

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第5781167号  
(P5781167)

(45) 発行日 平成27年9月16日 (2015.9.16)

(24) 登録日 平成27年7月24日 (2015.7.24)

(51) Int. Cl. F I  
**HO 4 M 1/675 (2006.01)** HO 4 M 1/675  
**HO 4 W 12/04 (2009.01)** HO 4 W 12/04  
**HO 4 W 8/20 (2009.01)** HO 4 W 8/20

請求項の数 2 (全 6 頁)

<p>(21) 出願番号 特願2013-542492 (P2013-542492)</p> <p>(86) (22) 出願日 平成23年12月5日 (2011.12.5)</p> <p>(65) 公表番号 特表2014-506033 (P2014-506033A)</p> <p>(43) 公表日 平成26年3月6日 (2014.3.6)</p> <p>(86) 国際出願番号 PCT/EP2011/071737</p> <p>(87) 国際公開番号 W02012/076464</p> <p>(87) 国際公開日 平成24年6月14日 (2012.6.14)</p> <p>審査請求日 平成25年7月8日 (2013.7.8)</p> <p>(31) 優先権主張番号 10306359.0</p> <p>(32) 優先日 平成22年12月6日 (2010.12.6)</p> <p>(33) 優先権主張国 欧州特許庁 (EP)</p> <p>前置審査</p>	<p>(73) 特許権者 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</p> <p>(74) 代理人 100086368                  弁理士 萩原 誠</p> <p>(72) 発明者 ポール ブラッドリー                  アメリカ合衆国 TX78759 テキサ                  ス オースティン ストーンレイクブルバ                  ード 9801</p> <p>審査官 永田 義仁</p>
--	---

最終頁に続く

(54) 【発明の名称】 端末間で加入者情報を転送する方法

(57) 【特許請求の範囲】

【請求項 1】

第1の汎用集積回路カード (UICC1) を備えた第1の端末から第2の汎用集積回路カード (UICC2) を備えた第2の端末へ、前記第1の汎用集積回路カード (UICC1) に格納された識別子 (IMSI-1) を含む加入者情報とユーザデータとを安全に転送する方法であって、前記方法は：

i) 前記第2の端末の識別子 (IMEI-2) を前記第1の端末へ送信するステップと；

ii) 前記第1の端末から前記第2の端末の加入者情報インストール用公開鍵を格納している保全倉庫へ、前記第2の端末の前記識別子 (IMEI-2) と前記第1の汎用集積回路カード (UICC-1) の前記識別子 (IMSI-1) とを送信するステップと；

iii) 前記保全倉庫から前記第1の端末へ、前記加入者情報インストール用公開鍵を送信するステップと；

iv) 前記第1の汎用集積回路カード (UICC1) において、前記加入者情報と前記ユーザデータとを、前記加入者情報インストール用公開鍵を用いてパッケージ化及び暗号化するステップと；

v) 前記パッケージ化及び暗号化された前記加入者情報と前記ユーザデータとを前記第2の端末の前記第2の汎用集積回路カード (UICC2) へ送信するステップと；

vi) 前記加入者情報と前記ユーザデータとを前記第2の汎用集積回路カード (UICC2) にインストールするステップと；

10

20

からなる方法。

【請求項2】

ステップi)及びv)はNFCを介して実行される、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、第1の端末から第2の端末へ、加入者情報及びユーザデータを安全に転送する方法に関する。

【背景技術】

【0002】

ユーザの加入者情報及びユーザデータは、電気通信の分野においては、UICC（汎用集積回路カード）と呼ばれる保全素子（secure element）に格納される。UICCはSIMアプリケーションを内蔵し、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】

10

20

30

40

50

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e-UICCとUICCとの間にも、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、加入者情報を格納する埋設型保全素子(埋設型UICC)を有する端末間で、NFCを介して加入者情報を転送する方法に関する。

【0017】

将来、端末内にソフトSIM又は埋設型SIMが設けられるようになると、無線通信を介することなくIMS、Ki、Opc等を新たな端末に再プロビジョニング(改めてプロビジョニング)するには、遠隔的に個人化を行なうことにより、加入者情報(IMS、Ki、Opc、電話帳などのユーザデータ等)を、ある端末から他の端末へ(例えばこれらを互いに接触させることにより)安全に転送することが必要となる。

10

20

30

40

50

## 【 0 0 1 8 】

今日、携帯端末を変更したい場合には、ユーザは単純にUICCカードを元の端末から抜き取り、これを新たな端末に挿入すればよい。しかしこれは、新たな端末にSIMカードの差し込み口がない（つまり、埋設型UICCを有している）場合や、UICCの形式が新たな端末に適合しない場合には、行なえない。同様の問題は、元の端末が埋設型保全素子を内蔵していて、SIMアプリケーションを手で取り出すことができない場合にも生じる。

本発明は、この問題を解決することを目的とする。

## 【 課題を解決するための手段 】

## 【 0 0 1 9 】

本発明は、加入者情報及びユーザデータを、第1の端末から第2の端末へ、安全に転送する方法に関する。第1及び第2の端末は、それぞれ第1及び第2のUICCを内蔵しているものとする。

## 【 0 0 2 0 】

本発明によれば、この方法は：

- i) 第2の端末の識別子を第1の端末へ送信するステップと；
  - ii) 第1の端末から保全倉庫 (secure vault) へ、第2の端末の識別子と、第1のUICCの識別子とを送信するステップと；
  - iii) 保全倉庫から第1の端末へ、第2の端末の加入者情報インストール用公開鍵を送信するステップと；
  - iv) 第1のUICC内で、第2の端末の加入者情報インストール用公開鍵を用いて、加入者情報及びユーザデータをパッケージ化及び暗号化するステップと；
  - v) 第2の端末の第2のUICCへパッケージを送信するステップと；
  - vi) 第2のUICCにパッケージをインストールするステップと；
- からなる。

## 【 0 0 2 1 】

ステップi)及びv)は、NFCを介して行なわれることが望ましい。本発明は、好ましくは（取り出すことができない）埋設型UICCに適用される。

## 【 発明を実施するための形態 】

## 【 0 0 2 2 】

以下の記載は、加入者情報及びユーザデータが、NFCを介して第1の端末から第2の端末に送信される場合の使用事例である。

例えば、ユーザが端末X（第1の端末）を有しており、端末Y（第2の端末）にアップグレードしたい場合、以下のようなフローになる：

- 装置Xを装置Yに接触させる。装置X上にメニューが表示され、「加入者情報転送」を含む選択肢一式がユーザに提示される。
- 装置Yのユーザインタフェース上に、新たな加入者情報をインストールしてよいか確認するポップアップが現れる。これは承認されなくてはならない。装置Yは、装置YのIMEIを、NFCを介して装置Xに返す。

## 【 0 0 2 3 】

- 装置Xは、装置XのIMSIを、装置YのIMEIと一緒に、無線ネットワークを介して保全倉庫に送信する。保全倉庫は、装置Yの加入者情報インストール鍵を格納し、（承認された場合）これを暗号化して装置Xに返す。

- すると装置Xは、装置Yの鍵を用いて、IMSI、K、Op c、及びユーザデータを安全にパッケージ化し、暗号化して、これに署名する。

- 装置Xの画面上に通知が表示され、転送を完了させるため、ユーザに再度装置をタップさせる。

- 装置Xは、NFCを介して加入者情報を装置Yへ安全に転送する。インストールが完了すると、装置Yは（トランザクションが実行されたか確認するために）、保全倉庫に対し変更について警告する。

10

20

30

40

50

- これでは装置 Y は、加入者情報を用いて無線ネットワークにアクセスできる。

【 0 0 2 4 】

また、2つの端末間に Bluetooth (登録商標) 通信又はその他のチャネルを確立することもできる。ただし Bluetooth を使用するには、ペアリングや鍵の交換等が必要となる。

w i f i 又は Z i g b e e (登録商標) 接続を使用することもできる。全般的に、あらゆるパーソナル通信ネットワーク、無線エリアネットワーク、短距離有線(無線)技術を使用することができる。

【 0 0 2 5 】

本発明は、無線通信サーバを介することなく、遠隔的に加入者情報を転送することを可能にする(ネットワークに接続するだけで、認証/鍵の交換/加入者情報転送完了の通知ができる)。

10

他の使用事例では、装置 Y が、装置 X にインストールされているものと同じプロフィール/機能(c a p a b i l i t y)を有していない場合、保全倉庫が装置 Y 中の U I C C の個人化を遠隔的に行なうことができる。

【 0 0 2 6 】

この場合、保全倉庫は、装置 X に対して現状の装置 X のプロフィール(プロフィール、加入者情報、鍵、ユーザデータ等)をパッケージ化し、保全倉庫にアップロードするよう要求する。2つの保全素子に互換性がない場合、又はこれら保全素子のバージョンが異なる場合、仮想プロフィールは、保全倉庫を通過して装置 Y の異なる埋設型 U I C C 用に変換された後、装置 Y 用に再度個人化されなくてはならない。

20

---

フロントページの続き

(56)参考文献 特開2006-050554(JP,A)  
特表2010-532107(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 12/14  
G06F 21/00 - 21/88  
H04B 7/24 - 7/26  
H04M 1/00  
H04M 1/24 - 1/82  
H04M 99/00  
H04W 4/00 - 99/00