(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2015-133122
(P2015-133122A)
(43)公開日　平成27年7月23日(2015.7.23)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/44	***(2013.01)***	G06F	21/44	
G06K 7/10	***(2006.01)***	G06K	7/10　２００	

審査請求 有　請求項の数 7　ＯＬ　（全 7 頁）

(21)出願番号　特願2015-18547(P2015-18547)
(22)出願日　平成27年2月2日(2015.2.2)
(62)分割の表示　特願2013-542475(P2013-542475)の分割
原出願日　平成23年12月2日(2011.12.2)
(31)優先権主張番号　10306359.0
(32)優先日　平成22年12月6日(2010.12.6)
(33)優先権主張国　欧州特許庁(EP)

(71)出願人　309014746
ジェムアルト　エスアー
フランス　エフ－９２１９０　ムードン　リュ　ドゥ　ラ　ヴェルリー　６
(74)代理人　100086368
弁理士　萩原　誠
(72)発明者　ファブリス　ヴェルニュ
フランス　フュヴォ　Ｆ－１３７１０　シュマン　ドゥ　メルイユ
(72)発明者　フレデリック　ファリア
フランス　ラ　シオタ　セデックス　Ｆ－１３７０５　ＢＰ９０　サービスブルベ　ジェムアルト　エスアー

最終頁に続く

(54)【発明の名称】端末に内蔵された保全素子を個人化する方法

(57)【要約】　（修正有）
【課題】第１の端末に含まれる第１の保全素子にサービスを追加して個人化する方法を提供する。
【解決手段】第１の端末のユーザに第１の保全素子のフォームファクタとは異なるフォームファクタを持った取り外し可能な保全素子を与え、第１の端末内で、又は第１の端末を介して、第１の保全素子と取り外し可能な保全素子とをリンクさせ、第１の保全素子と取り外し可能な保全素子との間における証明書認証と非対称暗号化とにより安全を担保しつつ、取り外し可能な保全素子に内蔵されたデータで第１の保全素子を安全に個人化する。
【選択図】なし

【特許請求の範囲】
【請求項１】
第１の端末に含まれる第１の保全素子にサービスを追加して個人化する方法であって、前記方法は、
－前記第１の端末のユーザに前記第１の保全素子のフォームファクタとは異なるフォームファクタを持った取り外し可能な保全素子を与え；
－前記第１の端末内で、又は前記第１の端末を介して、前記第１の保全素子と前記取り外し可能な保全素子とをリンクさせ、
－前記第１の保全素子と前記取り外し可能な保全素子との間における証明書認証と非対称暗号化とにより安全を担保しつつ、前記取り外し可能な保全素子に内蔵されたデータで前記第１の保全素子を安全に個人化する；ことからなる方法。
【請求項２】
前記第１の保全素子が、埋設型ＵＩＣＣ（ｅ－ＵＩＣＣ）である請求項１に記載の方法。
【請求項３】
前記取り外し可能な保全素子が、ＳＩＭカードである請求項１に記載の方法。
【請求項４】
前記取り外し可能な保全素子が、ドングルである請求項１に記載の方法。
【請求項５】
前記ドングルが、前記第１の保全素子へ転送されるアプリケーション又は認証情報を内蔵している請求項４に記載の方法。
【請求項６】
前記第１の保全素子と前記取り外し可能な保全素子とのリンクが、前記ドングルが挿入されるコンピュータによって実現される請求項４又は５に記載の方法。
【請求項７】
前記取り外し可能な保全素子が、銀行カードである請求項１に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、端末に内蔵された保全素子（ｓｅｃｕｒｅ　ｅｌｅｍｅｎｔ）を個人化する方法に関する。
【０００２】
電気通信の分野において、保全素子として典型的なのは、ＳＩＭアプリケーションが組み込まれたＵＩＣＣ（汎用集積回路カード）のような素子である。この保全素子は例えば携帯電話などの端末内に、固定されて、又は固定されずに組み込まれている。端末がＭ２Ｍ（マシン・ツー・マシン）アプリケーション用の、他の装置と通信する装置である場合もある。
【０００３】
ＵＩＣＣは、スマートカードの形をとりうるが、［特許文献１］に記載されているパッケージチップや、その他いかなる形をとるものであってもよい。ＵＩＣＣは、例えばＧＳＭ（登録商標）及びＵＭＴＳネットワークにおける携帯端末内で用いられうる。ＵＩＣＣは、ネットワーク認証、及びあらゆる種類の個人データの整合性と安全性を保証するものである。
【０００４】
ＵＩＣＣは、ＧＳＭネットワークでは主にＳＩＭアプリケーションを内蔵し、ＵＭＴＳネットワークではＵＳＩＭアプリケーションを内蔵している。
ＵＩＣＣにはその他複数のアプリケーションを内蔵させることができる。そうすると１つのスマートカードで、ＧＳＭ及びＵＭＴＳネットワークの双方にアクセスしたり、また電話帳及びその他のアプリケーションの格納領域を提供したりすることが可能となる。
【０００５】

また対応の携帯端末では、ＵＳＩＭアプリケーションでＧＳＭネットワークにアクセスしたり、ＳＩＭアプリケーションでＵＭＴＳネットワークにアクセスしたりすることもできる。

【０００６】

ＬＴＥ（登録商標）など、ＵＭＴＳリリース５以降のネットワークでは、ＩＭＳ（ＩＰマルチメディアサブシステム）におけるサービスに、新たなアプリケーション、即ちＩＰマルチメディアサービスアイデンティティモジュール（ＩＳＩＭ）が必要である。電話帳は別個のアプリケーションであり、いずれの加入者情報モジュールにも属さない。

【０００７】

ＵＩＣＣは、ＣＤＭＡネットワークでは、３ＧＰＰ　ＵＳＩＭ及びＳＩＭアプリケーションに加えて、ＣＳＩＭアプリケーションを内蔵している。これら３つの特徴を全て含むカードは、リムーバブルユーザアイデンティティカード、即ちＲ－ＵＩＭと呼ばれる。つまりＲ－ＵＩＭカードは、ＣＤＭＡ、ＧＳＭ、ＵＭＴＳハンドセットのいずれにも挿入でき、いずれにおいても機能するのである。

【０００８】

２Ｇネットワークにおいては、ＳＩＭカードとＳＩＭアプリケーションは一体であったため、“ＳＩＭカード”は、この物理的なカード、又はＳＩＭアプリケーションを有するあらゆる物理的なカードを意味していた。

ＵＩＣＣスマートカードは、ＣＰＵ、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ、及び入出力回路からなる。初期バージョンのスマートカードは、完全にフルサイズ（８５×５４ｍｍ，ＩＳＯ／ＩＥＣ　７８１０　ＩＤ－１）であった。

【０００９】

カードの差し込み口が標準化されているので、加入者は自分のワイヤレスアカウントや電話番号を、あるハンドセットから他のハンドセットへ簡単に移すことができる。これによって加入者の電話帳やテキストメッセージも移される。同様に加入者は、通常、自分の既存のハンドセットに新たなキャリアのＵＩＣＣカードを挿入することでキャリアを変更することもできる。しかしこれは、常に可能であるとは限らない。なぜなら、自社の販売する電話にＳＩＭロックをかけて（例、アメリカにおいてなど）、競合キャリアのカードが使用されないようにしているキャリアもあるからである。

【００１０】

ＥＴＳＩフレームワークとＧｌｏｂａｌ　Ｐｌａｔｆｏｒｍのアプリケーション管理フレームワークは統合され、ＵＩＣＣ仕様に一本化された。

ＵＩＣＣは３ＧＰＰ及びＥＴＳＩによって標準化された。

ＵＩＣＣは通常、例えばユーザが自分の携帯端末を変更したいときなどに、携帯端末から取り出すことができる。ユーザは、新たな端末に自分のＵＩＣＣを挿入して、それまで通り自分のアプリケーション、連絡先、認証情報（ネットワークオペレータ）にアクセスすることができる。

【００１１】

また、ＵＩＣＣを端末専用のものにする目的で、ＵＩＣＣを端末内にはんだ付け又は溶接することも周知である。これはＭ２Ｍ（マシン・ツー・マシン）アプリケーションにおいて行われている。上記の目的は、ＳＩＭ又はＵＳＩＭのアプリケーション及びファイルを内蔵するチップ（保全素子）を、端末に内蔵させることによっても達成できる。このチップは、例えば端末又は装置のマザーボードにはんだ付けされ、ｅ－ＵＩＣＣとなる。

【００１２】

また、遠隔端末内にあって、又は装置の奥深くに組み込まれていて、装置と完全に一体化しているわけではないが、元来取り外し用ではないために取り外しが困難なＵＩＣＣにも、本発明を同様に適用することができる。

【００１３】

ＵＩＣＣの特別なフォームファクタ（例えば非常に小さいので取り扱いが困難であるなど）も、そのＵＩＣＣを、実質的に端末に組み込まれているものと見なす理由になりうる

。同様のことは、開放が想定されていない装置内にＵＩＣＣが組み込まれている場合についてもいえる。
【００１４】
以下の記載では、ＵＩＣＣと同じアプリケーションを内蔵する、又は内蔵するよう設計されている、溶接されたＵＩＣＣ又はチップを総称して、（取り外し可能なＵＩＣＣ又は取り外し可能な保全素子に対し、）埋設型ＵＩＣＣ又は埋設型保全素子と呼ぶ。取り外し困難なＵＩＣＣ又は保全素子もこれに相当する。
【先行技術文献】
【特許文献】
【００１５】
【特許文献１】ＰＣＴ／ＳＥ２００８／０５０３８０
【発明の概要】
【発明が解決しようとする課題】
【００１６】
本発明は、ある保全素子を、別の保全素子を用いて、発行後（ｐｏｓｔ－ｉｓｓｕａｎｃｅ）に個人化することに関する。
保全素子を安全に個人化することは、保全素子に関するサービスの工業化及び流通における重大なステップである。
本発明は、このステップを、工場で行なうのではなく、ユーザに自身のニーズに応じて行なわせる、ということを提案する。
【００１７】
認証情報をある保全素子から別の保全素子に完全に移植することは、これまでできなかった。今まで移植とは、元の保全素子を、部分的に認証情報を移植してある新たな保全素子に取り替えることを指していた。
本発明は、ある保全素子から別の保全素子へ、認証情報を移植する方法を提案する。
【００１８】
本発明は、埋設型ＵＩＣＣへのデータ転送により、エンドユーザが埋設型保全素子（埋設型ＵＩＣＣ）の個人化を発行後に行なえるようにすることも目的としている。
例えば埋設型ＵＩＣＣに、銀行アプリケーションなどの新たなアプリケーションを転送することがこれにあたる。
【００１９】
埋設型ＵＩＣＣを個人化する場合について、本発明は第１の端末に内蔵された第１の保全素子にサービスを追加して個人化する方法を提案する。この方法は：
－第１の端末のユーザに第２の保全素子を与え；
－第１の端末内で、又は第１の端末を介して、第１及び第２の保全素子をリンクさせ；
－保全素子間における証明書認証と非対称暗号化とにより安全を担保しつつ、第２の保全素子に内蔵されたデータで第１の保全素子を安全に個人化する；
ことからなる。
【００２０】
第１の保全素子が第１の端末に内蔵されていて、第１の保全素子に内蔵された認証情報を第２の保全素子に転送する場合において、認証情報の転送方法は：
－第１の端末内で、又は第１の端末を介して、第１及び第２の保全素子をリンクさせ；
－保全素子間における証明書認証と非対称暗号化とにより安全を担保しつつ、第１の保全素子から第２の保全素子へ認証情報を安全に転送する；
ことからなる。
【００２１】
第１及び第２の保全素子は、取り外し可能なものでも、取り外しできないもの（埋設型ＵＩＣＣ）でもよい。
第２の保全素子が取り外し可能な場合、そのフォームファクタには例えばＳＩＭカードやドングルなどがありうる。

【００２２】
第２の保全素子は、第１の保全素子と無線接続を有する、いわゆる「スマートバッジ」に内蔵されている場合もある。また、携帯端末内に、取り外しできない形で（埋設型ＵＩＣＣ、即ちｅ－ＵＩＣＣとして）内蔵されている場合もありうる。
個人化は、いかなるネットワークにもアクセスできない公共空間でも、エンドユーザなど誰にでも、エンドユーザの家など、どこであっても、いかなる接続の制約もなく行なうことができる。
【００２３】
例えば銀行アプリケーションの認証情報（ＩＭＳＩ、Ｋｉ）を、携帯電話などの携帯端末から別の端末に転送することが、この個人化にあたる。
上記の例では、個人化のプロセスは例えば以下のようになる：
－ユーザが、携帯端末などに含まれる第１の保全素子を個人化しようと、自分の銀行又は移動体通信事業者の店舗へ行き、ドングルの形の第２の保全素子を受け取る。
【００２４】
このドングルは、第１の保全素子に転送されるべきアプリケーション又は認証情報を内蔵している。ドングルがユーザに郵便で送られることもありうる。
－家に帰ると、ユーザはこのドングルを自分のコンピュータに挿入し、このコンピュータに自分の携帯電話を接続する。
コンピュータと携帯電話との間の接続は、無線（Ｗｉｆｉ又は直通Ｗｉｆｉ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＮＦＣ、・・・）でも有線でもよい。
【００２５】
コンピュータ又はドングルに内蔵されたアプリケーションによって、第１の保全素子に書き込まれるべきアプリケーション又は認証情報が、第１の保全素子に転送される。
－アプリケーション又は認証情報は、転送されると、第１の保全素子内で例えば電子バンキングなどに使用できるようになる。
【００２６】
本発明は、例えばＰＣなどの端末に埋設された保全素子の個人化にも適用できる。第２の保全素子をＰＣにつなぐだけで、個人化が始まる。
個人化が1対１の通信で行なわれることを確実にするため、証明書認証及び非対称暗号化が用いられる。安全性は（あらゆるフォームファクタの）第２の保全素子と、２つの保全素子間での認証を可能にするＰＫＩスキームの使用とにかかっている。
【００２７】
個人化は、個人化されるべき保全素子の発行後に行なわれる。これは特に、エンドユーザがすでに自分の保全素子、例えば携帯電話内のスマートカード、銀行カード、ＰＣ内の保全素子、又はその他あらゆるデバイスでありうる保全素子を、有している場合に都合が良い。
【００２８】
ユーザが認証情報を、新品の保全素子に転送しなければならない／転送したいとき、既存の保全素子から、これに内蔵されている認証情報（ＭＮＯへの加入者情報、ＩＭＳＩ、ＫＩを含むＳＩＭアプリケーション全体、電子財布の内容・・・）を、新たな保全素子に転送することができる。
【００２９】
これは実用の場面で安全に行なうことができ、この際ユーザは両方の保全素子を物理的に保持していればよい。
これは、エンドユーザが既存の保全素子に新しくサービスを追加したいときに、このサービスがいかなるサービスプロバイダによるものであっても、適用できる。
エンドユーザは、インターネットに接続したり、店舗へ出向いたりしなくとも、第１の保全素子を個人化できる保全素子を入手できる。
【００３０】
本発明は、発行後に個人化された保全素子の更新を可能にする。またこれは、個人化さ

れた保全素子の更新についても適用できる。

本発明は、工場での個人化にかかるコストを削減し、保全素子の発行後における安全な個人化を可能にするものである。エンドユーザは、保全素子を個人化／更新するために、サービスプロバイダの店舗に出向いたり、インターネットに接続したりする必要はない。さらに安全性は、２つの保全素子による1対１の通信における個人化によって保証される。またこれは、非接続プロセスにより簡潔なものとなっており、ウイルスの脅威にもさらされない。

フロントページの続き

(72)発明者　フランク　イムーシャ
フランス　オリオール　Ｆ－１３３９０　レ　ジピエール－カルティエ　ポン　ドゥ　ジュ