I384829

公告本

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：94113083

※ 申請日期：94.4.25　　※IPC 分類：H04L9/00

一、發明名稱：（中文/英文）

認證廢止列表之分散式管理

DISTRIBUTED MANAGEMENT OF A CERTIFICATE REVOCATION LIST

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

湯姆森授權股份有限公司 / THOMSON LICENSING SA

代表人：（中文/英文）

曼費德 羅斯曼尼茲 / ROSMANITH, MANFRED

住居所或營業所地址：（中文/英文）

法國 92100 布羅紐市葛格-亞爾風斯路 46 號

46 Quai Alphonse Le Gallo, 92100 BOULOGNE, FRANCE

國　籍：（中文/英文）

法國 / FRANCE

三、發明人：（共 1 人）

姓　名：（中文/英文）

亞倫 杜蘭德 / DURAND, ALAIN

國　籍：（中文/英文）

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：

歐洲專利；2004.05.03；04 291 124.8

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

在用於管理認證廢止列表（CRL）的方法中，第一設備（31，61）接收包括至少一個廢止認證辨識元（SN_i）的該 CRL（33，67）。使用保密資料（K_{CRL}）計算與該 CRL（37_1，…，37_p）的項相關聯的完整性欄位（MAC_i），其中項包括該 CRL 的至少一個廢止認證辨識元。將該項以及所計算的其相關聯的完整性欄位傳輸到不同於該第一設備的第二設備（32，62）；並將其儲存到該第二設備中。該方法進一步包括檢查認證的有效性。

六、英文發明摘要：

In a method for managing a Certificate Revocation List (CRL), a first device (31, 61) receives the CRL (33, 67) which comprises at least one revoked certificate identifier (SN_i). An integrity field (MAC_i) associated to an entry of the CRL (37_1,..., 37_p) is calculated using a secret data (K_{CRL}), wherein an entry comprises at least one revoked certificate identifier of the CRL. The entry and its associated calculated integrity field are transmitted to a second device (32, 62), distinct from the first device and are stored into the second device. The method further comprises checking a validity of a certificate.

七、指定代表圖：

(一)本案指定代表圖為：第（ 3A及3B ）圖。

(二)本代表圖之元件符號簡單說明:

31	第一設備
32	第二設備
33	CRL
34	第二記憶體
35	處理裝置
36	第一記憶體
37_1，…，37_P	項
38	加密裝置
39	拾取裝置
SN_1，…，SN_P	廢止認證辨識元
MAC_i	完整性欄位
SN_{i0}	廢止認證辨識元
MAC_{i0}	完整性欄位
SES_i	安全項集
K_{CRL}	CRL 密鑰
$SES_1,\cdots,SES_i,\cdots,SES_p$	安全項集
SES_{i0}	安全項集
310	評估裝置
311	驗證裝置
$SES_1,\cdots,SES_j,\cdots,SESj_{MAX}$	安全項集

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

九、發明說明：

【發明所屬之技術領域】

本發明係關於安全數位網路。

【先前技術】

表示內容的數位資料經過通訊網路進行傳輸所引起的問題是需要對所交換的資料進行保護和對資料拷貝的許可或禁止進行管理。

爲了解決這些問題，多媒體硬體製造商已經提出的解決方案有，以數位形式傳輸內容而禁止這些內容的非法拷貝。這些解決方案通常牽涉到使用密碼系統，其中經過受託方、例如經過鑒定機構產生一個或多個密鑰，以及使用所謂的適應性設備或模組。每一密鑰與認證相關聯。該認證加密地將該密鑰及其所有者的身份結合在一起。

可能會出現這樣的情況，即密鑰或包含秘密的適應性設備或模組被盜用。在前一種情況下，“盜竊者”成功地得到了該密鑰。在後一種情況下，“盜竊者”得到了該秘密。

安全數位網路的一個範例是用於安全數位內容廣播的系統。

已知在用於安全數位內容廣播的系統中，需要管理包含密鑰、設備或模組的辨識元的廢止列表，其不再被受託第三方認爲是適應性的，因爲受託方已經知道了它們被盜用的事實。

該廢止列表必須傳輸給該系統中的所有參與方，使得不再適用的密鑰、設備或模組可以被標識，並不再被使用。例如，該系統的適應設備係拒絕與非適應設備通信，或與傳輸非適應密鑰的設備通信。

爲了使得這樣更有效，需要讓該適應設備總是能夠存取該廢止列表。

更具體地，該廢止列表可以包含不再被信任的認證列表。這種列表也就是熟知的認證廢止列表（CRL）。

CRL 典型地包括項列表。爲了進行唯一地標識，經過 CRL 發行者，例如經過受託第三方簽發該 CRL 及記上日期。每一 CRL 項可以包括所要廢止的認證的序列號和廢止日期。

在該安全數位網路中使用的設備可以在其硬體規範上有所限制。這種設備可能不具備足夠的儲存和/或處理能力來在其記憶體中儲存全部 CRL 和處理儲存在其記憶體中的 CRL，以檢查密鑰即與該密鑰相關聯的認證是否出現在該 CRL 中。這種設備的範例就是廣泛使用的智慧卡，其具有包括記憶體和處理單元的電子電路。智慧卡頻繁地被用來對資料進行加密或解密。

圖 1 所述的範例爲根據先前技術的智慧卡。該智慧卡 11 包括塑膠卡 12 和內置的微晶片 13，其能夠安全地儲存加密資訊。該微晶片 13 包括能夠與外部設備通信的接腳 14。該微晶片 13 具有相對較小尺寸的記憶體：該智慧卡可能不能夠儲存全部的 CRL。

然而，有可能使用智慧卡對於存在的所確定的認證逐步地檢查所簽發的 CRL。這樣就避免將全部的 CRL 儲存在該智慧卡的記憶體中。

圖 2A 所述的範例爲根據先前技術使用智慧卡檢查 CRL 的第一種方法。CRL21 以連續的小資料塊傳輸給智慧卡 22。典型地，CRL21 包括 CRL 辨識元 N_{CRL}、CRL 簽字 S_{CRL} 和複數個項（24_1、24_2、…24_{MAX}），每一項包含關聯的所廢止的認證的序列號（SN_1、SN_2、…SN_{MAX}）。所傳輸的每一小資料塊可以包括一個項或多個項，每一項包含單個所廢止認證的序列號 SN_i。智慧卡 22 處理每一小資料塊，以檢查是否存在對應於所確定認證的項：典型地，智慧卡 22 的處理裝置 23 將所確定認證的序列號 SN0 與所傳輸的廢止認證的序列號 SN_i 進行比較。

爲了檢查該 CRL 簽字 S_{CRL}，該智慧卡計算連續接收的小資料塊的雜湊值。設計在產生該 CRL 簽字 S_{CRL} 中所使用的雜湊函數，使得可以逐塊地計算雜湊值。在已經接收了所有的小資料塊、即全部 CRL，並獲得總雜湊值之後，將驗證函數施加於該雜湊值、產生簽字的受託第三方的公用密鑰以及該 CRL 簽字 S_{CRL}，從而可以檢查該 CRL 的完整性。對於該智慧卡所要檢查的每個新認證而言，需要重複 CRL 的該完整性檢查。

圖 2B 所述的範例爲根據先前技術，使用 CRL 用於對所確定的認證的有效性進行檢查的第二種方法。CRL21 儲存在主機設備 26 中，該主機設備不同於智慧卡 22。將所

確定認證的認證辨識元 SN0 從該智慧卡 22 傳輸到該主機設備 26。

第二設備 26 的處理裝置 25 在儲存在該主機設備 26 內的 CRL21 的廢止認證辨識元（SN_1、SN_2、…SN_{MAX}）中查找該認證辨識元 SN0。

該主機設備 26 接下來將查找的結果傳送給智慧卡 22，以指示所確定的認證是否有效。

例如，如果在 CRL21 內查找到相關的廢止認證辨識元等於所傳輸的認證辨識元 SN0，該主機設備 26 將第一值分配給布林變數 BV，例如將布林變數 BV 重置。如果處理裝置 25 在 CRL21 內沒有找到等於所傳輸的認證辨識元 SN0 的任何相關的廢止認證辨識元，該主機設備 26 將第二值分配給該布林變數 BV，例如重置該布林變數 BV。

該主機設備 26 將該布林變數 BV 傳輸給該智慧卡 22。該布林變數 BV 的值向該智慧卡 22 指示，該 CRL21 是否包括等於將檢查的該認證辨識元 SN0 的相關廢止認證辨識元。只有當所傳輸的布林變數 BV 被重置時，所確定的該認證才被評估爲有效。如果所傳輸的布林變數 BV 被重置時，所確定的該認證被評估爲無效。

該 CRL21 典型地包括 CRL 辨識元 N_{CRL} 和 CRL 簽字 S_{CRL}。

該智慧卡 22 也可以儲存 CRL 辨識元 N_{CRL}；當需要檢查所確定的認證時，該智慧卡 22 傳輸所儲存的 CRL 辨識元 N_{CRL} 的值，從而能夠檢查儲存在該主機設備 26 內的

CRL21 是當前有效的 CRL。

該 CRL 簽字 S_{CRL} 使得能夠檢查 CRL21 的整體性。

【發明內容】

在第一方面，本發明提供一種用於管理認證廢止列表（CRL）的方法。在第一設備處接收該 CRL。該 CRL 包括至少一個所廢止的認證辨識元。使用保密資料計算與該 CRL 的項相關聯的完整性欄位，其中項包括該 CRL 的至少一個所廢止的認證辨識元。將該項以及所計算的其相關聯的完整性欄位傳輸到不同於該第一設備的第二設備。該方法進一步包括：將所傳輸的該項和該相關的完整性欄位儲存到該第二設備中。

在第一較佳實施例中，在第一設備中執行將該認證廢止列表（CRL）劃分到各項中。

在第二較佳實施例中，該完整性欄位是訊息鑒別碼。將與所接收到的 CRL 相關聯的認證廢止列表（CRL）密鑰選擇作爲該保密資料並將其儲存在該第一設備中。

在第三較佳實施例中，該方法進一步包括對中間資料施加雜湊函數，以計算該訊息鑒別碼。可以從包含至少一個廢止認證辨識元的項以及從該 CRL 密鑰得到該中間資料。

在第四較佳實施例中，在該第二設備中儲存多個所廢止的認證辨識元。將所儲存的廢止認證辨識元組織成爲至少一個安全項集的列表。每一安全項集包括至少一個廢止

認證辨識元、至少一個相關聯的完整性欄位以及該 CRL 的 CRL 辨識元。對於每一安全項集，產生列表順序欄位。該列表順序欄位所具有的內容能夠在儲存於該第二設備中的該安全項集列表內確定安全項集的順序。

在第五較佳實施例中，將該 CRL 的 CRL 辨識元儲存到該第一設備中。

在第六較佳實施例中，該方法進一步包括使用包含在該 CRL 內並經過發行該 CRL 的受託第三方所產生的認證廢止列表（CRL）簽字來檢查所接收到的 CRL 的完整性。

在第七較佳實施例中，所接收到的 CRL 的完整性檢查包括計算所接收到的 CRL 的雜湊值，並對所計算的雜湊值、受託第三方的公用密鑰以及該簽字施加驗證函數，以評估該 CRL 的完整性。

在第八較佳實施例中，在該第一設備接收 CRL 的小資料塊。該 CRL 的小資料塊包括至少一個所廢止的認證辨識元。將包含至少一個所廢止的認證辨識元以及相關聯的完整性欄位的至少一個項傳輸給該第二設備。在任何接收 CRL 的其他小資料塊之前刪除所接收到的該 CRL 的小資料塊。

較佳地該第一設備是智慧卡，而該 CRL 辨識元是 CRL 的 CRL 序列號。

在第九較佳實施例中，該方法進一步包括檢查認證的有效性。將認證的認證辨識元從該第一設備傳輸到第二設備。檢查儲存在該第二設備中的項的列表，以估計該列表是否包括所具有的值對應於所傳輸的認證辨識元的值的相

關廢止認證辨識元。根據所檢查的結果將至少一個所廢止的認證辨識元以及相關聯的完整性欄位傳輸到該第一設備。該方法進一步包括：在該第一設備經過使用所傳輸的該相關完整性欄位來驗證該至少一個所傳輸的廢止認證辨識元的完整性，以及在該第一設備經過使用該至少一個所傳輸的廢止認證辨識元來評估該認證的有效性。

在第十較佳實施例中，使用該 CRL 密鑰來驗證所傳輸的該廢止認證辨識元的完整性。

在第十一較佳實施例中，儲存在第二設備中的列表的每一安全項集包括單個所廢止的認證辨識元。將相關安全項集的至少一部分傳輸到該第一設備。該相關的安全項集包含該相關的廢止認證辨識元。

在第十二較佳實施例中，該方法進一步包括：在該第一設備中，將包含在所傳輸的安全項集中的所傳輸的認證廢止列表（CRL）辨識元與所確定的 CRL 的辨識元進行比較。所傳輸的該 CRL 辨識元能夠確保儲存在該第二設備中的列表對應於所確定的該 CRL。該方法進一步包括：在該第一設備中，檢查相關的該廢止認證辨識元實際上等於該認證辨識元。

在第十三較佳實施例中，儲存在第二設備中的列表的每一安全項集包括單個所廢止的認證辨識元。該方法進一步包括將第一安全項集的至少一部分以及第二安全項集的至少一部分傳輸給該第一設備。該第一安全項集和該第二安全項集分別包含具有在所傳輸的認證辨識元的期望順序

之前和之後緊接的順序的廢止認證辨識元。

在第十四較佳實施例中，在該第一設備將包含在所傳輸的安全項集中的所傳輸的認證廢止列表（CRL）辨識元與所確定的 CRL 的辨識元進行比較。所傳輸的該 CRL 辨識元能夠確保儲存在該第二設備中的列表對應於所確定的該 CRL。該方法進一步包括：在該第一設備中，檢查該第一安全項集和該第二安全項集在儲存於該第二設備中的列表內是連續的。該方法進一步包括：在該第一設備中，檢查該第一安全項集和該第二安全項集分別包含具有在所傳輸的認證辨識元的期望順序之前和之後緊接的順序的廢止認證辨識元。

在第十五較佳實施例中，該列表的每一安全項集包括多個廢止認證辨識元。該多個廢止的認證辨識元在該安全項集內排序。

在第十六較佳實施例中，將相關安全項集的至少一部分傳輸到該第一設備。該相關的安全項集包含該相關的廢止認證辨識元。

在第十七較佳實施例中，該方法進一步包括：在該第二設備中，查找包括第一廢止認證辨識元和第二廢止認證辨識元的替代安全項集。該第一廢止認證辨識元和第二廢止認證辨識元分別具有在該相關認證辨識元的期望順序之前和之後緊接的順序。將該替代安全項集傳輸到該第一設備。

在第十八較佳實施例中，將第一替代安全項集和第二

替代安全項集傳輸到該第一設備。該第一替代安全項集和該第二替代安全項集分別包含該第一廢止認證辨識元和該第二廢止認證辨識元。

在第十九較佳實施例中，在該第一設備將包含在所傳輸的安全項集中的所傳輸的認證廢止列表（CRL）辨識元與所確定的 CRL 的辨識元進行比較。所傳輸的該 CRL 辨識元能夠確保儲存在該第二設備（62）中的列表對應於所確定的該 CRL。

在第二十較佳實施例中，該列表順序欄位的內容是索引，該索引對應於該列表內的安全項集的順序。該第一設備儲存最大索引，該最大索引對應於該列表的最後一個安全項集的索引。

在第二十一較佳實施例中，該列表順序欄位的內容是關於該列表內前一安全項集的資訊。該第一設備儲存該列表的第一個安全項集和最後一個安全項集。

較佳地，該認證辨識元是認證序列號。

在第三方面，本發明提供一種用於管理認證廢止列表（CRL）的設備，所述設備包括：

用於接收 CRL 的裝置，該 CRL 包括至少一個所廢止的認證辨識元；

用於使用保密資料計算與該 CRL 的項相關聯的完整性欄位的裝置，其中項包括該 CRL 的至少一個所廢止的認證辨識元；和

用於將該項以及所計算的其相關的完整性欄位傳輸到

不同於所述設備的第二設備的裝置。

在第二十二較佳實施例中，該設備進一步包括：

用於將所要檢查的認證的認證辨識元傳輸到該第二設備的裝置；

用於從該第二設備接收包含至少一個廢止認證辨識元和至少一個相關聯的完整性欄位的至少一個項的裝置；

用於經過使用所傳輸的該相關聯的完整性欄位來驗證該至少一個所傳輸的廢止認證辨識元的完整性的裝置；和

用於使用至少一個所傳輸的廢止認證辨識元評估該認證的有效性的裝置。

在第四方面，本發明提供一種用於儲存認證廢止列表（CRL）的設備，所述設備包括：

用於從第一設備接收包含該 CRL 的至少一個廢止認證辨識元的至少一個項以及與該項相關聯的完整性欄位的裝置；

記憶體，用於儲存多個廢止認證辨識元，所儲存的廢止認證辨識元被組織成爲至少一個安全項集的列表，每一安全項集包括至少一個廢止認證辨識元、至少一個相關聯的完整性欄位以及該 CRL 的 CRL 辨識元；其中每一安全項集包括列表順序欄位，該列表順序欄位具有能夠在儲存於所述設備中的該安全項集的列表內確定安全項集的順序的內容。

在第二十三較佳實施例中，該設備進一步包括：

用於從第一設備接收認證辨識元的裝置；

處理裝置，用於檢查儲存在該記憶體中的項的列表，從而估計該列表是否包括所具有的值對應於所傳輸的認證辨識元的值的相關廢止認證辨識元；和

用於根據所檢查的結果將至少一個廢止認證辨識元以及該相關聯的完整性欄位傳輸到該第一設備的裝置。

從下面的敘述和所附的申請專利範圍可以清楚本發明的其他方面和優點。

【實施方式】

一般經過將所要檢查的認證的辨識元與認證廢止列表（CRL）的廢止認證的辨識元進行比較來檢查認證的有效性。

單一設備可以包括用於儲存該 CRL 的記憶體和用於執行該比較的處理裝置。

可替代地，該設備可以是受限的記憶體：例如，能夠保護所要檢查的認證和其他安全資料，但是不能將全部 CRL 儲存在其記憶體中的智慧卡。

在根據現有技術的第一種方法中，每次需要檢查認證時，逐個小資料塊接著小資料塊將該 CRL 下載到該設備中。在該設備中處理所下載的每一小資料塊，並在下載其他小資料塊之前將其刪除。可以證明這樣是相對比較耗時的。

在根據現有技術的第二種方法中，主機設備儲存該 CRL，並在該 CRL 中進行查找認證辨識元。將所查找的結

果，例如表示該認證是否被檢查爲有效的布林變數傳輸給該設備，例如智慧卡。

然而，駭客可以向該智慧卡傳輸假的查找結果。將該查找的結果改變，使得該認證被評估爲有效。例如，該智慧卡接收假的布林變數，其具有表示該認證有效的值。

因此需要一種系統和方法，能夠使用記憶體受限的設備更加安全地檢查認證的有效性。

圖 3A 和 3B 所述的範例爲根據本發明的系統。

該系統包括第一設備 31 以及不同於該第一設備 31 的第二設備 32。如圖 3A 中所述，該第一設備 31 初始接收 CRL33，處理所接收到的 CRL33，並將所處理的 CRL 傳輸到該第二設備 32。該第二設備 32 包括能夠儲存所處理的 CRL 的第二記憶體 34。

在該第一設備 31 所接收到的該 CRL33 包括至少一個廢止認證辨識元（SN_1，…，SN_P）。

所接收到的 CRL33 在該第一設備 31 中進行處理，以將其劃分成多個項（37_1，…，37_P），每一項包括至少一個廢止認證辨識元，並然後爲該 CRL 的每一項計算完整性欄位（MAC_i）。該計算包括保密資料，例如保密函數或者密鑰。

將所計算的完整性欄位（MAC_i）以及相關聯的包括至少一個廢止認證辨識元的項（SN_i）傳輸到該第二設備（32），並儲存在其中。

如果需要評估具有認證辨識元 SN0 的認證，將該認證

辨識元 SN0 傳輸到該第二設備 32，如圖 3B 中所示。該第二設備的處理裝置 35 能夠檢查儲存在該第二記憶體 34 中的所處理的 CRL，從而估計該處理的 CRL 是否包括所具有的值等於該認證辨識元 SN0 的值的相關廢止認證辨識元。

可替代地，該處理裝置是第三設備的一部分，該第三設備不同於該第一設備和該第二設備。

該第二設備 32 根據該檢查的結果，將結果資料輸出到該第一設備 31。該結果資料包括該列表的至少一個廢止認證辨識元 SN_{i0} 以及相關聯的完整性欄位 MAC_{i0}。

所傳輸的該完整性欄位 MAC_{i0} 能夠檢查相關聯的該廢止認證辨識元 SN_{i0} 的完整性。

接下來使用所傳輸的廢止認證辨識元 SN_{i0} 來評估該認證 SN0 的有效性。

本發明的系統能夠快速地評估儲存在具有相對較小記憶體的第一設備中的認證的有效性。該第一設備必須在初始步驟僅一次處理 CRL，如圖 3A 中所述。將所處理的 CRL 儲存在第二設備中，其能夠在該第二設備查找該認證的認證辨識元。

根據先前技術的第一種方法包括將該 CRL 逐個小資料塊地下載到該第一設備，其比本發明的方法要更加耗時。

而且，本發明的方法包括驗證所傳輸的結果資料的完整性，其能夠檢查所傳輸的廢止認證辨識元 SN_{i0} 的內容中的任何改變。本發明的方法因此比根據現有技術的第二種方法能夠對認證的有效性進行更加安全的檢查。

再次參照圖 3A，典型地在該第一設備 31 逐個小資料塊的接收該 CRL33。處理每一小資料塊，並在第一設備 31 刪除其之前將其傳輸到第二設備 32。

在圖 3A 中所述的範例中，每一小資料塊可以包括一個或多個廢止 認證辨識元（SN_1，…，SN_p）。

對在該第一設備 31 所接收到的 CRL33 的小資料塊進行的處理包括：將該小資料塊劃分成一個或幾個項 37_i（每一項包括單個廢止認證辨識元或多個廢止認證辨識元），以及爲每一項 37_i 產生安全項集 SES_i。將每一安全項集 SES_i 傳輸到該第二設備 32 並將其儲存在該第二記憶體 34 中。

從相關聯的項 37_i 產生每一安全項集 SES_i。除了索引 i 之外，安全項集 SES_1 還包括至少一個相關聯的項 37_i 的廢止認證辨識元 SN_i、爲該項 37_i 計算的完整性欄位 MAC_i 以及 CRL33 的 CRL 辨識元 N_{CRL}。

將該 CRL 的 CRL 辨識元 N_{CRL} 保持在第一設備 31 的第一記憶體 36 中。

該完整性欄位較佳地是訊息鑒別碼 MAC_i。在該第一設備 31，根據該相關聯的項 37_i 的一個廢止認證辨識元或多個辨識元 SN_i 以及根據在該第一設備 31 中所選擇的 CRL 密鑰 K_{CRL} 計算該訊息鑒別碼 MAC_i。

該 CRL 密鑰 K_{CRL} 可以附屬到所確定的 CRL，並且因此當在第一設備 31 接收到新的 CRL 時將其替代。可替代地，將該 CRL 密鑰 K_{CRL} 附屬到該第一設備 31 並保持相同的值。

典型地，該第一設備 31 包括拾取裝置 39，以隨機地拾取 CRL 密鑰 K_{CRL}。對中間資料施加雜湊函數以計算該訊息鑒別碼 MAC_i。根據該相關聯的項 37_i 的一個廢止認證辨識元或多個辨識元 SN_i 以及根據 CRL 密鑰 K_{CRL} 得到該中間資料。

例如，該中間資料以二進位的形式儲存，並包括對應於該相關聯的項 37_i 的一個廢止認證辨識元或多個辨識元 SN_i 的辨識元比特，隨後是對應於 CRL 密鑰 K_{CRL} 的密鑰比特。所計算的訊息鑒別碼 MAC_i 具有取決於該一個廢止認證辨識元或多個辨識元 SN_i 以及該 CRL 密鑰 K_{CRL} 的值。

可替代地，在施加雜湊函數之前或之後使用 CRL 密鑰 K_{CRL} 對該項的一個廢止認證辨識元或多個辨識元 SN_i 進行加密。

也可以經過對該項的一個廢止認證辨識元或多個辨識元 SN_i 施加保密函數來計算該完整性欄位。該加密函數可以保存在該第一設備中。

更一般地，該完整性欄位可以是能夠驗證該項的一個廢止認證辨識元或多個辨識元 SN_i 的完整性的任何其他資料。

該訊息鑒別碼 MAC_i 的計算也可以包括安全項集 SES_i 的其他欄位，例如表示在儲存於該第二設備 32 中的列表中的該安全項集 SES_i 的順序的列表順序欄位。該訊息鑒別碼 MAC_i 因此能夠驗證該安全項集 SES_i 的完整性。

當在該第一設備 31 和該第二設備 32 之間進行傳輸時，

如果駭客成功地修改了廢止認證序列號 SN_i，則該完整性欄位 MAC_i 能夠檢查該修改。

該第一設備 31 經過包含在該 CRL33 內的 CRL 簽字 S_{CRL}，也能夠檢查所接收的 CRL33 自身的完整性，該簽字 S_{CRL} 經過發行該 CRL 的受託第三方產生。該第一設備 31 的加密裝置 38 能夠計算所接收到的 CRL33 的雜湊值。設計在產生該 CRL 簽字 S_{CRL} 中所使用的雜湊函數，使得可以逐塊地計算雜湊值。然後將驗證函數施加於所計算的該雜湊值、受託第三方的公用密鑰以及簽字 S_{CRL}，以評估該 CRL33 的完整性。

在根據現有技術的方法中需要爲每一個所要檢查的新認證重複該 CRL 的完整性檢查，與其不同的是，本發明的方法只需要在初始步驟，當下載了新 CRL 時執行該檢查。

圖 3A 中所示的系統能夠從該第一設備 31 存取該 CRL 的廢止認證辨識元。當需要評估認證時，將該認證辨識元 SN0 傳輸到該第二設備 32，如圖 3B 中所示。

認證辨識元 SN0 可以在所儲存的安全項集 $(SES_1,\cdots,SES_i,\cdots,SES_p)$ 的列表之中查找。該第二設備 32 根據該查找的結果將至少一個安全項集 SES_{i0} 的至少一部分傳輸到該第一設備 31。所傳輸的部分至少包括該安全項集 SES_{i0} 的廢止認證辨識元 SN_{i0} 以及完整性欄位 MAC_{i0}。

該第一設備 31 的驗證裝置 311 能夠驗證所傳輸的該廢止認證辨識元 SN_{i0} 的完整性。

接下來在該第一設備 31 的評估裝置 310 中至少使用所

傳輸的該廢止認證辨識元 SN_{i0} 來評估該認證的有效性。該評估典型地包括將所傳輸的廢止認證辨識元 SN_{i0} 與所要檢查的認證的辨識元 SN0 進行比較。

如果所傳輸的該廢止認證辨識元 SN_{i0} 與該認證辨識元 SN0 具有相同值，該認證被評估爲無效。

如果所傳輸的該廢止認證辨識元 SN_{i0} 與該認證辨識元 SN0 具有不同值，該認證被評估爲有效。

然而，該第一設備可以執行附加測試來檢測駭客所進行的攻擊。

該攻擊例如可以包括非法修改在該第二設備中所實施的演算法。例如，駭客修改該主機設備，使得該主機設備總是輸出舊的廢止認證辨識元以及相關聯的訊息鑒別碼：在這種情況下，該認證辨識元 SN0 與舊的廢止認證辨識元相等的機會非常小。

在將認證辨識元傳輸到該主機設備期間，駭客也可以成功地修改所要檢查的廢止認證的認證辨識元的值。該主機設備然後就不能找到該相關廢止認證辨識元。

該第一設備因此典型地執行附加測試，以檢測可能的攻擊，諸如修改主機設備所執行的演算法、或修改傳輸到該主機設備的認證辨識元的值。

例如，如果所傳輸的廢止認證辨識元 SN_{i0} 與該認證辨識元 SN0 之間的差值超出了預定的閾值，則該第一設備可以懷疑受到駭客攻擊。

該第一設備也可以儲存在檢查不同認證時從主機設備

接收到的先前的廢止認證辨識元：如果所傳輸的廢止認證辨識元 SN_{i0} 與所儲存的先前的廢止認證辨識元具有相同的值，則該認證可以被評估爲無效。

在本說明書進一步的段落中描述了一種較佳的方法，其能夠檢測可能出現的對主機設備執行的演算法所進行的修改，或者對所傳輸的認證辨識元進行的修改。

該第一設備 31 較佳地爲智慧卡。所要檢查的該認證可以附屬到該智慧卡上：例如，在製造智慧卡的時候將該認證下載到該智慧卡。可替代地，可以有規律地替代該認證。

該 CRL 辨識元 N_{CRL} 較佳地是該 CRL 的 CRL 序列號。

可替代地，該 CRL 辨識元 N_{CRL} 是該 CRL 的發行日期。

較佳地，每一認證辨識元是廢止認證的序列號或該序列號的一部分。

可替代地，該認證辨識元可以是認證本身。

該認證辨識元可以是能夠標示該對應認證的任何資料。

如圖 3A 和 3B 中所示，該拾取裝置 39、加密裝置 38、評估裝置 310 以及驗證裝置 311 可以是該第一設備 31 的四個不同元件。然而，該拾取裝置、加密裝置、評估裝置以及驗證裝置較佳地是單個處理單元，例如該智慧卡的微處理器的一部分。

該拾取裝置 39、加密裝置 38、評估裝置 310 以及驗證裝置 311 與該第一記憶體 36、例如與智慧卡記憶體通信。

本發明的第一較佳實施例

圖 4 所述爲在根據本發明第一較佳實施例的系統中，經過主機設備所執行的範例演算法。該第二設備是與第一設備，例如與智慧卡，通信的主機設備。

在初始步驟期間，該智慧卡將安全項集（$SES_1,\cdots,SES_j,\cdots,SESj_{MAX}$）的列表傳輸給該主機設備。每一安全項集包括單個廢止認證序列號（$SN_1,\cdots,SN_j,\cdots,SN_{jMAX}$）以及相關聯的訊息鑒別碼。

每一安全項集（$SES_1,\cdots,SES_j,\cdots,SESj_{MAX}$）進一步包括列表順序欄位。該列表順序欄位包括關於該列表內前一個安全項集的資訊。該列表內的第一個安全項集 SES_1 包括包含預定值的列表順序欄位。該智慧卡儲存第一個安全項集 SES_1 以及最後一個安全項集 $SESj_{MAX}$。該列表順序欄位的內容因此能夠在該列表內將該列表的安全項集$(SES_1,\cdots;SES_j,\cdots,SESj_{MAX})$進行排序。

可替代地，該列表順序欄位包含關於該列表內下一個安全項集的資訊，具有填充了預定值的列表順序欄位的最後一個安全項集 $SESj_{MAX}$。

可替代地，該列表順序欄位包括對應於該列表內的安全項集的順序的索引。

更一般地，該列表順序欄位具有能夠確定該列表內的安全項集的順序的內容。

該主機設備包括能夠儲存該列表的第二記憶體。在本發明的第一個較佳實施例中，該安全項集以關於廢止認證序列號$(SN_1,\cdots,SN_j,\cdots,SN_{jMAX})$的昇冪儲存在該列表中。

當認證需要被檢查時，該智慧卡將該認證的認證序列號 SN0 傳輸給主機設備。

該主機設備檢查該列表，以估計該列表是否包括所具有的值等於所傳輸的認證序列號 SN0 的值的相關廢止認證序列號。

首先，將所傳輸的認證序列號 SN0 與該列表的第一個廢止認證序列號 SN_1 進行比較（方塊 51）。

如果所傳輸的認證序列號 SN0 小於該第一個廢止認證序列號 SN_1，該主機設備將該第一安全項集 SES_1 傳輸給該智慧卡（方塊 52）。

如果所傳輸的認證序列號 SN0 大於該第一個廢止認證序列號 SN_1，進行第二檢測：將所傳輸的認證序列號 SN0 與該列表的最後一個廢止認證序列號 SN_{jMAX} 進行比較（方塊 53）。

如果所傳輸的認證序列號 SN0 大於該最後一個廢止認證序列號 SN_{jMAX}，該主機設備將該最後一個安全項集 SES_{jMAX} 傳輸給該智慧卡（方塊 54）。

如果所傳輸的認證序列號 SN0 大於該第一個廢止認證序列號 SN_1 並小於該最後一個廢止認證序列號 SN_{jMAX}，該主機設備將索引變數 i 重置（方塊 55）。該索引變數接下來開始遞增（方塊 56）。

進一步檢查所傳輸的認證序列號 SN0 是否等於對應於當前索引變數 i 的當前廢止認證序列號 SN_i（方塊 57）。

如果所傳輸的認證序列號 SN0 等於當前的廢止認證序

列號 SN_i，即該列表包括等於所傳輸的該認證序列號 SN0 的相關廢止認證序列號，該主機設備傳輸該相關安全項集 SES_i 作爲一個結果資料（方塊 58）。

否則，將當前的廢止認證序列號 SN_i 與所傳輸的該認證序列號 SN0 進行比較（方塊 59），如果 SN_i 小於 SN0，該索引變數 i 遞增（方塊 56）。

相反，如果 SN_i 大於 SN0，這就意味著 SN0 包括在 SN_{i-1} 與 SN_i 之間，該主機設備將對應於分跨在所傳輸的認證序列號 SN0 兩邊的兩個廢止認證序列號的兩個安全項集 SES_{i-1} 和 SES_i 作爲結果資料傳輸給該智慧卡（方塊 510）。

圖 4 中所示的在該列表中查找所傳輸的認證序列號 SN0 的演算法只是範例。可以使用各種演算法實施該查找。

圖 5 所述爲在根據本發明第一較佳實施例的系統中，經過智慧卡所執行的範例演算法。

該智慧卡與主機設備通信，其執行認證序列號 SN0 的查找，並且傳輸結果資料 RD，如圖 4 中所示。該智慧卡接收結果資料 RD（方塊 512），即儲存在該主機設備中的列表的一個或兩個安全項集。

該智慧卡檢查該結果資料 RD 是否包括一個或兩個安全項集（方塊 513）。

如果接收單個安全項集 SES_{i0} 作爲結果資料，那麼認爲儲存在該主機設備中的列表包括等於該認證序列號 SN0 的相關廢止認證序列號 SN_{i0}，或者認爲滿足“限制”條件之一（$SES_{i0}=SES_i$ 或者 $SES_{i0}=SES_{jMAX}$）。然後在將該認

證評估爲無效（方塊 517）之前執行多個檢查（方塊 514、515 和 516）。

第一個檢查包括驗證：包含在所接收的安全項集 SES_{i0} 內的所傳輸的 CRL 辨識元 $N_{CRL}^{(i0)}$ 等於在初始步驟中儲存在該智慧卡中的 CRL 辨識元 N_{CRL}。該第一個檢查能夠確保儲存在該主機設備中的該列表對應於所確定的實際生效的該認證廢止列表（CRL）。

第二個檢查（方塊 515）包括：根據包含在所傳輸的安全項集 SES_{i0} 中的訊息鑒別碼 MAC_{i0} 以及根據儲存在智慧卡中的 CRL 密鑰 K_{CRL}，驗證所傳輸的安全項集 SES_{i0} 的完整性。例如，該智慧卡對從該相關廢止認證序列號 SN_{i0} 以及從儲存在該智慧卡中的 CRL 密鑰 K_{CRL} 得到的中間資料施加雜湊函數，從而獲得該相關廢止認證序列號 SN_{i0} 的驗證碼。將該相關廢止認證序列號 SN_{i0} 的驗證碼與包含在所傳輸的安全項集 SES_{i0} 中的訊息鑒別碼 MAC_{i0} 進行比較：如果不同，則認爲所傳輸的安全項集 SES_{i0} 的內容發生了變化。

第三個檢查包括驗證該相關廢止認證序列號 SN_{i0} 實際等於認證序列號 SN0（方塊 516）。

如果成功地執行了這三個檢查(方塊 514、515 和 516)，那麼該認證被評估爲無效（方塊 517）。

如果在第三個檢查中，發現 SN_{i0} 不同於該認證序列號 SN0，那麼執行第四個檢查，其包括驗證 SN0 是否小於 SN_{i0}（方塊 524），僅當 $SES_{i0} = SES_1$ 時才出現這種情況。如果

該第四個檢查成功，那麼就認爲具有序列號 SN0 的該認證有效（方塊 522）。相反，執行第五個檢查，以驗證 SN0 是否大於 SN_{i0}（方塊 525），僅當 $SES_{i0} = SES_{jMAX}$ 時才出現這種情況。如果該第五個檢查成功，該認證就被評估爲有效（方塊 522）。

否則，如果在方塊 514、515 或 525 中所執行的任何一個檢查爲否，那麼就認爲該主機回應錯誤（方塊 523）。在這種情況下，根據所選擇的實施方式，該認證可以被評估爲無效或者重新啓動全部過程：該智慧卡 31 再次將所要檢查的該認證的序列號 SN0 傳輸給該主機 32，並等待另一個結果資料。可以重複從該主機對結果資料的請求，直至達到最大次數（例如兩次或三次）。

再次返回方塊 513，在對該結果資料的檢查之後，如果估計該結果資料包括一組兩個所傳輸的安全項集，則在能夠對該認證的有效性進行任何評估（方塊 522）之前執行多個檢查（方塊 518、519、520 和 521）。

將分別包含在第一個所接收到的安全項集 SES_{j0} 以及在第二個所接收到的安全項集 SES_{k0} 中的所傳輸的 CRL 辨識元 $N_{CRL}^{(j0)}$ 和 $N_{CRL}^{(k0)}$ 與儲存在該智慧卡中的 CRL 辨識元 N_{CRL} 進行比較（方塊 518）。這種第六檢查（方塊 518）能夠確保儲存在該主機設備中的列表對應於所確定的實際有效的認證廢止列表（CRL）。如果任何一個所傳輸的 CRL 辨識元 $N_{CRL}^{(j0)}$ 和 $N_{CRL}^{(k0)}$ 不同於儲存在該智慧卡中的 CRL 辨識元 N_{CRL}，就可以認爲該智慧卡或者該主機設備已經被

欺詐性地替代了。接下來可以認爲該認證是無效的。

根據包含在該第一個所傳輸的安全項集 SES_{j0} 中的訊息鑒別碼 MAC_{j0} 和根據儲存在該智慧卡中的 CRL 密鑰 K_{CRL} 驗證第一個所傳輸的安全項集 SES_{j0} 的完整性(方塊 519)。可以經過雜湊函數執行這種第七檢查：如在第二檢查（方塊 515）中的那樣，例如可以將該雜湊函數施加於從所傳輸的第一廢止認證序列號 SN_{j0} 和從該 CRL 密鑰 K_{CRL} 得到的中間資料。如果該第七檢查（方塊 519）導致認爲第一個所傳輸的安全項集 SES_{j0} 的內容發生了改變，可以將該認證評估爲無效。

類似地，根據包含在該第二個所傳輸的安全項集 SES_{k0} 中的訊息鑒別碼 MAC_{k0} 和根據儲存在該智慧卡中的 CRL 密鑰 K_{CRL} 驗證第二個所傳輸的安全項集 SES_{k0} 的完整性(方塊 519）。

接下來的檢查是該第一個所傳輸的安全項集 SES_{j0} 和該第二個所傳輸的安全項集 SES_{k0} 在儲存於該第二設備中的列表內實際上是連續的（方塊 520）。典型地經過使用所傳輸的安全項集 SES_{j0} 和 SES_{k0} 的列表順序欄位來執行這種第八檢查（方塊 520）。

如在第一較佳實施例中所述，如果該列表的給定安全項集的每一列表順序欄位包括關於前一安全項集的資訊，則該第八檢查可以包括：驗證包含在該第二個安全項集 SES_{k0} 的列表順序欄位內的資訊實際上對應於該第一個安全項集 SES_{j0}。

可替代地，該列表的給定安全項集的每一列表順序欄位包括給定安全項集的索引：在這種情況下，該檢查可以簡單地包括驗證與該第一個安全項集 SES_{j0} 以及該第二個安全項集 SES_{k0} 相關聯的索引實際上是連續的。

最後，該智慧卡檢查該第一個安全項集 SES_{j0} 和該第二個安全項集 SES_{k0} 分別位於緊接在儲存於該主機設備的列表內的相關安全項集之前和之後（方塊 521）。

在本發明的第一較佳實施例中，其中該列表的安全項集以關於該廢止認證序列號（$SN_1,\cdots,SN_j,\cdots,SN_{jMAX}$）的昇冪排列，該第九檢查（方塊 521）包括：驗證該認證序列號 SN0 具有介於分別包含在該第一個安全項集 SES_{j0} 和該第二個安全項集 SES_{k0} 中的第一個廢止認證序列號 SN_{j0} 的值與第二個廢止認證序列號 SN_{k0} 的值之間的值。

該第六檢查（方塊 518）、第七檢查（方塊 519）、第八檢查（方塊 520）和第九檢查（方塊 521）能夠提供更加完善安全的系統。實際上，該主機設備典型地是無保護的設備：駭客不僅可以改變在該智慧卡與該主機設備之間傳輸的資料，而且可以存取該主機設備的處理裝置以及修改所實施的演算法。

例如，使用現有技術的第二種方法，駭客可以修改該處理裝置，使得傳輸到該智慧卡的布林變數總是具有相同的值，即所要檢查的任何認證都被評估爲有效的。

使用根據本發明的系統，駭客可以修改所實施的演算法，使得對於所傳輸的認證辨識元 SN0 的任何值，總是向

該智慧卡傳輸相同配合的廢止認證辨識元和相關聯的訊息鑒別碼。典型地，該配合包括舊的廢止認證辨識元，從而確保任何相對新的認證被評估爲有效。然而，根據本發明第一實較佳施例的該方法能夠檢測主機設備的這種演算法的故障：具體而言，第九檢查（方塊 521）可以實現使得廢止認證辨識元的該配合實際上並不分跨在該列表內的所傳輸的辨識元的兩邊。接著，就可以將該認證辨識元評估爲無效。也可以阻止或禁止該智慧卡與該主機設備通信。

如果該第六檢查（方塊 518）、第七檢查（方塊 519）、第八檢查（方塊 520）和第九檢查（方塊 521）成功地執行，該認證就被評估爲有效（方塊 522）。

否則，如果在方塊 518、519、520 或 521 中所執行的任何一個檢查爲否，那麼就認爲該主機回應錯誤（方塊 523），這就意味著或者該認證被評估爲無效，或者再次啓動該處理，如前所述。

圖 5 所示只是在該智慧卡中實施的範例演算法。可以按照不同的順序執行檢查（方塊 514、515、516、518、519、520 和 521）。例如，可以在檢查該結果資料是否包括一個或兩個安全資料項目集之前，檢查所傳輸的 CRL 辨識元和所傳輸的安全項集的完整性：該智慧卡檢查一個所傳輸的 CRL 辨識元和單個所傳輸的安全項集的完整性，該結果資料是否包括一個或兩個安全項集。

本發明的第二較佳實施例

圖 6 所示的範例爲根據本發明第二較佳實施例的系

統。該系統包括第一設備，例如具有記憶體66的智慧卡61，以及與該第一設備61通信的第二設備，例如具有記憶體64和處理裝置65的主機設備62。首先在該智慧卡61中處理經過附圖標記67表示的認證廢止列表（CRL），以產生安全項集 SES_i，然後將其儲存在該主機記憶體64中。

在本發明的第二較佳實施例中，從該CRL的多個所廢止的認證序列號（$SN_1,\cdots SN_{jMAX}$）中產生每一安全項集 SES_i。每一安全項集 SES_i 可以包括預定數目的廢止認證序列號（例如四個），或者每一安全項集的廢止認證序列號的數目是可變的。

每一安全項集 SES_i 包括 CRL 辨識元 N_{CRL}，其是該CRL67的特徵，可以從其產生該安全項集。

該安全項集也包括定義該安全項集（$SES_1,\cdots, SES_i,\cdots, SES_{iMAX}$）之間的順序的列表順序欄位（$63_1,\cdots, 63_i,\cdots, 63_{iMAX}$），例如索引，如圖6中所示。

每一個單一安全項集 SES_i 的廢止認證序列號（$SN_{fi},\cdots SN_{li}$）也在該安全項集內排序，例如從第一個廢止認證序列號 SN_{fi} 至最後一個廢止認證序列號 SN_{li} 按照昇冪排列，如圖6中所示。

根據安全項集 SES_i 的多個廢止認證序列號（$SN_{fi},\cdots SN_{li}$）以及根據該CRL密鑰 K_{CRL} 進一步計算每一安全項集 SES_i 的訊息鑒別碼（$MAC_1,\cdots,MAC_i,\cdots, MAC_{iMAX}$）。可替代地，也可以使用安全項集 SES_i 的其他欄位來計算該 MAC_i 值。

該安全項集進一步可以包括附加欄位，例如具有該智慧卡的智慧卡辨識元的欄位，假設該主機設備能夠支援其工作。

該智慧卡儲存能夠進一步檢查從該主機設備接收到的結果資料的多個參數。典型地，該智慧卡儲存 CRL 辨識元 N_{CRL}，其是所確定的當前有效的 CRL 的特徵，在計算訊息鑒別碼（$MAC_1,\cdots,MAC_{16}$）中所使用的 CRL 密鑰 K_{CRL}。根據所選擇的實施方式，也可以在該智慧卡中儲存對應於該列表的最後一個安全項集 SES_{iMAX} 的最大索引 i_{MAX} 和/或每個安全項集的預定數目的廢止認證序列號。

當該智慧卡 61 需要檢查具有認證序列號 SN0 的認證的有效性，該智慧卡將認證序列號 SN0 傳輸給該主機設備 62，並且該主機設備在安全項集（$SES_1,\cdots,SES_i,\cdots,SES_{iMAX}$）的列表中查找該認證序列號 SN0。

如果該主機設備的處理裝置 65 發現該列表包括了相關安全項集 SES_{i0}，其所包含的相關廢止序列號 SN_{i0} 等於該認證序列號 SN0，則將該相關安全項集傳輸給該智慧卡作爲結果資料。

相反，如果該主機設備的處理裝置 65 沒有找到所包含的相關廢止序列號 SN_{i0} 等於該認證序列號 SN0 的任何相關安全項集，則該主機設備按照如下所述返回結果資料。

在第一替代形式中，我們假設該 CRL67 的廢止認證序列號（$SN_1,\cdots SN_{iMAX}$）沒有任何冗餘地儲存在該安全項集（$SES_1,\cdots,SES_i,\cdots,SES_{iMAX}$）中。在這種替代形式中：

或者該主機的處理裝置 65 可以找到相關的安全項集 SES_{i0}，其包含兩個廢止認證序列號 SN_j 和 SN_{j+1}，使得 $SN_j < SN0 < SN_{j+1}$，在這種情況下，該主機 62 將該相關的安全項集 SES_{i0} 作爲結果資料發送給該智慧卡 61；

或者該主機的處理裝置 65 發現相關認證序列號 SN0 包括在安全項集 SES_{i0} 的最後一個廢止認證序列號 SN_{li0} 與下一個安全項集 SES_{i0+1} 的第一個廢止認證序列號 SN_{fi0+1} 之間，在這種情況下，該主機 62 將該連續的安全項集 SES_{i0} 和 SES_{i0+1} 作爲結果資料發送給該智慧卡 61。

在第二替代形式中，我們假設該 CRL67 的廢止認證序列號（$SN_1, \cdots SN_{iMAX}$）儲存在該安全項集（$SES_1, \cdots, SES_i, \cdots, SES_{iMAX}$）中，使得給定安全項集 SES_i 的每一最後一個廢止認證序列號 SN_{li}（除了最後一個安全項集 SES_{iMAX}）也被儲存作爲接續的安全項集 SES_{i+1} 的第一個廢止認證序列號 SN_{fi+1}，即 $SN_{li} = SN_{fi+1}$。在該第二替代形式中，該主機的處理裝置 65 應該總是能夠找到包含兩個廢止認證序列號 SN_j 和 SN_{j+1} 的相關安全項集 SES_{i0}，使得 $SN_j < SN0 < SN_{j+1}$，在這種情況下，該主機 62 將該相關的安全項集 SES_{i0} 作爲結果資料發送給該智慧卡 61。

然而在上述兩個替代形式中，我們可以具有的“限制”條件是該認證序列號 SN0 小於該列表的第一個安全項集 SES_1 的第一個廢止認證序列號 $SN_{f1} = SN_1$，在這種情況下，該主機 62 向該智慧卡 61 傳輸第一個安全項集 SES_1。

類似地，如果該認證序列號 SN0 大於該列表的最後一

個安全項集 SES_{iMAX} 的最後一個廢止認證序列號 $SN_{liMAX}=SN_{jMAX}$，在上述兩種替代形式中可以滿足另一“限制”條件，在這種情況下，該主機設備 62 向該智慧卡 61 傳輸最後一個安全項集 SES_{iMAX}。

如在本發明的第一較佳實施例中所述，該智慧卡 61 根據所接收到的結果資料執行多個檢查。

在第二較佳實施例中，該結果資料包括該列表的至少一個安全項集 SES_{i0}。該智慧卡 61 檢查包含在所傳輸的安全項集中的所傳輸的 CRL 辨識元 N_{CRL} 實際上等於儲存在該智慧卡 61 中的 CRL 辨識元，於是能夠確保儲存在該主機設備中的列表對應於有效的 CRL。

也可以根據相關聯的訊息鑒別碼 MAC_{i0} 和根據儲存在該智慧卡 61 中的 CRL 密鑰 K_{CRL} 驗證至少一個所傳輸的安全項集 SES_{i0} 的完整性。

如果該結果資料包括單個安全項集，所傳輸的該安全項集可以包含等於該認證序列號 SN0 的相關廢止認證序列號，其可以包含使得 $SN_j < SN0 < SN_{j+1}$ 的兩個廢止認證序列號 SN_j 和 SN_{j+1}，或者如果滿足上述“限制”條件的其中一個，則所傳輸的該安全項集可以等於 SES_1 或 SES_{iMAX}。該智慧卡因此確定該單個安全項集 SES_{i0} 是否包括該相關的認證序列號 SN0。

在前一種情況下，估計該認證序列號 SN0 包含在當前認證廢止列表中，並且對應的認證是無效的。

在後一種情況下，該智慧卡檢查所接收的 SES_{i0} 的單

個安全項集實際上包括使得 $SN_j < SN0 < SN_{j+1}$ 的兩個廢止認證序列號 SN_j 和 SN_{j+1}，或者該認證序列號 SN0 小於該安全項集 SES_{i0} 的第一個廢止認證序列號 SN_{fi0}（如果 $SES_{i0} = SES_1$），或者 SN0 大於該安全項集 SES_{i0} 的最後一個廢止認證序列號 SN_{li0}（如果 $SES_{i0} = SES_{iMAX}$）。

如果該智慧卡所接收到的結果資料包括兩個安全項集 SES_{i0} 和 SES_{i0+1}，則該智慧卡 61 在兩個安全項集的廢止認證序列號中查找使得 $SN_j < SN0 < SN_{j+1}$ 的兩個廢止認證序列號 SN_j 和 SN_{j+1}。

當已經在該結果資料中識別兩個廢止認證序列號 SN_j 和 SN_{j+1} 時，不管該結果資料是否包括一個或兩個安全項集，該智慧卡檢查這兩個廢止認證序列號 SN_j 和 SN_{j+1} 實際上在該列表中是連續的。接下來將該認證評估爲有效。

當滿足“限制”條件之一時，即當該認證序列號 SN0 小於所接收到的安全項集 SES_{i0} 的第一個廢止認證序列號 SN_{fi0}（如果 $SES_{i0} = SES_1$），或者當 SN0 大於該安全項集 SES_{i0} 的最後一個廢止認證序列號 SN_{li0}（如果 $SES_{i0} = SES_{iMAX}$）時，具有序列號 SN0 的認證也可以估計爲有效。

雖然已經描述了本發明有限數目的實施例，但是熟習本項技術者在本說明書的基礎上可以理解的是，不脫離此處所描述的本發明的範圍可以得到其他的實施例。相應地，本發明之範疇係應該只受限於所附的申請專利範圍。

【圖式簡單說明】

圖 1 所述的範例爲根據先前技術的智慧卡。

圖 2A 所述的範例爲根據先前技術，使用智慧卡檢查 CRL 的方法。

圖 2B 所述的範例爲根據先前技術，使用 CRL 用於對所確定的認證的有效性進行檢查的第二種方法。

圖 3A 和 3B 所述的範例爲本發明的系統。

圖 4 所述爲在根據本發明第一較佳實施例的系統中，經過主機設備所執行的範例演算法。

圖 5 所述爲在根據本發明第一較佳實施例的系統中，經過智慧卡所執行的範例演算法。

圖 6 所述的範例爲根據本發明第二較佳實施例的系統。

【主要元件符號說明】

11	智慧卡
12	塑膠卡
13	微晶片
14	接腳
22	智慧卡
SN_1、SN_2、…SN_{MAX}	智慧卡
23	處理裝置
S_{CRL}	簽字
21	認證廢止列表(CRL)
26	主機設備

SN0	認證辨識元
24	處理裝置
SN_1、SN_2、…SN_{MAX}	廢止認證辨識元
BV	布林變數
N_{CRL}	CRL 辨識元
S_{CRL}	CRL 簽字
31	第一設備
32	第二設備
33	CRL
34	第二記憶體
SN_1，…，SN_P	廢止認證辨識元
37_1，…，37_P	項
MAC_i	完整性欄位
35	處理裝置
SN_{i0}	廢止認證辨識元
MAC_{i0}	完整性欄位
SES_i	安全項集
K_{CRL}	CRL 密鑰
39	拾取裝置
SES_1,…,SES_i,…,SES_p	安全項集
SES_{i0}	安全項集
311	驗證裝置
310	評估裝置
38	加密裝置

36	第一記憶體
$SES_1,\cdots,SES_j,\cdots,SESj_{MAX}$	安全項集
$SN_1,\cdots,SN_j,\cdots,SN_{jMAX}$	廢止認證序列號
66	記憶體
61	智慧卡
64	記憶體
65	處理裝置
62	主機設備
66	標記
$63_1,\cdots,63_i,\cdots,63_{iMAX}$	列表順序欄位
$SN_{fi},\cdots SN_{li}$	廢止認證序列號
$MAC_1,\cdots,MAC_{16}$	訊息鑒別碼
i_{MAX}	最大索引
67	CRL

十、申請專利範圍：

1.一種用於管理認證廢止列表（CRL）的方法，該方法包括：

在第一設備（31，61）接收該 CRL（33，67），該 CRL 包括至少一個所廢止的認證辨識元（SN_i）；

在第一設備（31，61）處使用保密資料（K_{CRL}）計算與該 CRL 的項（37_1，…，37_p）相關聯的完整性欄位（MAC_i），其中，一個項係包括該 CRL 的至少一個廢止認證辨識元；

將該項以及所計算的其相關聯的完整性欄位傳輸到不同於該第一設備的第二設備（32，62）；及

將所傳輸的該項與該相關的完整性欄位儲存到該第二設備中。

2.如申請專利範圍第 1 項的方法，其中該項包含該 CRL 的一個子集。

3.如申請專利範圍第 1 項的方法，其中在該第一設備（31，61）中執行將該認證廢止列表（CRL）劃分到各項中。

4.如申請專利範圍第 1 項的方法，其中：該完整性欄位係訊息鑒別碼（MAC_i）；

該方法進一步包括：

將與所接收到的 CRL（33，67）相關聯的認證廢止列表（CRL）密鑰（K_{CRL}）選擇作爲該保密資料：

將所選擇的 CRL 密鑰（K_{CRL}）儲存在該第一設備（31，36）中。

5.如申請專利範圍第 4 項的方法，進一步包括：

對中間資料施加雜湊函數，以計算該訊息鑒別碼（MAC_i）；從包含至少一個廢止認證辨識元（SN_i）的項以及從該 CRL 密鑰（K_{CRL}）得到該中間資料。

6.如申請專利範圍第 1 至 5 項中任一項的方法，進一步包括：

在該第二設備（32，62）中儲存多個廢止認證辨識元（SN_i），將所儲存的廢止認證辨識元組織成爲至少一個安全項集（SES_i）的列表；每一安全項集包括至少一個廢止認證辨識元、至少一個相關聯的完整性欄位（MAC_i）以及該 CRL（33）的 CRL 辨識元（N_{CRL}）；

產生每一安全項集的列表順序欄位（63_i），該列表順序欄位具有能夠在儲存於該第二設備中的該安全項集的列表內確定安全項集的順序的內容（i）。

7.如申請專利範圍第 6 項的方法，進一步包括：

將該 CRL（33）的 CRL 辨識元（N_{CRL}）儲存到該第一設備（31）中。

8.如申請專利範圍第 1 或 5 項的方法，進一步包括：

在該第一設備（31）中，使用包含在該 CRL 內並使用發行該 CRL 的受託第三方所產生的認證廢止列表（CRL）簽字（S_{CRL}）檢查所接收到的 CRL（33，67）的完整性。

9.如申請專利範圍第 8 項的方法，其中所接收到的 CRL 的完整性檢查包括：

計算所接收到的 CRL（33，67）的雜湊值；

對所計算的雜湊值、受託第三方的公用密鑰和該簽字

（S_{CRL}）施加驗證函數，以評估該 CRL（33，67）的完整性。

10.如申請專利範圍第 1 至 5 項中任一項的方法，進一步包括：

在該第一設備（31，61）接收 CRL（33，67）的小資料塊，該 CRL 的小資料塊包括至少一個廢止認證辨識元（SN_i）；和

將包含至少一個廢止認證辨識元以及相關聯的完整性欄位的至少一個項傳輸給該第二設備（32，62）；

在任何接收 CRL 的其他小資料塊之前刪除所接收到的該 CRL 的小資料塊。

11.如申請專利範圍第 6 項的方法，其中：

該第一設備（31，61）係智慧卡；

該 CRL 辨識元（N_{CRL}）係 CRL（33，37）的 CRL 序列號；

該至少一個廢止認證辨識元（SN_i）係廢止認證的序列號。

12.如申請專利範圍第 1 至 5 項中任一項的方法，進一步包括：

檢查認證的有效性，其中檢查該認證的有效性包括：

將該認證的認證辨識元（SN0）從該第一設備（31，61）傳輸到第二設備（32，62）；

在該第二設備中，檢查儲存在該第二設備中的項的列表，從而估計該列表是否包括所具有的值對應於所傳輸的認證辨識元（SN0）的值的相關廢止認證辨識元；

根據所檢查的結果將至少一個廢止認證辨識元以及相關聯的完整性欄位傳輸到該第一設備；

在該第一設備中，藉由使用所傳輸的該相關聯的完整性欄位來驗證至少一個所傳輸的該廢止認證辨識元的完整性；以及

在該第一設備中，藉由使用至少一個所傳輸的該廢止認證辨識元來評估該認證的有效性。

13.如申請專利範圍第 4 項的方法，進一步包括：

檢查認證的有效性，其中檢查該認證的有效性包括：

將該認證的認證辨識元（SN0）從該第一設備（31，61）傳輸到第二設備（32，62）；

在該第二設備中，檢查儲存在該第二設備中的項的列表，從而估計該列表是否包括所具有的值對應於所傳輸的認證辨識元（SN0）的值的相關廢止認證辨識元；

根據所檢查的結果將至少一個廢止認證辨識元以及相關聯的完整性欄位傳輸到該第一設備；

在該第一設備中，藉由使用所傳輸的該相關聯的完整性欄位來驗證至少一個所傳輸的該廢止認證辨識元的完整性；

在該第一設備中，藉由使用至少一個所傳輸的該廢止認證辨識元來評估該認證的有效性；以及

使用（515,519）該 CRL 密鑰來驗證所傳輸的該廢止認證辨識元的完整性。

14.如申請專利範圍第 6 項的方法，進一步包括：

檢查認證的有效性，其中檢查該認證的有效性包括：

將該認證的認證辨識元（SN0）從該第一設備（31，61）傳輸到第二設備（32，62）；

在該第二設備中，檢查儲存在該第二設備中的項的列表，從而估計該列表是否包括所具有的值對應於所傳輸的認證辨識元（SN0）的值的相關廢止認證辨識元；

根據所檢查的結果將至少一個廢止認證辨識元以及相關聯的完整性欄位傳輸到該第一設備；

在該第一設備中，藉由使用所傳輸的該相關聯的完整性欄位來驗證至少一個所傳輸的該廢止認證辨識元的完整性；

在該第一設備中，藉由使用至少一個所傳輸的該廢止認證辨識元來評估該認證的有效性，其中：

儲存在第二設備中的列表的每一安全項集包括單個廢止認證辨識元；該方法進一步包括：

將相關的安全項集（SES_i）的至少一部分傳輸（58）到該第一設備，該相關的安全項集包含該相關的廢止認證辨識元。

15.如申請專利範圍第14項的方法，該方法還包括：

在該第一設備將包含在所傳輸的安全項集（SES_{i0}）中的所傳輸的認證廢止列表（CRL）辨識元（$N_{CRL}^{(i0)}$）與所確定的CRL的辨識元（N_{CRL}）進行比較（514），所傳輸的該CRL辨識元能夠確保儲存在第二設備中的列表對應於所確定的該CRL；

在該第一設備檢查（516）相關的該廢止認證辨識元實際上等於該認證辨識元。

16.如申請專利範圍第6項的方法，進一步包括：

檢查認證的有效性，其中檢查該認證的有效性包括：

將該認證的認證辨識元（SN0）從該第一設備（31，61）傳輸到第二設備（32，62）；

在該第二設備中，檢查儲存在該第二設備中的項的列表，從而估計該列表是否包括所具有的值對應於所傳輸的認證辨識元（SN0）的值的相關廢止認證辨識元；

根據所檢查的結果將至少一個廢止認證辨識元以及相關聯的完整性欄位傳輸到該第一設備；

在該第一設備中，藉由使用所傳輸的該相關聯的完整性欄位來驗證至少一個所傳輸的該廢止認證辨識元的完整性；

在該第一設備中，藉由使用至少一個所傳輸的該廢止認證辨識元來評估該認證的有效性，其中：

儲存在第二設備中的列表的每一安全項集包括單一廢止認證辨識元；

該方法進一步包括：

將第一安全項集（SES_{i-1}）的至少一部分以及第二安全項集（SES_i）的至少一部分傳輸（510）給該第一設備，該第一安全項集和該第二安全項集分別包含具有在所傳輸的認證辨識元（SN0）的期望順序之前和之後緊接的順序的廢止認證辨識元。

17.如申請專利範圍第 16 項的方法，該方法進一步包括在該第一設備執行下列步驟：

將包含在所傳輸的安全項集（SES_{j0}，SES_{k0}）中的所傳輸的認證廢止列表（CRL）辨識元（$N_{CRL}^{(k0)}$，$N_{CRL}^{(j0)}$）與所確定的 CRL 的辨識元（N_{CRL}）進行比較（518），所傳輸的該 CRL 辨識元能夠確保儲存在該第二設備中的列表對應於所確定的該 CRL；

檢查（520）該第一安全項集（SES_{k0}）和該第二安全項集（SES_{j0}）在儲存於該第二設備中的列表內是連續的；以及

檢查（521）該第一安全項集（SES_{k0}）和該第二安全項集（SES_{j0}）分別包含具有在所傳輸的認證辨識元（SN0）的期望順序之前和之後緊接的順序的廢止認證辨識元（SN_{j0}；SN_{k0}）。

18.如申請專利範圍第 6 項的方法，進一步包括：

檢查認證的有效性，其中檢查該認證的有效性包括：

將該認證的認證辨識元（SN0）從該第一設備（31，61）傳輸到第二設備（32，62）；

在該第二設備中，檢查儲存在該第二設備中的項的列表，從而估計該列表是否包括所具有的值對應於所傳輸的認證辨識元（SN0）的值的相關廢止認證辨識元；

根據所檢查的結果將至少一個廢止認證辨識元以及相關聯的完整性欄位傳輸到該第一設備；

在該第一設備中，藉由使用所傳輸的該相關聯的完整

性欄位來驗證至少一個所傳輸的該廢止認證辨識元的完整性；

在該第一設備中，藉由使用至少一個所傳輸的該廢止認證辨識元來評估該認證的有效性，其中：

該列表的每一安全項集（SES_i）包括多個廢止認證辨識元（SN_{fi}，…，SN_{li}），該多個廢止的認證辨識元在該安全項集內排序。

19.如申請專利範圍第 18 項的方法，進一步包括：

將相關的安全項集的至少一部分傳輸到該第一設備（61），該相關的安全項集包含該相關的廢止認證辨識元（SN0）。

20.如申請專利範圍第 18 項的方法，進一步包括：

在該第二設備（62）中查找包括第一廢止認證辨識元（SN_j）和第二廢止認證辨識元（SN_{j+1}）的替代安全項集（SES_{i0}），該第一廢止認證辨識元和該第二廢止認證辨識元分別具有在該相關的認證辨識元（SN0）的期望順序之前和之後緊接的順序；以及將該替代安全項集（SES_{i0}）傳輸到該第一設備（61）。

21.如申請專利範圍第 20 項的方法，進一步包括：

將第一替代安全項集（SES_{i0}）和第二替代安全項集（SES_{i0+1}）傳輸到該第一設備（61），該第一替代安全項集和該第二替代安全項集分別包含該第一廢止認證辨識元和該第二廢止認證辨識元。

22.如申請專利範圍第 19 項的方法，進一步包括：

在該第一設備（61）中，將包含在所傳輸的安全項集（SES_{i0}；SES_{i0+1}）中的所傳輸的認證廢止列表（CRL）辨識元與所確定的 CRL 的辨識元（N_{CRL}）進行比較，所傳輸的該 CRL 辨識元能夠確保儲存在該第二設備（62）中的列表對應於所確定的該 CRL。

23.如申請專利範圍第 6 項的方法，其中：

該列表順序欄位（63_i）的內容是索引，該索引對應於該列表內的安全項集（SES_i）的順序；

該第一設備儲存最大索引（i_{MAX}），該最大索引對應於該列表的最後一個安全項集的索引。

24.如申請專利範圍第 6 項的方法，其中：

該列表順序欄位的內容是關於該列表內的前一安全項集的資訊；

該第一設備儲存該列表的第一個安全項集和最後一個安全項集。

25.一種用於管理認證廢止列表（CRL）的設備，所述設備（31，61）包括：

用於接收 CRL（33，67）的裝置，該 CRL 包括至少一個廢止認證辨識元（SN_i）；

用於使用保密資料（K_{CRL}）計算與該 CRL 的項（37_1，…，37_p）相關聯的完整性欄位（MAC_i）的裝置（36，38，39），其中項包括該 CRL 的至少一個廢止認證辨識元；和

用於將該項以及所計算的其相關的完整性欄位傳輸到不同於所述設備的第二設備（32，62）的裝置。

26. 如申請專利範圍第 25 項的設備，其中該項包含該 CRL 的一個子集。

27.如申請專利範圍第 25 項的設備，進一步包括：

用於將所要檢查的認證的認證辨識元（SN0）傳輸到所述第二設備（32，62）的裝置；

用於從所述第二設備接收包含至少一個廢止認證辨識元和至少一個相關聯的完整性欄位的至少一個項的裝置；

用於經過使用所傳輸的該相關聯的完整性欄位來驗證該至少一個所傳輸的廢止認證辨識元的完整性的裝置（311）；和

用於使用至少一個所傳輸的廢止認證辨識元評估該認證的有效性的裝置（310）。

28.一種用於儲存來自認證廢止列表（CRL）之相關經劃分項的設備，所述設備（32，62）包括：

用於從第一設備（31，61）接收包含該 CRL 的至少一個廢止認證辨識元（SN_i）的至少一個項以及與該項相關聯的完整性欄位（MAC_i）的裝置；

記憶體(34，64)，用於儲存多個廢止認證辨識元(SN_i)，所儲存的廢止認證辨識元被組織成爲至少一個安全項集（SES_i）的列表，每一安全項集包括至少一個廢止認證辨識元、至少一個相關聯的完整性欄位(MAC_i)以及該 CRL(33)的 CRL 辨識元（N_{CRL}）；其中每一安全項集（SES_i）包括列表順序欄位（63_i），該列表順序欄位具有能夠在儲存於所述設備中的該安全項集的列表內確定安全項集的順序的

內容（i）。

29.如申請專利範圍第 28 項的設備，進一步包括：

用於從第一設備（31，61）接收認證辨識元（SN0）的裝置；

處理裝置（35，65），用於檢查儲存在該記憶體（34，64）中的項的列表，從而估計該列表是否包括所具有的值對應於所傳輸的認證辨識元（SN0）的值的相關廢止認證辨識元；和

用於根據所檢查的結果將至少一個廢止認證辨識元以及該相關聯的完整性欄位傳輸到該第一設備的裝置。

十一、圖式：

如次頁

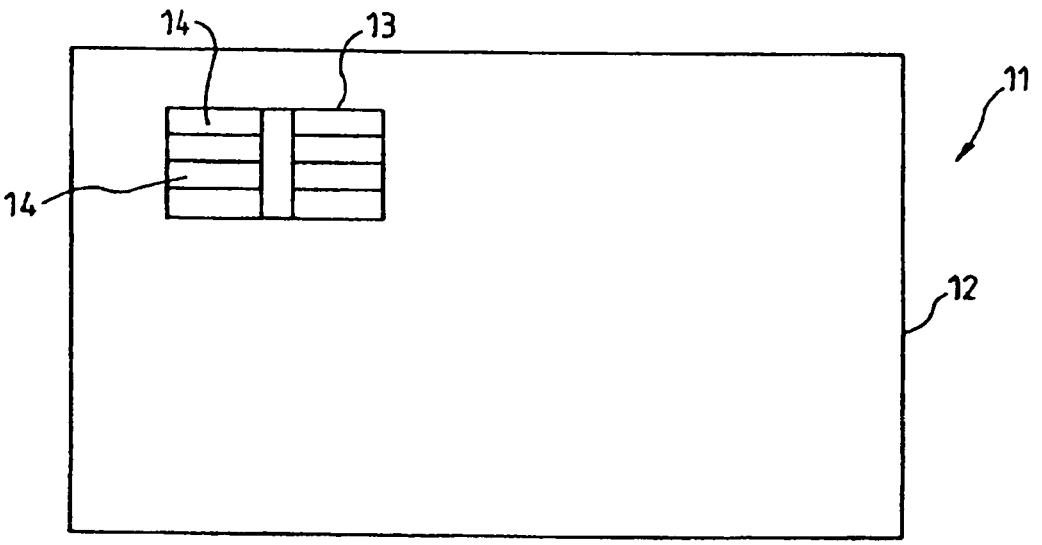


圖 1

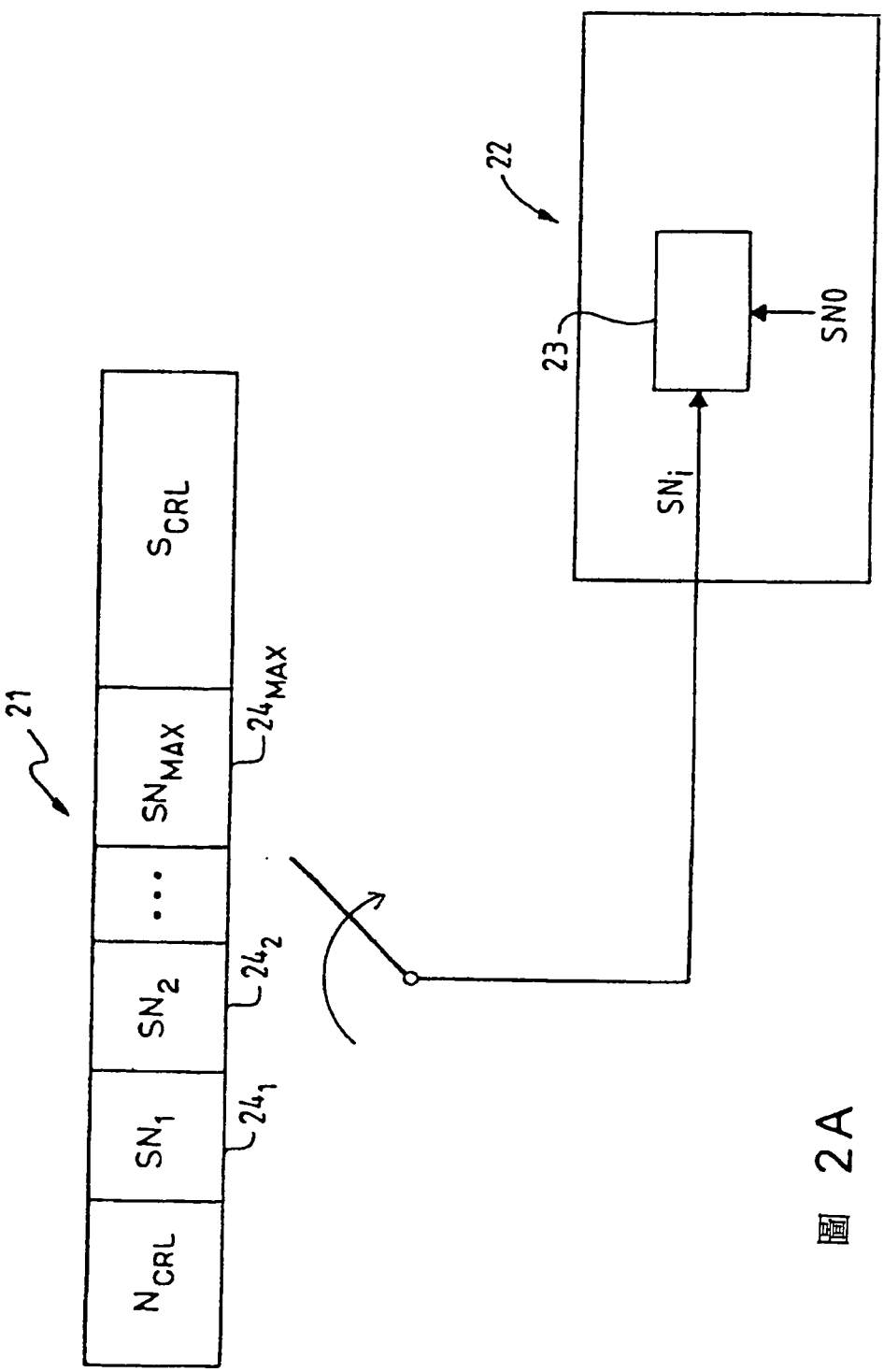


圖 2A

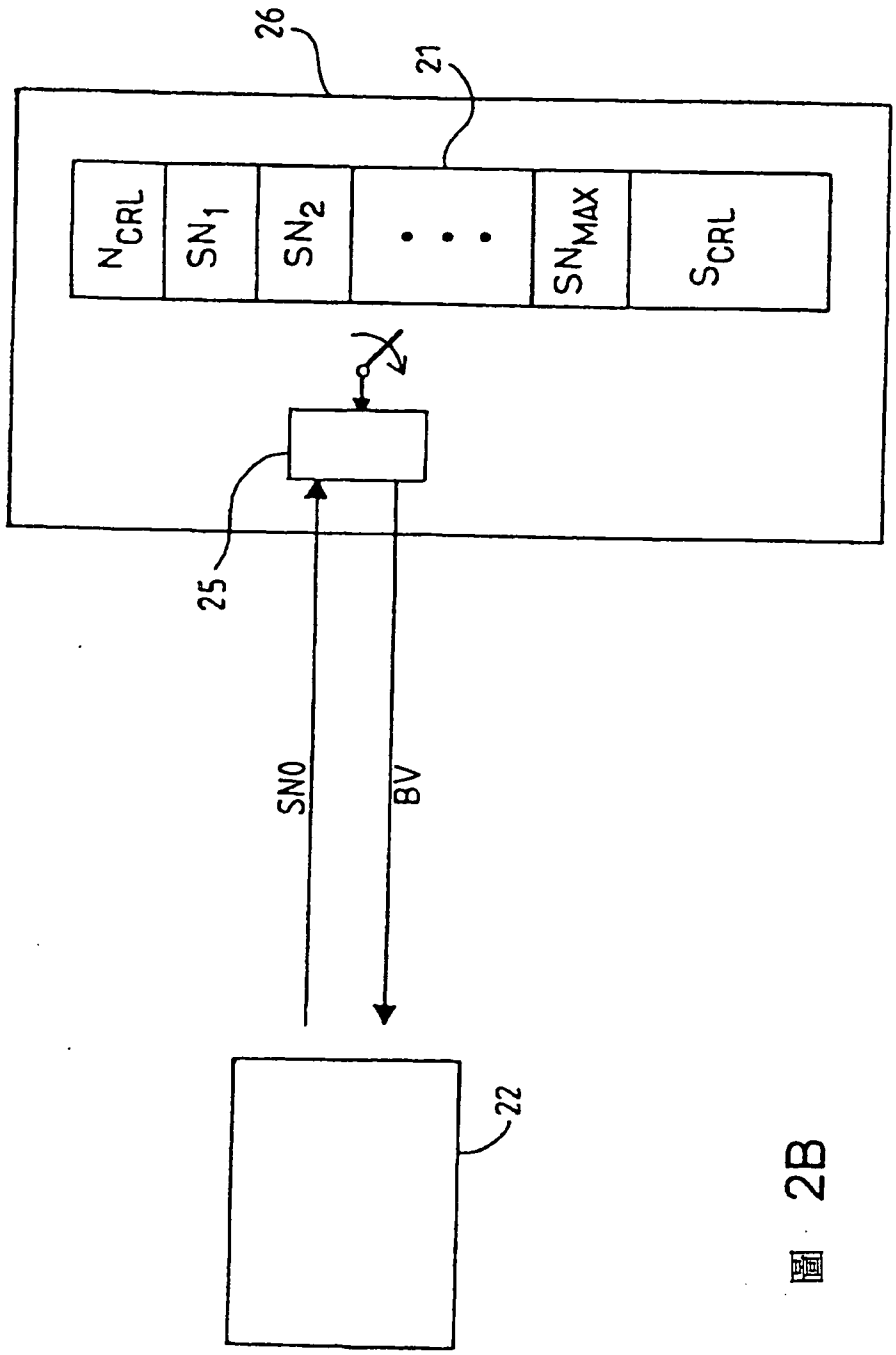
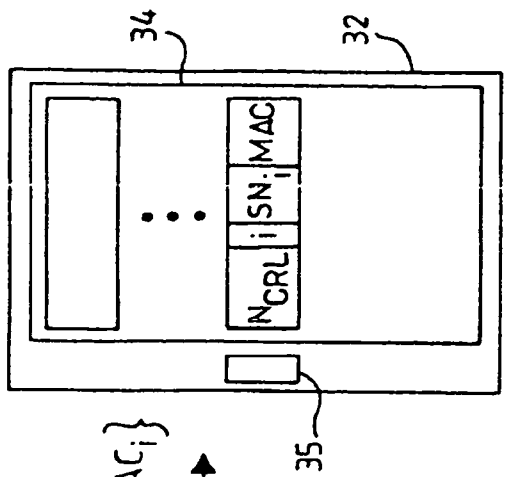


圖 2B



$SES_i = \{N_{CRL}, i, SN_i, MAC_i\}$

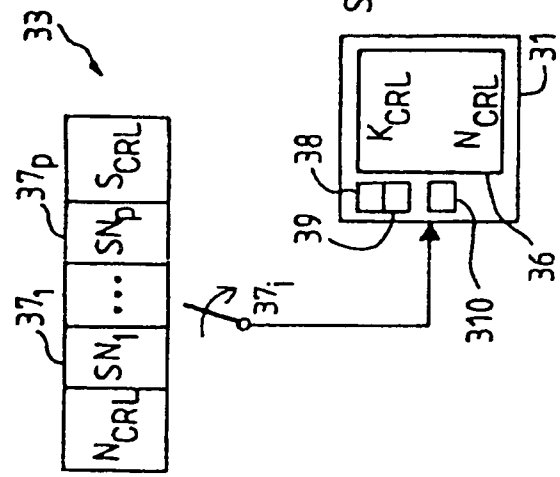


FIG.3A

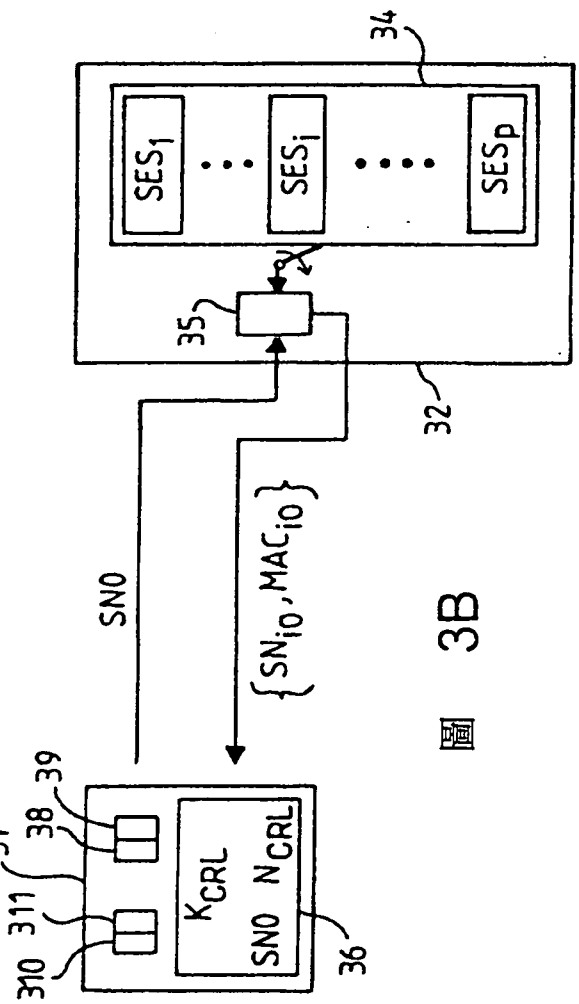


圖 3B

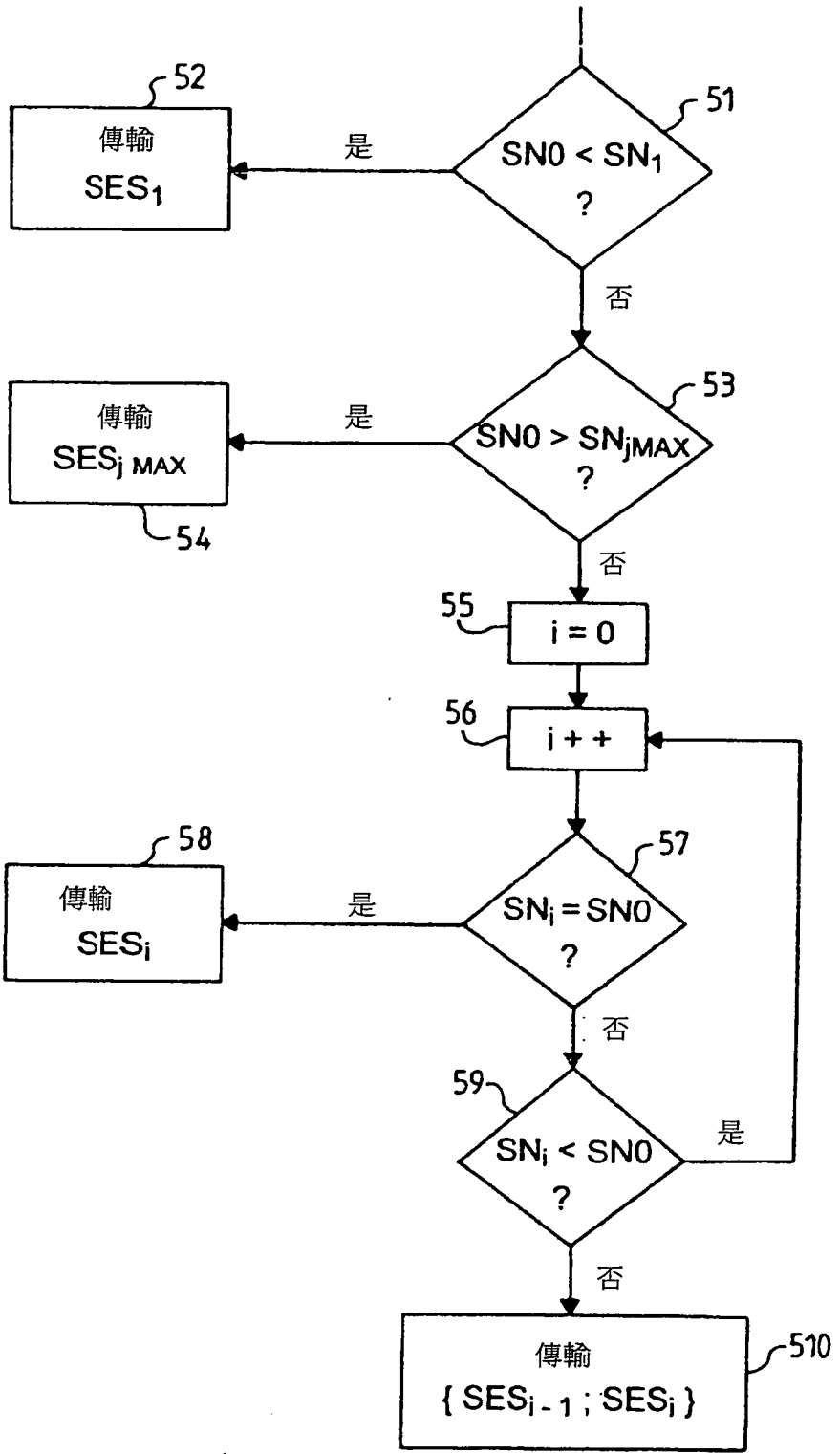
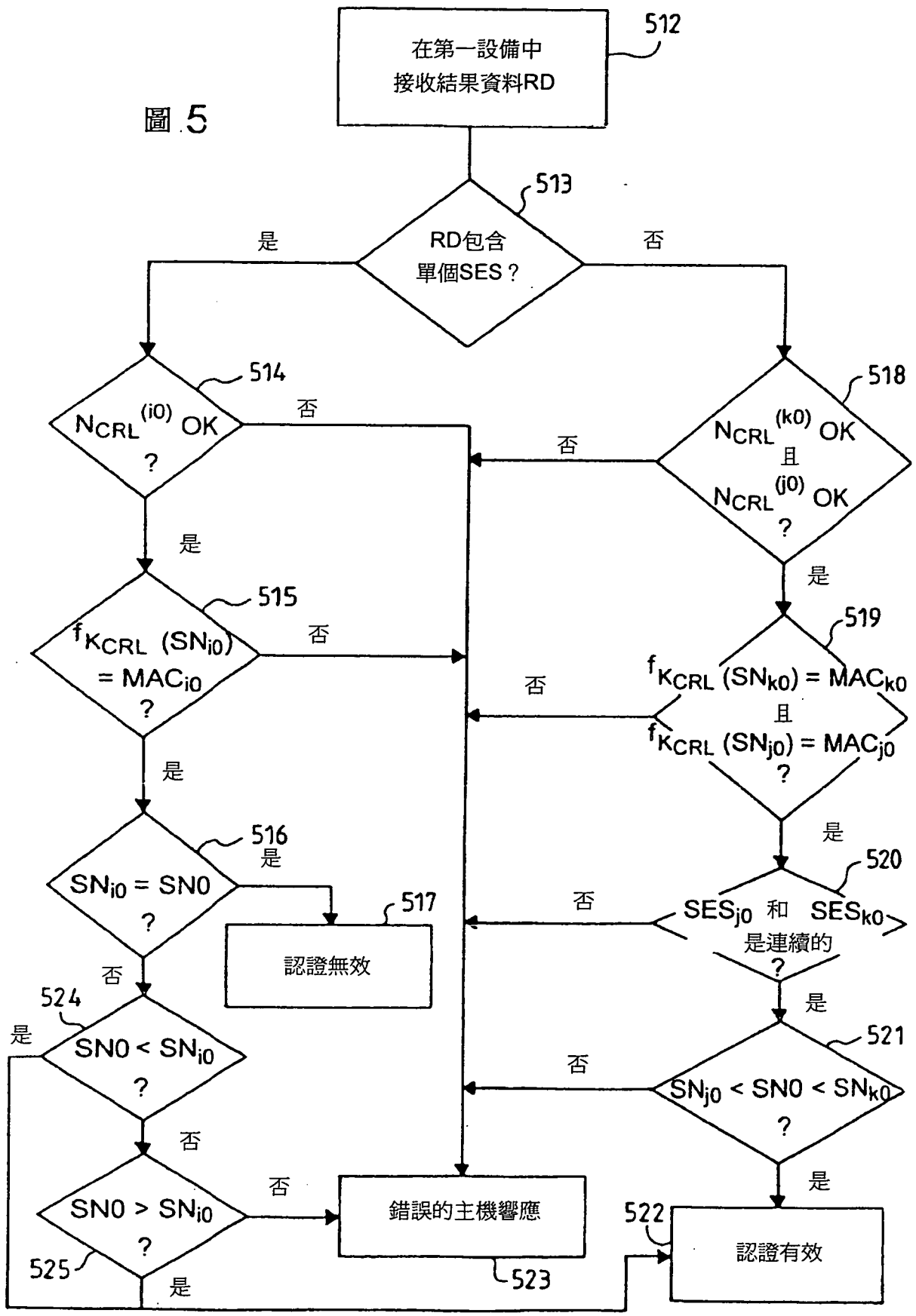

51
SN0 < SN1 ?
是
52
傳輸 SES1
否
53
SN0 > SNjMAX ?
是
傳輸 SESj MAX
54
否
55
i = 0
56
i + +
57
SNi = SN0 ?
是
58
傳輸 SESi
否
59
SNi < SN0 ?
是
否
傳輸 { SESi - 1 ; SESi }
510

圖 4

圖 5


512
在第一設備中
接收結果資料RD
513
RD包含
單個SES？
是
否
514
$N_{CRL}^{(i0)}$ OK
？
否
是
515
$f_{K_{CRL}}(SN_{i0}) = MAC_{i0}$
？
否
是
516
$SN_{i0} = SN0$
？
是
517
認證無效
否
524
$SN0 < SN_{i0}$
？
是
否
525
$SN0 > SN_{i0}$
？
否
是
518
$N_{CRL}^{(k0)}$ OK
且
$N_{CRL}^{(j0)}$ OK
？
否
是
519
$f_{K_{CRL}}(SN_{k0}) = MAC_{k0}$
且
$f_{K_{CRL}}(SN_{j0}) = MAC_{j0}$
？
否
是
520
SES_{j0} 和 SES_{k0}
是連續的
？
否
是
521
$SN_{j0} < SN0 < SN_{k0}$
？
否
是
522
認證有效
523
錯誤的主機響應

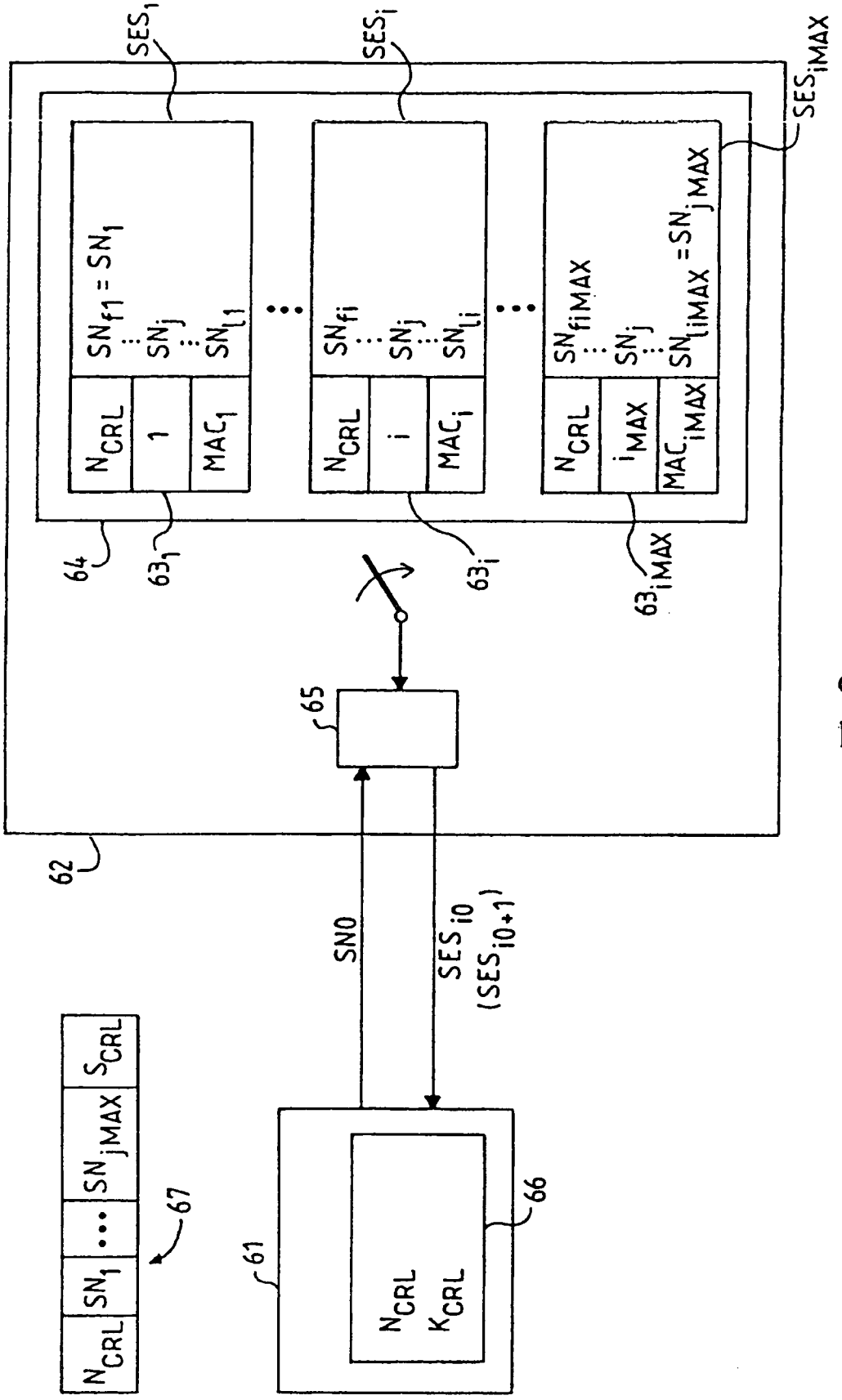

SES1
SESi
SESiMAX
NCRL
1
MAC1
SNf1 = SN1
SNj
SNl1
NCRL
i
MACi
SNfi
SNj
SNli
NCRL
iMAX
MACiMAX
SNfiMAX
SNj
SNliMAX =SNjMAX
64
631
63i
63iMAX
65
62
SN0
SESi0
(SESi0+1)
61
NCRL
KCRL
66
NCRL
SN1
SNjMAX
SCRL
67

圖 6