

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5883023号
(P5883023)

(45) 発行日 平成28年3月9日(2016.3.9)

(24) 登録日 平成28年2月12日(2016.2.12)

(51) Int. Cl.		F I			
HO4W 8/20	(2009.01)	HO4W 8/20			
HO4W 84/10	(2009.01)	HO4W 84/10	110		
HO4M 1/00	(2006.01)	HO4M 1/00		R	

請求項の数 5 (全 6 頁)

(21) 出願番号	特願2013-542477 (P2013-542477)	(73) 特許権者	309014746
(86) (22) 出願日	平成23年12月2日(2011.12.2)		ジェムアルト エスアー
(65) 公表番号	特表2014-500678 (P2014-500678A)		フランス エフ-92190 ムードン
(43) 公表日	平成26年1月9日(2014.1.9)		リュ ドゥ ラ ヴェルリー 6
(86) 国際出願番号	PCT/EP2011/071674	(74) 代理人	100086368
(87) 国際公開番号	W02012/076424		弁理士 萩原 誠
(87) 国際公開日	平成24年6月14日(2012.6.14)	(72) 発明者	ポール ブラッドリー
審査請求日	平成25年7月8日(2013.7.8)		アメリカ合衆国 TX78759 テキサ
(31) 優先権主張番号	10306359.0		ス オースティン ストーンレイクブルバ
(32) 優先日	平成22年12月6日(2010.12.6)		ード 9801
(33) 優先権主張国	欧州特許庁 (EP)		審査官 石田 紀之

最終頁に続く

(54) 【発明の名称】 加入者情報を端末に埋設されたUICCにダウンロードする方法

(57) 【特許請求の範囲】

【請求項1】

加入者情報を、端末に埋設されている汎用ICカード(UICC)内にダウンロードする方法であって、前記方法は：

ICカード固有番号(ICCID)が前記端末に転送され；

前記ICCIDがIPリンクを介して前記端末から保全倉庫へ送信され；

前記保全倉庫が保持している複数の加入者情報の中から前記ICCIDに対応する加入者情報を選択し；

選択された前記加入者情報が前記IPリンクを介して前記保全倉庫から前記端末へ送信され；

前記加入者情報が前記端末に埋設されている前記UICCへ格納される、ことからなる方法。

【請求項2】

前記ICCIDは、ICCIDの秘密活性コードとともに前記端末に転送され、

前記保全倉庫は、前記加入者情報を前記端末へ送信する前に、前記ICCIDと前記秘密活性コードとのペアリングを照合する、請求項1に記載の方法。

【請求項3】

前記ICCIDがトークン中に含まれ、NFCを介して前記トークンから前記端末へ転送される、請求項1又は2に記載の方法。

【請求項4】

前記トークンは、NFCタグである請求項3に記載の方法。

【請求項5】

前記ICCIDが、前記端末によって撮影可能なバーコードの形で内包されている、請求項1乃至4のいずれかに記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、例えば携帯端末（携帯電話）又は（M2M（マシン・ツー・マシン）アプリケーション用の）装置などの端末に埋設されたUICC（汎用集積回路カード）に、加入者情報をダウンロードする方法に関する。

10

【背景技術】

【0002】

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。

【0003】

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。

20

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。

【0004】

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。

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。

30

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。

【0005】

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。

【0006】

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。

40

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。すぐに、電話の小型化競争によって、より小型のカードが求められるようになった。

【0007】

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

50

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。

【0008】

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。

10

【0009】

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(secure element))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。

【先行技術文献】

20

【特許文献】

【0010】

【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】

【0011】

本発明は、上記のような、はんだ付けされたUICC(e-UICC)や、UICC中のチップと同じアプリケーションを内蔵するチップに適用される。

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

30

【0012】

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。

【0013】

以下の記述では、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。

40

【0014】

本発明は(取り外しできない)埋設型UICCに関する。

本発明の第1の実施形態は、埋設型(U)SIMアプリケーション(又は全般的にUICCアプリケーション一式)を選択し、上記のような埋設型の安全なUICCを内蔵する端末にダウンロードするために、NFCを用いる方法に関する。この端末は、例えば携帯電話でありうる。

【0015】

本発明の第2の実施形態は、バーコードを撮影可能な端末にダウンロードする、(U)SIMアプリケーション(又は全般的にUICCアプリケーション一式)を識別するため

50

に、バーコードを用いる方法に関する。

導入部で既に説明したように、将来、装置内にソフトSIM又は埋設型SIMが設けられるようになれば、装置にダウンロードするべき適切な加入者情報を選択することが必要となるだろう。装置にダウンロードするべき加入者情報を識別する、使い捨てNFCタグを提供することで、ユーザ経験が向上しうる。

【0016】

言い換えれば、加入者情報が、現在のUICCのような安全で取り外し可能な形態のものではなく、“ソフトSIM”又は、はんだ付けされた保全素子(VQFN8/DFN8保全素子)に格納される時代になれば、装置にダウンロードするべき正しい加入者情報を選択する必要が生じるのである。

10

【課題を解決するための手段】

【0017】

本発明は、加入者情報を、端末に埋設されたUICCにダウンロードする方法を提示する。この方法は：

- ICCIDを端末に転送し；
- ICCIDを、IPリンクを介して保全倉庫(secure vault)へ送信し；
- 保全倉庫から、ICCIDに対応する加入者情報を選択し；
- 加入者情報を、IPリンクを介して端末へ送信し；
- 加入者情報を、端末へ格納する；

ことからなる。

20

【0018】

ICCIDは、好ましくはICCIDの秘密活性コードと共に転送され、保全倉庫は、加入者情報を端末に送信する前に、ICCIDと秘密活性コードとのペアリングを照合する。

【発明を実施するための形態】

【0019】

第1の実施形態では、ICCIDはトークン中に内蔵され、NFCを介して端末に転送される。

このトークンは、NFCタグでありうる。

第2の実施形態では、ICCIDは、端末によって撮影可能なバーコードに内蔵されている。

30

【0020】

本発明の第1の実施例では、NFC端末が用いられる。

加入者情報のダウンロードは、ユーザインタフェース又は操作により行なわれる。しかし、ロックされていない端末については、(MNOが従来の手順で処理するために)今日の物理的なSIMカードのように、分配用の物理的なタグ/NFCカードを有する必要がある。

【0021】

このタグは(プロビジョニングシステムに通知されている、個々のICCIDに関連付けられた秘密活性コードを伴う)ICCIDへの参照情報を内蔵する。

40

プロビジョニングシステムに、正しい秘密活性コードと共にICCIDが与えられると、遠隔プロビジョニングサービスは、埋設型保全素子に対し、正しいソフトウェア(SIMプロファイル、加入者情報)の安全な転送を開始することができる。

【0022】

例えば、もしユーザが活性前の装置Xを有しており、オペレータAから加入者情報を買おうとする場合には、以下のようなフローとなる：

- 装置XがNFCトークンYに接触させられる。トークンはICCID及び好ましくはICCIDの活性コードを内蔵している。装置Xは、トークンYからICCID及び(好ましくは)固有のICCIDの秘密活性コード(このコードは、前述のプロビジョニングセンタに対する、しらみつぶしなICCIDの推測試行を防ぐ)を読み取る。

50

【0023】

- 装置XはこのICCIDをIPリンクを介して保全倉庫へ送信する。この保全倉庫はICCID / 秘密活性コードのペアリングを照合し、有効であれば、関連する埋設型UICC (SIMアプリケーション、USIMアプリケーション、ISIMアプリケーション、CSIMアプリケーション、その他のネットワーク認証アプリケーション、及びSIMアプリケーションツールキットアプリケーション、及び特定のMNOに関連するオペレーティングシステムカスタマイゼーション / メカニズムを含む) の個人化スクリプト全体と、IMS I、K、Op c、IMPUなどの関連する加入者情報と、アルゴリズム定数とを安全にパッケージ化し、暗号化し、これに署名する。

【0024】

前記保全倉庫は、ICCIDレンジにより、又は代替的には、前記システムに与えられるプロファイルコードにより、プロファイルの内容を通知される。

- 前記保全倉庫は装置Xの埋設型保全素子用に暗号化された(また、アンチリプレイのカウンタ機構を含んだ)上記個人化スクリプトを、IPリンクを介して装置Xに送信する。

【0025】

- 装置X (埋設型保全素子を含む) は、個人化スクリプトを復号して実行し、埋設型保全素子が加入者情報を使用できるように設定する。

これで装置Xは、加入者情報を用いて無線ネットワークにアクセスすることができる。

【0026】

第2の実施例においては、ICCIDは端末により撮影可能なバーコードに内蔵されている。バーコードを写真にとった後、端末は保全倉庫にこれを送信する。保全倉庫は、受信したバーコードを予め登録されているバーコードと比較するか、ICCIDを取り出すためにバーコードを復号する。その後は、上記と同じプロセスが実行される。

【0027】

本発明は、加入者情報および各種プロファイルを遠隔的に選択できるようにすることで、使いやすさを大いに向上させるものである。

10

20

フロントページの続き

- (56)参考文献 国際公開第2009/149788(WO, A2)
国際公開第2009/141035(WO, A1)
国際公開第2010/138592(WO, A2)
特開2006-107316(JP, A)
特開2005-323128(JP, A)
特表2011-525311(JP, A)
特表2012-528534(JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F	9/06
H04B	7/24 - 7/26
H04M	1/00
H04W	4/00 - 99/00