(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201017514 A1
(43)公開日： 中華民國 99 (2010) 年 05 月 01 日

(21)申請案號：099101123 (22)申請日： 中華民國 94 (2005) 年 12 月 21 日
(51)Int. Cl.： *G06F3/06 (2006.01)*
(30)優先權：2004/12/21 美國 60/638,804
2005/12/20 美國 11/314,410
2005/12/20 美國 11/314,411
(71)申請人：桑迪士克股份有限公司 (美國) SANDISK CORPORATION (US)
美國
狄斯奎科技公司 (以色列) DISCRETIX TECHNOLOGIES LTD. (IL)
以色列
(72)發明人：喬根得 庫倫巴 菲布利斯 JOGAND-COULOMB, FABRICE (FR)；侯茲曼 邁可 HOLTZMAN, MICHAEL (IL)；卡瓦蜜 巴曼 QAWAMI, BAHMAN (US)；巴利列 羅 BARZILAI, RON (IL)；巴 艾爾 哈吉依 BAR-EL, HAGAI (IL)
(74)代理人：黃章典
申請實體審查：有 申請專利範圍項數：34 項 圖式數：22 共 115 頁

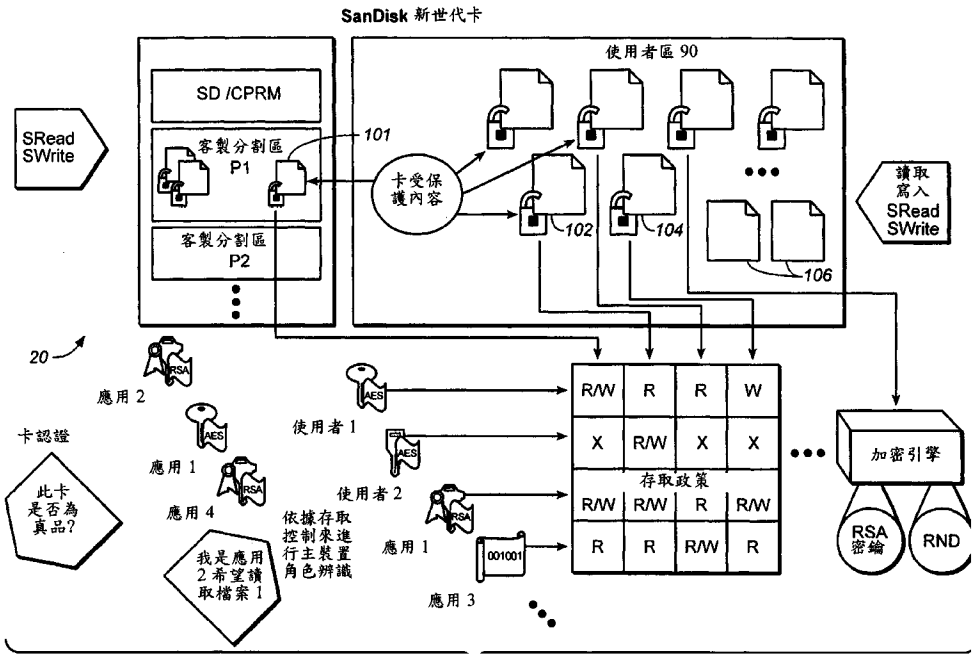
(54)名稱

具多功能內容控制之記憶體系統

MEMORY SYSTEM WITH VERSATILE CONTENT CONTROL

(57)摘要

倘若可將加密-解密密鑰儲存在媒體本身之中且實質上無法由外部裝置來存取的話，那麼私人重要資料的擁有者將可較佳地控制該媒體中已加密內容的存取作業。僅有具正確憑證的主裝置方能存取該密鑰。可儲存一存取政策，其會授予不同的權限(給不同的經授權實體)來存取該媒體中所儲存的資料。兼具上面兩項特點之組合的系統特別有用。就其中一方面來說，內容擁有者能夠利用外部裝置實質上無法存取的密鑰來控制該內容的存取作業；同時，還能夠授予不同的權限來存取該媒體中的內容。因此，即使外部裝置具存取能力，它們的存取動作仍可受到該內容擁有者設定記錄在該儲存媒體中的不同權限的管制。當設計於快閃記憶體中時，上面的特點可針對內容保護產生一特別有用的媒體。當眾多電腦主裝置讀取與寫入以檔案為形式的資料時，眾多儲存裝置並不知悉檔案系統。該主裝置會提供一密鑰參考值或ID，而該記憶體系統則會響應以產生一和該密鑰ID相關聯的密鑰值，讓該記憶體對用於暗碼處理的密鑰值的產生與運用保有完整與獨特的控制能力，同時讓該主機保有對檔案的控制能力。



20：快閃記憶體

101：檔案

102：檔案

104：檔案

106：檔案

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201017514 A1
(43)公開日： 中華民國 99 (2010) 年 05 月 01 日

(21)申請案號：099101123 (22)申請日： 中華民國 94 (2005) 年 12 月 21 日
(51)Int. Cl.： *G06F3/06 (2006.01)*
(30)優先權：2004/12/21 美國 60/638,804
2005/12/20 美國 11/314,410
2005/12/20 美國 11/314,411
(71)申請人：桑迪士克股份有限公司 (美國) SANDISK CORPORATION (US)
美國
狄斯奎科技公司 (以色列) DISCRETIX TECHNOLOGIES LTD. (IL)
以色列
(72)發明人：喬根得 庫倫巴 菲布利斯 JOGAND-COULOMB, FABRICE (FR)；侯茲曼 邁可 HOLTZMAN, MICHAEL (IL)；卡瓦蜜 巴曼 QAWAMI, BAHMAN (US)；巴利列 羅 BARZILAI, RON (IL)；巴 艾爾 哈吉依 BAR-EL, HAGAI (IL)
(74)代理人：黃章典
申請實體審查：有 申請專利範圍項數：34 項 圖式數：22 共 115 頁

(54)名稱

具多功能內容控制之記憶體系統

MEMORY SYSTEM WITH VERSATILE CONTENT CONTROL

(57)摘要

倘若可將加密-解密密鑰儲存在媒體本身之中且實質上無法由外部裝置來存取的話，那麼私人重要資料的擁有者將可較佳地控制該媒體中已加密內容的存取作業。僅有具正確憑證的主裝置方能存取該密鑰。可儲存一存取政策，其會授予不同的權限(給不同的經授權實體)來存取該媒體中所儲存的資料。兼具上面兩項特點之組合的系統特別有用。就其中一方面來說，內容擁有者能夠利用外部裝置實質上無法存取的密鑰來控制該內容的存取作業；同時，還能夠授予不同的權限來存取該媒體中的內容。因此，即使外部裝置具存取能力，它們的存取動作仍可受到該內容擁有者設定記錄在該儲存媒體中的不同權限的管制。當設計於快閃記憶體中時，上面的特點可針對內容保護產生一特別有用的媒體。當眾多電腦主裝置讀取與寫入以檔案為形式的資料時，眾多儲存裝置並不知悉檔案系統。該主裝置會提供一密鑰參考值或ID，而該記憶體系統則會響應以產生一和該密鑰ID相關聯的密鑰值，讓該記憶體對用於暗碼處理的密鑰值的產生與運用保有完整與獨特的控制能力，同時讓該主機保有對檔案的控制能力。

六、發明說明：

【發明所屬之技術領域】

本發明一般和記憶體系統有關，更明確地說，係關於一種具多樣性內容控制特徵的記憶體系統。

【先前技術】

計算裝置的市場正朝著於行動儲存裝置中納入內容儲存器的方向發展，以便進行更多資料交換以提高平均收益。此意謂著，當於計算裝置上使用時，行動儲存媒體中的內容必須受到保護。前述內容包含有價資料，其可能係製造或販售該儲存裝置以外的團體所擁有的資料。

其中一種具有加密功能的儲存裝置已於美國專利案第6,457,126號中作過說明。不過，該裝置所提供的功能相當有限。所以，本案希望提供一種具更多多樣性內容控制特徵的記憶體系統。

【發明內容】

保護行動儲存媒體中的內容可能涉及到對該媒體中的資料進行加密，俾使僅有經授權的使用者或應用方可存取用來加密該媒體中所儲存之資料的密鑰。於部份先前系統中，用來加密與解密資料的密鑰係儲存在該行動儲存媒體外部的裝置中。於此等情況中，於該內容中具有私人重要資料的公司或個人對該媒體中內容的運用上可能不具太多的控制能力。因為用來加密媒體中之資料的密鑰係位於媒體的外部，所以，此密鑰可能會以該內容擁有者無法控制的方式從一裝置傳送至另一裝置。根據本發明其中一項特

點，倘若可將加密-解密密鑰儲存在媒體本身之中且實質上無法由外部裝置來存取的話，那麼私人重要資料的擁有者將可較佳地控制該媒體中之內容的存取作業。

基本上讓該媒體外部無法存取該密鑰，此特點便可讓安全的內容具可攜性。因此，含有經此密鑰加密後之安全內容的儲存裝置便可利用各種主裝置來存取，而不會有危害安全之虞，因為該裝置係唯一可控制該密鑰的裝置。僅有具正確憑證的主裝置方能存取該密鑰。

為提高行動儲存媒體中所儲存之內容的商業價值，吾人會希望該內容中私人重要資料的擁有者能夠授予不同實體不同的權限來存取該內容。所以，本發明的另一項特點便基於可儲存一存取政策以授予不同的權限(給不同的經授權實體)來存取該媒體中所儲存的內容之認知。兼具上面兩項特點之組合的系統特別有用。就其中一方面來說，內容擁有者能夠利用外部裝置實質上無法存取的密鑰來控制該內容的存取作業；同時，還能夠授予不同的權限來存取該媒體中的內容。因此，即使外部裝置具存取能力，它們的存取動作仍可受到該內容擁有者設定記錄在該儲存媒體中的不同權限的管制。

本發明的另一項特點則係當於快閃記憶體系統中設計上述政策授予不同的權限給不同的經授權實體時，可針對內容保護產生一特別有用的媒體。

當眾多電腦主裝置讀取與寫入以檔案為形式的資料時，眾多儲存裝置並不知悉檔案系統。根據另一項特點，主裝

置會提供一密鑰參考值或ID，而記憶體系統則會據之產生一和該密鑰ID相關聯的密鑰值，其中該密鑰值係用來對和該密鑰ID相關聯的檔案中的資料進行暗碼(cryptographic)處理。該主裝置會將該密鑰ID與要被該記憶體系統進行暗碼處理的檔案產生關聯。因此，該計算裝置與記憶體便會利用該密鑰ID來讓該記憶體對用於暗碼處理的密鑰值的產生與運用保有完整與獨特的控制能力，同時讓該主機保有對檔案的控制能力。

於特定行動儲存裝置(如智慧卡)中，卡控制器會管理該檔案系統。於眾多其它類型的行動儲存裝置(如快閃記憶體、磁碟、或光碟)中，裝置控制器並不知悉該檔案系統；取而代之的係，該裝置控制器會依賴一主裝置(舉例來說，個人電腦、數位相機、MP3播放器、個人數位助理、蜂巢式電話)來管理該檔案系統。本發明的各項觀點可輕易地併入此等裝置控制器並不知悉檔案系統的儲存裝置類型之中。此意謂著，本發明的各項特點均可實現於各種既有的行動儲存裝置之中，而無需重新設計此等裝置來讓此等裝置中的裝置控制器知悉且能夠管理該檔案系統。

該儲存媒體中所儲存的樹狀結構可控制某一實體在取得存取權限後可施行何種作業。該樹之中的每個節點均會指定經由此節點進入的實體的權限。某些樹會具有不同的階層，該樹某一節點處的權限或複數權限會與同一樹中較高或較低或相同階層處的另一節點的權限或複數權限具有預設的關係。藉由要求實體符合每個節點處所指定的權限，

本申請案中的樹特徵便可讓內容擁有者控制哪些實體能夠採取動作以及控制每個實體能夠採取何種動作，而不必理會該樹是否具有不同的階層。

為提高行動儲存媒體所能提供的商業價值，吾人會希望行動儲存媒體能夠同時支援一種以上的應用。當有兩個或更多個應用同時在存取該行動儲存媒體時，能否分離該等兩個或更多個應用的作業使得它們不會彼此干擾而產生本文中所謂的串音(crosstalk)現象便非常重要。所以，本發明的另一項特點便係，能夠以階層的方式來提供二或更多樹，以控制該記憶體的存取作業。每樹於不同的階層處包括複數個節點，用以控制一對應實體集的資料存取作業，其中每樹中的某一節點均會指定該或該等對應實體存取記憶體資料的權限或複數權限。每樹中某一節點處的該或該等權限會與同一樹中較高或較低階層處的另一節點處的權限或複數權限具有預設的關係。較佳的係，於該等樹中至少兩棵之間不會有任何的串音。

從上述中可清楚看出，就內容安全性來說，樹狀結構係一種非常好用的結構。其中一種重要的控制能力係控制樹的產生。因此，根據本發明另一項特點，該行動儲存裝置可配備一系統代理(system agent)，該系統代理能夠產生至少一階層樹，其於不同階層處包括複數節點用來控制對應實體對該記憶體中所儲存之資料的存取作業。該樹中的每個節點均會指定一對應實體或複數實體存取記憶體資料的權限或複數權限。每樹中該節點處的該或該等權限均會與

同一樹中較高或較低或相同階層處的複數節點處的權限或複數權限具有預設的關係。因此，該等行動儲存裝置於發行(issued)時可能並未產生任何樹，因此，該等裝置的買者可自行產生階層樹，以適應於該買者心中想要的應用。或者，該等行動儲存裝置於發行時亦可能已產生該等樹，因此，買者便無需經歷產生該等樹的麻煩。於兩種情況中，較佳的係，於該等裝置產生該等樹的特定功能之後，該等功能便不會改變，俾使無法對該等功能作進一步變更或改變。如此便可讓內容擁有者對該裝置中之內容的存取作業具有更大的控制能力。因此，於其中一具體實施例中，較佳的係該系統代理能夠被取消而不會產生任何額外的樹。

於特定行動儲存裝置中，藉由將記憶體分成不同的區域在存取受保護區時則先經過認證，以達內容保護的目的。雖然此特點確實可提供特定的保護能力，不過，卻無法防止透過不正當方式取得密碼(password)的使用者。因此，本發明的另一項觀點係提供一種機制或結構，用來將一記憶體分成複數個分割區且可利用一密鑰來加密該等分割區中的至少特定資料，所以除了需要認證以存取部份該等分割區之外，還需要存取一或多個密鑰方能解密此等分割區中的已加密資料。

於特定應用中，更合宜的方式係，讓使用者能夠利用一應用來登入該記憶體系統，接著其便能夠利用不同的應用來存取受保護的內容而無需再次登入。於此情況中，該使用者希望依此方式來存取的所有內容可能與第一帳號相關

聯，俾使可透過不同的應用(舉例來說，音樂播放器、電子郵件、蜂巢式通信、...等)來存取所有此內容而無需於多次處進行登入。接著，即使相同的使用者或實體使用不同的帳號，利用一不同的認證資訊組來登入便可存取位在異於該第一帳號之帳號中的受保護內容。

上述特點可分開使用在儲存系統中，亦可以任何的組合方式來結合上述特點，以便提供內容擁有者更多功能的控制及/或保護能力。

【實施方式】

圖1的方塊圖圖解的係可實現本發明各項觀點的記憶體系統範例。如圖1所示，該記憶體系統10包含一中央處理單元(CPU)12、一緩衝器管理單元(BMU)14、一主介面模組(HIM)16、一快閃介面模組(FIM)18、一快閃記憶體20、以及一週邊存取模組(PAM)22。記憶體系統10會經由主介面匯流排26與埠26a來與主裝置24進行通信。快閃記憶體20(其可能係NAND類型)讓主裝置24具有資料儲存的能力。CPU 12的軟體碼亦可儲存在快閃記憶體20之中。FIM 18會經由快閃介面匯流排28與埠28a連接至快閃記憶體20。HIM 16適合連接至各種主系統，如數位相機、個人電腦、個人數位助理(PDA)、數位媒體播放器、MP3播放器、蜂巢式電話、或其它數位裝置。週邊存取模組22會選擇正確的控制器模組(如FIM、HIM、以及BMU)來與CPU 12進行通信。於其中一具體實施例中，虛線框內系統10的所有組件均可併入單一單元(如併入記憶卡或記憶棒10'之中)之中且較佳的係囊

封在一起。

雖然本文參考快閃記憶體來解釋本發明，不過，本發明亦可應用至其它類型的記憶體，如磁碟、光學CD、以及所有其它類型的可覆寫式非揮發性記憶體系統。

緩衝器管理單元14包含：一主直接記憶體存取(HDMA)32、一快閃直接記憶體存取(FDMA)34、一仲裁器36、一緩衝器隨機存取記憶體(BRAM)38、以及一加密引擎40。仲裁器36係一共享的匯流排仲裁器，所以任何時候均僅有一主裝置或起始裝置(其可能係HDMA 32、FDMA 34、或CPU 12)可發揮作用，而從裝置或目標裝置則為BRAM 38。該仲裁器係負責將正確的起始裝置要求送至BRAM 38。HDMA 32與FDMA 34則係負責在HIM 16、FIM 18與BRAM 38或CPU隨機存取記憶體(CPU RAM)12a之間傳輸的資料。HDMA 32與FDMA 34的運作均係習知技術，本文不予詳述。BRAM 38係用來儲存在主裝置24與快閃記憶體20之間傳送的資料。HDMA 32與FDMA 34則係負責在HIM 16/FIM 18與BRAM 38或CPU RAM 12a之間傳輸資料且表示區段作業是否完成。

為改善儲存在記憶體20中之內容的安全性，記憶體系統10會產生用於進行加密及/或解密的(複數個)密鑰值，其中外部裝置(如主裝置24)實質上無法存取該或該等密鑰值。不過，加密與解密通常係逐個檔案來進行，因為該主裝置係以檔案的形式來讀取記憶體系統10中的資料或將資料寫入記憶體系統10之中。和眾多其它類型的儲存裝置一樣，記

憶體裝置10並不知悉檔案或檔案系統。雖然記憶體20會儲存檔案配置表(FAT)用以識別該等檔案的邏輯位址，不過，該FAT實際上係由主裝置24來存取與管理，而非由控制器12來存取與管理。所以，為加密特殊檔案中的資料，控制器12便必須依賴該主裝置來傳送該檔案中該資料於記憶體20中的邏輯位址，如此方能找到該特殊檔案中的資料且利用僅有系統10可取得的密鑰值由系統10來進行加密及/或解密。

為讓主裝置24與記憶體系統10能夠依據相同的密鑰以暗碼的方式來處理檔案中的資料，該主裝置必須為系統10所產生的每個密鑰值提供一參考值，其中此參考值可能僅係一密鑰ID。因此，主裝置24會將經系統10暗碼處理過的每個檔案和一密鑰ID產生關聯，且系統10會將用來暗碼處理資料的每個密鑰值和該主裝置所提供的密鑰ID產生關聯。因此，當該主裝置要求暗碼處理一檔案時，其將會將該項要求連同一密鑰ID以及從記憶體20中取出或儲存在記憶體20之中的資料的邏輯位址一起傳送給系統10。系統10會產生一密鑰值且會將主裝置24所提供的密鑰ID和此值產生關聯，並且實施暗碼處理。依此方式便不必對記憶體系統10的運作方式作任何改變，同時可讓它利用該或該等密鑰來完整地控制該暗碼處理，包含獨特地存取該或該等密鑰值。換言之，系統10會繼續讓主裝置24獨特地控制FAT來管理該等檔案，同時可保持獨特地控制用於暗碼處理之密鑰值的產生與管理。在用於資料暗碼處理之密鑰值的產生與

管理方面，該主裝置24毫無任何作用。

於其中一實施例中，該主裝置24所提供的密鑰ID及該記憶體系統所產生的密鑰值會構成「內容加密密鑰」或CEK中的兩項屬性。雖然主裝置24可將每個密鑰ID與一或多個檔案產生關聯，不過，主裝置24亦可將每個密鑰ID與未組織的資料或以任何方式組織成的資料產生關聯，而不僅限於被組織成完整檔案的資料。

為讓使用者或應用可存取系統10之中受保護的內容或區域，必須利用系統10事先登錄的憑證來進行認證。一憑證係關於具有此憑證之特殊使用者或應用被受予的存取權利。於該事先登錄過程中，系統10會儲存該使用者或應用的身份與憑證，以及儲存和此由該使用者或應用決定且經由該主裝置24來提供的身份與憑證相關聯的存取權利。於完成事先登錄之後，當該使用者或應用要求將資料寫入系統20之中時，其便必須經由該主裝置來提供其身份與憑證、用於加密該資料的密鑰ID、以及該經加密資料要被儲存的位置的邏輯位址。系統10會產生一密鑰值且將此值與該主裝置所提供的密鑰ID產生關聯，並且針對此使用者或應用將用來加密要被寫入之資料的密鑰值的密鑰ID儲存在其記錄或表格之中。接著，便可加密該資料且將經加密的資料儲存在該主裝置以及其所產生之密鑰值所指定的位址處。

當一使用者或應用要求從記憶體20中讀取經加密的資料時，其便必須提供其身份與憑證、先前用於加密被要求之

資料的密鑰的密鑰ID、以及該經加密資料被儲存的位置的邏輯位址。接著，系統10會將該主裝置所提供之該使用者或應用的身份與憑證與儲存在其記錄中的身份與憑證進行匹配。倘若匹配的話，系統10將會從其記憶體中取出和該使用者或應用所提供之密鑰ID相關聯的密鑰值，利用該密鑰值來解密該主裝置所指定之位址處所儲存的資料，並且將經解密的資料傳送給該使用者或應用。

藉由將認證憑證與用於暗碼處理的密鑰的管理分離，其便可共享存取資料的權利，而不必共享憑證。因此，一群具有不同憑證的使用者或應用便可存取相同的密鑰以便存取相同的資料，而不屬於此群的使用者則無法作任何存取。雖然同一群中的所有使用者或應用可存取相同的資料，不過他們仍可能具有不同的權利。因此，一部份使用者或應用可能具有唯讀存取的權利，另一部份使用者或應用可能具有寫入存取的權利，而又一部份使用者或應用則可能兼具有兩種權利。因為系統10保有該等使用者或應用身份與憑證的記錄、他們所存取的該等密鑰ID、以及和每個密鑰ID相關聯的存取權利，所以，系統10便可針對特殊的使用者或應用來增加或刪除密鑰ID以及變更和此等密鑰ID相關聯的存取權利，將存取權利從其中一使用者或應用轉讓給另一使用者或應用，甚至刪除或增加使用者或應用的記錄或表格，上述作業均受控於一經正確認證的主裝置。所儲存的記錄可能會指定必須要有一安全的通道來存取特定的密鑰。認證作業可利用同步或不同步演算法以及

密碼來進行。

特別重要的係，記憶體系統10中的安全內容具可攜性。因為密鑰值係由該記憶體系統產生且外部系統實質上無法取用，所以，當該記憶體系統或含有該系統的儲存裝置從一外部系統轉移至另一系統時，仍可保有其中所儲存之內容的安全性，且外部系統亦無法存取此內容，除非該等外部系統經過該記憶體系統完整控制之方式的認證。即使經過此認證，存取作業依然完全由該記憶體系統來控制，而外部系統則僅能依照該記憶體系統中之預設記錄所控制的方式來進行存取。倘若一要求不符此等記錄的話，該項要求將會被拒絕。

為提供更大的彈性來保護內容，本案設計出僅能由經過正確認證之使用者或應用來存取的特定記憶體區域，下文稱為分割區。當結合上述密鑰型資料加密特點之後，系統10便提供更大的資料保護能力。如圖2所示，快閃記憶體20可將其儲存容量分成數個分割區：一使用者區或分割區以及複數個客製分割區(custom partition)。使用者區或分割區P0可讓所有使用者與應用來存取，無需經過認證。雖然一使用者區之中所儲存的資料的所有位元值均可由任何應用或使用者來讀取或寫入，不過，倘若所讀取的資料經過加密的話，那麼沒有解密授權的使用者或應用便無法存取該使用者區中所儲存之該等位元值所表示的資訊。舉例來說，如圖中使用者區P0中所儲存的檔案102與104所示。另外，該使用者區中還儲存未加密的檔案(如106)，所有的應

用與使用者均可讀取且瞭解。因此，經過加密的檔案均會加上鎖的符號(如圖示)，如檔案102與104。

雖然未經授權的應用或使用者無法瞭解使用者區P0中的加密檔案，不過，此等應用或使用者仍可刪除或破壞該檔案，此為某些應用所不樂見者。為解決上述問題，記憶體20還包含受保護的客製分割區，如分割區P1與P2，未經過事先認證便無法存取此等區域。下文將解釋本申請案各具體實施例中所允許的認證過程。

同樣如圖2所示，眾多使用者或應用可存取記憶體20中的檔案。因此，圖2中顯示出使用者1與使用者2以及應用1至4(在裝置上執行)。在該些實體被允許存取記憶體20中之受保護內容以前，他們必須以下文所解釋的方式先經過一認證過程的認證。於此過程中，要求存取的實體必須在進行角色型存取控制的主裝置端處被確認。因此，要求存取的實體會先提供「我是應用2，我希望讀取檔案1(I am application 2 and I wish to read file 1.)」之類的資訊來確認自己。接著，控制器12便會將該身份、認證資訊、以及要求和記憶體20或控制器12中所儲存的記錄進行匹配。倘若所有條件均符合的話，那麼便准予此實體進行存取。如圖2所示，使用者1除了可不受限制地讀取P0中的檔案106及寫入檔案106以外，使用者1還被准於在分割區P1中讀取檔案101及寫入檔案101，不過卻僅能讀取檔案102與104。相反地，使用者2則不被允許存取檔案101與104，但卻可讀取與寫入檔案102。如圖2所示，使用者1與2具有相同的登入演

算法(AES)，而應用1與3則具有不同的登入演算法(舉例來說，RSA與001001)，其對使用者1與2而言亦不相同。

安全儲存應用(SSA)係記憶體系統10的一安全應用，且可作為本發明的具體實施例，其可用來設計眾多的上述特點。SSA可設計成軟體或電腦碼，將資料庫儲存在CPU 12中的記憶體20或非揮發性記憶體(圖中未顯示)之中，且可讀入RAM 12a之中且由CPU 12來執行。下表所示的係SSA中所用到的縮寫字：

定義、縮寫&簡寫

ACR	存取控制記錄
AGP	ACR群
CBC	鏈接區塊密碼(cipher)
CEK	內容加密密鑰
ECB	電子編碼本
ACAM	ACR屬性管理
PCR	權限控制記錄
SSA	安全儲存應用
Entity	實際且個別存在的任何事物(主裝置端)，可登入SSA，從而運用其功能。

SSA系統說明

資料安全性、完整性、以及存取控制性係SSA的主要作用。資料係以明確未加密的方式儲存在特定類型的大量儲存裝置中的檔案。SSA系統係座落在該儲存系統的最上方，且會為該等已儲存的主檔案加入安全層。

SSA的主要任務係管理和該記憶體中所儲存的(安全)內容相關聯的不同權利。該記憶體應用必須管理多重已儲存內容的多重使用者以及內容權利。個別的主應用會看見此等應用可看見的磁碟機與分割區，且會看見用於管理與描述該等已儲存檔案在該儲存裝置上之位置的檔案配置表(FAT)。

雖然本例中的儲存裝置使用的係被分成複數個分割區的NAND快閃晶片，不過，亦可使用其它的行動儲存裝置且其同樣落在本發明的範疇之內。該些分割區係具有連續邏輯位址的線程(thread)，其中起始位址與結束位址則界定它們的邊界。所以，於必要時可透過軟體(如記憶體20中所儲存的軟體)對隱藏分割區的存取作業加上限制，該軟體會將此等限制與此等邊界內的位址產生關聯。SSA可完整地認出受其管理的分割區的邏輯位址邊界。SSA系統會利用分割區來實際保護資料，避免讓未經授權的主應用來存取。對主裝置來說，該等分割區係一種界定私有空間的機制，用以於該空間中儲存資料檔案。該些分割區可能係公眾分割區，可存取該儲存裝置的任何實體均可看見且會知悉該分割區存在於該裝置之上；該些分割區亦可能係私有或隱藏的分割區，僅有被選定的主應用方能存取且知悉該等分割區存在於該儲存裝置之中。

圖3為一記憶體的概略示意圖，其圖解的係該記憶體中的各種分割區：P0、P1、P2、以及P3(當然，亦可運用少於四個或多於四個的分割區)，其中P0係公眾分割區，任何實體

均可來存取無需經過認證。

一私有分割區(如P1、P2、或P3)則會隱藏其內部之檔案的存取作業。藉由讓主裝置無法存取該分割區，快閃裝置(舉例來說，快閃卡)便可保護該分割區內部的資料檔案。不過，此類保護涉及到該隱藏分割區中所駐存的所有檔案，其方式係對該分割區內之邏輯位址處所儲存的資料的存取作業加諸限制。換言之，該等限制和某一範圍的邏輯位址相關聯。可存取該分割區的所有使用者/主裝置將可無限制地存取其內部的所有檔案。為將不同的檔案(或不同的檔案群)彼此隔離，SSA系統會利用密鑰以及密鑰參考值或密鑰ID來為每個檔案(或檔案群)提供另一種安全等級以及完整性。用於對不同記憶體位址處的資料進行加密的某一特殊密鑰值的密鑰參考值或密鑰ID可被類推至一含有該已加密資料的資料盒或資料域。據此，於圖4中，該等密鑰參考值或密鑰ID(舉例來說，「密鑰1」以及「密鑰2」)會被顯示成包圍複數檔案的區域，該等檔案則係利用和該等密鑰ID相關聯的密鑰值來進行加密。

參考圖4，舉例來說，檔案A可讓所有的實體存取，無需進行認證，因為圖中的檔案A並未被任何密鑰ID包圍。雖然位於公眾分割區中的檔案B可被所有的實體存取或覆寫，不過，其含有以具有ID「密鑰1」的密鑰來加密的資料，所以，除非此實體可存取此密鑰，否則其並無法存取檔案B中內含的資訊。依此方式，利用密鑰值與密鑰參考值或密鑰ID可僅提供邏輯保護，不同於上述分割區所提供的保護類型。

所以，可存取一分割區(公眾或私有)的任何主裝置均能夠讀取或寫入整個分割區中的資料，包含已加密資料在內。不過，因為該資料已經過加密，所以未經授權的使用者便僅能夠破壞該資料。較佳的係，該等未經授權的使用者無法改變該資料而不被偵測到，亦無法使用該資料。藉由限制對該等加密及/或解密密鑰的存取作業，此項特點便可僅允許經授權的使用者來使用該資料。檔案B與C亦於P0中利用具有密鑰ID「密鑰2」的密鑰來加密。

經由利用內容加密密鑰(CEK)的對稱型加密方法便可提供資料機密性與完整性，每個CEK提供一種資料機密性與完整性。於SSA具體實施例中，該等CEK係由快閃裝置(舉例來說，快閃卡)來產生，僅供內部使用，且對外部保持隱密。經過加密的資料還可經過雜湊處理(hashed)，或是可對該密碼進行鏈接區塊處理(chain blocked)，以確保資料的完整性。

並非該分割區中的所有資料均利用不同的密鑰來加密及和不同的密鑰ID相關聯。公眾或使用者檔案中或作業系統區(也就是，FAT)中的特定邏輯位址便可能未和任何密鑰或密鑰參考值相關聯，因此，能夠存取該分割區本身的任何實體均可存取該等邏輯位址。

需要能夠產生密鑰與分割區以及於該等分割區中寫入與讀取資料或使用該等密鑰的任何實體均必須經由存取控制記錄(ACR)來登入該SSA系統。該SSA系統中的一ACR的特權(privilege)稱為動作(Action)。每個ACR均可能具有權限

(Permission)來實施下面三種類型的動作：產生分割區與密鑰/密鑰ID、存取分割區與密鑰、以及產生/更新其它ACR。

可將複數個ACR組織成群，稱為ACR群或AGP。一旦某一ACR已經過成功地認證，那麼該SSA系統便會開啟一交談(Session)，以便讓任何ACR的動作可經由此交談來執行。

使用者分割區

該SSA系統會管理一或多個公眾分割區，該等公眾分割區亦稱為使用者分割區。此分割區存在於儲存裝置上，且係可經由該儲存裝置的標準讀取寫入命令來存取的分割區。取得和該或該等分割區之大小以及其存在該裝置上之情形有關的資訊較佳的係不必對該主系統隱藏。

該SSA系統可經由標準的讀取寫入命令或SSA命令來存取該或該等分割區。所以，存取該分割區較佳的係不會受限於特定ACR。不過，該SSA系統卻可讓該等主裝置來限制該使用者分割區的存取。讀取存取與寫入存取可被個別地致能/取消。其允許產生所有四種組合，舉例來說，唯寫、唯讀(寫入保護)、讀取與寫入、以及無存取。

SSA系統可讓ACR將密鑰ID與該使用者分割區內的檔案產生關聯，並且利用和此等密鑰ID相關聯的密鑰來加密個別的檔案。存取該等使用者分割區內的已加密檔案以及設定該等分割區的存取權利將會利用SSA命令組來完成，參見附錄A中SSA命令的詳細說明，於該附錄中，密鑰ID稱為「域」。上面的特點亦可套用於未被組織成檔案的資料。

SSA分割區

該些分割區係隱藏的分割區(主作業系統或OS無法看見)，僅能經由SSA命令來存取。較佳的係，除非經由登入一ACR後所建立的交談(下文會作說明)，否則SSA系統便不允許該主裝置來存取SSA分割區。同樣地，較佳的係，除非要求係來自一已建立的交談，否則SSA便不會提供和下面相關的資訊，SSA分割區是否存在、SSA分割區的大小、SSA分割區的存取權限。

分割區的存取權利(access right)可從ACR權限(ACR permission)中推衍出來。一旦一ACR登入該SSA系統之後，其便能夠與其它的ACR共享該分割區(下文會作說明)。當產生一分割區之後，該主裝置便會為該分割區提供一參考名稱或ID(舉例來說，圖3與4中的P0至P3)。於該分割區的進一步讀取命令與寫入命令中會用到此參考名稱。

儲存裝置的分割

該裝置的所有可用儲存容量較佳的係分配給該使用者分割區以及目前已配置的SSA分割區。所以，任何的再分割作業均可能會涉及到重新配置既有的分割區。該裝置容量(所有分割區的大小總合)的淨變化(net change)將會係零。該裝置記憶體空間中該等分割區的ID係由主系統來定義。

該主系統可將既有的分割區中其中一者再分割成兩個較小的分割區，或是將兩個既有的分割區(兩者可能係相鄰分割區或不相鄰的分割區)合併成一個分割區。該等經分割或經合併的分割區中的資料可予以刪除或保持不變，由該主系統來判斷。

因為再分割該儲存裝置可能會造成資料損失(可能係已經於該儲存裝置的邏輯位址空間中刪除該資料或是移動該資料)，所以，該SSA系統會對再分割作業加諸嚴格的限制。僅有駐存在於根AGP(root AGP，下文將作解釋)之中的ACR才被允許發出再分割命令且其僅能夠參照其所擁有的分割區。因為，該SSA系統並不知悉資料被如何組成於該等分割區之中(FAT或其它檔案系統結構)，所以，係由該主裝置負責在該裝置被再分割的任何時候來重建該些結構。

再分割該使用者分割區將會改變此分割區被主OS所看見的大小以及其它屬性。

經過再分割之後，便由主系統負責確認該SSA系統中的任何ACR均未參考到不存在的分割區。倘若該些ACR未被正確地刪除或更新的話，那麼該系統便會在以後偵測到要存取該等不存在分割區的任何嘗試(代表該些ACR)並且予以拒絕。其同樣會留意已被刪除的密鑰以及密鑰ID。

密鑰、密鑰ID以及邏輯保護

當將一檔案寫入一特定隱藏分割區中之後，其便不會係公知的檔案。不過，一旦某一實體(不論是否為敵對實體)獲得承認且存取此分割區，那麼該檔案且可被取用且可被明確地看見。為進一步保護該檔案，SSA可於該隱藏分割區中對其進行加密，其中用於存取解密該檔案的密鑰的憑證較佳的係異於用於存取該分割區的憑證。由於SSA並不知悉該等檔案(完全受控於主裝置且由主裝置來管理)，所以將一CEK和一檔案產生關聯便會發生問題。將該檔案與SSA

所瞭解的事物(如密鑰ID)作連結便可改正此問題。因此，當該SSA產生一密鑰之後，該主裝置便會將用於此密鑰的密鑰ID與利用該SSA所產生之密鑰來加密的資料產生關聯。

該密鑰值與密鑰ID可提供邏輯安全性。和一特定密鑰ID相關聯的所有資料不論其位置為何均會利用相同的內容加密密鑰(CEK)來加密，該內容加密密鑰的參考名稱或密鑰ID係由該主應用來獨特產生。倘若一實體取得存取一隱藏分割區的權利(經由一ACR來認證)且希望讀取或寫入此分割區內的加密檔案的話，其便必須存取和此檔案相關聯的密鑰ID。當同意其存取此密鑰ID的密鑰時，該SSA便會載入和此密鑰ID相關聯的CEK中的密鑰值，並且於傳送給主裝置以前先加密該資料或於寫入該快閃記憶體20以前先加密該資料。和一密鑰ID相關聯的CEK中的密鑰值係由該SSA系統隨機產生一次且維護。該SSA系統外面的任何實體均無法瞭解或存取此CEK中的密鑰值。外界僅能提供且使用一參考值或密鑰ID，而非該CEK中的密鑰值。該密鑰值完全由該SSA來管理且僅可讓該SSA來存取。

該SSA系統會利用下面加密模式中任一者(由使用者定義)來保護和該密鑰ID相關聯的資料(所使用的實際暗碼演算法以及CEK中的密鑰值均係由系統控制且不會透露給外界)：

區塊模式：資料會被分成複數個區塊，每一區塊個別加密。此模式通常被認為安全性較低且易受到字典攻擊

(dictionary attack)。不過，其可讓使用者隨機存取該等資料區塊中任一者。

鏈接模式：資料會被分成複數個區塊，該等區塊會於加密過程中被鏈接在一起。每個區塊均可當作下一區塊之加密過程的其中一個輸入。此模式雖被認為比較安全，不過該資料卻需要一直被寫入且從起始處至結束處依序被讀取，用以產生一該等使用者未必接受的附加資料(overhead)。

雜湊模式：其係一種鏈接模式，不過還會額外產生一資料摘要(data digest)，該資料摘要可用來證實資料完整性。

ACR與存取控制

該SSA係被設計用來處理多重應用，每一種應用均由該系統資料庫中的一節點樹來代表。藉由確保該等樹分支間不會有任何的串音便可達到該等應用之間的互斥性。

為存取該SSA系統，一實體必須透過該系統的複數個ACR中其中一者來建立連接。登入程序係由該SSA系統依照該使用者選擇連接的ACR中所內建的定義來操控。

該ACR係該SSA系統的一個別登入點。該ACR保有登入憑證以及認證方法。於該記錄中還駐留著該SSA系統內的登入權限，其中有讀取特權及寫入特權。圖5所示的便係此情形，圖中圖解著同一AGP中有n個ACR。此意謂著該等n個ACR中至少其中數個可共享同一密鑰的存取作業。因此，ACR#1及ACR#n會共享具有密鑰ID「密鑰3」的密鑰的存取作業，其中ACR#1及ACR#n係ACR ID，而「密鑰3」則係用

來加密和「密鑰3」相關聯的資料的密鑰的密鑰ID。相同的密鑰還可用來加密及/或解密多個檔案或多組資料。

該SSA系統支援數種類型來登入該系統，其中一旦該使用者成功登入之後，認證演算法以及使用者憑證均可能改變，該使用者於該系統中的特權亦可能改變。圖5還圖解不同的登入演算法以及憑證。ACR#1需要一密碼登入演算法及作為憑證的密碼，而ACR#2則需要一PKI(公眾密鑰基礎結構)登入演算法及作為憑證的公眾密鑰。因此，為能登入，一實體便需要提交一合法的ACR ID，以及正確的登入演算法與憑證。

一旦一實體登入該SSA系統中的一ACR之後，其權限，使用SSA命令的權利，便會定義在和該ACR相關聯的權限控制記錄(PCR)之中。於圖5中，依照圖中所示的PCR，ACR#1授予唯讀權限給和「密鑰3」相關聯的資料，而ACR#2授予讀取與寫入權限給和「密鑰5」相關聯的資料。

不同的ACR可共享該系統中共同的利益與特權，例如用來讀取與寫入的密鑰。為達此目的，具有特定共同事物的ACR可聚集成AGP-ACR群。因此，ACR #1與ACR #n會共享具有密鑰ID「密鑰3」的密鑰的存取作業。

AGP以及其中的ACR會被組織成階層樹，且除了產生安全的密鑰來確保敏感資料的安全性以外，一ACR較佳的係還能夠產生對應它的密鑰ID/分割區的其它ACR實體。該些ACR子部的權限將會少於等於它們的父部：產生者，且可能係該父部ACR本身所產生的特定密鑰權限。無需增加任

何作業，該子部ACR便會取得它們所產生的任何密鑰的存取權限。圖6中所示的便係此情形。因此，ACR 122會產生AGP 120中的所有ACR，且其中兩個ACR會繼承ACR 122存取和「密鑰3」相關聯之資料的一或多個權限。

AGP

登入該SSA系統係藉由指定一AGP及該AGP內之一ACR來完成。

每個AGP均具有一獨特的ID(參考名稱)，其係作為該SSA資料庫中其實體的索引值(index)。當產生該AGP之後，便會將該AGP名稱提供給該SSA系統。倘若所提供的AGP名稱已存在於該系統中的話，那麼該SSA便將會拒絕該產生作業。

AGP係用來對存取權限與管理權限的轉讓實施限制，下面章節將作說明。圖6中兩樹所提供的其中一項功能係操控所有分離實體(如兩個不同應用或兩位不同的電腦使用者)的存取作業。為達此等目的，重要的係，該等兩個存取處理可能實質上要彼此獨立(也就是，實質沒有任何串音)，即使兩者同時發生。此意謂著，每樹中的認證、權限、以及額外ACR與AGP的產生均與另一樹無關。所以，當於記憶體10中使用該SSA系統時，便允許該記憶體系統10同時提供多項應用。其還允許兩項應用以彼此獨立的方式來存取兩組分離的資料(舉例來說，一組照片與一組歌曲)。圖6中所示的便係此情形。因此，和圖6上方透過該樹中的節點(ACR)進行存取的應用或使用者的「密鑰3」、「密鑰X」、以

及「密鑰Z」相關聯的資料可能包括照片。和圖6下方透過該樹中的節點(ACR)進行存取的應用或使用者的「密鑰5」、以及「密鑰Y」相關聯的資料可能包括歌曲。產生該AGP的ACR僅有在該AGP中已經沒有ACR實體時才有權限來刪除該AGP。

實體的SSA進入點：存取控制記錄(ACR)

該SSA系統中的一ACR會描述該實體被准予登入該系統的方式。當一實體要登入該SSA系統時，其必須指定和其要實施的認證處理相對應的ACR。一ACR包含一權限控制記錄(PCR)，其闡述的係一旦該使用者經過認證後能夠執行的動作，如圖5中所示之ACR中的定義。主端實體會提供所有的ACR資料欄位。

當一實體已經成功地登入一ACR之後，該實體便能夠詢問所有的ACR分割區以及密鑰存取權限以及ACAM權限(下文會作解釋)。

ACR ID

當一SSA系統實體開始進行登入程序時，其必須要指定和登入方法對應的ACR ID(其係在產生該ACR時由該主裝置來提供)，俾使當符合所有登入條件時，該SSA便可設定正確的演算法且選擇正確的PCR。當產生該ACR之後，便會將該ACR ID提供給該SSA系統。

登入/認證演算法

認證演算法會指定該實體將使用何種登入程序以及必須提供何種憑證來證明使用者的身份。該SSA系統支援數種

標準登入演算法，從無程序(且無憑證)及密碼型程序至以對稱或非對稱暗碼術(cryptography)為主的雙向認證協定。

憑證

該實體的憑證會對應於該登入演算法，且可讓該SSA用來驗證與認證該使用者。其中一種憑證範例可能係用於密碼認證的密碼/PIN數、用於AES認證的AES密鑰、...、等。該等憑證(也就是，PIN、對稱密鑰、...、等)的類型/格式會預先定義且從該認證模式中推演出來，當產生該ACR時便會將該等憑證送至該SSA系統。該SSA系統於定義、散佈、以及管理該些憑證方面毫無作用，不過，PKI型的認證除外，於該型認證中，可利用該裝置(舉例來說，快閃卡)來產生RSA密鑰對且可輸出該公眾密鑰以產生證書(certificate)。

權限控制記錄(PCR)

PCR所示的係，在該實體登入該SSA系統且成功地通過該ACR的認證程序之後，應該授予該實體何種權限。共有三種權限種類：分割區與密鑰的產生權限、分割區與密鑰的存取權限、以及實體ACR屬性的管理權限。

存取分割區

PCR的此部分含有於成功完成該ACR階段時該實體能夠存取的分割區清單(利用和送至該SSA系統的ID)。對每個分割區來說，該存取類型可能限定為唯寫或唯讀，或者亦可能指定完整的寫入/讀取存取權利。因此，圖5中的ACR#1可存取分割區#2而不會存取分割區#1。該PCR中所指定的

該等限制可套用至該等SSA分割區與該公眾分割區。

該公眾分割區可利用該SSA系統之主裝置(舉例來說，快閃卡)的正常讀取與寫入命令來存取，或者可利用SSA命令來存取。當產生一具有權限來限制該公眾分割區的根ACR(下文會作解釋)時，其便可將其傳送至其子部。一ACR較佳的係僅能限制正常讀取與寫入命令來存取該公眾分割區。該SSA系統中的複數ACR較佳的係僅可能在它們產生方面受到限制。一旦一ACR具有權限可讀取/寫入該公眾分割區時，較佳的係，其便不會被剝奪。

存取密鑰ID

PCR的此部分含有於該實體的登入程序符合該等ACR政策時和該實體能夠存取的密鑰ID清單(和該主裝置送至該SSA系統者相同)相關聯的資料。所指定的密鑰ID和駐存於出現在該PCR中之該分割區中的一檔案/複數檔案相關聯。因為該等密鑰ID和該裝置(舉例來說，快閃卡)中的邏輯位址無關，所以當有一個以上的分割區和一特定ACR相關聯時，該等檔案便可能係為於該等分割區中其中一者之中。該PCR中所指定的該等密鑰ID可能各具有一組不同的存取權利。存取密鑰ID所指到的資料可限制為唯寫或唯讀，或者亦可指定完整的寫入/讀取存取權利。

ACR屬性管理(ACAM)

此部分說明的係如何在特定情況中來改變ACR的系統屬性。

於SSA系統中可被允許的ACAM動作如下：

產生/刪除/更新AGP與ACR。

產生/刪除分割區與密鑰。

轉讓密鑰與分割區的存取權利。

父部ACR較佳的係不能夠編輯ACAM權限。此作法較佳的係會需要刪除與再產生該ACR。另外，由該ACR所產生之對一密鑰ID的存取權限較佳的係亦能夠不會被剝奪。

產生/刪除/更新AGP與ACR

一ACR可能具有產生其它ACR與AGP的功能。產生ACR可能還意謂著授予它們經過它們的產生者處理後的部分或全部ACAM權限。具有產生ACR的權限意謂著具有下面動作的權限：

1.定義與編輯子部的憑證：較佳的係，一旦因產生ACR而設定認證方法之後，該認證方法無法被編輯。該等憑證可在為該子部所界定的認證演算法的邊界內作變更。

2.刪除ACR。

3.轉讓該產生權限給子部ACR(從而會具有孫部)。

一有權來產生其它ACR的ACR便有權來轉讓解隔離權限(unblocking permission)給其所產生的ACR(不過，其可能無權為ACR來解隔離)。父部ACR將會於子部ACR中置放一和其解隔離者(unblocker)相關的參考值。

父部ACR係有權來刪除其子部ACR的唯一ACR。當一ACR刪除一其所產生的較低階ACR時，那麼便亦必須自動刪除由此較低階ACR所產生的所有ACR。當一ACR被刪除之後，那麼便要刪除其所產生的所有密鑰ID以及分割區。

一ACR能夠利用兩種例外條件(exception)來更新其自己的記錄：

密碼/PIN雖然係由產生者ACR(creator ACR)來設定，不過卻僅能由含有該等密碼/PIN的ACR來更新。

一根ACR可刪除本身以及其所駐存的AGP。

轉讓密鑰與分割區的存取權利

ACR與它們的AGP會被集合在階層樹之中，其中該根AGP及其中的ACR係位於該樹的頂端(舉例來說，圖6中的根AGP 130以及132)。於該SSA系統中可會有數棵AGP樹，不過，彼此完全分離。位於一AGP內部的ACR可將其密鑰的存取權限轉讓給其所在的相同AGP內的所有ACR，並且可轉讓給其所產生的所有ACR。用於產生密鑰的權限較佳的係包含轉讓存取權限的權限，以便使用該等密鑰。

密鑰的權限可分為下面三種：

1.存取：定義該密鑰的存取權限，也就是，讀取、寫入。

2.所有權：依定義，產生一密鑰的ACR便係其擁有者。此所有權可從一ACR轉讓至另一ACR(前提為兩者位在相同的AGP中或位於一子部AGP中)。一密鑰的所有權會提供權限來刪除該密鑰以及轉讓該密鑰的權限。

3.存取權利轉讓：此權限可讓該ACR來轉讓其所保有的權利。

一ACR能夠轉讓其所產生的分割區以及其有存取權限的其它分割區的存取權限。

藉由將該等分割區的名稱與密鑰ID加入該受指定ACR的

PCR之中便可完成權限轉讓。轉讓密鑰存取權限可藉由該密鑰ID來完成，或者可藉由聲明該存取權限係用於該要轉讓的ACR的所有已產生的密鑰來完成。

ACR的隔離及解隔離

一ACR可能具有一隔離計數，當該實體中具有本系統的ACR認證程序不成功時，該計數便會遞增。當抵達特定的最大不成功認證數(MAX)時，該SSA系統便會隔離該ACR。

經隔離的ACR可由該經隔離ACR相關的另一ACR來解隔離。與該解隔離ACR相關的參考值係由其產生者來設定。該解隔離ACR較佳的係位在和該經隔離ACR之產生者相同的AGP之中且具有「解隔離」權限。

該系統中的其它ACR均無法解隔離該經隔離的ACR。一ACR可能會配置一隔離計數，但卻不具有解隔離ACR。於此情況中，倘若此ACR被隔離之後，其便無法被解隔離。

根AGP：產生一應用資料庫

該SSA系統係被設計成用來處理多重應用且隔離每一應用的資料。該AGP系統的樹結構係用來辨識與隔離特定應用資料的主要工具。根AGP係位於一應用SSA資料庫樹的尖端且支持略不相同的表現規則(behavior rule)。可於該SSA系統中配置數個根AGP。圖6中顯示兩個根AGP 130與132。當然，亦可運用較少或較多的AGP，且其同樣落在本發明的範疇之內。

經由於該裝置中增加新的AGP/ACR樹的程序便可完成針對一新應用來登錄該裝置(舉例來說，快閃卡)及/或核發該

裝置之新應用的憑證的目的。

該SSA系統支援三種不同的根AGP(以及該根AGP之所有ACR與它們的權限)產生模式：

1.開放模式：無需任何種類認證的任何使用者或實體，或者經由該系統ACR認證過的使用者/實體(下文會作解釋)均能夠產生一新的根AGP。開放模式允許以下面方式來產生根AGP：沒有任何安全措施，而所有資料傳輸均係在一開放通道上進行(也就是，在一核發機構的安全環境中)；或者經由該系統ACR認證所建立的安全通道來產生(也就是，在空中進行(Over The Air，OTA)程序以及事後核發程序(post issuance procedure))。

倘若該系統ACR未經過配置(此為一選擇性特點)且該根AGP產生模式設為開放的話，那麼便僅可選擇開放通道。

2.受控模式：僅有經由該系統ACR認證過的實體方能產生一新的根AGP。倘若該系統ACR未經過配置的話，該SSA系統便無法被設為此模式。

3.鎖定模式：根AGP產生特點已經被取消，且無法於該系統中新加任何額外的根AGP。

有兩個SSA命令來控制此項特點(任何使用者/實體均可用到此二命令，無需經過認證)：

1.方法配置命令：用來配置該SSA系統，使其使用該等三種根AGP產生模式中任一模式。僅允許下面的模式變化：開放模式->受控模式，受控模式->鎖定模式(也就是，倘若該SSA系統目前被配置成受控模式的話，那麼其便僅能變

成鎖定模式)。

2.方法配置鎖定命令：用來取消前述方法配置命令且永久鎖定目前所選定的命令。

當產生一根AGP之後，其係位於一特殊的初始模式中使其可產生與配置它的ACR(利用和被套用至產生該根AGP相同的存取限制)。於結束該根AGP配置程序之後，當該實體明確地將其切換至操作模式中時，既有的ACR便不再會被更新且無法再產生額外的ACR。

一旦一根AGP被放入標準模式中之後，僅有經由該根AGP中複數個ACR中分配到可刪除該根AGP之權限的ACR來登入該系統方能刪除該根AGP。此為除了該特殊初始化模式以外的另一種根AGP例外條件，較佳的係，其為含有可刪除自己的AGP之權限的ACR的唯一AGP，不同於下一樹層中的AGP。

一根ACR與一標準ACR之間的第三項且為最後一項差異在於，其為該系統中由權限來產生與刪除分割區的唯一ACR。

SSA系統ACR

系統ACR可用於下面兩種SSA作業中：

1.於不利的環境下在一安全通道的保護下來產生一ACR/AGP樹。

2.辨識與認證該SSA系統的主裝置。

較佳的係，於該SSA中可能僅有一個系統ACR，且一旦定義之後，較佳的係便無法再改變。當產生系統ACR時無需

進行系統認證，僅需要一SSA命令即可。本項產生-系統-ACR特點可被取消(如同產生-根-AGP特點)。於產生該系統ACR之後，該產生-系統-ACR命令便不具任何作用，因為較佳的係僅允許有一個系統ACR。

於產生的過程中，該系統ACR並不會運作。在完成時，需要發出一特殊的命令，以便表示該系統ACR已被產生且就緒。而後，該系統ACR較佳的係便不會再被更新或置換。

該系統ACR會於該SSA中產生根ACR/AGP。其有權來增加/改變該根層，直到其符合該主裝置的要求且該主裝置將其隔離為止。隔離該根AGP基本上會切斷該根AGP與該系統ACR的連接且使其不再改變。此時便無法再改變/編輯該根AGP以及其中的ACR。此作業係經由一SSA命令來完成。取消根AGP的產生特點係永久性的效果且無法到逆。圖7中所示的便係上述和該系統ACR有關的特點。該系統ACR係用來產生三個不同的根AGP。於產生該些根AGP後的特定時間處，便會從該主裝置中送出該SSA命令用以將該等根AGP與該系統ACR隔離，從而取消該產生-根-AGP特點，如圖7中連接該系統ACR與該等根AGP的虛線所示。如此便不會改變此三個根AGP。該等三個根AGP可用來產生複數個子部AGP，以便於該等根AGP被隔離前或被隔離後來產生三棵不同的樹。

上述特點讓內容擁有者在配置含有內容的安全產品方面具有極大的彈性。安全產品必須要經過「核發(issued)」。於核發程序中會放置辨識密鑰，讓該裝置能夠辨識該主裝

置或讓該主裝置能夠辨識該裝置。辨識該裝置(舉例來說，快閃卡)會讓該主裝置判斷其是否能夠信賴其秘密資料。相反地，辨識該主裝置則會僅在該主裝置被許可下才讓該裝置來強化安全政策(同意與執行一特定主命令)。

被設計用來服務多重應用的產品將會具有數個辨識密鑰。該產品可被「事先核發(pre-issued)」--密鑰在運送以前的製造期間便已先被儲存；或者該產品亦可「事後核發(post-issued)」--在運送以後才加入新的密鑰。就事後核發來說，該記憶體裝置(舉例來說，記憶卡)必須含有某種主裝置級或裝置級的密鑰，以便利用該等密鑰來辨識被允許於該裝置中新增應用的實體。

上述特點讓一產品可被配置成用以致能/取消事後核發。此外，還可於運送後安全地進行該事後核發配置。該裝置可當作一零售產品來購買，於該裝置中除了上述的主裝置級或裝置級密鑰以外便沒有任何密鑰，接著便可由新的擁有者進行配置，以便致能另外的事後核發應用或取消該等應用。

因此，該項系統ACR特點能夠完成上面目的：

-沒有系統ACR的記憶體裝置將允許以無限制且不受控制的方式來進行應用新增。

-沒有系統ACR的記憶體裝置可被配置成用以取消系統ACR產生特點，其意謂著不能控制新應用的新增(除非同時取消產生新根AGP的特點)。

-具有系統ACR的記憶體裝置將僅允許以受控制的方式

透過一安全通道來進行應用的新增，以便經由利用該系統ACR憑證的認證程序來建立。

-具有系統ACR的記憶體裝置可被配置成用以在已經新增應用的前後來取消該項應用新增特點。

密鑰ID清單

雖然可依照特定的ACR要求來產生複數個密鑰ID，不過，於該記憶體系統10中，該等密鑰ID卻僅會由該SSA系統來使用。當產生一密鑰ID之後，產生ACR便會提供下面的資料或是會提供下面的資料給產生ACR：

1.密鑰ID。該ID會由該實體經由該主裝置來提供，且可用來與所有進一步讀取存取或寫入存取中利用該密鑰來加密或解密的密鑰及資料產生關聯。

2.密鑰密碼以及資料完整性模式(上述的區塊模式、鏈接模式、以及雜湊模式，下文將作解釋)

除了該等主裝置提供的屬性以外，該SSA系統還保有下面資料：

1.密鑰ID擁有者。作為擁有者的ACR的ID。當產生一密鑰ID之後，該產生者ACR便係該密鑰ID的擁有者。不過，密鑰ID所有權可傳輸給另一ACR。較佳的係，僅有該密鑰ID擁有者才能傳輸一密鑰ID的所有權且予以轉讓。轉讓相關密鑰的存取權限以及撤銷該些權利可由該密鑰ID內容擁有者或分配到轉讓權限的任何其它ACR來操控。當試圖施行該些作業中任一作業時，該SSA系統僅會在該提出要求的ACR有被授權才會同意其施行。

2.CEK。此CEK係用來對與該密鑰ID相關聯的內容或被該密鑰ID指到的內容進行加密。該CEK可能係由該SSA系統所產生的128位元AES隨機密鑰。

3.MAC值與IV值。鏈接區塊密碼(CBC)加密演算法中所用的動態資訊(訊息認證碼(message authentication codes，MAC)及初始向量(initiation vectors，IV))。

下文將參考圖8A至16中的流程圖來解釋該SSA的各項特點，其中，步驟左邊的「H」表示由主裝置來實施的作業，而「C」表示由該記憶卡來實施的作業。為產生一系統ACR，該主裝置會發出一命令給該記憶體裝置10中的SSA，用以產生系統ACR(方塊202)。該裝置10則會響應以檢查一系統ACR是否已經存在(方塊204、菱形206)。倘若存在的話，裝置10便會回傳失敗且停止(橢圓形208)。倘若不存在的話，裝置10便會檢查是否允許進行系統ACR產生(菱形210)，倘若不允許的話便會回傳一失敗狀態且停止(方塊212)。因此，可能會出現該裝置發行者不允許進行動儲存裝置系統ACR產生的情況，如在該等必要的安全特點已經被預設的情況，因而便不需要任何系統ACR。倘若允許的話，該裝置10便會回傳OK狀態且等待來自該主裝置的系統ACR憑證(方塊214)。該主裝置會檢查SSA狀態且檢查該裝置10是否已經表示允許產生系統ACR(方塊216及菱形218)。倘若不允許產生或系統ACR已經存在的話，該主裝置便會停止(橢圓形220)。倘若該裝置10已經表示允許產生系統ACR的話，那麼該主裝置便會發出一SSA命令來定義它的登入憑

證且將其送至裝置10(方塊222)。裝置10會利用所收到的憑證來更新一系統ACR記錄且會回傳OK狀態(方塊224)。響應此狀態信號之後，該主裝置便會發出用以表示該系統ACR已經就緒的SSA命令(方塊226)。該裝置10會響應以鎖定該系統ACR，使其無法再被更新或置換(方塊228)。此作法會將該系統ACR的特點及用來辨識該裝置10的身份鎖在該主裝置中。

用於產生新樹(新的根AGP及ACR)的程序係取決於該些功能配置在該裝置中的方式。圖9解釋的便係該等程序。主裝置24與記憶體系統10均會遵守該等程序。倘若一同取消新增根AGP的話，那麼便無法新增新的根AGP(菱形246)。倘若致能新增根AGP但卻需要一系統ACR的話，那麼該主裝置便會在發出Create Root_AGP命令(方塊254)以前先經由該系統ACR來認證且建立一安全通道(菱形250，方塊252)。倘若不需要系統ACR的話(菱形248)，該主裝置24便會逕行發出Create Root_AGP命令無需認證且會進入方塊254。倘若系統ACR存在的話，即使不需要，該主裝置亦可使用(該流程圖中未顯示)。倘若該項功能被取消的話，那麼該裝置(舉例來說，快閃卡)將會拒絕欲產生新的根AGP的任何試圖，而倘若需要系統ACR的話，其便會拒絕欲產生新的根AGP而不經過認證的任何試圖(菱形246與250)。於方塊254中新產生的AGP與ACR現在會被切換成運作模式，俾使可更新或改變此等AGP中的ACR，而不會於該等ACR中新增任何ACR(方塊256)。接著便會視情況來鎖定該系統，俾

使無法產生額外的根AGP(方塊258)。虛線框258表示此步驟係一非必要步驟。本申請案之圖式中的流程圖中的虛線框均為非必要步驟。如此便可讓內容擁有者阻止該裝置10用於仿製具有合法內容之真品記憶體裝置的其它非法用途中。

為產生ACR(上述之根AGP中的ACR以外的ACR)，可從有權產生ACR的任意ACR開始(方塊270)，如圖10中所示。一實體可試圖藉由提供該進入點ACR身份經由該主裝置24來進入，而該ACR則具有其希望產生的所有必要屬性(方塊272)。該SSA會查找一匹配該ACR身份的ACR，並且檢查具有此身份的ACR是否有權來產生ACR(菱形274)。倘若該項要求經過驗證後被授權的話，那麼裝置10中的SSA便會產生一ACR(方塊276)。

圖11中顯示兩個AGP，闡述的係一棵可用於利用圖10之方法的安全應用中的樹。因此，營銷AGP(marketing AGP)中具有身份m1的ACR有權來產生一ACR。ACR m1亦有權使用一密鑰來讀取與寫入和密鑰ID「營銷資訊」有關的資料以及和密鑰ID「價格表」有關的資料。利用圖10的方法，可產生具有兩個ACR的銷售AGP(Sales AGP)：s1與s2，僅具有用於存取和密鑰ID「價格表」有關之報價資料的密鑰的讀取權限，但卻無權讀取用於存取和密鑰ID「營銷資訊」有關的資料的密鑰。依此方式，具有ACR s1與s2的實體便僅能讀取報價資料而無法改變報價資料，且不能存取營銷資料。相反地ACR m2則無權產生ACR，僅具有用於存取和

密鑰ID「價格表」有關之資料的密鑰以及和密鑰ID「營銷資訊」有關之資料的讀取權限。

因此，可依上面解釋的方式來轉讓存取權利，其中m1會轉讓讀取報價資料的權利給s1與s2。當含有龐大營銷與銷售群時，此作法特別有效。當僅有一位或少數銷售人員時，便可能不必用到圖10的方法。取而代之的方法係，可由一ACR將該等存取權利轉讓給相同AGP內較低層或相同層處的ACR，如圖12所示。首先，該實體會藉由經由該主裝置於該樹中以上述的方式來指定一ACR以進入此AGP的樹之中(方塊280)。接著，該主裝置會指定該ACR以及要轉讓的權利。該SSA會查看此ACR的該或該等樹，並且查看該ACR是否有權來轉讓其權利給所指定的另一ACR(菱形282)。倘若有的話，則會轉讓該等權利(方塊284)；否則便會停止。結果如圖13中所示。此例中，ACR m1有權將讀取權限轉讓給ACR s1，致使s1能夠在經過轉讓之後利用一密鑰來存取報價資料。倘若m1具有相同或更大的權利來存取報價資料及要轉讓的權限的話，那麼便可施行此作業。於其中一具體實施例中，m1會在轉讓之後保留它的存取權利。較佳的係，可在限制條件下(而非永久性)來轉讓存取權利，如有限的時間、有限的存取次數、...、等。

圖14中所示的係產生一密鑰與密鑰ID的過程。該實體會經由一ACR來認證(方塊302)。該實體會要求產生一具有該主裝置所指定之ID的密鑰(方塊304)。該SSA會查看被指定的ACR是否有權來完成作業(菱形306)。舉例來說，倘若該

密鑰係要用於存取特殊分割區中的資料的話，該SSA便會查看該ACR是否可以存取此分割區。倘若該ACR被授權的話，那麼該記憶體裝置10便會產生一和該主裝置所提供之密鑰ID相關聯的密鑰值(方塊308)，並且將該密鑰ID儲存在該ACR之中，且將該密鑰值儲存在其記憶體(和控制器相關的記憶體或記憶體20)之中，並且依照該實體所提供的資訊來指派存取權利與權限(方塊310)，並且利用此等權利與權限來修改此ACR的PCR(方塊312)。因此，該密鑰的產生者會具有所有可用的權利，如讀取權限與寫入權限、轉讓及與相同AGP中其它ACR或下層處的其它ACR共享的權利、以及轉移該密鑰所有權的權利。

一ACR能夠改變該SSA系統中另一ACR的權限(甚至連同其存在性)，如圖15所示。一實體可如同前述般地經由一ACR來進入一樹；於其中一種情況中，該實體會被認證，然後其會指定一ACR(方塊330、332)。其會要求刪除一目標ACR或一目標ACR中的權限(方塊334)。倘若被指定的ACR或於此時呈主動狀態的ACR有權利來完成作業的話(菱形336)，那麼便會刪除該目標ACR，或者變更該目標ACR的PCR以刪除此權限(方塊338)。倘若未被授權的話，該系統便會停止。

經過上述過程之後，該目標將無法再存取其先前可存取的資料。如圖16所示，一實體可能會試圖從該目標ACR處進入(方塊350)，並且發現認證程序失敗，因為先前存在的ACR ID已經不存在於該SSA之中，所以該等存取權利便會

被拒絕(菱形352)。假設該ACR ID尚未被刪除，該實體便會指定一ACR(方塊354)以及一特殊分割區中的密鑰ID及/或資料(方塊356)，然後該SSA便會依照此ACR的PCR來查看該密鑰ID或分割區存取要求(菱形358)。倘若該權限已被刪除或逾期的話，那麼該項要求同樣會被拒絕。否則便會同意該項要求(方塊360)。

上面過程說明該裝置(舉例來說，快閃卡)如何管理受保護資料的存取作業，不管該ACR及其PCR是否被另一ACR改變或是否於初始時具此種配置。

交談

該SSA系統係被設計用來應付同時登入的多位使用者。此項特點必需規定該SSA所收到的每個命令均和一特定實體相關聯且僅在該用來認證此實體的ACR有權施行所要求的動作時才會被執行。

經由交談概念可支援多重實體。於認證程序期間會建立一交談且該SSA系統會指派一交談ID給該交談。該交談ID於內部係和用來登入該系統的ACR相關聯，且會被匯出給在所有進一步SSA命令中要被用到的實體。

該SSA系統支援兩種交談：開放式交談以及安全式交談。與一特定認證程序相關的交談類型會定義在ACR之中。該SSA系統會以和強化認證本身雷同的方式來強化交談的建立。因為該ACR會定義該等實體權限，所以，此機制可讓系統設計者將安全通道與存取特定密鑰ID產生關聯，或者將安全通道與施行特定ACR管理作業(也就是，產

生新的ACR及設計憑證)產生關聯。

開放式交談

開放式交談係一經由一交談ID來識別的交談，不過並未進行匯流排加密，所有的命令與資料均會安全地通過。此作業模式較佳的係可使用於多位使用者或多重實體的環境中，其中該等實體既非風險模型(threat model)的一部份，亦不會於匯流排上進行竊聽。

雖然並未保護資料的傳輸，亦未在主裝置端的各應用間建立有效的防火牆，不過，開放式交談模式卻仍讓該SSA系統僅能存取目前經過認證的ACR被允許存取的資訊。

該開放式交談還可用在必須保護分割區或密鑰的情況中。不過，在經過合法的認證程序後，便會同意該主裝置上所有的實體進行存取。各種主應用必須共享的唯一事物便係交談ID，以便取得該經認證ACR的權限。此作業圖解於圖17A。直線400上方的步驟係由主裝置24來施行。在一實體針對ACR1進行過認證之後(方塊402)，其便會要求存取記憶體裝置10中和密鑰ID X相關聯的檔案(方塊404、406、以及408)。倘若ACR 1的PCR允許進行此等存取的話，那麼裝置10便會同意該項要求(菱形410)。若不允許的話，那麼該系統便會返回方塊402。在完成認證之後，記憶體系統10便會僅利用被指派的交談ID(而非該等ACR憑證)來辨識發出命令的實體。一旦ACR 1同意存取和其PCR中的密鑰ID相關的資料的話，那麼於開放式交談中，任何其它應用或使用者便能夠藉由指定正確的交談ID(該交談ID係由主裝

置24上不同的應用來共享)來存取相同的資料。此項特點有利於下面的應用：使用者僅能登入一次，且可經由該次登入來存取和不同應用之帳號有關的所有資料。因此，蜂巢式電話使用者便可存取已儲存的電子郵件，並且聆聽記憶體20中所儲存的音樂，而不必進行多次登入。相反地，ACR 1未涵蓋的資料將無法存取。因此，相同的蜂巢式電話使用者便可經由不同的帳號ACR2來存取有價的內容，如遊戲以及照片。雖然該使用者並不介意其他使用者經由他的第一帳號ACR 1來存取可用的資料；不過該使用者卻不希望此資料會被向他借用電話的其他使用者取得。將資料存取分成兩個不同的帳號，同時允許於開放式交談中來存取ACR1，如此便可方便使用同時又可保護有價的資料。

為進一步解決於該等主應用間共享該交談ID的程序，當一ACR要求開放式交談時，其能夠特別要求指派「0(零)」ID給該交談。如此一來，便可將應用設計成使用一預定的交談ID。顯然地，唯一的限制係每次僅能認證一個要求交談0的ACR。倘若試圖認證另一個要求交談0的ACR的話，該項要求將會被拒絕。

安全式交談

為新增一安全層，可如圖17B所示般地使用該交談ID。接著，記憶體10還會儲存該等現用交談的交談ID。於圖17B中，舉例來說，為能夠存取和密鑰ID X有關的檔案，在允許該實體存取該檔案以前，該實體還必須提供一交談ID(如交談ID「A」)(方塊404、406、412、以及414)。依此方式，

除非該提出要求的實體知悉正確的交談ID，否則其便無法存取該記憶體10。因為該交談ID在該交談結束後便會被刪除，而且不同的交談會有不同的交談ID，所以，一實體僅在其能夠提供該交談數時方能進行存取。

該SSA系統若不使用該交談數便並無法確認一命令係確實來自經過正確認證的實體。於有入侵者(attacker)試圖利用一開放通道來傳送惡意命令之虞的應用與使用情況中，該主應用便可使用安全式交談(安全通道)。

當使用安全通道時，交談ID以及整個命令都會利用安全通道加密(交談)密鑰來進行加密，而且安全等級會和主裝置端的安全等級一般高。

終止交談

在下面的任一情形中會終止一交談，且該ACR會登出：

1.該實體發出一明確的end-session命令。

2.超過通信時間。一特定實體已經維持一段時間未發出任何命令，該段時間被定義為該等ACR參數中其中一項參數。

3.所有的開放式交談在裝置(舉例來說，快閃卡)重置及/或功率循環(power cycle)之後均被終止。

資料完整性服務

該SSA系統會驗證SSA資料庫(該資料庫含有所有的ACR、PCR、...、等)的完整性。此外，還會經由密鑰ID機制來為實體資料提供資料完整性服務。

倘若一密鑰ID利用雜湊模式作為其加密演算法來進行配

置的話，那麼該等雜湊值便會連同CEK與IV一起被儲存在該CEK記錄之中。雜湊值會在寫入作業期間被算出且儲存。在讀取期間會再次算出雜湊值，並且將其和先前寫入作業期間所儲存的數值作比較。每當該實體正在存取密鑰ID時，便會將額外的資料(以暗碼的方式)鏈接至舊資料及已更新的(用於讀取與寫入的)正確雜湊值。

因為僅有該主裝置知道和一密鑰ID有關或被一密鑰ID指到的資料檔案，所以，該主裝置會以下面的方式來明確地管理該資料完整性功能的數個方面：

1.從頭到尾來寫入或讀取和一密鑰ID有關或被一密鑰ID指到的資料檔案。希望存取該檔案其中一部份的任何試圖動作均會弄亂該檔案，因為該SSA系統係利用CBC加密法且會產生完整資料之經雜湊的訊息摘要。

2.不需要處理連續資料串中的資料(該資料串可能會與其它密鑰ID的資料串交錯且可分割於多次交談中)，因為SSA系統會保留中間的雜湊值。不過，倘若該資料串重頭開始的話，該實體則必須明確地指示該SSA系統來重置該等雜湊值。

3.當完成一讀取作業之後，該主裝置必須明確地要求該SSA系統藉由將所讀取的雜湊值與在寫入作業期間被算出的雜湊值作比較來驗證所讀取的雜湊值。

4.該SSA系統還會提供一「假讀取(dummy read)」作業。此項特點會讓資料流過加密引擎，但卻不會將其送出給主裝置。此項特點可於從該裝置(舉例來說，快閃卡)中實際讀

出資料前先用來驗證資料完整性。

亂數產生

該SSA系統將會讓外部實體運用內部的亂數產生器且索求一要在該SSA系統外部使用的亂數。此項服務可供任何主裝置使用且無需經過認證。

RSA密鑰對產生

該SSA系統將會讓外部使用者運用內部的RSA密鑰對產生特點且索求一要在該SSA系統外部使用的RSA密鑰對。此項服務可供任何主裝置使用且無需經過認證。

替代具體實施例

除了使用階層式的方式以外，利用資料庫型的方式亦可達到相同的結果，如圖18所示。

如圖18所示，於控制器12或記憶體20中所儲存的資料庫中可輸入一份由下面所組成的清單：實體的憑證、認證方法、最大的失敗試圖次數、以及用於解隔離所需要的最小憑證數，其會將此等憑證規定與該資料庫中由記憶體10之控制器12來施行的政策(讀取、寫入存取密鑰與分割區、安全通道規定)產生關聯。於該資料庫中還儲存著存取密鑰與分割區的條件與限制。因此，部份實體(舉例來說，系統管理者)可能係位於白名單(white list)中，其意謂著該些實體能夠一直存取所有的密鑰與分割區。其它實體有可能係位於黑名單(black list)中，該等實體對任何資訊的存取試圖均會被隔離。該限制可能係全域性，或者可能僅供特定的密鑰及/或分割區使用。此意謂著，僅有特定的實體能夠一直

存取特定的密鑰與分割區，而特定的實體則絕無法存取。亦可對內容本身加上約束，而不管該內容所在的分割區為何或者用來加密或解密該內容的密鑰為何。因此，特定的資料(舉例來說，歌曲)的屬性可能僅能被要存取該等資料的前面五個主裝置來存取；或者其它資料(舉例來說，電影)可能僅能被讀取有限次數，而不管哪個實體已經存取。

認證

密碼保護

· 密碼保護意謂著必須提出密碼方能存取被保護的區域。除非不能有一個以上的密碼，否則可有複數個密碼和不同的權利(如讀取存取或讀取/寫入存取)相關聯。

· 密碼保護意謂該裝置(舉例來說，快閃卡)能夠驗證主裝置所提供的密碼，也就是，該裝置同樣具有儲存在裝置管理安全記憶體區中的密碼。

問題與限制

· 密碼容易受到重播(replay)攻擊。因為密碼在每次提出後便不會改變，所以，可重覆地傳送相同的密碼。其意謂著，倘若要被保護的資料係有價的話便不能使用該密碼，且很容易存取該通信匯流排。

· 密碼能夠保護已儲存資料的存取作業，但卻不應該用來保護資料(其並非密鑰)。

· 為提高和密碼相關聯的安全等級，可利用一主密鑰來讓該等密碼呈現多變性，以便於其中一者遭到駭客攻擊時，並不會損毀整個系統。可利用交談密鑰型的安全通信

通道來傳送該密碼。

圖19為利用密碼進行認證的流程圖。該實體會於一帳號ID與密碼中傳送給系統10(舉例來說，快閃記憶卡)。該系統會查看該密碼是否和其記憶體中的密碼匹配。倘若匹配的話，便會返回已認證的狀態。否則，便遞增該帳號的誤差計數，且該實體會被要求重新輸入一帳號ID與密碼。倘若該計數溢位的話，該系統便會返回拒絕存取的狀態。

異議答覆(challenge response)

圖20為利用異議/答覆型的方法來進行認證的流程圖。該實體會送入一帳號ID並且向系統10索求一異議。系統10會產生一亂數並且提交給主裝置。該主裝置會從該數中算出一答覆，並且將其送至系統10。系統10將該答覆與所儲存的數值作比較。剩餘步驟均和圖19中所示者雷同，以便判斷是否同意存取。

圖21為利用另一種異議/答覆型的方法來進行認證的流程圖。圖21和圖20的不同處在於，除了要求系統10來認證該主裝置以外，還要求要由一異議/答覆來認證該系統10，其中系統10同樣會向該主裝置索求一異議並且送回一答覆來讓該主裝置查核。

圖22為利用另一種異議/答覆型的方法來進行認證的流程圖。於此情況中，僅系統10需要被認證，其中該主裝置會送交一異議給系統10，系統10會計算出一答覆供該主裝置查核，以便於其在系統10中的記錄中找出一匹配者。

對稱密鑰

對稱密鑰演算法意謂著於兩端均使用相同的密鑰來進行加密與解密。其意謂著該密鑰已於進行通信前便已被事先承認。另外，每一端還應該設計出彼此的逆演算法，也就是，於其中一端進行加密演算法而於另一端上進行解密。兩端並不必施行兩種演算法來進行通信。

認證

· 對稱密鑰認證意謂著裝置(舉例來說，快閃卡)與主裝置會共享相同的密鑰且具有相同的暗碼演算法(直接與逆向，舉例來說，DES與DES-1)。

· 對稱密鑰認證代表進行異議-答覆(避免受到重播攻擊)。受保護的裝置會產生另一裝置的異議，且兩部裝置均會算出答覆。進行認證的裝置會將該答覆送回，而受保護的裝置則會查核該答覆並且據此來驗證認證結果。接著，便可同意和認證相關聯的權利。

認證可能如下：

· 外部認證：該裝置(舉例來說，快閃卡)會認證外界的裝置，也就是，該裝置會驗證一特定主裝置或應用的憑證。

· 相互認證：於兩端均產生一異議。

· 內部認證：由該主應用來認證該裝置(舉例來說，快閃卡)，也就是，主應用會查核該裝置是否可用於其應用中。

提高整個系統的安全等級(也就是，破壞其中一者並不會破壞整個系統)

· 通常可利用一主密鑰來組合複數個對稱密鑰，使其呈現多變性

· 相互認證會使用來自兩端的異議，以便確保該異議為真正的異議。

加密

亦可利用對稱密鑰暗碼術進行加密，因為其係一種很有效的演算法，也就是，不需要一強大功能的CPU便可處理該暗碼術。

當用來確保一通信通道的安全時：

· 兩部裝置均必須知道用來確保該通道安全的交談密鑰(也就是，對所有外送資料進行加密且對所有進入資料進行解密)。此交談密鑰通常係利用一事先共享的秘密對稱密鑰來建立或利用PKI來建立。

· 兩部裝置均必須知道且設計相同的暗碼演算法。

簽章

對稱密鑰還可用來對資料進行簽章。於此情況中，該簽章會係加密的部份結果。保持部份的結果可於多次進行簽章，而不會洩漏該密鑰值。

問題與限制

對稱演算法係非常有效且安全的演算法，不過，必須依據一事先共享的秘密。其問題係要以動態的方式來共享此秘密並且使其保持隨機(random)(如同交談密鑰)。其概念為，共享的秘密便很難長期地保有安全性，且幾乎不可能和多人共用。

為促成此項作業，已經有人發明公眾密鑰演算法，其允許交換秘密而不必共享該等秘密。

公眾密鑰暗碼術

非對稱密鑰演算法通常稱為公眾密鑰暗碼術。其係一種非常複雜且通常需要眾多CPU的算術施行方式。已經有人提出發明，用來解決和對稱密鑰演算法相關聯的密鑰散佈的問題。其還提供簽章功能，用於確保資料完整性。

非對稱密鑰演算法會用到一具有私有元素與公眾元素的密鑰，該等私有元素與公眾元素分別稱為私有密鑰與公眾密鑰。私有密鑰與公眾密鑰兩者會以算術方式連結在一起。公眾密鑰係可被共享的密鑰，而私有密鑰則必須保持隱密。就該等密鑰來說，非對稱演算法會用到兩個算術函數(一者用於私有密鑰，一者用於公眾密鑰)，以便進行包封(wrap)與解封(unwrap)或者簽章與驗證。

密鑰交換與密鑰散佈

利用PK演算法，密鑰交換會變得非常簡單。該裝置會將它的公眾密鑰送至另一裝置。該另一裝置會利用該公眾密鑰對它的秘密密鑰進行包封，並且將加密後的資料回傳給該第一裝置。該第一裝置會利用它的私有密鑰來為該資料進行解封並且取出該秘密密鑰，此時兩端便都知道該秘密密鑰，並且能夠利用該秘密密鑰來交換資料。因為可如此簡單地交換該對稱密鑰，所以，其通常係一隨機密鑰。

簽章

因為本質的關係，公眾密鑰演算法通常僅用來對小型資料進行簽章。為確保資料完整性，其接著會結合一雜湊函數，該雜湊函數會提供該訊息的單向足印(one-way foot

print)。

該私有密鑰可用來對該資料進行簽章。公眾密鑰(可隨意取用)則可用來驗證該簽章。

認證

認證通常會用到簽章：一異議會被簽章且送回，以進行驗證。

該密鑰的公眾部係供驗證用。因為任何人均能夠產生一密鑰對，所以，必須證明該公眾密鑰的擁有者，方能假設此人可使用此正確密鑰。證明機關(certificate authority)會提供證明作業且將該公眾密鑰包含於一經簽章的證書中。該證書係由該機關本身來簽章。接著，會利用一公眾密鑰來驗證簽章，其意謂著，核發含有該密鑰之證書的機關可被信賴，且該機關能夠證明該證書並未遭到駭客攻擊，也就是，經由該機關簽章的雜湊證書係正確無誤的，其意謂著，該使用者同樣具有且信賴該授權公眾密鑰證書。

最常見用來提供PK認證的方式係信賴該機關或根證書，而不直接信賴經該特定機關證實的所有密鑰對。接著，認證的前提便在於該實體所擁有的私有密鑰匹配該證書，其方式係對一異議進行簽章且提供異議答覆以及證書。接著，便查核該證書，以確保其必未遭到駭客攻擊且經過值得信賴的機關簽章。接著，便會驗證該異議答覆。倘若該證書被信賴且該異議答覆正確的話，那麼便認證成功。

一裝置(舉例來說，快閃卡)中的認證意謂著該裝置載有可信賴的根證書，且該裝置能夠驗證該異議答覆以及該經

證書簽章的雜湊。

檔案加密

PK演算法並不能用來加密大型的資料，因為必須耗用大量的CPU，不過卻通常用於保護用來加密該內容的隨機式加密/解密密鑰。舉例來說，SMIME(安全電子郵件)會產生一密鑰，接著便會利用所有收信者的公眾密鑰來對該密鑰進行加密。

問題與限制

因為任何實體均可產生一密鑰對，所以必須對其進行證實方能確保其出處(origin)。於密鑰交換期間，可能會希望確保該秘密密鑰會被送至正確的裝置，也就是，必須檢查所提供之公眾密鑰的出處。接著，證書管理便會成為安全性的一部份，因為其能夠提供和該密鑰之合法性有關的資訊，並且提供該密鑰是否已經被撤銷的資訊。

雖然上文已經參考各種具體實施例來說明本發明，不過，應該瞭解的係，可在不脫離本發明範疇下對本發明進行變更與修正，其中本發明範疇僅由隨附的申請專利範圍及等效範圍來界定。本文以引用的方式併入下文所有參考資料。

【圖式簡單說明】

圖1為一根據本發明之和主裝置進行通信的記憶體系統的方塊圖。

圖2為一根據本發明一具體實施例的記憶體不同分割區以及不同分割區中所儲存的未加密檔案與已加密檔案的概

略示意圖，其中特定分割區及加密檔案的存取係受控於存取政策與認證程序。

圖3為一記憶體中不同分割區的概略示意圖。

圖4為根據本發明一具體實施例圖3中所示之記憶體的不同分割區的檔案配置表的概略示意圖，其中該等分割區中的部份檔案會經過加密。

圖5為根據本發明一具體實施例一存取受控記錄群中的存取控制記錄以及相關聯的密鑰參考值的概略示意圖。

圖6為根據本發明一具體實施例由存取受控記錄群以及存取受控記錄所構成的結構的概略示意圖。

圖7為一樹的概略示意圖，圖中圖解三棵由複數存取受控記錄群所組成的階層樹，用以圖解該等樹的構成過程。

圖8A與8B為流程圖，用以圖解一主裝置與一記憶體裝置(如記憶卡)產生與使用一系統存取控制記錄所執行的過程。

圖9為一根據本發明的流程圖，用以圖解使用一系統存取控制記錄來產生一存取受控記錄群的過程。

圖10為一用於產生一存取控制記錄之過程的流程圖。

圖11為用於圖解該階層樹之特殊應用的兩種存取控制記錄群的概略示意圖。

圖12為一轉讓特定權利之過程的流程圖。

圖13為一存取受控記錄群與一存取控制記錄的概略示意圖，用於圖解圖12之轉讓過程。

圖14為圖解用於產生一密鑰以達加密及/或解密之目的之過程的流程圖。

圖15為依照一存取受控記錄來移除資料存取權利及/或權限之過程的流程圖。

圖16為當存取權利及/或權限已經被刪除或逾期時，用來要求存取的過程的流程圖。

圖17A與17B為根據本發明另一具體實施例，用於驗證之規則結構以及用於准予存取暗碼密鑰之政策的概略示意圖。

圖18為開啟部份交談時，驗證交談與存取交談的流程圖。

圖19至22為不同驗證過程的流程圖。

為簡化說明，本申請案中相同的組件會以相同的符號來表示。

【主要元件符號說明】

10	記憶體系統
10'	記憶卡或記憶棒
12	中央處理單元
12a	中央處理單元隨機存取記憶體
14	緩衝器管理單元
16	主介面模組
18	快閃介面模組
20	快閃記憶體
22	週邊存取模組
24	主裝置
26	主介面匯流排
26a	埠

28	快閃介面匯流排
28a	埠
32	主直接記憶體存取
34	快閃直接記憶體存取
36	仲裁器
38	緩衝器隨機存取記憶體
40	加密引擎
101	檔案
102	檔案
104	檔案
106	檔案

附件A

1 SSA命令

該等SSA系統命令會被送至用到標準寫入與讀取命令(用於相關的外型因數協定(form factor protocol))的記憶卡中。所以，從主裝置的觀點來說，傳送一SSA命令的真正意涵係將資料寫入該記憶體裝置上作為緩衝檔案的一特殊檔案之中。從SSA系統中取得資訊可透過從該緩衝檔案中讀取資料來完成。該主應用必須確保必定係從該緩衝檔案的第一LBA處進行資料的寫入與讀取。管理主裝置OS中的緩衝檔案已經超出本說明的範疇。

1.1 和SSA系統進行通信

下面章節會定義如何利用該等外型因數標準寫入/讀取命令來與SSA系統交換SSA相關的命令與資料。

1.1.1 傳送命令/資料給SSA系統

每個寫入命令的第一個資料區塊均會被掃描，以尋找一穿透(pass through)簽章。若有找到的話，該資料便會被解釋為SSA命令。若未找到的話，該資料便會被寫入所指定的位址中。

SSA應用特定寫入命令可能包含多區段傳輸，其中第一區段會保有必要的簽章與命令的引數，而剩餘的資料區塊則會保有相關的資料(若有的話)。

表...定義一SSA命令的第一區塊的格式(於標準OS檔案系統中，資料區塊必定係512個位元組)。

位元組編號	長度[位元組]	說明	註解
0-31	32	應用穿透簽章	必須係ASCII字串：「支援SSTA穿透模式」
32	4	SSA應用ID	必須係：0x00000000
36	4	SSA交談ID	SSA交談ID由SSA系統經由認證程序來提供。倘若沒有任何交談係開放式交談的話，此欄位便應該含有數值0x00000000。當用到一安全通道時，便利用交談密鑰來加密剩餘的命令引數(始於第一區塊的位元組偏移64處)及資料區塊。
40	24	保留以後使用	資料未定義
64	4	SSA交談ID	SSA交談ID的第二複本。本欄位係用來驗證交談密鑰的使用。
68	4	SSA應用命令op-Code	定義於下面章節中的詳細SSA命令說明中
72	4	SSA應用資料區塊	額外資料區塊的數量。若未用到任何資料區塊的話則為0。
76-511	436	SSA應用命令引數	定義於下面章節中的詳細SSA命令說明中。

表1：SSA命令引數LBA格式

1.1.2 從SSA系統中讀取資料

讀取命令將會以下面兩個部份來執行：

1.先送出一具有單一資料區塊的寫入命令來定義該讀取命令的所有引數，以發出該讀取命令。

2.於該寫入命令將該卡應用設定在正確的傳輸狀態後，利用一讀取命令從該卡進行真實的資料傳輸至該主裝置。該讀取命令所利用的LBA位址必須和先前寫入命令所用的LBA位址相同。此為送至該卡的唯一指示信號，用以表示

該主裝置正試圖取得先前所要求的SSA資料。

該寫入/讀取命令對必須謹慎地同步化。下一次交談會定義如何處理序列錯誤及如何還原。如定義，SSA系統支援多位主端使用者，該等使用者可同時登入。每位使用者均預期可獨立且非同步地發出寫入/讀取命令對，從而不需要該主OS實施任何特殊作用。從該卡的觀點來說，可藉由寫入該序列所用的LBA位址來辨識該些個別的寫入/讀取命令對。從該主裝置的觀點來說，其意謂著每位使用者均必須利用一不同的檔案緩衝器。

1.1.3 寫入/讀取序列錯誤

1.2 命令詳細說明

表2為SSA命令的總覽。命令名稱行對命令的用途作基本的說明，同時索引至該命令的詳細說明。命令op-code為用於SSA命令中的實際值。引數長度(Arg Len)行則定義該命令的引數欄的大小(零表示沒有引數)。該等引數係命令特有的，且會在詳細的命令說明中指出。

資料長度為和該等命令相關聯的額外資料區塊中的命令資料的大小。零表示沒有任何資料，「Var」值表示該命令具有變動的資料大小且實際大小係由該命令本身來指定。對固定大小的資料命令來說，此行則儲存該資料大小值。資料方向可能係：空白，倘若該命令沒有任何資料的話(其意謂著表1中指定的命令引數全部落在位元組76與位元組511之間的空間中，此範圍以外者為伴隨該命令部的資料酬載)；「寫入」，倘若資料係從主裝置移至該卡的話(附加在該

寫入命令的引數區塊中)；或「讀取」，倘若資料係從該卡移至該主裝置的話(於提供該等引數的寫入命令後面的讀取命令中，如上述)。

所有大小相關的行均以位元組為單位。

Cmd Op-code	Cmd 名稱	Arg Len	資料 Len	資料 Dir	說明
ACR/AGP管理命令					
1	CREATE_SYSTEM ACR	1	0		於SSA資料庫中產生一系統ACR進入點，並且啟動該系統ACR配置序列
2	SYS_ACR_ CREATION_DONE	0	0		終止該系統ACR配置序列且讓該系統ACR發揮作用
3	PASSWORD_ CREDENTIAL			寫入	為使用密碼認證的ACR提供憑證資料
4	SYMMETRIC_ CREDENTIAL			寫入	為使用對稱認證的ACR提供憑證資料
5	ASYMETRIC_ CREDENTIAL			寫入	為使用非對稱認證的ACR提供憑證資料
6	GET_ACR_ PUBLIC_KEY			寫入	由CA取得一ACR的公眾密鑰以進行簽章。當產生該ACR時產生於該SSA系統中的ACR RSA密鑰對。
7	SEND_CERTIFICATE			讀取	提供一證書以簽章該ACR公眾密鑰
8	CONFIGURE_ACAM			寫入	設定一ACR的ACAM(ACR管理權限)記錄。
9-15	保留以後使用				
16	CREATE_ROOT_ AGP			寫入	於SSA系統資料庫中產生一根AGP進入點
17	ROOT_AGP_ CREATION_DONE	0	0		終止一根AGP的配置程序且讓它發揮作用

18	DISBALE_SYSTEM_ ACR_CREATION	0	0		取消產生與配置系統ACR的特點
19	SET_ROOT_AGP_ CREATION_MODE	1			定義根AGP產生的模式(開放模式、受控模式、或阻隔模式)
20	DISBALE_ROOT_ AGP_CHANGE_ MODE				取消改變根AGP之產生模式的特點
21-25	保留以後使用				
26	CREATE AGP			寫入	於SSA系統資料庫中產生一AGP進入點
27	DELETE AGP			寫入	於SSA系統資料庫中刪除一AGP進入點
28	CREATE_ACR			寫入	於SSA系統資料庫中產生一ACR進入點
29	CREATE_ACR_DONE	0	0		終止一ACR的產生與配置程序且讓它發揮作用
30	DELETE_ACR			寫入	於SSA系統資料庫中刪除一ACR進入點
31	UNBLOCK_ACR			寫入	解隔離一(因認證失敗)被隔離的ACR
32-49	保留以後使用				
分割區&域管理命令					
50	CREATE_PARTITION			寫入	本命令會將一特定分割區分割成兩個。本命令僅能由根ACR發出。
51	UPDATE_PARTITION			寫入	改變兩個既有分割區的大小。此兩個分割區之總大小的淨變化必須為0。
52	DELETE_PARTITION			寫入	將兩個既有分割區合併成一個。

53	RESTRIC_PUBLIC_ PARTITION_ACCESS			寫入	致能/取消利用標準(非SSA)命令來存取該裝置之公眾分割區的ac。
54-59	保留以後使用				
60	CREATE_DOMAIN			寫入	於SSA資料庫中產生一安全域
61	DELET_DOMAIN			寫入	刪除SSA資料庫中的一安全域
62-69	保留以後使用				
70	DELEGATE_DOMAIN _PERMISSIONS			寫入	轉讓一域的存取與所有權權限給一特定ACR
71	DELEGATE_ PARTITION_ PERMISSION			寫入	轉讓一分割區的存取權限給一特定ACR
72-99	保留以後使用				
系統登入與認證命令					
100	SYSTEM_LOGIN			寫入	
101	SYSTEM_LOGOUT	0	0		
102-109	保留以後使用				
110	SEND_PASSWORD TO SSA			寫入	
111-119	保留以後使用				
121	GET_SYMETRIC_ CHALLENGE			讀取	
122	SEND_SYMETRIC_ CHALLENGE			寫入	
123	GET_SYMETRIC_ CHLLENGE_ RESPONSE			讀取	
124	SEND_SYMETRIC_ CHLLENGE_ RESPONSE			寫入	

125-129	保留以後使用				
130	SEND_ASYMETRIC_ CHALLENGE			寫入	
131	GET_ASYMTERIC_ CHALLENGE			讀取	
132	SEND_USER_ CERTIFICATE			寫入	
133	GET_SSA_PRE_ MASTER_SECRETE			讀取	
134	GET_ACR_ CERTIFICATE			讀取	
135	SEND_HOST_PRE_ MASTER_SECRET			寫入	
136	START_SERSSION			寫入	
137	AHUTHENTICATION _COMPLETE	0	0	讀取	
138-199	保留以後使用				
讀取寫入與狀態命令					
200	WRITE		Var	寫入	寫入資料命令
201	READ		Var	讀取	讀取資料命令
202	COMMAND_STATUS		Var	讀取	取得目前的SSA命令執行狀態
203	SYSTEM_QUERY		Var	讀取	取得該提出要求的ACR的目前配置資料

表2：SSA命令

1.2.1 Create System ACR

Create System ACR會於SSA資料庫中建立一系統ACR進入點。一旦產生該進入點之後，便可依照指定登入演算法來配置該等憑證。

最後可利用CREATE_SYSTEM_ACR_DONE命令來終止該序列且讓該系統ACR發揮作用。

倘若ACR進入點已經存在或產生系統ACR特點被取消的話，便會拒絕Create System ACR命令。系統ACR僅可利用可用登入模式所構成的子集來進行配置(詳情請參考第1.3.2節)。倘若用到不合法的模式的話，該命令將會被拒絕。

表3為命令引數。位元組偏移係以命令引數LBA的起點為準(參見第1.1.1節)。引數長度係以位元組數為單元。引數名稱定義的係該引數的用途，且可索引至詳細的引數說明。

位元組偏移	引數長度	引數名稱	註解
76	1	Login Algorithm	系統ACR僅能利用下面的登入演算法進行配置： • AES、DES、3DES、相互非對稱認證模式。

表3：Create System ACR命令引數

1.2.2 System ACR Creation Done

本命令僅在開始進行系統ACR產生之後才會被送出。在其它時候，該命令均會被拒絕。傳送本命令會結束系統ACR產生作業，且會讓該ACR永久保持目前的配置。

本命令沒有任何引數。

1.2.3 PASSWORD_CREDENTIAL

在傳送SSA命令[28]，CREATE_ACR，之後，便會接著傳送該ACR的憑證。於此情況中為具有特定長度的密碼，最大的位元組長度為20。

位元組偏移	引數長度	引數名稱	註解
76	指定於Password Length in Bytes引數欄位中。	PASSWORD_CREDENTIAL	參見第1.3.2節有關密碼詞組格式與長度的部份。

表4：Password Credential命令引數

1.2.4 SYMMETRIC CREDENTIAL

當針對一ACR進行對稱登入程序時，便會接著以AES、DES或3DES密鑰的形式來傳送該ACR的對稱憑證。該演算法的本質會以位元組來表示該憑證的(密鑰)長度。在正常的ACR與系統ACR的產生時便會用到本命令。

表13說明不同類型的非對稱憑證。

位元組偏移	引數長度	引數名稱	註解
76	1	Credential Type	參見表13關於類型值與符號
78	1	Credential Length in Bytes	
79	指定於Credential Length in Bytes欄位中	Symmetric Credential	

表5：Symmetric Credential命令引數

1.2.5 ASYMETRIC CREDENTIAL

對一具有非對稱登入程序的ACR來說，必須傳送數個憑證給SSA。下面的表14說明不同類型的非對稱憑證：

位元組偏移	引數長度	引數名稱	註解
76	1	Session ID	有Session ID便無需ACR ID。當於系統ACR產生的情況中，本欄位會保持NULL。
77	1	Credential Type	參見類型碼
78	1	Credential Length in Bytes	
79	指定於Credential Length in Bytes欄位中。	Symmetric Credential	

表6：Asymmetric Credential命令引數

1.2.6 EXPORT PUBLIC KEY

1.2.7 IMPORT CERTIFICATE

1.2.8 CONFIGURE ACAM

傳送本命令會配置該等ACR管理權限。本命令僅會於進行動儲存裝置ACR產生期間才會被傳送。本命令不適用於系統ACR。ACAM類型與代碼描述在表16之中：ACAM類型

位元組偏移	引數長度	引數名稱	註解
76	1	Session ID	僅適用於施行過系統ACR登入程序的後面。 否則便保持NULL。
77	1	AGP NAME/ID Length in Bytes	最大長度為20個位元組。
78	指定於AGP NAME/ID Length in Bytes引數欄位中。	AGP NAME/ID	

表7：Configure ACAM命令引數

1.2.9 Create Root AGP

為於一安全通道下產生一根AGP，一SSA系統會經由必須被執行的系統ACR來登入。登入後，便會產生一交談ID且用於產生序列。當於完成系統ACR登入序列後要求系統命令回傳狀態權利時，便可用到該交談ID。

產生一根AGP而未先登入該系統ACR(具有一安全通道的CREATE_ROOT_AGP)則不需要一交談ID。

表8為命令引數。當未使用該系統ACR時，交談ID欄位便會保留NULL(NA)。AGP name/ID前面則係它的長度位元組數。

位元組偏移	引數長度	引數名稱	註解
76	1	Session ID	僅適用於施行過系統ACR登入程序的後面。否則便保持NULL。
77	1	AGP NAME/ID Len in Bytes	最大長度為20個位元組。
78	指定於AGP NAME/ID Length in Bytes引數欄位中。	AGP NAME/ID	

表8：Create Root AGP命令引數

命令結構：

- Command Name/OP Code-1個位元組：SSA_CREATE_ROOT_AGP_CMD [3]
- 命令引數

  1. Session ID - is it needed???
  2. AGP Name/ID Length in Bytes-1個位元組
  3. AGP Name/ID

1.2.10 Root AGP Creation Done

當完成該根AGP之後便會送出本命令，其意謂著已經產生該AGP中的所有ACR。本命令會鎖定該AGP，使其無法再產生任何的ACR。

本命令無引數。

命令結構：

- Command Name/OP Code-1個位元組：SSA_ROOT_AGP_CREATION_DONE_CMD [4]
- 命令引數-

1. Session ID - is it needed???
2. AGP Name/ID Length in Bytes-1個位元組
3. AGP Name/ID

1.2.11 DISBALE SYSTEM_ACR_CREATION

送出本命令將會終止產生系統ACR的功能。

本命令無引數。

1.2.12 SET_ROOT AGP_CREATION MODE

控制根AGP的產生係由SSA命令[19]SET_ROOT_AGP_CREATION_MODE來負責。表9中說明不同模式的代碼。本命令無須登入SSA，所以並不需要任何Session ID。

模式名稱	代碼	說明
開放模式	1	根AGP產生可經由系統ACR或正常的開放通道。
受控模式	2	根AGP產生僅可經由系統ACR。
鎖定模式	3	不能產生任何的根AGP。

表9：根AGP產生模式

位元組偏移	引數長度	引數名稱	註解
76	1	Root AGP Creation Mode	

表10：Set Root AGP Creation Mode命令引數

1.2.13 DISBALE_ROOT_AGP_CHANGE_MODE

本命令會讓SET_ROO_AGP_CREATION_MODE命令無法運作且會被SSA拒絕。本命令沒有引數。

1.2.14 Create AGP

位元組偏移	引數長度	引數名稱	註解
76	1	Session ID	
77	1	AGP Name/ID Length in Bytes	最大長度為20個位元組。
78	指定於AGP NAME/ID Length in Bytes引數欄位中。	AGP Name/ID	

表11：Create AGP命令引數

命令結構：

- Command Name/OP Code-1個位元組：SSA_CREATE_AGP_CMD [5]
- 命令引數-

1. Session ID-1個位元組

2. AGP Name/ID Length in Bytes-1個位元組

3. AGP Name/ID

1.2.15 Delete AGP

本命令適用於已產生AGP的ACR中，前提係ACR必須係空乏的。

命令結構：

- Command Name/OP Code-1個位元組：SSA_DELETE_AGP_CMD [6]
- 命令引數-

1. Session ID-1個位元組

2. AGP Name/ID Length in Bytes-1個位元組

3. AGP Name/ID

1.2.16 Create ACR

命令結構：

- Command Name/OP Code-1個位元組：SSA_CREATE_ACR_CMD [7]
- 命令引數-

1. AGP Name/ID

2. ACR Name/ID

3. Login Algorithm - 1個位元組

4. Key Length

5. Unblocking ACR Name/ID

6. Number of Management Rights (ACAM) - 1個位元組

7. ACAM #1

8. ACAM #n

1.2.17 Uadate ACR

本命令僅能由ACR產生者來傳送，用以更新子部ACR。位在根AGP中的ACR無法被更新，因為它們並沒有父部ACR。

命令結構：

- Command Name/OP Code-1個位元組：SSA_UPDATE_ACR_CMD [8]
- 命令引數-

1. Session ID-1個位元組
2. AGP Name/ID Length in Bytes-1個位元組
3. AGP Name/ID
4. ACR Name/ID Length in Bytes-1個位元組
5. ACR Name/ID

1.2.18 Delete_ACR

本命令僅能由ACR產生者來傳送，用以刪除子部ACR。位在根AGP中的ACR無法刪除本身。

命令結構：

- Command Name/OP Code-1個位元組：SSA_DELETE_ACR_CMD [9]
- 命令引數-

1. Session ID-1個位元組
2. AGP Name/ID Length in Bytes-1個位元組

3. AGP Name/ID

4. ACR Name/ID Length in Bytes-1個位元組

5. ACR Name/ID

1.2.19 Unblock ACR

本命令僅能由具有此明確權限的ACR來傳送，用以解隔離一特定ACR。

命令結構：

- Command Name/OP Code-1個位元組：SSA_UNBLOCK_ACR_CMD [10]
- 命令引數-

1. Session ID-1個位元組
2. AGP Name/ID Length in Bytes-1個位元組
3. AGP Name/ID
4. ACR Name/ID Length in Bytes-1個位元組
5. ACR Name/ID

1.2.20 Delecrate Domain Permissions

命令結構：

- Command Name/OP Code-1個位元組：SSA_DELEGATE_DOMAIN_PERMISSION_CMD [11]
- 命令引數-

1. Session ID-1個位元組
2. Number of Permissions to Delegate-1個位元組
3. Delegated Permission Code
4. Domain Name/ID Length in Bytes-1個位元組

5. Domain Name/ID

1.2.21 Create Partition

本命令僅能由位於根AGP中的ACR來傳送。

命令結構：

- Command Name/OP Code-1個位元組：SSA_CREATE_PARTITION_CMD [12]
- 命令引數-
  1. Session ID-1個位元組
  2. Partition Name/ID Length in Bytes-1個位元組
  3. Partition Name/ID
  4. Partition Size in Sectors [512個位元組]-4個位元組
  5. Decreased Partition Name/ID Length in Bytes-1個位元組
  6. Decreased Partition Name/ID

1.2.22 Update Partition

本命令僅能由位於根AGP中的ACR來傳送。

命令結構：

- Command Name/OP Code-1個位元組：SSA_UPDATE_PARTITION_CMD [13]
- 命令引數-
  1. Session ID-1個位元組
  2. Partition Name/ID Length in Bytes-1個位元組
  3. Partition Name/ID
  4. Partition Size in Sectors [512個位元組]-4個位元組

5. Decreased Partition Name/ID Length in Bytes-1個位元組

6. Decreased Partition Name/ID

1.2.23 Delete Partition

本命令僅能由位於根AGP中的ACR來傳送。

命令結構：

- Command Name/OP Code-1個位元組：SSA_DELETE_PARTITION_CMD [14]
- 命令引數-

1. Session ID-1個位元組
2. Partition Name/ID Length in Bytes-1個位元組
3. Partition Name/ID

1.2.24 Restrict Public Domain Access

本命令將會限制送至/來自公眾分割區(又稱使用者區)的正常讀取/寫入命令(由主裝置送出且並非係SSA命令協定一部份的命令)。

命令結構：

- Command Name/OP Code-1個位元組：SSA_RESTRICT_PAUBLIC_PARTITION_CMD [15]
- 命令引數

1. Session ID-1個位元組
2. Public Partition Restriction Code-1個位元組

1.2.25 Create Domain

命令結構：

- Command Name/OP Code-1個位元組：SSA_CREATE_OMAIN_CMD [16]
- 命令引數
  1. Session ID-1個位元組
  2. Partition Name/ID Length in Bytes-1個位元組
  3. Partition Name/ID
  4. Domain Name/ID Length in Bytes-1個位元組
  5. Domain Name/ID

1.2.26 Delete Domain

僅有域主(domain owner)可傳送此命令且刪除某一域。

命令結構：

- Command Name/OP Code-1個位元組：SSA_DELETE_DOMAIN_CMD [17]
- 命令引數-
  1. Session ID-1個位元組
  2. Partition Name/ID Length in Bytes-1個位元組
  3. Partition Name/ID
  4. Domain Name/ID Length in Bytes-1個位元組
  5. Domain Name/ID

1.2.27 Svstem Loqin

當主裝置使用者希望經由其中一個ACR來使用該SSA系統時，便會發出本命令。本命令將會啟動登入/認證程序。

命令結構：

- Command Name/OP Code-1個位元組：SSA_SYSTEM_

LOGIN_CMD [18]

- 命令引數-

1. AGP Name/ID Length in Bytes-1個位元組
2. AGP Name/ID
3. ACP Name/ID Length in Bytes-1個位元組
4. ACR Name/ID

1.2.28 System Logout

當主裝置使用者希望終止一正與該SSA系統進行中的交談時，便會發出本命令。本命令會針對目前的登入交談來結束所有的使用者活動。於本命令之後，主裝置使用者便必須再次啟動登入程序，方能執行與該SSA系統有關的進一步動作。

命令結構：

- Command Name/OP Code-1個位元組：SSA_SYSTEM_LOGOUT_CMD [19]
- 命令引數-

1. AGP Name/ID Length in Bytes-1個位元組
2. AGP Name/ID
3. ACR Name/ID Length in Bytes-1個位元組
4. ACR Name/ID

1.2.29 Read

命令結構：

- Command Name/OP Code-1個位元組：SSA_READ_CMD [20]

- 命令引數-

1. Session ID-1個位元組
2. Partition Name Length in Bytes-1個位元組
3. Partition Name
4. Domain Name Length in Bytes-1個位元組
5. Domain Name
6. Partition Address (LBA) - 4個位元組
7. Number of LBAs (Sectors - Sector=512個位元組) to read-4個位元組

1.2.30 Write

命令結構：

- Command Name/OP Code-1個位元組：SSA_WRITE_CMD [21]
- 命令引數-

1. Session ID-1個位元組
2. Partition Name Length in Bytes-1個位元組
3. Partition Name
4. Domain Name Length in Bytes-1個位元組
5. Domain Name
6. Partition Address (LBA)-4個位元組
7. Number of LBAs (Sectors-Sector=512個位元組) to read - 4個位元組

1.2.31 Command Status

送出本狀態命令時可取得前面送出之命令的回傳狀態。

該狀態係關於該命令處理及SSA系統狀態。

命令結構：

- Command Name/OP Code-1個位元組：SSA_CMD_STATUS_CMD [22]
- 命令引數-

1. Session ID-1個位元組

1.2.32 System Query

本System Query命令會讀取落在被登入之ACR的範圍中的SSA資訊。

命令結構：

- Command Name/OP Code-1個位元組：SSA_SYS_QUERY_CMD [23]
- 命令引數-

1. Session ID-1個位元組

1.2.33 密碼認證命令

1.2.33.1 Send Password To SSA

本命令會傳送要被該SSA驗證的真實ACR密碼。傳送Command Status命令(22)，主裝置便能夠讀取命令狀態，且能夠於命令完成時讀取該認證程序的狀態-成功/失敗(PASS/FAIL)。

命令結構：

- Command Name/OP Code-1個位元組：SSA_PWD_AUTH_SEND PWD_CMD [24]
- 命令引數-

1. Password Length in Bytes-1個位元組

2. Password Data

1.2.34 對稱認證命令

1.2.34.1 Get Challenge from SSA

命令結構：

- Command Name/OP Code-1個位元組：SSA_SYM_AUTH_GET_CHLG_CMD [25]
- 命令引數

1.2.34.2 Send Challenge to SSA

命令結構：

- Command Name/OP Code-1個位元組：SSA_SYM_AUTH_SEND_CHLG_CMD [26]
- 命令引數

1.2.34.3 Get Challenge Response from SSA

命令結構：

- Command Name/OP Code-1個位元組：SSA_SYM_AUTH_GET_CHLG_RES_CMD [27]
- 命令引數

1.2.34.4 Send Challenge Response from SSA

命令結構：

- Command Name/OP Code-1個位元組：SSA_SYM_AUTH_SEND_CHLG_RES_CMD [28]
- 命令引數

1.2.35 非對稱認證程序命令

1.2.35.1 Send Challenge to SSA

命令結構：

- Command Name/OP Code-1個位元組：SSA_ASYM_AUTH_SEND_CHLG_CMD [29]
- 命令引數-Challenge random number - 28個位元組

1.2.35.2 Get Challenge from SSA

命令結構：

- Command Name/OP Code-1個位元組：SSA_ASYM_AUTH_GET_CHLG_CMD [30]
- 命令引數-NA

1.2.35.3 Send CA Certificate to SSA

命令結構：

- Command Name/OP Code-1個位元組：SSA_ASYM_AUTH_SEND_CA_CERT_CMD [31]
- 命令引數

1.2.35.4 Get SSA Pre-Master Secret

命令結構：

- Command Name/OP Code-1個位元組：SSA_ASYM_AUTH_GET_PRE_MASTER_SECRET_CMD [32]
- 命令引數

1.2.35.5 Get ACR Certificate from SSA

命令結構：

- Command Name/OP Code-1個位元組：SSA_ASYM_AUTH_GET_CHLG_CMD [33]

- 命令引數

1.2.35.6 Send Host Pre-Master Secret to SSA

命令結構：

- Command Name/OP Code-1個位元組：SSA_ASYM_AUTH_SEND_PRE_MASTER_SECRET CMD [34]
- 命令引數

1.2.35.7 Send Start Session Massage

命令結構：

- Command Name/OP Code-1個位元組：SSA_ASYM_AUTH_SEND_START_SESSION_MSG_CMD [35]
- 命令引數-

1. PIN option
2. PIN Length in Bytes
3. PIN string

1.2.35.8 Get Authentication Complete Massage from SSA

命令結構：

- Command Name/OP Code-1個位元組：SSA_SYM_AUTH_GET_CHLG_CMD [36]
- 命令引數

1.3 SSA命令引數

1.3.1 Not Applicable

引數清單中被定義成Not Applicable(NA)的所有欄位均必須設定成0。

1.3.2 Password and PIN Structure

密碼與PIN詞組長度為20個位元組，且係以二進制值的方式送入該SSA系統中。短於20個位元組的任何詞組均必須添加「0」。

「0」填補							詞組											
MSB 19																		LSB 0
00	00	00	00	00	00	00	49	F3	70	15	CC	52	74	A1	EC	2B	00	01	05

1.3.3 Login Alogrithm

此引數定義一ACR的登入演算法。其長度為1個位元組。可用數值定義於下表中：

符號	數值	說明
NONE	0	不需要認證。當發出此ACR的系統登入命令之後便立即開啟交談。
PASSWORD	1	密碼型認證
保留以後使用	2-9	
AES_HOST_AUTH	10	利用AES演算法的單向對稱認證。卡為認證使用者。
AES_HOST_AUTH_SEC	11	利用AES演算法的單向對稱認證。卡為提供認證的使用者。 建立安全通道且供此ACR使用。
AES_HOST_AUTH_SEC_PIN	12	利用AES演算法的單向對稱認證。卡為提供認證的使用者。 建立安全通道且供此ACR使用。 於提供額外的PIN之後便完成認證。

AES_MUTUAL_AUTH	13	利用AES演算法的雙向對稱認證。卡與主裝置會相互認證
AES_MUTUAL_AUTH_SEC	14	利用AES演算法的雙向對稱認證。卡與主裝置會相互認證。建立安全通道且供此ACR使用。
AES_MUTUAL_AUTH_SEC_PIN	15	利用AES演算法的雙係數認證。卡與主裝置會相互認證。建立安全通道且供此ACR使用。於提供額外的PIN之後便完成認證。
保留以後使用	16-19	
DES_HOST_AUTH	20	和AES的登入模式群相雷同，不同處在於所用的係DES演算法。
DES_HOST_AUTH_SEC	21	
DES_HOST_AUTH_SEC_PIN	22	
DES_MUTUAL_AUTH	23	
DES_MUTUAL_AUTH_SEC	24	
DES_MUTUAL AUTH_SEC_PIN	25	
保留以後使用	26-29	
3DES_HOST_AUTH	30	和AES的登入模式群相雷同，不同處在於所用的係3DES演算法。
3DES_HOST_AUTH_SEC	31	
3DES_HOST_AUTH_SEC_PIN	32	
3DES_MUTUAL_AUTH	33	
3DES_MUTUAL_AUTH_SEC	34	
3DES_MUTUAL_AUTH_SEC_PIN	35	
保留以後使用	36-39	
RSA_HOST_AUTH	40	

RSA_HOST_AUTH_PIN	41	
RSA_MUTUAL_AUTH	42	
RSA_MUTUAL_AUTH_PIN	43	
保留以後使用	44-255	

表12：Login Algorithm類型

1.3.4 Symmetric Credential符號

符號	數值	說明
SYMMETRIC_KEY	1	對應於選定的對稱認證序列的對稱密鑰。選定的認證序列還會反映在密鑰長度上。
USER_PIN	2	PIN係最大20個位元組的二進制值

表13：Symmetrical Credential類型

1.3.5 Asymmetrical Credential類型

符號	數值	說明
CA_ID		
CA_PUBLIC_RSA_KEY	1	
ACR_CERTIFICATE	2	
USER_PIN	4	

表14：Asymmetrical Credential類型

1.3.6 Partition Rights

Partition Rights位元組位元映圖							
讀取	寫入	轉讓	保留	保留	保留	保留	保留

1.3.7 Domain Rights

Domain Rights位元映圖							
讀取	寫入	轉讓	保留	保留	保留	保留	保留

1.3.8 Domain Permission代碼

符號	數值	說明
READ	1	
WRITE	2	
DOMAIN_PERMISSION_DELEGATION	3	
DOMAIN_OWNERSHIP	4	

表 15：Domain Permission類型

1.3.9 ACAM

符號	數值	說明
CREATE_AGP	1	
ACAM_CREATE_ACR	2	產生/刪除/更新AGP與ACR。
ACAM_CREATE_PARTITION	3	產生/刪除分割區。
ACAM_CREATE_DOMAIN	4	產生/刪除域。
ACAM_DELEGATE_DOMAIN_RIGHTS	5	轉讓存取權利給域：此特點係依照每個域來進行。
ACAM_DELEGATE_PARTITION_RIGHTS	6	轉讓存取權利給分割區：此特點係依照每個分割區來進行。
UNBLOCK_ACR	7	

表 16：ACAM類型

1.3.10 Public Partition restriction代碼

符號	數值	說明
READ_RESTRICTION	1	
WRITE_RESTRICTION	2	
LREAD_WRITE_RESTRICTION	3	

表 17：Public Partition Restriction類型

1.3.11 Command Status

欄位名稱	內容	位元組數
Session ID	ID數值	1
Last Command OP-Code	合法的SSA命令OP-Code	1
Last Command Status	●COMPLETE_OK-0 ●COMPLETE_ERROR-1 ●BUSY-2	1
Error Code		1
Authentication state	僅適用於認證命令	1
Number of transferred sectors	僅適用於資料傳輸命令	

1.3.12 SSA Query

欄位名稱	內容	位元組數
Session ID	ID數值	1
Last Command OP-Code	合法的SSA命令OP-Code	1
Last Command Status	●COMPLETE_OK-0 ●COMPLETE_ERROR-1 ●BUSY-2	
Error Code		1
SSA Version	版本號碼	
List of accessible 隔間)	分割區ID、淨大小以及存取權限	
List of accessible domains	域ID與存取權限	

1.3.13 命令序列

1.3.13.1 透過相互對稱認證進行SSA登入的命令序列

序列編號	命令名稱&Op-Code	引數說明	一般說明
1.	SSA_SYSTEM_LOGIN_CMD [18]	ACR與AGP名稱	開始登入序列。僅作為要求。
2.	SSA_CMD_STATUS_CMD [22]	Session ID-NA	取得CMD18的狀態。倘若CMD18失敗，便終止登入序列。
3.	SSA_SYM_AUTH_SEND_CHLG_CMD [26]	異議#1	傳送異議#1給SSA
4.	SSA_CMD_STATUS_CMD [22]	Session ID-NA	取得CMD26的狀態。倘若CMD26失敗，便終止登入序列。
5.	SSA_SYM_AUTH_GET_CHLG_RES_CMD [27]	NA	讀取異議#1的SSA答覆。主裝置驗證該答覆是否合法。
6.	SSA_CMD_STATUS_CMD [22]	Session ID-NA	取得CMD27的狀態。倘若CMD27失敗，便終止登入序列。
7.	SSA_SYM_AUTH_GET_CHLG_CMD [25]	NA	從SSA讀取異議#2。
8.	SSA_CMD_STATUS_CMD [22]	Session ID-NA	取得CMD25的狀態。倘若CMD25失敗，便終止登入序列。
9.	SSA_SYM_AUTH_SEND_CHLG_RES_CMD [28]	異議#2答覆	傳送異議#2答覆給SSA。
10.	SSA_CMD_STATUS_CMD [22]	Session ID-NA	取得CMD28的狀態。倘若CMD28失敗，便終止登入序列。此時，該命令狀態應該顯示認證程序究竟係成功或失敗。

當成功地完成此序列之後，便會登入SSA中的此ACR之中，且可以開始進行SSA作業。

1.3.13.2 用於產生根AGP的命令序列

可透過該系統ACR來產生一根AGP(其必須執行該系統ACR的登入序列)，或是放棄該安全通道且省略系統ACR認證程序。連同該根AGP的身份一起傳送命令

SSA_CREATE_ROOT_AGP_CMD[3]。

本命令後面會跟著SSA _CMD_STATUS_CMD [22]，確保SSA不會拒絕本命令且確保而無誤地完成本命令。

當產生該根AGP及其所有ACR之後，若要封閉該根AGP的話，便會送出SSA_ROOT_AGP_CREATION_DONE_ CMD [4]命令。

1.3.13.3 用於產生AGP的命令序列

為產生一AGP，使用者必須執行1.3.13.1中所示的登入命令序列先登入SSA。於產生新的ACR群以前必須先產生AGP。該AGP係藉由傳送具有AGP名稱/ID的命令SSA CREATE_AGP_CMD [5]來產生。

為驗證CMD [5]有被收到且無誤地執行，使用者會傳送SSA_CMD_STATUS_CMD [22]且讀取先前送出的命令的狀態。當使用者完成作業產生AGP之後，其便能夠繼續產生一ACR或登出SSA系統。

1.3.13.4 用於產生ACR的命令序列

為產生一ACR，使用者必須執行1.3.13.1中所示的登入命令序列先登入SSA。另外，必須要有一讓該ACR歸屬的AGP。接著，使用者便會送出具有所有新ACR資料(名稱、AGP、登入方法...等)的命令SSA_CREATE_ACR_CMD [7]。為驗證CMD [7]有被收到且無誤地執行，使用者會傳送SSA_CMD_STATUS_CMD [22]且讀取先前送出的命令的狀態。

當使用者完成作業產生ACR之後，其便能夠繼續進行其

它的SSA作業或登出SSA系統。

1.4 產品參數

- 所有實體(MARO、ARCR、平行交談、...、等)的最大數。
- 可以的話，增加暗碼參數的定義，也就是，RSA密鑰長度。
- 必須定義每種協定的錯誤條件與訊息。
- 必須定義逾時與忙碌。
- 指定該等樹上的階層數。
- 根MAROS的限制#。
- on all? delegate up to (根上面的)子部的限制#。
- 平行的CBC內容數量會有限制，如5至10個。
- 協定與產品版本

201017514

件 1

發明專利說明書

割案

（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：99101173

※ 申請日期：99.1.21　　※IPC 分類：G06F 3/06 (2006.01)

原申請案號：094145711

一、發明名稱：（中文/英文）

具多功能內容控制之記憶體系統

MEMORY SYSTEM WITH VERSATILE CONTENT CONTROL

二、中文發明摘要：

倘若可將加密-解密密鑰儲存在媒體本身之中且實質上無法由外部裝置來存取的話，那麼私人重要資料的擁有者將可較佳地控制該媒體中已加密內容的存取作業。僅有具正確憑證的主裝置方能存取該密鑰。可儲存一存取政策，其會授予不同的權限(給不同的經授權實體)來存取該媒體中所儲存的資料。兼具上面兩項特點之組合的系統特別有用。就其中一方面來說，內容擁有者能夠利用外部裝置實質上無法存取的密鑰來控制該內容的存取作業；同時，還能夠授予不同的權限來存取該媒體中的內容。因此，即使外部裝置具存取能力，它們的存取動作仍可受到該內容擁有者設定記錄在該儲存媒體中的不同權限的管制。當設計於快閃記憶體中時，上面的特點可針對內容保護產生一特別有用的媒體。當眾多電腦主裝置讀取與寫入以檔案為形式的資料時，眾多儲存裝置並不知悉檔案系統。該主裝置會提供一密鑰參考值或ID，而該記憶體系統則會響應以產

生一和該密鑰ID相關聯的密鑰值，讓該記憶體對用於暗碼處理的密鑰值的產生與運用保有完整與獨特的控制能力，同時讓該主機保有對檔案的控制能力。

三、英文發明摘要：

The owner of proprietor interest is in a better position to control access to the encrypted content in the medium if the encryption-decryption key is stored in the medium itself and substantially inaccessible to external devices. Only those host devices with the proper credentials are able to access the key. An access policy may be stored which grants different permissions (e.g. to different authorized entities) for accessing data stored in the medium. A system incorporating a combination of the two above features is particularly advantageous. On the one hand, the content owner or proprietor has the ability to control access to the content by using keys that are substantially inaccessible to external devices and at the same time has the ability to grant different permissions for accessing content in the medium. Thus, even where external devices gain access, their access may still be subject to the different permissions set by the content owner or proprietor recorded in the storage medium. When implemented in a flash memory, the above features result in a particularly useful medium for content protection. Many storage devices are not aware of file systems while many computer host devices read and write data in the form of files. The host device provides a key reference or ID, while the memory system generates a key value in response which is associated with the key ID, which is used as the handle through which the memory retains complete and exclusive control over the generation and use of the key value for cryptographic processes, while the host retains control of files.

七、申請專利範圍：

1. 一種主裝置，包含：

一介面，其經配置以與一儲存裝置通信；及

一與該介面通信的控制器，其中該控制器係操作以：

傳送一產生一密鑰之要求至該儲存裝置，該要求包括用於該密鑰之一參考名稱，在該儲存裝置中之該密鑰之產生係獨立於其參考名稱，其中該密鑰係僅能從該儲存裝置中之內部存取；及

傳送至該儲存裝置以儲存一或多個可應用於該密鑰之使用的政策，該一或多個政策係關於授予經認證的實體不同的權限，以向該儲存裝置要求使用該密鑰而加密及/或解密儲存於該儲存裝置中的資料，其中傳送至該儲存裝置的一要求可基於該一或多個政策被允許或拒絕，該要求包含該參考名稱，該參考名稱係用於使用該密鑰以分別加密或解密該儲存裝置中被寫入或被讀取之資料。

2. 如請求項1之主裝置，其中該一或多個政策允許在一實體集中的一或多個實體利用該密鑰來存取儲存於該儲存裝置中的該資料並防止不在該實體集的實體利用該密鑰來存取儲存於該儲存裝置中的資料。

3. 如請求項1之主裝置，其中該一或多個政策允許由一或多個實體所組成的第一實體集利用該密鑰來加密及/或解密資料且自該儲存裝置進行資料寫入與讀取，並僅允許由一或多個實體所組成的第二實體集利用該密鑰來解密該

記憶體中的資料及讀取解密後的資料。

4. 如請求項1之主裝置，其中該一或多個政策僅允許由一或多個實體所組成的實體集利用該密鑰來加密資料且將加密後的資料寫入該儲存裝置，以及僅允許解密該儲存裝置中的資料及讀取解密後的資料，或者上述兩者。

5. 如請求項1之主裝置，其中該一或多個政策允許一實體刪除另一實體的儲存裝置存取權利；或是變更該一或多個政策而不允許另一實體利用該密鑰存取，其中該另一實體於變更前被允許施行此存取作業。

6. 如請求項1之主裝置，其中該一或多個政策允許一實體將該密鑰的存取權利轉讓給另一實體；或是變更該一或多個政策以允許施行此轉讓作業。

7. 如請求項1之主裝置，其中該一或多個政策需要為至少一實體建立一安全通道，以便存取該儲存裝置或存取該密鑰。

8. 如請求項1之主裝置，其中該一或多個政策需要建立一安全通道，以便存取該儲存裝置或存取該密鑰。

9. 如請求項1之主裝置，其中該一或多個政策僅允許有限數量的實體存取該儲存裝置或存取該密鑰。

10. 如請求項1之主裝置，其中，不論一實體是否已經過認證，該一或多個政策均僅允許有限數量的實體存取該儲存裝置或存取該密鑰。

11. 如請求項1之主裝置，其中該一或多個政策不需要為至少一實體建立一安全通道，以便存取該儲存裝置或存取該

密鑰。

12. 如請求項1之主裝置，其中該控制器進一步操作以傳送以下至少之一者至該儲存裝置：

一可應用於該密鑰之使用的額外政策；以及

用於產生額外密鑰之一要求。

13. 如請求項1之主裝置，其中該一或多個政策允許不同實體集的實體對該密鑰作出不同使用，並具有不同的資料存取權限，該密鑰之不同使用包含加密或解密中之一或兩者，且該不同存取權限包括讀取或寫入資料中之一或兩者。

14. 如請求項1之主裝置，其中該控制器進一步操作以傳送一關聯至該儲存裝置，該關聯連結該密鑰與一將被該密鑰加密並儲存於該儲存裝置中的檔案。

15. 如請求項14之主裝置，其中該控制器進一步操作以傳送一要求至該儲存裝置，以讀取該檔案及用於該密鑰之該參考名稱。

16. 如請求項1之主裝置，其中該控制器進一步操作以：

傳送兩筆或兩筆以上的記錄至該儲存裝置，每一筆記錄包含一認證規定及一或多個權限，用以控制一實體存取該儲存裝置中的資料，其中所接收之該兩筆或兩筆以上的記錄具有不同於彼此的該認證規定及該一或多個權限的至少其中之一。

17. 如請求項16之主裝置，其中該至少兩筆記錄的每一個包含一或多個權限以讓該對應實體存取該儲存裝置中的分

割區，其中該等至少兩個對應實體的該等記錄中的該一或多個用以存取分割區的權限並不完全相同。

18. 一種保護儲存於一儲存裝置之資料的方法，該方法包含：

藉由一主裝置實現與一儲存裝置之通信；

傳送產生一密鑰之一要求至該儲存裝置，該要求包括用於該密鑰之一參考名稱，在該儲存裝置中之該密鑰之產生係獨立於其參考名稱，其中該密鑰僅在該儲存裝置中可存取；及

傳送至該儲存裝置用以儲存一或多個可應用於該密鑰之使用的政策，該一或多個政策係關於授予經認證的實體之不同權限，以向該儲存裝置要求使用該密鑰而加密及/或解密儲存於該儲存裝置中的資料，其中傳送至該儲存裝置的一要求可基於該一或多個政策被允許或拒絕，該要求包含該參考名稱，該參考名稱係用於使用該密鑰以分別加密或解密該儲存裝置中被寫入或被讀取之資料。

19. 如請求項18之方法，其中該一或多個政策允許在一個實體集中的一或多個實體利用該密鑰來存取儲存於儲存裝置中的該相同資料，並防止不在該實體集中的實體利用該密鑰來存取儲存於儲存裝置中的資料。

20. 如請求項18之方法，其中該一或多個政策允許由一或多個實體所組成的第一實體集利用該密鑰來加密及/或解密資料且對該儲存裝置進行資料寫入與讀取，且僅允許由一或多個實體所組成的第二實體集利用該密鑰來解密該

儲存裝置中的資料及讀取解密後的資料。

21. 如請求項18之方法，其中該一或多個政策僅允許由一或多個實體所組成的實體集利用該密鑰來加密資料且將加密後的資料寫入該儲存裝置，以及僅允許解密該儲存裝置中的資料及讀取解密後的資料，或者上述兩者。

22. 如請求項18之方法，其中該一或多個政策允許一實體刪除另一實體的儲存裝置存取權利；或是變更該一或多個政策而不允許另一實體利用該密鑰存取，其中該另一實體於變更前被允許施行此存取作業。

23. 如請求項18之方法，其中該一或多個政策允許一實體將該密鑰的存取權利轉讓給另一實體；或是變更該一或多個政策以允許施行此轉讓作業。

24. 如請求項18之方法，其中該一或多個政策需要為至少一實體建立一安全通道，以便存取該儲存裝置或存取該密鑰。

25. 如請求項18之方法，其中該一或多個政策需要建立一安全通道，以便存取該儲存裝置或存取該密鑰。

26. 如請求項18之方法，其中該一或多個政策僅允許有限數量的實體存取該儲存裝置或存取該密鑰。

27. 如請求項18之方法，其中，不論一實體是否已經過認證，該一或多個政策均僅允許有限數量的實體存取該儲存裝置或存取該密鑰。

28. 如請求項18之方法，其中該一或多個政策不需要為至少一實體建立一安全通道，以便存取該儲存裝置或存取該密鑰。

29. 如請求項18之方法，進一步包含傳送以下之至少一者至該儲存裝置：

一可應用於該密鑰之使用的額外政策；以及

用於產生額外密鑰之一要求。

30. 如請求項18之方法，其中該一或多個政策允許不同實體集的實體對該密鑰作出不同使用，並具有不同的資料存取權限，該密鑰之不同使用包含加密或解密中之一或兩者，且該不同存取權限包括讀取或寫入資料中之一或兩者。

31. 如請求項18之方法，進一步包含傳送一關聯至該儲存裝置，該關聯連結該密鑰與一將被該密鑰加密並儲存於該儲存裝置中的檔案。

32. 如請求項31之方法，進一步包含傳送一要求至該儲存裝置，以讀取該檔案及用於該密鑰之該參考名稱。

33. 如請求項18之方法，進一步包含：

傳送兩筆或兩筆以上的記錄至該儲存裝置，每一筆記錄包含一認證規定及一或多個權限，用以控制一實體存取該儲存裝置中的資料，其中所接收的該兩筆或兩筆以上的記錄具有不同於彼此的該認證規定及該一或多個權限的至少之一者。

34. 如請求項33之方法，其中該至少兩筆記錄的每一個包含一或多個權限以讓該對應實體存取該儲存裝置中的分割區，其中該等至少兩個對應實體的該等記錄中的該一或多個用以存取分割區的權限並不完全相同。

八、圖式：

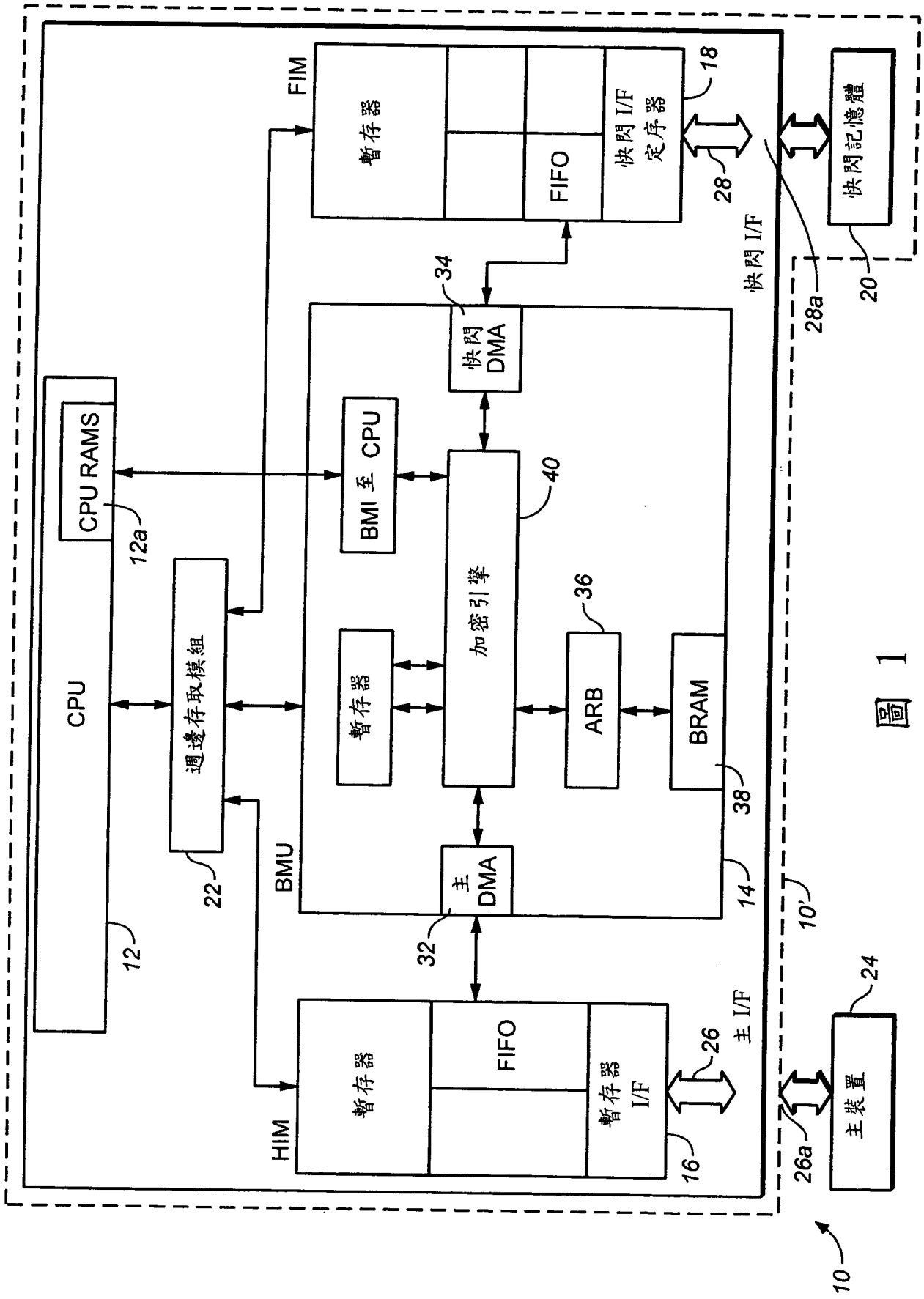

FIM
暫存器
FIFO
快閃 I/F 定序器
18
28
快閃記憶體
20
28a
快閃 I/F
34
快閃 DMA
BMI 至 CPU
40
CPU RAMS
12a
CPU
週邊存取模組
22
暫存器
加密引擎
36
ARB
BRAM
38
BMU
主 DMA
14
10'
32
12
HIM
暫存器
FIFO
暫存器 I/F
26
主 I/F
24
主裝置
26a
16
10

圖 1

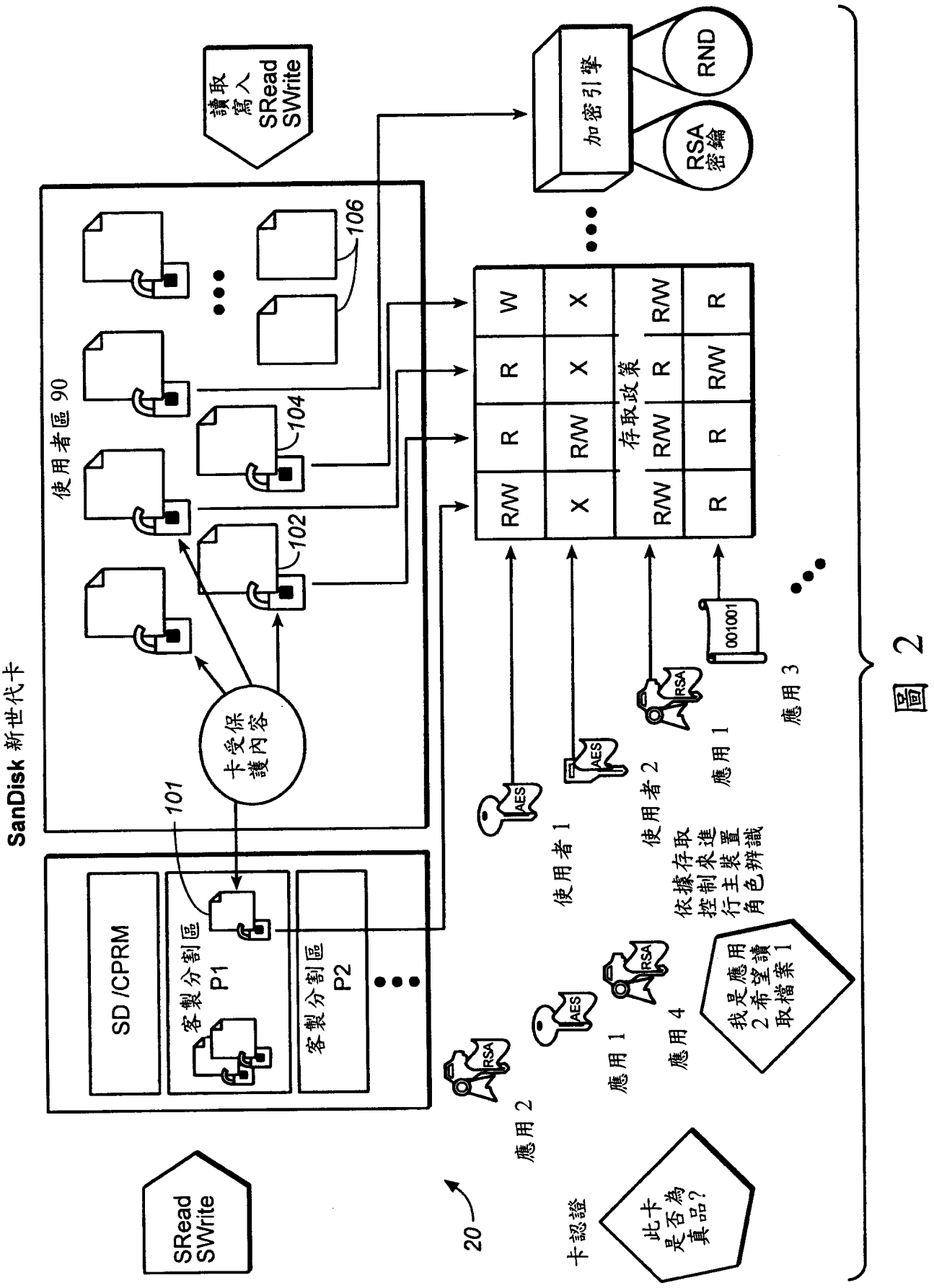

SanDisk 新世代卡
使用者區 90
101
102
104
106
卡受保護內容
SD /CPRM
客製分割區 P1
客製分割區 P2
讀取寫入 SRead SWrite
SRead SWrite
加密引擎
RND
RSA密鑰
存取政策
R/W
R
W
X
001001
使用者 1
使用者 2
應用 1
應用 2
應用 3
應用 4
依據存取控制來進行主裝置角色辨識
我是應用2希望讀取檔案1
卡認證
此卡是否為真品?
20

圖 2

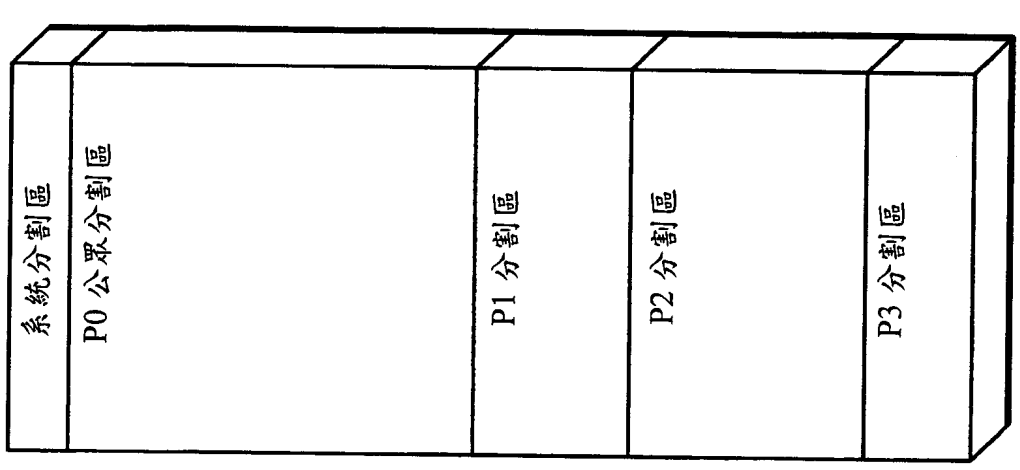

系統分割區
P0 公眾分割區
P1 分割區
P2 分割區
P3 分割區

圖 3

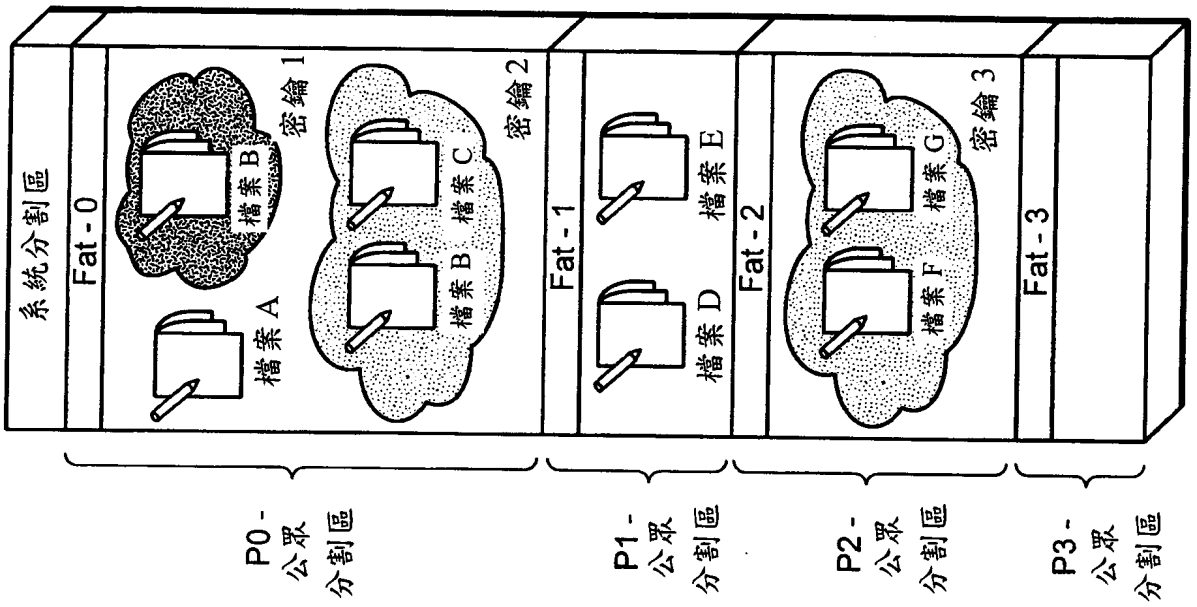

系統分割區
Fat - 0
檔案 A
檔案 B
密鑰 1
檔案 B
檔案 C
密鑰 2
Fat - 1
檔案 D
檔案 E
Fat - 2
檔案 F
檔案 G
密鑰 3
Fat - 3
P0 - 公眾分割區
P1 - 公眾分割區
P2 - 公眾分割區
P3 - 公眾分割區

圖 4

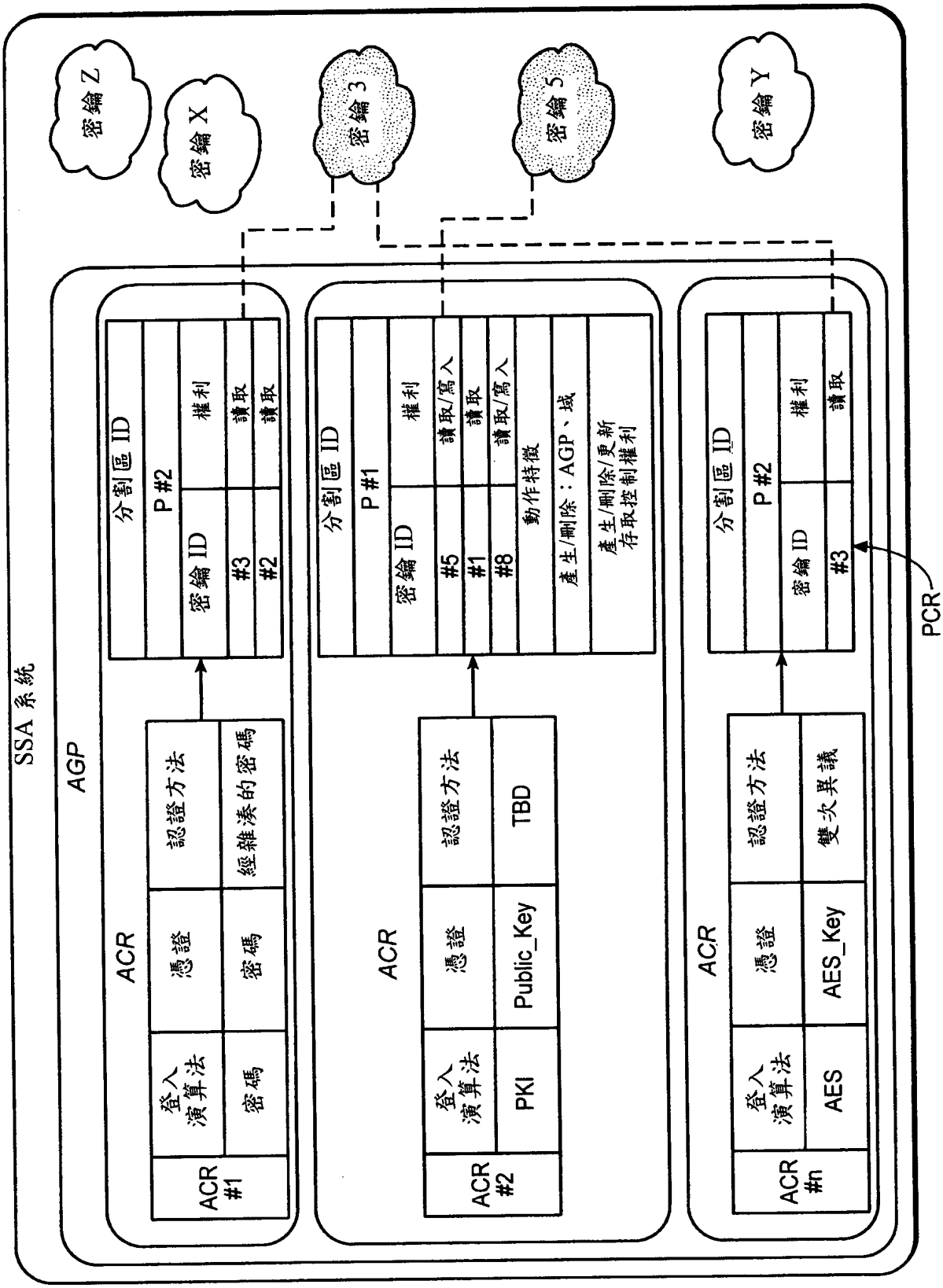

SSA 系統
AGP
ACR
ACR #1
登入演算法
密碼
憑證
密碼
認證方法
經雜湊的密碼
分割區 ID
P #2
密鑰 ID
權利
#3
讀取
#2
讀取
ACR
ACR #2
登入演算法
PKI
憑證
Public_Key
認證方法
TBD
分割區 ID
P #1
密鑰 ID
權利
#5
讀取/寫入
#1
讀取
#8
讀取/寫入
動作特徵
產生/刪除：AGP、域
產生/刪除/更新存取控制權利
ACR
ACR #n
登入演算法
AES
憑證
AES_Key
認證方法
雙次異議
分割區 ID
P #2
密鑰 ID
權利
#3
讀取
PCR
密鑰 Z
密鑰 X
密鑰 3
密鑰 5
密鑰 Y

圖 5

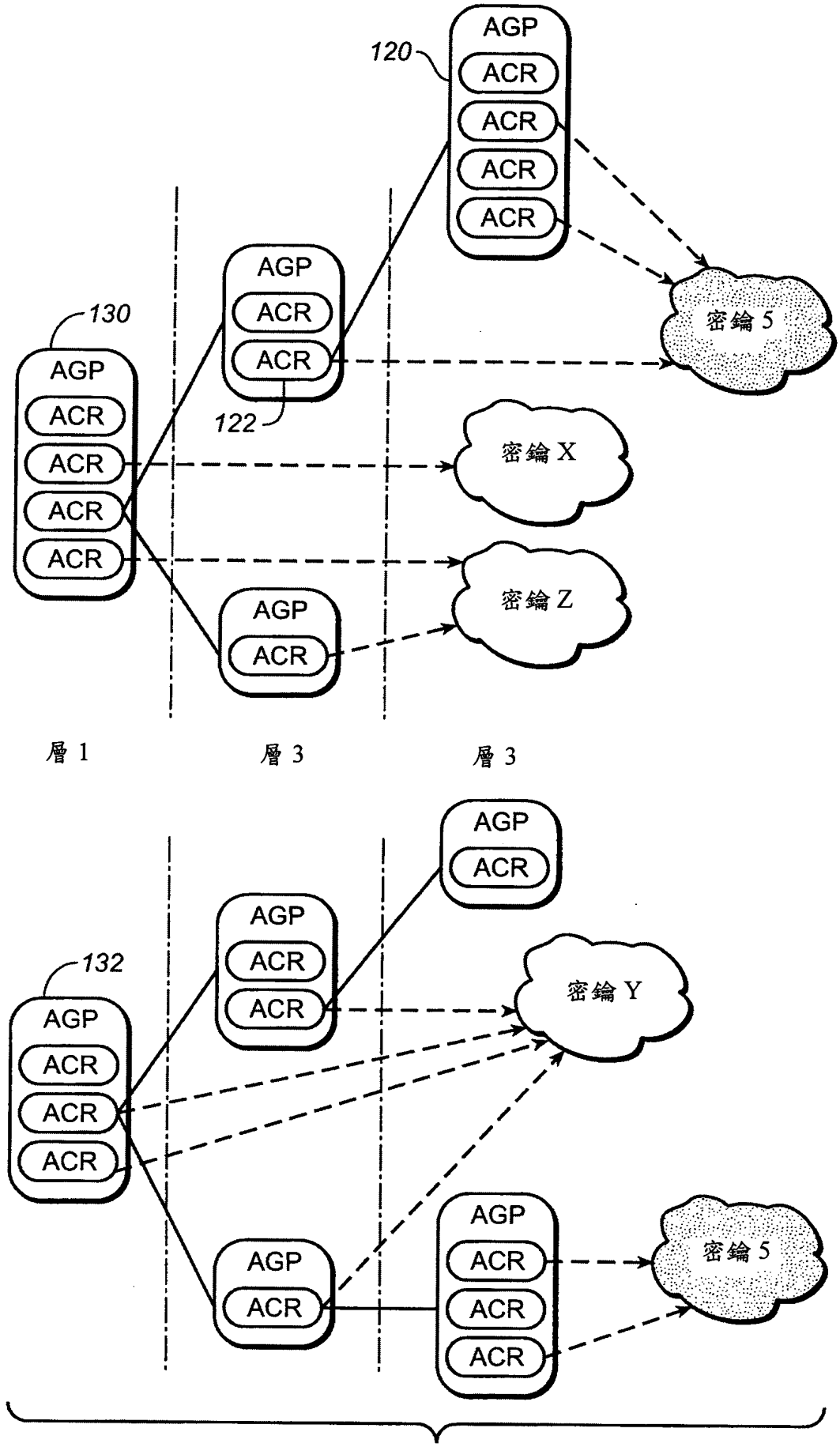

AGP
ACR
ACR
ACR
ACR
120
密鑰 5
AGP
ACR
ACR
122
130
AGP
ACR
ACR
ACR
ACR
密鑰 X
密鑰 Z
AGP
ACR
層 1
層 3
層 3
AGP
ACR
AGP
ACR
ACR
132
AGP
ACR
ACR
ACR
密鑰 Y
AGP
ACR
AGP
ACR
ACR
ACR
密鑰 5

圖 6

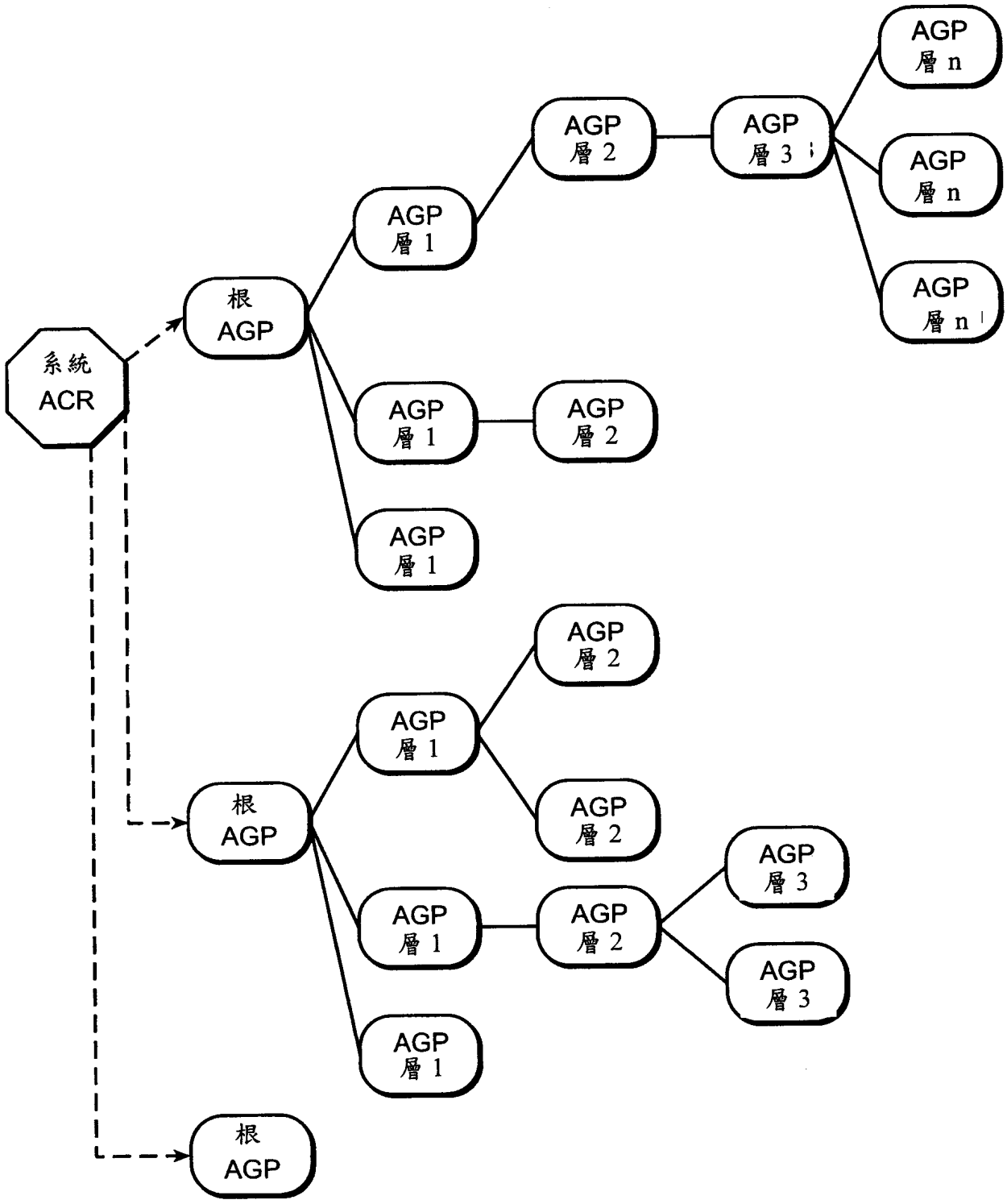

系統
ACR
根
AGP
AGP
層 1
AGP
層 2
AGP
層 3
AGP
層 n
AGP
層 n
AGP
層 n
AGP
層 1
AGP
層 2
AGP
層 1
根
AGP
AGP
層 2
AGP
層 1
AGP
層 2
AGP
層 1
AGP
層 2
AGP
層 3
AGP
層 3
AGP
層 1
根
AGP

圖 7

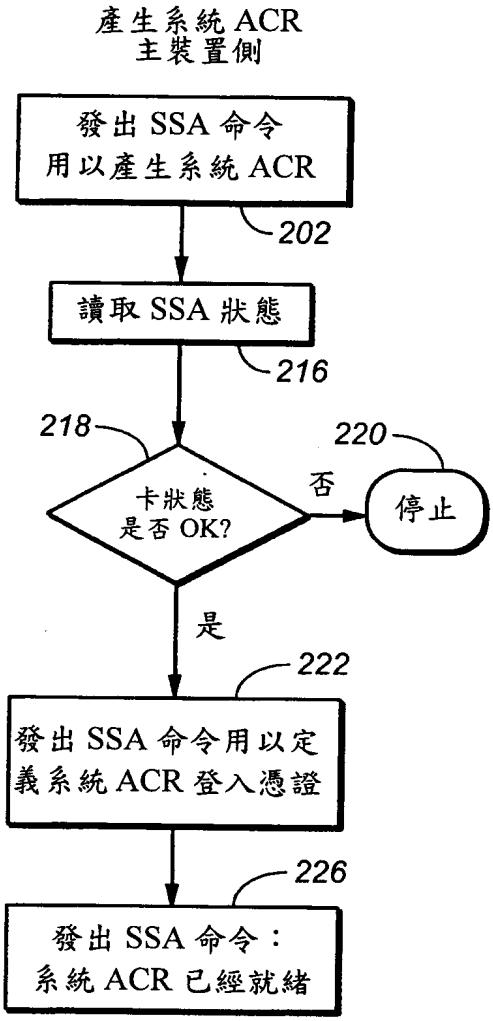

產生系統 ACR
主裝置側
發出 SSA 命令
用以產生系統 ACR
202
讀取 SSA 狀態
216
218
卡狀態
是否 OK?
否
220
停止
是
222
發出 SSA 命令用以定
義系統 ACR 登入憑證
226
發出 SSA 命令：
系統 ACR 已經就緒

圖 8A

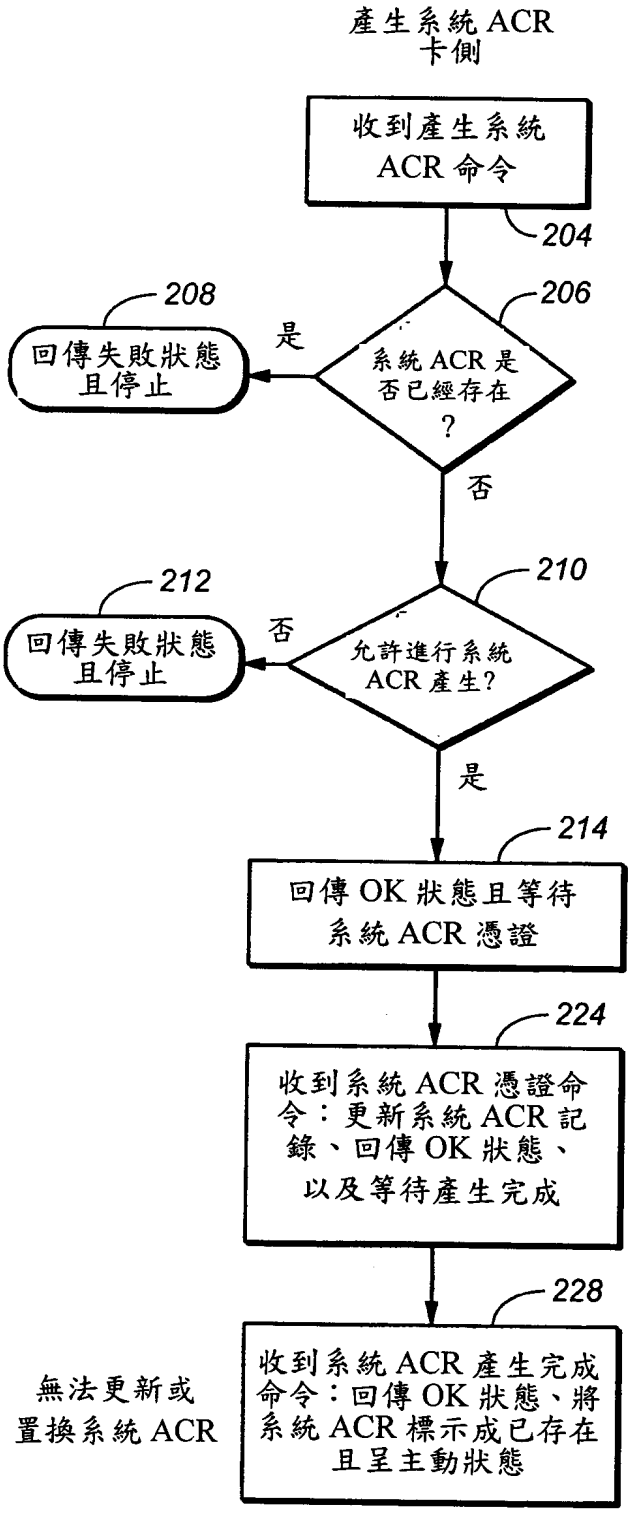

產生系統 ACR
卡側
收到產生系統
ACR 命令
204
208
回傳失敗狀態
且停止
是
206
系統 ACR 是
否已經存在
?
否
212
回傳失敗狀態
且停止
否
210
允許進行系統
ACR 產生?
是
214
回傳 OK 狀態且等待
系統 ACR 憑證
224
收到系統 ACR 憑證命
令：更新系統 ACR 記
錄、回傳 OK 狀態、
以及等待產生完成
228
收到系統 ACR 產生完成
命令：回傳 OK 狀態、將
系統 ACR 標示成已存在
且呈主動狀態
無法更新或
置換系統 ACR

圖 8B

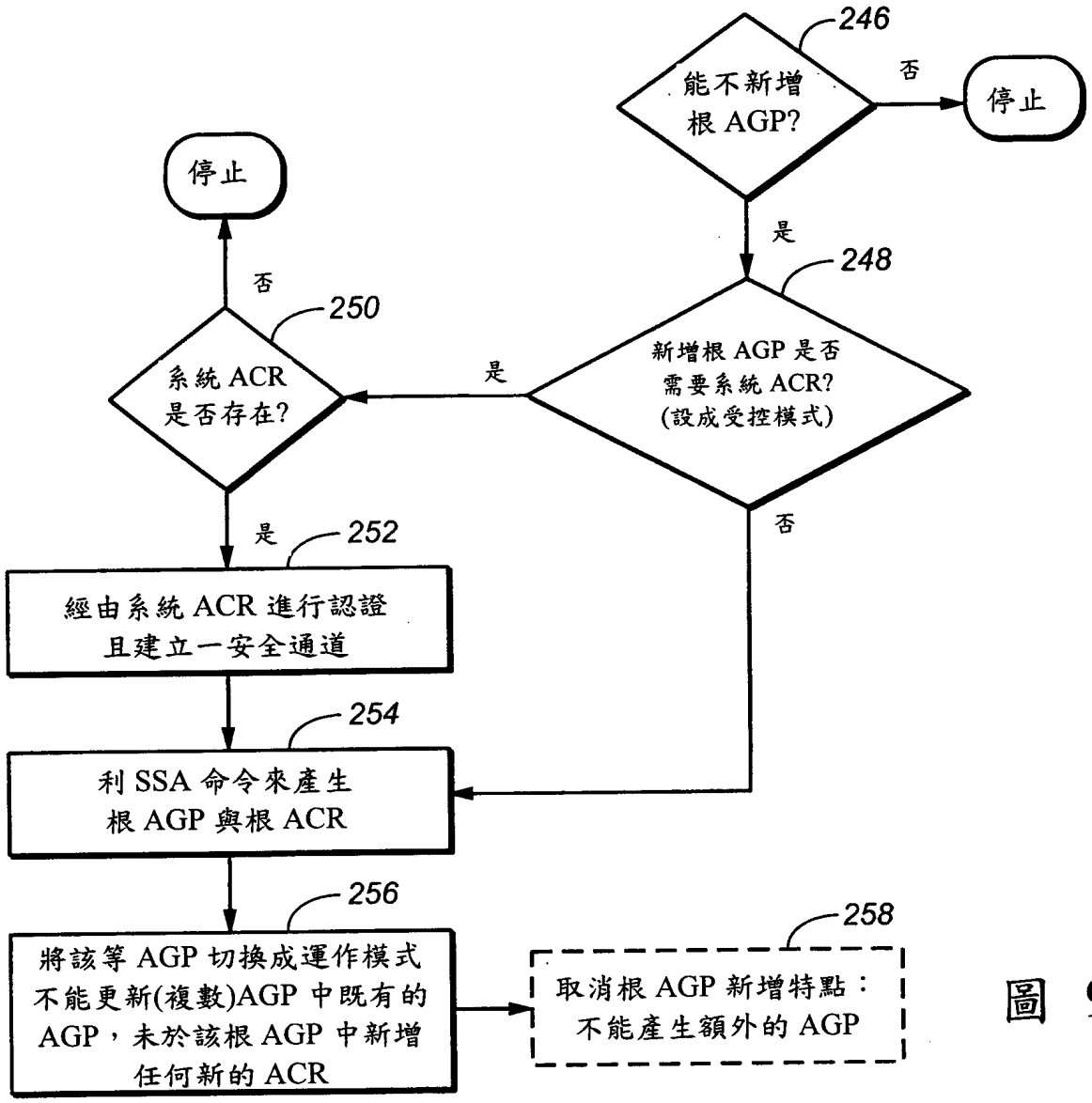

246
能不新增根 AGP?
否
停止
是
248
新增根 AGP 是否需要系統 ACR? (設成受控模式)
是
250
系統 ACR 是否存在?
否
停止
否
是
252
經由系統 ACR 進行認證且建立一安全通道
254
利 SSA 命令來產生根 AGP 與根 ACR
256
將該等 AGP 切換成運作模式不能更新(複數)AGP 中既有的 AGP，未於該根 AGP 中新增任何新的 ACR
258
取消根 AGP 新增特點：不能產生額外的 AGP

圖 9

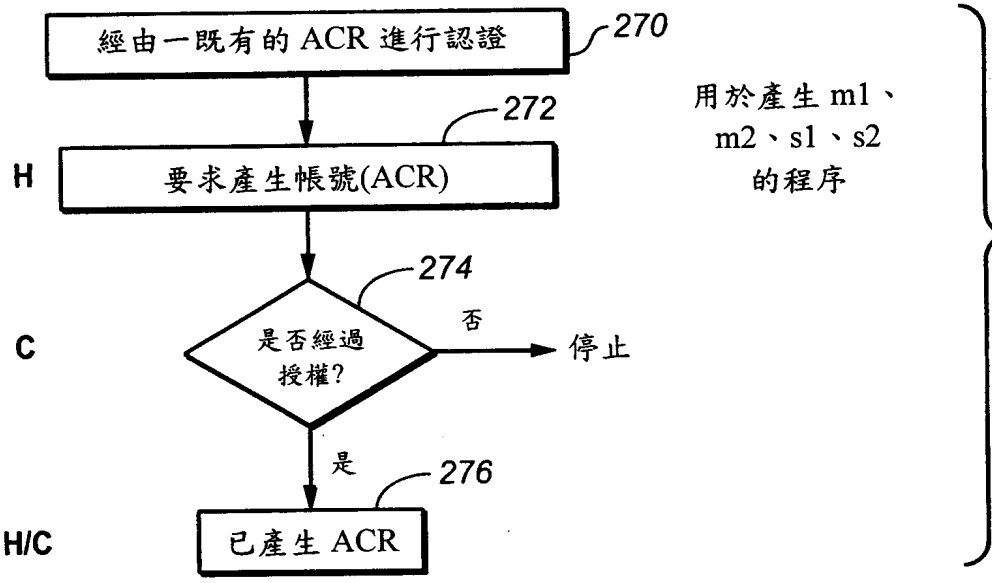

270
經由一既有的 ACR 進行認證
272
H
要求產生帳號(ACR)
274
C
是否經過授權?
否
停止
是
276
H/C
已產生 ACR
用於產生 m1、m2、s1、s2 的程序

圖 10

於營銷 AGP 中產生 2 個 ACR(m1、m2)，於銷售 AGP 中產生 2 個 ACR(s1、s2)

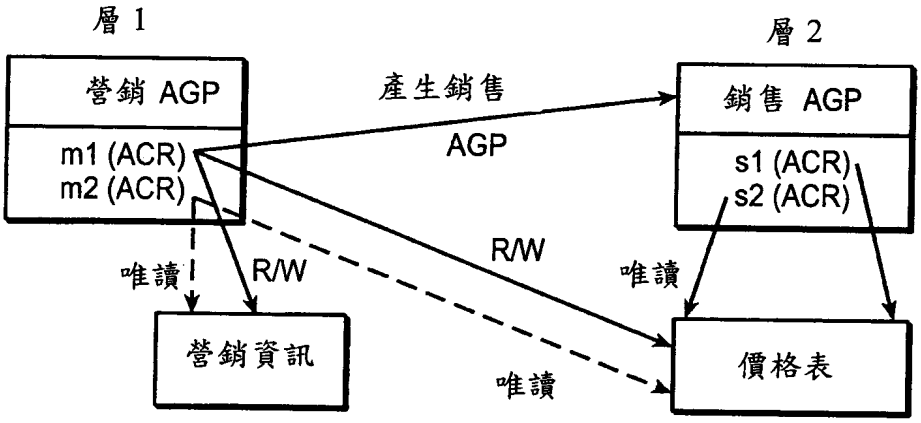


圖 11

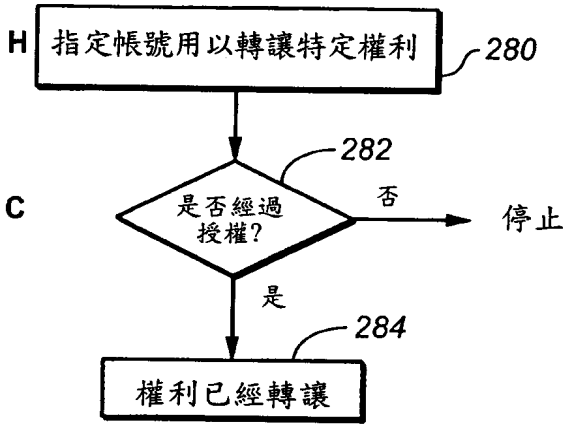


圖 12

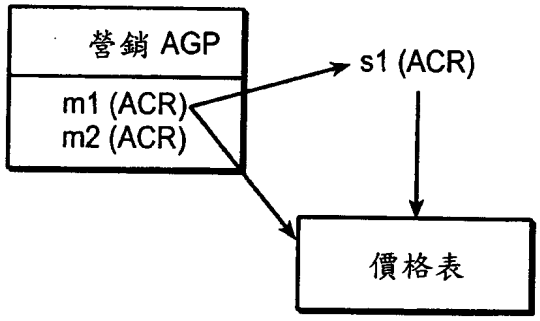


圖 13

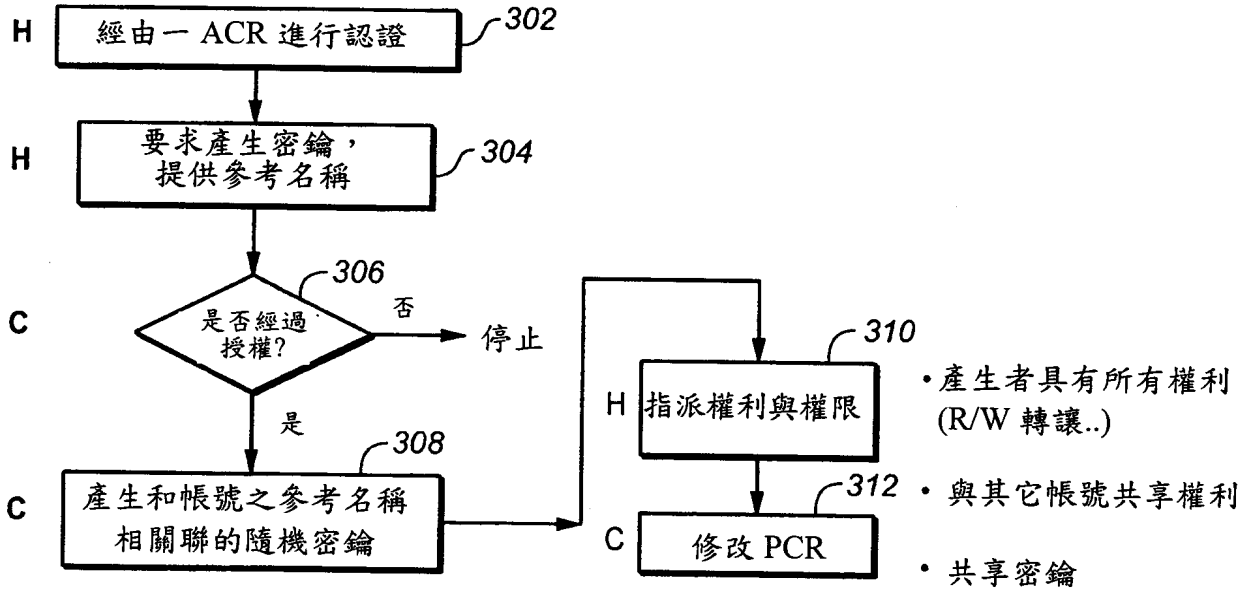


圖 14

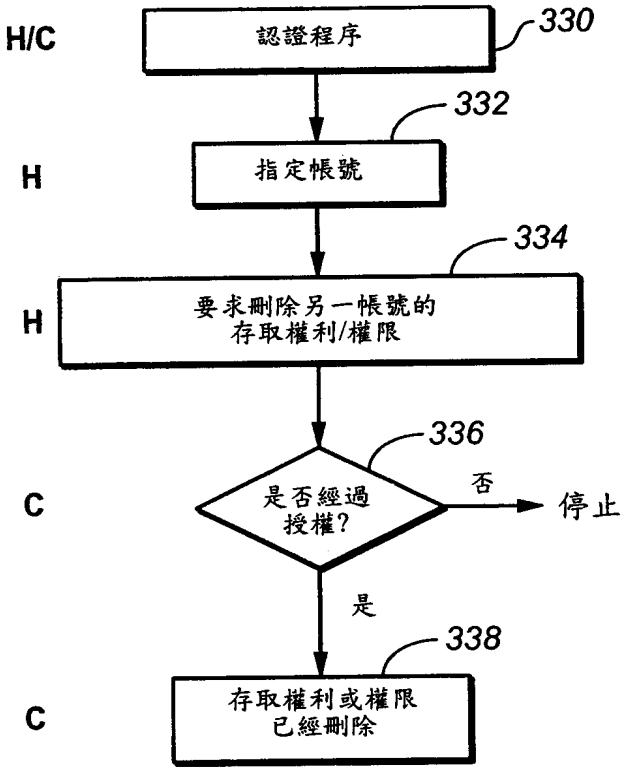

H/C
認證程序
330
332
H
指定帳號
334
H
要求刪除另一帳號的
存取權利/權限
336
C
是否經過
授權?
否
停止
是
338
C
存取權利或權限
已經刪除

圖 15

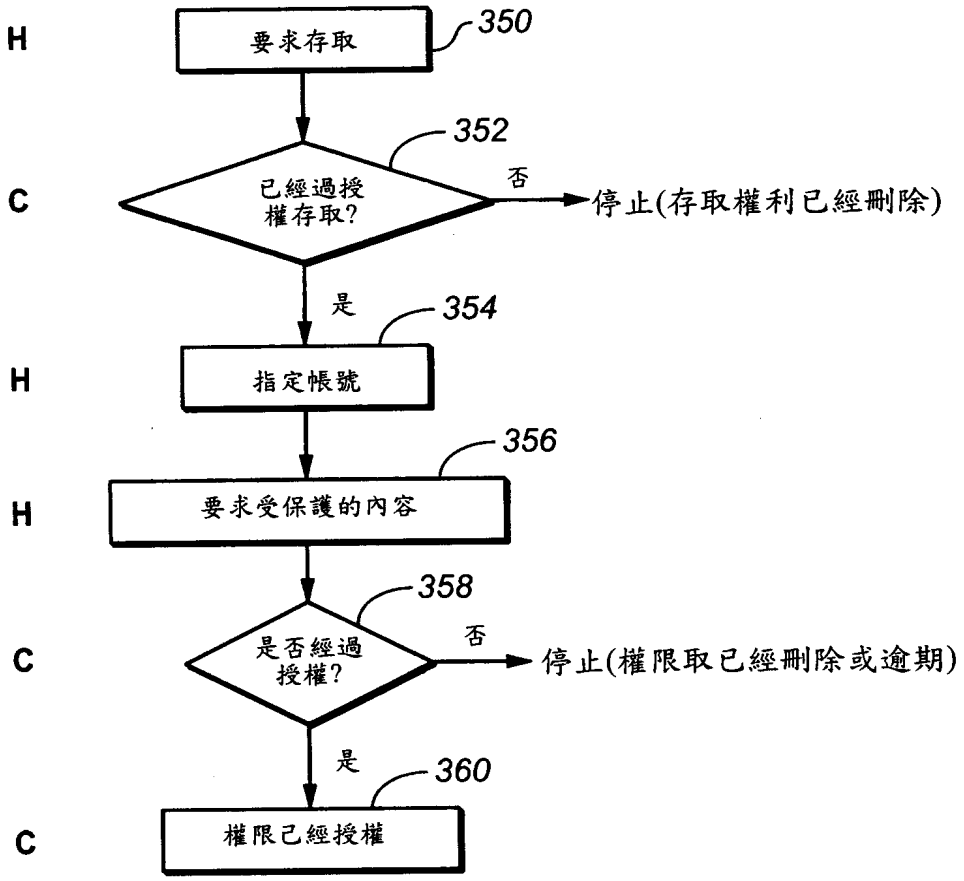

H
要求存取
350
352
C
已經過授
權存取?
否
停止(存取權利已經刪除)
是
354
H
指定帳號
356
H
要求受保護的內容
358
C
是否經過
授權?
否
停止(權限取已經刪除或逾期)
是
360
C
權限已經授權

圖 16

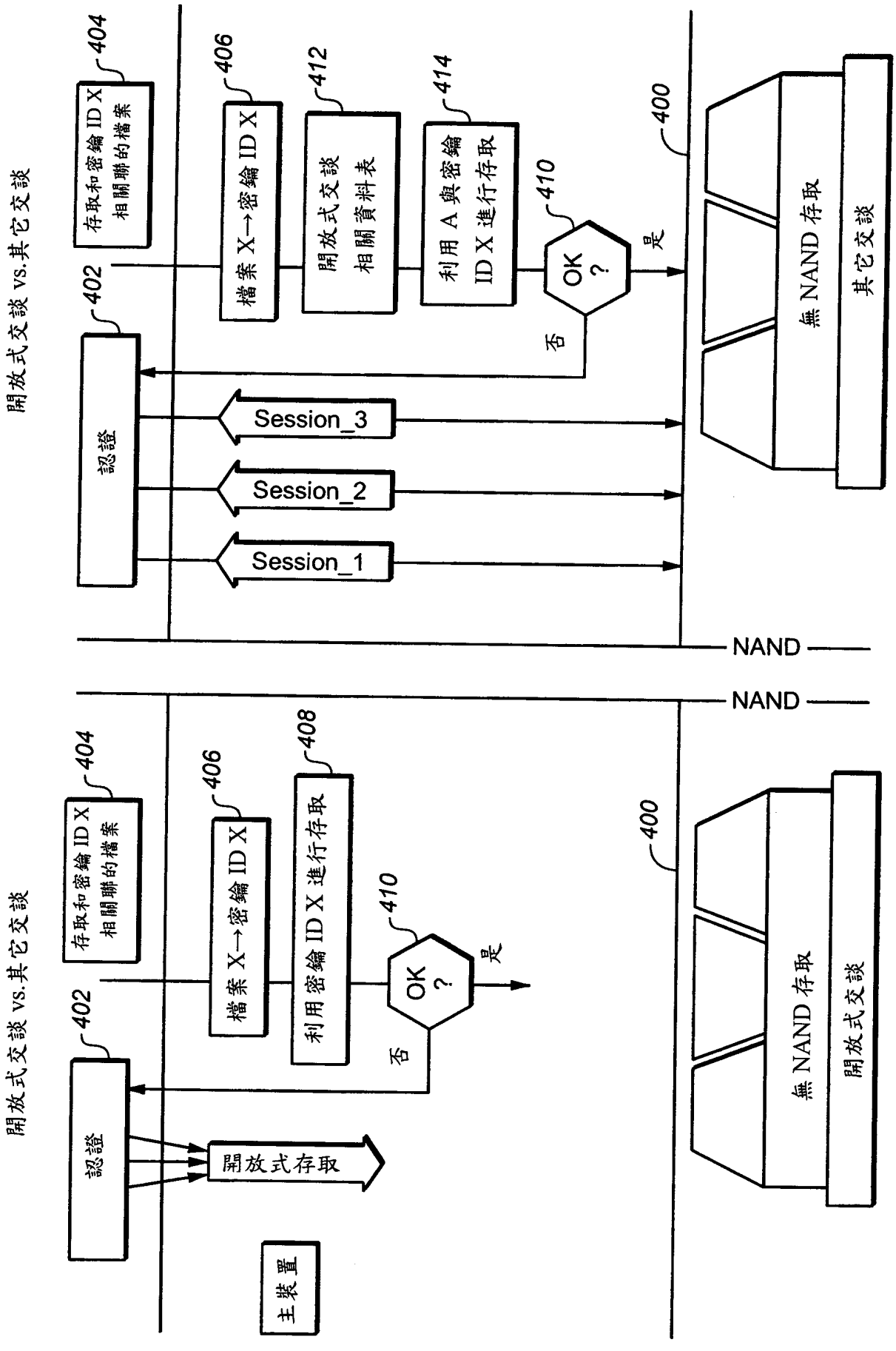

開放式交談 vs.其它交談
主裝置
認證
開放式存取
存取和密鑰 ID X 相關聯的檔案
404
檔案 X→密鑰 ID X
406
利用密鑰 ID X 進行存取
408
OK ?
410
是
否
402
NAND
400
無 NAND 存取
開放式交談
開放式交談 vs.其它交談
認證
存取和密鑰 ID X 相關聯的檔案
404
檔案 X→密鑰 ID X
406
開放式交談相關資料表
412
利用 A 與密鑰 ID X 進行存取
414
OK ?
410
是
否
402
Session_3
Session_2
Session_1
NAND
400
無 NAND 存取
其它交談

圖 17A

圖 17B

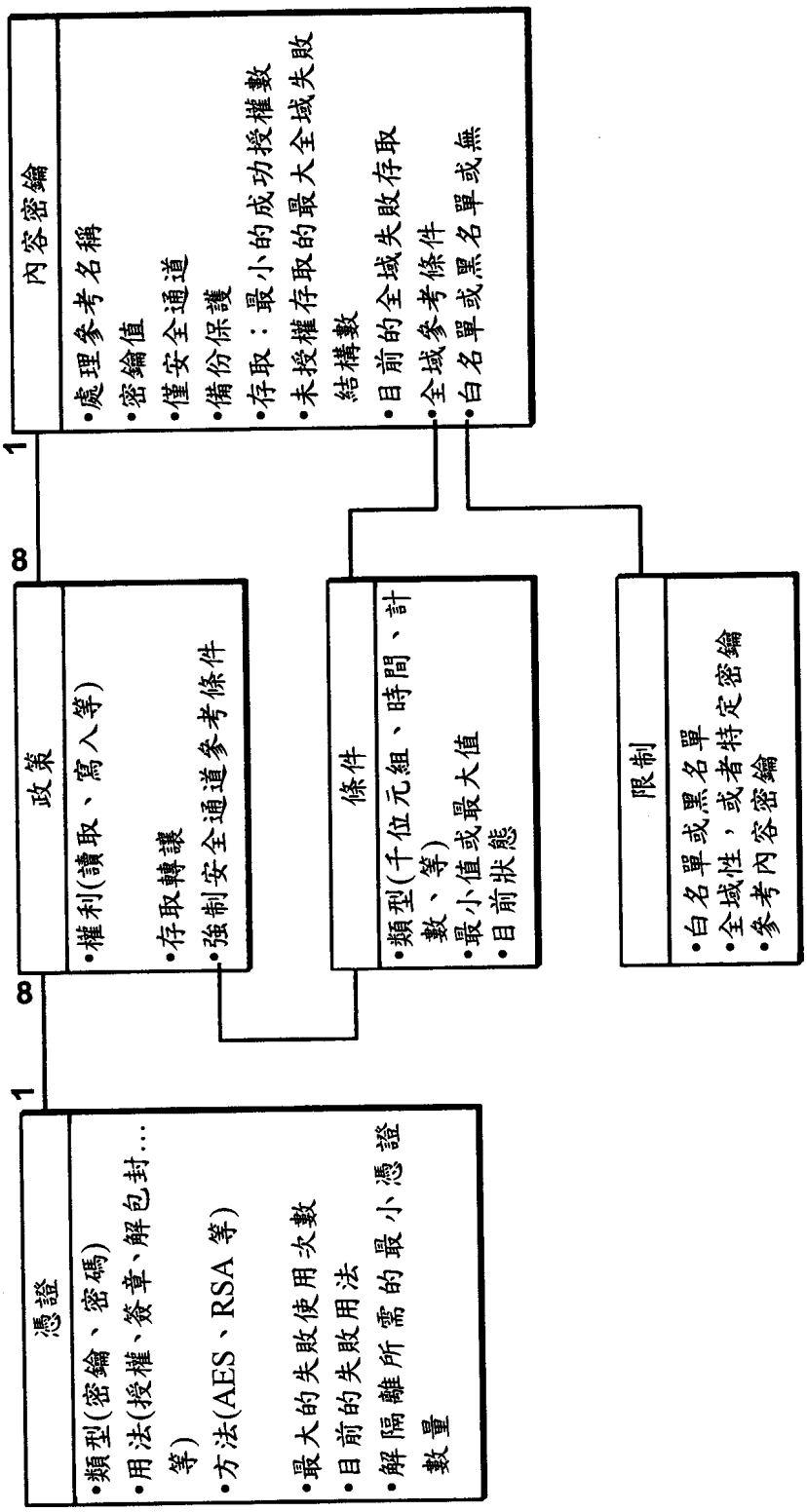

憑證
•類型(密鑰、密碼)
•用法(授權、簽章、解包封…等)
•方法(AES、RSA 等)
•最大的失敗使用次數
•目前的失敗用法
•解隔離所需的最小憑證數量
政策
•權利(讀取、寫入等)
•存取轉讓
•強制安全通道參考條件
條件
•類型(千位元組、時間、計數、等)
•最小值或最大值
•目前狀態
限制
•白名單或黑名單
•全域性，或者特定密鑰
•參考內容密鑰
內容密鑰
•處理參考名稱
•密鑰值
•僅安全通道
•備份保護
•存取：最小的成功授權數
•未授權存取的最大全域失敗結構數
•目前的全域失敗存取
•全域參考條件
•白名單或黑名單或無
1
8
8
1

圖 18

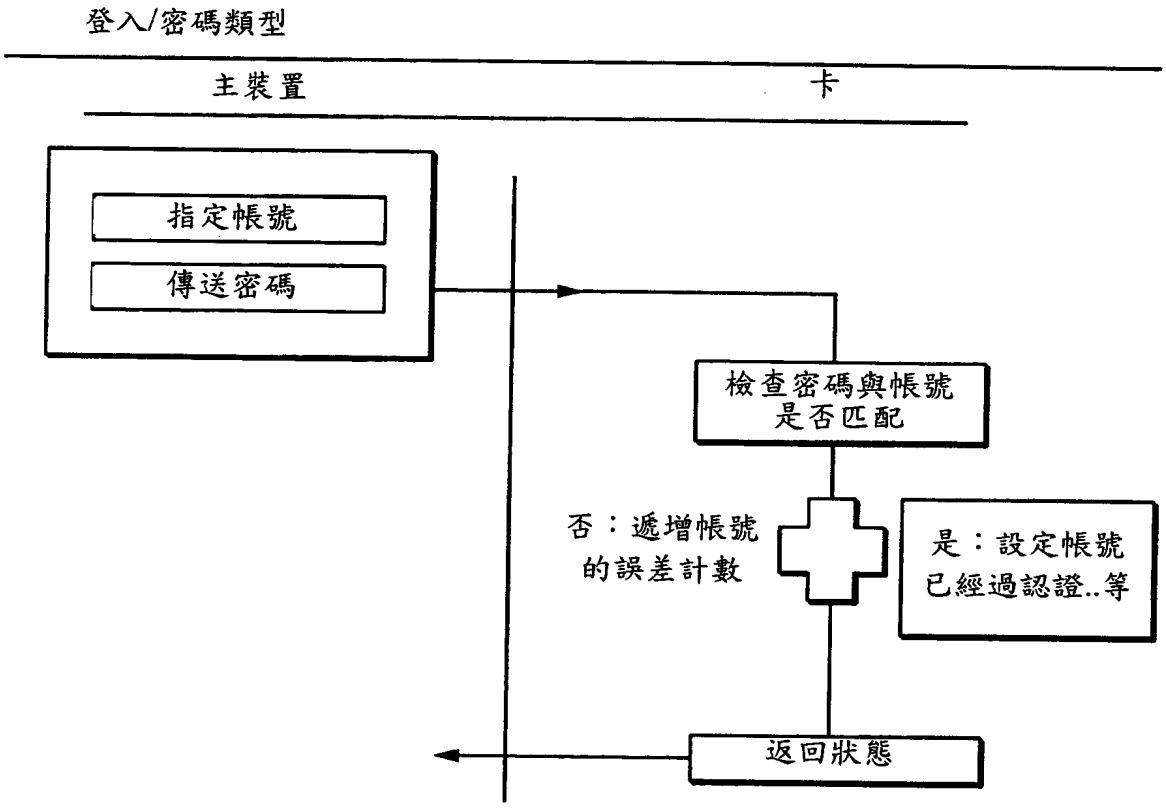

登入/密碼類型
主裝置
卡
指定帳號
傳送密碼
檢查密碼與帳號
是否匹配
否：遞增帳號
的誤差計數
是：設定帳號
已經過認證..等
返回狀態

圖 19

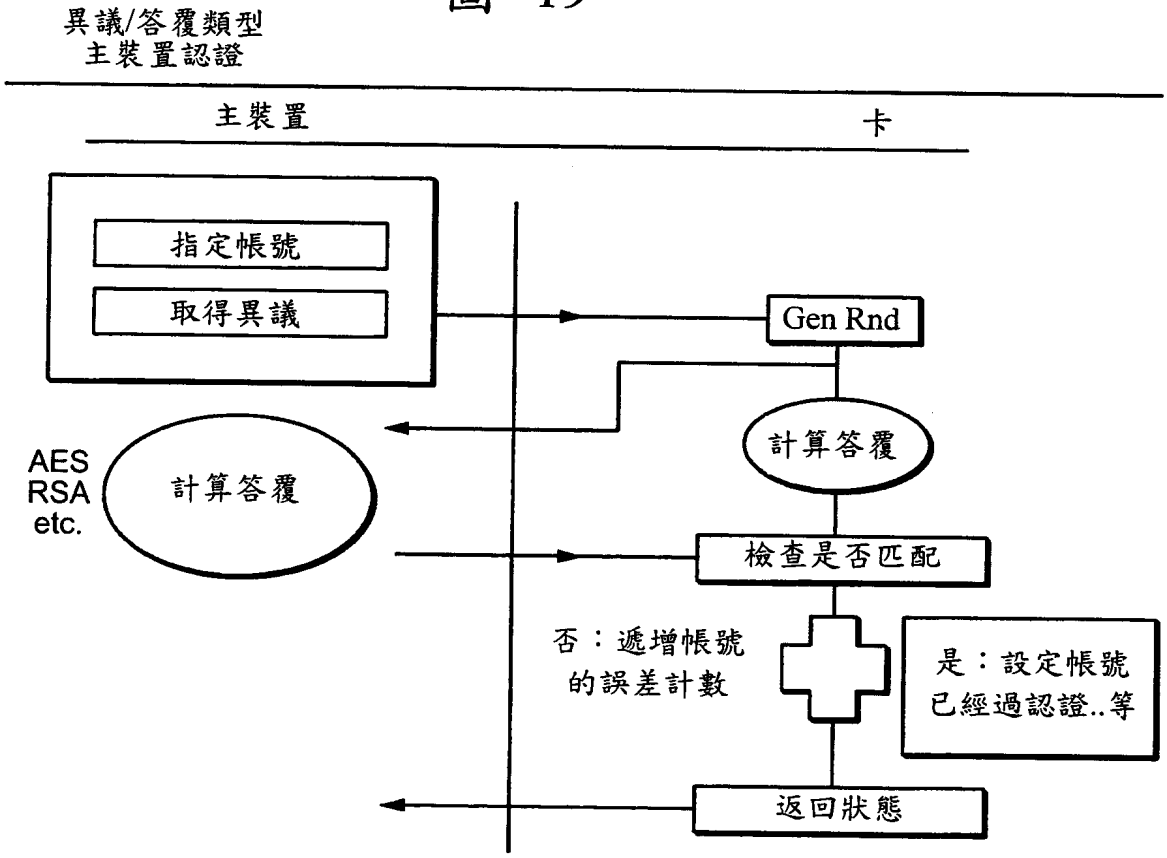

異議/答覆類型
主裝置認證
主裝置
卡
指定帳號
取得異議
Gen Rnd
計算答覆
AES
RSA
etc.
計算答覆
檢查是否匹配
否：遞增帳號
的誤差計數
是：設定帳號
已經過認證..等
返回狀態

圖 20

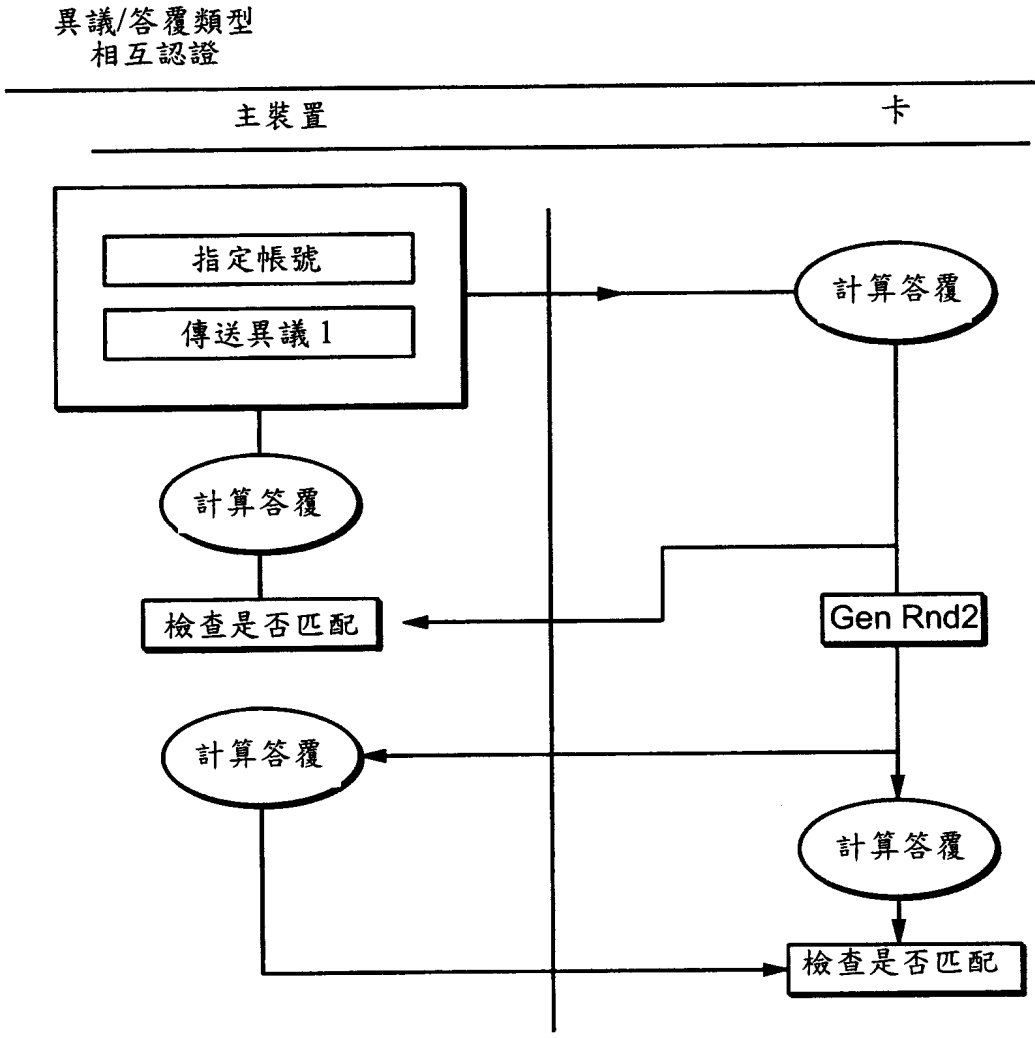

異議/答覆類型
相互認證
主裝置
卡
指定帳號
傳送異議 1
計算答覆
計算答覆
檢查是否匹配
Gen Rnd2
計算答覆
計算答覆
檢查是否匹配

圖 21

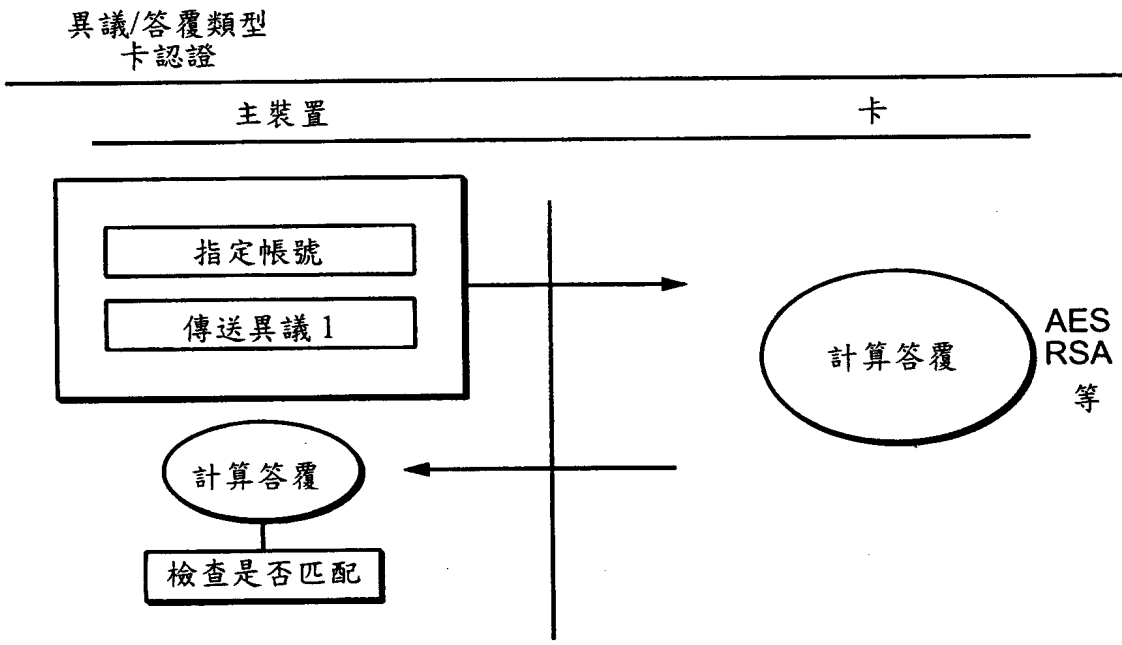

異議/答覆類型
卡認證
主裝置
卡
指定帳號
傳送異議 1
計算答覆
AES
RSA
等
計算答覆
檢查是否匹配

圖 22

四、指定代表圖：

(一)本案指定代表圖為：第（ 2 ）圖。

(二)本代表圖之元件符號簡單說明：

20	快閃記憶體
101	檔案
102	檔案
104	檔案
106	檔案

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

（無）