I442772

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：96140354

※ 申請日期：96.10.26　※IPC 分類：H04N 7/16 (2011.01)

一、發明名稱：（中文/英文）

檢測安全處理器異常使用狀況的方法

METHOD OF DETECTING AN ABNORMAL USE OF A SECURITY PROCESSOR

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

薇瑟斯公司 / VIACCESS

代表人：（中文/英文）

克里斯汀　毛瑞-派寧斯 / CHRISTINE, MAURY-PANIS

住居所或營業所地址：（中文/英文）

法國巴黎德芬斯希德克斯・杜爾歐普拉 C・柯林斯亞契

Les Collines de l'Arche, Tour Opera C, 92057 PARIS LA DEFENSE CEDEX, FRANCE

國　籍：（中文/英文）

法國 / FRANCE

三、發明人：（共 7 人）

姓　名：（中文/英文）

1. 曲易茲　昆騰 / CHIEZE, QUENTIN
2. 庫伯茲　阿拉恩 / CUABOZ, ALAIN
3. 吉拉得　亞歷山卓 / GIARD, ALEXANDRE
4. 格那特　奧利佛 / GRANET, OLIVIER
5. 那爾　路易斯 / NEAU, LOUIS
6. 羅傑　馬修 / ROGER, MATTHIEU
7. 托那爾　布朗諾 / TRONEL, BRUNO

國　籍：(中文/英文)

1.-7. 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：。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 法國、　2006/10/27、　06 54599

☐ 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：

本發明係有關於檢測被至少一接收終端機激發之安全處理器的異常使用之方法，以控制對被至少一操作員供應至該接收終端機的被打散之數位內容的存取。

此方法包含下列之步驟：

分析在一預置觀察期間T_{Obs}之際的安全處理器使用，

以該分析為基準來決定在該觀察期間T_{Obs}之際之該安全處理器每單位時間的激發數的平均值M_{ECM}，

比較該平均值M_{ECM}與一預置臨界值S_{max}，以及

若平均值M_{ECM}大臨界值S_{max}，對該終端機施用一制裁，此處其嚴重程度漸進地提高。

六、英文發明摘要：

The invention relates to a method of detecting an abnormal use of a security processor invoked by at least one receiving terminal in order to control access to a scrambled digital content supplied by at least one operator to said receiving terminal.

This method comprises the following steps:

- analysing security processor use during a preset observation period T_{obs},

- determining on the basis of said analysis the mean value M_{ECM} of the number of invocations per time unit of said security processor during said observation period T_{obs},

- comparing said mean value M_{ECM} with a preset threshold S_{max}, and

- if the value M_{ECM} is greater than the threshold S_{max}, applying to said terminal a sanction whereof the level of severity increases progressively.

七、指定代表圖：

(一)本案指定代表圖為：第（ 2 ）圖。

(二)本代表圖之元件符號簡單說明：

30-40...步驟
50...步驟
52...步驟
53...步驟
54...步驟

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】

發明領域

本發明係位於多媒體服務存取控制之領域中，且更明確地關於檢測被至少一接收終端機激發之安全處理器的異常使用之方法，以控制對被至少一操作員供應至該接收終端機的被打散之數位內容的存取。

本發明亦有關於一安全處理器，其欲控制對被至少一操作員供應至該接收終端機的被打散之數位內容的存取。

本發明係不管支援網路種類或內容型式(現場電視、隨選視訊VOD、個人視訊紀錄器(PVR))地應用。

【先前技術】

發明背景

運用存取控制之接收系統的非法使用為習知的。存取控制之第一個目的為要藉由以語法上不正確的訊息(其例如具有假簽署或為不完整的，或包含非法之命令字串) 欺詐地提給接收器來分析接收器中所運用的存取控制處理器、第二個目標為要針對正常被授權之使用開拓接收系統的條件存取資源。該第二種使用可藉由在考慮特別是其安全處理器之共用該接收系統(典型上為卡片共享)或藉由共用或重新分配控制句組(CW共享)而被施作。

更特別的是，在接收系統資源之共享使用的事件中，數個終端機藉由以語法上正確但過於多樣之訊息經由雙向通訊網路提給終端機而激發其安全處理器。

本發明之目的係要阻礙上述之欺詐的形式。

當安全處理器與終端機間之介面未被保護時本發明具有特別但非排它的應用。

EP 1 447 976 A1文件描述用於防止安全處理器倍數個終端機共用之方法。

此方法係由測量二個連續之給予權利控制訊息(ECM)的呈現之時間隔離及驗證如此被觀察的訊息處理時序符合預置率型態所組成。

由於實際上ECM訊息對不適當的使用之呈現特別是依下列而定的，此方法不允許對ECM訊息串之任何擾亂：

- 這些ECM訊息附掛至節目係如何被組織，視對存取節目係一整體存取狀況、或針對視訊、音頻或其他元件為數個存取狀況而定，
- 如在允許一節目被錄製而另一個正在被觀賞之多調諧器接收器的情形中用於同時處理單一或數個節目被解碼器提供之能力，
- 使用者重複「刪除」之習慣造成穩定的ECM訊息處理串流之中斷。

本發明之另外的目的為要上述習知技藝之缺點。

【發明內容】

發明概要

本發明推薦一種欲允許安全處理器檢測其中該安全處理器針對正常被授權使用非法地被使用之情況的方法。

此方法包含下列之步驟：

分析在一預置觀察期間T_{Obs}之際的安全處理器使用，

以該分析為基準來決定在該觀察期間T_{Obs}之際之該安全處理器每單位時間的激發數的平均值M_{ECM}，

比較該平均值M_{ECM}與一預置臨界值S_{max}，以及

若平均值M_{ECM}大於臨界值S_{max}，對該終端機施用一制裁，此處其嚴重程度漸進地提高。

假設該比較係使用每單位時間之激發數的平均值M_{ECM}，本發明之方法為屬於統計性質，且不能被所處理之節目的時間結構之局部干擾與被使用者行為之變異欺騙。

依據本發明之一特徵，在觀察期間T_{Obs}之際的平均值M_{ECM}係針對藉由累計多個被該安全處理器的不活動之最小期間T_{InaMin}分隔的連續活動期間所構成之該安全處理器的活動期間T_{Act}被決定。

一活動期間代表一累計時間槽，此際一安全處理器在連續之時間跨幅中被激發。其必須有一最小長度T_{ActMin}以保證分析的重大特點。針對此最小長度T_{ActMin}，其意為當檢測安全處理器就算是正常且合法下偶而之重大的不當使用時風險被降低。

在本發明之方法的特別實施例中，安全處理器之激發係由以被打亂的內容相關聯之存取控制提給安全處理器及承載一控制句組CW與至少一存取狀況的描述組成。

在此情形中之安全處理器使用的分析包含下列之步驟：

- 決定在該活動期間T_{Act}之際被該安全處理器處理之

ECM訊息的次數，

- 計算$M_{ECM}=N_{ECM}/T_{Act}$之關係式，
- 比較M_{ECM}關係與臨界值S_{max}，
- 若平均值M_{ECM}大於臨界值S_{max}則施用制裁。

在此實施例中，安全處理器使用的分析包含下列之運算：

於目前的日期t_c，

- 一方面決定具有與該目前的日期t_c同時之分配日期的ECM訊息，且其以觀看內容之一第一次使用被提給該安全處理器，及另一方面具有在該目前的日期t_c之前的分配日期之ECM訊息以觀看內容之再次使用被提給該安全處理器，
- 測量該安全處理器之活動期間T_{Act}，此際其處理連續的當時之ECM訊息，
- 在至少如小於預置最小長度T_{ActMin}之活動期間T_{Act}的長度計算當時之ECM訊息的次數N_{ECM}。

依據本發明，於目前的日期t_c，一舊的ECM訊息藉由比較此ECM訊息被處理之日期t與日期(t_c-t_{Diff})而被決定，此處t_{Diff}代表分隔日期t與日期t_c之先前被定出的最小延遲。

在一實施例變形中，計算成功地被處理之當時的ECM訊息之次數N_{ECM}包含下列之運算：

- 比較日期t與日期(t_c-t_{Diff})，
- 若日期(t_c-t_{Diff})小於或等於日期t，以$(t-t_c)$值增加次數N_{ECM}，否則將次數N_{ECM}維持於目前值，

- 若日期t為介於日期t_c與日期t_c+t_{InaMin}間，提高活動期間T_{Act}，否則將活動期間T_{Act}維持於目前值。

依據本發明之另一個有利的特徵，該制裁係依下列的步驟被施用：

- 首先該制裁以嚴重程度n_i被施用一預置次數R_i，
- 然後該制裁以下一個嚴重程度n_{i+1}被施用一預置次數R_{i+1}，
- 最後當最終嚴重程度n_{imax}被到達時，該最大制裁被施用。

在一實施例變形中，該制裁包含由暫時封鎖內容接收所組成之一第一嚴重程度、由具有需要與供應該內容之操作員連絡的封鎖內容接收所組成之一第二嚴重程度、及由永久封鎖內容接收所組成之一第三嚴重程度。

較佳的是，嚴重性處理器使用內建於該不適當的使用內之軟體被分析。

就此點而言，該軟體包含：

- 一第一模組用於分析在一預置觀察期間T_{Obs}之際的安全處理器使用，
- 一第二模組用於以該分析為基準來決定在該觀察期間T_{Obs}之際之該安全處理器每單位時間的激發數的平均值M_{ECM}，及用於比較該平均值M_{ECM}與一預置臨界值S_{max}，以及
- 一第三模組用於在若平均值M_{ECM}大於臨界值S_{max}，對該終端機施用一制裁，此處其嚴重程度漸進地提高。

圖式簡單說明

本發明之其他特徵與優點將由下列描述被採用為非限制性例並參照附圖而浮現，其中：

第1圖示意地顯示一流程圖，其顯示在觀察期間T_{Obs}之際該安全處理器之每單位時間的激發次數之平均值的計算。

第2圖示意地顯示依據本發明之分析與制裁的步驟。

【實施方式】

較佳實施例之詳細說明

本發明將以被條件存取系統(CAS)保護之視聽節目的操作員的分配為背景被描述。這些節目係為用於被配備典型上為一晶片卡之一安全處理器的數個訂戶終端機。

在此文意中，對被打散之節目的存取係被操作員藉由對存有一控制句組CW之終端機及對可得可用之商業廣告授權做出內容存取條件而被控制。就此點而言，該操作員對該內容附加一存取條件，訂戶要能存取該內容則必須符合於此。該控制句組CW與該存取條件描述經由特定之給予權立控制訊息(ECM)以讓其安全性被檢查。當這些訊息之有效性已被安全處理器檢查，其所戴有之存取條件與被保存在安全處理器之非依電性記憶中的存取權狀被比較。在本質上已習知的一方法中，這些存取權狀在先前已經由給予權利管理訊息(EMM)被終端機接收。若該存取條件被這些存取權狀之一所符合，該安全處理器用解密擷取控制句組CW並將之供應至終端機而允許該內容不被打散。在本質

上已習知的一方法中，ECM與EMM訊息不被加密方法保護、運用運算法則與金鑰已保證該等訊息之整合性、其認證與其可能承載的敏感資料之保密性、及該等金鑰特別被安全特定EMM管理訊息更新。

按照依據本內文被選擇之可變的策略或多或少地修改控制句組之隨機值為慣常的。例如，一控制句組在廣播電視中以慣常方式每10秒或在極端情形於只具有被訂戶之各別客製化的影片之每一個隨選視訊被修改。

於此背景中施用本方法之目的為允許安全處理器檢測對之已被施加且對此反應的任何不適當之使用。於針對受考慮的使用在於控制內容存取(因安全處理器所處理之ECM訊息而被呈現者)。

為了檢測不適當之使用，一參數乃統計式地被測量，其呈現安全處理器之使用，且此參數與代表安全處理器的正常使用之預置臨界值S_{max}被比較。

測量安全處理器包含在一預置觀察期間T_{Obs}之激發、然後根據該分析來決定在預置觀察期間T_{Obs}之際之每時間單位的激發數之平均值M_{ECM}。

比較平均值M_{ECM}與一預置臨界值S_{max}允許安全處理器之不適當的使用在被考慮下之觀察期間T_{Obs}上被檢測。

臨界值S_{max}藉由在一重大之觀察期間T_{Obs}上檢查使用者的平均行為被建立。

為了涵蓋末端使用者之接收終端機的至少一特徵使用週期特徵，安全處理器之一活動期間在預置觀察期間T_{Obs}

之際被定出，代表其間後者在連續時間槽中不論合法或非法地被激發的時間槽。一最小活動期間T_{ActMin}亦被定出，代表為了保證在活動期間之際的安全處理器使用之分析的重大特徵被活動期間所達成之期間。針對此最小期間意為檢測卡片之就算是整體上正常之偶而重大的不適當使用之風險可被最小化。實際上，正常使用典型上可代表在繁重刪除的事件中之類似於在不適當使用中的卡片激發之暫時的激發尖峰。

最小活動期間T_{InaMin}亦被定出而代表由最後成功被處理之ECM訊息起已經歷的時間，且超過此其被視為前一個活動期間已結束。

進而言之，一方面為了在對應於ECM訊息的最後一個成功之處理的目前的日期t_c決定與被提給安全處理器之對內容的第一次使用之目前的日期t_c同時的ECM訊息及另一方面之相對於對內容的再次使用之日期t_c的舊ECM訊息，隔離舊ECM訊息與目前日期之最小期間用參數T_{Diff}被表示，且此ECM訊息的日期以大於或等於T_{Diff}之期間比t_c提早，其被視為一ECM訊息被提給安全處理器之對內容的再次使用。

其應被注意到ECM訊息之分配日期可用本質上已習知的不同技術解法被決定。例如，其以該存取條件與該控制句組被ECM訊息產生器ECM-G鍵入，且在此ECM訊息被處理時被安全處理器抽取。

該發明性之過程的步驟將在此後參照第1與2圖被描

述。

第1圖顯示在計算於活動期間T_{Act}之際被安全處理器處理之ECM訊息次數N_{ECM}與該活動期間T_{Act}之準同步測量的步驟。

參照第1圖，在瞬間t_0開始的觀察期間T_{Obs}之際之目前的日期t_c，安全處理器具有一分配日期t之一訊息ECM_t(步驟10)。

在步驟12，安全處理器分析訊息ECM_t之語法、認證與整合性，然後決定其日期t與存取準則。

在步驟14，安全處理器驗證存取準則之有效性，與訊息的認證及整合性。

若後者不被滿足或該訊息不為確實或整合的，安全處理器分析下一個ECM訊息(箭頭16)。

若後者被滿足(箭頭18)安全處理器在步驟20處理訊息ECM_t並比較訊息ECM_t之日期t與日期t_c-T_{Diff}以決定訊ECM_t是針對內容的第一次使用或針對在其已被錄製後之再次使用被提出。

若t_c-T_{Diff}小於t，換言之若訊息ECM_t係有關於被打散的節目之第一次使用，安全處理器在步驟22以一單位增加被處理的ECM訊息之次數。

若訊息ECM_t之日期t為介於日期t_c與t_c+T_{InaMin}間(步驟24)，安全處理器得到的結論為前一個活動期間尚未結束，且在步驟26，目前活動期間T_{Act}之長度以長度t-t_c被增加。

因而，活動期間T_{Act}被決定且被安全處理器處理之ECM

訊息次數N_{ECM}因而被計算至觀察期間T_{Obs}結束為止。

第2圖示意地顯示依據本發明之安全處理器使用的分析與制裁中的步驟。

在步驟30，安全處理器計算關係式$M_{ECM}=N_{ECM}/T_{Act}$，其中N_{Ecm}代表被計算之ECM訊息的次數及T_{Act}代表在觀察期間T_{Obs}之計的活動期間之總長度。

在步驟32，安全處理器檢查T_{Act}是否大於或等於預置長度T_{ActMin}。此步驟之目的是要檢查活動期間T_{Act}足以保證分析的重大特徵。

在肯定之答覆的事件中，安全處理器將N_{ECM}， T_{Act}與t_0值重新預置(步驟36)。

在否定之答覆的事件中，該值不被重新預置。

在此二種情形中，該處理在步驟38被繼續，其包含檢查訊息ECM_t之日期t是否隨後於目前的日期t_c。

若為是，日期t被指定為目前的日期t_c。

此過程係由計算(第1圖)之步驟10被繼續。

若T_{Act}大於或等於T_{ActMin}，安全處理器檢查(步驟50)被計算之平均值M_{ECM}是否大於臨界值S_{max}。

若為是，一制裁被施用且制裁次數及/或被施用之制裁的嚴重程度被提高(步驟52)，且N_{ECM}， T_{Act}與t_0將被重新預置。

否則，控制句組CW被解密且被發射至終端機以允許內容不被打散。

然後該處理在步驟34被繼續，其包含檢查長度$(t-t_0)$是

否大於觀察期間T_{Obs}之長度。在肯定之答覆的事件中，安全處理器將N_{ECM}，T_{Act}與t_0值重新預置(步驟36)。

在否定之答覆的事件中，該值不被重新預置。

在此二種情形中，該處理在步驟38被繼續，其包含檢查訊息ECM_t之日期t是否隨後於目前的日期t_c。

若為訊息ECM_t之日期t是隨後於目前的日期t_c，日期t在步驟40，被指定為目前的日期t_c，且此過程係由計算(第1圖)之步驟10被繼續。

在步驟52之制裁管理包括增加制裁次數及/或制裁嚴重程度。此制裁管理為本發明的特徵。假設本方法為如將在下面被描述之根據習知的模型化的安全處理器之激發的統計分析，定出單一制裁及在不適當之使用被檢測立刻施用之為超額的且最終會使本方法為無效的。為了由統計分析對不適當之使用的檢測所帶來之漸進性獲益，最適當的制裁及因而為在本方法中為固有的者為漸進之管理。該管理定義提高嚴重性及在階段上漸進被制裁之制裁的嚴重程度。

舉例而言，安全處理器之不適當的使用之初始的檢測藉由防止內容之不打散造成對內容存取的岔斷。當此低嚴重性制裁因不適當的使用已被確認而已被重複某些次數，另一個具有平均嚴重性之制裁被施用，其包含以要求使用者聯絡他的操作員不要封鎖終端機而暫時地封鎖終端機。當此第二個制裁已根據不適當的使用正在持續被施用某些次數，高嚴重性之一最終制裁被施用，其包含永久地使安

全處理器失能。

上述之處理運用在EEPROM式(電氣式可擦拭可程式唯讀記憶體)的安全處理器記憶體中經常被更新之參數以在對安全處理器供電岔斷的事件中確保分析之連續性。

事實上，此型式之記憶體支援有限次數的寫入。所以為補償此技術性的限制，最常被計算激發之參數N_{ECM}，t_c與T_{Act}被儲存於非永久性記憶體(RAM)中並規律地被儲存至EEPROM記憶體內。

就此點而言，下列新的參數被定出：

- 由參數N_{ECM}，t_C與T_{Act}最後一次傳送至EEPROM記憶體內起成功地被處理之ECM訊息的次數N_{Buf}。
- 代表參數N_{ECM}，t_C與T_{Act}之EEPROM記憶體內觸發更新的次數N_{Buf}的最大臨界值之次數N_{max}。

然後參數N_{ECM}，t_C與T_{Act}以下列方法被管理：

當安全處理器被供電或安全處理器使用被啟動，參數N_{ECM}，t_C與T_{Act}在其於先前若未曾被鍵入以其預置值被鍵入以其預置值被創立即被鍵入EEPROM記憶體內。

在安全處理器已被供電後或在啟動安全處理器使用之分析時：

- 參數N_{ECM}，t_C與T_{Act}被載入RAM記憶體內
- 這些參數之任何施作在RAM記憶體內被做成
- 若$N_{Buf} > N_{max}$，其值在EEPROM記憶體內額外地被更新。

在此方式下，於每次ECM訊息在期間T_{Obs}之際成功地

被處理之次數被預置臨界值S_{max}提供時，參數N_{ECM}，t_C與T_{Act}被傳送至EEPROM記憶體內。

其應被注意到，若參數N_{ECM}，t_C與T_{Act}值為已知的，一惡意操作員會藉由將安全處理器規律地斷電而使該方法失效。然後該等被儲存之值被漏失而妨礙安全處理器被分析及讓一詐騙者以完全無事地共用之。

為防止該方法以此方式非法地陷害，一解決之道為在安全處理器內載入新的較低值之臨界值N_{max}。另一解決之道包含在每次供電後分別提高T_{Act}，N_{ECM}與$T_{Act,ini}$(活動時間之校正)及$N_{ECM,ini}$(成功地被處理之ECM訊息的校正次數)之值。

此相當於降低臨界值N_{max}之值。

在一較佳實施例中，分析參數化與啟動可被操作員藉由發送一ECM訊息而以程式被規劃。

此參數化亦可在卡片客製化階段中被施作。

此包含：

- 由被給予之一清單中選擇平均與高嚴重程度的每一個之制裁；
- 設定低與平均嚴重程度之制裁的重複次數。

此外，該ECM訊息承載至少一個下列之參數：

- 觀察期間之長度T_{Obs}，
- 最小活動期間T_{ActMin}，
- 延遲T_{Diff}，
- 最小不活動期間T_{InaMin}，

- 臨界值S_{max}之值，
- 臨界值N_{Buf}之值。

這些參數用下列關於本發明之施作的參數被企劃：

N_{max}：被表達為數個ECM訊息之儲存臨界值，

$T_{Act,ini}$：以秒被表達之活動時間的校正，

$N_{ECM,ini}$：成功地被處理之ECM訊息的校正次數，

T_{SFA}：以秒被表達之在低嚴重程度制裁下的ECM之非處理期間，

R_{SFA}：低嚴重程度制裁之重複次數，

R_{SMO}：平均嚴重程度制裁之重複次數。

吾人在下面描述由安全處理器之正常使用的模型化之此種參數化結果的例子。

其被考慮到使用者之行為係依週的日期而定的，但由一週至下一週被重複。

該分析係進一步根據下面之假設：

- 刪除之假設：在每一刪除有一額外之ECM訊息，
- 低嚴重程度刪除：每小時有20個額外之ECM訊息，即每3分鐘1個，
- 中嚴重程度刪除：每小時有60個額外之ECM訊息，即每1分鐘1個，
- 正常刪除：每小時有120個額外之ECM訊息，即每30秒1個，
- 超額刪除：每小時有1000個額外之ECM訊息，即每3秒1個。

在將被描述之實施例中，分析係在7天的觀察期間上被檢測，然後在15天的觀察期間上被檢測。在包含數個被打散之成份的節目之情形中，例如只有關於視訊的主要ECM路徑被計算。

然後下列之值被設定：

- 最小不活動時間：15秒，
- 延期遲緩：5分鐘，
- 加密期間：10秒，
- 在接收終端機中之調諧器個數被限制為2，允許對二個內容的同步存取，一個在直接顯示器中、另一個在終端機之大量儲存器被錄製。
- 觀察期間：7至14天。

根據上面之假設與習知的使用，接收終端機之合法與非法使用的數個剖面已被製作。為了能辨別此二分類之使用剖面，模型化導致下列的參數值T_{Obs}，T_{ActMin}與S_{max}被決定：

- 觀察期間T_{Obs}為14天，即1209600秒。
- 每秒0.22 ECM之一激發允許為具有一個或多個調諧器的合法使用者提供行為之廣大寬容度的安全餘裕被要求知該辨別。該最大合法制裁S_{max}在此值被設定。
- 最小活動期間T_{ActMin}被設定為30小時，即108000秒。

本發明之方法被一安全處理器施作，包含：

- 一第一模組用於分析在一預置觀察期間T_{Obs}之際的

安全處理器使用，

- 一第二模組用於以該分析為基準來決定在該觀察期間T_{Obs}之際之每單位時間的激發數的平均值M_{ECM}，及用於比較該平均值M_{ECM}與一預置臨界值S_{max}，以及
- 一第三模組用於在若平均值M_{ECM}大臨界值S_{max}，對該終端機施用一制裁，此處其嚴重程度漸進地提高。

此安全處理器運用之軟體包含：

- 指令用於分析在一預置觀察期間T_{Obs}上被該終端機對該晶片卡之使用，
- 指令用於由該分析來決定在該觀察期間T_{Obs}之際被該終端機對該晶片卡之每單位時間的激發次數之平均值M_{ECM}，及用於比較該平均值M_{ECM}與一預置臨界值S_{max}，以及
- 指令用於對該終端機施用一制裁，其嚴重程度在該平均值M_{ECM}若大於該臨界值S_{max}時漸進地提高。

本發明已在計算與分析中被考慮之ECM為成功地被處理的ECM之情形中被描述，即其被認知為語法上正確的、確認的、整合的、且被相關之給予權利滿足以允許對內容的存取。作為一替選方式，本方法亦可藉由考量ECM被安全處理器特別是在關於語法、認證及/或整合性被認知為錯誤的時被施作。此意為被故意地不正確之ECM的重複進行之呈現的暴力攻擊可重要地被整合至不適當的使用之分析內。在此事件中，圖中之步驟不被執行且在第1圖中之方法

於步驟20被繼續。

【圖式簡單說明】

第1圖示意地顯示一流程圖，其顯示在觀察期間T_{Obs}之際該安全處理器之每單位時間的激發次數之平均值的計算。

第2圖示意地顯示依據本發明之分析與制裁的步驟。

【主要元件符號說明】

10-26...步驟

30-40...步驟

50...步驟

52...步驟

53...步驟

54...步驟

102年10月28日修正本

P22～28

十、申請專利範圍：

1. 一種為了控制由至少一操作員所供應至接收終端機的被打散之數位內容之第一次使用而控制該接收終端機之一安全處理器的操作之方法，該方法包含下列之步驟：

分析在一預置觀察期間T_{Obs}之際的該安全處理器之使用，

以該分析為基準來決定在該觀察期間T_{Obs}之際之該安全處理器每單位時間的激發數的平均值M_{ECM}，

比較該平均值M_{ECM}與一預置臨界值S_{max}，

若該平均值M_{ECM}大於該臨界值S_{max}，對該終端機施用一制裁，此處其嚴重程度漸進地提高，及

其中進行該安全處理器之該第一次使用的分析係於目前的日期t_c，基於下列之其他步驟來實施：

• 針對一內容之一第一次使用，決定具有與該目前的日期t_c同時之一分配日期的ECM訊息而提給該安全處理器，及針對一內容之再次使用，決定具有在該目前的日期t_c之前的分配日期之ECM訊息而提給該安全處理器，

• 測量該安全處理器之活動期間T_{Act}，其中處理連續的當時之ECM訊息，

• 在至少如小於預置最小長度T_{ActMin}之活動期間T_{Act}的長度計算經處理之當時之ECM訊息的次數N_{ECM}。

2. 如申請專利範圍第1項之方法，其中在該觀察期間T_{Obs}

之際，該平均值M_{ECM}係藉由累計多個被該安全處理器的不活動之最小期間T_{InaMin}分隔的連續活動期間所構成之該安全處理器的活動期間T_{Act}所決定。

3. 如申請專利範圍第2項之方法，其特徵在於該安全處理器之每一次激發係由以被打亂的內容相關聯之ECM存取控制訊息提給該安全處理器及承載一控制字組CW與至少一存取條件的描述組成，以為了不將該內容打散而將該控制字組提供給該終端機，及在於：

該安全處理器使用的分析包含下列之步驟：

• 決定在該活動期間T_{Act}之際被該安全處理器處理之ECM訊息的次數N_{ECM}，

• 計算$M_{ECM}=N_{ECM}/T_{Act}$之關係式，

• 比較該關係式之值M_{ECM}與該臨界值S_{max}，

• 若M_{ECM}大於臨界值S_{max}則施用制裁。

4. 如申請專利範圍第3項之方法，其中安全處理器使用係被內建於該安全處理器內的軟體加以分析。

5. 如申請專利範圍第1項之方法，其中該制裁係依下列的步驟被漸進地施用：

• 首先該制裁以嚴重程度n_i被施用一預置次數R_i，

• 然後該制裁以下一個嚴重程度n_{i+1}被施用一預置次數R_{i+1}，

• 最後當最終嚴重程度n_{imax}被到達時，最大制裁被施用。

6. 如申請專利範圍第5項之方法，其中該制裁包含由暫時

封鎖內容接收所組成之一第一嚴重程度、由具有需要與供應該內容之操作員連絡的封鎖內容接收所組成之一第二嚴重程度、及由永久封鎖該內容之接收所組成之一第三嚴重程度。

7. 如申請專利範圍第5項之方法，其中分析參數化與啟動可被操作員藉由發送一EMM訊息而被程式規劃。

8. 如申請專利範圍第1項之方法，其中於目前的日期t_c，一舊的ECM訊息藉由比較此ECM訊息之分配日期t與日期(t_c-t_{Diff})而被決定，此處t_{Diff}代表分隔日期t與日期t_c之先前被定出的最小延遲。

9. 如申請專利範圍第8項之方法，其中於日期t_c計算成功地被處理之當時的ECM訊息之次數N_{ECM}包含下列之運算：

- 比較日期t與日期(t_c-t_{Diff})，
- 若日期(t_c-t_{Diff})小於或等於日期t，增加次數N_{ECM}，否則將次數N_{ECM}維持於目前值，
- 若日期t為介於日期t_c與日期t_c+t_{InaMin}間，以$(t-t_c)$值提高活動期間T_{Act}，否則將活動期間T_{Act}維持於目前值。

10. 如申請專利範圍第1項之方法，其中在瞬間t_0開始的觀察期間之際的安全處理器使用之分析包含下列的運算：

- 計算關係式$M_{ECM} = N_{ECM}/T_{Act}$，
- 檢查T_{Act}是否大於或等於一預置期間T_{ActMin}及M_{ECM}是否大於S_{max}，

若為是，

• 施用該制裁，

• 提高制裁之次數n及/或被施用的該制裁之嚴重程度，

• 重新預置N_{ECM}，T_{Act}與t_0值，

否則，

• 將控制字組CW解密，

• 若期間$(t-t_O)$大於觀察期間T_{Obs}之長度，

--重新預置N_{ECM}，T_{Act}與t_0值，

• 若日期t大於日期t_c，則

--以日期t替換日期t_c。

11. 如申請專利範圍第10項之方法，其中於觀察期間T_{Obs}之際所成功地處理之ECM訊息之次數被增加預置臨界值N_{Buf}時，參數N_{ECM}，t_C與T_{Act}被傳送至EEPROM記憶體內。

12. 如申請專利範圍第1項之方法，其中分析參數化與啟動可被操作員藉由發送一EMM訊息而被程式規劃。

13. 如申請專利範圍第12項之方法，其中該EMM訊息攜載至少一個下列之參數：

• 觀察期間之長度T_{Obs}，

• 最小活動期間T_{ActMin}，

• 延遲T_{Diff}，

• 最小不活動期間T_{InaMin}，

• 臨界值S_{max}，

• 臨界值N_{Buf}。

14. 一種欲控制由至少一操作員供應到一接收終端機之被

打散的數位內容之第一次使用之安全處理器，其特徵在於其包含：

• 一第一模組，其用於分析在一預置觀察期間T_{Obs}之際的該安全處理器之使用，

• 一第二模組，其用於以該分析為基準來決定在該觀察期間T_{Obs}之際之該安全處理器每單位時間的激發數的平均值M_{ECM}，及用於比較該平均值M_{ECM}與一預置臨界值S_{max}，以及

• 一第三模組，其用於在若平均值M_{ECM}大於臨界值S_{max}，對該終端機施用一制裁，此處其嚴重程度漸進地提高，

其中於該安全處理器之該第一模組內所進行之該分析係於目前的日期t_c來決定具有與該目前的日期t_c同時之一分配日期的ECM訊息，以判定內容之一第一次使用，及決定具有在該目前的日期t_c之前的分配日期之ECM訊息，以判定內容之再次使用，及

其中於目前的日期t_c所判定之當時之ECM訊息的次數N_{ECM}係在如小於預置最小長度T_{ActMin}之活動期間T_{Act}的長度來計算，用以計算$M_{ECM}=N_{ECM}/T_{Act}$之關係式，以判定該平均值M_{ECM}是否大於該臨界值S_{max}。

15. 如申請專利範圍第14項之安全處理器，其中分析參數化與啟動可被操作員藉由發送一EMM訊息而被程式規劃。

16. 一種電腦程式，包括程式碼指令，用於當該程式儲存於

一晶片卡且於一安全處理器上被執行時施作如申請專利範圍第1項之方法中的步驟，其中該安全處理器與一終端機相關聯用以使用被一操作員供應至該終端機之數位內容，其特徵在於該程式碼包含：

• 用於分析在一預置觀察期間T_{Obs}上被該終端機使用之該晶片卡之指令，

• 用於以該分析為基準來決定在該觀察期間T_{Obs}之際被該終端機對該晶片卡之每單位時間的激發次數之平均值M_{ECM}，及用於比較該平均值M_{ECM}與一預置臨界值S_{max}之指令，以及

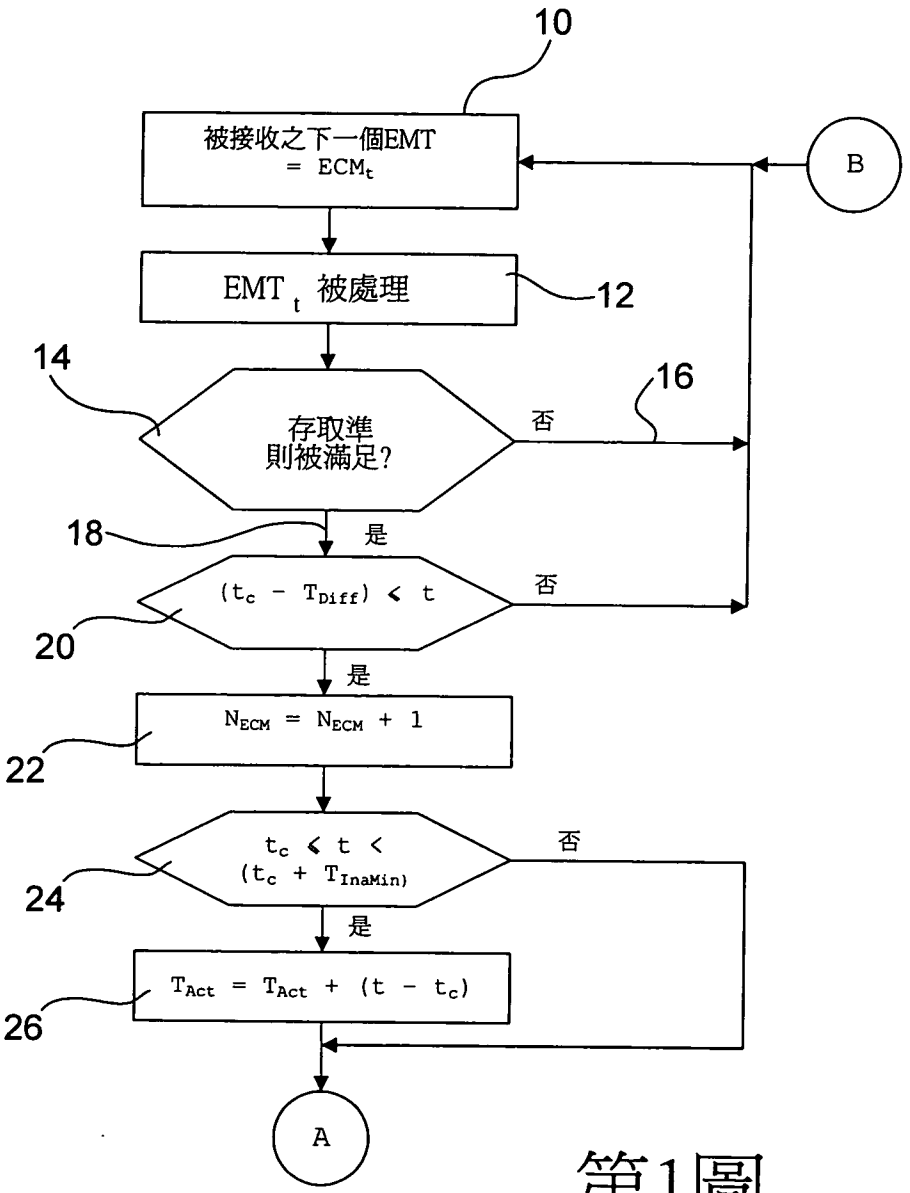
• 若該平均值M_{ECM}大於該臨界值S_{max}時用於對該終端機施用一制裁之指令，此處其嚴重程度漸進地提高。

17. 一種電腦程式，包括程式碼指令，用於當該程式儲存於一晶片卡且於一安全處理器上被執行時施作如申請專利範圍第5項之方法中的步驟，其中該安全處理器與一終端機相關聯用以使用被一操作員供應至該終端機之數位內容，其特徵在於該程式碼包含：

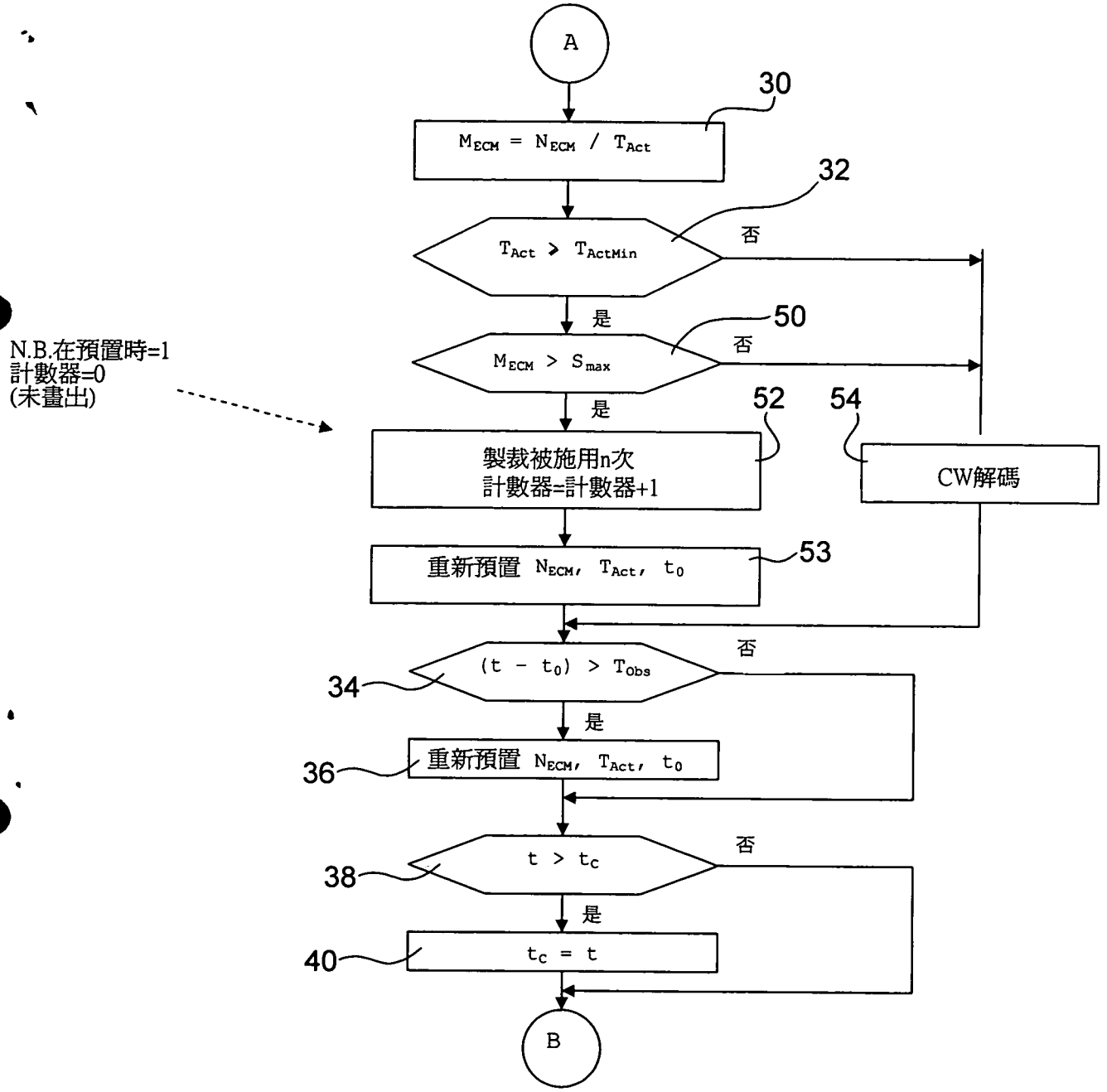
• 用於分析在一預置觀察期間T_{Obs}上被該終端機使用之該晶片卡之指令，

• 用於以該分析為基準來決定在該觀察期間T_{Obs}之際被該終端機對該晶片卡之每單位時間的激發次數之平均值M_{ECM}，及用於比較該平均值M_{ECM}與一預置臨界值S_{max}之指令，以及

• 若該平均值M_{ECM}大於該臨界值S_{max}時用於對該終端機施用一制裁之指令，此處其嚴重程度漸進地提高。


10
被接收之下一個EMT
= ECMt
B
EMT t 被處理
12
14
存取準
則被滿足?
16
否
是
18
(tc - TDiff) < t
否
20
是
NECM = NECM + 1
22
tc < t <
(tc + TInaMin)
否
24
是
TAct = TAct + (t - tc)
26
A

第1圖


A
30
$M_{ECM} = N_{ECM} / T_{Act}$
32
$T_{Act} > T_{ActMin}$
否
是
50
$M_{ECM} > S_{max}$
否
是
N.B.在預置時=1
計數器=0
(未畫出)
52
54
製裁被施用n次
計數器=計數器+1
CW解碼
重新預置 N_{ECM}, T_{Act}, t_0
53
否
$(t - t_0) > T_{Obs}$
34
是
重新預置 N_{ECM}, T_{Act}, t_0
36
否
$t > t_c$
38
是
$t_c = t$
40
B

第2圖