，該驗證當事人首先藉由上述程序驗證是否該憑證內之公開密鑰係真實的。假如該公開密鑰係被驗證為真實的，則該驗證當事人可接著使用該憑證內之公開密鑰來解密該回應，且比較該結果及原始傳送之該隨機號碼隨機號碼。假如其係匹配，此係意謂另一當事人確實具有正確的私有密鑰，且因此理由而證明其身份。假如該憑證內的公開密鑰係非真實的，或者假如該解密之回應無法匹配該挑戰，則鑑認失敗。因此，一想要證明其身份之當事人將需要持有該憑證及相關的私有密鑰。

藉由上述機制，可能不彼此信任的兩個當事人可以使用上述程序，藉由驗證另一當事人中另一當事人之公開密鑰而建置信任。由國際電信聯盟(ITU)之電信標準化部門(ITU-T)而來的建議書X.509係規定憑證架構之標準。關於憑證及其之使用之更詳細資訊，請參閱此標準。

在行政機構中及在大型組織中，為了便利，對於稱為根憑證授權單位之較高層級憑證授權單位而言，委派發佈憑證之責任給若干較低層級憑證授權單位係可能適當的。舉例而言，於一種兩層級式階層架構中，於最高層級之根憑證授權單位發佈憑證給較低層級憑證授權單位，以檢定彼等較低層級授權單位之公開密鑰係真實的。接著，彼等較低層級授權單位係透過上述之登錄程序發佈憑證給當事人。此驗證程序係自該憑證鏈之頂端開始。該驗證當事人將首先使用該根憑證授權單位之該公開密鑰(已知為真實

的)以首先驗證該較低層級憑證授權單位之公開密鑰之真實性。一旦該較低層級憑證授權單位之該公開密鑰之真實性已經被驗證，則可藉由使用該較低層級憑證授權單位之經驗證公開密鑰來驗證經受到較低層級憑證授權單位發佈一憑證至其之當事人之公開密鑰之真實性。接著，由該根憑證授權單位及較低層級憑證授權單位所發佈之該等憑證係形成一含其身份正被驗證之當事人之兩個憑證的憑證鏈。

憑證階層架構當然可以包含兩層以上層級，其中，除了根憑證授權單位以外之於較低層級之每一個憑證授權單位自一較高層級憑證授權單位推導出其授權，且係具有一含有由較高層級憑證授權單位所發佈之其公開密鑰的憑證。因此，為了驗證另一當事人之公開密鑰之真實性，可能需要追蹤至該根憑證授權單位之路徑或憑證鏈。換句話說，為了建置一當事人的身份，其身份需要被證明之當事人係可能需要產生整個憑證鏈，由其自己的憑證至該根憑證授權單位憑證之所有路徑。

一個憑證係發佈某一有效時期。然而，憑證可能在有效時期期滿之前歸因於諸如名稱改變、與憑證發佈者之關聯性改變、對應私密密鑰之損害或可疑損害的事件而變得無效。在此等情況下，憑證授權單位(CA)需要廢止該憑證。憑證授權單位週期性地公布憑證廢止清單，其列出已被廢止之所有憑證的序號。在習知的憑證驗證方法中，期望驗認實體擁有或能夠擷取來自憑證授權單位(CA)之憑證廢止

清單且對照該清單來檢查為驗認而提交之憑證的序號，以判定所提交之憑證是否已被廢止。在驗認實體為記憶體或儲存裝置時，該裝置本身尚未被用以擷取來自憑證授權單位之憑證廢止清單。結果，為驗認而提交之憑證不能藉由記憶體或儲存裝置來驗證。因此，需要提供一種使記憶體或儲存裝置能夠驗證憑證而不必獲得憑證廢止清單之改良系統。

【發明內容】

記憶體裝置尚未被獨自使用於獲得憑證廢止清單。因此，當主機裝置向儲存裝置提交憑證以供驗認，而不提交與該憑證有關之憑證廢止清單時，儲存裝置將不能確定由主機裝置所提交之憑證是否在有關憑證廢止清單上。因此，本發明之一實施例係基於以下體認：可藉由其中主機裝置除了提交憑證以外亦提交與該憑證有關之憑證廢止清單的系統來避免此問題。以此方式，儲存裝置能夠藉由檢查憑證之識別(諸如，在由主機裝置所發送之憑證廢止清單中之其之序號)來驗證憑證之真實性。

若憑證廢止清單含有被廢止之憑證的大量識別(諸如，其序號)，則該清單可能相當長。因此，在另一實施例中，由一裝置接收憑證廢止清單之若干部分，且該裝置循序地處理該等部分。該裝置亦搜尋對在清單上自主機所接收之憑證之參照或該憑證之識別，其中處理與搜尋同時發生。由於處理與搜尋同時發生，所以驗證憑證之程序變得更有效效。

如上文所述，儲存裝置尚未被用以獲得憑證廢止清單，而主機裝置已被用以獲得憑證廢止清單。因此，在另一實施例中，雖然主機裝置需要提交憑證廢止清單連同供驗認主機裝置用之憑證，但不存在使儲存或記憶體裝置提交憑證廢止清單連同供驗認主機裝置用之憑證的此需要，該儲存或記憶體裝置將僅需要提交憑證。接著，由主機裝置獲得有關憑證廢止清單以用於驗證記憶體裝置憑證。

雖然有可能將主機裝置用以自由地獲得憑證廢止清單，但許多消費者可能發現必須頻繁地(諸如，每當消費者希望存取儲存裝置中之經加密內容時)獲得憑證廢止清單是十分麻煩的。因此，在另一實施例中，將至少一憑證廢止清單儲存於記憶體之公開區域中；該記憶體亦儲存使用者或消費者希望存取之受保護資料或內容。以此方式，每當需要對儲存於記憶體中之內容進行存取時，消費者或使用者將無需自憑證授權單位獲得憑證廢止清單。反而是，消費者或使用者可僅僅擷取儲存於記憶體之公開區域中的至少一憑證廢止清單，且接著轉向並將相同的憑證廢止清單提交給記憶體以供驗認及內容存取。許多類型之記憶體的公開區域通常由主機裝置管理，而非由記憶體自身管理。

在此處所參照的所有專利、專利申請案、文章、書籍、規格、標準、其它出版物、文件與事物皆完全在此引述其整體作為參考。在任何所引用的出版物、文件或事物與本文件的內容之間在一詞彙的用法或定義上有某種程度的不一致或衝突時，應以在本文件中之詞彙的定義與用法為

準。

【實施方式】

圖1之方塊圖顯示示範性記憶體系統，可在該示範性記憶體系統中實施本發明之各項態樣。如示於圖1，該記憶體系統10包含一中央處理單元12、一緩衝管理單元(BMU)14、一主機介面模組(HIM)16及一快閃記憶體介面模組(FIM)18、一快閃記憶體20及一周邊裝置存取模組(PAM)22。記憶體系統10係透過一主機介面匯流排26及埠26a而與一主機裝置24通訊。快閃記憶體20(其可屬於反及(NAND)型)提供用於該主機裝置24之資料儲存，該主機裝置24可以係一數位相機、一個人電腦、一個人數位助理(PDA)、一數位媒體播放機(諸如一MP3播放機)、一行動電話、一視訊轉換器或其他數位裝置或設備。用於中央處理單元12之軟體碼係亦可以儲存於快閃記憶體20之中。快閃記憶體介面模組18係透過一快閃記憶體介面匯流排28及埠28a而連接至該快閃記憶體20。主機介面模組16係適合用於連接至一主機裝置。該周邊裝置存取模組22選擇用於與該中央處理單元12通訊之適當的控制器模組，諸如快閃記憶體介面模組、主機介面模組及緩衝管理單元。於一項實施例中，該系統10於虛線方塊內之所有組件可被包封於一單一單元之中，諸如於記憶體卡或記憶體條10'之內，較佳地係被囊封。該記憶體系統10係可卸除地連接至主裝置24，使得系統10內的內容可被許多不同的主機裝置之每一者所存取。

於下文中，記憶體系統10亦被稱為記憶體裝置10，或僅稱為記憶體裝置或裝置。雖然本文中藉由引用快閃記憶體來闡釋本發明，但是本發明亦可以應用於其他類型記憶體，諸如磁碟，光碟，以及其他類型可重寫非揮發性記憶體系統。

該緩衝管理單元14包含一主機直接記憶體存取(HDMA)32，一快閃直接記憶體存取(FDMA)34，一仲裁器36，一緩衝隨機存取記憶體(BRAM)38及一密碼編譯引擎40。該仲裁器36係一共用匯流排仲裁器，使得僅一主控器(master)或起始器(其可以係該主機直接記憶體存取32、該快閃直接記憶體存取34或中央處理單元12)可於任何時間為作用中狀態，且從屬器或目標係緩衝隨機存取記憶體38。該仲裁器負責通道化適當的起始器請求至該緩衝隨機存取記憶體38。該主機直接記憶體存取32及該快閃直接記憶體存取34負責介於該主機介面模組16、該快閃記憶體介面模組18與該緩衝隨機存取記憶體38或者中央處理單元隨機存取記憶體(CPU RAM)12a之間傳輸之資料。該主機直接記憶體存取32及該快閃直接記憶體存取34之操作係傳統的，且不需要於本文詳細敘述。該緩衝隨機存取記憶體38係用於儲存介於該主機裝置24與快閃記憶體20之間傳通之資料。該主機直接記憶體存取32及該快閃直接記憶體存取34負責介於該主機介面模組16/該快閃記憶體介面模組18與該緩衝隨機存取記憶體38或者中央處理單元隨機存取記憶體12a之間傳送資料，且用於指示區段(sector)完成。

於一項實施例中，記憶體系統10產生用於加密及/或解密之密鑰值，其中，該密鑰值較佳地係實質上無法被外部裝置(諸如主機裝置24)所存取。或者，該密鑰值亦可以在該系統10之外產生(諸如藉由一使用權伺服器(license server)所產生)且被傳送至系統10。不論該密鑰值係如何產生，一旦該密鑰值被儲存於系統10之中，僅經鑑認之實體將能夠存取該密鑰值。然而，加密及解密典型地係以逐一檔案方式實施，此乃因該主機裝置係以檔案之形式將資料讀取及寫入至記憶體系統10。類似於許多其他類型儲存裝置，記憶體裝置10係不管理檔案。雖然記憶體20確實儲存一檔案配置表(FAT)(其中，該等檔案之邏輯位址係被識別)，但是該檔案配置表典型地係由該主機裝置24所存取及管理，而非由該控制器12所存取及管理。因此，為了加密於一特定檔案內的資料，該控制器12係必須依賴該主機裝置，以傳送該記憶體20內該檔案中之資料的邏輯位址，使得可由該系統10使用僅限於系統10可取得之密鑰值來尋找及加密及/或解密該特定檔案之資料。

為了提供對於該主機裝置24及記憶體系統10兩者之控制代碼(handle)，以指向用於以密碼編譯方式處理檔案內的資料之相同的密鑰，該主機裝置係提供用於由該系統10產生或被傳送至系統10之每一密鑰值之參照(reference)，其中，此類參照係可以僅為一密鑰ID。因此，使該主機裝置24相關聯於由系統10用一密鑰ID以密碼編譯方式處理的每一檔案，且使該系統10相關聯於用於用由該主機所提供之

密鑰ID以密碼編譯方式處理資料的每一密鑰值因此，當該主機請求經以密碼編譯方式處理之資料時，其將傳送該請求連同一密鑰ID以及將自記憶體20擷取或儲存於記憶體20內之資料的邏輯位址至系統10。系統10產生或接收一密鑰值，並且使由該主機裝置24所提供之該密鑰ID相關聯於此密鑰值，且實施密碼編譯處理。以此方式，不需要改變記憶體系統10操作之方式，同時允許其使用密鑰而完全控制密碼編譯處理，包含對於密鑰值之獨佔式存取。換句話說，一旦該密鑰值被儲存於系統10之中或由系統10予以產生，該系統係持續允許該主機裝置24藉由具有對於檔案配置表之獨佔式控制而管理該等檔案，同時其係維持對於使用於密碼編譯處理之密鑰值的管理之獨佔式控制。在該等密鑰值被儲存於記憶體系統10之後，該主機裝置24無管理用於資料密碼編譯處理之密鑰值的責任。

於一項實施例中，由該主機裝置24所提供之密鑰ID及傳送至該記憶體系統或由該記憶體系統所產生之密鑰值係形成一數量的兩個屬性，於下文稱為"內容加密密鑰(Content Encryption Key, CEK)"或"CEK"。雖然該主機裝置24可使每一密鑰ID相關聯於一或多個檔案，但是該主機裝置24亦可使每一密鑰ID相關聯於未經組織的資料或者以任何方式組織之資料，且係不受限於組織成為完整檔案之資料。

為了使一使用者或應用程式獲得存取系統10內受保護的內容或區域，將需要使用向系統10預登錄的一認證(credential)來鑑認該使用者或應用程式。一認證相關聯於

經授予給具有該認證之特定使用者或應用程式之存取權。於預登錄程序中，系統10儲存一記錄，該記錄包含該使用者或應用程式之該身份及認證，以及由該使用者或應用程式所決定且透過該主機裝置24提供之與此身份及認證相關聯之存取權。在已經完成該預登錄之後，當該使用者或應用程式請求將資料寫入至記憶體20時，其將需要透過該主機裝置提供其身份及認證、一用於加密該資料之密鑰ID、及經加密資料被儲存之邏輯位址。系統10產生或接收一密鑰值，且使該密鑰值相關聯於由該主機裝置所提供之密鑰ID，且將用於加密待寫入之資料的密鑰值之密鑰ID儲存於用於該使用者或應用程式之記錄或表中。接著，加密該資料且儲存經加密資料於該主機所指定之位址處以及其產生或接收之密鑰值。

當一使用者或應用程式請求自記憶體20讀取經加密資料時，其將需要提供其身份及認證、用於先前用於加密該請求資料之密鑰之密鑰ID、及該經加密資料被儲存之邏輯位址。系統10接著比對由該主機所提供之使用者或應用程式身份及認證與儲存於其之記錄內的身份及認證。假如匹配，則系統10將接著自其之記憶體內擷取與由該使用者或應用程式所提供之密鑰ID相相關聯的密鑰值，使用該密鑰值解密儲存於該主機裝置所指定之位址處之資料，且傳送該解密資料至該使用者或應用程式。

藉由分離該等鑑認認證與用於密碼編譯處理之密鑰的管理，接著分享存取資料之權利而不共用認證係可能的。因

此，一群組具有不同認證之使用者或應用程式可存取用於存取相同資料之相同的密鑰，而該群組以外的使用者係不能存取。雖然一群組內所有使用者或應用程式係可以存取相同的資料，其可以仍然具有不同的權利。因此，某些使用者可以具有唯讀存取，而其他使用者可以具有唯寫存取，而又其他使用者係可以具有唯讀存取及唯寫存取兩者。因為系統10維持一含有該使用者或應用程式之身份及認證、其可存取之密鑰ID以及每一密鑰ID所相關聯之存取權的記錄，所以對於系統10而言，增加或刪除特定使用者或應用程式之密鑰ID且改變與此密鑰ID相關聯的存取權、自一使用者或應用程式委派存取權給另一使用者或應用程式、或者甚至刪除或增加用於使用者或應用程式之記錄或表係可能的，所有皆受控於一適當經鑑認之主機裝置。儲存之記錄可指定一用於存取某些密鑰所需要的安全通道。可使用對稱或非對稱演算法以及密碼來實行鑑認。

特別重要的是該記憶體系統10內的受到保護的內容之可攜性。於存取該密鑰值係受到該記憶體系統控制之實施例中，當併入該系統之記憶體系統或儲存裝置係自一外部系統轉移至另一外部系統時，維持儲存於其內之內容的安全性。不論該密鑰係由該記憶體系統所產生或者起源於該記憶體系統外，外部系統無法存取系統10內之此類內容，除非已以一完全受到該記憶體系統控制之方式鑑認外部系統。甚至在經此鑑認之後，存取係完全受控於該記憶體系統，且外部系統可僅以一根據該記憶體系統內預設記錄所

控制之方式進行存取。假如一請求係不符合此類記錄，則該請求將被拒絕。

為了提供在保護內容上較大的彈性，可以想像僅限於經適當鑑認的使用者或應用程式才能存取該記憶體之某些區域(下文稱為分割區)。當結合上述以密鑰為基礎之資料加密之特徵時，系統10係提供較大的資料保護能力。如示於圖2，該快閃記憶體20係可以使其之儲存容量被分割成為許多分割區：一使用者區域或分割區及自訂分割區。所有使用者及應用程式可存取使用者區域或分割區P0，而不需要鑑認。雖然任何應用程式或使用者可讀取或寫入至儲存於該使用者區域內的資料的所有位元值，假如所讀取之資料係被加密，則無授權解密之使用者或應用程式無法存取由儲存於一使用者區域內的位元值所表示的資訊。舉例而言，由儲存於使用者區域P0內的檔案102及104所顯示。亦儲存於該使用者區域的是未經加密檔案，諸如106，其可被所有應用程式及使用者讀取及瞭解。因此，象徵而言，被加密之檔案係顯示為具有與其相關聯之鎖，諸如對於檔案102及104而言。

雖然未經授權的應用程式或使用者無法瞭解於一使用者區域P0內的經加密檔案，然而此類應用程式或使用者仍然能夠刪除或破壞該檔案，這對於一些應用程式而言可能為不期望的。為了此目的，記憶體20亦包含受保護的自訂分割區，諸如分割區P1及P2，在無事先鑑認情況下無法存取彼等自訂分割區。於此申請案內實施例中所允許的鑑認程

序係說明如下。

如亦顯示於圖2中，各種使用者或應用程式可以存取記憶體20內的檔案。因此，圖2顯示使用者1及2及(執行於裝置上之)應用程式1-4。在彼等實體被允許存取記憶體20內受保護的內容之前，首先藉由一鑑認程序以下文說明之方式鑑認彼等實體。於此程序中，需要於該主機端識別正在請求存取之實體，以用於角色為基礎的存取控制。因此，正在請求存取之實體首先藉由提供諸如"我是應用程式2且我想要讀取檔案1"之資訊，而識別自己。接著，控制器12比對該身份、鑑認資訊及請求與儲存於記憶體20或控制器12內之記錄。假如所有條件係符合，則存取係被授予給此類實體。如示於圖2，使用者1被允許讀取及寫入檔案101至分割區P1，然而除了使用者1具有讀取及寫入檔案106至分割區P0之不受限制的權利之外，其僅可讀取檔案102及104。另一方面，使用者2不被允許存取檔案101及104，然而可讀取及寫入存取檔案102。如示於圖2，使用者1及2具有相同的登入演算法(AES)，而應用程式1及3具有不同的登入演算法(例如，RSA及001001)，其係亦與使用者1及2之登入演算法不同。

安全儲存應用程式(SSA)係一種記憶體系統10之安全性應用程式，且闡釋本發明之一項實施例，其可被使用於實施許多上述的特徵。安全儲存應用程式係可以建構為具有儲存於該記憶體20或中央處理單元12內的非揮發記憶體(未顯示)內的資料庫之軟體或電腦碼，且被讀入至隨機存

取記憶體12a中且由中央處理單元12所執行。所使用參照安全儲存應用程式之字母縮寫係說明於下表：

定義、字母縮寫及縮寫

| | |
|---|---|
| ACR | Access Control Records(存取控制記錄) |
| AGP | ACR Group(存取控制記錄群組) |
| CBC | Chain Block Cipher(鏈區塊編密) |
| CEK | Content Encryption Key(內容加密密鑰) |
| ECB | Electronic Codebook(電子碼本) |
| ACAM | ACR Attributes Management(存取控制記錄屬性管理) |
| PCR | Permissions Control Record(權限控制記錄) |
| SSA | Secure Storage Application(安全儲存應用程式) |
| Entity | 實體，具有真實及個別存在(主機端)且登入該安全儲存應用程式且因而利用其之功能的任何事物 |

**安全儲存應用程式系統說明**

資料安全性、完整性及存取控制係安全儲存應用程式之主要角色。資料係明確地儲存於某種大量儲存裝置上的檔案。安全儲存應用程式系統係位於儲存系統的上方，且增加用於被儲存主機檔案之安全性層級，且透過安全性資料結構而提供安全性功能，如下文所述。

該安全儲存應用程式之主要工作係管理相關聯於記憶體內被儲存的(及安全的)內容的不同權利。記憶體應用程式需要管理多個使用者及對於多個儲存的內容的內容權利。自其之側而來的主機應用程式係看見此類應用程式可見之

驅動程式及分割區，以及管理及描繪該儲存裝置上儲存檔案之位置的檔案配置表(FAT)。

於此情況下，該儲存裝置使用分割成分割區之反及快閃記憶體晶片，然而亦可使用其他行動儲存裝置且係屬於本發明之範疇內。這些分割區係連續的邏輯位址緒(thread)，其中，一起始及一結束位址定義其邊界。因此，假如想要，可以藉由軟體(諸如儲存於記憶體20內的軟體，)而將限制賦加於對於隱藏分割區的存取，此類軟體使此類限制相關聯於此類邊界內的位址。藉由該安全儲存應用程式所管理之分割區邏輯位址邊界，使該安全儲存應用程式可完全辨識分割區。該安全儲存應用程式系統使用分割區，以實際上使資料安全免於未經授權之主機應用程式。對於主機而言，該等分割區係一種定義儲存資料檔案之專屬空間之機制。這些分割區可以係：公開的，其中，可存取該儲存裝置的任何者可看見及知道該分割區存在於該裝置上；或者私有的或隱藏的，其中，僅被選擇的主機應用程式可存取及知道其存在於該儲存裝置上。

圖3係記憶體之示意圖，其顯示記憶體之分割區：P0、P1、P2及P3(顯然地，可採用少於或多於4個的分割區)，其中，P0係一公開分割區，其可由任何實體存取而不需要鑑認。

一私有分割區(諸如P1、P2及P3)隱藏對於其內之檔案的存取。藉由防止該主機存取該分割區，快閃記憶體裝置(例如，快閃記憶體卡)係傳送該分割區內的資料檔案之保

護。然而，此種保護係藉由附加限制於存取儲存於該分割區內該等邏輯位址處之資料，而吞沒駐留於該隱藏分割區內所有檔案。換句話說，該等限制係相關聯於一邏輯位址範圍。可存取該分割區的所有使用者/主機係可未無限制存取內部的所有檔案。為了隔離不同的檔案及另一不同的檔案或者檔案群組，該安全儲存應用程式系統使用密鑰及密鑰參照或密鑰ID，而提供每一檔案或者檔案群組另一層級安全性及完整性。用於加密在不同的記憶體位址處之資料的一特定密鑰值之一密鑰參照或密鑰ID可被類推至一含有該經加密資料之容器(container)或定義域(domain)。因此，於圖4中，該等密鑰參照或密鑰ID(例如，"密鑰1"及"密鑰2")係以繪圖方式顯示為圍繞使用相關聯於該等密鑰ID之密鑰值加密之檔案之區域。

參照圖4，舉例而言，檔案A係可被所有實體存取而不需要任何鑑認，因為其係顯示為不被任何密鑰ID所封入。即使所有實體可讀取或覆寫公開分割區內的檔案B，然而檔案B含有以一具有ID"密鑰1"之密鑰予以加密之資料，所以使得檔案B中所含有的資訊係不能被一實體存取，除非此類實體有權存取此類密鑰。以此方式，使用密鑰值及密鑰參照或密鑰ID係僅提供邏輯保護，其係相對於由上述分割區所提供之保護類型。因此，可存取一分割區(公開的或私有的)之任何主機能夠讀取或寫入整個分割區內的資料，包含經加密資料。然而，因為該資料係被加密，所以未經授權的使用者係僅能夠破壞該資料。較佳地，其在無

偵測之下無法改變資料。藉由限制對於加密及/或解密密鑰之存取，此特徵可僅允許經授權實體使用該資料。於P0中，亦使用一具有密鑰ID"密鑰2"之密鑰來加密檔案B及C。

可透過對稱加密法而提供資料機密性及完整性，該等對稱加密方法使用內容加密密鑰(Content Encryption Key；CEK)，每內容加密密鑰一個。於該安全儲存應用程式實施例中，於內容加密密鑰內的密鑰值係由快閃記憶體裝置(例如，快閃記憶體卡)所產生或接收，該密鑰值係僅內部使用且保持為避開外面世界的秘密。被加密或以密碼編譯處理之資料係亦可以為雜湊的(hashed)或者密碼編譯係鏈區塊的，以確保資料完整性。

並非於該分割區內的所有資料係以不同的密鑰予以加密及相關聯於不同的密鑰ID。於公開或使用者檔案內或於作業系統區域(亦即檔案配置表)內之某些邏輯位址係可以不相關聯於任何密鑰或密鑰參照，且因而係可供可存取該分割區本身之任何實體所使用。

一要求建立密鑰及分割區以及寫入及自其讀取資料或使用該等密鑰之能力的實體係需要透過一存取控制記錄(ACR)而登入該安全儲存應用程式系統。於該安全儲存應用程式系統內一存取控制記錄的特殊權限(privilege)係稱為"動作"(action)。每一存取控制記錄係具有實施下列三種類別的動作之權限：建立分割區及密鑰/密鑰ID；存取分割區及密鑰；以及建立/更新其他存取控制記錄。

存取控制記錄係被組織成群組，稱為存取控制記錄群組或AGP。一旦已經成功鑑認一存取控制記錄，則該安全儲存應用程式開啟一會期(session)，透過該會期，可執行任何存取控制記錄之動作。存取控制記錄及存取控制記錄群組係用於根據原則而控制存取分割區及密鑰之安全性資料結構。

**使用者分割區**

該安全儲存應用程式系統管理一或多個公開分割區，亦稱為使用者分割區。此分割區係存在於該儲存裝置上且係可透過儲存裝置之標準讀取寫入命令予以存取之一或多個分割區。獲得關於分割區之大小以及其存在於該裝置上的資訊較佳地無法對於該主機系統隱藏。

該安全儲存應用程式系統係透過標準讀取寫入命令或該安全儲存應用程式命令而能夠存取分割區。因此，較佳地，存取分割區無法被限用於特定存取控制記錄。然而，該安全儲存應用程式系統可使該等主機裝置能夠限制存取該使用者分割區。可個別啟用/停用讀取及寫入存取。允許所有4種組合(例如，唯讀，唯寫(防寫保護)，讀取及寫入，以及無存取權)。

該安全儲存應用程式系統使存取控制記錄能夠使密鑰ID相關聯於該使用者分割區內的檔案，且使用相關聯於此類密鑰ID之密鑰來加密個別檔案。存取該等使用者分割區內的經加密檔案以及設定對於該等分割區之存取權將使用該安全儲存應用程式命令集而實行。上述特徵亦應用於未經

組織成檔案之資料。

**安全儲存應用程式分割區**

有能夠僅透過該安全儲存應用程式命令存取之(避免未經鑑認的當事人之)隱藏分割區。較佳地，該安全儲存應用程式系統將不允許該主機裝置存取一安全儲存應用程式分割區，除了透過一由登入至一存取控制記錄所建置之會期之外。類似地，較佳地，該安全儲存應用程式將不提供關於一安全儲存應用程式分割區之存在、大小及存取權限之資訊，除非此請求係透過一已建置的會期而來。

對於分割區之存取權係自該存取控制記錄權限推導而來。一旦一存取控制記錄登入至該安全儲存應用程式系統，其可與其他存取控制記錄共用該分割區(敘述如下文)。當建立一分割區時，該主機提供用於該分割區之一參照名稱或者ID(例如，圖3及4中之P0-P3)。在對於該分割區之進一步的讀取及寫入命令之中使用此參照。

**儲存裝置之分割區**

較佳地，該裝置之所有可用儲存容量被配置給使用者分割區及目前組態的安全儲存應用程式分割區。因此，任何重新分割操作可牽涉到現有分割區之重新組態。對於該裝置容量的淨改變(所有分割區之大小的總和)將為零。該裝置記憶體空間內的分割區之ID係由該主機系統所定義。

該主機系統可重新分割現有分割區之一者成為兩個較小的分割區，或者合併兩個現有分割區(其係可以或可以不為相鄰的)成為一分割區。於經分割或經合併分割區內的

資料可被刪除或者保留不碰觸，其係根據該主機之判斷。

因為該儲存裝置之重新分割可導致資料的遺失(由於資料被刪除或者使資料在該儲存裝置之邏輯位址空間內移動)，對重新分割之嚴格限制係由該安全儲存應用程式系統所管理。僅一駐留於一根存取控制記錄群組內的存取控制記錄(下文說明)被允許發佈一重新分割命令，且其僅可參照由其所擁有的分割區。因為該安全儲存應用程式系統不知道資料係如何於該等分割區中組織(檔案配置表或其他檔案系統結構)，所以每當該裝置被重新分割時，重新建構這些結構係該主機之責任。

使用者分割區之重新分割將改變主作業系統所觀看之此分割區的大小及其他屬性。

在分割之後，確保該安全儲存應用程式系統內任何存取控制記錄係不正在參照非現有分割區係該主機系統的責任。假如未適當地刪除或更新這些存取控制記錄，則未來企圖代表這些存取控制記錄存取非現有分割區，將被該系統偵測到及拒絕。關於被刪除的密鑰及密鑰ID採用類似的考量。

**密鑰、密鑰ID及邏輯保護**

當一檔案被寫入至某一隱藏分割區時，其係對於公眾為隱藏。然而，一旦一實體(有敵意的或者無敵意的)獲得對該分割區之知識及存取，則該檔案係變成可用且易於瞭解。為了進一步使該檔案安全，該安全儲存應用程式可加密該隱藏分割區內的檔案，其中，用於存取解密該檔案之

密鑰之認證較佳地不同於用於存取該分割區的認證。由於事實上檔案係完全由該主機所控制及管理，使一內容加密密鑰相關聯於一檔案係一問題。連結該檔案與該安全儲存應用程式認知的某物件(該密鑰ID)修正此問題。因此，當由該安全儲存應用程式建立一密鑰時，該主機係使用由該安全儲存應用程式所建立之該密鑰，使用於該密鑰之該密鑰ID相關聯於經加密之資料。假如該密鑰連同密鑰ID一起被傳送至該安全儲存應用程式，則該密鑰及密鑰ID可輕易地彼此相關聯。

該密鑰值及該密鑰ID提供邏輯安全性。相關聯於一給定密鑰ID之所有資料(不論其之位置為何)係以該內容加密密鑰(CEK)內相同的密鑰值予以編密(cipher)，該內容加密密鑰之參照名稱或密鑰ID係由主機應用程式在建立時獨一地提供。假如一實體(藉由透過一存取控制記錄進行鑑認)獲得對一隱藏分割區之存取，且想要讀取或寫入該分割區內的一經加密檔案，則其係需要可存取與該檔案相關聯之密鑰ID。當授予用於該密鑰ID之密鑰之存取時，該安全儲存應用程式載入相關聯於此密鑰ID之內容加密密鑰內的密鑰值，且在將資料傳送至該主機之前解密該資料，或在將資料寫入至該快閃記憶體20之前加密該資料。於一項實施例中，相關聯於一密鑰ID之內容加密密鑰內的一密鑰值係由該安全儲存應用程式系統隨機建立一次且由其維護。在該安全儲存應用程式系統外的任一實體皆不知道或不可存取內容加密密鑰內之該密鑰值。外面的世界僅提供及使用一

參照或密鑰ID，而非內容加密密鑰內的密鑰值。該密鑰值係受到徹底管理，且較佳地僅可由該安全儲存應用程式存取。或者，該密鑰可被提供給該安全儲存應用程式系統。

該安全儲存應用程式系統使用任一(使用者定義的)下列編密模式(所使用之真正的密碼編譯演算法以及內容加密密鑰內的密鑰值係系統控制的，且係不透露給外面世界)：

區塊模式-資料被分割成為區塊，該等區塊的每一者被個別加密。此模式一般被認為較不安全且易受字典攻擊。然而，其將允許使用者隨機存取任一資料區塊。

鏈模式-資料被分割成為區塊，其係於加密程序期間被鏈鎖(chain)。每一區塊係被使用作為至下一加密程序之輸入之一。於此模式中，雖然被認為較安全，然而資料係自開始至結束予以循序寫入及讀取，建立一可能不被使用者接受的過度耗用(overhead)。

雜湊的-具有額外建立一資料摘要之鏈模式，該資料摘要可被用於確認資料完整性。

**存取控制記錄及存取控制**

該安全儲存應用程式係設計成處置多個應用程式，其中，該等應用程式之每一者於該系統資料庫內被表示為一具有節點的樹。介於該等應用程式之間之相互排斥係藉由確保該等樹的分支之間無串擾而達成。

為了獲得存取該安全儲存應用程式系統，一實體需要透過該系統之存取控制記錄之一者來建置連接。由該安全儲

存應用程式系統根據內建於該使用者選擇待連接之存取控制記錄內的定義來管理登入程序。

該存取控制記錄係一對於該安全儲存應用程式系統之個別登入點。該存取控制記錄係保有登入認證及鑑認方法。亦駐留於該記錄內的係該安全儲存應用程式系統內的登入權限，於其中係讀取及寫入特殊權限。此係顯示於圖5，其係顯示相同存取控制記錄群組中的n個存取控制記錄。此係意謂該n個存取控制記錄中至少一些者可共用對相同密鑰之存取。因此，存取控制記錄#1及存取控制記錄#n共用對具有密鑰ID"密鑰3"之密鑰之存取，其中，存取控制記錄#1及存取控制記錄#n係存取控制記錄ID，且"密鑰3"係用於加密相關聯於"密鑰3"之資料的密鑰之密鑰ID。亦可使用相同的密鑰來加密及/或解密多個檔案，或者多組資料。

該安全儲存應用程式系統支援數種登入該系統的類型，其中，鑑認演算法及使用者認證係可以改變，因為一旦使用者成功登入，該系統內的使用者特殊權限可改變。圖5係再次顯示不同的登入演算法及認證。存取控制記錄#1指定一密碼登入演算法及密碼為認證，而存取控制記錄#2指定一公開密鑰基礎結構(PKI)登入演算法及公開密鑰為認證。因此，為了登入，一實體將需要提交一有效的存取控制記錄ID以及正確的登入演算法及認證。

一旦一實體登入至該安全儲存應用程式系統之一存取控制記錄，則在相關聯於該存取控制記錄的權限控制記錄

(PCR)中定義其權限(其使用安全儲存應用程式命令之權利)。於圖5中，根據所顯示之權限控制記錄，存取控制記錄#1授予對相關聯於"密鑰3"之資料的唯讀權限，且存取控制記錄#2授予對相關聯於"密鑰5"之資料的讀取及寫入權限。

不同的存取控制記錄可共用該系統內共同的利益及特殊權限，諸如藉以讀取及寫入之密鑰。為了達成此目的，共同具有某些事物之存取控制記錄被分組於存取控制記錄群組(ACR群組)中。因此，存取控制記錄#1及存取控制記錄#n共用對一具有密鑰ID"密鑰3"之密鑰之存取。

存取控制記錄群組及其內之存取控制記錄係以樹狀階層架構予以組織，且因此，除了建立保持敏感資料安全之安全密鑰之外，一存取控制記錄較佳地係亦可夠建立對應於其密鑰ID/分割區之其他存取控制記錄實體。這些存取控制記錄子代將具有與其之父代(建立者)相同的或較少的權限，且可被給予父代建立之任何密鑰的權限。不需要增加，該等子代獲得對於其建立之任何密鑰的存取權限。此係顯示於圖6。因此，存取控制記錄群組120內所有存取控制記錄係由存取控制記錄122所建立，且此類存取控制記錄中之兩者係繼承自存取控制記錄122之對存取相關聯於"密鑰3"之資料之權限。

**存取控制記錄群組**

登入至該安全儲存應用程式系統係藉由指定一存取控制記錄群組及該存取控制記錄群組內的一存取控制記錄而實

行。

每一存取控制記錄群組具有一獨一ID(參照名稱)，其係使用作為一索引，以指向在安全儲存應用程式資料庫中的其項目。當建立該存取控制記錄群組時，該存取控制記錄群組名稱被提供給該安全儲存應用程式系統。假如所提供之存取控制記錄群組名稱係已經存在該系統內，則該安全儲存應用程式將拒絕該建立操作。

存取控制記錄群組係用於管理對存取權限及管理權限之委派的限制，如同將於下文中敘述。圖6內兩個樹所提供之功能之一係管理完全分開實體(諸如兩個不同的應用程式，或者兩個不同的電腦使用者)之存取。為此目的，對於兩個存取程序實質上彼此獨立(亦即，實質上無串擾)係可能重要的，即使兩者皆同時發生亦如此。此係意謂每一樹內額外存取控制記錄及存取控制記錄群組的鑑認、權限以及建立未連接至其他樹並且非相依於其他樹。因此，當於記憶體10中使用該安全儲存應用程式系統時，允許該記憶體系統10同時伺服複數個應用程式。亦允許兩個應用程式彼此獨立地存取兩組分開的資料(例如，一組相片及一組歌曲)。此係顯示於圖6。因此，應用程式或使用者正在透過圖6之上方部分的樹內之節點(存取控制記錄)存取之相關聯於"密鑰3"、"密鑰X"及"密鑰Z"之資料可包含相片。應用程式或使用者正在透過圖6之下方部分的樹內之節點(存取控制記錄)存取之相關聯於"密鑰5"及"密鑰Y"之資料可包含歌曲。建立該存取控制記錄群組之存取控制記錄僅

限於當該存取控制記錄群組係無存取控制記錄項目時才具有刪除該存取控制記錄群組的權限。

實體之安全儲存應用程式進入點(entry point)：存取控制記錄

於該安全儲存應用程式系統內的一存取控制記錄敘述該實體被允許登入該系統之方式。當一實體登入該安全儲存應用程式系統時，其係需要指定對應於其將執行之鑑認程序的存取控制記錄。一存取控制記錄包含一權限控制記錄(PCR)，其係顯示使用者一旦如示於圖5之存取控制記錄中定義經鑑認後，該使用者可執行的經授予之動作。該主機端的實體提供所有存取控制記錄資料欄位。

當一實體係成功地登入至一存取控制記錄時，該實體將能夠查詢所有存取控制記錄之分割區及密鑰存取權限以及存取控制記錄屬性管理(ACAM)權限(下文予以敘述)。

**存取控制記錄ID**

當一安全儲存應用程式系統實體起始登入程序時，其係需要指定對應於該登入方法的存取控制記錄ID(如同當建立該存取控制記錄係被時由該主機予以提供)，使得當已經符合所有登入需求時，該安全儲存應用程式將設定正確的演算法及選擇正確的權限控制記錄。當建立該存取控制記錄時，該存取控制記錄ID被提供給該安全儲存應用程式系統。

**登入/鑑認演算法**

該鑑認演算法指定何種登入程序將被該實體所使用，及

何種認證係需要，以提供使用者身份的證明。該安全儲存應用程式系統支援數種標準的登入演算法，範圍為自無程序(及無認證)及以密碼為基礎的程序至一根據對稱或非對稱密碼編譯之雙向鑑認協定。

**認證**

該實體之認證係對應於該登入演算法，且係由該安全儲存應用程式所使用以驗證及鑑認該使用者。一用於認證之範例可以係一用於密碼鑑認之密碼/個人識別碼數字，用於登入演算法驗證之登入演算法密鑰，等等。該等認證(亦即，個人識別碼，對稱密鑰等等)之類型/格式係預先定義的，且係自該鑑認模式中推導出；當建立該存取控制記錄時，該等認證被提供給該安全儲存應用程式系統。該安全儲存應用程式系統對於定義、散佈及管理這些認證沒有責任，惟以公開密鑰基礎結構為基礎的鑑認例外，其中，可使用該裝置(例如快閃記憶體卡)來建立該RSA或其他類型密鑰對，並且公開密鑰可被匯出，以用於認證建立。

**權限控制記錄(PCR)**

權限控制記錄顯示在登入該安全儲存應用程式系統之後授予該實體之事項，及成功地傳送該存取控制記錄之鑑認程序。有三種類型權限類別：分割區及密鑰之建立權限；分割區及密鑰之存取權限；及實體存取控制記錄屬性之管理權限。

**存取分割區**

此段落的權限控制記錄含有該實體於成功地完成該存取

控制記錄階段時可存取之分割區的清單(使用提供給該安全儲存應用程式系統之其ID)。對於每一分割區，存取類型被被限定為唯寫或唯讀或者可以指定完全的寫入/讀取權利。因此，圖5中之該存取控制記錄#1可存取分割區#2並且不可存取分割區#1。指定於該權限控制記錄內的限制套用於該等安全儲存應用程式分割區及公開分割區。

可藉由至裝載該安全儲存應用程式系統之裝置(例如，快閃記憶體卡)之正規讀取及寫入命令來存取該公開分割區，或者藉由安全儲存應用程式命令來存取該公開分割區。當一根存取控制記錄(下文予以說明)被建立成具有限制該公開分割區之權限時，其可傳送權限至其子代。較佳地，一存取控制記錄僅可限制正規讀取及寫入命令存取該公開分割區。較佳地，於該安全儲存應用程式系統內的存取控制記錄係僅只有當其建立時，能夠被限制。一旦一存取控制記錄具有讀取/寫入該公開分割區之權限時，較佳地，無法去除其權限。

**存取密鑰ID**

此段落的權限控制記錄含有當該實體登入程序符合存取控制記錄原則時該實體可存取的密鑰ID之清單所相關聯的資料。所指定之密鑰ID係相關聯於一駐留於出現於該權限控制記錄中之分割區內的一或多個檔案。因為該等密鑰ID係不相關聯於該裝置(例如，快閃記憶體卡)內的邏輯位址，所以當一個以上的分割區係相關聯於一特定存取控制記錄時，該等檔案可位於該等分割區之任一者中。於該權

限控制記錄內指定之密鑰ID可各具有一組不同存取權利。對密鑰ID所指向之資料的存取可被限制成唯寫或唯讀，或者可以指定完全的寫入/讀取權利。

**存取控制記錄屬性管理(ACAM)**

本段落敘述於某些情況下，如何可改變該存取控制記錄系統之屬性。

於該安全儲存應用程式系統中可准許之存取控制記錄屬性管理動作係：

1.建立/刪除/更新存取控制記錄群組及存取控制記錄。

2.建立/刪除分割區及密鑰。

3.委派存取權給密鑰及分割區。

一父代存取控制記錄較佳地無法編輯存取控制記錄屬性管理權限。較佳地，此需要該存取控制記錄之刪除及重新建立。再者，較佳地，對於由該存取控制記錄所建立之一密鑰ID的存取權限無法被去除。

一存取控制記錄係可以具有建立其他存取控制記錄及存取控制記錄群組的容量。建立存取控制記錄亦可以意謂委派由其建立者所持有的一些或全部存取控制記錄屬性管理給彼等存取控制記錄。具有建立存取控制記錄之權限係意謂具有下列動作的權限：

1.定義及編輯子代的認證-較佳地，一旦被該建立存取控制記錄所設定，該鑑認方法無法被編輯。該等認證係可以於已經定義用於子代的鑑認演算法之邊界內被改變。

2.刪除一存取控制記錄。

3.委派建立權限給子代存取控制記錄(因而具有孫代)。

一具有建立其他存取控制記錄權限之存取控制記錄係具有委派解除封鎖(unblock)權限給其建立之存取控制記錄的權限(雖然其係可能不具有解除封鎖存取控制記錄之權限)。該父代將於該子代存取控制記錄中置放一指向其解除封鎖者之參照。

該父代存取控制記錄係具有刪除其子代存取控制記錄的權限之唯一存取控制記錄。當一存取控制記錄刪除其建立之一較低層級存取控制記錄時，由該較低層級存取控制記錄所繁衍的所有存取控制記錄係亦自動被刪除。當一存取控制記錄被刪除，則其建立之所有密鑰ID及分割區被刪除。

一存取控制記錄可更新其自己的記錄係具有兩項例外：

1.密碼/個人識別碼，雖然密碼/個人識別碼係由該建立存取控制記錄所設定，僅由包含密碼/個人識別碼之存取控制記錄可更新該密碼/個人識別碼。

2.一根存取控制記錄係可以刪除自己及其駐留的存取控制記錄群組。

**委派存取權利給密鑰及分割區**

存取控制記錄及其之存取控制記錄群組被組合於樹狀階層架構之中，其中，該根存取控制記錄群組及其內之該等存取控制記錄係於該樹的上方(例如圖6中之根存取控制記錄群組130及132)。於該安全儲存應用程式系統中可具有數個存取控制記錄群組，雖然該等存取控制記錄群組係彼

此完全分離。於一存取控制記錄群組內的一存取控制記錄可委派對於其之密鑰的存取權限給其所在的相同存取控制記錄群組內的所有存取控制記錄，且委派給所有由其建立之存取控制記錄。較佳地，建立密鑰之權限包含委派使用該等密鑰之存取權限之權限。

對於密鑰之權限係分為三種類別：

1.存取-此係定義對於該密鑰之存取權限，亦即，讀取，寫入。

2.擁有權-依據定義，一建立一密鑰之存取控制記錄係其擁有者。此擁有權可自一存取控制記錄委派給另一存取控制記錄(前提係彼等存取控制記錄係在相同的存取控制記錄群組中或在一子代存取控制記錄群組中)。一密鑰之一擁有權提供將其刪除以及委派權限給它之權限。

3.存取權委派-此權限使該存取控制記錄能夠委派其所保有的權利。

一存取控制記錄可委派對其建立之分割區以及其具有存取權限之其他分割區的存取權限。

權限委派係藉由將該等分割區之名稱及密鑰ID加入至指定的存取控制記錄的權限控制記錄之中而實行。委派密鑰存取權限係可以藉由該密鑰ID或者藉由敘述存取權限係用於委派存取控制記錄之所有建立的密鑰而實行。

**存取控制記錄之封鎖及解除封鎖**

一存取控制記錄可具有一封鎖計數器，當該實體對於該系統之存取控制記錄鑑認程序係不成功時累加該封鎖計數

器。當達到某一最大數量之不成功鑑認時，該安全儲存應用程式系統將封鎖該存取控制記錄。

該被封鎖存取控制記錄可被另一存取控制記錄解除封鎖，該另一存取控制記錄係被該被封鎖存取控制記錄所參照。對於該解除封鎖存取控制記錄之參照係被其之建立者予以設定。較佳地，該解除封鎖存取控制記錄係於位於與該被封鎖存取控制記錄之建立者相同的存取控制記錄群組中，且具有"解除封鎖"權限。

該系統內的任何其他存取控制記錄皆無法解除封鎖該被封鎖存取控制記錄。一存取控制記錄可被組態成具有一封鎖計數器，但是無一解除封鎖者存取控制記錄。於此情況下，假如此存取控制記錄被封鎖，則其無法被解除封鎖。

**根存取控制記錄群組-建立一應用程式資料庫**

該安全儲存應用程式系統係設計成處置多個應用程式，並且隔離該多個應用程式之每一者的資料。該存取控制記錄群組系統之該樹結構係用於識別及隔離應用程式特定之資料的主要工具。該根存取控制記錄群組係於一應用程式安全儲存應用程式資料庫樹之頂端，且遵守某些不同的行為規則。可於該安全儲存應用程式系統中組態若干根存取控制記錄群組。於圖6中顯示兩個根存取控制記錄群組130及132。顯然地，可使用較多或較少個存取控制記錄群組，且係屬於本發明之範疇內。

登錄用於一新的應用程式之裝置(例如，快閃記憶體卡)及/或發佈一用於該裝置之新的應用程式之認證係透過將

新的存取控制記錄群組/存取控制記錄樹加入至該裝置的程序而實行。

該安全儲存應用程式系統支援三種不同模式的根存取控制記錄群組建立(以及該根存取控制記錄群組之所有存取控制記錄及其權限)：

1.開放式：不需要任何種類的鑑認之任何使用者或實體，或透過該系統存取控制記錄鑑認之使用者/實體(下文予以敘述)，可建立一新的根存取控制記錄群組。該開放式模式實現在無任何安全性措施之下進行根存取控制記錄群組之建立，同時所有資料傳送係於一開放式通道上(亦即，於一發佈代理者(issuance agency)之安全環境下)或者經由一透過該系統存取控制記錄鑑認所建置之安全通道(亦即，透過空氣(OTA)及後置發佈程序)而實行。

假如該系統存取控制記錄未經組態(此係一選用特徵)，且該根存取控制記錄群組建立模式係設定成"開放式"，則僅該開放式通道選項係可用。

2.受控制的：僅透過該系統存取控制記錄鑑認之實體可建立一新的根存取控制記錄群組。假如系統存取控制記錄未經組態，則該安全儲存應用程式系統無法被設定為此模式。

3.已封鎖：根存取控制記錄群組之建立被停用，且無額外的根存取控制記錄群組可被加入至該系統。

兩個安全儲存應用程式命令控制此特徵(這些命令係可被任何使用者/實體所使用，而不必鑑認)：

1.方法組態命令-用於組態該安全儲存應用程式系統，以使用三種根存取控制記錄群組建立模式中之任一者。僅下列模式改變係被允許：開放式→受控制的，受控制的→已封鎖(亦即，假如該安全儲存應用程式系統目前被組態為受控制的，則其係僅能夠被改變成已封鎖)。

2.方法組態鎖定命令-用於停用該方法組態命令，且永久鎖定目前選擇的方法。

當一根存取控制記錄群組被建立，其處於啟用其存取控制記錄之建立及組態(使用與套用至該根存取控制記錄群組之建立相同的存取限制)之特殊初始化模式。於該根存取控制記錄群組組態程序結束處，當該實體明確地將其切換至操作模式時，不再可更新現有的存取控制記錄，且不再可建立額外的存取控制記錄。

一旦一根存取控制記錄群組係置放於標準模式中，僅能夠藉由透過其存取控制記錄中經指派具有刪除該根存取控制記錄群組之權限的一存取控制記錄登入該系統，才能刪除該根存取控制記錄群組。此係除了該特殊初始化模式之外，根存取控制記錄群組之另一例外；較佳地，其係可含有一具有刪除其自己的存取控制記錄群組之存取控制記錄的僅有的存取控制記錄群組，此係相對於下一樹層級內的存取控制記錄群組。

一根存取控制記錄及一標準存取控制記錄之間之第三及最後差異在於，其係該系統中唯一可具有建立及刪除分割區之權限的存取控制記錄。

**安全儲存應用程式系統之存取控制記錄**

該系統存取控制記錄可用於下列兩項安全儲存應用程式操作：

1.在敵意環境內一安全通道的保護下建立一存取控制記錄/存取控制記錄群組樹。

2.識別及鑑認裝載該安全儲存應用程式系統之裝置。

較佳地，該安全儲存應用程式系統內可僅有一系統存取控制記錄，且一旦被定義，較佳地，其無法被改變。當建立該系統存取控制記錄時，係不需要系統鑑認；只需要一安全儲存應用程式命令。"建立系統存取控制記錄"特徵可被停用(類似於"建立根存取控制記錄群組"特徵)。在該系統存取控制記錄係被建立之後，該"建立系統存取控制記錄"特命令係無效果，因為較佳地，僅一系統存取控制記錄係被允許的。

當於建立之程序中，該系統存取控制記錄係不操作的。於完成時，一特殊的命令係需要被發佈，其指示該系統存取控制記錄係被建立且係準備好進行。在此點之後，該系統存取控制記錄較佳地無法被更新或取代。

該系統存取控制記錄於該安全儲存應用程式中建立該根存取控制記錄/存取控制記錄群組。其具有增加/改變該根層級之權限，直到該主機係滿意其且封鎖其之時間為止。封鎖該根存取控制記錄群組基本上係切斷其接至該系統之連接，且呈現其防竄改證明(tamper proof)。此時，任一者皆無法改變/編輯該根存取控制記錄群組及其內之存取控

制記錄。此係透過一安全儲存應用程式命令而實行。停用根存取控制記錄群組之建立具有一永久的效果且無法進行還原。於圖7顯示牽涉到該系統存取控制記錄的上述特徵。該系統存取控制記錄係用於建立三個不同的根存取控制記錄群組。於這些根存取控制記錄群組被建立之後某一時點時，自該主機傳送該安全儲存應用程式命令，以自該系統存取控制記錄封鎖該等根存取控制記錄群組，藉此停用該"建立根存取控制記錄群組"特徵，如圖7中連接該系統存取控制記錄及該等根存取控制記錄群組之虛線所示。此呈現該三個根存取控制記錄群組之防竄改證明。於該等根存取控制記錄群組被封鎖之前或之後，可使用該三個根存取控制記錄群組來建立子代存取控制記錄群組，以形成三個個別的樹。

上述之特徵係提供內容擁有者於組態具有內容之安全產品的大彈性。安全產品需要被"發佈"。發佈係置放識別密鑰之程序，藉由該識別密鑰，該裝置可識別該主機，且反之亦然。識別該裝置(例如，快閃記憶體卡)係使該主機能夠決定是否其可相信具有其之秘密。另一方面，識別該主機係使該裝置能夠僅限於該主機被允許之情況下強制實行安全性原則(授予及執行一特定主機命令)。

被設計成伺服多數個應用程式之產品將具有數個識別密鑰。該產品可被："預先發佈"，於製造期間在裝運之前儲存密鑰；或者"後發佈"，於裝運之後增加新的密鑰。對於後發佈而言，記憶體裝置(例如，記憶體卡)係需要含有某

種主控或裝置層級密鑰，其係被用於識別被允許將應用程式加入至該裝置之實體。

上述特徵實現將一產品組態成啟用/停用後發佈。此外，可在裝運之後安全地進行該後置發佈組態。該裝置係可以作為一零售產品被購買，該零售產品上不具有除了上述主控或裝置層級密鑰之外的密鑰，且接著係由新的擁有者組態，以啟用或停用進一步的後發佈應用程式。

因此，該系統存取控制記錄之特徵提供完成上述目標之能力：

-不具有系統存取控制記錄之記憶體裝置將允許無限制及無控制增加應用程式。

-不具有系統存取控制記錄之記憶體裝置可被組態成停用該系統存取控制記錄建立，其係意謂無任何控制增加新應用程式之方法(除非建立新的根存取控制記錄群組之特徵亦被停用)。

-具有系統存取控制記錄之記憶體裝置將僅允許經由一透過使用該系統存取控制記錄認證之鑑認程序所建置之安全通道以受控制方式增加應用程式。

-具有系統存取控制記錄之記憶體裝置可被組態成在應用程式已經被加入之前或之後，停用該加入應用程式特徵。

**密鑰ID清單**

密鑰ID係根據特定存取控制記錄請求而建立；然而，於記憶體系統10中，其係僅由該安全儲存應用程式系統所使

用。當一密鑰ID被建立時，下列資料係由建立存取控制記錄所提供或提供給建立存取控制記錄：

1.密鑰ID。該ID係由該實體透過該主機所提供，且係用於參照該密鑰及於所有進一步讀取或寫入存取中使用該密鑰加密或解密之資料。

2.密鑰編密及資料完整性模式(上述已封鎖、已鏈鎖及雜湊模式且如下文所敘述)。

除了主機提供的屬性之外，下列資料係由該安全儲存應用程式系統所維護：

1.密鑰ID擁有者。該存取控制記錄之ID係該擁有者。當一密鑰ID被建立時，該建立者存取控制記錄係其擁有者。然而，密鑰ID擁有權可被轉移至另一存取控制記錄。較佳地，僅該密鑰ID擁有者係被允許轉移一密鑰ID之擁有權及委派一密鑰ID。委派存取權限給相關聯的密鑰及廢止這些權利可由該密鑰ID擁有者或被指派具有委派權限之任何其他存取控制記錄所管理。每當企圖實施彼等操作之任一者時，只有在該請求的存取控制記係被授權之下，該安全儲存應用程式系統才授予此企圖。

2.內容加密密鑰(CEK)。此係其之密鑰值係被用於編密相關聯於該密鑰ID或該密鑰ID所指向之內容之內容加密密鑰。該密鑰值可以係一由該安全儲存應用程式系統所建立之128位元之登入演算法隨機密鑰。

3.MAC及IV值。用於鏈區塊編密(CBC)加密演算法中之動態資訊(訊息鑑認碼及起始向量)。

參照圖8A至16之流程圖而顯示該安全儲存應用程式之各種特徵，其中，一步驟之左方的"H"係意謂該操作係由該主機所實施，且"C"係意謂該操作係由該記憶體卡所實施。雖然參照記憶體卡而顯示這些安全儲存應用程式特徵，應瞭解的是，這些特徵係亦可應用於其他實體形式中之記憶體裝置。為了建立一系統存取控制記錄，該主機發佈一命令給該記憶體裝置10內的安全儲存應用程式，以建立系統存取控制記錄(方塊202)。該裝置10係藉由檢查是否一系統存取控制記錄係已經存在而回應(方塊204，菱形206)。假如其係已經存在，則裝置10傳回失敗及停止(橢圓形208)。假如其係尚未存在，則記憶體10係檢查系統存取控制記錄建立是否被允許(菱形210)，且假如不被允許，則傳回一失敗狀態(方塊212)。因此，可有若干案例，其中，該裝置發行者係不允許一系統存取控制記錄的建立，諸如於所需之安全性特徵係已經被預先決定，使得不需要系統存取控制記錄的情況。假如此係被允許，則該裝置10傳回確定(OK)狀態且等待來自該主機的系統存取控制記錄認證(方塊214)。該主機檢查該安全儲存應用程式狀態及是否該裝置10係已經指示一系統存取控制記錄的建立係被允許(方塊216及菱形218)。假如建立係不被允許或者一系統存取控制記錄係已經存在，則該主機停止(橢圓形220)。假如該裝置10係已經指示一系統存取控制記錄的建立係被允許，則該主機係發佈一安全儲存應用程式命令，以定義其之登入認證，且傳送該登入認證至該裝置10(方塊222)。該

裝置10用所接收之認證來更新一系統存取控制記錄記錄，且傳回"確定"狀態(方塊224)。為了回應此狀態訊號，該主機發佈安全儲存應用程式命令，其指示該系統存取控制記錄係準備好(方塊226)。該裝置10係以鎖定該系統存取控制記錄使得其無法被更新或取代而回應(方塊228)。此係鎖定該系統存取控制記錄之特徵及其用於對於主機識別該裝置10之身份。

用於建立新的樹(新的根存取控制記錄群組及存取控制記錄)的程序係由於該裝置內組態這些功能之方式而決定。圖9係說明該等程序。該主機24及該記憶體系統10兩者遵循此。假如增加新的根存取控制記錄群組係全然被停用，則無法增加新的根存取控制記錄群組(菱形246)。假如其係被啟用但需要一系統存取控制記錄，則該主機透過該系統存取控制記錄進行鑑認，且在發佈"建立根存取控制記錄群組"命令之前建置一安全通道(方塊254)。假如不需要系統存取控制記錄(菱形248)，則該主機24可發佈該"建立根存取控制記錄群組"命令而不需鑑認，且進行至方塊254。假如系統存取控制記錄確實存在，則該主機係可以使用它，即使其係不需要亦如此(未示於該流程圖)。假如該功能被停用，則該裝置(例如快閃記憶體卡)將拒絕建立一新的根存取控制記錄群組的任何企圖，且假如需要系統存取控制記錄，則其將拒絕一建立一新的根存取控制記錄群組而不鑑認之企圖(菱形246及250)。於方塊254中新建立的存取控制記錄群組及存取控制記錄現在係切換成操作模

式，使得於此類存取控制記錄群組內的存取控制記錄無法被更新或改變，且無存取控制記錄可被加入彼等存取控制記錄群組之中(方塊256)。接著，該系統係可選用地被鎖定，使得無法建立額外的根存取控制記錄群組(方塊258)。虛線方塊258係一指示此步驟係選用的步驟的慣例。於本申請案之圖式內的流程圖內所有虛線方塊係選用的步驟。此係允許該內容擁有者封鎖將該裝置10用於可模仿一具有合法內容的真品記憶體裝置的其他非法目的。

為了建立存取控制記錄(除了該根存取控制記錄群組內存取控制記錄以外，如上文所述)，可以具有建立一存取控制記錄之權利的任何存取控制記錄開始(方塊270)，如示於圖10。任何實體可企圖透過該主機24藉由提供進入點之存取控制記錄身份以及具有所有想要建立之必要的屬性之存取控制記錄而進入(方塊272)。該安全儲存應用程式檢查對於該存取控制記錄身份之匹配及具有如此身份之存取控制記錄是否具有建立一存取控制記錄的權限(方塊274)。假如該請求係被驗證為經授權，則該裝置10內的安全儲存應用程式係建立一存取控制記錄(方塊276)。

圖11係顯示兩個存取控制記錄群組，其係顯示一對於使用圖10之方法之安全性應用程式有用的樹。因此，於行銷存取控制記錄群組內具有身份m1之存取控制記錄具有建立一存取控制記錄的權限。該存取控制記錄m1亦具有使用用於讀取或寫入相關聯於密鑰ID"行銷資訊"的資料及相關聯於密鑰ID"價格清單"的資料之密鑰的權限。使用圖10之方

法，建立具有兩個存取控制記錄的銷售存取控制記錄群組：s1及s2，其係僅具有對於用於存取相關聯於該密鑰ID"價格清單"之定價資料之密鑰的讀取權限，而無存取相關聯於該密鑰ID"銷售資訊"之資料所需的密鑰的讀取權限。以此方式，具有存取控制記錄s1及s2之實體係僅能夠讀取而不能夠改變定價資料，且將不可存取行銷資料。另一方面，存取控制記錄m2不具有建立存取控制記錄的權限，且僅具有對於用於存取相關聯於密鑰ID"價格清單"及相關聯於密鑰ID"行銷資訊"之資料的密鑰之讀取權限。

因此，可以使用上述之方式委派存取權，其中，m1委派讀取定價資料的權利給s1及s2。在牽涉到大型行銷及銷售群組之情況下，此係特別有用的。在僅一或少數銷售人員之下，可以不需要使用圖10之方法。反而是，存取權係可以由一存取控制記錄委派給於相同的存取控制記錄群組內於一較低層級或相同層級的存取控制記錄，如示於圖12。首先，該實體進入用於此類存取控制記錄群組的樹，其方式係藉由以一上述方法透過該主機指定該樹中之一存取控制記錄(方塊280)。接著，該主機將指定該存取控制記錄及委派給其之權利。該安全儲存應用程式係檢查用於此類存取控制記錄的樹及該存取控制記錄是否具有委派權利給指定的另一存取控制記錄的權限(方塊282)。假如其是，則該等權利係被委派(方塊284)；假如不是，則停止。該結果係顯示於圖13。於此情況下，存取控制記錄m1具有委派讀取權限給該存取控制記錄s1的權限，使得在委派之後，

s1將能夠使用一存取價格資料的密鑰。假如m1係具有存取定價資料及如此委派之權限的相同或較大的權利，則此可被實施。於一項實施例中，m1在委派之後維持其存取權。較佳地，可在受限制條件下(而非永久地)委派存取權，諸如一段有限的時間、有限的存取次數等等。

圖14顯示用於建立一密鑰及密鑰ID之程序。該實體透過一存取控制記錄進行鑑認(方塊302)。該實體請求用由該主機所指定之ID來建立密鑰建立(方塊304)。該安全儲存應用程式檢查及觀看所指定之存取控制記錄是否具有如此實施之權限(菱形306)。舉例而言，假如該密鑰係被用於存取一特別分割區內的資料，則該安全儲存應用程式將檢查及觀看該存取控制記錄是否可存取此分割區。假如該存取控制記錄經授權，則該記憶體裝置10建立一相關聯於由該主機所提供之密鑰ID的密鑰值(方塊308)，且儲存該密鑰ID於該存取控制記錄之中，及儲存該密鑰值於其記憶體(控制器相關聯的記憶體或記憶體20)內，且根據由該實體所提供之資訊而指派權利及權限(方塊310)，且用此類經指派的權利及權限來修改此類存取控制記錄的權限控制記錄(方塊312)。因此，該密鑰之建立者具有所有可取得的權利，諸如讀取及寫入權限、委派及與相同存取控制記錄群組內其他存取控制記或於一較低層級之存取控制記錄共用之權利，及轉移該密鑰之擁有權之權利。

一存取控制記錄可改變於該安全儲存應用程式系統內另一存取控制記錄之權限(或全然存在)，如示於圖15。一實

體係可以如前一樣透過一存取控制記錄而進入一樹；於一情況下，該實體被鑑認且接著其指定一存取控制記錄(方塊330，332)。其請求一目標存取控制記錄之刪除或一目標存取控制記錄內之權限(方塊334)。假如所指定之存取控制記錄或於如此時間為作用中狀態之存取控制記錄具有如此實施之權利(菱形336)，則該目標存取控制記錄被刪除，或者該目標存取控制記錄之權限控制記錄被改變以刪除此類權限(方塊338)。假如此未經授權，則該系統停止。

在上述程序之後，該目標將不再能夠存取在該程序之前其能夠存取之資料。如示於圖16，一實體係可能企圖進入該目標存取控制記錄(方塊350)，且發現到該鑑認程序失敗，因為先前存在的存取控制記錄ID係不再出現於該安全儲存應用程式之中，使得存取權係被拒絕(菱形352)。假設該存取控制記錄ID尚未被刪除，則該實體指定一存取控制記錄(方塊354)及於一特別分割區內的密鑰ID及/或資料，且接著該安全儲存應用程式根據此類存取控制記錄的權限控制記錄檢查是否准許該密鑰ID或分割區存取請求(菱形358)。假如該權限已被刪除或已經過期，則該請求再次被拒絕。否則，該請係被授予(方塊360)。

上述程序敘述該裝置(例如，快閃記憶體卡)如何管理對受保護的資料之存取，而不論是否該存取控制記錄及其之權限控制記錄係剛剛被另一存取控制記錄予以改變或者開始係如此組態。

**會期**

該安全儲存應用程式系統被設計成處置同時登入的多個使用者。當使用此特徵時，僅在用於鑑認一特定實體的存取控制記錄具有用於所請求動作的權限之情況下，由該安全儲存應用程式所接收之所有命令係相關聯於該實體且被執行。

多個實體係透過會期觀念予以支援。一會期係於該鑑認程序期間予以建置，且由該安全儲存應用程式系統指派一會期ID。該會期ID係內部相關聯於用於登入該系統之存取控制記錄，且被匯出給該實體，以在所有進一步的安全儲存應用程式命令中使用。

該安全儲存應用程式系統支援兩種類型會期：開放式會期及安全會期。與一特定鑑認程序相關的會期類型係定義於存取控制記錄之中。該安全儲存應用程式系統將以類似於強制實行該鑑認本身之方式強制實行會期建置。因為該存取控制記錄定義該等實體權限，所以此機制使系統設計者能夠使安全通道相關聯於存取特定密鑰ID或調用特定存取控制記錄管理操作(亦即，建立新的存取控制記錄及設定認證)。

**開放式會期**

開放式會期係一用一會期ID識別但不以匯流排加密之會期，所有命令及資料係公開被傳送。此種操作模式較佳地係用於一多使用者或多實體環境中，其中，該等實體係非構成威脅模型亦非於該匯流排上的竊聽的一部分。

雖然不保護資料之傳送亦不實現該主機端之應用程式之

間之有效率的防火牆，但是該開放式會期模式使該安全儲存應用程式系統能夠僅允許存取目前經鑑認的存取控制記錄所允許的資訊。

該開放式會期係亦能夠被使用於一分割區或一密鑰係需要被保護之情況。然而，在一有效鑑認程序之後，存取被授予給該主機上所有實體。各種主機應用程式用以獲得經鑑認存取控制記錄之權限而需要共用的唯一事物係會期ID。此係顯示於圖17A。在線400上方之步驟係由該主機24所採用之步驟。在一實體係對於存取控制記錄1經鑑認(方塊402)之後，其請求存取該記憶體裝置10內一相關聯於一密鑰ID X之檔案(方塊404，406及408)。假如該存取控制記錄1之該權限控制記錄允許此類存取，則裝置10授予該請求(菱形410)。假如不允許，則該系統返回方塊402。在鑑認完成之後，該記憶體系統10係僅藉由該指派的會期ID(且非該等存取控制記錄認證)而識別正在發佈一命令的實體。一旦該存取控制記錄1係於一開放式會期中獲得存取其之權限控制記錄內相關聯於該等密鑰ID之資料，則任何其他應用程式或使用者可藉由指定介於該主機24上不同的應用程式所共用的正確會期ID，來存取相同的資料。此特徵於應用程式中為有利的，其中，對於使用者而言，僅能夠登入一次、能夠存取所有關聯於不同應用程式用以實行登入之帳戶的資料，係更方便的。因此，一行動電話的使用者可能夠存取記憶體20內儲存的電子郵件且聽儲存的音樂，而不需要多次登入。另一方面，不被該存取控制記

錄1所內含的資料係不可存取。因此，相同的行動電話的使用者係可以具有有價值的內容，諸如可透過一分離的帳戶存取控制記錄2存取之遊戲及相片。此係他不想要借他的電話的其他人存取的資料，即使他可能不介意其他人可以透過他的第一帳戶存取控制記錄1存取資料。於開放式會期中將對資料之存取分開成為兩個分離帳戶且同時允許存取存取控制記錄1，提供容易使用以及提供有價值的資料之保護。

為了更進一步易於在該等主機應用程式之間共用該會期ID之程序，當一存取控制記錄正在請求一開放式會期時，其可明確地請求該會期將被指派"0" ID。以此方式，應用程式可被設計成使用一預先定義的會期ID。唯一限制係，因為明顯的理由，於一特定時間僅可鑑認一正在請求會期0之存取控制記錄。一鑑認另一正在請求會期0之存取控制記錄的企圖將被拒絕。

**安全會期**

為了增加一層安全性，該會期ID可被使用，如示於圖17B。接著，該記憶體10亦儲存作用中狀態會期之會期ID。於圖17B中，舉例而言，為了能夠存取一相關聯於密鑰ID X之檔案，在該實體被允許存取該檔案之前，該實體亦將需要提供一會期ID，諸如會期ID "A"(方塊404，406，412及414)。以此方式，除非該請求實體係知道正確的會期ID，否則其無法存取該記憶體10。因為該會期ID係於該會期結束之後被刪除且對於每一會期而言係不同的，所以

一實體係僅當其已經能夠提供會期號碼時，才能能夠獲得存取。

該安全儲存應用程式系統係藉由使用該會期號碼，而追蹤是否一命令係真的來自正確經鑑認的實體。對於有攻擊者將嘗試使用一開放式通道以傳送有惡意的命令之恐嚇的應用程式及使用情況而言，該主機應用程式係使用一安全會期(一安全通道)。

當使用一安全通道時，該會期ID以及整個命令係以安全通道加密(會期)密鑰予以加密，且該安全性等級係與該主機端實施一樣高。

**終止一會期**

於下列任一狀況中，終止一會期，且登出該存取控制記錄：

1.該實體係發佈一明確的會期結束命令。

2.通訊時間逾期。一特定實體在一段期間(如存取控制記錄參數之一者所定義)未發佈任何命令。

3.在裝置(例如快閃記憶體卡)重設及/或電源循環之後，終止所有開放式會期。

**資料完整性服務**

該安全儲存應用程式系統驗證該安全儲存應用程式資料庫(其係含有所有存取控制記錄、權限控制記錄等等)之完整性。此外，透過密鑰ID機制而提供用於實體資料的資料完整性服務。

假如一密鑰ID經組態以用雜湊作為其加密演算法，則該

雜湊值係與該內容加密密鑰及IV並排地儲存於該內容加密密鑰記錄之中。於寫入操作期間計算及儲存雜湊值。雜湊值係於讀取操作期間再次被計算，且與於先前寫入操作期間所儲存之值相比較。每當該實體正在存取該密鑰ID時，額外的資料係(以密碼編譯方式)串接至舊的資料及經更新的(用於讀取或寫入之)適合雜湊值。

因為僅該主機知道相關聯於一密鑰ID或由一密鑰ID指向的資料檔案，所以該主機係以下列方式明確地管理該資料完整性功能的數項態樣：

1.一相關聯於一密鑰ID或由一密鑰ID指向的資料檔案係從頭到尾被寫入或讀取。存取該檔案之部分的任何企圖將使其混亂，原因係該安全儲存應用程式系統正在使用一鏈區塊密碼加密方法且產生該整個資料的一雜湊訊息摘要。

2.不需要處理一連續串流內(該資料串流可交錯其他密鑰ID之資料串流，且係可以於多個會期上分割)的資料，原因係中間的雜湊值係由該安全儲存應用程式系統所維護。然而，假如該資料串流係重新開始，則該實體將需要明確地指示該安全儲存應用程式系統重設該等雜湊值。

3.當一讀取操作完成時，該主機明確地請求該安全儲存應用程式系統藉由比較所讀取雜湊其及寫入操作期間所計算之雜湊值來確認該讀取之雜湊。

4.該安全儲存應用程式系統亦提供一"設設讀取"操作。此特徵係將串流經過加密引擎的資料，然而將不傳送其出去至該主機。此特徵可被用於在資料真正自該裝置(例如

快閃記憶體卡)讀取出之前，確認資料完整性。

**隨機號碼產生**

該安全儲存應用程式系統將使外部實體能夠使用內部隨機號碼產生器，且請求隨機號碼被使用於該安全儲存應用程式系統之外。此服務係可被任何主機使用，且不需要鑑認。

**RSA密鑰對產生**

該安全儲存應用程式系統將使外部使用者能夠使用內部RSA密鑰對建立特徵，且請求一對密鑰對被使用於該安全儲存應用程式系統之外。此服務係可被任何主機使用，且不需要鑑認。

**替代實施例**

不使用階層架構方式，類似的結果可使用一資料庫方式而達成，如示於圖18。

如示於圖18，一含有用於實體之認證、鑑認方法、失敗嘗試的最大次數及解除封鎖所需之認證最小數目的清單可被輸入儲存於控制器12或記憶體20內之一資料庫之中，該清單使認證需求相關於由該記憶體10之該控制器12所實施該資料庫中之原則(對於密鑰及分割區之讀取、寫入存取，安全通道需求)。亦儲存於該資料庫的係對於存取密鑰及分割區之約束及限制。因此，一些實體(例如，系統管理者)係可以於一白色清單上，其係意謂這些實體可存取所有密鑰及分割區。其他實體係可以於一黑色清單上，且其存取任何資訊之企圖將被封鎖。該限制可以係全域

性，或密鑰及/或分割區特定的。此係意謂僅某些實體可存取某些特定密鑰及分割區，且某些實體無法如此實施。約束亦能夠被置放於內容本身上，而不論內容所在的分割區或用於加密或解密該內容之密鑰為何。因此，某些資料(例如，歌曲)係可以具有其僅能夠被前5個存取它們的主機裝置所存取的屬性，或者其他資料(例如，電影)係僅能夠被讀取有限次數的屬性，而不論哪些實體具有存取權。

鑑認

密碼保護

· 密碼保護係意謂需要提交一密碼，以存取受保護的區域。除非其無法超過一個密碼，否則密碼可相關聯於不同的權利，諸如讀取存取及/或寫入存取。

· 密碼保護係意謂該裝置(例如，快閃記憶體卡)可驗證由該主機所提供之密碼，亦即該裝置亦具有儲存於裝置管理安全記憶體區域內的密碼。

發佈及限制

· 密碼係受限於重新播放攻擊。因為在每一提交之後密碼係不改變，所以其可相同地重新傳送。其係意謂假如將被保護的資料係有價值的，則密碼係不應該被使用，且通訊匯流排係容易被存取。

· 密碼可保護存取儲存的資料，然而係不應該被使用於保護資料(非一密鑰)。

· 為了增加與密碼相關聯的安全性等級，其可使用一主控密鑰而多樣化，結果為駭客一份資料係不搞垮整個系

統。一以會期密鑰為基礎的安全通訊通道可被用於傳送該密碼。

圖19繪示使用一密碼進行鑑認之流程圖。該實體係傳送一帳戶ID及密碼至系統10(例如，快閃記憶體卡)。該系統係檢查看看是否該密碼係匹配於其記憶體內的密碼。假如其係匹配，則傳回經鑑認狀態。否則，累加用於該帳戶之錯誤計數器，且該實體係被要求重新輸入一帳戶ID及密碼。假如該計數器係滿溢，則該系統傳回存取被拒絕的狀態。

對稱密鑰

對稱密鑰演算法係意謂於加密及解密兩端使用相同的密鑰。其係意謂該密鑰係在通訊之前已經預先同意。此外，每一端應該實施彼此的逆演算法，亦即，於一端之加密演算法及於另一端之解密演算法。兩端係不需要實施該兩種演算法以通訊。

鑑認

· 對稱密鑰鑑認係意謂裝置(例如，快閃記憶體卡)及主機共用相同的密鑰且具有相同的密碼編譯演算法(直接及逆向，例如，DES及DES-1)。

· 對稱密鑰鑑認係意謂挑戰-回應(保護防止重新播放攻擊)。受保護的裝置產生一用於其他裝置的挑戰，且兩者計算回應。該鑑認裝置傳回該回應，且該受保護裝置檢查該回應，且據此因而確認鑑認。接著，與鑑認相關的權利可被授予。

鑑認可以係：

· 外部的：該裝置(例如快閃記憶體卡)鑑認外部的世界，亦即，該裝置確認一給定主機或應用程式之認證。

· 相互的：於兩端上產生一挑戰。

· 內部的：該主機應用程式鑑認該裝置(亦即，快閃記憶體卡)，亦即，主機檢查是否裝置對於其之應用程式而言係真實的。

為了增加整個系統的安全性等級(亦即，破壞一者係非破壞全部)：

· 對稱密鑰係通常使用一主控密鑰而與多樣化結合。

· 相互鑑認使用來自兩端的挑戰，以確保挑戰係一真實的挑戰。

加密

對稱密鑰密碼編譯亦用於加密，因為其係一非常有效率的演算法，亦即，其係不需要一功能強大的中央處理單元來處置密碼編譯。

當用於使一通訊通道安全時：

· 兩端裝置必須知道用於使該通道安全(亦即，加密所有傳出資料且解密所有傳入資料)的會期密鑰。通常使用一預先共用的安全對稱密鑰或使用公開密鑰基礎結構而建置此會期密鑰。

· 兩端裝置係必須知道及實施相同的密碼編譯演算法。

簽名

對稱密鑰亦可使用於簽名資料。於此情況下，簽名係加

密的一部分結果。保持該結果為部分的允許簽名與所需一樣多次，而不顯露該密鑰值。

發佈及限制

對稱演算法係非常有效率且安全的，然而其係以一預共用秘密為基礎。該發佈係以一動態方式安全地共用此秘密，且可能使其為隨機的(像是一會期密鑰)。此想法係一共用的秘密係不易於長期保持安全的，且係幾乎不可能與多個人員共用。

為了促進此操作，已經發明公開密鑰演算法，因為其係允許秘密交換，而不共用該等秘密。

非對稱鑑認程序

以非對稱密鑰為基礎的鑑認使用傳送命令之一系列資料，其係最終建構用於安全通道通訊之會期密鑰。基本協定係對於該安全儲存應用程式系統鑑認該使用者。協定變化係允許：相互鑑認，其中，該使用者係必須鑑認他想要使用的存取控制記錄；以及雙因素鑑認。

較佳地，該安全儲存應用程式之非對稱鑑認協定使用公開密鑰基礎結構(PKI)及RSA演算法。如由這些演算法所定義，該鑑認程序內每一當事人係被允許建立其自己的RSA密鑰對。每一RSA密鑰對係由公開密鑰及私有密鑰所組成。因為該等密鑰係匿名的，所以其無法提供身份的證明。該公開密鑰基礎結構層尋求一第三方且受信任的當事人，其簽名該等公開密鑰之每一者。該受信任的當事人之公開密鑰係於將彼此鑑認之當事人之間預先共用，且係使

用於驗證該等當事人的公開密鑰。一旦信任係被建置(兩個當事人決定由另一當事人所提供之公開密鑰可被信任)，該協定係持續鑑認(驗證每一當事人保存匹配的私有密鑰)以及密鑰交換。此可透過示於圖22及23中之挑戰回應機制而實施，如下文所述。

含有該加上簽名的公開密鑰之結構被稱為一憑證。簽名該等憑證的受信任當事人被稱為憑證授權單位(CA)。為了使一當事人成為經鑑認，其具有一RSA密鑰對及一證明該公開密鑰的真實性之憑證。該憑證係由一憑證授權單位加上簽名，該憑證授權單位係受到另一(鑑認)當事人信任。該鑑認當事人係被期望於其之財產上具有其受信任的憑證授權單位之公開密鑰。

該安全儲存應用程式系統允許憑證鏈。此係意謂被識別之當事人的公開密鑰係可以由一與該識別當事人所信任的不同的憑證授權單位加上簽名。於此情況下，該被識別當事人除了提供其自己的憑證之外，亦提供對其公開密鑰加上簽名之憑證授權單位的憑證。假如該第二層級憑證係仍然不被另一當事人所信任(未被其受信任的憑證授權單位加上簽名)，則可提供一第三層級憑證。於此憑證鏈演算法之中，每一當事人係將持有需要鑑認其公開密鑰之憑證的完整清單。此係顯示於圖23及24。用於此種類型存取控制記錄相互鑑認所需要之認證係所選長度之RSA密鑰對。

安全儲存應用程式憑證

安全儲存應用程式係採用[X.509]第3版數位憑證。

[X.509]係一種一般用途標準；於此所述之該安全儲存應用程式憑證資料檔係進一步說明及限制憑證定義欄位之內容。該憑證資料檔亦定義用於憑證鏈、安全儲存應用程式憑證之確認及憑證廢止清單(CRL)資料檔之管理所定義之信任的階層架構。

該憑證係被認為為公開資訊(如同內部的公開密鑰)，且因而係不被加密。然而，其包含一RSA簽名，其係驗證該公開密鑰以及所有其他資訊欄位未被竄改。

[X.509]係定義每一欄位係使用ASN.1標準而格式化，其接著使用用於資料編碼之DER格式。

安全儲存應用程式憑證概觀

顯示於圖20及21之該安全儲存應用程式憑證管理架構之一項實施例包含用於該主機之無限層級階層架構及用於該裝置至多3層級階層架構，然而對於該裝置可使用多於或少於3的層級數。

主機憑證階層架構

該裝置係根據兩項因素而鑑認主機：儲存於該裝置內的根憑證授權單位憑證(作為一存取控制記錄認證，於該存取控制記錄之建立時予以儲存)及由嘗試存取該裝置之實體所提供的憑證/憑證鏈(用於該特定存取控制記錄)。

對於每一存取控制記錄而言，該主機憑證授權單位係作為該根憑證授權單位(此係駐留於該等存取控制記錄認證內的憑證)。舉例而言，對於一存取控制記錄而言，該根憑證授權單位可以係"主機1憑證授權單位(第2層級)憑證"，

且對於另一存取控制記錄而言，該根憑證授權單位可以係"主機根憑證授權單位憑證"。對於每一存取控制記錄而言，持有由該根憑證授權單位簽名之一憑證(或者一連接該根憑證授權單位至終端實體憑證之憑證鏈)之每一實體可登入該存取控制記錄，前提係其具有用於該終端實體憑證之對應的私有密鑰。如上文所述，憑證係公開的知識，且係非保持秘密的。

由該根憑證授權單位所發佈之所有憑證擁有者(及對應的私有密鑰)可登入該存取控制記錄的事實係意謂，對於一特定存取控制記錄之鑑認係由儲存於該存取控制記錄認證內之根憑證授權單位的發行者所決定。換句話說，該根憑證授權單位之發行者可以係管理該存取控制記錄的鑑認方案的實體。

主機根憑證

該根憑證係該安全儲存應用程式正在用於開始驗證嘗試登入(主機)之實體的公開密鑰之受信任的憑證授權單位憑證。當該存取控制記錄被建立以作為該等存取控制記錄認證之部分時，提供此憑證。其係用於該公開密鑰基礎結構系統之信任的根，且因此，其係假設由一受信任的實體(一父代存取控制記錄或製造/組態受信任的環境)所提供。該安全儲存應用程式使用其公開密鑰以驗證該憑證簽名而驗證該憑證。該主機根憑證係經加密地儲存於一非揮發性記憶體之中(未顯示於圖1)，且該裝置之秘密密鑰較佳地係僅可由系統10之圖1的中央處理單元12所存取。

主機憑證鏈

主機憑證鏈係於鑑認期間提供給該安全儲存應用程式的憑證。在完成該主機憑證鏈之處理之後，於該裝置中應未儲存該主機憑證鏈之回憶。

圖20繪示若干不同的主機憑證鏈之主機憑證層級階層架構之示意圖。如示於圖20，該主機憑證係可以具有許多不同的憑證鏈，其中，僅三個係被顯示：

A1. 主機根憑證授權單位憑證502、主機1憑證授權單位(第二層級)憑證504及主機憑證506；

B1. 主機根憑證授權單位憑證502、主機n憑證授權單位(第二層級)憑證508，主機1憑證授權單位(第三層級)憑證510及主機憑證512；

C1. 主機根憑證授權單位憑證502、主機n憑證授權單位(第二層級)憑證508及主機憑證514。

上述之三個憑證鏈A1、B1及C1係顯示可被用於證明該主機之公開密鑰係為真實的之三個可能的主機憑證鏈。參照上述憑證鏈A1及圖20，該主機1憑證授權單位(第二層級)憑證504內的公開密鑰係藉由該主機根憑證授權單位的私有密鑰而被簽名(亦即，藉由加密該公開密鑰之摘要)，該主機根憑證授權單位的公開密鑰係於該主機根憑證授權單位憑證502之內。於該主機憑證506內的主機公開密鑰係接著由該主機1憑證授權單位(第二層級)之該私有密鑰所簽名，該主機1憑證授權單位(第二層級)的公開密鑰係提供於該主機1憑證授權單位(第二層級)憑證504之內。因此，一

具有該主機根憑證授權單位的公開密鑰之實體係將能夠驗證上述憑證鏈A1之真實性。作為第一步驟，該實體係使用其擁有之該主機根憑證授權單位之該公開密鑰，以解密由該主機傳送至其之主機1憑證授權單位(第二層級)憑證504內經簽名的公開密鑰，且比較該經解密的經簽名公開密鑰及由該主機所傳送之該主機1憑證授權單位(第二層級)憑證504內之未經簽名的公開密鑰的摘要。假如該兩者係匹配，則該主機1憑證授權單位(第二層級)之該公開密鑰係被鑑認，且該實體接著將使用該主機1憑證授權單位(第二層級)之該經鑑認公開密鑰，以解密由該主機傳送之該主機憑證506內之該主機1憑證授權單位(第二層級)的私有密鑰所簽名之主機的公開密鑰。假如該經解密的簽名值匹配由該主機所傳送之該主機憑證506內之該公開密鑰的摘要之值，則該主機之該公開密鑰係接著亦被鑑認。可用類似的方式使用該憑證鏈B1及C1以用於鑑認。

如同將由上述牽涉到憑證鏈A1之程序所注意到，來自需要被該實體驗證之該主機的第一公開密鑰係於該主機1憑證授權單位(第二層級)內的密鑰，且非為該主機根憑證授權單位憑證。因此，該主機僅需要傳送該主機1憑證授權單位(第二層級)憑證504及該主機憑證506給該實體，使得該主機1憑證授權單位(第二層級)憑證將為該憑證鏈中需要被傳送的第一憑證。如上文所示，憑證驗證的序列係如下。該驗證實體(於此情況下，即記憶體裝置10)首先驗證該憑證鏈中該第一憑證內的公開密鑰的真實性，其在此情

況下係在該根憑證授權單位下方的憑證授權單位的憑證504。在此類憑證內的公開密鑰被驗證為真實的之後，裝置10接著係進行至驗證下一憑證，於此情況下係該主機憑證506。藉由相同的符記，可應用一類似的驗證序列，其中，該憑證鏈含有兩個以上憑證，其開始於緊接在該根下方的憑證，而結束於將被鑑認之實體的憑證。

裝置憑證階層架構

該主機係根據兩項因素而鑑認該裝置：儲存於該主機內的裝置根憑證授權單位憑證及由該裝置提供給該主機之憑證/憑證鏈(其係於該存取控制記錄建立時提供給該裝置，以作為一認證)。用於由該主機鑑認該裝置的程序係類似於上文所述該裝置鑑認該主機之程序。

裝置憑證鏈

裝置憑證鏈係該存取控制記錄之密鑰對的憑證。其係當該存取控制記錄被建立時提供給該卡。該安全儲存應用程式個別儲存這些憑證，且將於鑑認期間，逐一地提供憑證給該主機。該安全儲存應用程式使用這些憑證以鑑認該主機。該裝置能夠處理一含3個憑證的憑證鏈，然而可使用不同於3個的若干憑證。憑證的數量係因存取控制記錄不同而改變。其係當該存取控制記錄被建立時予以決定。該裝置可傳送該憑證鏈給該主機，然而，其係不需要分析它們，原因係其係不使用該憑證鏈資料。

圖21顯示裝置憑證層級階層架構之示意圖，用於顯示使用安全儲存應用程式用於諸如儲存裝置之裝置的1至n不同

的憑證鏈。示於圖21之該n個不同的憑證鏈係如下：

A2. 裝置根憑證授權單位憑證520，裝置1憑證授權單位(製造商)憑證522及裝置憑證524；

B2. 裝置根憑證授權單位憑證520，裝置n憑證授權單位(製造商)憑證526及裝置憑證528。

該安全儲存應用程式裝置係可以由1至n個不同的製造商所製造，每一製造商係具有其自己的裝置憑證授權單位憑證。因此，於用於一特定裝置之裝置憑證內的公開密鑰係藉由其製造商的私有密鑰予以簽名，且接著該製造商的公開密鑰係由該裝置根憑證授權單位的私有密鑰予以簽名。該裝置之該公開密鑰被驗證的方式係類似於上述該主機之公開密鑰之情況下的方式。當在上述用於主機之憑證鏈A1之驗證之情況時，不需要傳送該裝置根憑證授權單位憑證，且該等憑證鏈內需要被傳送之第一憑證係裝置i憑證授權單位(製造商)憑證，其後接著裝置憑證，i係自1至n的整數。

於示於圖21之實施例中，該裝置將提交兩個憑證：裝置i憑證授權單位(製造商)憑證，其後接著其自己的裝置憑證。該裝置i憑證授權單位(製造商)憑證係製造該如此裝置之製造商且係提供私有密鑰以簽名該裝置之公開密鑰的製造商的憑證。當該裝置i憑證授權單位(製造商)憑證係由該主機予以接收時，該主機使用其擁有的根憑證授權單位之公開密鑰，以解密及驗證該裝置i憑證授權單位(製造商)公開密鑰。假如此驗證失敗，則該主機將中止該程序，且通

知該裝置鑑認已失敗。假如鑑認成功，則該主機係傳送一請求給該裝置，以用於下一憑證。接著，該裝置係以一類似的方式，傳送其將被該主機驗證之自己的裝置憑證。

上述驗證程序係亦更詳細地顯示於圖22及23。於圖22中，"安全服務模組系統"係一軟體模組，其係實施本文所述之安全儲存應用程式系統以及下文敘述之其他功能。安全服務模組系統係可以建構為軟體或電腦碼，其具有儲存於記憶體20或中央處理單元12內的一非揮發性記憶體(未顯示)內的資料庫，且係由該中央處理單元12讀取至隨機存取記憶體12a之中且予以執行。

如示於圖22，該程序內有三個階段，其中，裝置10內的安全服務模組系統542鑑認一主機系統540。於第一公開密鑰驗證階段中，該主機系統540傳送該安全服務模組命令內該主機憑證鏈給該安全服務模組系統542。該安全服務模組系統542使用位於該存取控制記錄550內之該主機根憑證548內的根憑證授權單位公開密鑰，而驗證(方塊552)該主機憑證544及該主機公開密鑰546之真實性。若牽涉到介於該根憑證授權單位與該主機之間的一中間憑證授權單位549，則於方塊552，該中間憑證授權單位549亦被用於驗證。假設該驗證或程序(方塊552)係成功的，則該安全服務模組系統542係接著進行至第二階段。

該安全服務模組系統542產生一隨機號碼554且傳送該隨機號碼554作為一挑戰而至該主機系統540。系統540使用該主機系統的私有密鑰547簽名該隨機號碼554(方塊556)，

且傳送該經簽名的隨機號碼作為對於該挑戰的回應。該回應係使用該主機公開密鑰546予以解密(方塊558)，且與該隨機號碼554相比較(方塊560)。假設該經解密回應匹配該隨機號碼554，則該挑戰回應係成功的。

於第三階段中，隨機號碼562係使用該主機公開密鑰546予以加密。接著，該隨機號碼562係會期密鑰。該主機系統540可藉由使用其之私有密鑰解密(方塊564)來自該安全服務模組系統542之該經加密的隨機號碼562，而獲得該會期密鑰。藉由此會期密鑰，接著可起始介於該主機系統540與該安全服務模組系統542之間的安全通訊。圖22係顯示一單向非對稱鑑認，其中，該主機系統540係由裝置10內之該安全服務模組系統542予以鑑認。圖23係一協定圖，其顯示一類似於圖22之單向鑑認協定之雙向相互鑑認程序，其中，圖23中之該安全服務模組系統542係亦由該主機系統540予以鑑認。

圖24繪示本發明之一項實施例之憑證鏈590的圖式。如上文所述，需要被提交用於驗證之憑證鏈可包含若干憑證。因此，圖24之憑證鏈包含總計9個憑證，該等憑證全部係可以需要被驗證以用於鑑認。如說明於上文之先前技術部分，於用於憑證驗證的現有系統中，在傳送一不完整的憑證鏈，或者若傳送整個憑證，而該等憑證係不以任何特定的順序予以傳送，使得接收者係將不能夠分析該等憑證，直到整個憑證群組係已經被接收及儲存為止。因為於一憑證鏈內憑證之數量係事先不知道，所以此可呈現一問

題。一大量的儲存空間係可能需要被保留，以用於儲存不確定長度的憑證鏈。此可以係一對於實施驗證之儲存裝置的問題。

本發明之一項實施例係根據：該問題可藉由主機裝置以與該憑證鏈將被該儲存裝置驗證之相同順序傳送其之憑證鏈之一系統所減輕之認知。因此，如示於圖24，憑證之憑證鏈590係：開始於憑證鏈590(1)，其係緊接在該主機根憑證下方的憑證；且結束於憑證590(9)，其係該主機憑證。因此，裝置10將首先驗證憑證590(1)內之公開密鑰，其後接著憑證590(2)內之公開密鑰的驗證，以此類推，直到憑證590(9)內的主機公開密鑰被驗證為止。接著，此係完成整個憑證鏈590之驗證程序。因此，假如該主機裝置係以與該憑證鏈將被驗證之相同順序或序列而傳送該憑證鏈590至記憶體裝置10，則記憶體裝置10可當每一憑證被接收時開始驗證每一憑證，而不需要等待直到該憑證鏈590內全部9個憑證已經被接收為止。

因此，於一項實施例中，該主機裝置係一次傳送該憑證鏈590內一憑證至記憶體裝置10。接著，記憶體裝置10將必須一次儲存一單一憑證。在該憑證係已經被驗證之後，其可被由該主機所傳送之下一憑證予以覆寫，惟該憑證鏈中最後一憑證除外。以此方式，在任何時間，記憶體裝置10將需要保留用於僅儲存一單一憑證的空間。

該記憶體裝置係將需要知道該整個憑證鏈590何時已經被接收。因此，較佳地，最後一憑證590(9)係含有其係該

憑證鏈內最後一憑證之一指示項或一項指示。此特徵係顯示於圖25，其顯示一控制區段的資訊的表，該控制區段係在由該主機傳送至該記憶體裝置10之憑證緩衝區之前。如示於圖25，憑證590(9)之控制區段含有一引數名稱"'為最後的'旗標"。接著，記憶體裝置10可藉由檢查是否該"為最後的"旗標係被設定，而驗證憑證590(9)係該憑證鏈內最後一憑證，以決定是否所接收之憑證係該憑證鏈中最後一個憑證。

於一替代實施例中，憑證鏈590內之憑證係可非以逐一方式予以傳送，而係以含一個、兩個或三個憑證之群組予以傳送。明顯地，可使用具有其他數量之憑證的群組或者群組中相同數量之憑證。因此，憑證鏈590包含5個連續的憑證串591、593、595、597及599。該等憑證串之每一者含有至少一憑證。一連續的憑證串係含有下列憑證的憑證串：緊接於該憑證鏈中位於該討論中憑證串之前的憑證串之憑證(開始憑證)；緊接在該憑證鏈內該討論中憑證串的後的憑證串的憑證(結尾憑證)；以及介於該開始憑證與結尾憑證之間之所有憑證。舉例而言，憑證串593含有三個憑證590(2)、590(3)及590(4)。該5個憑證串係由記憶體裝置10以下列序列驗證：591、593、595、597且以599結束。因此，假如該5個憑證串係以與記憶體裝置10所實施之驗證相同的序列予以傳送及接收，則該記憶體裝置在彼等憑證串已經被驗證之後，將不需要儲存任一憑證串，且惟最後一憑證串除外的所有可被來自該主機而到達的下一

憑證串所覆寫。如同先前的實施例，期望該憑證鏈內最後一憑證係含有一諸如一旗標的指示項，其係被設定為一特定的值，以指示其係該憑證鏈內最後一憑證。於此實施例中，該記憶體裝置將僅需要保留足以儲存該5個憑證串內最大數量的憑證的空間。因此，假如該主機首先係通知該記憶體裝置10其意欲傳送之最長憑證串，該記憶體裝置10係僅需保留用於最長憑證串列之足夠空間。

較佳地，由該主機所傳送之該憑證鏈內每一憑證的長度不超過由該憑證所檢定的公開密鑰之長度的4倍。類似地，較佳地，由該記憶體裝置10傳送至一主機裝置以檢定該記憶體裝置之公開密鑰之憑證的長度不超過由該憑證所檢定的公開密鑰之長度的4倍。

上述用於憑證鏈之驗證的實施例係顯示於圖26之流程圖之中，其中，對於簡化起見，於每一群組內的憑證數量係假設為1。如示於圖26，該主機係循序傳送該憑證鏈內之憑證至該卡。以該憑證鏈內之第一憑證(典型地，接在該根憑證之後的憑證，如上文所述)開始，該卡循序接收來自正被鑑認之該主機的憑證鏈(方塊602)。接著，該卡係驗證每一接收到的憑證，且假如任一憑證係驗證失敗，則中止該程序。假如該等憑證之任一驗證失敗，則該卡通知該主機(方塊604，606)。接著，該卡係偵測是否最後一憑證已經被接收及驗證(菱形608)。假如最後一憑證尚未被接收及驗證，則該卡返回方塊602，以繼續接收及驗證來自該主機的憑證。假如最後一憑證已經被接收及驗證，則該卡

在憑證驗證之後，進行至下一階段(610)。雖然圖26及以下後續圖內之特徵係引用記憶體卡作為範例，應瞭解的是，這些特徵係亦可應用於具有非記憶體卡之實體形式之記憶體裝置。

當該卡正在鑑認該主機時由該主機所實施之程序係顯示於圖27。如示於圖27，該主機傳送該憑證鏈內下一憑證至該卡(方塊620)，典型地係以一接在該根憑證之後的憑證開始。接著，該主機係決定是否已經接收到來自該卡之一指示鑑認失敗的中止通知(菱形622)。假如已經接收一中止通知，則該主機停止(方塊624)。假如尚未接收一中止通知，則該主機係藉由檢查是否已經於被傳送之最後一憑證中設定"為最後的旗標"，而檢查看看是否已經傳送該憑證鏈內最後一憑證(方塊626)。假如已經傳送最後一憑證，則在憑證驗證之後，該主機進行至下一階段(方塊628)。如示於圖22及23，下一階段可以係一挑戰回應，其後係接著會期密鑰建立。假如尚未傳送該憑證鏈內最後一憑證，則該主機返回方塊620，以傳送該憑證鏈內下一憑證。

當該卡正被鑑認時由該卡及該主機所採取的動作係顯示於圖28及29。如示於圖28，在開始之後，該卡係等待一來自該主機的請求，以傳送該憑證鏈內之一憑證(方塊630，菱形632)。假如未接收到來自該主機的一請求，則該卡將返回菱形632。假如接收到來自該主機的一請求，則該卡接著將傳送該憑證鏈內下一憑證，其係以應該被傳送之第一憑證開始(典型地，以接在該根憑證之後的憑證開始)(方

塊634)。該卡決定是否已接收到而來自該主機的一失敗通知(方塊636)。假如已接收到一失敗通知，則該卡停止(方塊637)。假如未接收到任何失敗通知，則該卡決定是否已傳送最後一憑證(菱形638)。假如尚未傳送最後一憑證，則該卡返回菱形632且等待直到其接收來自該主機的下一請求為止，以用於傳送該憑證鏈內之下一憑證。假如已傳送最後一憑證，則該卡係進行至下一階段(方塊639)。

圖29顯示當該卡係正在被鑑認時，該主機所採取之動作。該主機傳送對於該憑證鏈內之下一憑證之請求至該卡，其係以對於將被傳送之第一憑證的請求開始(方塊640)。接著，該主機驗證每一接收到的憑證，且假如驗證失敗，則中止該程序且通知該卡(方塊642)。假如驗證通過，則該主機檢查看看是否已接收且成功地驗證最後一憑證(菱形644)。假如尚未接收及成功地驗證最後一憑證，則該主機返回方塊640，以傳送一對於該憑證鏈內下一憑證之請求。假如已接收及成功地驗證最後一憑證，則在憑證驗證之後，該主機進行至下一階段(方塊646)。

憑證廢止

當發佈一憑證時，期望於其整個有效期間被使用。然而，各種情況可能導致一憑證在有效期間到期之前變成無效的。此類情況包含名稱改變，主題與憑證授權單位之間之關聯性改變(例如，一員工終止與一組織之雇用關係)，及危及或懷疑危及對應的私有密鑰。於此類情況下，該憑證授權單位係需要廢止該憑證。

安全儲存應用程式係以不同的方式啟用憑證廢止，每一存取控制記錄可被組態以用於一用於廢止憑證之特定方法。一存取控制記錄可被組態成不支援一廢止方案。於此情況下，每一憑證係被認為有效的，直到其之到期日期為止。或者可採用憑證廢止清單。作為又另一替代方式，該廢止方案可特定用於一特別的應用程式，或者應用程式特定的，其係將於下文說明。一存取控制記錄係藉由指定一廢止值，而指定三種廢止方案中被採用的廢止方案。假如一存取控制記錄被建立成不具有廢止方案，則對於其而言，採用一能夠被該存取控制記錄擁有者啟動的廢止方案係可能的。記憶體裝置憑證之廢止係由該主機予以強制實行，而非由該安全儲存應用程式安全性系統予以強制實行。一存取控制記錄擁有者負責管理一主機根憑證的廢止，藉由主機根憑證而實施之機制係藉由更新該等存取控制記錄的憑證而實施。

憑證廢止清單(CRL)

該安全儲存應用程式系統使用一廢止方案，其係牽涉到週期性發佈一稱為一憑證廢止清單之經簽名資料結構之每一憑證授權單位。一憑證廢止清單係一時間戳記清單，其識別由一憑證授權單位(發佈討論中的憑證之相同憑證授權單位)所簽名之經廢止憑證，且實施成可由公眾所自由使用。每一經廢止憑證係藉由其憑證序號而於一憑證廢止清單中予以識別。該憑證廢止清單的大小係任意的，且係取決於經廢止的未到期憑證之數量。當一裝置使用一憑證

(例如，用於驗證一主機的身份)時，該裝置不僅檢查該憑證簽名(及有效性)，而且亦比對透過一憑證廢止清單接收之序號清單而驗證該憑證。假如於發佈該憑證的憑證授權單位所發佈之憑證廢止清單上找到一諸如一憑證之序號的識別，則此係指示該等憑證係已經被廢止且不再有效。

該憑證廢止清單亦將需要被驗證為真實的，以使其作為確認憑證之目的。憑證廢止清單係使用發佈該憑證廢止清單的憑證授權單位的私有密鑰予以簽名，且可藉由使用該憑證授權單位的公開密鑰解密該經簽名的憑證廢止清單而被驗證為真實的。假如該經解密的憑證廢止清單匹配該未經簽名的憑證廢止清單之摘要，則此係意謂該憑證廢止清單係未曾被竄改且係真實的。憑證廢止清單係通常使用一雜湊演算法而被雜湊，以獲得其之摘要，且該等摘要係藉由該憑證授權單位的私有密鑰予以加密。為了驗證是否一憑證廢止清單係有效的，該經簽名的憑證廢止清單(亦即，經雜湊及經加密的憑證廢止清單)係使用該憑證授權單位的公開密鑰予以解密，以得出一經解密及經雜湊的憑證廢止清單(亦即，該憑證廢止清單的一摘要)。接著，其係與該經雜湊的憑證廢止清單比較。因此，該驗證程序可時常牽涉到雜湊該憑證廢止清單以用於與經解密及經雜湊的憑證廢止清單相比較的步驟。

該等憑證廢止清單方案的特性之一係，該憑證(對於該憑證廢止清單)之確認可與獲得該憑證廢止清單分開實施。憑證廢止清單係亦由適切的憑證之發行者予以簽名，

且係以上述之方式，使用發佈該等憑證廢止清單之憑證授權單位的公開密鑰，以一類似於憑證驗證之類似方式來驗證憑證廢止清單。該記憶體裝置驗證該簽名係屬於該憑證廢止清單且該憑證廢止清單之發行者匹配該憑證之發行者。該憑證廢止清單方案之另一特性係，可藉由完全相同於該等憑證本身的手段散佈憑證廢止清單，亦即，經由不受信任的伺服器及不受信任的通訊。憑證廢止清單及其之特性係詳細說明於X.509標準之中。

憑證廢止清單之安全儲存應用程式基礎架構

安全儲存應用程式使用該憑證廢止清單方案而提供一用於主機廢止之基礎結構。當以憑證廢止清單廢止方案鑑認一RSA為基礎的存取控制記錄時，該主機係將作為一額外的欄位之一憑證廢止清單(假如發行者憑證授權單位未廢止任何憑證，則可能為一空的憑證廢止清單)加入至一集合憑證命令之中。此欄位將含有一由該憑證的發行者所簽名之憑證廢止清單。當此欄位係存在時，該記憶體裝置10首先驗證該集合憑證命令內的憑證。獲得及存取該憑證廢止清單存放庫(repository)係完全為該主機之責任。憑證廢止清單係於其為有效期間的時期(憑證廢止清單到期時期(CET)而發佈。於驗證期間，假如目前的時間係被發現為不在此時期內，則該憑證廢止清單係被認為有缺陷的，且不能夠被用於憑證驗證。接著，結果係該憑證的鑑認失敗。

於傳統的憑證驗證方法中，該鑑認或驗證實體被期望持

有憑證廢止清單或能夠自憑證授權單位(CA)擷取憑證廢止清單，且比對該清單以檢查提交用於鑑認之憑證的序號，以決定是否所提交的憑證係已經被廢止。在鑑認或驗證實體係一記憶體裝置之情況下，該記憶體裝置係可能尚未被使用於自己自憑證授權單位擷取憑證廢止清單。假如一憑證廢止清單係預先儲存於該裝置內，則此類清單係可變成過期的，使得在該安裝日期之後所廢止的憑證將不出現於該清單上。此將使使用者能夠使用一經廢止憑證存取該儲存裝置。此係不期望的。

在一項實施例中，可藉由一種系統來解決上述問題，其中，想要被鑑認之實體提交一憑證廢止清單連同將被鑑認之憑證給該鑑認實體，該鑑認實體可以係一記憶體裝置10。該鑑認實體接著驗證接收到之憑證及憑證廢止清單的真實性。該鑑認實體藉由檢查是否該憑證之識別(諸如該憑證之序號)係出現於該憑證廢止清單上，而檢查是否該憑證係於該憑證廢止清單上。

鑑於上述內容，一非對稱鑑認方案可被用於介於一主機裝置與記憶體裝置10之間的相互鑑認。想要對於該記憶體裝置10而被鑑認之該主機裝置係將需要提供其憑證鏈及對應的憑證廢止清單。另一方面，主機裝置係已經被用於連接至憑證授權單位以獲得憑證廢止清單，使得當記憶體裝置10係將被主機裝置予以鑑認時，該記憶體裝置不需要將憑證廢止清單連同其憑證或憑證鏈提交給該等主機裝置。

近年來，係有擴大數量之不同類型可用於播放內容的可

攜式裝置，諸如不同內建的或獨立的音樂播放機、mp3播放機、行動電話、個人數位助理及筆記型電腦。雖然連接此類裝置至全球網路(WWW)以自憑證授權單位存取憑證驗證清單係可能的，然而典型地，許多使用者非每天連接至web，反而是僅獲得新的內容或更新訂購(諸如每幾週)才連接至web。因此，對於此類使用者而言，必須更頻繁地自憑證授權單位獲得憑證廢止清單可能係麻煩的。對於此類使用者而言，可於該儲存裝置本身之一較好為未受保護區域中儲存該憑證廢止清單及亦可選用之將需要被提交給一儲存裝置以存取受保護內容之主機憑證。於許多類型儲存裝置(例如快閃記憶體)之中，該等儲存裝置之未受保護區域係由主機裝置所管理，而非該等儲存裝置自己所管理。以此方式，對於該使用者(至該主機裝置)而言，不需要必須連接至該網路，以獲得更多最新的憑證廢止清單。該主機裝置係可以僅自該儲存裝置之不安全區域擷取此類資訊，且接著轉向及提交此類憑證及清單給該儲存器或記憶體裝置，以存取該儲存裝置內受保護內容。因為用於存取受保護內容的憑證及其對應的憑證廢止清單典型地係於某時期為有效的，所以只要其係仍然有效的，則該使用者將不需要獲得最新的憑證或憑證廢止清單。上述特徵使使用者能夠於相當長的期間當該憑證及憑證廢止清單皆為有效時，方便存取該憑證及憑證廢止清單，而不需要連接至該憑證授權單位，以用於經更新資訊。

上述程序係顯示於圖30及31之流程圖之中。如示於圖

30，該主機24自該記憶體裝置10之不安全公開區域讀取關於該主機將提交給該記憶體裝置以用於鑑認之一憑證的憑證廢止清單(方塊652)。因為該憑證廢止清單係儲存於該記憶體之一不安全區域，所以在該憑證廢止清單能夠被該主機獲得之前，係不需要鑑認。因為該憑證廢止清單係儲存於該記憶體裝置之公開區域，所以該憑證廢止清單的讀取係受到該主機裝置24控制。接著，該主機傳送憑證廢止清單連同將被驗證之憑證至該記憶體裝置(方塊654)，且進行至下一階段，除非其接收來自該記憶體裝置10之一失敗通知(方塊656)。參照圖31，該記憶體裝置係接收來自該主機的憑證廢止清單及憑證(方塊658)，且檢查是否該憑證之序號係於該憑證廢止清單上(方塊660)，以及其他方面(例如，是否該憑證廢止清單係已經過期)。假如於該憑證廢止清單上找到該憑證之序號或者因其他理由而失敗，則該記憶體裝置傳送一失敗通知給該主機(方塊662)。以此方式，不同的主機可獲得儲存於該記憶體裝置之公開區域內的憑證廢止清單，原因係相同的憑證廢止清單可被用於不同主機的鑑認。如上文所述，為了使用者方便，將使用該憑證廢止清單而被驗證之憑證較佳地係亦可以與該憑證廢止清單一起儲存於記憶體裝置10之一不安全區域內。然而，該憑證係可用於僅由該憑證被發佈之該主機對於記憶體裝置之鑑認。

在該憑證廢止清單係於其欄位內含有一用於下一更新時間之情況下，如示於圖32，於裝置10內的安全儲存應用程

式係亦對照此時間而檢查目前時間，以看看是否目前時間係於此時間之後；假如其係如此，則鑑認亦失敗。因此，較佳地，該安全儲存應用程式對照目前的時間(或者對照該憑證廢止清單被該記憶體裝置10接收到的時間)檢查下一更新的時間以及憑證廢止清單到期時期。

如上文所述，假如該憑證廢止清單含有長經廢止憑證識別清單，則處理(例如雜湊)及搜尋清單中是否有由該主機提交之憑證的序號可能花費一段長時間，特別是在該處理及搜尋係依序實施之情況下。因此，為了加速該程序，處理及搜尋係可以同時被實施。再者，假如整個憑證廢止清單在其被處理及搜尋之前需要被接收，則該程序係亦可以為費時的。申請人係體認到：可藉由隨著該憑證廢止清單之部分被接收時(迅速地)予以處理及搜尋而迅速執行該程序，使得當該憑證廢止清單之最後一部分被接收時，該程序係即將完成。

圖33及34係顯示上述廢止方案之特徵。於該鑑認實體(例如，一諸如一記憶體卡之記憶體裝置)處，自想要被鑑認之實體接收憑證及憑證廢止清單(方塊702)。未經加密的憑證廢止清單之部分被處理(例如雜湊)並且同時搜尋此等部分中是否有所提交之憑證的識別(例如，序號)。該等經處理的(例如經雜湊的)憑證廢止清單部分被編譯成為一經雜湊的完整憑證廢止清單，其係與該完整經解密及經雜湊的憑證廢止清單相比較，該完整經解密及經雜湊的憑證廢止清單係由編譯自想要被鑑認之實體接收之該等部分的經

解密憑證廢止清單部分而形成。假如該比較係指示該比較中無匹配，則鑑認係失敗。該鑑認實體亦對照目前的時間來檢查下一更新的時間以及憑證廢止清單到期時期(方塊706，708)。假如於該憑證廢止清單上找到所提交的憑證之識別，或者假如目前的時間係不在該憑證廢止清單到期時期之內，或者假如已超過下一更新憑證廢止清單之時間(方塊710)，則鑑認亦失敗。於一些實施方式中，儲存用於編譯之該等經雜湊憑證廢止清單部分及該等級解密雜湊憑證廢止清單部分可不需要大量的記憶體空間。

當一實體(例如，該主機)想要被鑑認，其將傳送其憑證及憑證廢止清單給該鑑認實體(方塊722)，且進行至下一階段(方塊724)。此係顯示於圖34。

假如該實體係提交一用於鑑認之憑證鏈，則可實施一類似於上述之程序。於此事件中，將需要對於該憑證鏈內每一憑證連同其對應的憑證廢止清單重複上述程序。每一憑證及其憑證廢止清單係可隨著其被接收時予以處理，而不需要等待接收該憑證鏈中之其餘憑證及其對應的憑證廢止清單。

身份物件(IDO)

身份物件係一受保護物件，其係設計成允許諸如一快閃記憶體卡之該記憶體裝置10儲存一RSA密鑰對或其他類型密碼編譯ID。該身份物件包含任何類型密碼編譯ID，其可被用於簽名及驗證身份、以及加密及解密資料。該身份物件亦包含一來自一憑證授權單位的憑證(或者來自多個憑

證授權單位的一憑證鏈)，以檢定該密鑰對內之公開密鑰為真實的。該身份物件可被用於提供一外部實體或一內部卡實體(亦即，該裝置本身、一內部應用程式等等，稱為該身份物件之擁有者)之身份證明。因此，該卡非正在透過一挑戰回應機制使用該RSA密鑰對或其他類型密碼編譯ID以鑑認該主機，而是透過簽名提供給其之資料流而作為身份證明。換句話說，該身份物件係含有其擁有者的密碼編譯ID。為了存取該身份物件內的密碼編譯ID，該主機將首先需要被鑑認。如上文所述，該鑑認程序係受控於一存取控制記錄。在該主機係已經被成功鑑認之後，該身份物件擁有者可使用該密碼編譯ID來建置該擁有者對於另一當事人之身份。舉例而言，該密碼編譯ID(例如，一公開-私有密鑰對之私有密鑰)可被用於簽名由其他當事人透過該主機提交之資料。該經簽名的資料及該身份物件內之憑證係代表該身份物件之擁有者提交給其他當事人。由一憑證授權單位(亦即，一受信任的授權單位)檢定該憑證內之該公開-私有密鑰對之公開密鑰為真實的，使得其他當事人可信任該公開密鑰為真實的。接著，其他當事人可使用該憑證內之該公開密鑰來解密該經簽名的資料，且比較該經解密的資料與由其他當事人所傳送之資料。假如該經解密的資料匹配於由其他當事人所傳送之資料，則此係顯示該身份物件之擁有者係真的具有存取該真實的私有密鑰之權利，且因而其代表之實體係真實的。

該身份物件之一第二用途係使用該密碼編譯ID(諸如該

RSA密鑰本身)來保護指定給該身份物件之擁有者之資料。該資料係期望使用該身份物件公開密鑰而被加密。諸如一記憶體卡之該記憶體裝置10將使用該私有密鑰來解密該資料。

該身份物件係一可對於任何類型存取控制記錄予以建立之物件。於一項實施例中，一存取控制記錄可具有僅一個身份物件。資料簽名及保護特徵兩者係該安全儲存應用程式系統提供給任何能夠鑑認該存取控制記錄的實體之服務。該身份物件之保護等級係與該存取控制記錄之登入鑑認方案一樣高。對於經繫結以具有一身份物件之一存取控制記錄，可選擇任何鑑認演算法。由建立者(主機)決定及評估哪一演算法可最佳地保護該身份物件使用方式。一具有一身份物件之存取控制記錄提供其憑證鏈，以回應於一獲得該身份物件公開密鑰之命令。

當正在使用該身份物件以進行資料保護時，自該卡輸出的經解密的資料係可能需要進一步的保護。於此情況下，該主機係被鼓勵使用一透過可用之鑑認演算法之任一者所建置之安全通道。

當建立該身份物件時，選擇密鑰長度以及PKCS#1版本。於一項實施例中，公開密鑰及私有密鑰正在使用如PKCS#1 2.1版本定義之(指數，模數)表示。

於一項實施例中，於一身份物件建立期間所包含之資料係具有所選長度的RSA密鑰對以及一憑證鏈，其係迂迴地證明該公開密鑰之真實性。

擁有該身份物件之存取控制記錄將允許使用者資料的簽名。此係透過兩個安全儲存應用程式命令而實施：

- 設定使用者資料：提供一將被簽名之自由格式之資料緩衝區。
- 獲得安全儲存應用程式簽名：該卡將提供一RSA簽名(使用該存取控制記錄私有密鑰)。取決於該物件之類型，可根據PKCS#1 1.5版本或2.1版本來設定該簽名的格式及大小。

使用一身份物件之操作係顯示於圖35至37，其中，該記憶體裝置10係一快閃記憶體卡，且該卡係該身份物件之擁有者。圖35係顯示一由該卡簽名傳送給一主機之資料所實施之程序。參照圖35，在一主機被鑑認之後(方塊802)，如由上述一樹狀結構之一節點處之一存取控制記錄所控制，該卡係等待用於一憑證之一主機請求(菱形804)。在接收該請求之後，該卡傳送該憑證，且返回菱形804，以用於下一主機請求(方塊806)。假如需要傳送一憑證鏈以檢定由該卡所擁有之該身份物件的公開密鑰，則重複上述動作，直到該憑證鏈內所有憑證已經被傳送至該主機。在每一憑證已經被傳送至該主機之後，該卡等待來自該主機之其他命令(菱形808)。假如於一預設時期期間內未接收到來自該主機的命令，則該卡返回菱形804。於接收來自該主機的資料及一命令時，該卡檢查以看看是否該命令係用於簽名資料(菱形810)。假如該命令係用於簽名資料，則該卡係以該身份物件內之該私有密鑰簽名該資料，且接著傳送該經簽

名的資料至該主機(方塊812)，且返回菱形804。假如來自該主機的命令係非用於簽名來自該主機的資料，則該卡使用該身份物件內之該私有密鑰，以解密該接收到的資料(方塊814)，且返回菱形804。

圖36顯示在該卡簽名之資料傳送給該主機時由該主機所實施之程序。參照圖36，該主機傳送鑑認資訊給該卡(方塊822)。在如上文之一樹狀結構之一節點處之一存取控制記錄所控制之成功鑑認之後，該主機傳送請求至該卡以用於憑證鏈，且接收該憑證鏈(方塊824)。在已經驗證該卡之該公開密鑰之後，該主機傳送資料給該卡以用於簽名，且接收藉由該卡之私有密鑰所簽名之資料(方塊826)。

圖37係顯示當該主機使用該卡之公開密鑰解密資料且傳送該經解密的資料至該卡時由該主機所實施之程序。參照圖37，該主機傳送鑑認資訊給該卡(方塊862)。在成功實施由一存取控制記錄控制之鑑認之後，該主機傳送請求給該卡，以要求憑證鏈(方塊864)，該憑證鏈係驗證該身份物件內該卡的公開密鑰所需的，且傳送請求至該卡，以要求資料。在已驗證該身份物件內之該卡的該公開密鑰之後，該主機使用該卡之經驗證公開密鑰來加密來自該卡的資料，且傳送其至該卡(方塊866，868)。

查詢

主機及應用程式係需要持有關於其正一起工作以執行系統操作之記憶體裝置或卡的某些資訊。舉例而言，主機及應用程式可需要知道儲存於該記憶體卡上的哪些應用程式

係可供調用(invocation)。該主機所需之資訊有時候不是公開的知識，其係意謂並非每一實體係具有擁有它的權利。為了鑑別經授權與未經授權之使用者，需要提供一主機可使用之兩種問方法。

一般資訊查詢

此查詢公佈系統公開資訊，而無限制。儲存於該等記憶體裝置內之機密資訊包含兩個部分：一共用部分及一非共用部分。該機密資訊的一部分包含可以對於個別實體為專屬的資訊，使得每一實體應被允許僅存取其自己的專屬資訊，而不能夠存取其他實體的專屬機密資訊。此種機密資訊類型係不被共用，且形成該機密資訊的未共用部分。

通常被想成公開的某些資訊於某些情況下係可能被認為機密的，諸如駐留於該卡內的應用程式之名稱及其生命週期狀態。此之另一範例可係根存取控制記錄名稱，其被認為公開的，然而對於某些安全儲存應用程式使用情況而言可以係機密的。對於這些情況而言，該系統應回應於一般資訊查詢而提供一選項，保持此資訊僅能由所有經鑑認的使用者使用，然而係不能被未經鑑認的使用者使用。此類資訊構成該機密資訊的共用部分。該機密資訊的共用部分的一範例可包含一根存取控制記錄清單，即目前出現於該裝置上的所有根存取控制記錄的清單。

透過該一般資訊查詢來存取公開資訊係不需要該主機/使用者登入一存取控制記錄。因此，具有安全儲存應用程式標準知識之任何實體可執行及接收該資訊。就安全儲存

應用程式而論，此查詢命令係在無一會期號碼之下被處置。然而，假如期望由一實體存取該機密資訊的共用部分，則需要首先透過控制存取該記憶體裝置內的資料之任何控制結構(例如，任一存取控制記錄)來鑑認該實體。在一成功鑑認之後，該實體將能夠透過一般資訊查詢而存取該機密資訊的該共用部分。如上文所說明，該鑑認程序將導致用於存取之一安全儲存應用程式會期號碼或者ID。

謹慎資訊查詢

關於個別存取控制記錄及其系統存取及資產的私有資訊係被認為謹慎的，且需要明確鑑認。因此，此種查詢要求在接收用於資訊查詢的授權之前，進行存取控制記錄登入及鑑認(假如鑑認係由該存取控制記錄所指定)。此項查詢係需要一安全儲存應用程式會期號碼。

在詳細敘述兩種類型查詢之前，首先敘述索引群組作為一用於實施該等查詢之實務解決方案之觀念係將為有用的。

索引群組

執行於可能的安全儲存應用程式主機上之應用程式係被該主機上的作業系統及系統驅動程式要求指定意欲被讀取之區段數。接著，此係意謂該主機應用程式需要知道對於每一安全儲存應用程式讀取操作而言，需要讀取多少個區段。

因為查詢操作的本質旨在供應對於一請求資訊的實體而言通常係不知道的資訊，所以對於該主機應用程式而言，

發佈該查詢且猜測該操作所需之區段數係有困難的。

為了解決此問題，該安全儲存應用程式查詢輸出緩衝區僅包含每一查詢請求一區段(512位元組)。為輸出資訊的一部分之物件係組織於稱為索引群組之中。每一類型物件可具有一不同的位元組大小，其係考慮到可以適配於一單一區段之物件數。此定義該物件之索引群組。假如一物件具有一20個位元組的大小，則用於該物件之索引群組將含有至多25個物件。假如總共有56個此類物件，則其將已經被組織成3個索引群組，其中，物件"0"(第一物件)起始第一索引群組，物件"25"起始第二索引群組且物件"50"起始第三且為最後索引群組。

系統查詢(一般資訊查詢)

此查詢提供關於該裝置內之該支援安全儲存應用程式系統及被設定之目前的系統之一般公開資訊，像是執行於該裝置上之不同的樹及應用程式。類似於下文所述之存取控制記錄查詢(謹慎查詢)，該系統查詢經結構化以給予數個查詢選項：

- 一般的-安全儲存應用程式支援版本。
- 安全儲存應用程式-目前出現於該裝置上之所有安全儲存應用程式之應用程式清單，包含其之執行狀態。

上述列出的資訊係公開資訊。如同該存取控制記錄查詢，為了使主機不需要知道對於該查詢輸出緩衝區待讀取多少個區段，將有一自該裝置傳回的區段，同時仍然使該主機能夠進一步查詢額外的索引群組。因此，假如根存取

控制記錄物件之數量超過用於索引群組"0"之輸出緩衝區大小的數量，則該主機可以接下來的索引群組"1"傳送另一查詢請求。

存取控制記錄查詢(謹慎資訊查詢)

該安全儲存應用程式存取控制記錄查詢命令意欲供應該存取控制記錄使用者關於該存取控制記錄之系統資源的資訊，像是密鑰及應用程式ID，分割區及子代存取控制記錄。該查詢資訊係僅關於登入存取控制記錄且非關於該系統樹上之其他存取控制記錄。換句話說，存取係限於僅僅在牽涉到的存取控制記錄之權限下可存取的機密資訊的部分。

使用者可查詢下列三個不同的存取控制記錄物件：

- 分割區-名稱及存取權(擁有者，讀取，寫入)。
- 密鑰ID及應用程式ID-名稱及存取權(擁有者，讀取，寫入)。
- 子代存取控制記錄--一直接子代存取控制記錄的存取控制記錄及存取控制記錄群組名稱。
- 身份物件及安全資料物件(下文敘述)-名稱及存取權(擁有者，讀取，寫入)。

因為與一存取控制記錄連接之物件數量係可以改變，且該資訊係可能超過512個位元組(一區段)。在未事先知道物件數量之下，該使用者無法知道需要自該裝置內之該安全儲存應用程式系統讀取多少個區段，以獲得全部的清單。因此，由該安全儲存應用程式系統所提供之每一物件清單

係被分割成為若干索引群組，其係類似於上述系統查詢之情況。一索引群組係適配於一區段的物件數量，亦即可自該裝置內之安全儲存應用程式系統於一區段內傳送多少個物件至該主機。此使該裝置內之該安全儲存應用程式系統傳送一被請求的索引群組之一區段。該主機/使用者將接收該等被查詢物件之一緩衝區，該緩衝區內之物件數量。假如該緩衝區係滿的，則該使用者可查詢下一物件索引群組。

圖38顯示一牽涉到一般資訊查詢之操作的流程圖。參照圖38，當該安全儲存應用程式系統接收來自一實體的一般資訊查詢(方塊902)時，該系統決定是否該實體已經被鑑認(菱形904)。假如該實體已經被鑑認，則該系統向該實體供應公開資訊及該機密資訊之共用部分(方塊906)。假如其該實體尚未被鑑認，則該系統向該實體供應僅公開資訊(方塊908)。

圖39顯示一牽涉到一謹慎資訊查詢之操作的流程圖。參照圖39，當該安全儲存應用程式系統係接收來自一實體的一謹慎資訊查詢(方塊922)時，該系統決定是否該實體已經被鑑認(菱形924)。假如該實體已經被鑑認，則該系統向該實體供應機密資訊(方塊926)。假如該實體尚未被鑑認，則該系統係拒絕該實體存取機密資訊(方塊928)。

特徵組延伸(FSE)

於許多情況下，於該卡上執行該安全儲存應用程式內的資料處理活動(例如，DRM使用權物件確認)係非常有利

的。相對於所有資料處理工作係於該主機上執行之替代解決方案，該所得系統係將為更安全的，更有效率的，且較不依賴於主機。

該安全儲存應用程式安全性系統包含一組鑑認演算法及授權原則，其係設計成控制存取及使用由該記憶體卡所儲存、管理及保護的物件之集合。一旦一主機獲得存取權，該主機將接著處理儲存於該記憶體裝置內之資料，其中，存取該記憶體裝置係受控於該安全儲存應用程式。然而，假設該資料本質係非常應用程式特定的，且因此，該資料格式及資料處理係皆非定義於該安全儲存應用程式之中，該安全儲存應用程式不處理儲存於該等裝置上的資料。

本發明之一項實施例係根據下列認知：該安全儲存應用程式系統可被增強，以允許主機執行通常由該記憶體卡內之主機所實施之一些功能。因此，該等主機之一些軟體應用程式可被分割成為兩個部分：仍然由該主機實施之一部分；以及現在由該卡實施之另一部分。對於許多應用程式，此增強資料處理的安全性及效率。為了此目的，可加入一稱為特徵組延伸之機制，以增強該安全儲存應用程式之能力。在本文中，由該卡以此方式所執行之特徵組延伸內的主機應用程式亦稱為內部應用程式，或裝置內部應用程式。

該增強的安全儲存應用程式系統提供一種延伸基本安全儲存應用程式命令組的機制，其係透過導入卡應用程式而提供該卡之鑑認及存取控制。一卡應用程式被假設為亦實

施除了該安全儲存應用程式之服務以外的服務(例如，DRM機制，電子商務交易)。該安全儲存應用程式特徵組延伸係一種設計成增強具有資料處理軟體/硬體模組之標準安全儲存應用程式安全性系統的機制，其可以係專屬的。除了能夠使用上述查詢獲得的資訊之外，由該安全儲存應用程式特徵組延伸系統所定義之服務使主機裝置能夠查詢該卡，以用於可用之應用程式，選擇及與一特定應用程式通訊。上述之一般查詢及謹慎查詢係可以使用於此目的。

使用兩種延伸卡之安全儲存應用程式特徵組延伸內特徵組之方法：

- 提供服務-實現此特徵之方式為，透過允許經授權實體使用一稱為通訊管道(pipe)之命令通道直接與該內部應用程式通訊，該通訊管道可以係專屬的。
- 安全儲存應用程式標準存取控制原則的延伸--實現此特徵之方式為透過使內部的受保護資料物件(例如，內容加密密鑰、下文敘述之安全資料物件(SDO))相關聯於內部卡應用程式。每當此類物件被存取時，假如滿足所定義之標準的安全儲存應用程式原則，則調用相關聯的應用程式，藉此除了利用該等標準的安全儲存應用程式原則之外，還利用至少一條件。較佳地，該條件將不與該等標準的安全儲存應用程式原則衝突。只有亦滿足在此額外的條件之情況下，才授予存取。在進一步詳細說明該特徵組延伸之能力之前，現在將說明特徵組延伸以及該通訊管道及與全資

料物件之架構態樣。

**安全服務模組(SSM)及相關模組**

圖40A係一記憶體裝置10(諸如一快閃記憶體卡)連接至一主機裝置24的系統架構1000之功能方塊圖，以闡釋本發明之一項實施例。該卡20之該記憶體裝置內的軟體模組之主要組件如下：

安全儲存應用程式傳輸層1002

該安全儲存應用程式傳輸層係卡協定相依的。其處置該卡10之該協定層上之主機端安全儲存應用程式請求(命令)，且接著將其中繼至安全服務模組API。所有主機-卡同步化及安全儲存應用程式命令識別係於此模組內實施。該傳輸層亦係負責主機24與卡10之間所有資料傳送。

安全服務模組核心(SSM Core) 1004

此模組係該安全儲存應用程式實施方案之一重要的部分。該安全服務模組核心實施該安全儲存應用程式架構。更明確言之，該安全服務模組核心實施該安全儲存應用程式樹及存取控制記錄系統以及組成該系統之所有上述對應規則。該安全服務模組核心模組使用一密碼編譯庫1012，以支援該安全儲存應用程式安全性及密碼編譯特徵，諸如加密、解密及雜湊。

安全服務模組核心API 1006

此係主機及內部應用程式將介接於該安全服務模組核心以實行安全儲存應用程式操作之層。如示於圖40A，主機24及裝置內部應用程式1010將使用相同的API。

安全性應用程式管理員模組(SAMM)1008

安全性應用程式管理員模組非屬該安全儲存應用程式系統之部分，然而其係控制介接於該安全儲存應用程式系統之裝置內部應用程式之卡內的一重要的模組。

該安全性應用程式管理員模組管理所有裝置內部執行中之應用程式，其包含：

1. 應用程式生命週期監視及控制。

2. 應用程式初始化。

3. 應用程式/主機/安全服務模組介面。

裝置內部應用程式1010

裝置內部應用程式係經准許於該卡端上執行之應用程式。彼等裝置內部應用程式係被安全性應用程式管理員模組所管理，且係可存取該安全儲存應用程式系統。該安全服務模組核心亦提供該等主機端應用程式與該等內部應用程式之間之一通訊管道。用於此類內部執行應用程式之範例係DRM應用程式及單次密碼(one time password；OTP)應用程式，如下文作進一步說明。

裝置管理系統(DMS)1011

此模組含有在一後裝運(通常稱為後發佈)模式中更新該卡之系統及應用程式韌體以及增加/移除服務所需之處理程序及協定。

圖40B係該安全服務模組核心1004之內部軟體模組之功能方塊圖。如示於圖40B，核心1004包含一安全儲存應用程式命令處理常式(command handler)1022。處理常式1022

係於命令被傳送至該安全儲存應用程式管理員1024之前，剖析起源於該主機或起源於該裝置內部應用程式1010的該等安全儲存應用程式命令。所有安全儲存應用程式安全性資料結構(諸如存取控制記錄群組及存取控制記錄)以及所有安全儲存應用程式規則及原則係儲存於該安全儲存應用程式資料庫1026之中。安全儲存應用程式管理員1024實行由該等存取控制記錄及存取控制記錄群組以及儲存於資料庫1026內之其他控制結構所行使之控制。其他物件(諸如身份物件)以及安全資料物件亦係儲存於該安全儲存應用程式資料庫1026之中。安全儲存應用程式管理員1024實行由該等存取控制記錄及存取控制記錄群組以及儲存於資料庫1026內之其他控制結構所行使之控制。由該安全儲存應用程式非安全操作模組1028處置不牽涉到安全儲存應用程式之非安全操作。由該安全儲存應用程式安全操作模組1030處置在該安全儲存應用程式架構下的安全操作。模組1032係一連接模組1030至該密碼編譯庫1012之介面。模組1034係一連接模組1026及1028至圖1中該快閃記憶體20之層。

通訊(或傳遞(Pass-Through))管道

當由該安全服務模組核心及安全性應用程式管理員模組控制時，該等傳遞管道物件使經授權主機端之實體能夠與該等內部應用程式通訊。介於該主機與該內部應用程式之間之資料傳送係透過SEND及RECEIVE命令(定義如下)而實行。實際的命令係應用程式特定的。建立該管道之該實

體(存取控制記錄)將需要提供該管道名稱及將開啟一通道至其之應用程式的ID。如同具有所有其他受保護物件，該存取控制記錄係變成其擁有者，且被允許根據標準的委派規則及限制而委派使用權利以及擁有權給其他存取控制記錄。

假如在被鑑認實體之存取控制記錄屬性管理中設定CREATE_PIPE權限，則一該被鑑認實體將被允許建立管道物件。只有於該實體之權限控制記錄中設定在寫入或讀取管道權限之情況下，才允許與內部應用程式之通訊。只有在該實體係該管道擁有者或於該實體之權限控制記錄中設定委派存取權之情況下，才允許擁有權及存取權委派。如同所有其他權限，當委派擁有權給另一存取控制記錄時，較佳地，剝除該原始擁有者對於該裝置應用程式之所有權限。

較佳地，對於一特定應用程式，建立僅一通訊管道。較佳地，建立一第二管道及連接該第二管道至一已經連接之應用程式之嘗試將被該安全服務模組系統1000所拒絕。因此，較佳地，介於該等裝置內部應用程式1010之一者與一通訊管道之間係有1對1之關係。然而，多個存取控制記錄可與一裝置內部應用程式通訊(透過委派機制)。一單一存取控制記錄可與數個裝置應用程式通訊(透過連接至不同應用程式之多個管道之委派或擁有權)。較佳地，控制不同的管道之存取控制記錄係位於完全分離的樹之節點上，使得該等通訊管道之間係無串擾。

介於該主機與一特定應用程式之間傳送資料係使用下列命令而實行：

- WRITE PASS THROUGH(寫入傳遞)-將自該主機傳送一未格式化的資料緩衝區至該裝置內部應用程式。
- READ PASS THROUGH(讀取傳遞)-將自該主機傳送一未格式化的資料緩衝區至該裝置內部應用程式，且一旦該內部處理係完成，將輸出一未格式化的資料緩衝區回到該主機。

寫入傳遞命令及讀取傳遞命令提供主機想要通訊之裝置內部應用程式1010之ID作為參數。該實體權限將被確認，且假如該請求實體(亦即，主控該實體正在使用之會期之存取控制記錄)具有使用連接至該被請求應用程式之管道的權限，則該資料緩衝區將被中斷，且命令被執行。

此通訊方法係允許該主機應用程式透過該安全儲存應用程式存取控制記錄會期通道傳送廠商/專屬的特定命令至一裝置內部應用程式。

安全資料物件(SDO)

一能夠結合特徵組延伸而被使用之有用的物件係安全資料物件。

該安全資料物件係作為一用於安全儲存敏感資訊的一般用途容器。類似於內容加密密鑰物件，其係由一存取控制記錄擁有，且可於存取控制記錄之間委派存取權及擁有權。安全資料物件含有根據預先定義的原則限制而被保護及使用之資料，且可選擇地，具有至一裝置內部應用程式

1010之連結。較佳地，該敏感資料非係由該安全儲存應用程式系統予以使用或解譯，而是由該物件之擁有者及使用者所使用或解譯。換句話說，該安全儲存應用程式系統不辨明其所處置之資料內的資訊。以此方式，當於主機與該等資料物件之間傳送資料時，該物件內之該資料的擁有者及使用者可較不關心歸因於介接於該安全儲存應用程式系統所造成的敏感資訊之損失。因此，安全資料物件係由該主機系統(或內部應用程式)所建立，且被指派一串ID，類似於建立內容加密密鑰之方式。於建立時，該主機係除了提供名稱之外，亦提供經連結至該安全資料物件之應用程式之一應用程式ID及將被該安全儲存應用程式儲存、完整性驗證及接收之一資料區塊。

類似於內容加密密鑰，安全資料物件較佳地係僅於一安全儲存應用程式會期內予以建立。用於開啟該會期之存取控制記錄變成該安全資料物件之擁有者，且係具有刪除該安全資料物件之權利、寫入及讀取敏感資料以及委派擁有權及存取該安全資料物件之權限給另一存取控制記錄(為其之子代或於相同的存取控制記錄群組之內)。

該等寫入及讀取操作係專門為該安全資料物件之擁有者所保留。一寫入操作用，提供的資料緩衝區來覆寫現有安全資料物件之物件資料。一讀取操作將擷取該安全資料物件之完整的資料記錄。

允許具有適當存取權限的非擁有者存取控制記錄進行安全資料物件存取操作係。定義下列操作：

- SDO Set(安全資料物件設定)，應用程式ID被定義：將由具有該應用程式ID之該內部安全儲存應用程式處理該資料。藉由相關聯於該安全資料物件而調用該應用程式。作為一選用結果，該應用程式將寫入該安全資料物件。
- SDO Set(安全資料物件設定)，應用程式ID係空值(null)：此選項無效，且將提示一不合法命令錯誤。該Set命令需要一執行於該卡內的內部應用程式。
- SDO Get(安全資料物件獲得)，應用程式ID被定義：將由具有該應用程式ID之該裝置內部應用程式處理該請求。藉由相關聯於該安全資料物件而調用該應用程式。輸出(雖然未被定義)將被傳回該請求者。該應用程式將可選擇地讀取該安全資料物件。
- SDO Get(安全資料物件獲得)，應用程式ID係空值：此選項無效，且將提示一不合法命令錯誤。該Get命令需要一執行於該卡內的內部應用程式。
- 安全資料物件相關權限：一存取控制記錄可以係一安全資料物件擁有者或只是具有存取權限(Set，Get，或者兩者)。此外，一存取控制記錄可被允許傳遞對於非其擁有的安全資料物件的存取權至另一存取控制記錄。假如一存取控制記錄具有存取控制記錄屬性管理權限，則該存取控制記錄係可以明確地被准許建立安全資料物件且委派存取權。

**會期密鑰**

內部存取控制記錄類似於具有一權限控制記錄的任何存

取控制記錄，惟該裝置10之外部的實體無法登入該存取控制記錄除外。而是，當在圖40B之該安全儲存應用程式管理員1024之控制下的物件或相關聯於其之應用程式被調用時，圖40B之該安全儲存應用程式管理員1024自動登入該內部存取控制記錄。因為嘗試獲得存取之實體係一該卡或記憶體裝置內部的實體，所以係不需要鑑認。該安全儲存應用程式管理員1024將僅傳送一會期密鑰至該內部存取控制記錄，以啟用內部通訊。

將使用兩個範例顯示特徵組延伸之能力：單次密碼產生及數位權管理。在敘述單次密碼產生之範例之前，首先將說明雙因素鑑認之發佈。

**單次密碼之實施例**

雙因素鑑認(DFA)

雙因素鑑認係一項鑑認協定，其設計成藉由加入一額外的秘密"一第二因素"至標準使用者認證(亦即，使用者名稱及密碼)，而增強個人登入至(例如)一web服務伺服器之安全性。該第二秘密典型地係該使用者於其持有物中所具有的實體安全符記內儲存的某事物。於登入程序期間，該使用者需要提供持有證明作為該登入認證之一部分。一證明持有之常用方式係使用一單次密碼，其係一僅適合於一單一登入之密碼，其係由該安全符記所產生及輸出。假如該使用者能夠提供正確的單次密碼，則其係被認為充分證明持有該符記的擁有，因為無該符記之下以密碼編譯方式計算該單次密碼係不可實行的。因為該單次密碼係僅適合於

單次登入，所以該使用者係應該於登入時具有該符記，因為使用一自一先前登入所捕捉到的舊密碼將不再有效。

敘述於下面段落的產品係使用該安全儲存應用程式安全性資料結構，加上一特徵組延伸設計，以計算於該單次密碼系列中下一密碼，以實行一具有多個"虛擬"安全符記之快閃記憶體卡，每一符記產生一不同系列的密碼(其可被使用於登入不同的web網站)。此系統之一方塊圖係顯示於圖41。

完整的系統1050包含一鑑認伺服器1052、一網際網路伺服器1054及一具有符記1058之使用者1056。第一步驟係同意該鑑認伺服器與該使用者之間的一共用秘密(亦稱為種子供應)。該使用者1056將請求一將被發佈之秘密或種子，且將儲存其於該安全符記1058之中。下一步驟係繫結發佈之秘密或種子與一特定web服務伺服器。一旦此係完成，該鑑認可發生。該使用者將指示該符記產生一單次密碼。具有該使用者名稱及密碼之單次密碼係被傳送至網際網路伺服器1054。該網際網路伺服器1054轉遞該單次密碼至該鑑認伺服器1052，要求其驗證該使用者之ID。該鑑認伺服器亦將產生一單次密碼，且因為該單次密碼係自一共用秘密連同該符記予以產生，所以其係應該匹配自該符記產生的單次密碼。假如一項匹配係被找到，則該使用者之ID係被驗證，且該鑑認伺服器將傳回一肯定確認給該網際網路伺服器1054，該網際網路伺服器1054將完成該使用者登入程序。

用於該單次密碼產生之特徵組延伸實施方案具有下列特性：

- 於該卡內安全地儲存(經加密)該單次密碼種子。
- 該密碼產生演算法係於該卡內執行。
- 該裝置10可模擬多個虛擬符記，每一虛擬符記係存一不同的種子，且可以使用不同的密碼產生演算法。
- 該裝置10係提供一安全協定，以自該鑑認伺服器傳送該種子至該裝置。

用於單次密碼種子供應及單次密碼產生之安全儲存應用程式特徵係顯示於圖42，其中，實線箭頭係顯示擁有權或存取權，且虛線箭頭係顯示關聯性或連結。如示於圖42，於安全儲存應用程式特徵組延伸系統1100中，可透過一或多個通訊管道1104來存取軟體程式碼特徵組延伸1102，通訊管道1104係受控於N個應用程式存取控制記錄1106之各者。於下述實施例中，僅顯示一特徵組延伸軟體應用程式，且對於每一特徵組延伸應用程式，僅有一通訊管道。然而應瞭解的是，可以利用一個以上特徵組延伸應用程式。雖然圖42係僅顯示一通訊管道，應瞭解的是，可以使用複數個通訊管道。所有此類變化係可行的。參照圖40A、40B及42，該特徵組延伸1102可以係一用於單次密碼供應之應用程式，且形成圖40A之裝置內部應用程式1010之子集合。控制結構(存取控制記錄1101、1103、1106、1110)係安全儲存應用程式內之安全性資料結構的一部分，且係儲存於該安全儲存應用程式資料庫1026之

中。諸如身份物件1120、身份物件1122及通訊管道1104之資料結構亦係儲存於該安全儲存應用程式資料庫1026之中。

參照圖40A及40B，牽涉到該等存取控制記錄及資料結構之安全性相關操作(例如會期內之資料傳送，以及諸如加密、解密與雜湊之操作)係在介面1032及密碼編譯庫1012之輔助之下，由模組1030所處置。安全服務模組核心API 1006不區別牽涉到與主機互動之存取控制記錄(外部的存取控制記錄)的操作及不與主機互動之內部的存取控制記錄之操作，且因而係不區別牽涉到主機之操作相對於裝置內部應用程式1010之操作。以此方式，控制由主機端實體所實行之存取以及由裝置內部應用程式1010所實行之存取係使用相同的控制機制。此導致用於劃分主機端應用程式與裝置內部應用程式1010之間之資料處理的彈性。該等內部應用程式1010(例如圖42中之特徵組延伸1102)相關聯於該等內部存取控制記錄(例如圖42中之存取控制記錄1103)，且係透過該等內部存取控制記錄之控制予以調用。

再者，諸如具有相關聯的安全儲存應用程式規則及原則之存取控制記錄及存取控制記錄群組之安全性資料結構較佳地係控制對重要資訊的存取，諸如安全資料物件內之內容或能夠自安全資料物件內之內容推導出之資訊，使得外部或內部應用程式係僅能夠根據該等安全儲存應用程式規則及原則而存取該內容或資訊。舉例而言，假如兩個不同

的使用者可調用該等裝置內部應用程式1010之一個別裝置內部應用程式來處理資料，則使用位於分離的樹狀階層架構內之內部存取控制記錄來控制該兩個使用者所實施之存取，使得其之間係無串擾。以此方式，該兩個使用者皆能夠存取一共同組裝置內部應用程式1010以用於處理資料，而不擔心該等安全資料物件內之內容或資訊的擁有者喪失對於該內容或資訊的控制。舉例而言，對儲存由該等裝置內部應用程式1010所存取之安全資料物件資料之存取可受控於位於分開的樹狀階層架構內之存取控制記錄，使得其之間係無串擾。此種控制方式係類似於上述安全儲存應用程式控制存取資料之方式。此係對於內容擁有者及使用者提供儲存於該等資料物件內的資料的安全性。

參照圖42，對於該單次密碼相關主機應用程式所需之軟體應用程式碼之一部分被儲存(例如，在記憶體卡發佈之前預先儲存或在記憶體卡發佈之後載入)於該記憶體裝置10內作為特徵組延伸1102內之應用程式係可能的。為了執行此類程式碼，該主機將首先需要透過該N個驗證存取控制記錄1106中之一者進行鑑認(N係一正整數)，以獲得對於管道1104之存取。該主機亦將需要提供一用於識別其想要調用之單次密碼相關之應用程式的應用程式ID。在一成功鑑認之後，可存取此類程式碼，以用於透過相關聯於該單次密碼相關之應用程式的管道1104而執行。如上文所注意到，較佳地，介於一管道1104與一特定應用程式(諸如一單次密碼相關內部應用程式)之間係有1對1的關係。如

示於圖42，多個存取控制記錄1106可共有對一共同管道1104之控制。一存取控制記錄亦可控制一個以上管道。

圖42顯示統稱為物件1114之安全資料物件1、安全資料物件2及安全資料物件3，每一者係含有資料，諸如用於單次密碼產生之一種子，該種子係有價值的且較佳為被加密。介於該三個資料物件與特徵組延伸1102之間之連結或關聯性1108顯示該等物件之屬性在於：當存取該等物件中之任一者時，於具有該安全資料物件之屬性內一應用程式ID之特徵組延伸1102內之應用程式將被調用，且該應用程式將由該記憶體裝置之中央處理單元12所執行，而不需要接收任何進一步的主機命令(圖1)。

參照圖42，在一使用者可開始該單次密碼程序之前，該等安全性資料結構(存取控制記錄1101、1103、1106及1110)已被建立成具有用於控制該單次密碼程序之權限控制記錄。該使用者將需要具有存取權，以透過鑑認伺服器存取控制記錄1106之一而調用一單次密碼裝置內部應用程式1102。該使用者亦將需要具有對於將透N個使用者存取控制記錄1110之一而產生之單次密碼的存取權。可以於該單次密碼種子供應程序期間被建立該等安全資料物件1114。較佳地，該內部存取控制記錄1103已建立及控制該身份物件1116。該內部存取控制記錄1103係在其被建立之後，亦控制該等安全資料物件1114。當存取該等安全資料物件1114時，於圖40B內之該安全儲存應用程式管理員1024自動登入該內部存取控制記錄1103。該內部存取控制

記錄1103係相關聯於特徵組延伸1102。於該單次密碼種子供應程序期間，該等安全資料物件1114可變成相關聯於該特徵組延伸，如虛線1108所示。在該關聯性就緒之後，當該主機存取該等安全資料物件時，該關聯性1108係將導致特徵組延伸1102被調用，而不需要來自該主機的一進一步請求。當透過N個存取控制記錄1106之一存取通訊管道1104時，圖40B內之該安全儲存應用程式管理員1024亦自動登入該存取控制記錄1103。於此兩者情況下(存取安全資料物件1114及管道1104)，該安全儲存應用程式管理員將傳送一會期號碼至該特徵組延伸1102，該會期號碼將識別至該內部存取控制記錄1103之通道。

該單次密碼操作係牽涉到兩個階段：一示於圖43之種子供應階段；及一示於圖44之單次密碼產生階段。參照圖40至42將亦能夠有助於說明。圖43繪示該種子供應程序之協定圖。如示於圖43，由主機(諸如主機24)以及由該卡採取各種動作。採取各種動作之卡上的一實體係圖40A及40B之該安全服務模組系統，其包含該安全服務模組核心1004。採取各種動作之卡上的另一實體係顯示於圖42之該特徵組延伸1102。

於雙因素鑑認之中，該使用者係請求一種子被發佈，且一旦該種子被發佈，該種子係被儲存於一安全符記之中。於此範例中，該安全符記係該記憶體裝置或卡。該使用者向圖42中該等鑑認存取控制記錄1106之一者進行鑑認，以獲得存取該安全服務模組系統(箭頭1122)。假設鑑認成功

(箭頭1124)，則該使用者請求一種子(箭頭1126)。該主機傳送該請求，以藉由選擇一用於簽名該種子請求之特別的應用程式1102而將該種子請求簽名至該卡。假如該使用者不知道需要被調用之該特別的應用程式之ID，則可自裝置10獲得該資訊，舉例而言，透過一對於該裝置之謹慎查詢。接著，該使用者輸入應被調用之應用程式之應用程式ID，藉此亦選擇一對應於該應用程式之通訊管道。接著，透過該對應的通訊管道，在一傳遞命令中轉遞該使用者命令至來自該使用者之該應用程式ID所指定之應用程式(箭頭1128)。被調用之應用程式係藉由該指定之身份物件(諸如圖42內之身份物件1112)內的公開密鑰而請求一簽名。

該安全服務模組系統使用該身份物件之該公開密鑰簽名該種子請求，且通知該應用程式該簽名係完成(箭頭1132)。接著，該被調用之應用程式請求該身份物件之憑證鏈(箭頭1134)。為了回應，該安全服務模組系統提供由該存取控制記錄1103所控制之該身份物件之憑證鏈(箭頭1136)。接著，該被調用之應用程式透過該通訊管道，提供該經簽名的種子請求及該身份物件之該憑證鏈至該安全服務模組系統，該安全服務模組系統轉遞該經簽名的種子請求及該身份物件之該憑證鏈至該主機(箭頭1138)。透過該通訊管道傳送該經簽名的種子請求及該身份物件之該憑證鏈的係透過建置於圖40A之該安全性應用程式管理員模組1008及該安全服務模組核心1004之間的回呼(callback)功能，其中，將於下文說明該回呼功能。

接著，由該主機接收到的該經簽名的種子請求及該身份物件之該憑證鏈被傳送至如示於圖41之該鑑認伺服器1052。由該卡所提供之憑證鏈檢定該經簽名的種子請求係起源於受信任的符記，使得該鑑認伺服器1052係想要提供該秘密種子給該卡。因此，該鑑認伺服器1052傳送以該身份物件之該公開密鑰加密之種子連同該使用者存取控制記錄資訊一起給該主機。該使用者資訊指示出在該N個使用者存取控制記錄中使該使用者具有存取將被產生之該單次密碼的權利的存取控制記錄。該主機藉由提供該應用程式ID而調用特徵組延伸1102內一單次密碼應用程式，藉此亦選擇對應於該應用程式之通訊管道，且轉遞該使用者存取控制記錄資訊至該安全服務模組系統(箭頭1140)。接著，該經加密的種子及該使用者存取控制記錄資訊係透過該通訊管道被轉遞至該選擇出之應用程式(箭頭1142)。該被調用之應用程式傳送一請求至該安全服務模組系統，以用於使用該身份物件之私有密鑰，而解密該種子(箭頭1144)。該安全服務模組系統解密該種子且傳送一解密已經完成之通知給該應用程式(箭頭1146)。接著，該被調用之應用程式請求建立一安全資料物件之及於該安全資料物件內儲存該種子。其亦請求使該安全資料物件相關聯於用於產生該單次密碼之該單次密碼應用程式(其可以係相同於正在請求之應用程式)之ID(箭頭1148)。該安全服務模組系統建立該等安全資料物件1114之一者，且儲存該種子於該安全資料物件內，且使該安全資料物件相關聯於該單次密碼應用

程式之ID，且當完成時傳送通知給該應用程式(箭頭1150)。接著，該應用程式請求該安全服務模組系統根據由該主機所提供之使用者資訊，委派該內部存取控制記錄之用於存取該安全資料物件1114之存取權，給適當的使用者存取控制記錄(箭頭1152)。在已經完成委派之後，該安全服務模組系統通知該應用程式(箭頭1154)。接著，該應用程式係藉由一回呼功能，透過該通訊管道傳送該安全資料物件之名稱(槽ID)給該安全服務模組系統(箭頭1156)。接著，安全服務模組系統係轉遞該安全資料物件之名稱至該主機(箭頭1158)。接著，該主機繫結該安全資料物件之名稱與該使用者存取控制記錄，使得該使用者係現在能夠存取該安全資料物件。

現在將參照圖44中之協定圖而敘述單次密碼產生之程序。為了獲得該單次密碼，該使用者將登入其具有存取權之使用者存取控制記錄(箭頭1172)。假設該鑑認成功，則該安全服務模組系統通知該主機，且該主機傳送一"get SDO"(獲得安全資料物件)命令給該安全服務模組(箭頭1174，1176)。如上文所述，儲存該種子之該安全資料物件已經相關聯於一用於產生該單次密碼之應用程式。因此，不像是以前一樣透過該通訊管道選擇一應用程式，該單次密碼產生應用程式係藉由介於由該命令存取之安全資料物件(箭頭1176)與該單次密碼產生應用程式之間的關聯性所調用(箭頭1178)。接著，該單次密碼產生應用程式請求該安全服務模組系統自該安全資料物件讀取該內容(亦

即，該種子)(箭頭1180)。較佳地，該安全服務模組不知道該安全資料物件之內容內包含的資訊，且將僅按該特徵組延伸指示來處理該安全資料物件內之資料。假如該種子被加密，則此係可以牽涉到按該特徵組延伸命令在讀取之前解密該種子。該安全服務模組系統自該安全資料物件讀取該種子，且提供該種子至該單次密碼產生應用程式(箭頭1182)。接著，該單次密碼產生應用程式產生該單次密碼且提供該單次密碼給該安全服務模組系統(箭頭1184)。接著該單次密碼係由該安全服務模組轉遞至該主機(箭頭1186)，接著，該主機轉遞該單次密碼至該鑑認伺服器1052，以完成該雙因素鑑認鑑認程序。

回呼功能

於圖40A之該安全服務模組核心1004與安全性應用程式管理員模組1008之間建置一泛用回呼功能。不同的裝置內部應用程式及通訊管道可被登錄以具有此類功能。因此，當調用一裝置內部應用程式時，該應用程式可使用此回呼功能，以透過被用於傳送一主機命令至該應用程式之相同通訊管道，將處理後之資料傳送至該安全服務模組系統。

DRM系統實施例

圖45繪示DRM系統的功能方塊圖，該DRM系統採用通訊管道1104'、具有至特徵組延伸應用程式1102'之連結1108'的內容加密密鑰1114'及用於控制該等功能以實施DRM功能之控制結構1101'、1103'及1106'。如將被注意到，圖45中之架構係相當類似於圖42之架構，惟該安全性

資料結構現在包含使用權伺服器存取控制記錄1106'及播放存取控制記錄1110'(取代鑑認伺服器存取控制記錄及使用者存取控制記錄)以及內容加密密鑰1114'(取代安全資料物件)除外。此外，不牽涉到該身份物件，且因而於圖45中省略該身份物件。可以於使用權供應程序中建立該等內容加密密鑰1114'。圖46之協定圖顯示一種用於使用權供應及內容下載之程序，其中，於使用權物件中提供密鑰。如同於該單次密碼之實施例中，一想要獲得一授權之使用者將首先需要在N個存取控制記錄1106'之一者及N個存取控制記錄1110'之一者之下取得存取權，使得可藉由一媒體播放機(諸如一媒體播放機軟體應用程式)呈現內容。

如示於圖46，該主機向一使用權伺服器存取控制記錄1106'(箭頭1202)進行鑑認。假設鑑認成功(箭頭1204)，則該使用權伺服器提供一使用權檔案(license file)連同一內容加密密鑰(密鑰ID及密鑰值)給該主機。該主機亦藉由提供該應用程式ID至該卡上之該安全服務模組系統，而選擇被調用之應用程式。該主機亦傳送播放機資訊(例如，於一媒體播放機軟體應用程式上之資訊)(箭頭1206)。該播放機資訊將指示在該N個播放機存取控制記錄1110'之哪一者之下，該播放機具有存取權。該安全服務模組系統係透過對應於該選擇出之應用程式之通訊管道，而轉遞該使用權檔案及該內容加密密鑰至該DRM應用程式(箭頭1208)。接著，該被調用之應用程式請求該安全服務模組系統將該使用權檔案寫入至隱藏分割區之中(箭頭1210)。當係如此寫

入該使用權檔案時，該安全服務模組系統通知該應用程式(箭頭1212)。接著，該DRM應用程式請求一被建立之內容加密密鑰物件1114'，且將來自該使用權檔案的密鑰值儲存於該被建立之內容加密密鑰物件1114'之中。該DRM應用程式亦請求使該內容加密密鑰物件與相關聯於一DRM應用程式的ID(該DRM應用程式檢查相關聯於所提供之密鑰的授權)(箭頭1214)。該安全服務模組系統完成這些工作，且因而通知該應用程式(箭頭1216)。接著，該應用程式請求根據由主機傳送之播放機資訊，而將對該內容加密密鑰1114'之讀取存取權委派給一播放機存取控制記錄(該播放機具有對該播放機存取控制記錄的存取內容之權限)(箭頭1218)。該安全服務模組系統實行該委派，且因而通知該應用程式(箭頭1220)。由該應用程式透過該通訊管道傳送一已經完成儲存該授權之訊息至該安全服務模組系統，且該安全服務模組系統轉遞該訊息至該使用權伺服器(箭頭1222及1224)。使用一回呼功能以透過該通訊管道進行此動作。一旦接收到該通知時，接著該使用權伺服器提供以提供給該卡之該內容加密密鑰內之密鑰值加密之內容檔案。該經加密的內容係由該主機儲存於該公開卡區域中。儲存該經加密的內容檔案不牽涉到安全性功能，使得該安全服務模組系統係不牽涉到該儲存。

該播放操作係顯示於圖47。該使用者係透過該主機而向適合的播放存取控制記錄(亦即，於上文箭頭1152及1154中已被委派讀取權至其之播放存取控制記錄)進行鑑認(箭

頭1242)。假設鑑認成功(箭頭1244)，則該使用者接著傳送一請求，以讀取相關聯於該密鑰ID之內容(箭頭1246)。於接收該請求時，該安全服務模組系統將發現一DRM應用程式之ID係相關聯於正被存取之內容加密密鑰物件，且因而將導致調用該被識別之DRM應用程式(箭頭1248)。該DRM應用程式請求該安全服務模組系統讀取相關聯於該密鑰ID之資料(亦即，使用權)(箭頭1250)。該安全服務模組不知道其被請求讀取之資料內的資訊，且僅處理來自該特徵組延伸的請求，以實行該資料讀取程序。該安全服務模組系統自該隱藏分割區讀取資料(亦即，使用權)，且提供該資料至該DRM應用程式(箭頭1252)。接著，該DRM應用程式解譯該資料，且檢查該資料內之使用權資訊，以看看該使用權是否有效。假如該使用權仍然有效，則該DRM應用程式將向該安全服務模組系統通知准許進行內容解密(箭頭1254)。接著，該安全服務模組系統使用該內容加密密鑰物件內之該密鑰值解密該請求的內容，且提供該經解密的內容至該主機，以用於播放(箭頭1256)。假如該使用權不再有效，則用於內容存取之請求係被拒絕。

假使來自該使用權伺服器的使用權內未提供任何密鑰，則該使用權供應及內容下載係將稍微不同於示於圖46之方式。此類不同的方案係顯示於圖48之協定圖之中。圖46與圖48之間相同的步驟係以相同的元件符號予以識別。因此，該主機及該安全服務模組系統首先進行鑑認(箭頭1202，1204)。該使用權伺服器提供該使用權檔案及該密

鑰ID(但是無該密鑰值)給該主機，且該主機將轉遞所提供之該使用權檔案及該密鑰ID連同該主機想要調用之該DRM應用程式的ID至該安全服務模組系統。該主機亦傳送播放機資訊(箭頭1206')。接著，該安全服務模組系統係透過對應於該選擇出之應用程式之通訊管道，而轉遞該使用權檔案及該密鑰ID至該選擇出之DRM應用程式(箭頭1208)。接著，該DRM應用程式請求將該使用權檔案寫入至隱藏分割區之中(箭頭1210)。當已經如此寫入該使用權檔案時，該安全服務模組系統通知該DRM應用程式(箭頭1212)。接著，該DRM應用程式請求該安全服務模組系統產生一密鑰值、建立一內容加密密鑰物件、儲存該密鑰值於其中及使該內容加密密鑰物件相關聯於一DRM應用程式之ID(箭頭1214')。在已經符合該請求之後，該安全服務模組系統傳送一通知給該DRM應用程式(箭頭1216)。接著，該DRM應用程式將請求該安全服務模組系統根據由主機傳送之播放機資訊，而委派對該內容加密密鑰物件之讀取存取權給該播放機存取控制記錄(箭頭1218)。該其係完成時，該安全服務模組系統因而通知該DRM應用程式(箭頭1220)。接著，該DRM應用程式向該安全服務模組系統通知已經儲存該使用權，其中，該通知係藉由一回呼功能透過該通訊管道而被傳送(箭頭1222)。此項通知被轉遞至該使用權伺服器(箭頭1224)。該使用權伺服器接著傳送相關聯於一密鑰ID之內容檔案至該安全服務模組系統(箭頭1226)。該安全服務模組系統以該密鑰ID所識別之該密鑰值加密該內容，

而不牽涉到任何應用程式。如此加密及儲存於該卡上之內容係可以使用圖47之協定而被播放。

於上述之單次密碼及DRM實施例中，該特徵組延伸1102及1102'可含有許多不同的單次密碼及DRM應用程式，以供主機裝置選擇。使用者具有選擇及調用所要裝置內部應用程式之選擇機會。雖然如此，介於該安全服務模組與該特徵組延伸之間之整體關係係維持相同，使得使用者及資料提供者可使用標準的協定組，以用於與該安全服務模組互動及用於調用該特徵組延伸。使用者及提供者係不需要變成牽涉到許多不同的裝置內部應用程式之特質，該等裝置內部應用程式之一些者可以係專屬的。

再者，該等供應協定可些微不同，如同於圖46及48之情況。在圖46之情況下，該使用權物件含有一密鑰值，然而在圖48之情況下，該使用權物件無密鑰值。此差異要求略微不同的協定，如上文所述。然而，圖47中之播放係相同的，而不論如何供應該使用權。因此，此差異將僅關於內容提供者及散佈者，然而典型地係與消費者無關，消費者典型地係僅牽涉到播放階段。因此，此架構提供給內容提供者及散佈者客製化協定的大彈性，同時維持顧客容易使用。明顯地，自兩組以上供應協定所供應之資料推導而來的資訊係可以仍然可使用第二協定存取。

由上述之實施例所提供之另一優點係，雖然外部實體(諸如使用者)及該等裝置內部應用程式可共用對由該安全性資料結構所控制之資料的使用，但是使用者僅能夠存取

由該等裝置內部應用程式自所儲存的資料推導出之結果。因此，於該單次密碼之實施例中，該經過該等主機裝置之使用者僅能夠獲得該單次密碼，而無法獲得該種子值。於該DRM實施例中，該經過該等主機裝置之使用者係僅能夠獲得所呈現的內容，然而不存取該使用權檔案或密碼編譯密鑰。此特徵係允許消費者方便，而不損及安全性。

於一DRM實施例中，該等裝置內部應用程式及主機皆不能存取該等密碼編譯密鑰；僅該安全性資料結構可存取該等密碼編譯密鑰。於其他實施例中，除了該安全性資料結構以外之實體係亦能夠存取該密碼編譯密鑰。該等密鑰亦能夠藉由該等裝置內部應用程式所產生，且接著由該安全性資料結構所控制。

存取該等裝置內部應用程式及存取資訊(例如，單次密碼及所呈現之內容)係受控於相同的安全性資料結構。此減少控制系統及成本之複雜度。

藉由提供自該內部存取控制記錄(其控制對該等裝置內部應用程式之存取)委派存取權給一存取控制記錄(其控制該等主機存取由調用該等裝置內部應用程式所獲得之資訊)之能力，此特徵使達成上述特徵及功能係可能的。

應用程式特定之廢止方案

當被調用一裝置內部應用程式係時，亦可被修改該安全性資料結構之存取控制協定。舉例而言，該憑證廢止協定可以係一使用憑證廢止清單之標準協定或一專屬協定。因此，藉由調用一特徵組延伸，該標準的憑證廢止清單廢止

協定可被一特徵組延伸專屬協定所取代。

除了支援該憑證廢止清單廢止方案，安全儲存應用程式使一駐留於該裝置內的特定內部應用程式，能夠透過介於該裝置內部應用程式與該憑證授權單位或任何其他廢止授權單位之間之一私有通訊通道而廢止主機。該內部應用程式專屬廢止方案係受限於該主機-應用程式之關係。

當組態應用程式特定之廢止方案時，該安全儲存應用程式系統將拒絕該憑證廢止清單(假如被提供)，否則將使用該憑證及該專屬應用程式資料(先前透過一應用程式特定通訊管道予以提供)，以決定是否該給定的憑證被廢止。

如上文所述，一存取控制記錄係藉由指定一廢止值，而指定三種廢止方案(無廢止方案、標準憑證廢止清單方案及應用程式特定廢止方案)之哪一者被採用。當選擇該應用程式特定廢止方案選項時，該存取控制記錄將亦指定用於管理該廢止方案之內部應用程式ID之一ID，且該憑證廢止清單到期時期/APP_ID欄位內之值將對應於管理該廢止方案之內部應用程式ID。當鑑認該裝置時，安全儲存應用程式系統接著將支持該內部應用程式之專屬方案。

不以另一組協定取代一組協定，一裝置內部應用程式之調用可對已經由該安全儲存應用程式所行使之存取控制附加額外的存取條件。舉例而言，可由一特徵組延伸進一步詳細檢查存取內容加密密鑰內之一密鑰值之權利。在該安全儲存應用程式系統決定一存取控制記錄具有對一密鑰值之存取權利之後，將在授予該存取之前查詢該特徵組延

伸。此特徵允許內容擁有者控制對該內容之存取的大彈性。

雖然上文已參照各種實施例而敘述本發明，將瞭解的是，可實行變化及修改，而未不偏離本發明之範疇，本發明之範疇僅由後附申請專利範圍及其均等物所定義。

【圖式簡單說明】

圖1繪示有助於闡釋本發明之與主機裝置通訊之記憶體系統之方塊圖。

圖2繪示有助於闡釋本發明之不同實施例之記憶體的不同分割區及儲存於不同分割區之未經加密及經加密檔案之示意圖，其中，對某些分割區及經加密檔案之存取係由存取原則及鑑認程序所控制。

圖3繪示記憶體內不同分割區之記憶體的示意圖。

圖4繪示有助於闡釋本發明之不同實施例之示於圖3之記憶體的不同分割區之檔案位置表的示意圖，其中，該等分割區內某些檔案係被加密。

圖5繪示有助於闡釋本發明之不同實施例之一存取控制記錄群組內之存取控制記錄及相關密鑰參照之示意圖。

圖6繪示有助於闡釋本發明之不同實施例之由存取控制記錄群組及存取控制記錄所形成之樹狀結構之示意圖。

圖7繪示存取控制記錄群組之三個樹狀階層架構之樹的示意圖，以闡釋樹的形式程序。

圖8A及8B繪示由一主機裝置及一諸如一記憶體卡之記憶體裝置所實行用於建立及使用一系統存取控制記錄之程

序的流程圖。

圖9繪示有助於闡釋本發明之不同實施例之一使用一系統存取控制記錄以建立一存取控制記錄群組之程序的流程圖。

圖10繪示一用於建立一存取控制記錄之程序的流程圖。

圖11繪示樹狀階層架構之特定應用程式的兩個存取控制記錄群組之示意圖。

圖12繪示一用於委派特定權利之程序的流程圖。

圖13繪示一存取控制記錄群組及一存取控制記錄之示意圖，以闡釋圖12之委派特程序。

圖14繪示用於建立一用於加密及/或解密用途之密鑰的程序的流程圖。

圖15繪示一用於根據一存取控制記錄移除存取權及/或資料存取權限之程序的流程圖。

圖16繪示一用於當存取權及/或存取權限係已經被刪除或已經過期時請求存取的程序的流程圖。

圖17A及17B繪示有助於闡釋本發明之不同實施例之用於鑑認及授予存取密碼編譯密鑰之原則之規則結構的組織之示意圖。

圖18繪示一用於根據原則來控制對受保護資訊之存取的替代方法之資料結構的方塊圖。

圖19繪示使用密碼之鑑認程序的流程圖。

圖20繪示若干主機憑證鏈之圖式。

圖21繪示若干裝置憑證鏈之圖式。

圖22及圖23(包含圖23A及23B)繪示用於單向及互相鑑認方案之程式的協定圖。

圖24繪示有助於闡釋本發明之一項實施例之一憑證鏈之圖式。

圖25繪示在憑證緩衝區之前之一控制區段內的資訊的表，該資訊係由該主機傳送，用於傳送最後一憑證至一記憶體裝置，其係顯示該憑證係該憑證鏈內最後一憑證之一項指示，以闡釋本發明之另一項實施例。

圖26及27係分別顯示用於鑑認方案之卡及主機程序的流程圖，其中，一記憶體卡正在鑑認一主機裝置。

圖28及29係分別顯示用於鑑認方案之卡及主機程序的流程圖，其中，主機裝置正在鑑認一記憶體卡。

圖30及31繪示分別由一主機裝置及一記憶體裝置所實施之程序的流程圖，其中，該主機裝置擷取儲存於該記憶體裝置內的憑證廢止清單，以闡釋本發明之另一項實施例。

圖32繪示列出憑證廢止清單內之欄位的憑證廢止清單圖式，以闡釋本發明之另一項實施例。

圖33及34分別繪示用於使用憑證廢止清單來驗證憑證之卡及主機程序的流程圖。

圖35繪示用於卡對傳送至該主機之資料加上簽名及用於自該主機解密資料的卡程序的流程圖。

圖36繪示主機程序的流程圖，其中，卡對傳送至該主機之資料加上簽名。

圖37繪示主機程序的流程圖，其中，該主機傳送經加密

資料至該記憶體卡。

圖38及39分別繪示用於一般資訊查詢及謹慎資訊查詢之程序的流程圖。

圖40A係一記憶體裝置(諸如一快閃記憶體卡)連接至一主機裝置的系統架構之功能方塊圖，以闡釋本發明之一項實施例。

圖40B繪示圖40A之安全服務模組核心的內部軟體模組之功能方塊圖。

圖41繪示用於建立單次密碼之系統之方塊圖。

圖42繪示單次密碼種子供應及單次密碼產生之功能方塊圖。

圖43繪示種子供應階段的協定圖。

圖44繪示單次密碼產生階段的協定圖。

圖45繪示DRM系統的功能方塊圖。

圖46繪示用於使用權供應及內容下載之程序的協定圖，其中，使用權物件中提供密鑰。

圖47繪示用於播放操作之程序的協定圖。

圖48繪示一用於使用權供應及內容下載之程序的協定圖，其中，使用權物件中未提供密鑰。

【主要元件符號說明】

| | |
|---|---|
| 10 | 記憶體系統 |
| 10' | 記憶體卡或記憶體條 |
| 12 | 中央處理單元 |
| 12a | 中央處理單元隨機存取記憶體 |

| | |
|---|---|
| 14 | 緩衝管理單元(BMU) |
| 16 | 主機介面模組(HIM) |
| 18 | 快閃記憶體介面模組(FIM) |
| 20 | 快閃記憶體 |
| 22 | 周邊裝置存取模組(PAM) |
| 24 | 主機裝置 |
| 26 | 主機介面匯流排 |
| 26a | 埠 |
| 28 | 快閃記憶體介面匯流排 |
| 28a | 埠 |
| 32 | 主機直接記憶體存取(HDMA) |
| 34 | 快閃直接記憶體存取(FDMA) |
| 36 | 仲裁器 |
| 38 | 緩衝隨機存取記憶體(BRAM) |
| 40 | 密碼編譯引擎 |
| 101 | 檔案 |
| 102及104 | 檔案 |
| 106 | 未經加密檔案 |
| 130 | 根存取控制記錄群組 |
| 132 | 根存取控制記錄群組 |
| 502 | 主機根憑證授權單位憑證 |
| 504 | 主機1憑證授權單位(第二層級)憑證 |
| 506 | 主機憑證 |
| 508 | 主機n憑證授權單位(第二層級)憑證 |

| | |
|---|---|
| 510 | 主機1憑證授權單位(第三層級)憑證 |
| 512 | 主機憑證 |
| 514 | 主機憑證 |
| 520 | 裝置根憑證授權單位憑證 |
| 522 | 裝置1憑證授權單位(製造商)憑證 |
| 524 | 裝置憑證 |
| 526 | 裝置n憑證授權單位(製造商)憑證 |
| 528 | 裝置憑證 |
| 542 | 安全服務模組系統 |
| 540 | 主機系統 |
| 550 | 存取控制記錄 |
| 548 | 主機根憑證 |
| 544 | 主機憑證 |
| 546 | 主機公開密鑰 |
| 549 | 中間憑證授權單位 |
| 554 | 隨機號碼 |
| 547 | 私有密鑰 |
| 562 | 隨機號碼 |
| 590 | 憑證鏈 |
| 590(1) | 憑證鏈 |
| 590(2) | 憑證 |
| 590(9) | 憑證 |
| 591、593、595、597及599 | 憑證串 |

| | |
|---|---|
| 1000 | 系統架構 |
| 1002 | 安全儲存應用程式傳輸層 |
| 1004 | 安全服務模組核心 |
| 1012 | 密碼編譯庫 |
| 1006 | 安全服務模組核心API |
| 1010 | 裝置內部應用程式 |
| 1008 | 安全性應用程式管理員模組 |
| 1011 | 裝置管理系統 |
| 1022 | 安全儲存應用程式命令處理常式 |
| 1024 | 安全儲存應用程式管理員 |
| 1026 | 安全儲存應用程式資料庫 |
| 1028 | 安全儲存應用程式非安全操作模組 |
| 1030 | 安全儲存應用程式安全操作模組 |
| 1032 | 模組 |
| 1034 | 模組 |
| 1050 | 系統 |
| 1052 | 鑑認伺服器 |
| 1054 | 網際網路伺服器 |
| 1058 | 符記 |
| 1056 | 使用者 |
| 1100 | 安全儲存應用程式特徵組延伸系統 |
| 1102 | 軟體程式碼特徵組延伸 |
| 1104 | 通訊管道 |
| 1106 | 應用程式存取控制記錄 |

| | |
|---|---|
| 1101 | 存取控制記錄 |
| 1103 | 存取控制記錄 |
| 1106 | 存取控制記錄 |
| 1110 | 存取控制記錄 |
| 1120 | 身份物件 |
| 1122 | 身份物件 |
| 1114 | 安全資料物件 |
| 1116 | 身份物件 |
| 1104' | 通訊管道 |
| 1102' | 特徵組延伸應用程式 |
| 1108' | 連結(關聯性) |
| 1114' | 內容加密密鑰 |
| 1101'、1103'及 1106' | 控制結構 |
| 1110' | 存取控制記錄 |

## 五、中文發明摘要：

主機裝置將主機憑證及有關憑證廢止清單提交給記憶體裝置以供鑑認，使得該記憶體裝置無需自己獲得清單。可由該記憶體裝置同時執行對該憑證廢止清單之處理與對於憑證識別之搜尋。為了方便使用者起見，可將用於向記憶體裝置驗證主機裝置之憑證廢止清單儲存於該記憶體裝置之一未受保護區域中。

## 六、英文發明摘要：

Host devices present both the host certificate and the pertinent certificate revocation lists to the memory device for authentication so that the memory device need not obtain the list on its own. Processing of the certificate revocation list and searching for the certificate identification may be performed concurrently by the memory device. The certificate revocation lists for authenticating host devices to memory devices may be stored in an unsecured area of the memory device for convenience of users.

## 十、申請專利範圍：

1. 一種用於使用一憑證廢止清單來驗證一憑證之方法，其中於一裝置處接收來自一實體的該憑證廢止清單之部分該方法包含：

使用該裝置來循序地處理一憑證廢止清單之該等部分；及

使用該裝置在該清單上搜尋對該憑證之一參照，其中該處理與該搜尋被同時執行。

2. 如請求項1之方法，其中該清單之部分係以一時間序列而接收自該實體，且該處理在該清單之該等部分被接收時同時被執行。

3. 如請求項1之方法，其中該處理在該憑證廢止清單之部分已被處理之後丟棄該等部分。

4. 如請求項1之方法，其中該處理包括在該清單之該等部分被接收時，藉由一雜湊演算法來雜湊該清單之該等部分，以獲得一經雜湊憑證廢止清單。

5. 如請求項4之方法，其中在該裝置處接收一經加密雜湊憑證廢止清單之部分，該處理包括對該等經加密雜湊部分進行解密以獲得一經解密且經雜湊之憑證廢止清單，及比較該經雜湊憑證廢止清單與該經解密且經雜湊之憑證廢止清單。

6. 如請求項1之方法，其中該等部分包括該清單上被廢止之憑證的序號。

7. 一種用於向一記憶體系統驗認一主機之方法，該記憶體

系統被組態成可移除式地連接至該主機，該記憶體系統包含：

一非揮發性記憶體，其儲存至少一憑證廢止清單，該非揮發性記憶體能夠儲存資料；及

一控制器，其經由一驗認程序而控制由該主機對該資料之存取，在該驗認程序中，該主機將至少一憑證提交給該記憶體系統；該方法包含：

回應於一來自該主機之請求，將該至少一憑證廢止清單提供給該主機，而無需驗認該主機；

接收由該主機所提交之該至少一憑證及該至少一憑證廢止清單；

檢查由該主機所提交之該至少一憑證是否在該至少一憑證廢止清單上；及

當由該主機所提交之該至少一憑證在該至少一憑證廢止清單上時，使該驗認程序失敗。

8. 一種用於一非揮發性記憶體裝置與一主機之間的相互驗認之方法，該非揮發性記憶體裝置可移除式地連接至該主機，其中：

由該主機向該記憶體裝置提交一第一憑證及一憑證廢止清單，該憑證廢止清單係用於由該記憶體裝置對該第一憑證進行驗證；及

由該記憶體裝置向該主機提交一用於由該主機進行驗證之第二憑證，而無一憑證廢止清單。

9. 如請求項8之方法，其中該非揮發性記憶體裝置儲存用

於該主機之該憑證廢止清單，該方法進一步包含該主機獲得來自該非揮發性記憶體裝置之該憑證廢止清單。

10. 如請求項9之方法，進一步包含該非揮發性記憶體裝置接收來自該主機之該憑證廢止清單，以用於驗認來自該主機之該第一憑證。

11. 一種用於藉由一記憶體系統來驗認一主機裝置之方法，包含：

將該記憶體系統可移除式地連接至該主機裝置；及

將來自該主機裝置之一憑證及一憑證廢止清單發送至該記憶體系統。

12. 一種被組態成可移除式地連接至一主機之記憶體系統，包含：

一非揮發性記憶體，其儲存至少一憑證廢止清單，該非揮發性記憶體能夠儲存資料；及

一控制器，其經由一驗認程序而控制由該主機對該資料之存取，在該驗認程序中，該主機將至少一憑證提交給該記憶體系統，且該控制器檢查由該主機所提交之該至少一憑證是否在該至少一憑證廢止清單上，且當由該主機所提交之該至少一憑證在該至少一憑證廢止清單上時，使該驗認程序失敗。

13. 如請求項12之記憶體系統，該非揮發性記憶體包括一未受保護區域，該未受保護區域可供該主機存取而無需經由該驗認程序驗認該主機，其中該至少一憑證廢止清單被儲存於該未受保護區域中。

14. 一種可移除式地連接至一主機之非揮發性記憶體裝置，該主機將一憑證廢止清單之部分循序地發送至該記憶體裝置以用於一憑證之驗證，該記憶體裝置包含一控制器，該控制器驗證該憑證廢止清單、循序地處理該憑證廢止清單之該等部分以及在該清單上搜尋一憑證之一識別，其中該處理與該搜尋被同時執行。

15. 如請求項14之裝置，其中該控制器在該清單之該等部分自該主機被接收時同時執行該處理。

16. 如請求項14之裝置，其中該控制器在該憑證廢止清單之部分已被處理之後丟棄該等部分。

17. 如請求項14之裝置，其中該控制器在該清單之該等部分被接收時，藉由雜湊該等部分來處理該清單之該等部分以獲得一經雜湊憑證廢止清單。

18. 如請求項17之裝置，其中在該裝置處被接收一經加密雜湊憑證廢止清單之部分，且該控制器藉由對一經加密雜湊憑證廢止清單之部分進行解密來處理該等經加密雜湊部分以獲得一經解密且經雜湊憑證廢止清單，並比較該經雜湊憑證廢止清單與該經解密且經雜湊憑證廢止清單。

19. 如請求項14之裝置，其中該等部分包括該清單上被廢止之憑證的序號。

十一、圖式：

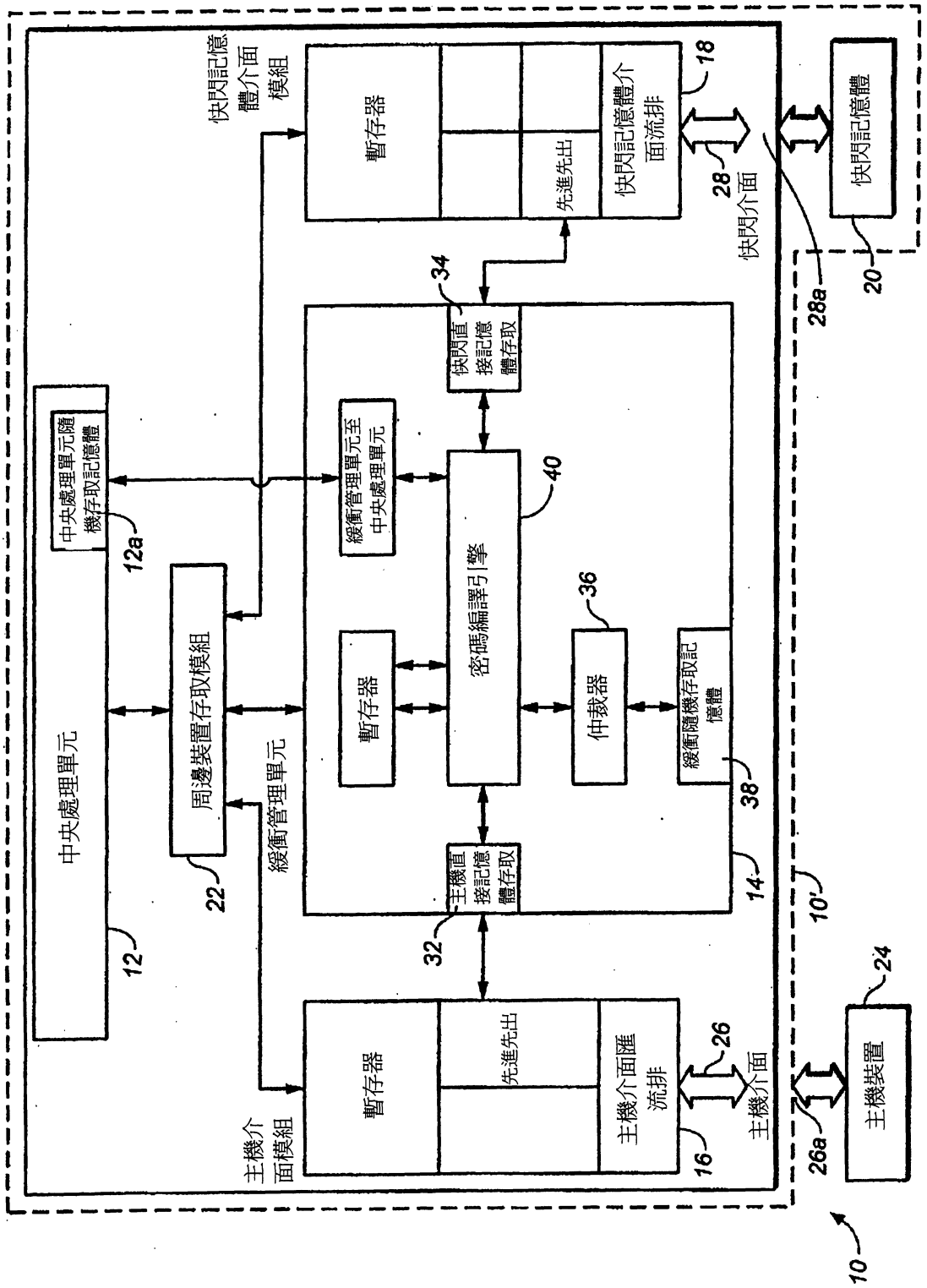
中央處理單元
中央處理單元隨機存取記憶體
12a
12
周邊裝置存取模組
22
緩衝管理單元
主機介面模組
暫存器
先進先出
主機介面匯流排
16
主機介面
26
26a
主機裝置
24
10
32
主機直接記憶體存取
14
10'
緩衝管理單元至中央處理單元
暫存器
密碼編譯引擎
40
仲裁器
36
緩衝隨機存取記憶體
38
34
快閃直接記憶體存取
快閃記憶體介面模組
暫存器
先進先出
快閃記憶體介面流排
18
28
快閃介面
28a
20
快閃記憶體

圖 1

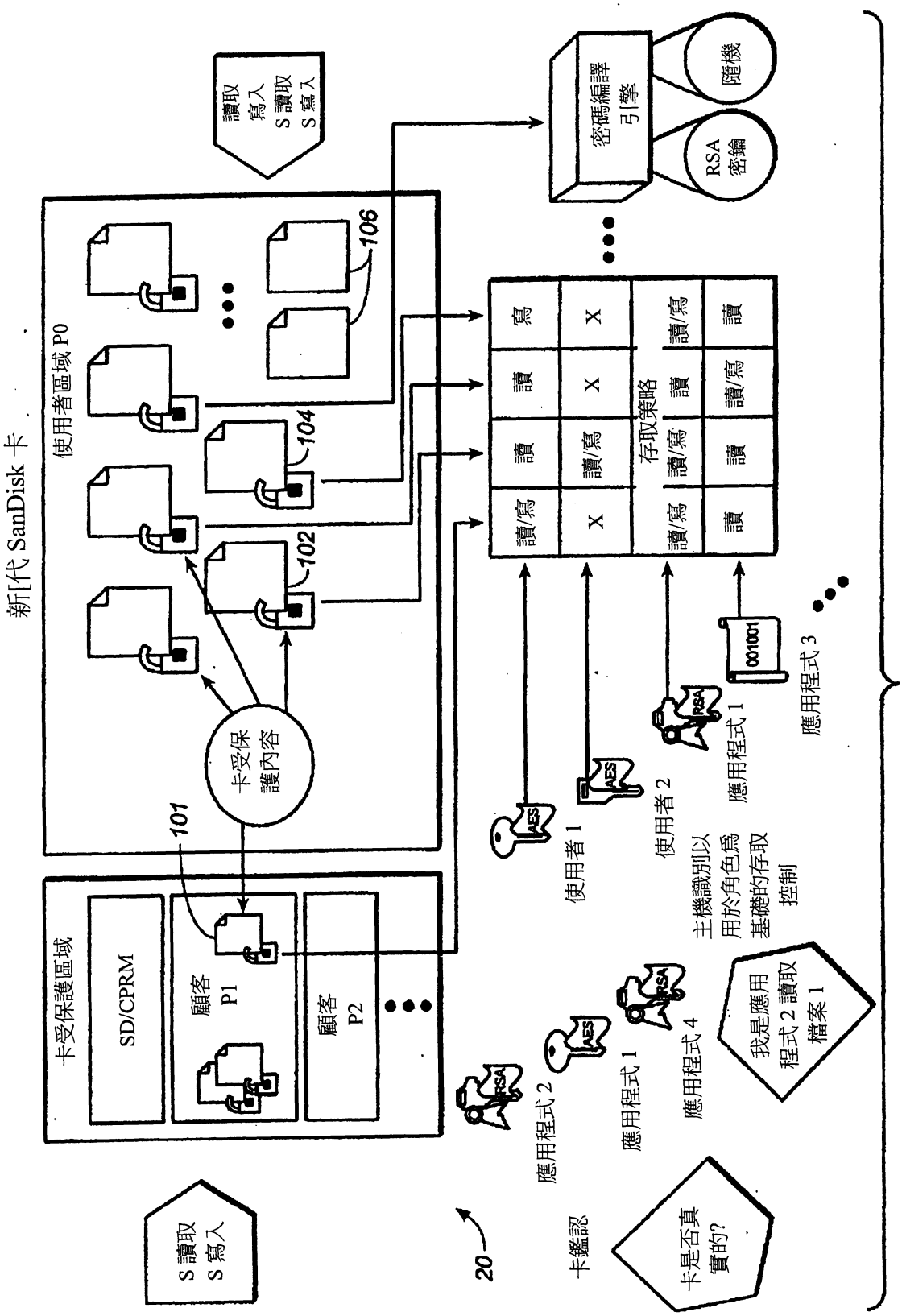
新代 SanDisk 卡
使用者區域 P0
卡受保護區域
SD/CPRM
顧客 P1
顧客 P2
卡受保護內容
101
102
104
106
讀取 寫入 S 讀取 S 寫入
密碼編譯引擎
RSA 密鑰
隨機
存取策略
讀/寫
讀
寫
X
使用者 1
使用者 2
應用程式 1
應用程式 3
主機識別以用於角色爲基礎的存取控制
我是應用程式 2 讀取檔案 1
S 讀取 S 寫入
卡是否真實的?
卡鑑認
應用程式 2
應用程式 1
應用程式 4
20

圖 2

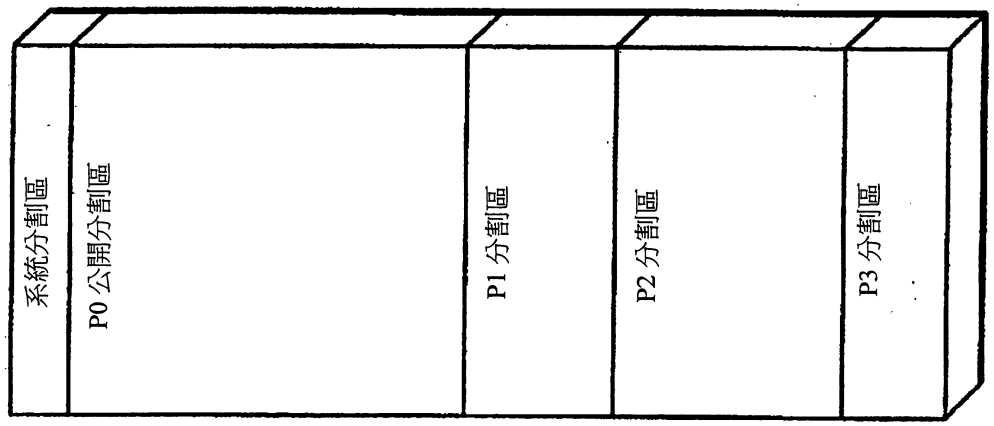
系統分割區
P0 公開分割區
P1 分割區
P2 分割區
P3 分割區

圖 3

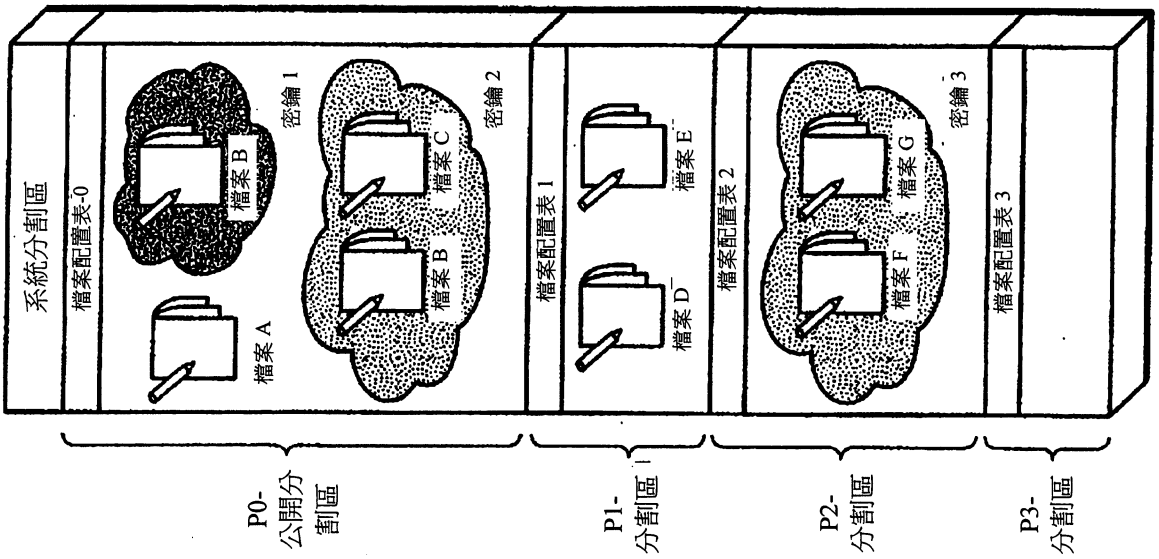
系統分割區
檔案配置表-0
檔案 A
檔案 B
密鑰 1
檔案 B
檔案 C
密鑰 2
檔案配置表 1
檔案 D
檔案 E
密鑰 3
檔案配置表 2
檔案 F
檔案 G
檔案配置表 3
P0-
公開分
割區
P1-
分割區
P2-
分割區
P3-
分割區

圖 4

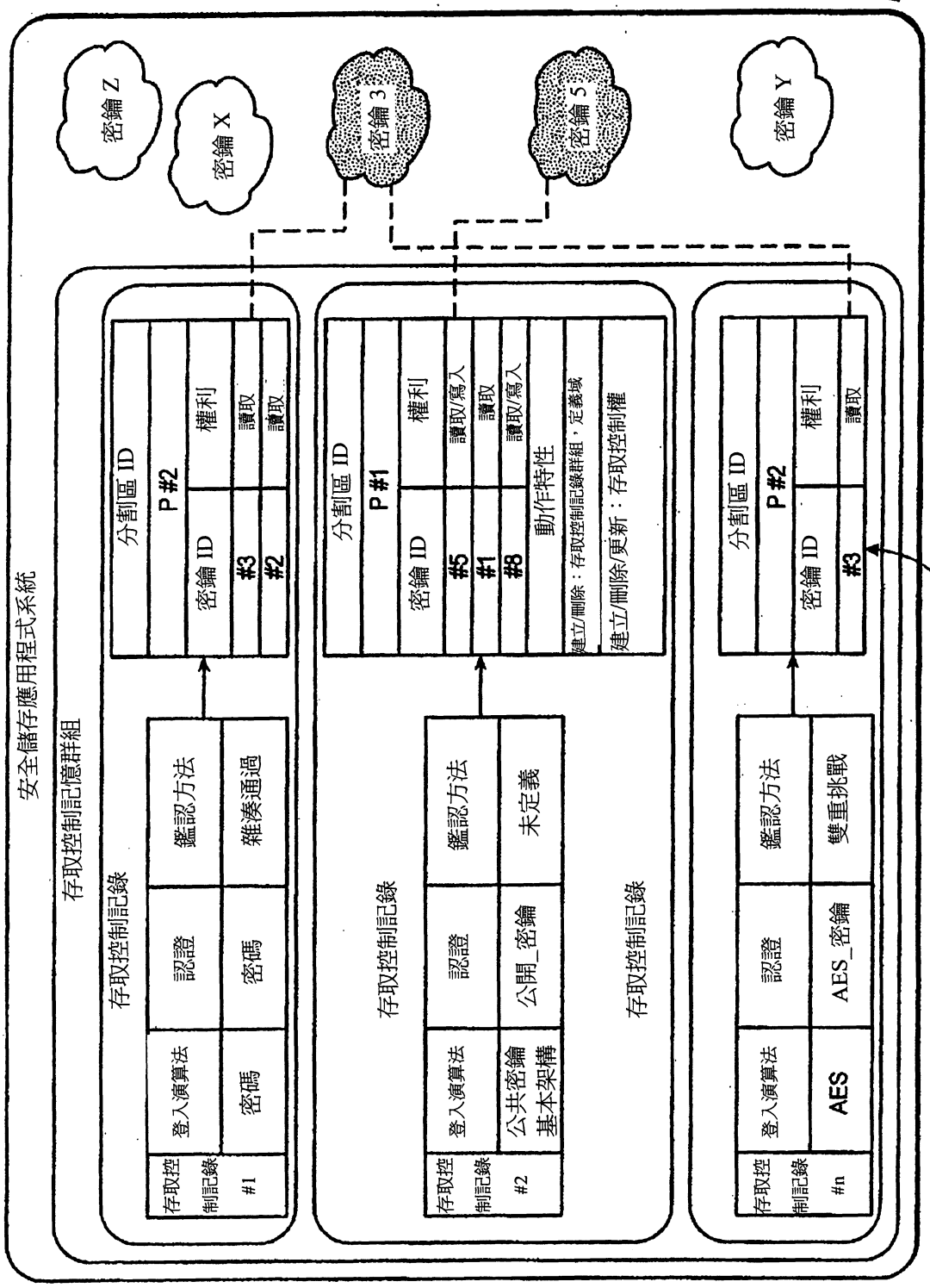
安全儲存應用程式系統
存取控制記憶群組
存取控制記錄
存取控制記錄
#1
登入演算法
密碼
認證
密碼
鑑認方法
雜湊通過
分割區 ID
P #2
密鑰 ID
權利
#3
讀取
#2
讀取
存取控制記錄
#2
登入演算法
公共密鑰基本架構
認證
公開_密鑰
鑑認方法
未定義
分割區 ID
P #1
密鑰 ID
權利
#5
讀取/寫入
#1
讀取
#8
讀取/寫入
動作特性
建立/刪除：存取控制記錄群組，定義域
建立/刪除/更新：存取控制權
存取控制記錄
#n
登入演算法
AES
認證
AES_密鑰
鑑認方法
雙重挑戰
分割區 ID
P #2
密鑰 ID
權利
#3
讀取
密鑰 Z
密鑰 X
密鑰 3
密鑰 5
密鑰 Y
權限控制記錄

圖 5

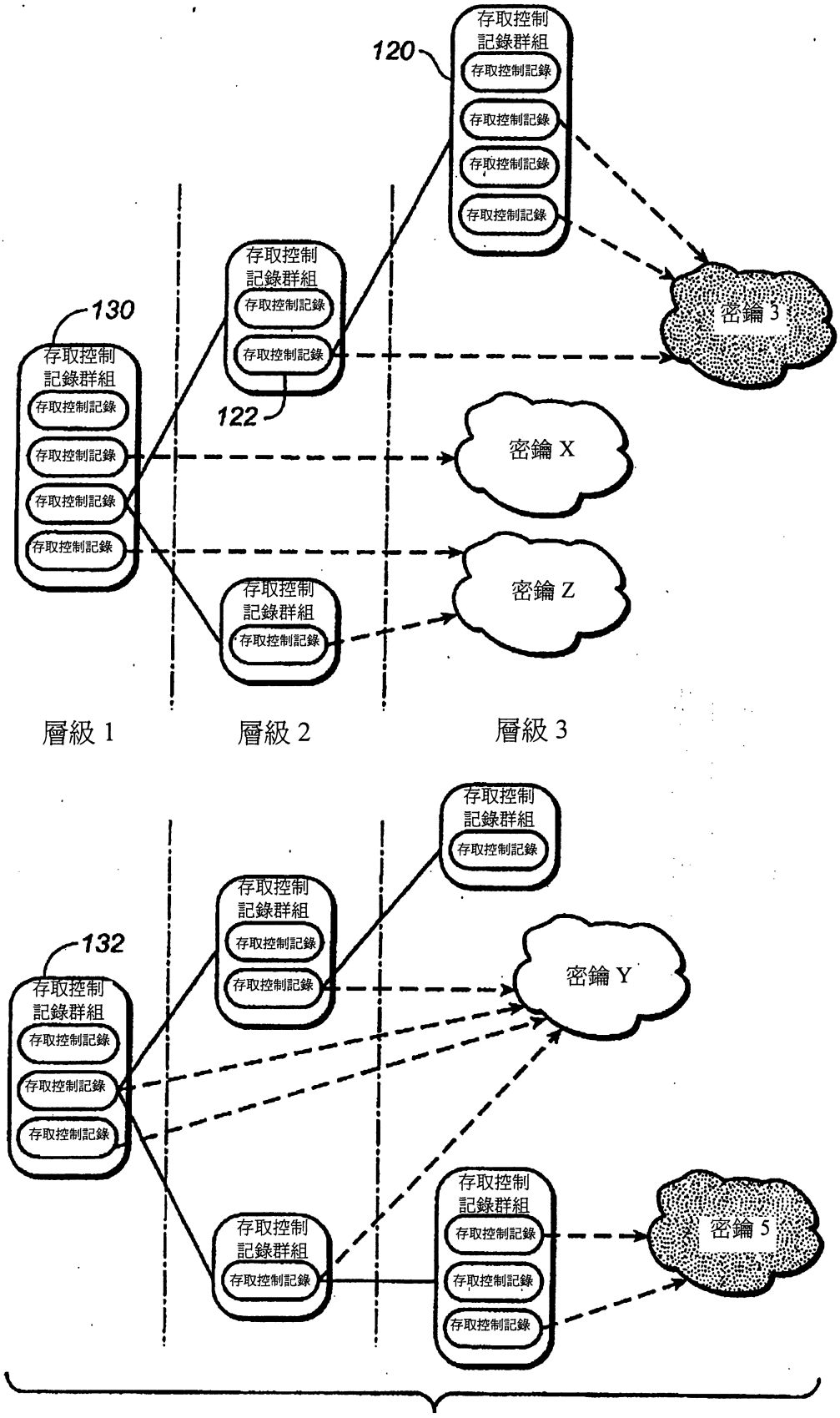
120
存取控制記錄群組
存取控制記錄
存取控制記錄
存取控制記錄
存取控制記錄
130
存取控制記錄群組
存取控制記錄
存取控制記錄
存取控制記錄
存取控制記錄
122
存取控制記錄群組
存取控制記錄
存取控制記錄
密鑰 3
密鑰 X
密鑰 Z
存取控制記錄群組
存取控制記錄
層級 1
層級 2
層級 3
132
存取控制記錄群組
存取控制記錄
存取控制記錄
存取控制記錄
存取控制記錄群組
存取控制記錄
存取控制記錄
密鑰 Y
存取控制記錄群組
存取控制記錄
存取控制記錄群組
存取控制記錄
存取控制記錄
存取控制記錄
密鑰 5

圖6

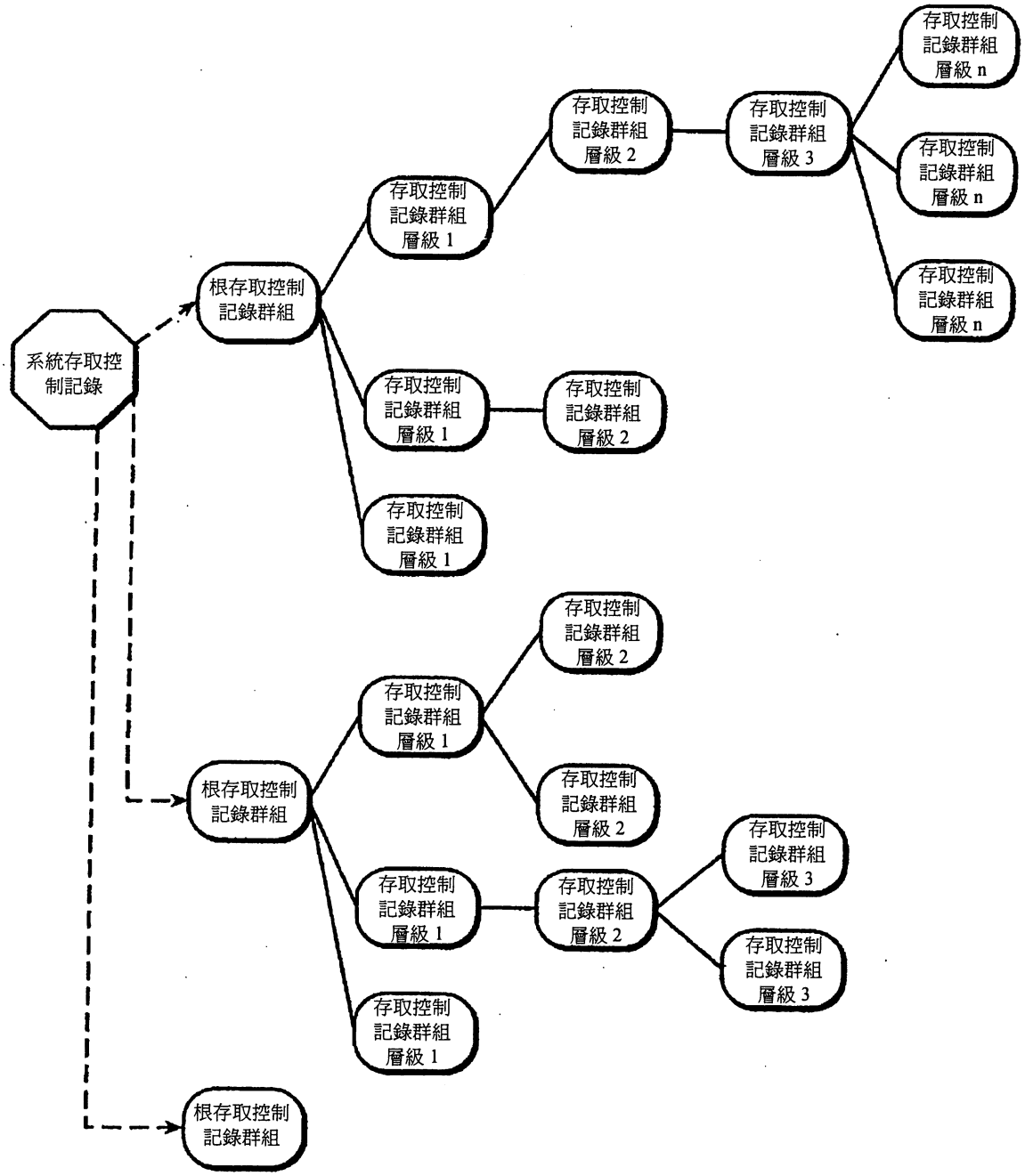
系統存取控制記錄
根存取控制記錄群組
存取控制記錄群組層級 1
存取控制記錄群組層級 2
存取控制記錄群組層級 3
存取控制記錄群組層級 n
存取控制記錄群組層級 n
存取控制記錄群組層級 n
存取控制記錄群組層級 1
存取控制記錄群組層級 2
存取控制記錄群組層級 1
根存取控制記錄群組
存取控制記錄群組層級 1
存取控制記錄群組層級 2
存取控制記錄群組層級 2
存取控制記錄群組層級 1
存取控制記錄群組層級 2
存取控制記錄群組層級 3
存取控制記錄群組層級 3
存取控制記錄群組層級 1
根存取控制記錄群組

圖7

建立系統存取控制記錄

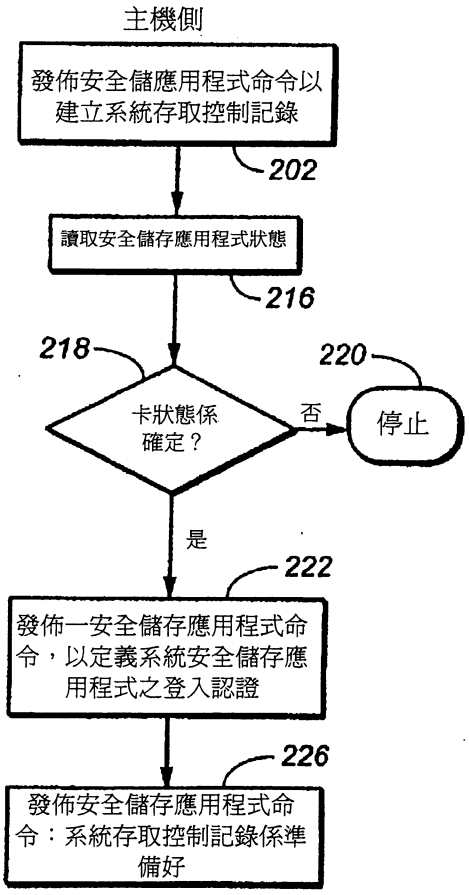


圖 8A

建立系統存取控制記錄

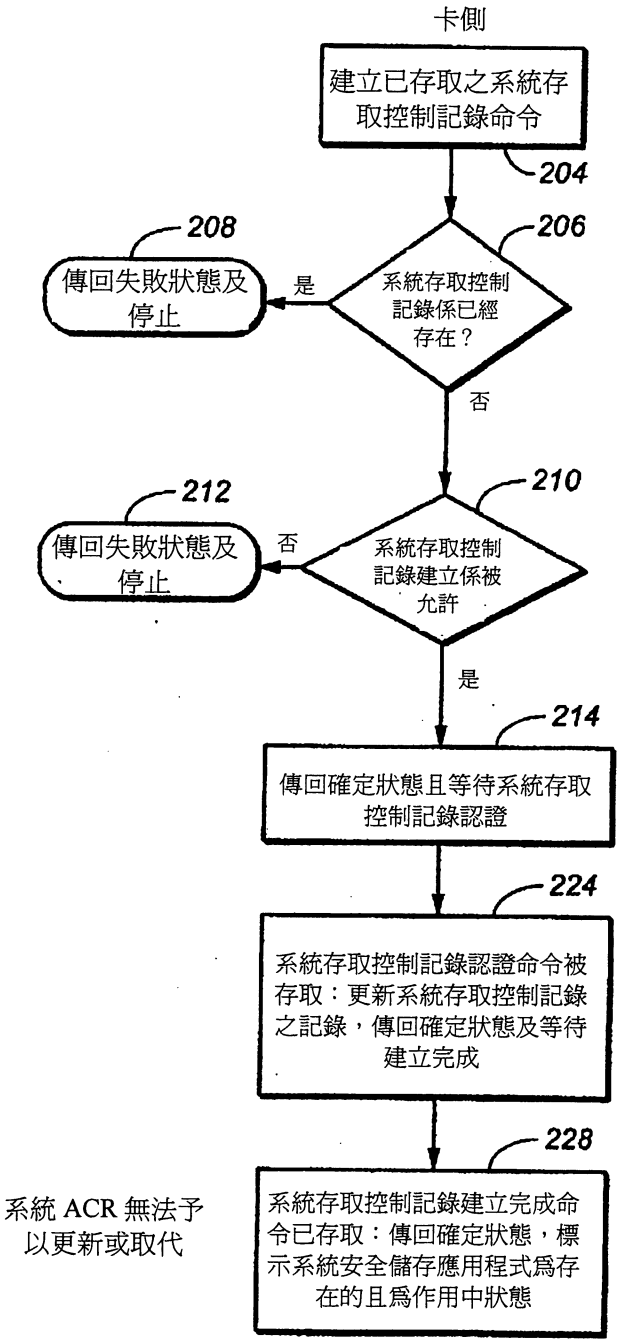


圖 8B

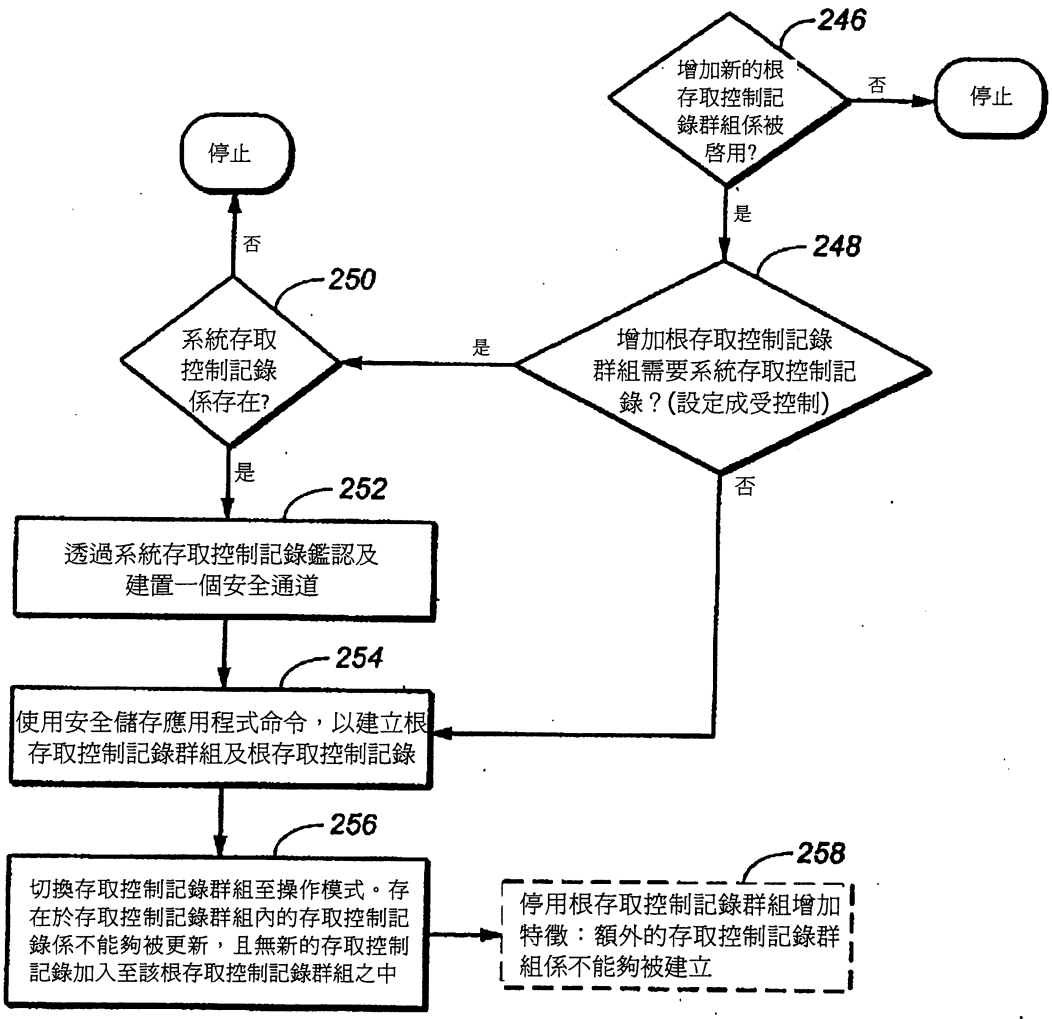
246
增加新的根存取控制記錄群組係被啓用?
否
停止
是
248
增加根存取控制記錄群組需要系統存取控制記錄？(設定成受控制)
是
250
系統存取控制記錄係存在?
否
停止
是
252
透過系統存取控制記錄鑑認及建置一個安全通道
否
254
使用安全儲存應用程式命令，以建立根存取控制記錄群組及根存取控制記錄
256
切換存取控制記錄群組至操作模式。存在於存取控制記錄群組內的存取控制記錄係不能夠被更新，且無新的存取控制記錄加入至該根存取控制記錄群組之中
258
停用根存取控制記錄群組增加特徵：額外的存取控制記錄群組係不能夠被建立

圖 9

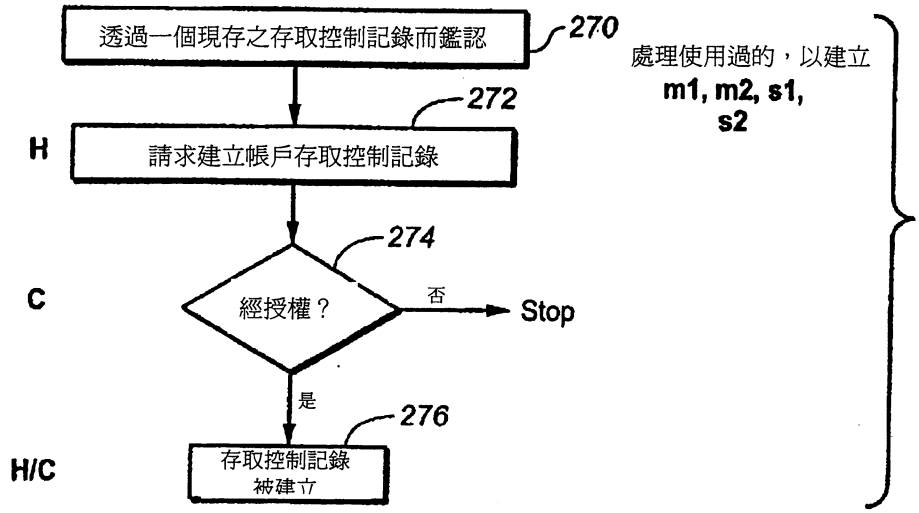
透過一個現存之存取控制記錄而鑑認
270
處理使用過的，以建立
m1, m2, s1, s2
272
H
請求建立帳戶存取控制記錄
274
C
經授權？
否
Stop
是
276
H/C
存取控制記錄被建立

圖 10

於行銷存取控制群組內建立 2 個存取控制(記錄)(m1, m2)
於銷售存取控制群組內建立 2 個存取控制(記錄)(s1, s2)

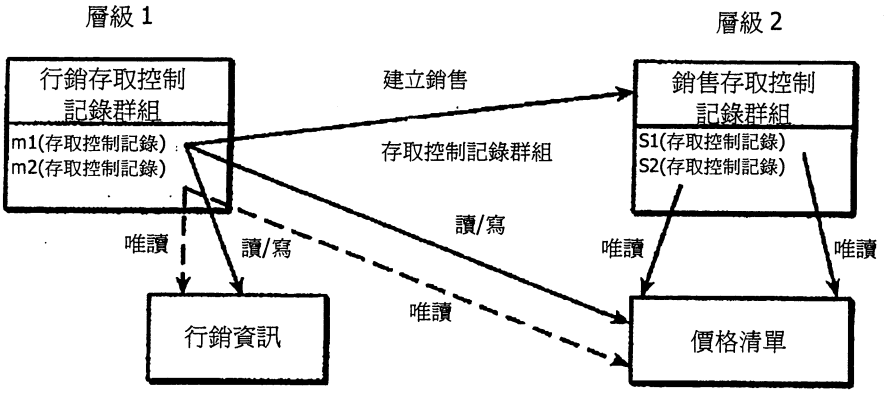


圖 11

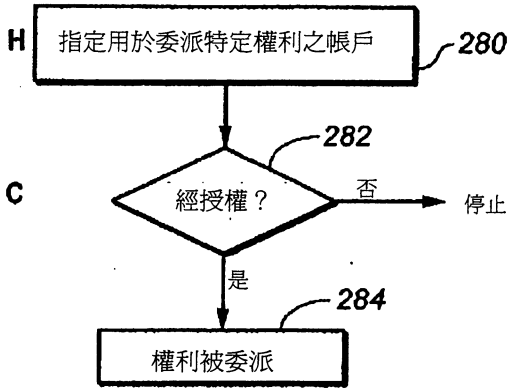


圖 12

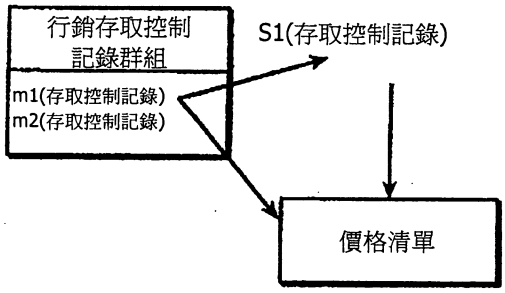


圖 13

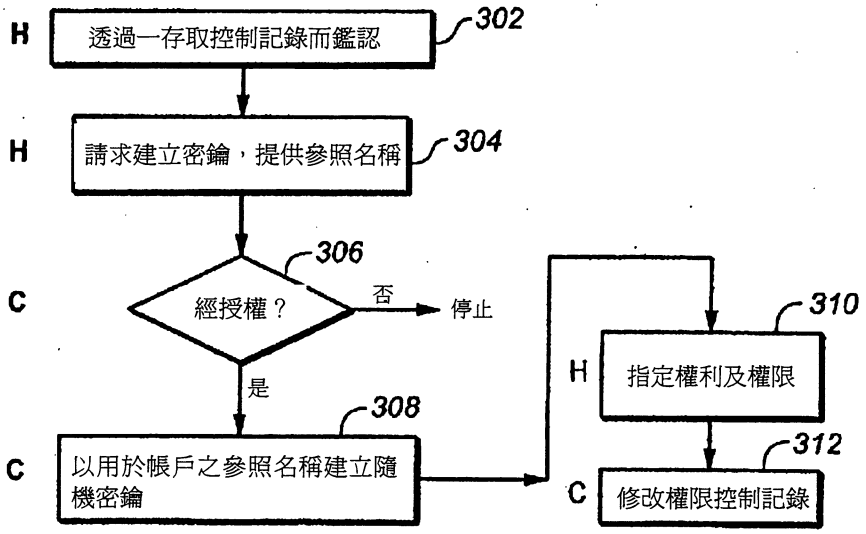


圖 14

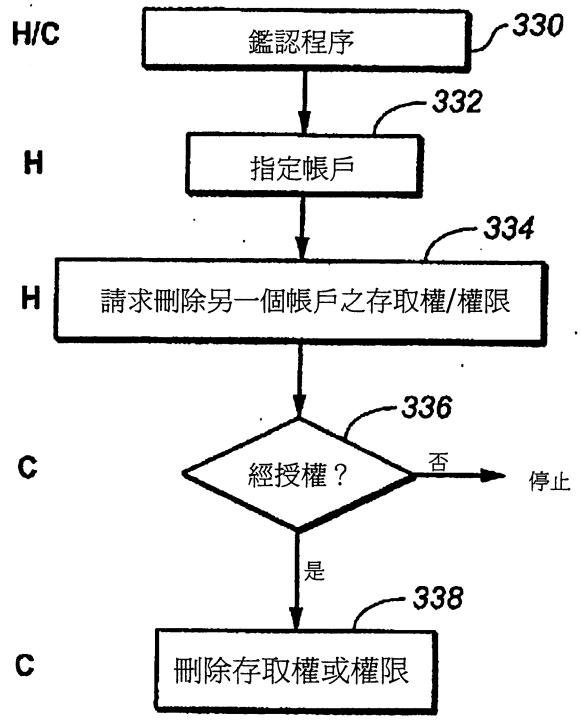
H/C
鑑認程序
330
332
H
指定帳戶
334
H
請求刪除另一個帳戶之存取權/權限
336
C
經授權？
否
停止
是
338
C
刪除存取權或權限

圖 15

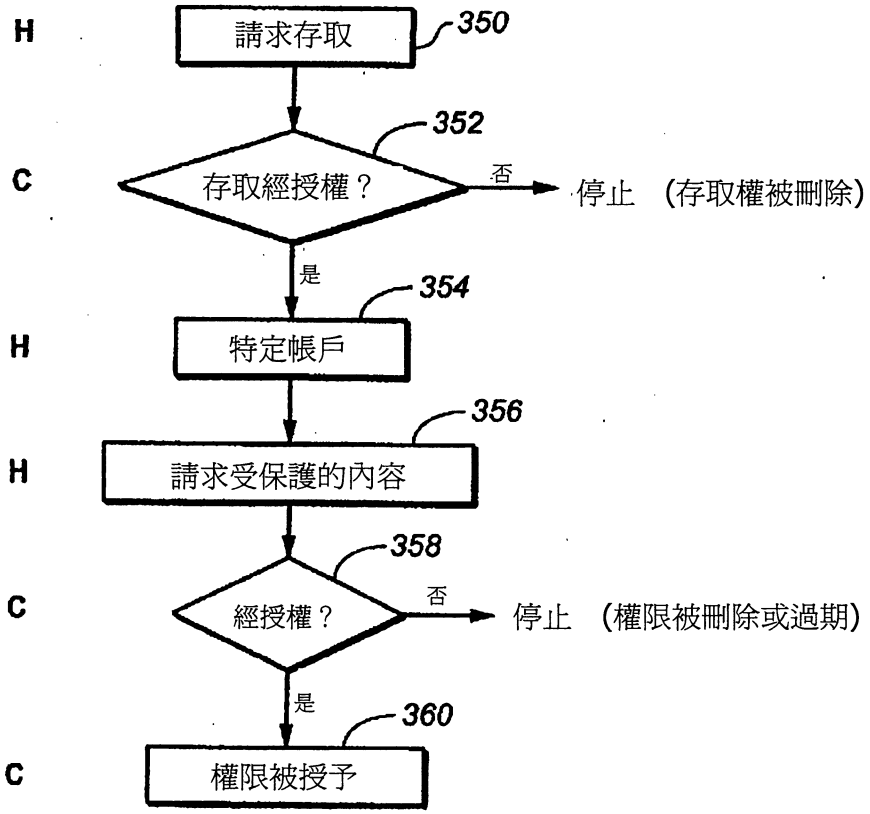
H
請求存取
350
352
C
存取經授權？
否
停止 (存取權被刪除)
是
354
H
特定帳戶
356
H
請求受保護的內容
358
C
經授權？
否
停止 (權限被刪除或過期)
是
360
C
權限被授予

圖 16

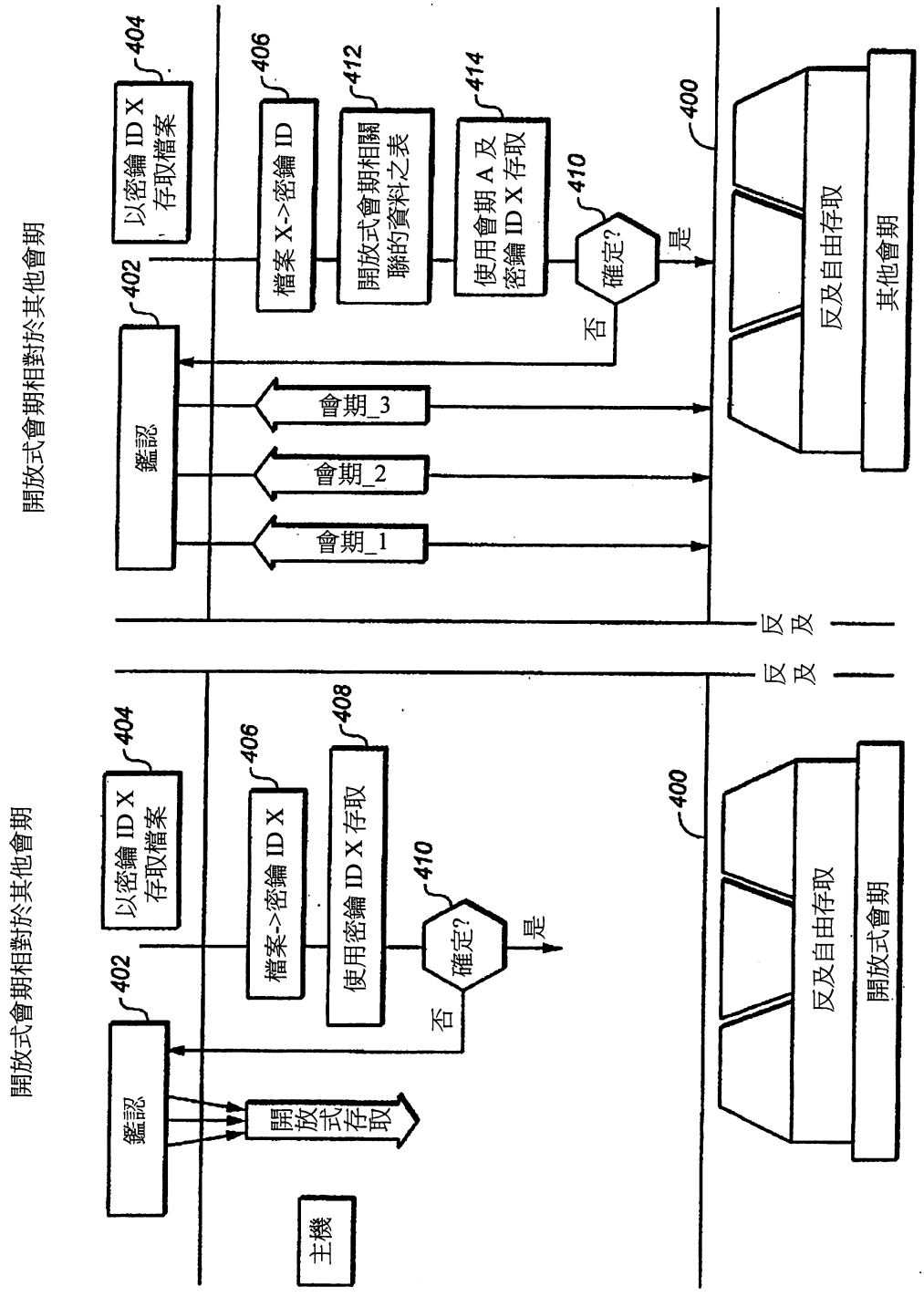
開放式會期相對於其他會期
主機
鑑認
開放式存取
以密鑰 ID X 存取檔案
404
檔案->密鑰 ID X
406
使用密鑰 ID X 存取
408
確定?
410
否
是
400
反及自由存取
開放式會期
開放式會期相對於其他會期
鑑認
402
以密鑰 ID X 存取檔案
404
檔案 X->密鑰 ID
406
開放式會期相關聯的資料之表
412
使用會期 A 及密鑰 ID X 存取
414
確定?
410
否
是
會期_3
會期_2
會期_1
400
反及自由存取
其他會期

圖 17A

圖 17B

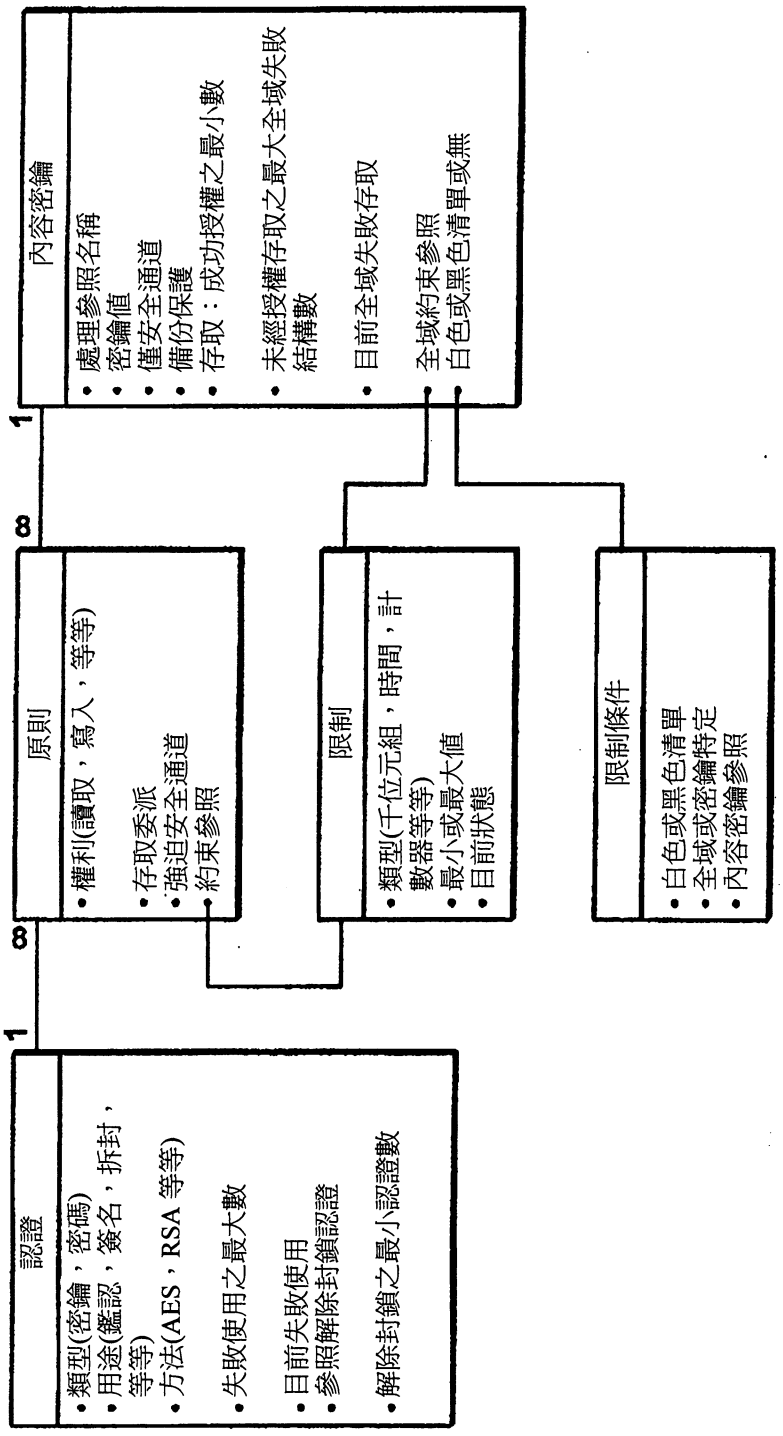
認證
• 類型(密鑰，密碼)
• 用途(鑑認，簽名，拆封，等等)
• 方法(AES，RSA 等等)
• 失敗使用之最大數
• 目前失敗使用
• 參照解除封鎖認證
• 解除封鎖之最小認證數
原則
• 權利(讀取，寫入，等等)
• 存取委派
• 強迫安全通道
• 約束參照
限制
• 類型(千位元組，時間，計數器等等)
• 最小或最大值
• 目前狀態
限制條件
• 白色或黑色清單
• 全域或密鑰特定
• 內容密鑰參照
內容密鑰
• 處理參照名稱
• 密鑰值
• 僅安全通道
• 備份保護
• 存取：成功授權之最小數
• 未經授權存取之最大全域失敗結構數
• 目前全域失敗存取
全域約束參照
白色或黑色清單或無
1
8
8
1

圖 18

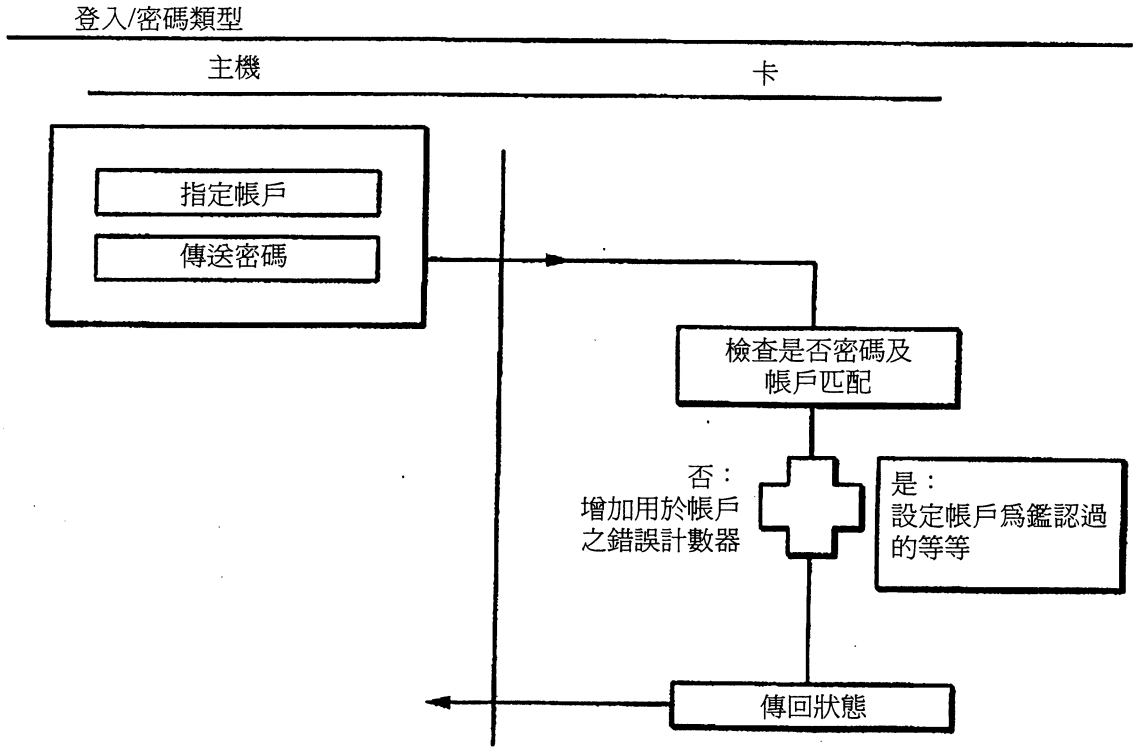
登入/密碼類型
主機
卡
指定帳戶
傳送密碼
檢查是否密碼及
帳戶匹配
否：
增加用於帳戶
之錯誤計數器
是：
設定帳戶爲鑑認過
的等等
傳回狀態

圖 19

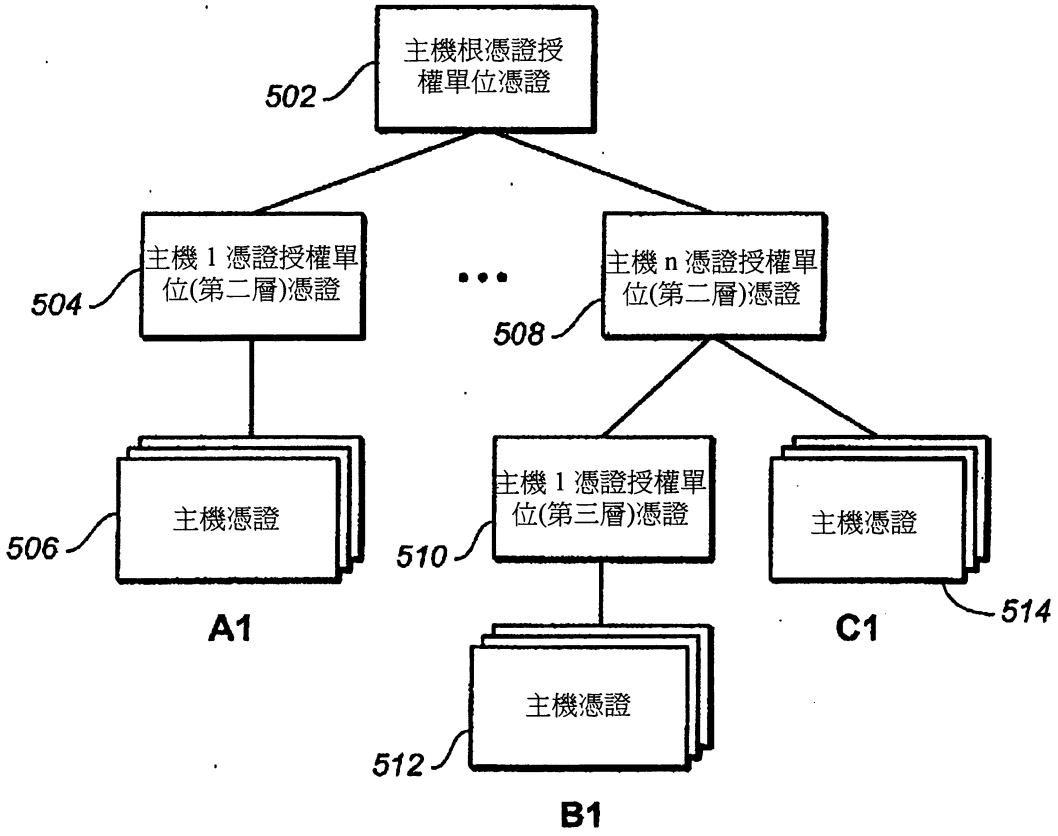
主機根憑證授權單位憑證
502
主機 1 憑證授權單位(第二層)憑證
504
主機 n 憑證授權單位(第二層)憑證
508
主機憑證
506
A1
主機 1 憑證授權單位(第三層)憑證
510
主機憑證
514
C1
主機憑證
512
B1

圖 20

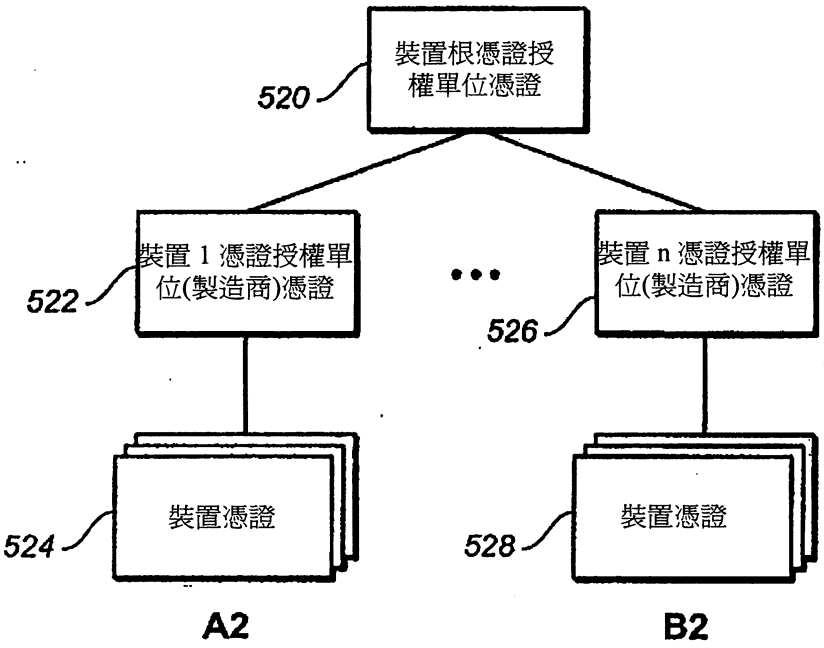
裝置根憑證授權單位憑證
520
裝置 1 憑證授權單位(製造商)憑證
522
裝置 n 憑證授權單位(製造商)憑證
526
裝置憑證
524
A2
裝置憑證
528
B2

圖 21

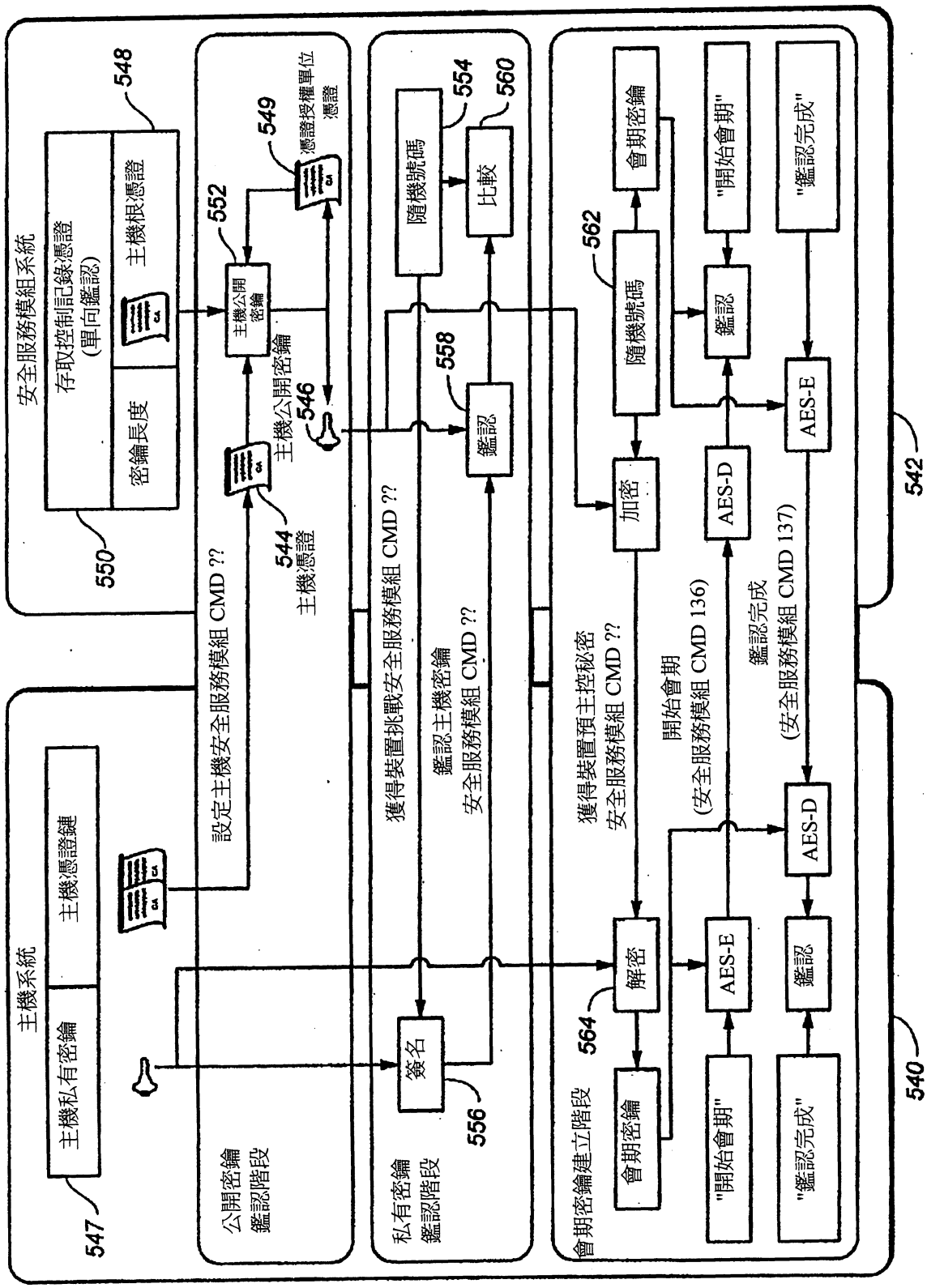
主機系統
主機私有密鑰
主機憑證鏈
547
公開密鑰
鑑認階段
設定主機安全服務模組 CMD ??
安全服務模組系統
存取控制記錄憑證
(單向鑑認)
密鑰長度
主機根憑證
550
548
主機公開
密鑰
552
主機公開密鑰
546
主機憑證
544
憑證授權單位
憑證
549
私有密鑰
鑑認階段
簽名
556
獲得裝置挑戰安全服務模組 CMD ??
鑑認主機密鑰
安全服務模組 CMD ??
鑑認
558
隨機號碼
554
比較
560
會期密鑰建立階段
獲得裝置預主控秘密
安全服務模組 CMD ??
564
解密
加密
562
隨機號碼
會期密鑰
開始會期
(安全服務模組 CMD 136)
鑑認完成
(安全服務模組 CMD 137)
AES-E
AES-D
AES-D
AES-E
鑑認
鑑認
"開始會期"
"鑑認完成"
"開始會期"
"鑑認完成"
540
542

圖 22

圖 23

圖 23A

圖 23B

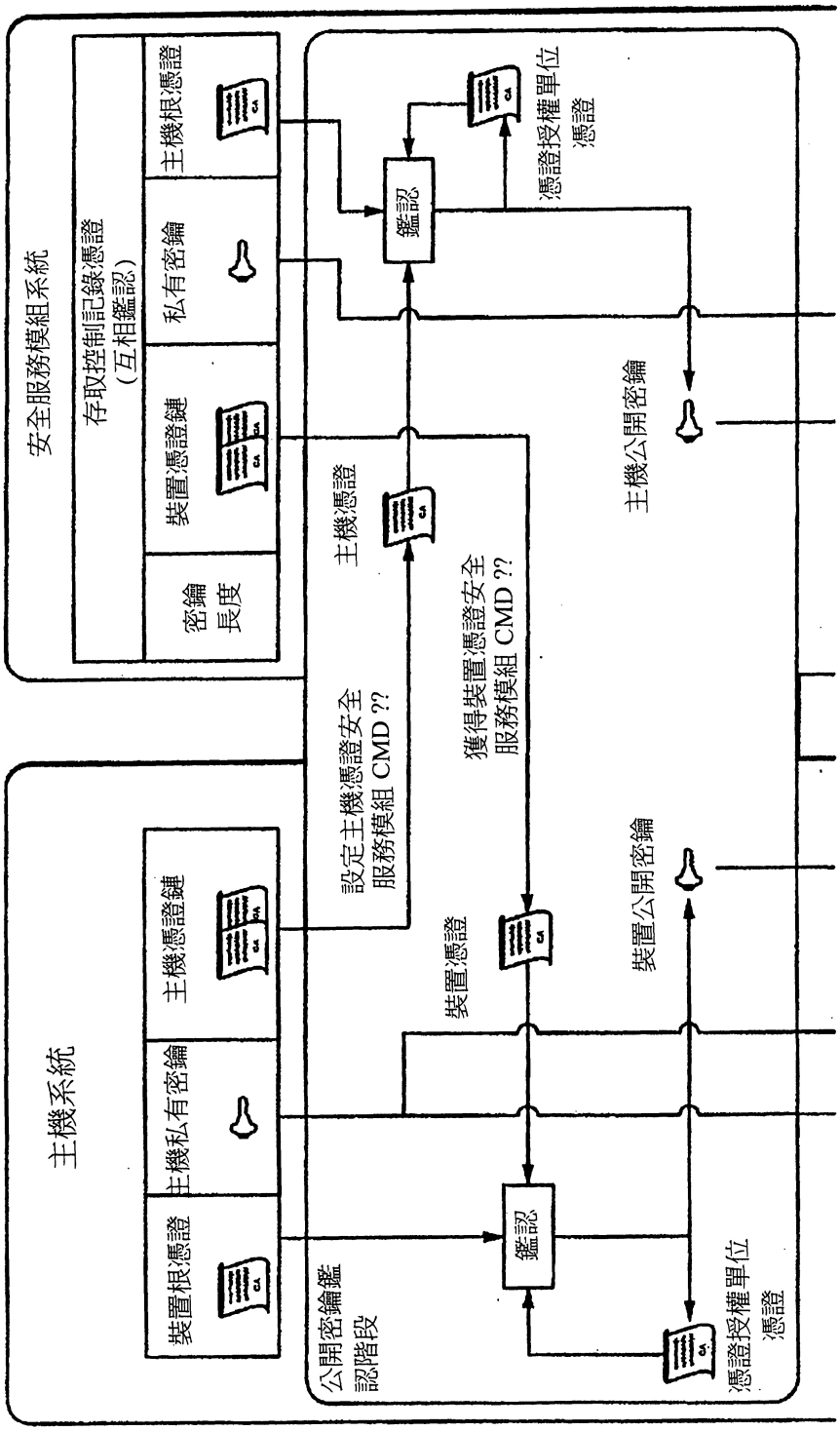


圖 23A

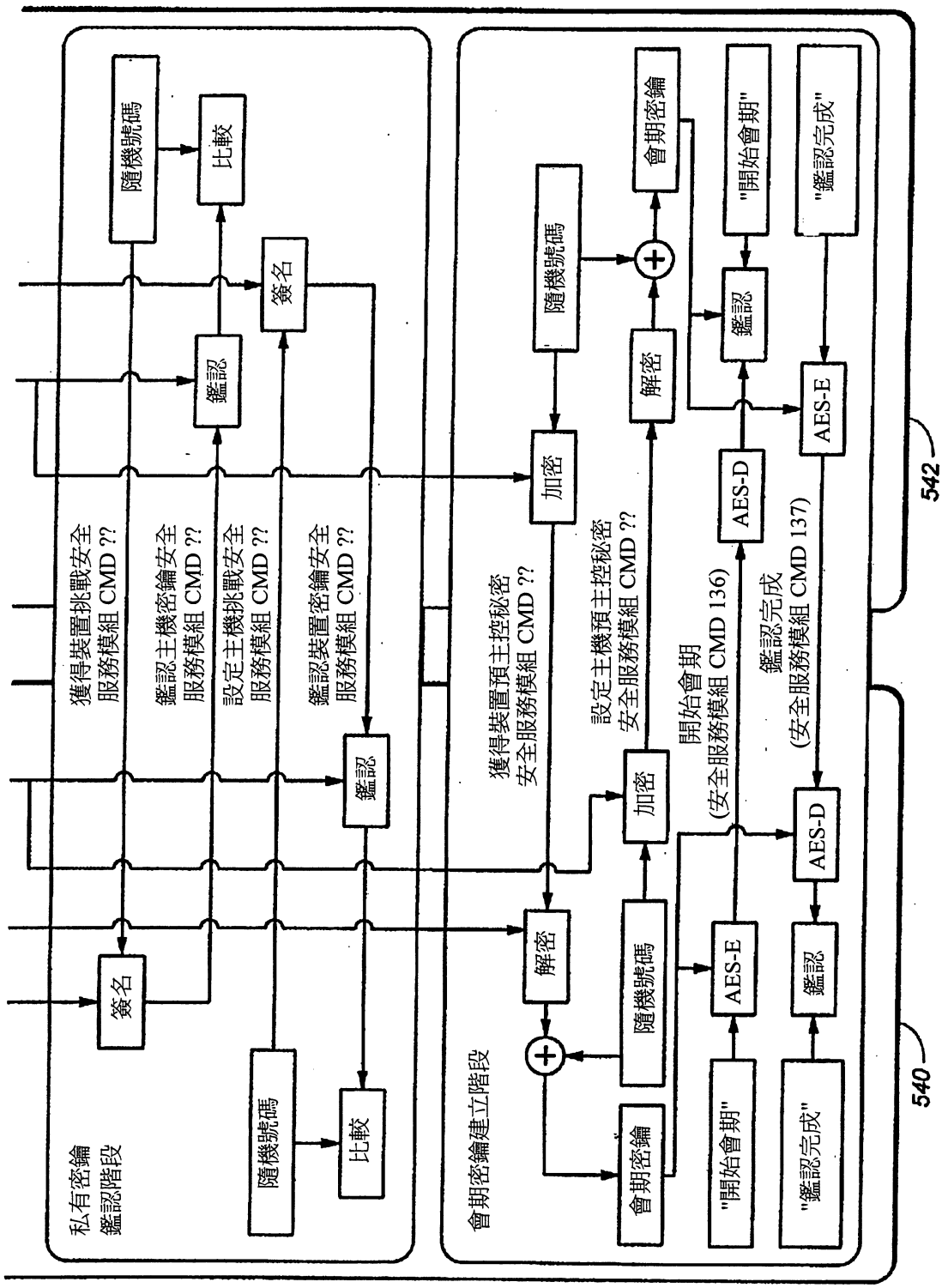
私有密鑰
鑑認階段
獲得裝置挑戰安全
服務模組 CMD ??
鑑認主機密鑰安全
服務模組 CMD ??
設定主機挑戰安全
服務模組 CMD ??
鑑認裝置密鑰安全
服務模組 CMD ??
隨機號碼
比較
簽名
鑑認
隨機號碼
比較
簽名
鑑認
會期密鑰建立階段
獲得裝置預主控秘密
安全服務模組 CMD ??
設定主機預主控秘密
安全服務模組 CMD ??
開始會期
(安全服務模組 CMD 136)
鑑認完成
(安全服務模組 CMD 137)
隨機號碼
加密
解密
會期密鑰
隨機號碼
加密
解密
會期密鑰
AES-E
AES-D
AES-E
AES-D
鑑認
鑑認
"開始會期"
"鑑認完成"
"開始會期"
"鑑認完成"
540
542

圖 23B

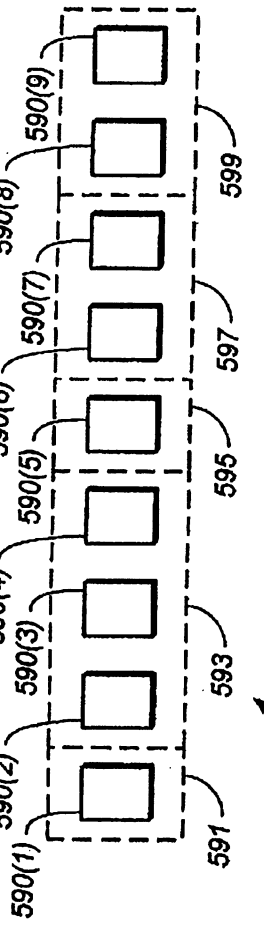


圖 24

| 位元組偏移 | 引數長度 | 引數名稱 | 引數類型 | 注解 |
|---|---|---|---|---|
| 0-1 | 2 | 以位元組爲單位之憑證大小 | 整數 | 以位元組爲單位之憑證密鑰長度 |
| 2 | 1 | "爲最後的" 旗標 | 離散的 | 此旗 標係指示是否於憑證鏈內之目前憑證係爲最後一個 |

圖 25

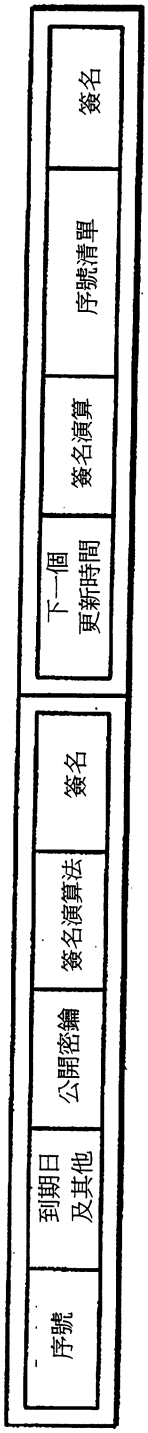


圖 32

憑證鏈卡
(卡鑑認主機)

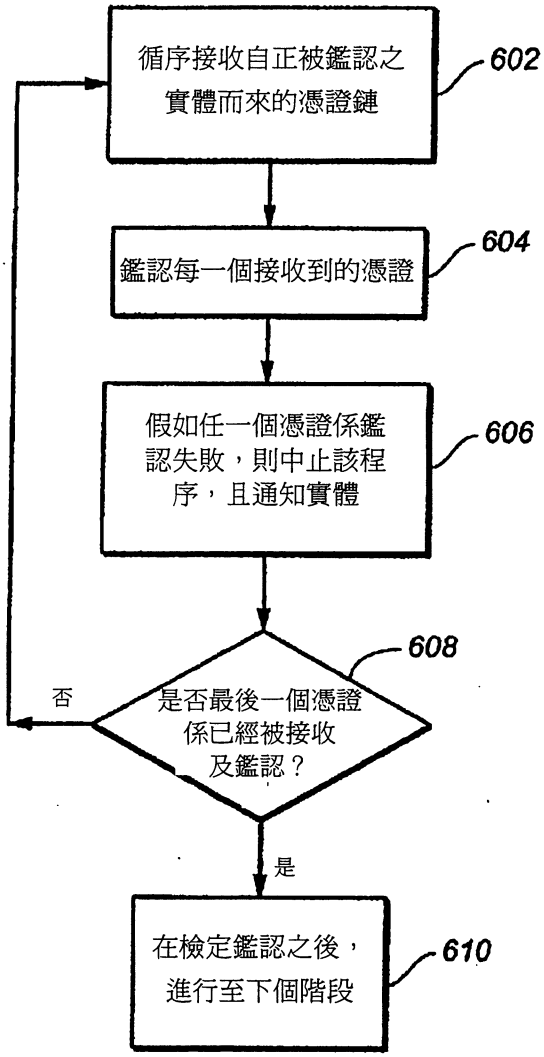


圖 26

憑證鏈主機
(卡鑑認主機)

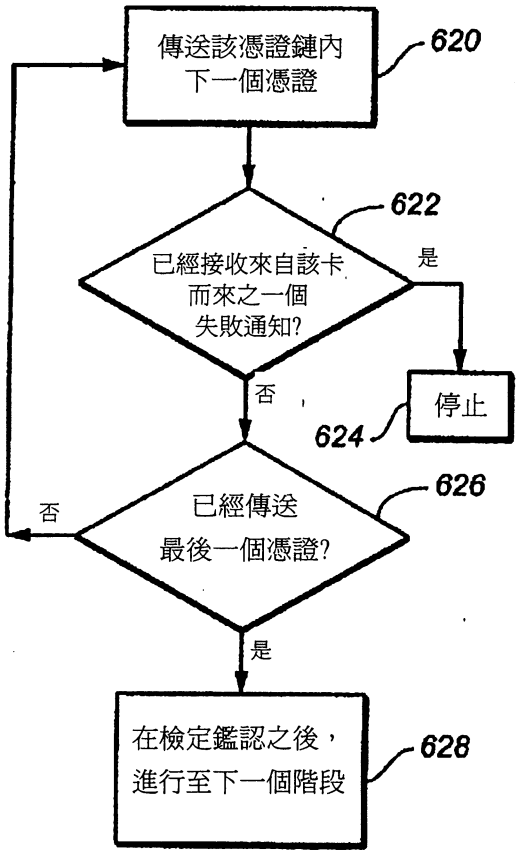


圖 27

憑證鏈卡動作
(主機鑑認卡)

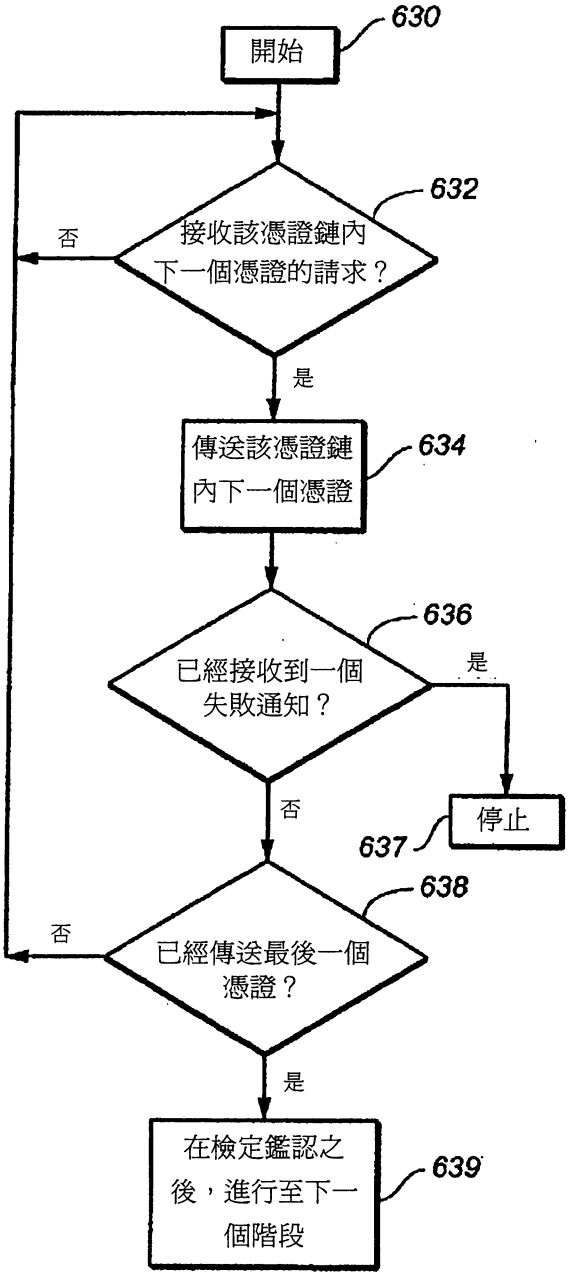


圖 28

憑證鏈主機
(主機鑑認卡)

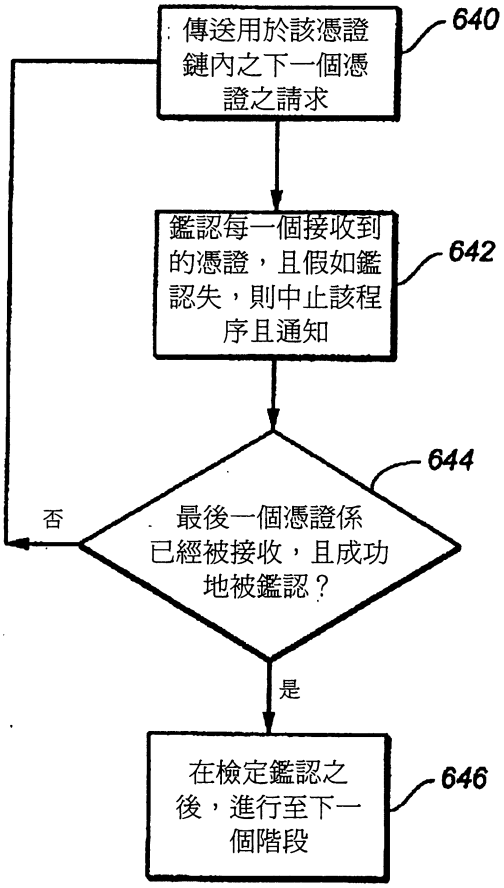


圖 29

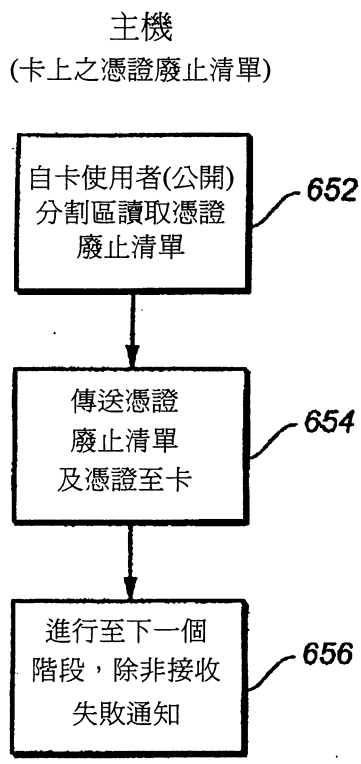
主機
(卡上之憑證廢止清單)
自卡使用者(公開)分割區讀取憑證廢止清單
652
傳送憑證廢止清單及憑證至卡
654
進行至下一個階段，除非接收失敗通知
656

圖 30

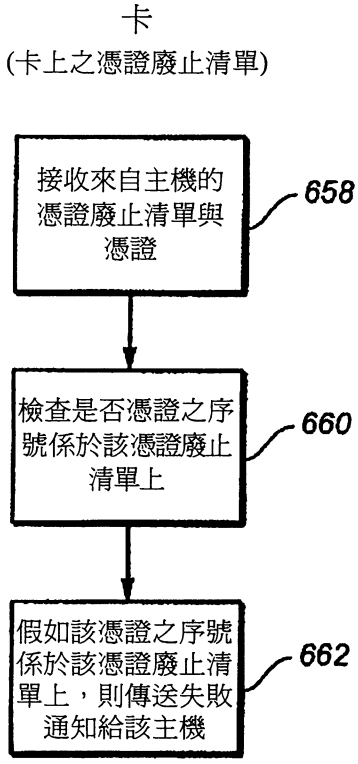
卡
(卡上之憑證廢止清單)
接收來自主機的憑證廢止清單與憑證
658
檢查是否憑證之序號係於該憑證廢止清單上
660
假如該憑證之序號係於該憑證廢止清單上，則傳送失敗通知給該主機
662

圖 31

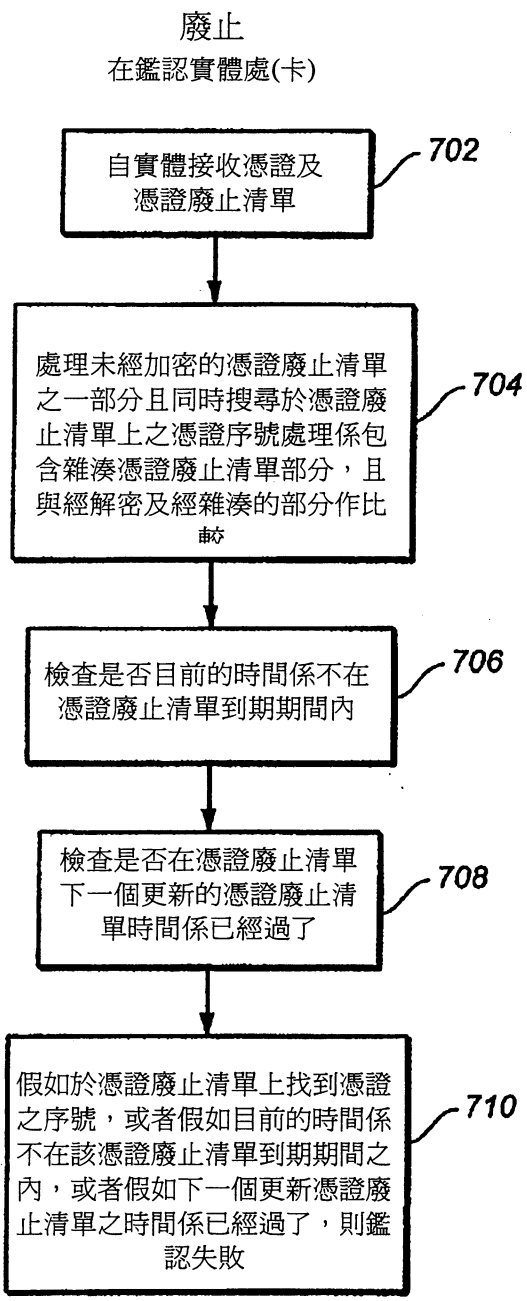
廢止
在鑑認實體處(卡)
自實體接收憑證及憑證廢止清單
702
處理未經加密的憑證廢止清單之一部分且同時搜尋於憑證廢止清單上之憑證序號處理係包含雜湊憑證廢止清單部分，且與經解密及經雜湊的部分作比較
704
檢查是否目前的時間係不在憑證廢止清單到期期間內
706
檢查是否在憑證廢止清單下一個更新的憑證廢止清單時間係已經過了
708
假如於憑證廢止清單上找到憑證之序號，或者假如目前的時間係不在該憑證廢止清單到期期間之內，或者假如下一個更新憑證廢止清單之時間係已經過了，則鑑認失敗
710

圖 33

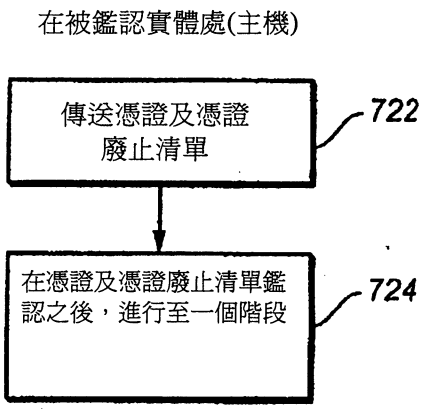
在被鑑認實體處(主機)
傳送憑證及憑證廢止清單
722
在憑證及憑證廢止清單鑑認之後，進行至一個階段
724

圖 34

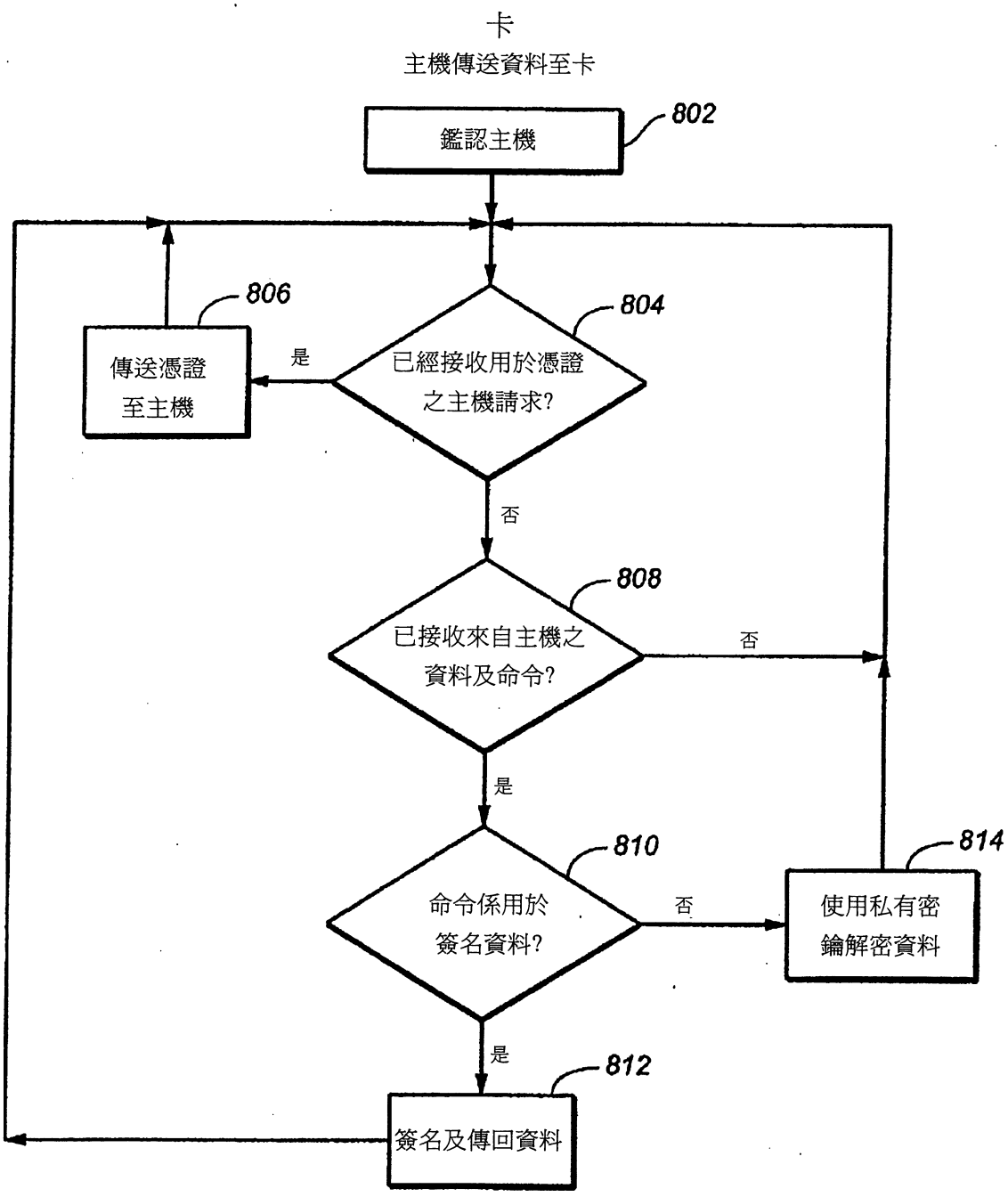
卡
主機傳送資料至卡
鑑認主機
802
已經接收用於憑證之主機請求?
804
是
傳送憑證至主機
806
否
已接收來自主機之資料及命令?
808
否
是
命令係用於簽名資料?
810
否
使用私有密鑰解密資料
814
是
簽名及傳回資料
812

圖 35

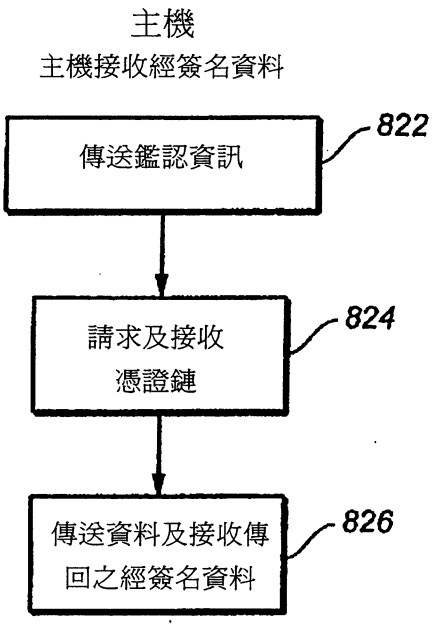
主機
主機接收經簽名資料
傳送鑑認資訊
822
請求及接收
憑證鏈
824
傳送資料及接收傳
回之經簽名資料
826

圖 36

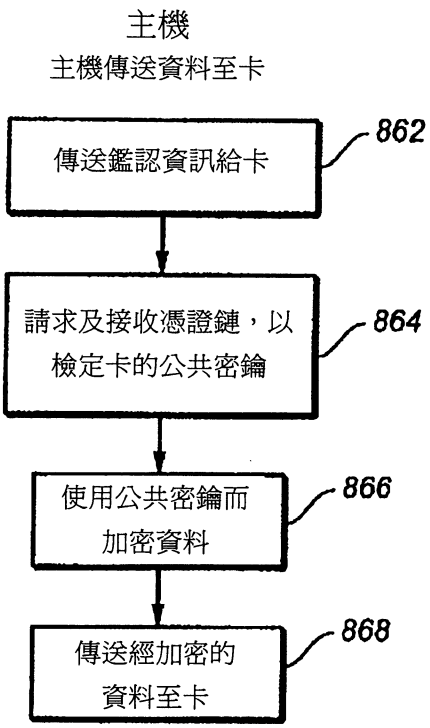
主機
主機傳送資料至卡
傳送鑑認資訊給卡
862
請求及接收憑證鏈，以
檢定卡的公共密鑰
864
使用公共密鑰而
加密資料
866
傳送經加密的
資料至卡
868

圖 37

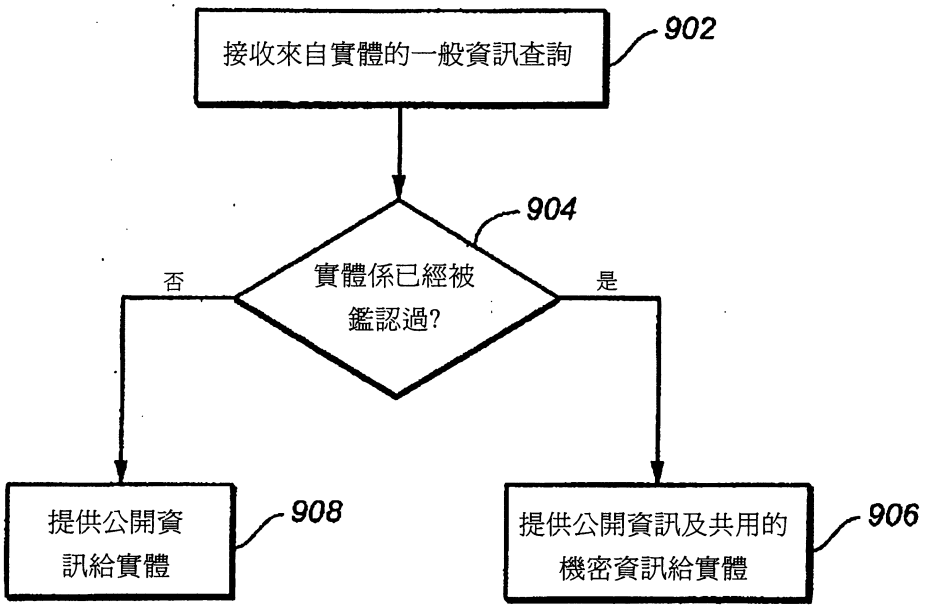
接收來自實體的一般資訊查詢
902
904
實體係已經被鑑認過?
否
是
提供公開資訊給實體
908
提供公開資訊及共用的機密資訊給實體
906

圖 38

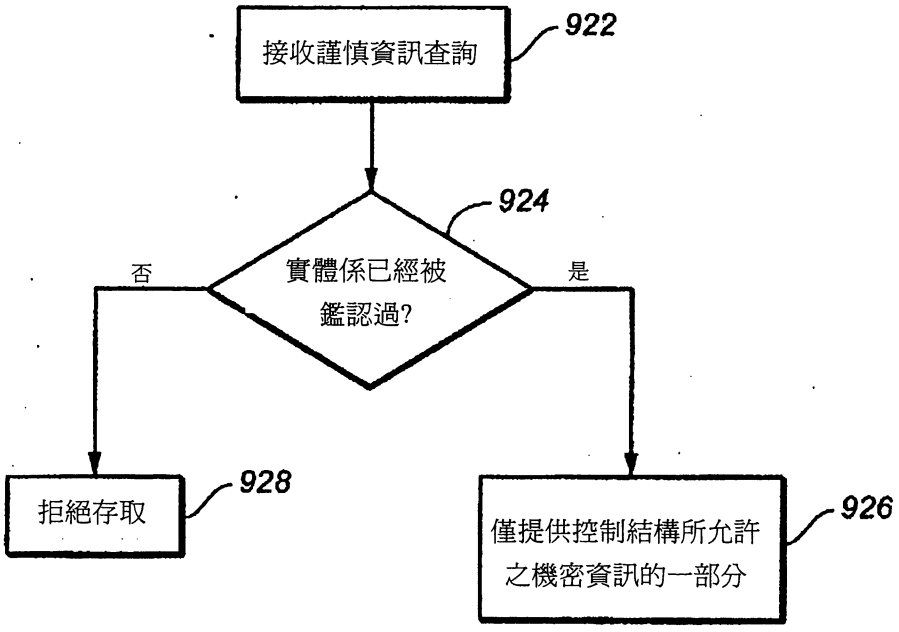
接收謹慎資訊查詢
922
924
實體係已經被鑑認過?
否
是
拒絕存取
928
僅提供控制結構所允許之機密資訊的一部分
926

圖 39

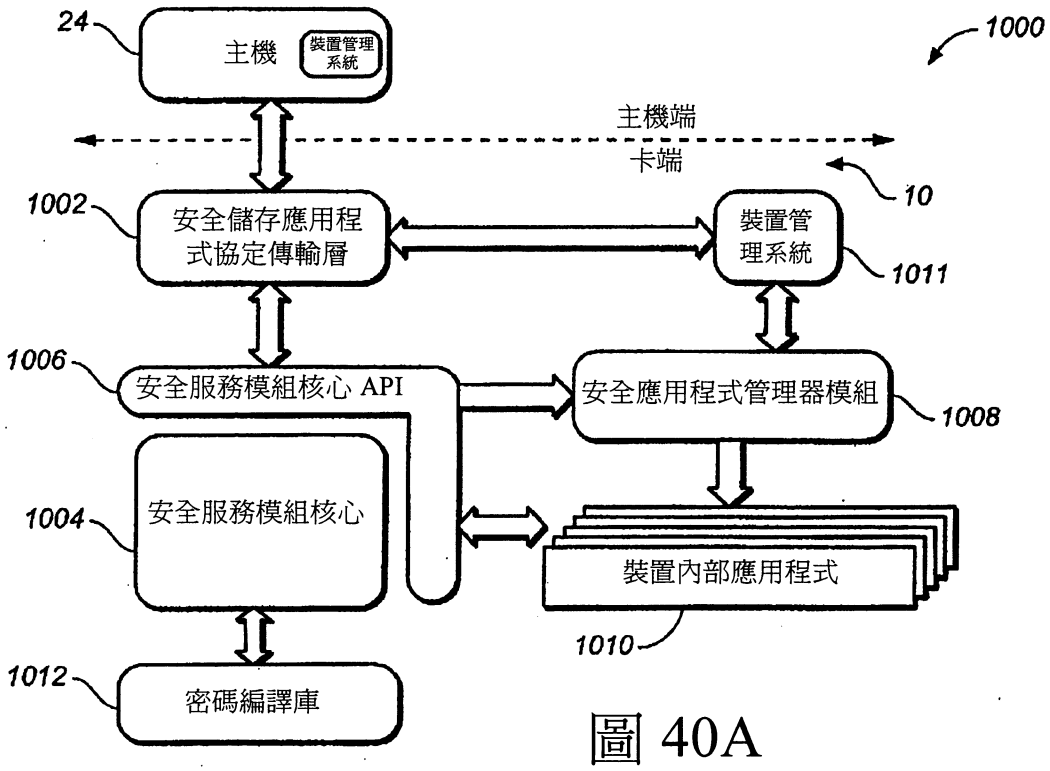
24
主機
裝置管理系統
1000
主機端
卡端
10
1002
安全儲存應用程式協定傳輸層
裝置管理系統
1011
1006
安全服務模組核心 API
安全應用程式管理器模組
1008
1004
安全服務模組核心
裝置內部應用程式
1010
1012
密碼編譯庫

圖 40A

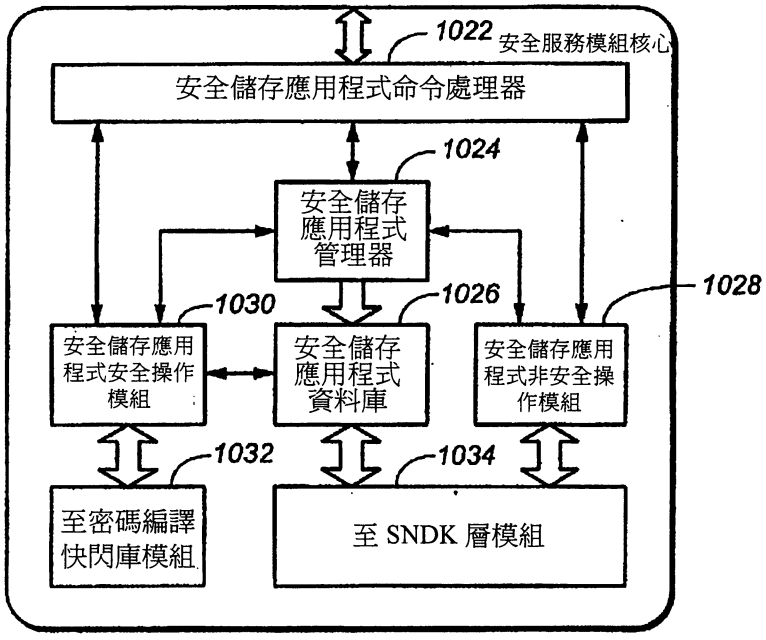
1022
安全服務模組核心
安全儲存應用程式命令處理器
1024
安全儲存應用程式管理器
1030
1026
1028
安全儲存應用程式安全操作模組
安全儲存應用程式資料庫
安全儲存應用程式非安全操作模組
1032
1034
至密碼編譯快閃庫模組
至 SNDK 層模組

圖 40B

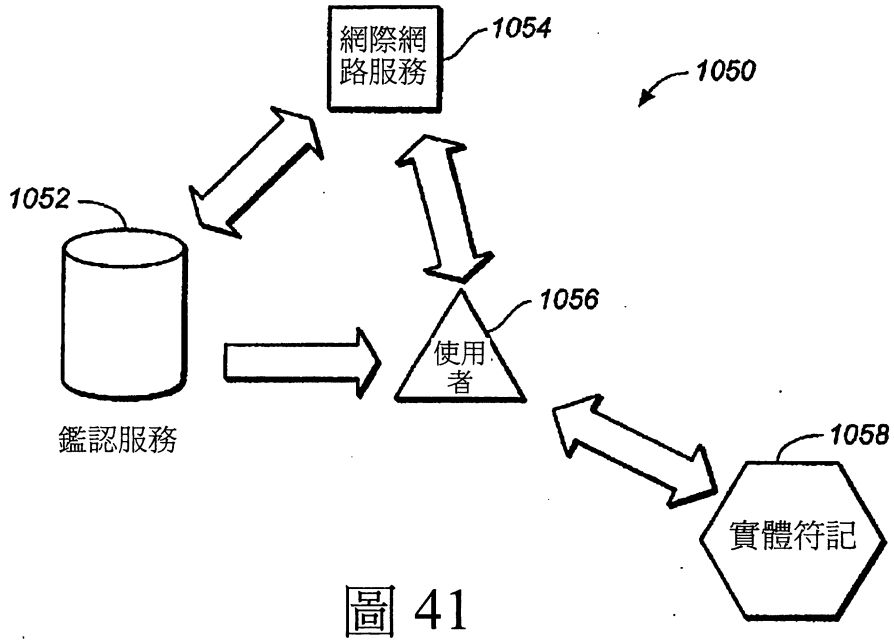
網際網路服務
1054
1050
1052
1056
使用者
鑑認服務
1058
實體符記

圖 41

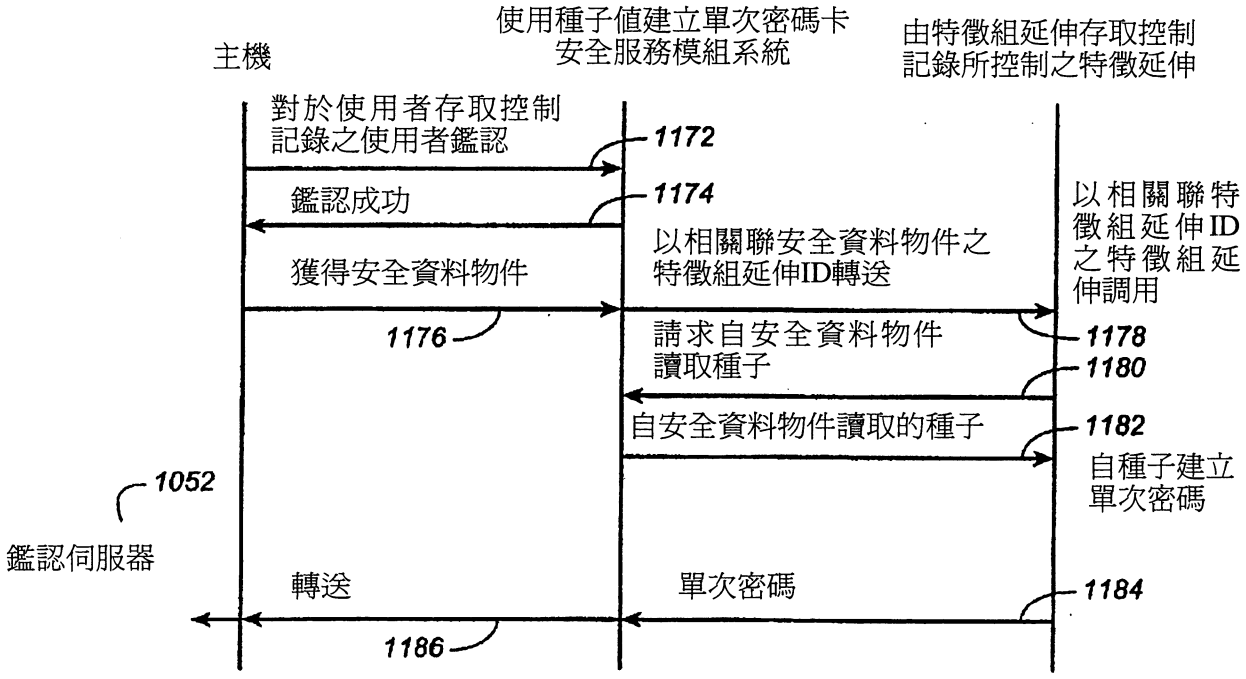
主機
使用種子值建立單次密碼卡安全服務模組系統
由特徵組延伸存取控制記錄所控制之特徵延伸
對於使用者存取控制記錄之使用者鑑認
1172
鑑認成功
1174
以相關聯特徵組延伸ID之特徵組延伸調用
以相關聯安全資料物件之特徵組延伸ID轉送
獲得安全資料物件
1176
請求自安全資料物件讀取種子
1178
1180
自安全資料物件讀取的種子
1182
自種子建立單次密碼
1052
鑑認伺服器
轉送
單次密碼
1184
1186

圖 44

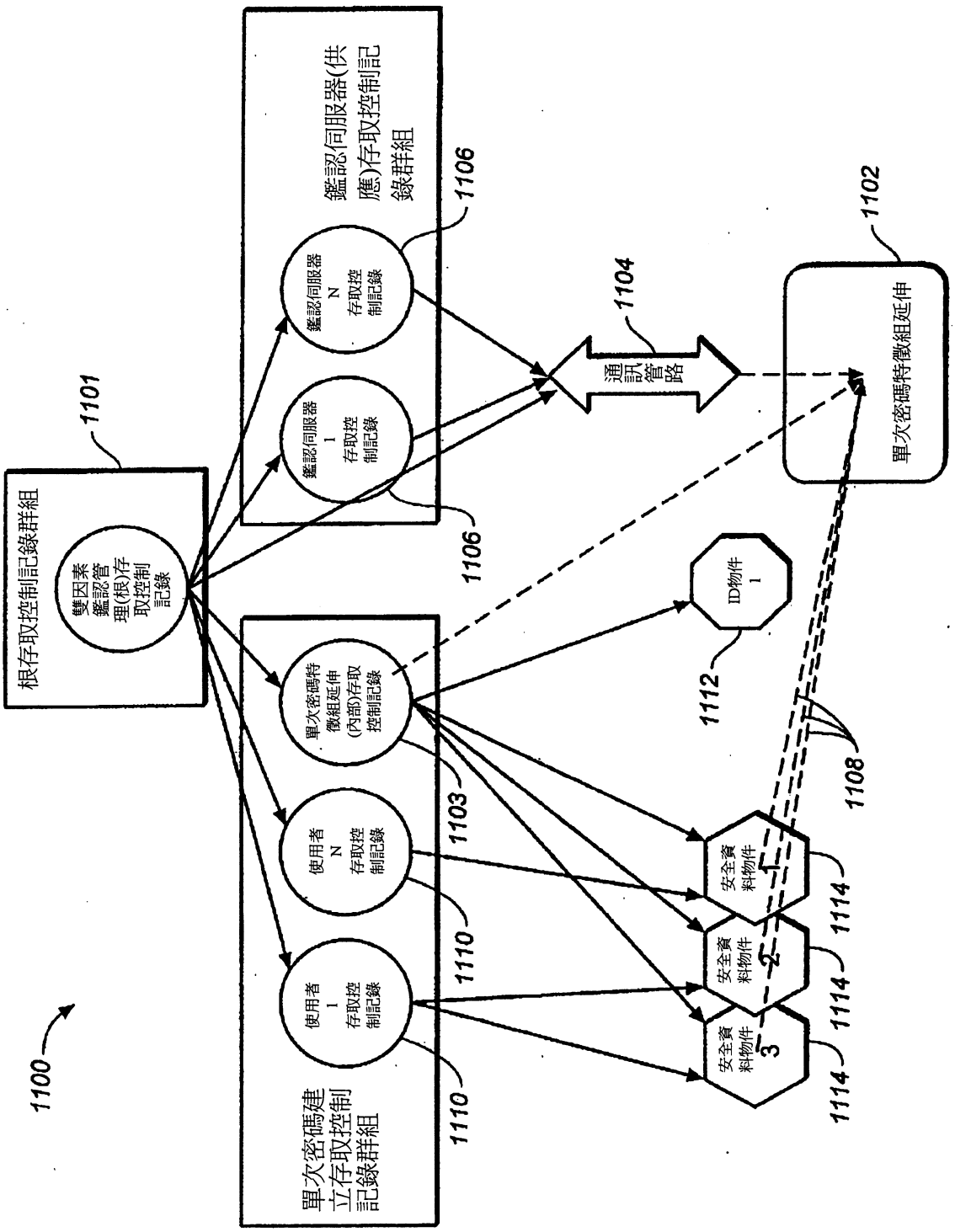
根存取控制記錄群組
雙因素鑑認管理(根)存取控制記錄
1101
鑑認伺服器(供應)存取控制記錄群組
鑑認伺服器 N 存取控制記錄
鑑認伺服器 1 存取控制記錄
1106
1106
1104
通訊管路
1102
單次密碼特徵組延伸
單次密碼建立存取控制記錄群組
單次密碼特徵組延伸(內部)存取控制記錄
使用者 N 存取控制記錄
使用者 1 存取控制記錄
1103
1110
1110
ID物件 1
1112
安全資料物件 1
安全資料物件 2
安全資料物件 3
1108
1114
1114
1114
1100

圖 42

種子供應

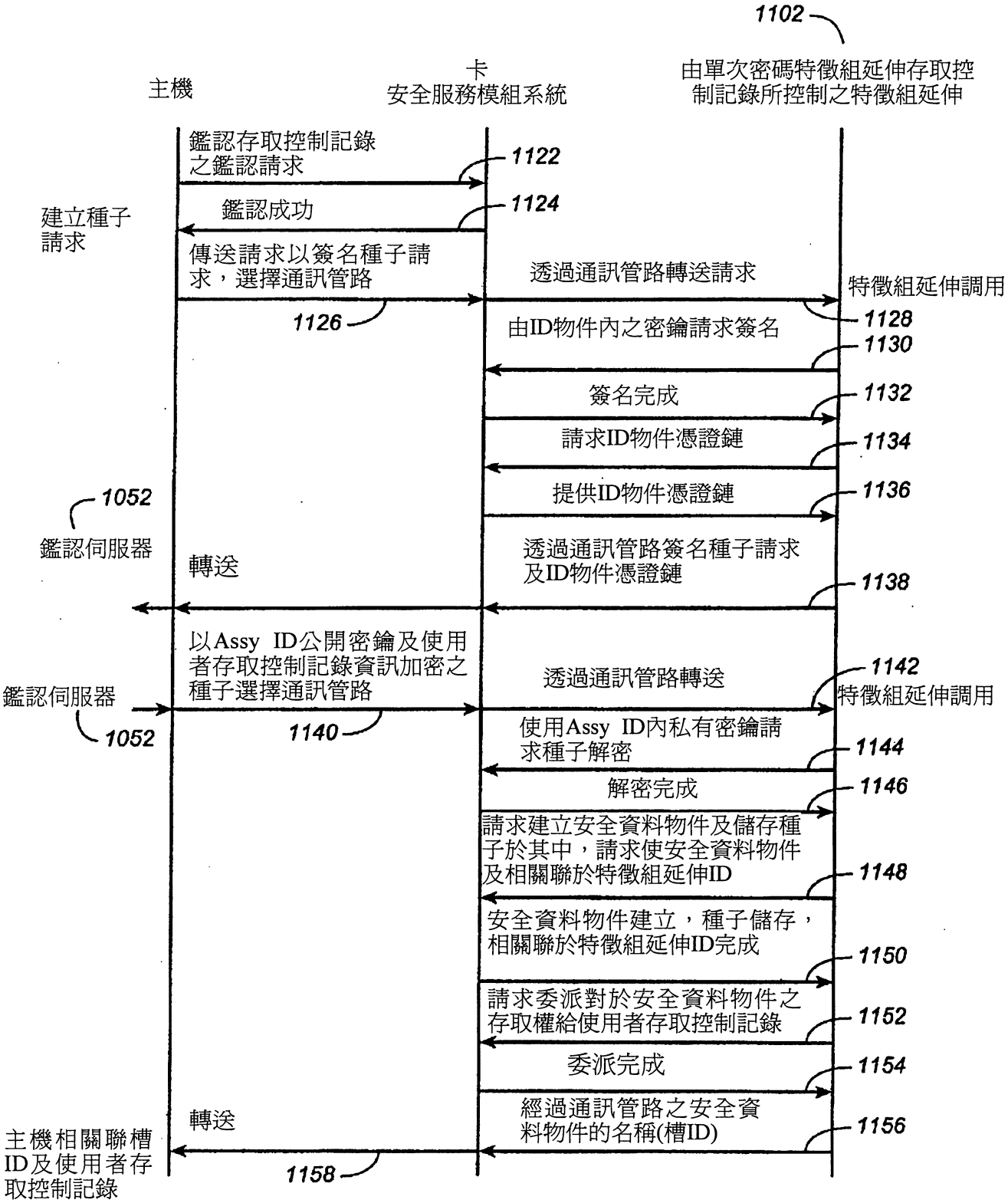
1102
主機
卡
安全服務模組系統
由單次密碼特徵組延伸存取控制記錄所控制之特徵組延伸
鑑認存取控制記錄之鑑認請求
1122
鑑認成功
1124
建立種子請求
傳送請求以簽名種子請求，選擇通訊管路
透過通訊管路轉送請求
特徵組延伸調用
1126
1128
由ID物件內之密鑰請求簽名
1130
簽名完成
1132
請求ID物件憑證鏈
1134
提供ID物件憑證鏈
1136
1052
鑑認伺服器
轉送
透過通訊管路簽名種子請求及ID物件憑證鏈
1138
以Assy ID公開密鑰及使用者存取控制記錄資訊加密之種子選擇通訊管路
透過通訊管路轉送
1142
鑑認伺服器
特徵組延伸調用
1052
1140
使用Assy ID內私有密鑰請求種子解密
1144
解密完成
1146
請求建立安全資料物件及儲存種子於其中，請求使安全資料物件及相關聯於特徵組延伸ID
1148
安全資料物件建立，種子儲存，相關聯於特徵組延伸ID完成
1150
請求委派對於安全資料物件之存取權給使用者存取控制記錄
1152
委派完成
1154
經過通訊管路之安全資料物件的名稱(槽ID)
1156
轉送
主機相關聯槽ID及使用者存取控制記錄
1158

圖 43

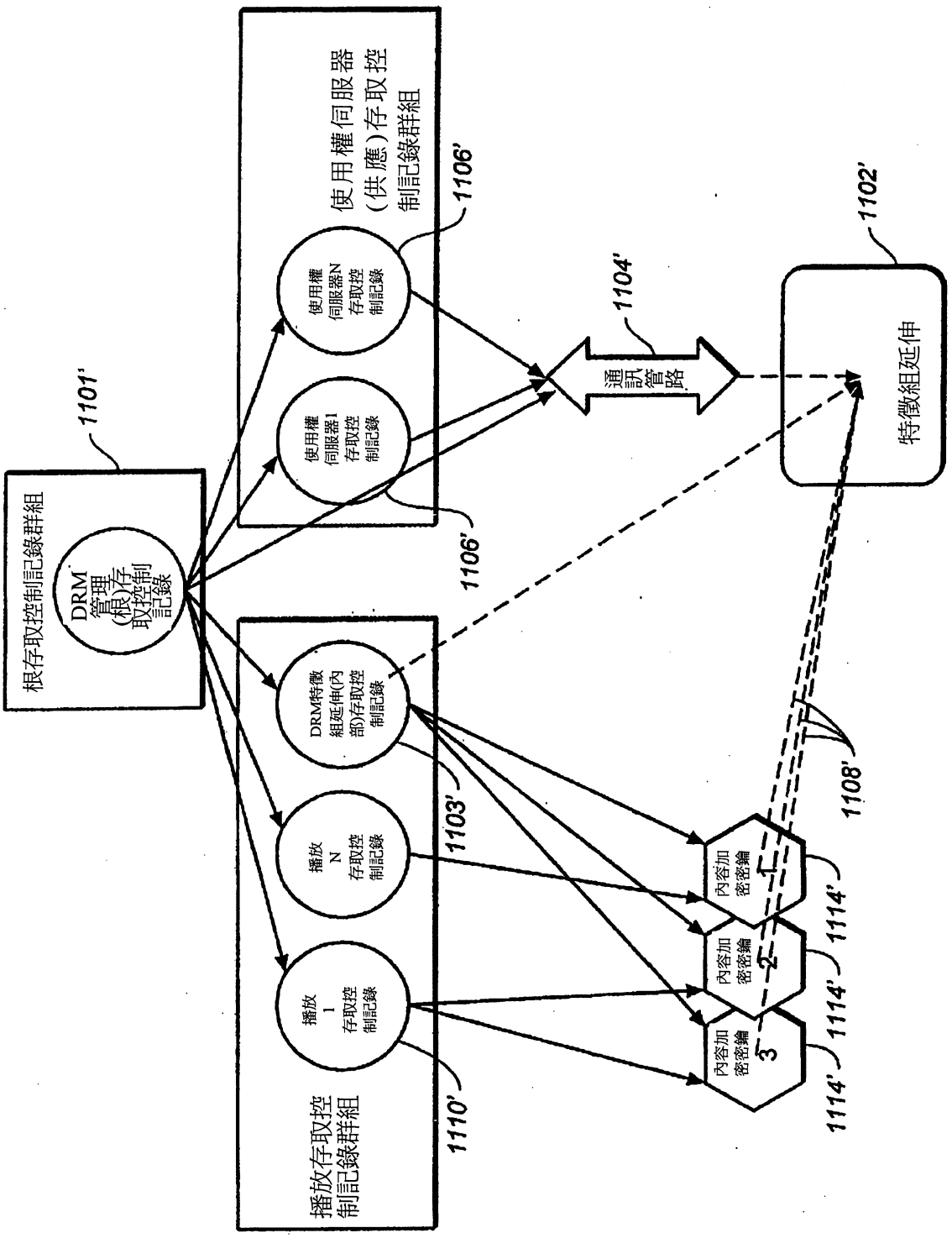
根存取控制記錄群組
DRM管理(根)存取控制記錄
1101'
播放存取控制記錄群組
播放1存取控制記錄
播放N存取控制記錄
DRM特徵組延伸(內部)存取控制記錄
1110'
1103'
使用權伺服器(供應)存取控制記錄群組
使用權伺服器1存取控制記錄
使用權伺服器N存取控制記錄
1106'
1106'
通訊管路
1104'
特徵組延伸
1102'
內容加密密鑰1
內容加密密鑰2
內容加密密鑰3
1114'
1114'
1114'
1108'

圖 45

使用權供應及內容下載，
使用權中之密鑰

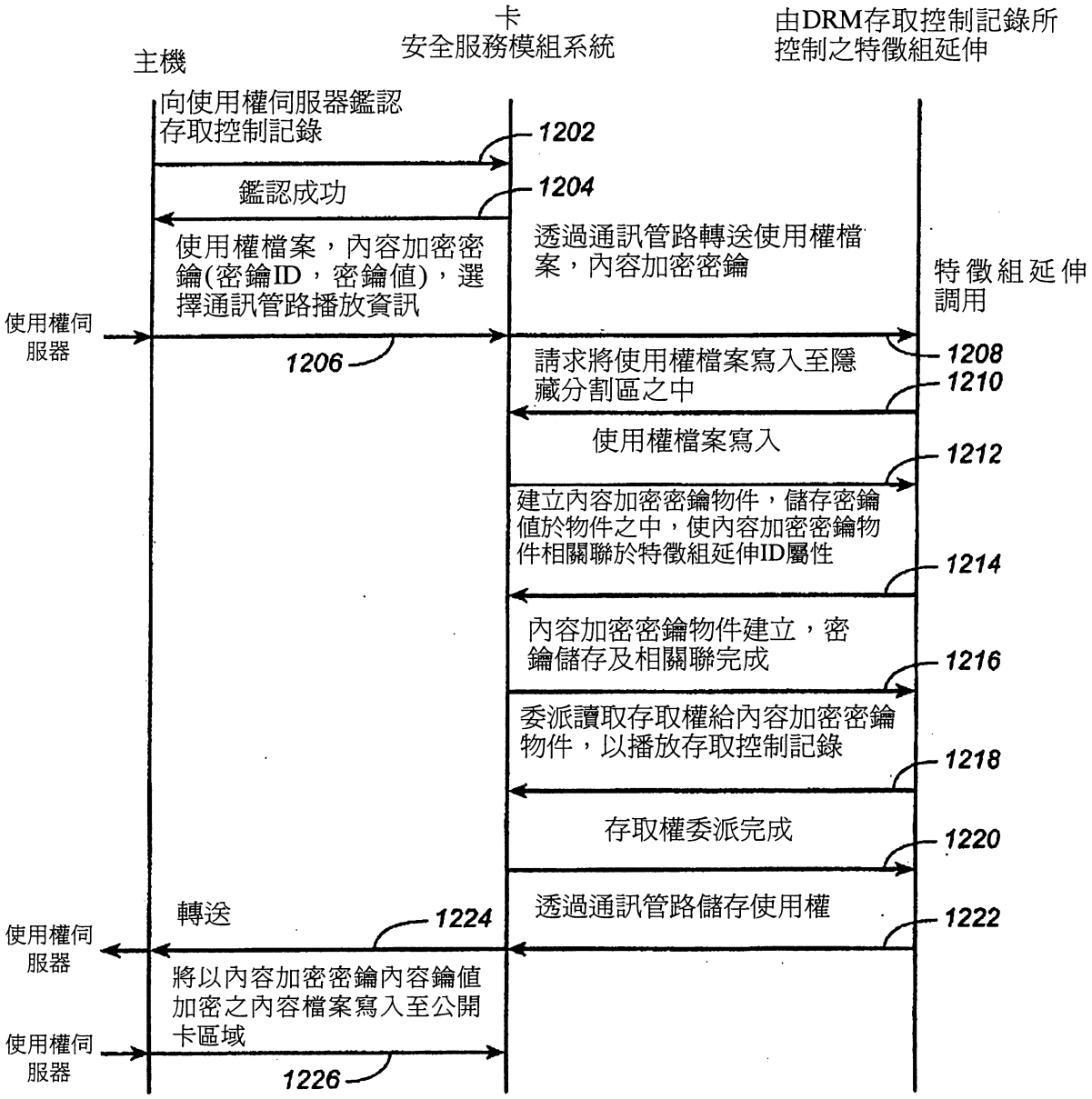


圖 46

播放

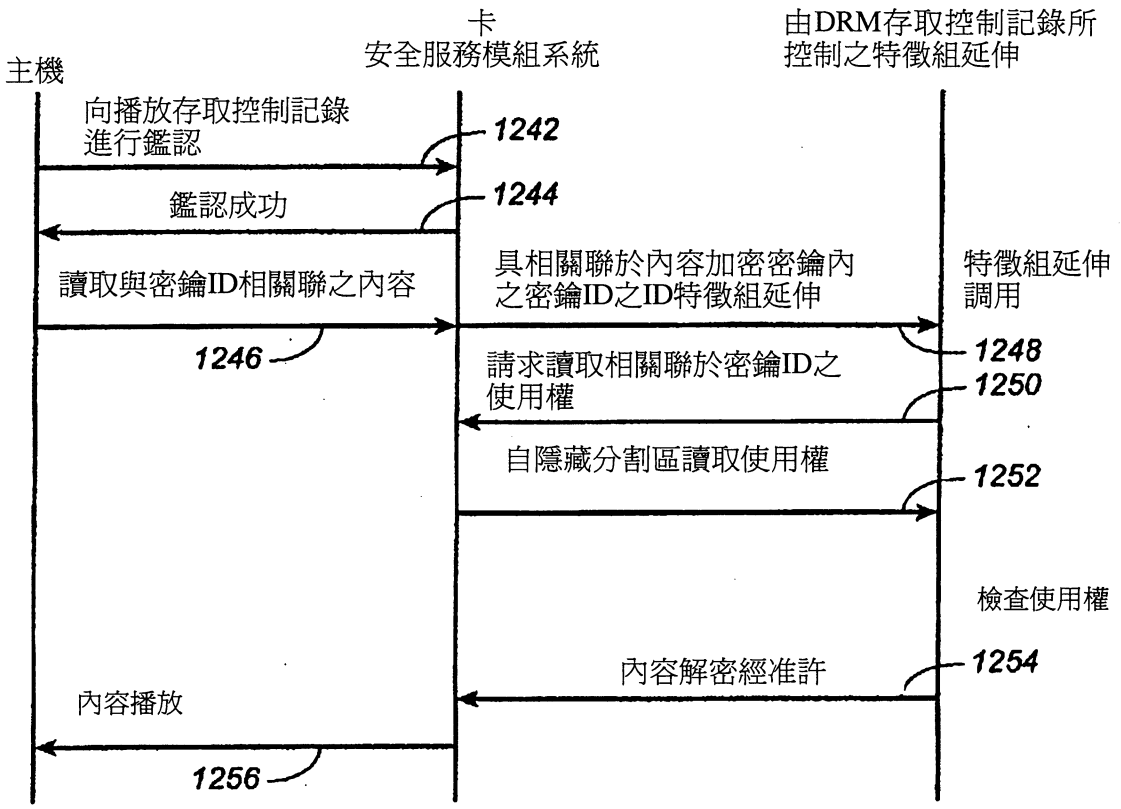
主機
卡
安全服務模組系統
由DRM存取控制記錄所
控制之特徵組延伸
向播放存取控制記錄
進行鑑認
1242
鑑認成功
1244
讀取與密鑰ID相關聯之內容
具相關聯於內容加密密鑰內
之密鑰ID之ID特徵組延伸
特徵組延伸
調用
1246
1248
請求讀取相關聯於密鑰ID之
使用權
1250
自隱藏分割區讀取使用權
1252
檢查使用權
內容解密經准許
1254
內容播放
1256

圖 47

使用權供應及內容下載，
由卡建立密鑰

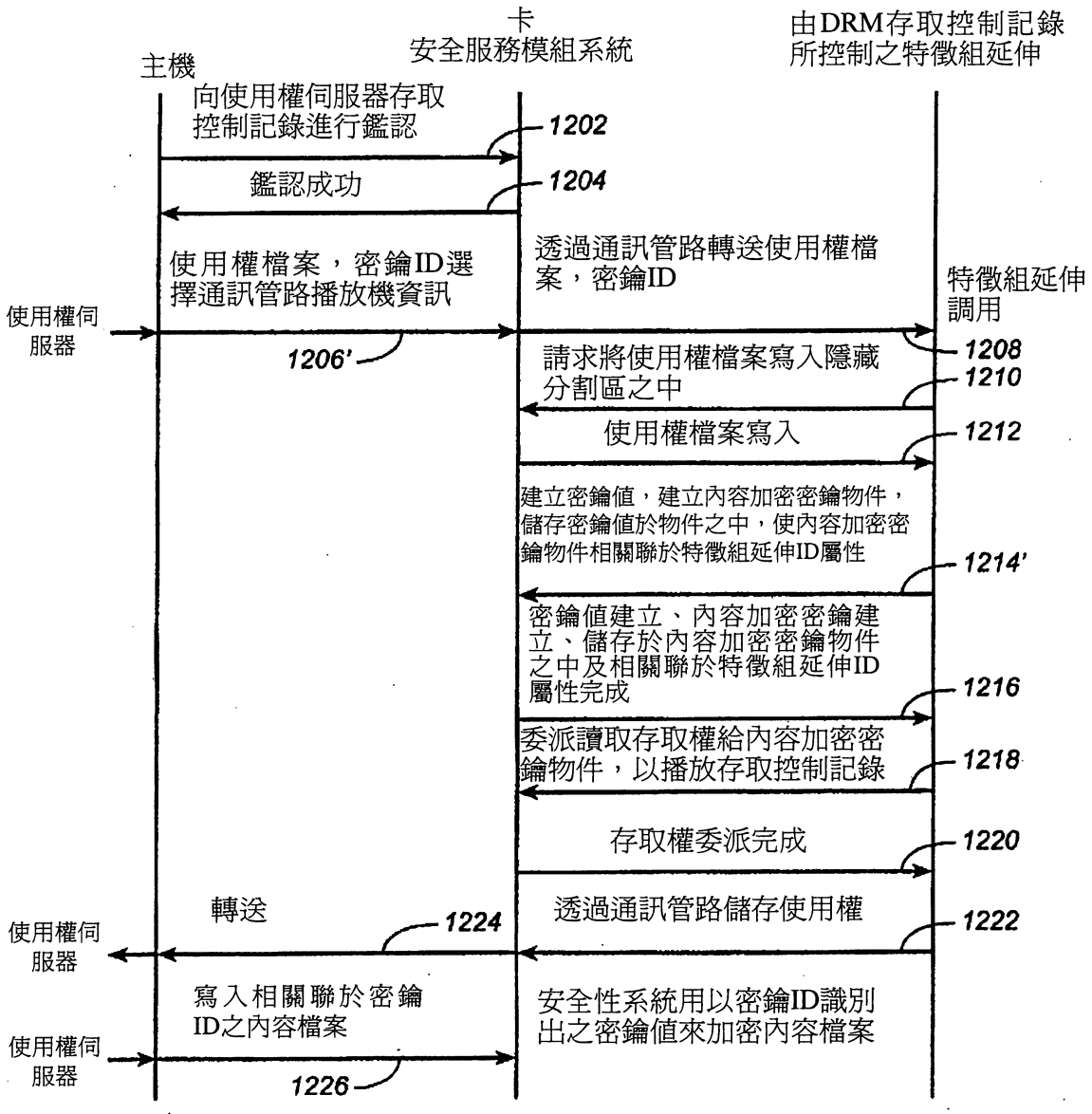


圖 48

## 七、指定代表圖：

(一)本案指定代表圖為：第（ 33 ）圖。

(二)本代表圖之元件符號簡單說明：

(無元件符號說明)

## 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)