(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6889161号
(P6889161)

(45)発行日　令和3年6月18日(2021.6.18)　(24)登録日　令和3年5月24日(2021.5.24)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601B
H04L	9/32	(2006.01)	H04L	9/00	601E
G06F	21/60	(2013.01)	H04L	9/00	675A
			G06F	21/60	320

請求項の数 12　(全 18 頁)

(21)出願番号　特願2018-532423 (P2018-532423)
(86)(22)出願日　平成28年12月20日 (2016.12.20)
(65)公表番号　特表2019-500798 (P2019-500798A)
(43)公表日　平成31年1月10日 (2019.1.10)
(86)国際出願番号　PCT/FR2016/053581
(87)国際公開番号　WO2017/109389
(87)国際公開日　平成29年6月29日 (2017.6.29)
審査請求日　令和1年10月8日 (2019.10.8)
(31)優先権主張番号　1562996
(32)優先日　平成27年12月21日 (2015.12.21)
(33)優先権主張国・地域又は機関
フランス(FR)

(73)特許権者　519260337
アイデミア　フランス
フランス国，９２４００　クルブボア，プラス　サミュエル　ドゥ　シャンプラン　２
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100123582
弁理士　三橋　真二
(74)代理人　100114018
弁理士　南山　知広
(74)代理人　100119987
弁理士　伊坪　公一

最終頁に続く

(54)【発明の名称】電子エンティティにおけるデータ受信方法および関連する電子エンティティ

(57)【特許請求の範囲】
【請求項１】
電子エンティティ（２）がデータ（Ｄｉ；ＤＡＴＡＳＥＮＤ）を受信する方法であって、
第１の暗号キー（ＳＫ－ＥＮＣ）を用いた暗号化によってセキュアされた第１のセキュアチャネルを、前記電子エンティティ（２）と外部電子機器との間に確立するステップ（Ｅ２、Ｅ４、Ｅ６、Ｅ８、Ｅ１０）と、
前記第１のセキュアチャネルを介して、第１のコマンド（ＣＨＭ）を受信するステップ（Ｅ１４）と、
前記第１のセキュアチャネルを介して、少なくとも一つの第２の暗号キー（ＢＫ－ＥＮＣ）を受信するステップと、
前記第１のコマンド（ＣＨＭ）を実行することにより、前記第２の暗号キー（ＢＫ－ＥＮＣ）を用いた暗号化によってセキュアされた第２のセキュアチャネルを設定するステップ（Ｅ２０）と、
前記第２のセキュアチャネルにおいて前記データ（Ｄｉ；ＤＡＴＡＳＥＮＤ）を受信するステップ（Ｅ２２）と、
前記データおよび第２のコマンド（ＣＨＭ）を受信するステップの後、前記第１のセキュアチャネルへ変更するステップ（Ｅ３０）と、
前記変更するステップの後、前記第１のセキュアチャネルにおいて認証コマンドを待機するステップと、を有する、ことを特徴とする方法。

【請求項２】
前記第１のコマンドを受信するステップの後で、前記第２のセキュアチャネルを設定するステップの前に、前記電子エンティティ（２）のメモリ（８）の中に前記第１の暗号キー（ＳＫ－ＥＮＣ）をセーブするステップ（Ｅ１８）を有する、請求項１に記載の方法。
【請求項３】
前記変更するステップは、前記メモリ（８）の中にセーブされた前記第１の暗号キーを読み取るサブステップを有する、請求項２に記載の方法。
【請求項４】
前記変更するステップの後、前記第１のセキュアチャネルに関するリストアデータを無効化するステップを有する、請求項１～３のいずれか一項に記載の方法。
【請求項５】
前記第１のセキュアチャネルにおいて完全性検証コード（ＭＡＣ）を検査するステップを有する、請求項１～４のいずれか一項に記載の方法。
【請求項６】
前記第１の暗号キー（ＳＫ－ＥＮＣ）は、前記電子エンティティ（２）の中に記憶される静的キー（Ｋ）から導出されるセッションキーである、請求項１～５のいずれか一項に記載の方法。
【請求項７】
前記第２の暗号キー（ＢＫ－ＥＮＣ）は、他の電子エンティティによって確立されたセキュアチャネルを暗号化するのに用いられるブロードキャストキーである、請求項１～６のいずれか一項に記載の方法。
【請求項８】
前記データ（ＤＡＴＡＳＥＮＤ）は、前記電子エンティティ（２）のオペレーティングシステムの一部、または前記電子エンティティによって後で用いられることができるアプリケーションもしくはデータの少なくとも一部を表す、請求項１～７のいずれか一項に記載の方法。
【請求項９】
前記受信されたデータは、前記電子エンティティ（２）の不揮発性メモリ（６）の中に記憶される、請求項１～８のいずれか一項に記載の方法。
【請求項１０】
前記電子エンティティは、セキュアエレメント（２）である、請求項１～９のいずれか一項に記載の方法。
【請求項１１】
前記外部電子機器は、携帯端末、エネルギ供給メータ、接続されたオブジェクトまたは携帯オブジェクトである、請求項１～１０のいずれか一項に記載の方法。
【請求項１２】
第１の暗号キー（ＳＫ－ＥＮＣ）を用いた暗号化によってセキュアされた第１のセキュアチャネルを、電子エンティティと外部電子機器との間に確立するモジュールと、
前記第１のセキュアチャネルを介して、第１のコマンド（ＣＨＭ）および第２の暗号キー（ＢＫ－ＥＮＣ）を受信するモジュールと、
前記第１のコマンド（ＣＨＭ）を実行することにより、前記第２の暗号キー（ＢＫ－ＥＮＣ）を用いた暗号化によってセキュアされた第２のセキュアチャネルを設定するモジュールと、
前記第２のセキュアチャネルにおいてデータ（Ｄｉ；ＤＡＴＡＳＥＮＤ）を受信するモジュールと、
前記データおよび第２のコマンド（ＣＨＭ）を受信するモジュールの後、前記第１のセキュアチャネルへ変更するモジュールと、
前記変更するモジュールの後、前記第１のセキュアチャネルにおいて認証コマンドを待機するモジュールと、を有する、ことを特徴とする電子エンティティ（２）。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、電子デバイス間のデータのセキュアされた交換に関する。
【０００２】
特に、電子エンティティにおけるデータ受信方法および関連する電子エンティティに関する。
【０００３】
本発明は、特に同じデータが多数の電子エンティティにセキュアされた（セキュリティ保護された、se’curise’）方法で伝達されなければならない場合に、有利に適用される。
【背景技術】
【０００４】
２つの電子デバイス間で機密を守るようにデータを交換するためには、これらの２つの電子デバイス間に、暗号キーを用いた暗号化によってセキュアされたチャネル（セキュアチャネル、canal se’curise’）を確立することが知られている。これに関しては、例えば、「GlobalPlatform Card Technology - Secure Shannel Protocol 03 - Card Specification v2.2 Amendment D」（ｖ１．１）という文書に記載された「ＳＣＰ０３」と呼ばれるプロトコルによって規定されている（pre’vu）。
【発明の概要】
【発明が解決しようとする課題】
【０００５】
このプロトコルの枠組みの中で、データの効果的な保護を保証するために、暗号キーは、２つの電子デバイスによってのみ知られる静的キーによって導出されるセッションキーである。
【０００６】
しかしながら、この解決法は、（例えば、多数のセキュアエレメント（セキュアされたエレメント、e’le’ments se’curise’s）のオペレーティングシステムの一部を更新するキャンペーンの場合のように）多数の電子エンティティへの同じデータセットの伝達には適用されていない。なぜなら、そのために関係する電子エンティティそれぞれのために専用に暗号化されたバージョンを準備する必要があるからである。
【課題を解決するための手段】
【０００７】
この状況において（dans ce contexte）、本発明は、
－第１の暗号キーを用いた暗号化によってセキュアされた第１のセキュアチャネルを、電子エンティティと外部電子機器との間に確立するステップと、
－第１のセキュアチャネルを介して、第１のコマンドを受信するステップと、
－第１のセキュアチャネルを介して、少なくとも一つの第２の暗号キーを受信するステップと、
－第１のコマンドを実行することにより、第２の暗号キーを用いた暗号化によってセキュアされた第２のセキュアチャネルを設定するステップと、
－第２のセキュアチャネルにおいてデータを受信するステップと、を有することを特徴とする、電子エンティティがデータを受信する方法を提案する。
【０００８】
このように、第１のセキュアチャネルは、例えば上記で示したようにＳＣＰ０３タイプのプロトコルを使うことによって、第２の暗号キーを電子エンティティにセキュアされた方法で伝達するために多様化されることができる。
【０００９】
しかしながら、第２のセキュアチャネルの設定によって、望まれる場合、多数の電子エンティティに宛てられるデータを暗号化するのに用いられる第２の暗号キーに基づいて、異なる暗号化を用いることができる。

【００１０】
第１のセキュアチャネルは、例えば予測不能モードでＳＣＰ０３タイプのプロトコルに基づく一方、第２のセキュアチャネルは、例えば予測可能モードでＳＣＰ０３タイプのプロトコルに基づく。
【００１１】
第２の暗号キーは、例えば第１のコマンドに含まれる。
【００１２】
場合によっては、下記の他の特徴が想定される。
－上記方法は、第１のコマンドを受信するステップの後で、第２のセキュアチャネルを設定するステップの前に、電子エンティティの（例えばランダムアクセスメモリなどの）メモリの中に第１の暗号キー（および例えばさらに関連するコンテキストデータ（donne’es contextuelles））をセーブする（第１の暗号キーと、場合によっては関連するコンテキストデータとは、第１のセキュアチャネルのリストアデータを形成する）ステップを有する。
－上記方法は、データおよび第２のコマンドを受信するステップの後、第１のセキュアチャネルへ変更する（basculement）ステップを有する。
－変更するステップは、（ランダムアクセス）メモリにセーブされた第１の暗号キーを読み取るサブステップを有する。
－変更するステップの後、第１のセキュアチャネルに関するリストアデータを無効化するステップを有する。
－変更するステップの後、第１のセキュアチャネルにおいて認証コマンドを待機するステップを有する。
－変更するステップの後、第１のセキュアチャネルにおいて完全性検証コードを受信するステップを有することがある。
－第１の暗号キーは、電子エンティティの中に記憶されている静的キーから導出されるセッションキーである。
－第２の暗号キーは、他の電子エンティティによって確立されたセキュアなチャネルを暗号化するのに用いられるブロードキャストキーである。
－データは、例えばオペレーティングシステムの一部、または電子エンティティによって後で用いられることができるアプリケーションもしくはデータの少なくとも一部を表す。
－受信されたデータは、電子エンティティの不揮発性メモリの中に記憶される。
－電子エンティティは、セキュアエレメントである。
－外部電子機器は、携帯端末、エネルギ供給メータ、接続されたオブジェクトまたは携帯オブジェクトである。
【００１３】
本発明は、同様に、第１の暗号キー（ＳＫ－ＥＮＣ）を用いた暗号化によってセキュアされた第１のチャネルを、電子エンティティと外部電子機器との間に確立するモジュールと、第１のセキュアチャネルを介して、第１のコマンドおよび第２の暗号キーを受信するモジュールと、第１のコマンドを実行することにより、第２の暗号キーを用いた暗号化によってセキュアされた第２のセキュアチャネルを設定するモジュールと、第２のセキュアチャネルにおいてデータを受信するモジュールと、を有することを特徴とする電子エンティティを提案する。
【００１４】
電子エンティティがプロセッサを有する場合、少なくともいくつかのモジュールは、電子エンティティのメモリの中に保存され、命令がプロセッサによって実行される場合に対象のモジュールの動作の実施に寄与するよう設計されたコンピュータプログラム命令を用いて、少なくとも部分的に実現される。
【発明の効果】
【００１５】
提案された解決策は、特に以下の利点を提示する。

－上記解決策のおかげで、セキュアエレメントのオペレータや製造業者、さらにはサプライヤの要望（セキュリティエレメント（e’le’ments se’curitaires）（例えば、ＭＡＣ）と同様に、多様化されたあるいは多様化されていないチャネルで送られるデータの選択）に従ってセキュリティレベルを調整することができ、これによりセキュリティレベルのフレキシビリティを可能にする。
－解決策のおかげで、端末上の異なる展開（de’ploiement diffe’re’）を行うことができる。データはブロードキャストモードで送られ、認証コマンドはロードされたデータの使用をトリガするために、後で送られることができる。この認証コマンドによって、（サプライヤまたは製造業者の）サーバは、常にセキュアエレメントの検査（contro^le）を維持できる（なぜなら、認証の前には、完全性を検査するフェーズがあるからである）。このコマンドのための多様化されたチャネルを使用することで、端末に個別に宛てて（s'adresser）、所望の時間および効果で動作が行われることを保証することができる。
－コンテキストをセーブする規定（詳細はステップＥ１８を参照）によって、１つのモードから他のモードへ変更する際に、多様化されたモードの設定を再開せずにすむ。

【００１６】

詳細には、以下の例において、多様化されたモードのコンテキストをセーブすることを規定できる。しかしながら、他の実施形態では、他のモードへの変更の前に、使用されたモード（例えば多様化されたマルチユーザモード）のそれぞれのために、コンテキストのセーブを規定することができる。

【図面の簡単な説明】

【００１７】

【図１】本発明の枠組みの中で使用されるセキュアエレメントの例を示す図である。
【図２】図１のセキュアエレメントにおいて実施される方法の例を示すフローチャートである。
【図３】図２の方法を使用する可能な第１のコンテキストを示す図である。
【図４】図２の方法を使用する可能な第２のコンテキストを示す図である。
【図５】図１のセキュアエレメントのオペレーティングシステムの更新方法の例を示すフローチャートである。

【００１８】

添付の図を参照する以下の説明は、制限のない例として与えられ、本発明が何で構成されているのかと、それはどのように実現されうるのかと、についてより良く理解できる。

【００１９】

図１は、本発明の枠組みの中で使用されるセキュアエレメント２の例を示す。

【００２０】

このセキュアエレメント（あるいは 「Secure Element」のＳＥ）２は、例えばマイクロコントローラの形で実現される。セキュアエレメント２は、例えば電子機器の中にはんだ付けされて、場合によっては（e’ventuellement）電子機器に統合されることができる。すなわち、セキュアエレメントはｅＳＥ（つまり「embedded Secure Element」）タイプである。

【００２１】

変形例として、セキュアエレメント２は、マイクロサーキットカード（ＩＣカード、carte microcircuit）（例えばユニバーサルマイクロサーキットカードもしくはＵＩＣＣつまり「Universal Integrated Circuit Card」）、はんだ付けされたユニバーサルマイクロサーキットカード、またはｅＵＩＣＣつまり「embedded Universal Circuit Card」のいずれかである。

【００２２】

セキュアエレメント２は、プロセッサ４（例えばマイクロプロセッサ）と、不揮発性メモリ６（例えば再書き込み可能不揮発性メモリ）と、ランダムアクセスメモリ８と、を有する。

【００２３】

不揮発性メモリ６は、例えばＦｌａｓｈタイプまたはＮＶＲＡＭタイプである。

【００２４】

不揮発性メモリ６は、プロセッサ４によって実行される場合、（詳細には図２を参照して以下に説明される）セキュアエレメント２によるデータ処理方法の実施を可能にする、プログラムの命令を記憶する。

【００２５】

不揮発性メモリ６は、さらに、そのような方法の実施の際に使用されるデータを記憶する。つまり、不揮発性メモリ６は、詳細には、以下に説明される方法で使われる（静的キーと呼ばれる）暗号キー、特に静的暗号キーセットＫを記憶する。

【００２６】

ランダムアクセスメモリ８は、セキュアエレメント２において実施される方法によって操作されるデータを記憶する。

【００２７】

セキュアエレメント２は、少なくとも一つのインターフェイス１０を同様に有し、他の電子機器とデータを交換することを、プロセッサ４に可能にさせる。セキュアエレメント２がマイクロコントローラである場合、インターフェイス１０は、マイクロコントローラの１つまたは複数のピンによって形成されることができる。セキュアエレメントがマイクロサーキットカードである場合、インターフェイスは、マイクロサーキットカードの上面に露出されるコンタクトのうち、少なくとも一つを有する。インターフェイスは同様に、ＩＳＯタイプ、ＳＷＰタイプまたはＳＰＩタイプのポートでもよい。

【００２８】

図２は、セキュアエレメント２において実施される方法の例を示す。

【００２９】

この方法は、ステップＥ２において、プロセッサ４がインターフェイス１０でホストチャレンジ（英語では「host challenge」）ＨＣＨを有する起動コマンドＩＵを受信することから始まる。

【００３０】

このような起動コマンドＩＵは、以下に述べるようなセキュアエレメント２によって受信される他のコマンドのように、セキュアエレメント２とセキュアされたデータを交換するために、セキュアされた通信チャネルを確立することを望む（セキュアエレメント２と異なる）電子機器によって事前に送信される。

【００３１】

起動コマンドＩＵは、例えばＩＮＩＴＩＡＬＩＺＥ　ＵＰＤＡＴＥタイプのコマンドで、「GlobalPlatform Card Technology - Secure Channel Protocol 03 - Card Specification v 2.2 Amendment D」という文書の段落７．１．１または「GlobalPlatform Card Specification v 2.2」という文書の付録Ｄ４．１で定義されている。

【００３２】

起動コマンドＩＵを受信すると、プロセッサＥ４は、次に記載されるステップＥ４およびＥ６を実現する。

【００３３】

ステップＥ４において、プロセッサ４は、例えば、ランダム抽出（tirage ale’atoire）によって、変数として、または疑似ランダムの決定（de’termination pseudo-ale’atoire）によって、カードチャレンジ（英語では「card challenge」）ＣＣＨを生成する。疑似ランダムの決定によって、電子エンティティ２の中に記憶されたデータから計算して、認証されていない第三者にとって予測不能なＣＣＨカードチャレンジを取得することができる。しかしながら、認証された第三者にとっては、疑似ランダムの決定によって、カードチャレンジを計算して場合によっては事前にそれを生成することができる。

【００３４】

ここで、例えば、「GlobalPlatform Card Techinology - Secure Channel Protocol 03 - Card Specification v 2.2 Amendment D」（ｖ１．１）という文書の段落６．２．２

．１で定義されるカードチャレンジＣＣＨの疑似ランダムの決定を用いることとする。この例では、カードチャレンジＣＣＨは、シーケンスカウンタ（英語では「sequence counter」）と、起動コマンドＩＵを送信するアプリケーションのＩＤと、不揮発性メモリ６の中に記憶された静的暗号キーセットＫの暗号キーＫ－ＥＮＣと、に従って決定される。

【００３５】

そして、ステップＥ６において、プロセッサ４は、ここでは、不揮発性メモリ６の中に記憶された静的暗号キーセットＫの静的キーを用いて、セッションキーセットＳＫを生成する。プロセッサ４は、詳細には、このステップにおいて、例えば「GlobalPlatform Card Technology-Secure Channel Protocol 03 - Card Specification v2.2 Amendment D」（ｖ１．１）という文書の段落６．２．１における規定に従って、既に述べた暗号キーＫ－ＥＮＣに基づいて、ここではさらにホストチャレンジＨＣＨおよびカードチャレンジＣＣＨに基づいて、暗号化または解読セッションキー（cle’ de session de chiffrement ou de de’chiffrement）ＳＫ－ＥＮＣを生成する。

【００３６】

セキュアエレメント２は、したがって、場合によってはステップＥ４で生成されたカードチャレンジＣＣＨを、コマンドの送信側である電子機器に向けて送り返すことができる。ここで記載されるような疑似ランダムの決定によってカードチャレンジＣＣＨが取得される場合、カードチャレンジＣＣＨの送信は必要ない。なぜなら、コマンド送信側の電子機器は、疑似ランダムの同じ決定方法によってカードチャレンジＣＣＨを取得できるからである。

【００３７】

したがって、プロセッサ４は、インターフェイス１０上で、ホストの暗号文（cryptogramme d'ho^te）ＨＡＣが後に続く認証コマンドＥＡを受信する。このホストの暗号文ＨＡＣは、セッションキーセットのセッションキーＳ－ＭＡＣと、（上記に示された通り、起動コマンドＩＵと共に事前に送信される）ホストチャレンジＨＣＨと、（上記に示された通り、疑似ランダムの決定によってここで取得される）カードチャレンジＣＣＨと、を用いて、コマンドの送信側である電子機器において事前に決定されている。

【００３８】

例えば、起動コマンドＥＡは、「Global Platform Card Technology - Secure Channel Protocol 03 - Card Specification v2.2 Amendment D」（ｖ１．１）という文書の段落７．１．２、または「GlobalPlatform Card Specification v2.2」という文書の付録Ｄ．４．２で定義されているＥＸＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ（外部認証）タイプのコマンドである。

【００３９】

したがって、ステップＥ１０において、プロセッサは、コマンドの送信側である電子機器を認証するために、受信されたホストの暗号文ＨＡＣが期待される暗号文に正しく対応しているかを検証する。

【００４０】

対応しない場合、方法はステップＥ１２に進み、そこで、プロセッサ４は、セキュアチャネル（canal se’curise’）を確立せずに交換を終える。

【００４１】

反対に、受信されたホストの暗号文ＨＡＣが期待された暗号に実際に対応する場合、コマンドの送信側である電子機器とセキュアエレメント２との間にセキュアなチャネルが確立される。このセキュアなチャネルは、交換の機密性を保証するために使われるセッションキーＳＫ（特に暗号化または解読セッションキーＳＫ－ＥＮＣ）が、コマンドの送信側である電子機器およびセキュアエレメント２によってのみ知られている（そして例えばコマンドの送信側である電子機器が他のセキュアエレメントとセキュアなチャネルを確立することを望む場合は異なる）という事実をもって、多様化されている（図２の符号「ＤＩＶＥＲＳＩＦ」を参照）と認められる。

【００４２】

プロトコルＳＣＰ－０３の場合、通常の名前ＳＫ－ＥＮＣとＳＫ－ＭＡＣとＳＫ－ＲＭＡＣとの下で、３つの多様化されたキーが使われていることに気づくであろう。

【００４３】

したがって、ステップＥ１４において、プロセッサ４は、セキュアなチャネルを介して、ブロードキャストキーセットＢＫが付随する（さらに、ここで記載される例では、暗号化カウンタ（compteur de chiffrement）および認証コードチェーン値（valeur de chaînage de code de ve’rification）が付随する）変更コマンドＣＨＭを受信する。ここで、ＣＨＡＮＧＥ　ＭＯＤＥと名付けられた専用コマンドの形で、このような変更コマンドを導入することを提案する。

【００４４】

上記のように、セキュアなチャネルの確立をもって、コマンドに付随するデータ（特に、ここでは、例えば第２のセキュアチャネルの設定を可能にする付随データと共にあるブロードキャストキーＢＫ）は、暗号化または解読セッションキーＳＫ－ＥＮＣによって暗号化される。

【００４５】

そこで、ステップＥ１６において、プロセッサ４は、（上記で説明されている通りにステップＥ６で取得した）暗号化または解読セッションキーＳＫ－ＥＮＣを用いた（ここでは対称的な）解読の暗号アルゴリズム（algorithme cryptographique (ici syme’trique) de de’chiffrement）を用いてブロードキャストキーＢＫを解読する。用いられる暗号のアルゴリズムは、例えばＡＥＳタイプである。

【００４６】

そして、ステップＥ１８において、プロセッサ４は、ランダムアクセスメモリ８（または、変形例として不揮発性メモリ６）の専用領域の中のコンテキストをセーブする（図２にてＢＣＫ．ＵＰと記載されている）。特に、プロセッサ４は、（暗号化または解読セッションキーＳＫ－ＥＮＣである）セッションキーＳＫをランダムアクセスメモリ８の専用領域にセーブする。

【００４７】

セキュアチャネルのタイプがＳＣＰ０３であるここに記載されている例においては、プロセッサ４は、同様に、専用領域に、多様化されたセキュアチャネルに関連付けられた（そしてステップＥ１４において受信されたものとは別個の）暗号化カウンタ（英語で「encryption counter」）および認証コードチェーン値（英語では「ＭＡＣ chaining value」）をセーブする。

【００４８】

そして、ステップＥ２０において、プロセッサ４は、ブロードキャストキーＢＫがセッションキーＳＫの代わりに用いられる、ブロードキャストモードまたはマルチユーザモード（図２のＭＵＬＴＩＵ．を参照）へ変更する。さらに、ここで、ブロードキャストモードにおいて、ステップＥ１４で受信された暗号化カウンタおよびチェーン値を用いる。

【００４９】

特に、ブロードキャスト（またはマルチユーザ）動作モードにおいて、コマンド送信側である電子機器とセキュアエレメント２とは、（暗号化または解読セッションキーＳＫ－ＥＮＣの代わりに用いられる）暗号化または解読ブロードキャストキーＢＫ－ＥＮＣを用いて、暗号化によって機密性が保証されるセキュアなチャネルの中で交換することができる。

【００５０】

後に説明されるように、ブロードキャストキーが複数の（または膨大な数の）セキュアエレメントに宛てられたデータを処理する（特に暗号化する）ために用いられることをもって、この動作モードを、「ブロードキャスト」または「マルチユーザ」と名付ける。

【００５１】

そして、ステップＥ２２において、プロセッサ４は、データＤｉが付随するコマンドＣＭＤｉを受信する。既に示している通り、ステップＥ２０におけるブロードキャストモー

ド（またはマルチユーザモード）への変更をもって、現在、受信されたコマンドに付随するデータは、暗号化または解読ブロードキャストキーＢＫ－ＥＮＣによって暗号化されている。

【００５２】

こうして、ステップＥ２４において、プロセッサ４は、ステップＥ１４で受信した暗号化または解読ブロードキャストキーＢＫ－ＥＮＣを用いて、（ここでは対称的な）解読の暗号アルゴリズム（algorithme cryptographique (ici syme ’ trique) de de ’ chiffrement）の適用によって、データＤｉの解読に進む。

【００５３】

解読されたデータＤｉは、同様にして、ここでは不揮発性メモリ６の中にセーブされることによって、セキュアエレメント２において用いられることができる（ステップＥ２６）。以下に説明されるように、例えばデータＤｉが、遠隔サーバからセキュアエレメント２にロードされたアプリケーションオペレーティングシステムの少なくとも一部を表すことを提案する。しかしながら、変形例としてこれらのデータは、（オペレーティングシステムの一部でない）アプリケーション、暗号キーまたはオペレーティングシステムの外部のアプリケーションコンポーネントによって用いられるデータを表すことがある。

【００５４】

場合によっては、ステップＥ２２からＥ２６を繰り返すことによって、（例えば、図２に示されるように、ｉ＝１，…，Ｎであるｎ個のコマンドＣＭＤｉなどの）複数のコマンドＣＭＤｉを受信することができる。

【００５５】

ブロードキャストモード（またはマルチユーザモード）で実施すべき全てのコマンドが受信された場合、プロセッサ４は、例えばＣＨＡＮＧＥ　ＭＯＤＥタイプのコマンドなどの、多様化されたモードへ戻るための変更コマンドＣＨＭ（ステップＥ２８）を受信する。

【００５６】

実際には、同じ１つのコマンドで、プロセッサ４が多様化されたモードで動作する場合はブロードキャストモード（またはマルチユーザ）へ、プロセッサ４がブロードキャストモードで動作する場合は多様化されたモードへ変更できることを規定できる。変形例として、これらの２通りの変更をそれぞれ実現するために、２つの異なるコマンドを規定することができる。

【００５７】

ステップＥ３０において、このコマンドを受信すると、プロセッサ４は、（上記で説明したように、ステップＥ１８においてセッションキーがセーブされた）ランダムアクセスメモリ８の領域においてセッションキーＳＫを読み取り、ここでは同様に暗号化カウンタおよびチェーン値を読み取り、これらのセッションキーＳＫを用いて多様化されたモードへ変更する。このようにして、プロセッサ４は、ステップＥ２からＥ１０によって設定されたセキュアなチャネルを再び用いることができる。そして、場合によっては、多様化されたモードへの変更に続き、このような変更を再び後で実行することができないように、リストアデータ（donne ’ es de restauration）が無効化される（例えば消されるなど）ことを規定できる。

【００５８】

そして、ステップＥ３２において、場合によってはこのステップを複数回実行する間に、プロセッサ４は、ステップＥ２６においてインストールされた（installe ’ es）（つまりここでは不揮発性メモリ６の中に記憶された）データＤｉの検証ができる完全性検証（ve ’ rification d'inte ’ grite ’ ）コードＭＡＣが付随された認証（autorisation）コマンドＡＴＨＺを受信する。完全性検証コードＭＡＣの取得の例は、以下の通りである。

【００５９】

認証コマンドは、例えばＡＵＴＨＯＲＩＺＥ＿ＡＣＴＩＯＮという名の下で、ここで導入を提案する新しいコマンドである。

【００６０】
認証コマンドＡＴＨＺは、セキュアなチャネルの中の交換の一部を成し、このコマンドに付随するデータ（ここでは完全性検証コードＭＡＣ）は、暗号化または解読セッションキーＳＫ－ＥＮＣを用いて暗号化される。
【００６１】
そこで、ステップＥ３４において、プロセッサ４は、暗号化または解読セッションキーＳＫ－ＥＮＣを用いた（ここでは対称的な）解読の暗号アルゴリズムの適用によって、完全性検証コードＭＡＣを解読する。ここでの暗号アルゴリズムはＡＥＳタイプのアルゴリズムである。
【００６２】
そして、ステップＥ３６において、プロセッサ４は、解読された完全性検証コードＭＡＣを用いて、ステップＥ２６変更の実行中に不揮発性メモリ６の中に記憶されたデータＤｉの完全性を検証することができる。
【００６３】
ステップＥ３６の検証に失敗した場合、プロセッサ４は、データＤｉを用いず、例えば遠隔サーバなどのコマンド生成を担当する電子機器に、例えばエラーメッセージを送り返すことによって、ステップＥ３８のエラー処理を実施する。
【００６４】
ステップＥ３６の検証に成功した場合、ステップＥ４０において、プロセッサ４は、インターフェイス１０を介して、例えば正常動作メッセージ（message de bon fonctionnement）の送信などを指示する。そして、プロセッサ４は、動作中、ステップＥ２６で不揮発性メモリ６の中に記憶されたデータＤｉを用いるであろう。後に記載する実施例において、データＤｉによって表されるアプリケーションオペレーティングシステムの少なくともいくつかのパーツ（部分）（parties）は、プロセッサ４によって実行されるであろう。
【００６５】
図３および４は、これまでに記載された方法の２つの使用可能なコンテキスト（contextes）を表す。
【００６６】
これらの２つのコンテキストにおいて、セキュアな方法でセキュアエレメント２に、オペレーティングシステムのアプリケーションパーツＤＡＴＡＳＥＮＤまたは他のアプリケーションをインストールする（つまり不揮発性メモリ６の中にロードする）ことが所望される。セキュアエレメント２上の（つまり不揮発性メモリ６の中に記憶されている）主要なパーツＬＯＡＤＥＲは、例えばここでは送られたデータのロードを担当する。一実施形態において、送られたデータは、主要なパーツＬＯＡＤＥＲの展開なしにセキュアエレメント２によって用いられることができる（ロード後に主要なパーツＬＯＡＤＥＲの介入なしに実行することのできるスタンドアローンアプリケーションの場合）。他の実施形態において、主要なパーツＬＯＡＤＥＲは、ロードされたデータの展開を開始するためにさらに用いられることができる。
【００６７】
アプリケーションパーツＤＡＴＡＳＥＮＤは、デザイン情報システム（syste`me informatique de conception）３０で（au niveau de）入手可能（disponible）である。このデザイン情報システム３０は、例えばセキュアエレメント２の製造業者によって管理される。デザイン情報システム３０は、高いセキュリティレベルを示す。
【００６８】
アプリケーションパーツＤＡＴＡＳＥＮＤは、例えば、携帯電話のオペレータまたは製造業者によって管理されて、管理サーバ２０を介してセキュアエレメント２に送信されなければならない。セキュアエレメント２は、携帯電話のオペレータまたは製造業者に正確に関連付けられる。厳密には、セキュアエレメント２は、セキュアエレメント２を持つユーザ端末が、携帯電話のオペレータによって運用される少なくとも一つの携帯電話ネット

ワークにアクセスすることを可能にするデータを記憶する。

【００６９】

ユーザ端末は、簡単のため図３および４では言及されていない。しかしながら、管理サーバ２０とセキュアエレメント２との間のデータの交換は、（場合によっては上記携帯電話ネットワークと同様に）ユーザ端末の通信手段を用いることがわかる。

【００７０】

管理サーバ２０は、中レベルのセキュリティを有する。しかしながら、（例えばここではＥｔｈｅｒｎｅｔ（登録商標）タイプのワイヤードリンク（liaison filaire）などによって）管理サーバ２０に（セキュリティリンクを介して）リンクされ、それに関しては高レベルのセキュリティを示す、セキュリティモジュール２５が規定される。

【００７１】

セキュリティモジュール２５は、例えば（「Hardware Security Module」に対する）ＨＳＭタイプである。

【００７２】

図３の場合でも図４の場合と同様に、セキュリティモジュール２５は、セキュアエレメント２に関連付けられる（また前述したようにセキュアエレメント２の不揮発性メモリ６の中に記憶される）静的キーセットＫを記憶する。セキュリティモジュール２５は、管理サーバ２０によって管理される全てのセキュリティエレメントのために、固有の静的キーセットＫを記憶する（または、例えばセキュアエレメントのＩＤおよびマスターキーから導出して取得できる）ことに留意されたい。

【００７３】

図３および４で示されている通り、デザイン情報システム３０およびセキュアエレメント２は、ここでは多数のセキュアエレメントに共通で、セキュアエレメントにインストールされるアプリケーションパーツＤＡＴＡＳＥＮＤを暗号化するために使われる対称的なキーＫｏｓを記憶する。この共通キーＫｏｓは、セキュアエレメント２の製造業者によって管理され、セキュアエレメント２およびデザイン情報システム３０内に封じられる（reste confine’e）。

【００７４】

次に、図３の解決策に固有の特徴を説明する。

【００７５】

図３の実施例において、ここでは上述した暗号化または解読ブロードキャストキーＢＫ－ＥＮＣと、完全性検証コードを生成するよう設計されたブロードキャストキーＢＫ-ＭＡＣと、を有するブロードキャストキー（またはキャンペーンキー）セットＢＫをさらに記憶する。ブロードキャストキー（またはキャンペーンキー）ＢＫは、アプリケーションパーツＤＡＴＡＳＥＮＤを受信（つまり、実際はそれらのオペレーティングシステムを更新またはアプリケーションを更新）しなければならない全てのセキュアエレメントのために使われる。

【００７６】

したがって、デザイン情報システム３０は、管理サーバ２０に、
－暗号化または解読ブロードキャストキーＢＫ－ＥＮＣを用いて（ここでは対称的な）暗号化の暗号アルゴリズム（algorithme cryptographique (ici syme’trique) de chiffrement）の適用によって暗号化されたアプリケーションパーツＤＡＴＡＳＥＮＤと、
－ブロードキャストキーＢＫ－ＭＡＣおよびアプリケーションパーツＤＡＴＡＳＥＮＤに基づいて決定される、完全性検証コードＭＡＣと、
－共通キーＫｏｓを用いた（ここでは対称的な）暗号化の暗号アルゴリズムの適用によって暗号化されたブロードキャストキーＢＫ－ＥＮＣおよびＢＫ－ＭＡＣと、を送ることができる。

【００７７】

これらの要素（e’le’ments）は、（例えばセキュアエレメントのオペレーティングシステムの更新の場合などに）アプリケーションパーツＤＡＴＡＳＥＮＤを受信しなければ

ならない全てのセキュアエレメントに共通であることと、したがってデザイン情報システム３０は、更新すべきそれぞれのセキュアエレメントのためにアプリケーションパーツＤＡＴＡＳＥＮＤの暗号化されたバージョンを生成する必要がないことに留意されたい。

【００７８】

暗号化または解読セッションキーＳＫ－ＥＮＣを用いた（ここでは対称的な）暗号化の暗号アルゴリズムの適用によってデータを暗号化するために、管理サーバ２０は、セキュリティモジュール２５に暗号化されたブロードキャストキーＢＫ－ＥＮＣおよびＢＫ－ＭＡＣを送る。暗号化または解読セッションキーＳＫ－ＥＮＣは、（セキュリティモジュール２５およびセキュアエレメント２の不揮発性メモリ６の中に記憶される）特に静的キーセットＫの静的キーＫ－ＥＮＣに基づいて、（上記で説明したように）セキュリティモジュール２５とセキュアエレメント２とにおいて並行して取得される。

【００７９】

ブロードキャストキーＢＫ－ＥＮＣおよびＢＫ－ＭＡＣ並びに完全性検証コードＭＡＣのみが、多様化された方法で（つまり更新されるべきそれぞれのセキュアエレメントに関して暗号化されたバージョンを作成することにより）暗号化される。したがって、セキュリティモジュールでの処理動作は、（特にアプリケーションパーツＤＡＴＡＳＥＮＤ全体の暗号化されたバージョンが、更新されるべきそれぞれのセキュリティエレメントに関して生成されなければならない事態（situation）と比較して）限定される。

【００８０】

この実施例では、ブロードキャストキーＢＫ－ＥＮＣおよびＢＫ－ＭＡＣは、二重に暗号化されて（共通キーＫｏｓによって暗号化され、セッションキーＳＫ－ＥＮＣによって暗号化されて）送られることに留意されたい。

【００８１】

ブロードキャストキーＢＫ－ＥＮＣおよびＢＫ－ＭＡＣは、図２のステップＥ２からＥ１０に従ってセキュアリンクを確立した後、図２のステップＥ１４に従って管理サーバ２０からセキュアエレメント２に送られることができる。

【００８２】

ブロードキャストキーＢＫ－ＥＮＣおよびＢＫ－ＭＡＣは、まず（図２のステップＥ１６に示されているとおり）暗号化または解読セッションキーＳＫ－ＥＮＣを用いて、それからここでは（前述した通り不揮発性メモリ６の中に記憶される）共通キーＫｏｓを用いて、セキュアエレメント２において解読される。

【００８３】

そして、アプリケーションパーツＤＡＴＡＳＥＮＤは、セキュアエレメント２に管理サーバ２０から送られることができる（上述したように、アプリケーションパーツＤＡＴＡＳＥＮＤは、暗号化または解読ブロードキャストキーＢＫ－ＥＮＣを用いて暗号化される）。

【００８４】

セキュアエレメント２は、図２のステップＥ２２からＥ２６に従ってアプリケーションパーツＤＡＴＡＳＥＮＤを受信し、解読し、（不揮発性メモリ６の中に）記憶する（アプリケーションパーツＤＡＴＡＳＥＮＤは、場合によっては、ｉ＝１，…，Ｎである複数のデータブロックＤｉに割り当てられる）。

【００８５】

そして、図２のステップＥ３２からＥ３６に従って、セキュアエレメント２は、暗号化または解読セッションキーＳＫ－ＥＮＣによるセキュアチャネルを介して、管理サーバ２０から（ここでは対称的なキーＫｏｓによって暗号化された）完全性検証コードＭＡＣを受け取り、完全性検証コードＭＡＣおよびブロードキャストキーＢＫ－ＭＡＣを用いてアプリケーションパーツＤＡＴＡＳＥＮＤの完全性を検証する。

【００８６】

次に、図４の解決策に固有の特徴を説明する。

【００８７】

図４の実施例において、デザイン情報システム３０は、多数のセキュアエレメントの中に記憶され、これらのセキュアエレメントにインストールされたアプリケーションパーツＤＡＴＡＳＥＮＤの完全性を検証するために用いられる完全性共通キーK_{MAC}を記憶する。完全性共通キーK_{MAC}は、セキュアエレメント２の製造業者によって管理され、セキュアエレメント２およびデザイン情報システム３０内に封じられる。

【００８８】

したがってデザイン情報システム３０は、管理サーバ２０に、

共通キーＫｏｓを用いた（ここでは対称的な）暗号化の暗号アルゴリズムの適用によって暗号化されたアプリケーションパーツＤＡＴＡＳＥＮＤと、

完全性共通キーK_{MAC}およびアプリケーションパーツＤＡＴＡＳＥＮＤに基づいて決定された完全性検証コードＭＡＣと、を送ることができる。

【００８９】

管理サーバ２０に関連付けられたセキュリティモジュール２５は、それ自体に関しては、（静的キーセットＫと共に）暗号化または解読ブロードキャスト（またはキャンペーン）キーＢＫ－ＥＮＣを記憶する。

【００９０】

したがって、セキュリティモジュール２５は、図２のステップＥ２からＥ１０に従って、セキュアエレメント２と（静的キーＫ－ＥＮＣに基づいて生成された暗号化または解読セッションキーＳＫ－ＥＮＣを用いた暗号化によって）セキュアなチャネルを確立し、そして、図２のステップＥ１４に従って、このセキュアなチャネルを介してセキュアエレメント２が受信するための暗号化または解読ブロードキャストキーＢＫ－ＥＮＣを送ることができる。

【００９１】

そこで、管理サーバ２０は、図２のステップＥ２２からＥ２６に従って、（暗号化または解読ブロードキャストキーＢＫ－ＥＮＣを用いた暗号化を用いて）マルチユーザのセキュアなチャネルを介して暗号化されたアプリケーションパーツＤＡＴＡＳＥＮＤ（アプリケーションパーツＤＡＴＡＳＥＮＤは、場合によってはｉ＝１，…，Ｎである複数のデータブロックＤｉに分けられる）を送る。

【００９２】

ここで、暗号化または解読ブロードキャストキーＢＫ－ＥＮＣを用いた解読のアルゴリズムによる解読の後に取得されるデータＤｉは、共通キーＫｏｓを用いて暗号化されたアプリケーションパーツＤＡＴＡＳＥＮＤの少なくとも一部を表すことに留意されたい。したがって、ここで、プロセッサ２は、さらに共通キーＫｏｓを用いた解読のアルゴリズムの適用によってアプリケーションパーツＤＡＴＡＳＥＮＤを解読する。

【００９３】

そして、アプリケーションパーツＤＡＴＡＳＥＮＤは、不揮発性メモリ６の中に記憶される（これは図２のステップＥ２６に対応する）。

【００９４】

最後に、図２のステップＥ３２からＥ３６に従って、セキュアエレメント２は、暗号化または解読セッションキーＳＫ－ＥＮＣによるセキュアチャネルを介して管理サーバ２０から完全性検証コードＭＡＣを受信し、完全性検証コードＭＡＣおよび完全性共通キーK_{MAC}を用いてアプリケーションパーツＤＡＴＡＳＥＮＤの完全性を検証する。

【００９５】

図３および図４の実施例において、使用されている図２の各ステップは、プロセッサ２が主要なオペレーティングシステムＬＯＡＤＥＲの命令を実行した結果として実施されることに留意されたい。

【００９６】

さらに、上記の実施例において、暗号化または解読セッションキーＳＫ－ＥＮＣは、セキュアエレメント２と、セキュアエレメント２とセキュアなチャネルを確立しようとする電子機器（ここではセキュリティモジュール２５）と、の両方で記憶される静的キーＫ－

ＥＮＣから導出して取得される対称的なキーである。

【００９７】

しかしながら、また、変形例として、暗号化または解読セッションキーＳＫ－ＥＮＣは、例えば「Card Secure Channel Protocol ‘11’ Card Specification v2.2 - Amendment F (v1.0)」という文書において規定されるように、公開鍵（cle’ publique）に基づく鍵交換技術（technique de ne’gociation de cle’s）に従って、セキュアエレメント２では、特にセキュアエレメント２の中に記憶される秘密鍵（cle’ prive’e）K_{SE}から導出され、電子機器では、特に電子機器の中に記憶される他の秘密鍵K_{EXT}から導出されることにより、取得される対称的なキーであると規定できる。

【００９８】

図５は、セキュアエレメント２のオペレーティングシステムの更新の方法の例を示すフローチャートである。

【００９９】

この方法は、ステップＥ１００において、デザイン情報システム３０内で、セキュアエレメント２の不揮発性メモリ６の中にロードされるデータセットP_{SE}を準備することにより始まる。

【０１００】

データセットP_{SE}は、ここでは更新すべきオペレーティングシステムのアプリケーションパーツＤＡＴＡＳＥＮＤを有する。このため、データセットP_{SE}は、例えば、それぞれが、ブロードキャスト（またはキャンペーン）キーＢＫ－ＥＮＣによって暗号化された形のアプリケーションパーツＤＡＴＡＳＥＮＤの一部を有する、Ｎ個の書き込みコマンドＣＭＤｉから形成される。図２のステップＥ２８で言及されている通り、（付随する暗号キーのない）コマンドＣＨＭは、Ｎ個の書き込みコマンドＣＭＤｉのシーケンスの終わりに、さらに配置することができる。

【０１０１】

ブロードキャストキーＢＫ－ＥＮＣは、多数のセキュアエレメントのために用いられ、したがって準備されたデータは、それらのオペレーティングシステムの更新のために、（以下で説明するように）全てのセキュアエレメントに同じ形で送られることができる。

【０１０２】

ステップＥ１０２において、デザイン情報システム３０は、データセットP_{SE}を管理サーバ２０に送信する。

【０１０３】

ステップＥ１０４において、管理サーバ２０は、データセットP_{SE}を受信し、ここでは、ステップＥ１０６において、このデータセットP_{SE}を、セキュアエレメント２を有する（例えば携帯電話またはセルラホーンなどの）ユーザ端末１５にロードされるように意図された他のデータセットP_{MOB}と結合する。

【０１０４】

ステップＥ１０８において、管理サーバ２０は、（例えば、特に管理サーバ２０およびセキュアエレメント２に関連付けられた携帯電話ネットワークを用いて）ユーザ端末１５にデータセットP_{SE}およびP_{MOB}を送信する。

【０１０５】

ステップＥ１１０において、ユーザ端末１５は、データセットP_{SE}およびP_{MOB}を受信する。このため、例えば、ユーザ端末１５が、リッチ実行環境またはＲＥＥつまり「Rich Execution Environment」から、（例えば信頼されるオペレーティングシステムの実行の結果として設定される）高信頼実行環境またはＴＥＥつまり「Trusted Execution Environment」に変更する動作と、この高信頼実行環境において（例えば「midlet」タイプの）アプリケーションの実行の枠の中で受信されるデータセットP_{SE}およびP_{MOB}と、を規定することができる。

【０１０６】

ユーザ端末１５は、例えばユーザ端末１５のメモリにこれらのデータを記憶することに

より、ステップＥ１１２で受信したデータP_{SE}およびP_{MOB}からデータセットP_{SE}を抽出し、ステップＥ１１４で他のデータセットP_{MOB}を処理する。

【０１０７】

そして、ステップＥ１１６において、ユーザ端末１５は、管理サーバ２０に更新許可のリクエストＲＥＱを（例えば動作の後のタイミングで）送信する。ステップＥ１１８において、このリクエストＲＥＱは、管理サーバ２０によって受信される。

【０１０８】

そして、ステップＥ１２４において、管理サーバ２０は、認証データセットP_{AUT}を準備する。

【０１０９】

この認証データセットP_{AUT}は、例えば、セキュアエレメント２に固有に関連付けられた暗号キーによって暗号化されたブロードキャストキーＢＫ－ＥＮＣと、例えば、管理サーバ２０およびセキュアエレメント２のみが生成できるセッションキーＳＫ－ＥＮＣと、を有する。

【０１１０】

ここで、認証データセットP_{AUT}は、図２を参照して上記にて提示した、コマンドシーケンスの形ＩＵ、ＥＡ、ＣＨＭ、ＡＴＨＺで実現される。

【０１１１】

ステップＥ１２８において、管理サーバ２０は、ユーザ端末に認証データセットP_{AUT}を送る。

【０１１２】

ステップＥ１３０において、ユーザ端末１５は、認証データセットP_{AUT}を受信する。

【０１１３】

そして、ステップＥ１３２において、ユーザ端末１５は、ここでは認証データセットP_{AUT}のモード変更コマンドＣＨＭの直後にデータセットP_{SE}のコマンドを挿入することによって、（ステップＥ１１０で受信され、ステップＥ１１２で抽出される）データセットP_{SE}と認証データセットP_{AUT}とを結合することができる。

【０１１４】

詳細には、上記で説明したように、データセットP_{SE}のコマンドの中に含まれているデータは、（実際は多数のセキュアエレメントである）複数のセキュアエレメントによって共有されるブロードキャストキーＢＫ－ＥＮＣを用いて暗号化されており、したがって、これらのコマンドは、セキュアエレメント２をマルチユーザモードに切り換えた後で受信されなければならない。

【０１１５】

ステップＥ１３４において、ユーザ端末１５は、セキュアエレメント２に、ステップＥ１３２で（結合によって）準備したコマンドを送る。簡単のため、図５では、コマンドの連続した送信をただ１つのステップで示した。実際は、それぞれのステップは、ユーザ端末１５からセキュアエレメント２に別々に送られる。

【０１１６】

図２を参照しながら上記で説明した（ステップＥ１３６によって概略的に示される）ように、セキュアエレメント２は、コマンドのそれぞれを連続して受信して実行する。

【０１１７】

一旦全てのコマンドが実行されると、セキュアエレメント２は、図２のステップＥ４０にて上記で説明したように、状態情報ＳＴ（ステップＥ１３８）を送信する。

【０１１８】

ステップＥ１４０において、状態情報ＳＴは、ユーザ端末１５によって受信され、ステップＥ１４２において、管理サーバ２０に送られる。

【０１１９】

ステップＥ１４４において、管理サーバ２０は、状態情報ＳＴを受信し、例えば、状態情報ＳＴが、セキュアエレメント２がオペレーティングシステムを正しく更新したことを

承認する場合は、セキュアエレメント２を備えたユーザ端末が携帯電話ネットワークへアクセスすることを認証し、状態情報ＳＴが正しい更新を承認しない場合は、（例えば、ロードの再試行、対象のユーザ端末のネットワークへのアクセス禁止などの）他のアクションを実行することによって、状態情報ＳＴに従って処理動作を実行する。

【０１２０】

認証データセットP_{AUT}は、例えばデータセットP_{SE}およびP_{MOB}によって定義された動作の活性化を可能にする。

【０１２１】

このようにして、上記にて説明される方法は、動作の活性化の際に交換を最小にすることを可能にする。詳細には、ステップＥ１００からＥ１１４までにデータセットP_{SE}およびP_{MOB}を事前にロードすることにより、活性化の際に送られるデータは、認証データセットP_{AUT}のみである。

【図１】

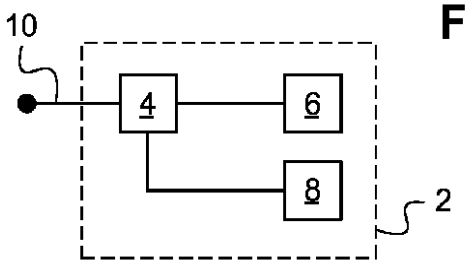


Fig.1

【図２】

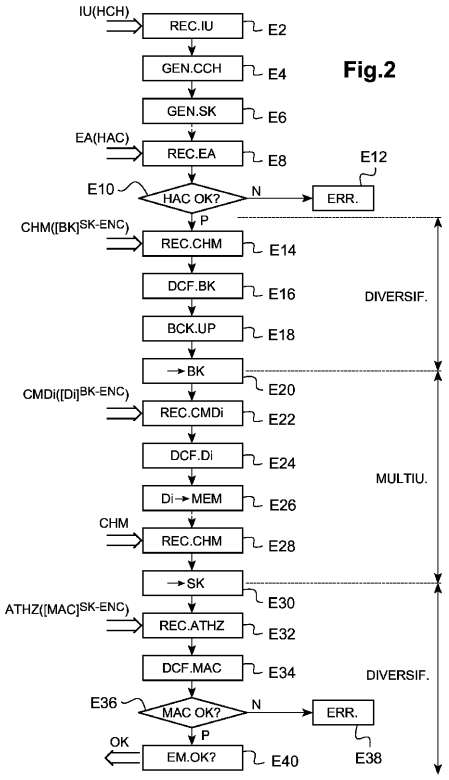
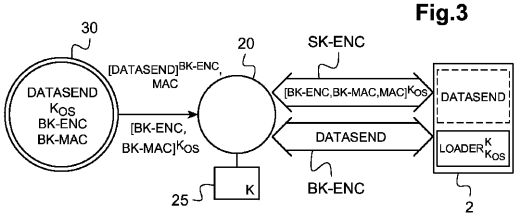


Fig.2

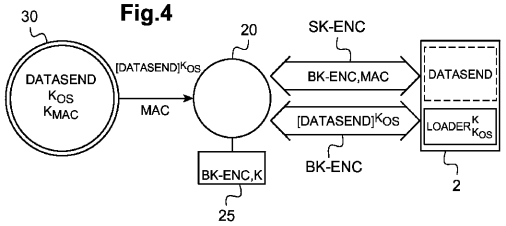
【図３】

Fig.3



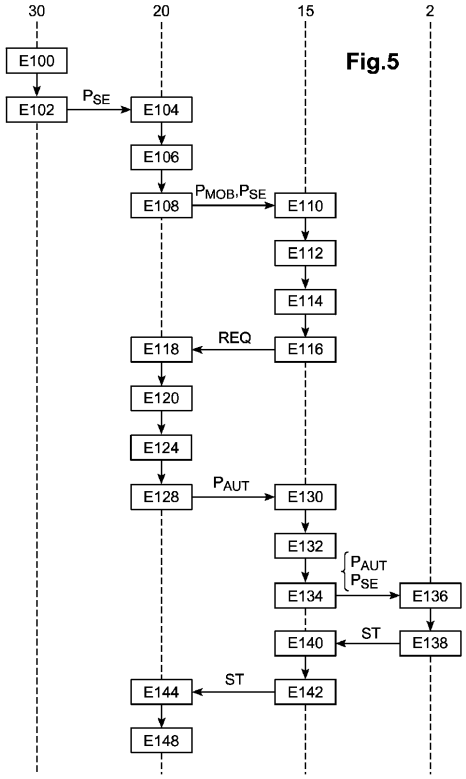
【図４】

Fig.4



【図５】

Fig.5



フロントページの続き

(72)発明者　ジャン－フィリップ　バリエール
フランス国，９２７００　コロンブ，リュ　デスティエンヌ　ドルヴ　４２０，オベルトゥル　テクノロジ
(72)発明者　フロリアン　ガルド
フランス国，９２７００　コロンブ，リュ　デスティエンヌ　ドルヴ　４２０，オベルトゥル　テクノロジ
(72)発明者　エマニュエル　ドッタクス
フランス国，９２７００　コロンブ，リュ　デスティエンヌ　ドルヴ　４２０，オベルトゥル　テクノロジ
(72)発明者　フランク　ロンドピエール
フランス国，９２７００　コロンブ，リュ　デスティエンヌ　ドルヴ　４２０，オベルトゥル　テクノロジ
(72)発明者　ミケーレ　サルトーリ
フランス国，９２７００　コロンブ，リュ　デスティエンヌ　ドルヴ　４２０，オベルトゥル　テクノロジ

審査官　中里　裕正

(56)参考文献　特開２００５－２４４５９４（ＪＰ，Ａ）
特表２００９－５１３０８９（ＪＰ，Ａ）
特表２０１５－５３２５６５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／６０
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／６０
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／３２