(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-524455
(P2006-524455A)
(43)公表日　平成18年10月26日(2006.10.26)

(51)Int.Cl.		F I			テーマコード（参考）
H04N 7/16	(2006.01)	H04N	7/16	Z	5B017
G06F 21/24	(2006.01)	G06F	12/14	520D	5C164
G09C 1/00	(2006.01)	G06F	12/14	520P	5J104
		G06F	12/14	540A	
		G09C	1/00	660D	

審査請求 未請求　予備審査請求 未請求　（全 20 頁）

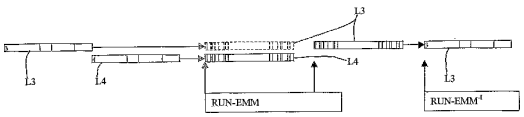
(21)出願番号　特願2006-506665 (P2006-506665)
(86)(22)出願日　平成16年3月2日 (2004.3.2)
(85)翻訳文提出日　平成17年10月4日 (2005.10.4)
(86)国際出願番号　PCT/IB2004/050185
(87)国際公開番号　WO2004/079672
(87)国際公開日　平成16年9月16日 (2004.9.16)
(31)優先権主張番号　CH00325/03
(32)優先日　平成15年3月3日 (2003.3.3)
(33)優先権主張国　スイス(CH)

(71)出願人　500477997
ナグラカード　エス．　アー．
スイス国　セー　アッシュ　－　１０３３　シュゾ　－　シュル　－　ローザンヌ　ルート　ドゥ　ジュネーヴ　２２
(74)代理人　100085372
弁理士　須田　正義
(72)発明者　クデルスキ，エンリ
スイス　ＣＨ－１０７１　シェクスブル，リュ　ドゥ　ブルグ　７
(72)発明者　ブリック，オリヴィエ
スイス　ＣＨ－１０５２　ル　モン－スュール－ローザンヌ，　シュマン　ドゥ　ラ　ペローズ　３９

最終頁に続く

(54)【発明の名称】セキュリティモジュールのオフ操作及び再度オン操作方法

(57)【要約】
本発明は、特に限定受信データへのアクセス管理のためのセキュリティモジュールのオフ操作及び再度オン操作方法に関する。そのようなセキュリティモジュールは値を格納する複数のレジスタ（R_1，R_2，R_3，R_n）を含む。本方法は、セキュリティモジュールのメモリーにロードされついで実行される１つの実行可能コードを含む少なくとも１つの管理メッセージ（ＲＵＮ－ＥＭＭ）を送信する工程を含む。このコードの実行は特に、レジスタの値のスクランブル及び／又は暗号化を発生させること、即ちこれらの値を読めなくすることができる。またこの方法により、予めオフになっているセキュリティモジュールを再度オンすることも可能である。この場合、本方法は、セキュリティモジュールのオフ操作のために用いられる実行可能コードの機能とは逆の機能を有する、モジュールの再度オン操作のための実行可能コード（$RUN-EMM^{-1}$）を含む別のコードを送信する工程を含む。



【特許請求の範囲】
【請求項１】
値を格納する複数のレジスタ(R_1 , R_2 , R_3 , R_n)を含む、特に限定受信データへのアクセス管理のためのセキュリティモジュールのオフ操作及び再度オン操作方法であって、１つの実行可能コードを含む少なくとも１つの管理メッセージ(RUN-EMM)を送信する工程を含み、前記実行可能コードはセキュリティモジュールのメモリーにロードされついで実行されることを特徴とするセキュリティモジュールのオフ操作及び再度オン操作方法。
【請求項２】
前記実行可能コード(RUN-EMM)がレジスタ(R_1 , R_2 , R_3 , R_n)に格納された前記値を可逆的に変更することを特徴とする、請求項１記載の方法。
【請求項３】
前記実行可能コード(RUN-EMM)がレジスタ(R_1 , R_2 , R_3 , R_n)に格納された前記値をスクランブルさせることを特徴とする、請求項１又は２記載の方法。
【請求項４】
前記実行可能コード(RUN-EMM)がレジスタ(R_1 , R_2 , R_3 , R_n)に格納された前記値を暗号化することを特徴とする、請求項１又は２記載の方法。
【請求項５】
マーカーを含むメッセージの送信という予備工程を含み、前記マーカーはセキュリティモジュールのある決まったロットに共通であって各ロット毎に異なることを特徴とする、請求項１記載の方法。
【請求項６】
前記実行可能コード(RUN-EMM)が、マーカーを含む全てのセキュリティモジュールに作用することを特徴とする、請求項５記載の方法。
【請求項７】
前記実行可能コード(RUN-EMM)が、マーカーがある決まった値を有する全てのセキュリティモジュールに作用することを特徴とする、請求項５記載の方法。
【請求項８】
モジュールの再度オン操作のための実行可能コード($RUN\text{-}EMM^{-1}$)を含む別のメッセージを送信する工程を含み、前記実行可能コードはセキュリティモジュールのオフ操作のために用いられる実行可能コード(RUN-EMM)の機能とは逆の機能を有することを特徴とする、請求項１記載のオフ操作及び再度オン操作方法。
【請求項９】
各セキュリティモジュールのマーカーの値を決める工程と、再度オン操作のための実行可能コード($RUN\text{-}EMM^{-1}$)を含む少なくとも１つのメッセージを送信する工程とを含み、前記実行可能コード($RUN\text{-}EMM^{-1}$)はセキュリティモジュールのオフ操作のために用いられる実行可能コード(RUN-EMM)の機能とは逆の機能を有し、前記コードは値が予め決められたマーカーを有する各セキュリティモジュールのために実行されることを特徴とする、セキュリティモジュールがマーカーを含む、請求項８記載の方法。
【請求項１０】
値が予め決められたマーカーが予め決められたユニークな設定値をもつように、このマーカーを有する全てのセキュリティモジュールに作用するメッセージであるマーカー値変更メッセージを送信する工程と、実行可能コード($RUN\text{-}EMM^{-1}$)を含む少なくとも１つのメッセージを送信する工程とを含み、前記実行可能コード($RUN\text{-}EMM^{-1}$)はセキュリティモジュールのオフ操作のために用いられる実行可能コード(RUN-EMM)の機能とは逆の機能を有し、前記コードは値が予め決められた設定値であるマーカーを有する各セキュリティモジュールのために実行されることを特徴とする、請求項８記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、特に、条件付アクセスデータへのアクセス制御のためのセキュリティモジュ

ールのオフ操作及び再度オン操作方法であって、更新の一環として、例えばチップカードの形態で作製されたセキュリティモジュールを新しいセキュリティモジュールに交換することができる方法に関する。

【背景技術】

【０００２】

特に有料テレビの分野においては、セキュリティモジュールにより異なる３つの当事者が介入することになり、各当事者は権利を有し、それぞれ異なる、権利転送又は使用手段を有する。これらの当事者とは、このセキュリティモジュールのユーザー、運用者、及び製造者である。

【０００３】

ユーザーは、運用者が提供するイベント又はイベントグループに関する権利を取得することができる。ユーザーが、購読という形態で或いは衝動買いによりこれらの権利を取得した場合、これらのメッセージは管理メッセージ（ＥＭＭ）によりユーザーのセキュリティモジュール内にロードされる。受信者が、権利を取得したイベントに対応する暗号化コンテンツを受信すると、セキュリティモジュールはコンテンツを復号化する手段を受信者に与える。こうしてイベントをノンスクランブルで表示することができる。

【０００４】

権利がセキュリティモジュール内に存在しない場合、イベントに対応するコンテンツを暗号化するために使われた制御語は、セキュリティモジュールによって復号器に返送されることはなく、イベントをノンスクランブルで表示することはできない。

【０００５】

上述の第２の当事者である運用者は、自身が配信を所望するイベントに関する権利並びに暗号手段を有する。これらの暗号手段は、権利を取得したユーザーのみがイベントをノンスクランブルでみることができるように、配信するイベントのコンテンツを暗号化するのに使用される。通常、送信するコンテンツは、制御語が暗号化されたイベントの大部分を表示するのに制御語の復号化が用いられるのを防止するために、一定間隔で変更される制御語を用いて暗号化される。

【０００６】

既知のように、これらの制御語は、イベントに対応するコンテンツのフローとは別の制御メッセージ（ＥＣＭ）のフローにてユーザーに送信される。

【０００７】

第３の当事者はセキュリティモジュールのサプライヤである。セキュリティモジュールのサプライヤは、運用者の場合のようなイベントに関する権利ではなく、セキュリティモジュールの管理に関する権利を有する。セキュリティモジュールのサプライヤは極めて高いセキュリティレベルを有する暗号手段も有する。実際、セキュリティモジュールの安全性が破壊された場合、ある特定のイベントに関連する権利がセキュリティモジュール内に含まれているかどうかをデコーダが問い合わせる際、常に肯定応答する偽造セキュリティモジュールを使用することが容易である。この場合、運用者はもはや、配信用に提供するイベントに関連する権利を販売することができなくなる。

【０００８】

これらの様々な理由により、セキュリティに関わる進化した機能にアクセスするエンティティの数を最小限にとどめることが推奨される。

【０００９】

しかしながら実際には、セキュリティモジュールのパラメータ全体に関わるいくつかの進化した機能に運用者がアクセスする必要が生じることがある。特に、モジュールの更新の結果、新しいセキュリティモジュールを設置しなければならない時にそのようなことが生じる。

【００１０】

現状では、更新の際、ユーザーは例えば郵送により新しいセキュリティモジュールを受け取るとともに、旧のセキュリティモジュールの回収、破壊、又はモジュールサプライヤ

への返送及び新規モジュールとの交換のため、一定の猶予時間を有する。
【００１１】
モジュールのサプライヤの観点から見るとこれらの交換に関して２つの手法を用いることができる。その手法のうちの一方は予め決められた値をレジスタに入力し、カードはもはや使用できないことを知らせるようにすることであり、もう一方は、レジスタの全ての値を消去することである。
【００１２】
ある値をレジスタに入力することを内容とする第１の手法においては、コマンドがセキュリティモジュールに送信される。このコマンドは、管理センターにより、セキュア化された管理メッセージ（ＥＭＭ）の形態で送信される。メッセージは各ユーザー、単数又は複数のユーザーグループ、或いは全てのユーザーに個別に送ることができる。このメッセージは、セキュリティモジュールがもはや有効でないことを、そのために設けたメモリー領域に記録することを目的とする。前記モジュールの内部のソフトウェアは、毎回の始動時にこの値を確認し、モジュールが無効であることをこの値が示している場合には待機状態になる。この手法は、更新に問題がある時、当該レジスタ内の既定値を再度変更し、その結果、カードを再度オン操作にする新しいメッセージを送信することが可能である、という長所を有する。この手法の欠点は、セキュリティモジュール内に含まれているデータレジスタの構造を知る者は、適当なレジスタ内のデータの値を変更し、セキュリティモジュールを再度オンすることができないことである。このように２つのセキュリティモジュールが共存することは可能であるが、これは好ましいことではない。
【００１３】
第２の手法は、レジスタの全ての値、即ち権利を消去するものであり、暗号化されたメッセージである管理メッセージ内に含まれるコマンドにより実施される。このコマンドは、セキュリティモジュール内に存在し同モジュールの製造時に入力されるソフトウェアをオンにする。この手法は、セキュリティモジュールによってコマンドが送受信されると、レジスタのうちの１つのレジスタの値に作用させてカードを再度オンすることが不可能であるという長所を有する。これにより、許可されていないカードの使用が防止される。欠点は、それによってセキュリティモジュールの運用者又はサプライヤによるカードの再起動も阻まれることであるが、このことは更新の問題がある時には望ましい状況となることもある。
【発明の開示】
【発明が解決しようとする課題】
【００１４】
本発明は、許可されている当事者には再度オンできる可能性を提供しつつ、事前にオフにされているモジュールを許可されていない方法で再度オンすることが極めて難しいセキュリティモジュールの更新方法を実現することにより、先行技術による方法の欠点を解消することを目的とする。更に、サプライヤが所持するセキュリティを運用者に提示する必要なく、事前にオフにされているモジュールの再度オン操作は、運用者及び／又はモジュールのサプライヤによって実現することができる。
【課題を解決するための手段】
【００１５】
この目的は、値を格納する複数のレジスタを含む、特に限定受信データへのアクセス管理のためのセキュリティモジュールのオフ操作及び再度オン操作方法であって、１つの実行可能コードを含む少なくとも１つの管理メッセージを送信する工程を含み、前記実行可能コードはセキュリティモジュールのメモリーにロードされついで実行されることを特徴とするモジュールのオフ操作及び再度オン操作方法により達成される。
【００１６】
本発明及びその長所は、種々の実施形態についての記述並びに添付の図面を参照することにより、よりよく理解されよう。
【発明を実施するための最良の形態】

【００１７】
本発明による方法の第１の実施形態においては、セキュリティモジュールは全て同時に或いはロット毎にオフすることができる。この実施形態の記述においては同時オフ操作とロット別オフ操作とを区別していない。この第１実施形態は、更新に問題がある時、処理すべきモジュールの数も、時間の経過におけるこれらのモジュールの処理間隔も気にすることなくセキュリティモジュールをオフし、再度オンする方法を記述している。
【００１８】
本発明による方法において、ある１つのセキュリティモジュール又はモジュール全体の更新を所望する時には、管理センターは、ある特定の管理メッセージをこのモジュール全体に送信する。この管理メッセージは実行可能コード（ＲＵＮ－ＥＭＭ）を含む。
【００１９】
このコードはセキュリティモジュールのメモリー内にロードされ、レジスタR_1，R_2，R_3，R_n並びにこれらのレジスタ内に格納されているデータの値或いはこれらの値の読み取り方法に対し作用し、その結果、モジュールの運用者及び／又はサプライヤにとって既知の方法によりこれらのデータが変更される。そのために、データを変更する方法として複数の方法を想定することができる。レジスタ内に格納されているデータは対称又は非対称暗号化鍵を使用して暗号化することができる。単純な機能（排他的ＯＲ、シフト．．．）によりレジスタをスクランブルさせることが可能である。複数のレジスタの内容をスクランブルさせることが可能である。また、割り当てテーブル内のポインタをスクランブル又は暗号化することにより、データ又はレジスタの内容を変更することなく、データ又は内容の読み取りを不可能にすることも可能である。更に、セキュリティモジュールの主な要素の代わりとなる実行コードを送信することも可能である。これら主な要素は例えば制御メッセージ（ＥＣＭ）の読み取り能力に関わることがある。ただし主な要素の中には変更してはならないものもあり、それを守らないと、オフしたモジュールを再度オンすることが不可能になることがある。そのような要素は例えば管理メッセージ（ＥＭＭ）の処理能力である。また、これらの様々な手法を併用することも可能であることは明らかである。
【００２０】
プログラム又は実行可能コードは、ある決まったレジスタの値にのみ作用するのではなく、複数のレジスタの複数の値に作用する。レジスタ内に格納されている全てのデータはセキュリティモジュール内に残っているものの、モジュールを使用不可能にする変更を受けていることに留意しなければならない。実際には、運用上の理由から、モジュールが、変更されたデータを有効なデータとして処理することを防止するために、メモリーの変更に伴い、この無効化がレジスタに登録される。実行可能コードは、セキュリティモジュールのメモリー内でこのコードを消去することにより終了することができ、その結果、いったんコードが実行されるとそのコードはモジュール内に存在しなくなるか、或いは少なくともこのコードのうちの一部は存在しなくなる。強制ではないが実際の実施例によれば、実行可能コードは、セキュリティモジュール内に記憶されている単数又は複数のプログラム要素と協動することがあるため、モジュールの更新を実施することができるようにするためには、実行可能コード及びこれらのプログラム要素が存在していなければならない。
【００２１】
これらのプログラム要素は例えばメモリーへの書き込み、メモリーの一部の消去等のために使用することができる。上で記述したような操作を行うことにより、たとえモジュールのレジスタの構造を知っていても、スクランブル又は暗号化に用いられた実行可能コードをもっていない限り、いったんオフされたモジュールを再度オンすることは不可能である。このスクランブルの略図を図１に示す。実行可能コードは、上で言及したように管理センターによって送信される部分と、セキュリティモジュールに記憶される部分とをもつことができ、モジュールをオフするためにはこれら２つの部分が協動しなければならないことに留意すべきである。セキュリティモジュール内に記憶されている実行コードの部分を分析しても、実行可能コードの送信された部分を推測することはできない。従って、事

前にオフにされているモジュールを許可なく再度オンすることは不可能である。

【００２２】

図２は、図１を参照して記述した方法によりオフにしたセキュリティモジュールの一部又は全てを再度オンすることを所望する場合を図示したものである。この状況は、例えばモジュールの更新時に問題が発生した場合に、望ましくなることがある。この場合、管理センターは、その前に送信したコードの作用とは逆の作用を有する実行可能コード（ＲＵＮ－ＥＭＭ$^{-1}$）を、再度オンさせたいモジュール又はモジュール全体に送信する。この新しいコードは、スクランブル又は暗号化のために使用した実行可能コードにより前回処理されたレジスタの値を変更し、セキュリティモジュールのレジスタの値のスクランブル解除又は復号化を行い、このモジュールを再度使用可能にする機能を有する。この再度オン操作は、ある決まった集合に属する全てのモジュールについても、或いはその中の一部についても行うことができる。この再度オン操作は、スクランブル解除又は復号化が可能な実行可能コードを入手した時点以降でないと実行できないことは明らかである。

【００２３】

この方法は先行技術の方法と比べ様々な長所を有する。まずこの方法は可逆的である、即ちそのことは、何らかの理由により、ある決まったロットのセキュリティモジュールの再度オンを所望する場合、それを容易に実施することができることを意味する。他方、スクランブルの解除が可能なコードを知らない限り、オフになっているモジュールを再度オンにすることは不可能であるため、この方法によって極めて良好なセキュリティが提供される。

【００２４】

上で記述した方法は、セキュリティモジュールの運用者でもサプライヤでも適用することができる。しかしながら、この操作中は、セキュリティのレベルは極めて高いものであることが必要であるため、セキュリティモジュールのサプライヤが本方法を受け持つのが望ましいことがある。

【００２５】

以下の記述においては、本発明による方法について記述する実施形態は、処理するセキュリティモジュールの数に関する強制的遵守事項、使用可能帯域、及びこれらのモジュールの処理に必要な時間を考慮している。

【００２６】

実際、交換するセキュリティモジュールが多数ある場合、実行可能コードを含むメッセージを各モジュールに送ることは不可能である。実際、更新が有効であるようにするためには、例えば１年というような長期間更新メッセージが配信されることが必要である。反対に、更新する全てのモジュールに対し、或いは少なくともそれらのモジュールのうちの多くの部分にただ１つのメッセージを配信できるのが望ましい。

【００２７】

最初にセキュリティモジュールをロット別に分けるが、これらのロットは、例えばセキュリティモジュールの製造年月日に従って決められ、セキュリティモジュールの交換を所望する加入者グループ又はその一部に対応する。

【００２８】

一例として、図３に略図で示すように、新しいセキュリティモジュールを受け取る人の集合をＬ１からＬ４までの４つのロットに分離することが可能である。各ロットは、そのロットが属するロット番号Ｌ１，Ｌ２，Ｌ３，又はＬ４を特定のマーカーの形態で含む管理メッセージを受け取る。このメッセージは例えば６ヶ月から１年という比較的長い期間で送信することができ、その結果、全てのユーザーがメッセージを受信したことを確認することができる。マーカーとは、セキュリティモジュール内に設けられたレジスタのうちの１つに入力された特別な値である。マーカーを含む管理メッセージは全てのセキュリティモジュールに同時に送信するか、反対に、一回に、ある１つのロットに送信することができるが、これは処理するモジュール数及び使用可能な透過帯域に特に依存する。有利な方法は、あるロットに対し、例えば毎週というように一定間隔で管理メッセージを送信す

ることである。なお、初期設定では各セキュリティモジュールは値が０のマーカーを１つ含むことができることに留意する必要がある。マーカーを含むメッセージをモジュールが受信したことがわかっている時には、明白な記載がある場合を除き、このマーカーは０ではない値を持っていると理解しなければならない。

【００２９】

ある時間の経過後、全てのロットの大部分のセキュリティモジュールがマーカーを受信したことが確実と思われるようになると、モジュールのサプライヤは、上で図１を参照して記述したような実行可能コードＲＵＮ－ＥＭＭを送信する。実行可能コードはまず、マーカーを含むレジスタの内容を確認し、その結果、セキュリティモジュールが、更新を行わなければならないロットのうちの１つに属しているかどうかを確認する。個別の実施形態によれば、通常の使用の場合、即ち更新の予定がない場合、マーカーのレジスタの内容は０とすることができるが、更新が予定されておりモジュールがマーカーを受信した場合は、０より大きい値とすることができる。この場合、実行可能コードは、マーカーが必ず０より大きいあらゆるセキュリティモジュールについて、即ちマーカーを含む管理メッセージを受信し処理したあらゆるモジュールについて実行される。上で記述したように、このコードは、スクランブル解除又は復号化コードをもたない人に対しセキュリティモジュールを使用不可能にするように、セキュリティモジュールの様々なレジスタの内容をスクランブル化又は暗号化する効果を有する。

【００３０】

この実行可能コードＲＵＮ－ＥＭＭは、上で定義したようなマーカーを含む全てのセキュリティモジュールに作用するように、非常に長期間、定期的に送信することができる。従って、マーカーを含むセキュリティモジュールが、同モジュールに一定期間結合されていたデコーダから抜き取られた場合、同モジュールは、再度デコーダに挿入された時にオフにされる。

【００３１】

ある変形形態によれば、マーカーが０より大きい全てのモジュールについてコードを実行する代わりに、マーカーが、例えば３というような、ある決まった数値を有するセキュリティモジュールについてのみコードを実行することも可能である。この場合、各ロットのセキュリティモジュールは個別に処理されるため、モジュールの更新に関してはより高い柔軟性が得られるが、実行可能コードを含むメッセージに関してより複雑な管理が求められる。

【００３２】

実行可能コードを含むメッセージの送信、従ってそれに関するセキュリティは、サプライヤによって管理される。一方、運用者は、マーカーを含むメッセージの送信を管理し、どのタイミングから、実行可能コードを含むメッセージの送信を開始することができるかをサプライヤに知らせる。

【００３３】

例えば不正確な更新のため、あるロットのセキュリティモジュールを再度オンしなければならない時には、２つの変形形態が可能である。第１の変形形態においては、ある決まったロットを再度オンする。例として、上で記述したように、図４のロット３をオフにした後、再度オンする。この場合、再度オンするロットがそのマーカーにより識別される時には、セキュリティモジュールのサプライヤは、図２を参照して記述した実行可能コードと同様のコードであって、レジスタ及びモジュールの値のスクランブルを解除するよう作用するコードを送信する。この場合、この実行可能コードはまずセキュリティモジュールのマーカーの値を決める。次にこの値を、変更対象となっているロットのモジュールの値と比較する。この値がマーカーと同一である場合、コードは実行されレジスタのスクランブルは解除される。このようにして、該当するセキュリティモジュールが再度オンされる。再度オンすべきロットの値とは異なる値をマーカーが有するモジュールはオフの状態のままであり、使用不可能である。

【００３４】

この方法の一変形形態では、再度オン操作はある決まったロットに作用するのではなく、ある決まった特性を有するあらゆるセキュリティモジュールに作用することができる。あるモジュール、又はあるモジュールのロットを再度オンしなければならない時、運用者は、例えば－１の値を有する決まったマーカーを含むメッセージをまず送信する。該当するモジュールに以前含まれていたマーカーはこのマーカーにとって代えられる。

【００３５】

この場合、サプライヤは次に、上で定義したような実行可能コードを含むメッセージを送信するが、このメッセージは、マーカーが－１の値をもつセキュリティモジュールの値及びレジスタに作用する。そのようなメッセージはセキュリティモジュールのサプライヤにより定期的に送信することができる。一方、運用者は、マーカーが－１の値をとるようにマーカーの値を変更するメッセージを送信することができる。従って運用者は、モジュールのサプライヤとは無関係に、自身でセキュリティモジュールの再度オン操作を管理することができ、その場合モジュールのサプライヤは、運用者にとって極めて機密な暗号情報を送信する必要がない。

【００３６】

この方法は先行技術の方法と比べていくつかの長所を有している。例えば、先行技術の方法では、セキュリティモジュールは、予め決められたレジスタの値を変更し、モジュールをオン又はオフすることは可能である。この場合、モジュールを詳細に分析することによりプログラムの効果を知ることができ、場合によってはプログラムのシミュレーションを行うことは可能である。また、プログラムはモジュール内に記憶されるので、モジュールの製造時に想定された方法でしか作用しない。従ってプログラムは進化する可能性を全く有さない。本発明による方法では、実行可能コードの使用時に同コードが送信されるため、その内容の分析が防止され、そのタイミングの実際の利用に対応するコードを送信することができるので、コードはニーズに応じて著しく進化することができる。

【図面の簡単な説明】

【００３７】

【図１】図１はセキュリティモジュールがオフの状態である本発明による方法の第１実施形態を示す図である。

【図２】図２は図１に示すオフの状態のモジュールが再度オンされる方法の実施形態を示す図である。

【図３】図３は本発明の方法による複数のロットのセキュリティモジュールのオフ操作を示す略図である。

【図４】図４は図３に略図で示した方法によりオフにされたロットのうちの１つのロットのセキュリティモジュールの再度オン操作を示す図である。

【図１】

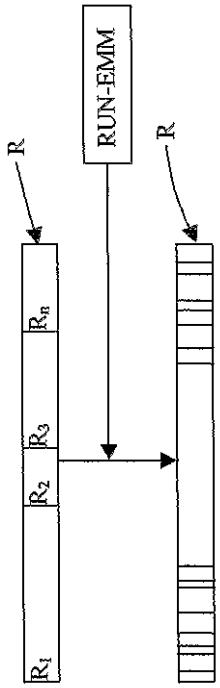


FIG. 1

【図２】

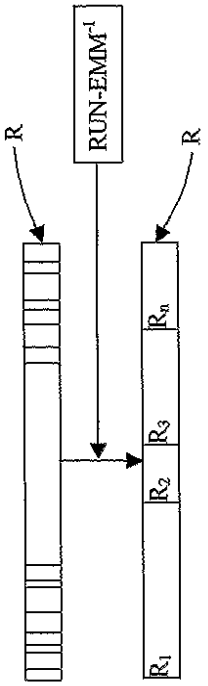


FIG. 2

【図３】

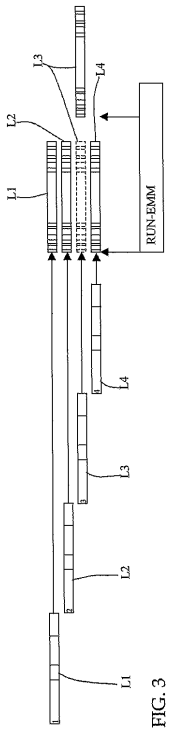


FIG. 3

【図４】

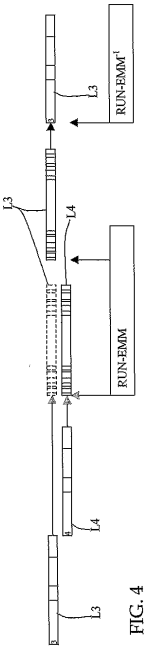


FIG. 4

【手続補正書】
【提出日】平成18年3月28日(2006.3.28)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
値を格納する複数のレジスタ(R_1，R_2，R_3，R_n)を含む、特に限定受信データへのアクセス管理のためのセキュリティモジュールのオフ操作及び再度オン操作方法であって、１つの実行可能コードを含む少なくとも１つの管理メッセージ(RUN-EMM)を送信する工程を含み、前記実行可能コードはセキュリティモジュールのメモリーにロードされついで実行され、その実行がレジスタ(R_1，R_2，R_3，R_n)に格納された前記値を可逆的な方法で変更し、変更後レジスタの内容はモジュールを使用不可能にすることを特徴とするセキュリティモジュールのオフ操作及び再度オン操作方法。
【請求項２】
前記実行可能コード(RUN-EMM)がレジスタ(R_1，R_2，R_3，R_n)に格納された前記値をスクランブルさせることを特徴とする、請求項１記載の方法。
【請求項３】
前記実行可能コード(RUN-EMM)がレジスタ(R_1，R_2，R_3，R_n)に格納された前記値を暗号化することを特徴とする、請求項１記載の方法。
【請求項４】
マーカーを含むメッセージの送信という予備工程を含み、前記マーカーはセキュリティモジュールのある決まったロットに共通であって各ロット毎に異なることを特徴とする、請求項１記載の方法。
【請求項５】
前記実行可能コード(RUN-EMM)が、マーカーを含む全てのセキュリティモジュールに作用することを特徴とする、請求項４記載の方法。
【請求項６】
前記実行可能コード(RUN-EMM)が、マーカーがある決まった値を有する全てのセキュリティモジュールに作用することを特徴とする、請求項４記載の方法。
【請求項７】
モジュールの再度オン操作のための実行可能コード($RUN\text{-}EMM^{-1}$)を含む別のメッセージを送信する工程を含み、前記実行可能コードはセキュリティモジュールのオフ操作のために用いられる実行可能コード(RUN-EMM)の機能とは逆の機能を有することを特徴とする、請求項１記載のオフ操作及び再度オン操作方法。
【請求項８】
各セキュリティモジュールのマーカーの値を決める工程と、再度オン操作のための実行可能コード($RUN\text{-}EMM^{-1}$)を含む少なくとも１つのメッセージを送信する工程とを含み、前記実行可能コード($RUN\text{-}EMM^{-1}$)はセキュリティモジュールのオフ操作のために用いられる実行可能コード(RUN-EMM)の機能とは逆の機能を有し、前記コードは値が予め決められたマーカーを有する各セキュリティモジュールのために実行されることを特徴とする、セキュリティモジュールがマーカーを含む、請求項７記載の方法。
【請求項９】
値が予め決められたマーカーが予め決められたユニークな設定値をもつように、このマーカーを有する全てのセキュリティモジュールに作用するメッセージであるマーカー値変更メッセージを送信する工程と、実行可能コード($RUN\text{-}EMM^{-1}$)を含む少なくとも１つのメッセージを送信する工程とを含み、前記実行可能コード($RUN\text{-}EMM^{-1}$)はセキュリティモジュールのオフ操作のために用いられる実行可能コード(RUN-EMM)の機能とは逆の機能

を有し、前記コードは値が予め決められた設定値であるマーカーを有する各セキュリティモジュールのために実行されることを特徴とする、請求項７記載の方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１５
【補正方法】変更
【補正の内容】
【００１５】
この目的は、値を格納する複数のレジスタを含む、特に限定受信データへのアクセス管理のためのセキュリティモジュールのオフ操作及び再度オン操作方法であって、１つの実行可能コードを含む少なくとも１つの管理メッセージを送信する工程を含み、前記実行可能コードはセキュリティモジュールのメモリーにロードされついで実行され、その実行がレジスタ(R_1，R_2，R_3，R_n)に格納された前記値を可逆的な方法で変更し、変更後レジスタの内容はモジュールを使用不可能にすることを特徴とするモジュールのオフ操作及び再度オン操作方法により達成される。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/050185

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/25278 A (GUNGL KLAUS P ; WENTKER DAVID C (US); VISA INT SERVICE ASS (US)) 4 May 2000 (2000-05-04)	1-4
A	page 8, line 6 - page 16, line 28 figure 1 figure 4 figure 6	5-10
X	WO 98/09257 A (GEMPLUS) 5 March 1998 (1998-03-05)	1
A	abstract; claims; figures page 18, line 22 - page 20, line 19	2-10
A	FR 2 083 960 A (OMRON TATEISI ELECTRONICS) 17 December 1971 (1971-12-17) page 8, line 24 - page 9, line 5	1
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 June 2004	17/06/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Rachkov, V

3

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/050185

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 971 324 A (EUROPAY) 12 January 2000 (2000-01-12) abstract; claims; figures	1,7
A	WO 98/39743 A (DEUTSCHE TELEKOM) 11 September 1998 (1998-09-11) abstract; claims; figures	1,7
A	EP 0 817 485 A (THOMSON MULTIMEDIA) 7 January 1998 (1998-01-07) abstract; claims; figures	1
A	EP 0 713 188 A (DEUTSCHE TELEKOM) 22 May 1996 (1996-05-22)	
A	US 5 682 031 A (GEMPLUS CARD INTERNATIONAL) 28 October 1997 (1997-10-28)	
P,X	EP 1 318 488 A (MATSUSHITA ELECTRIC IND CO LTD) 11 June 2003 (2003-06-11) column 5, paragraph 23 - column 8, paragraph 45 figure 1 figure 2	1-4
A	DE 199 41 550 A (DEUTSCHE TELEKOM AG) 8 March 2001 (2001-03-08)	

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/050185

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0025278 A	04-05-2000	AU 770396 B2	19-02-2004
		AU 1452600 A	15-05-2000
		CA 2347684 A1	04-05-2000
		EP 1125262 A1	22-08-2001
		WO 0025278 A1	04-05-2000
		US 2002040936 A1	11-04-2002
WO 9809257 A	05-03-1998	US 5923884 A	13-07-1999
		AT 235725 T	15-04-2003
		AU 732887 B2	03-05-2001
		AU 4842897 A	19-03-1998
		CA 2233217 A1	05-03-1998
		CN 1206482 A ,B	27-01-1999
		DE 69720181 D1	30-04-2003
		DE 69720181 T2	05-02-2004
		EP 0858644 A1	19-08-1998
		ES 2196358 T3	16-12-2003
		WO 9809257 A1	05-03-1998
		RU 2159467 C2	20-11-2000
FR 2083960 A	17-12-1971	JP 49029083 B	01-08-1974
		JP 49025061 B	27-06-1974
		FR 2083960 A5	17-12-1971
		GB 1325101 A	01-08-1973
		HK 51377 A	07-10-1977
		US 3731076 A	01-05-1973
EP 0971324 A	12-01-2000	EP 0971324 A1	12-01-2000
		AU 4386099 A	24-01-2000
		WO 0002170 A1	13-01-2000
WO 9839743 A	11-09-1998	WO 9839743 A2	11-09-1998
		EP 0970446 A2	12-01-2000
		HU 0001506 A2	28-09-2000
		NO 994236 A	29-10-1999
EP 0817485 A	07-01-1998	FR 2750554 A1	02-01-1998
		CN 1171015 A ,B	21-01-1998
		DE 69715535 D1	24-10-2002
		DE 69715535 T2	22-05-2003
		EP 0817485 A1	07-01-1998
		JP 10164052 A	19-06-1998
		US 6035038 A	07-03-2000
EP 0713188 A	22-05-1996	DE 4441038 A1	23-05-1996
		EP 0713188 A2	22-05-1996
US 5682031 A	28-10-1997	FR 2676294 A1	13-11-1992
		DE 69203233 D1	03-08-1995
		EP 0583348 A1	23-02-1994
		ES 2080505 T3	01-02-1996
		WO 9220042 A1	12-11-1992
		JP 8033914 B	29-03-1996
		JP 6502268 T	10-03-1994
		US 5471045 A	28-11-1995
EP 1318488 A	11-06-2003	JP 2003173427 A	20-06-2003
		CN 1423232 A	11-06-2003

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2004/050185

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1318488 A		EP 1318488 A2	11-06-2003
		US 2003146277 A1	07-08-2003
DE 19941550 A	08-03-2001	DE 19941550 A1	08-03-2001
		AU 765278 B2	11-09-2003
		AU 2808401 A	26-03-2001
		WO 0117249 A1	08-03-2001
		EP 1234449 A1	28-08-2002

Form PCT/ISA/210 (patent family annex) (January 2004)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/IB2004/050185

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10 H04N7/16

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 00/25278 A (GUNGL KLAUS P ; WENTKER DAVID C (US); VISA INT SERVICE ASS (US)) 4 mai 2000 (2000-05-04)	1-4
A	page 8, ligne 6 - page 16, ligne 28 figure 1 figure 4 figure 6	5-10
X	WO 98/09257 A (GEMPLUS) 5 mars 1998 (1998-03-05)	1
A	abrégé; revendications; figures page 18, ligne 22 - page 20, ligne 19	2-10
A	FR 2 083 960 A (OMRON TATEISI ELECTRONICS) 17 décembre 1971 (1971-12-17) page 8, ligne 24 - page 9, ligne 5	1

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
10 juin 2004	17/06/2004

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Rachkov, V

Formulaire PCT/ISA/210 (deuxième feuille) (Janvier 2004)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/IB2004/050185

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 971 324 A (EUROPAY) 12 janvier 2000 (2000-01-12) abrégé; revendications; figures	1,7
A	WO 98/39743 A (DEUTSCHE TELEKOM) 11 septembre 1998 (1998-09-11) abrégé; revendications; figures	1,7
A	EP 0 817 485 A (THOMSON MULTIMEDIA) 7 janvier 1998 (1998-01-07) abrégé; revendications; figures	1
A	EP 0 713 188 A (DEUTSCHE TELEKOM) 22 mai 1996 (1996-05-22)	
A	US 5 682 031 A (GEMPLUS CARD INTERNATIONAL) 28 octobre 1997 (1997-10-28)	
P,X	EP 1 318 488 A (MATSUSHITA ELECTRIC IND CO LTD) 11 juin 2003 (2003-06-11) colonne 5, alinéa 23 - colonne 8, alinéa 45 figure 1 figure 2	1-4
A	DE 199 41 550 A (DEUTSCHE TELEKOM AG) 8 mars 2001 (2001-03-08)	

3

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/IB2004/050185

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0025278	A	04-05-2000	AU	770396 B2	19-02-2004
			AU	1452600 A	15-05-2000
			CA	2347684 A1	04-05-2000
			EP	1125262 A1	22-08-2001
			WO	0025278 A1	04-05-2000
			US	2002040936 A1	11-04-2002
WO 9809257	A	05-03-1998	US	5923884 A	13-07-1999
			AT	235725 T	15-04-2003
			AU	732887 B2	03-05-2001
			AU	4842897 A	19-03-1998
			CA	2233217 A1	05-03-1998
			CN	1206482 A ,B	27-01-1999
			DE	69720181 D1	30-04-2003
			DE	69720181 T2	05-02-2004
			EP	0858644 A1	19-08-1998
			ES	2196358 T3	16-12-2003
			WO	9809257 A1	05-03-1998
			RU	2159467 C2	20-11-2000
FR 2083960	A	17-12-1971	JP	49029083 B	01-08-1974
			JP	49025061 B	27-06-1974
			FR	2083960 A5	17-12-1971
			GB	1325101 A	01-08-1973
			HK	51377 A	07-10-1977
			US	3731076 A	01-05-1973
EP 0971324	A	12-01-2000	EP	0971324 A1	12-01-2000
			AU	4386099 A	24-01-2000
			WO	0002170 A1	13-01-2000
WO 9839743	A	11-09-1998	WO	9839743 A2	11-09-1998
			EP	0970446 A2	12-01-2000
			HU	0001506 A2	28-09-2000
			NO	994236 A	29-10-1999
EP 0817485	A	07-01-1998	FR	2750554 A1	02-01-1998
			CN	1171015 A ,B	21-01-1998
			DE	69715535 D1	24-10-2002
			DE	69715535 T2	22-05-2003
			EP	0817485 A1	07-01-1998
			JP	10164052 A	19-06-1998
			US	6035038 A	07-03-2000
EP 0713188	A	22-05-1996	DE	4441038 A1	23-05-1996
			EP	0713188 A2	22-05-1996
US 5682031	A	28-10-1997	FR	2676294 A1	13-11-1992
			DE	69203233 D1	03-08-1995
			EP	0583348 A1	23-02-1994
			ES	2080505 T3	01-02-1996
			WO	9220042 A1	12-11-1992
			JP	8033914 B	29-03-1996
			JP	6502268 T	10-03-1994
			US	5471045 A	28-11-1995
EP 1318488	A	11-06-2003	JP	2003173427 A	20-06-2003
			CN	1423232 A	11-06-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/IB2004/050185

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1318488 A		EP 1318488 A2	11-06-2003
		US 2003146277 A1	07-08-2003
DE 19941550 A	08-03-2001	DE 19941550 A1	08-03-2001
		AU 765278 B2	11-09-2003
		AU 2808401 A	26-03-2001
		WO 0117249 A1	08-03-2001
		EP 1234449 A1	28-08-2002

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 ヴィルツ, クリスティアン
スイス ＣＨ－１００４ ローザンヌ, シュマン デ バンセル ６
(72)発明者 ハウエルト, パトリック
スイス ＣＨ－１００６ ローザンヌ, アヴェニュ デュ ドゥナントゥ ２３

Ｆターム(参考) 5B017 AA04 AA07 BA06 BA07 CA15
5C164 FA04 PA01 UA12P UB61P UC22P
5J104 NA39 NA41