(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2019-501461
(P2019-501461A)
(43)公表日　平成31年1月17日(2019.1.17)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/31 (2013.01)	G06F 21/31	

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2018-535112 (P2018-535112)
(86)(22)出願日	平成28年12月27日 (2016.12.27)
(85)翻訳文提出日	平成30年9月5日 (2018.9.5)
(86)国際出願番号	PCT/CN2016/112265
(87)国際公開番号	WO2017/118315
(87)国際公開日	平成29年7月13日 (2017.7.13)
(31)優先権主張番号	201610006062.2
(32)優先日	平成28年1月5日 (2016.1.5)
(33)優先権主張国	中国 (CN)

(71)出願人　505032849
アリババ　グループ　ホウルディング　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ジョージ　タウン　ピーオーボックス　８４７　ワン　キャピタル　プレイス　フォース　フロア
(74)代理人　100097320
弁理士　宮川　貞二
(74)代理人　100215049
弁理士　石川　貴志
(74)代理人　100131820
弁理士　金井　俊幸
(74)代理人　100155192
弁理士　金子　美代子

最終頁に続く

(54)【発明の名称】スマートカードアプリケーションのためのセキュリティ検証方法及びデバイス

(57)【要約】
本願は、情報セキュリティ技術の分野に関し、特に、スマートカードアプリケーションのためのセキュリティ検証方法及びデバイスに関する。この方法は、スマートカードアプリケーションが外部とのサービス処理を実行するときに、現在のサービスの関連データを取得するステップと、現在のサービスの関連データとセキュリティパラメータとを特定するステップと、現在のサービスの関連データがセキュリティパラメータと一致しない場合、現在のサービスを終了するステップとを含む。記載の方法を実行するために、この方法に対応するデバイスを、仮想スマートカードアプリケーションに組み込む、又はｅＳＥチップにスマートカードアプリケーションとは別に組み込むことができる。スマートカードアプリケーションを用いてサービスを実行する上でセキュリティを確保するために、本願の実施における方法及びデバイスに基づいて、サービスの地理的位置、時刻、取引情報等を求める。

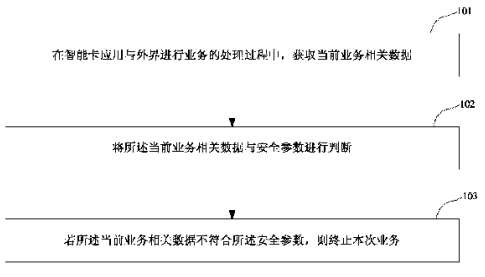


图1

101 IN A PROCESS IN WHICH A SMART CARD APPLICATION CARRIES OUT A SERVICE WITH THE OUTSIDE, OBTAINING DATA RELATED TO THE CURRENT SERVICE
102 DETERMINING DATA AND SECURITY PARAMETERS RELATED TO THE CURRENT SERVICE
103 IF THE DATA RELATED TO THE CURRENT SERVICE DOES NOT SATISFY THE SECURITY PARAMETERS, TERMINATING THIS SERVICE

【特許請求の範囲】
【請求項１】
スマートカードアプリケーションのためのセキュリティ検証方法であって：
前記スマートカードアプリケーションが外部とのサービス処理を実行するときに、現在のサービスの関連データを取得するステップと；
前記現在のサービスの前記関連データとセキュリティパラメータとを特定するステップと；
前記現在のサービスの前記関連データが前記セキュリティパラメータと一致しない場合、前記現在のサービスを終了するステップと；を備える、
セキュリティ検証方法。
【請求項２】
前記現在のサービスの前記関連データが前記セキュリティパラメータと一致する場合、前記現在のサービスの継続を許可するステップを更に備える、
請求項１に記載のセキュリティ検証方法。
【請求項３】
前記現在のサービスの前記関連データが、現在地情報、現在時刻情報、取引情報のうちの少なくとも１つ、又はこれらの組み合わせを含む、
請求項１に記載のセキュリティ検証方法。
【請求項４】
前記スマートカードアプリケーションが外部との前記サービス処理を実行するときに、前記現在のサービスの前記関連データを取得する前記ステップは：
埋め込み型セキュリティチップに組み込まれたスマートカードアプリケーションがＮＦＣコントローラと通信するときに、前記両者間での通信を監視して、前記現在のサービスの前記関連データを取得するステップを更に備える、
請求項１に記載のセキュリティ検証方法。
【請求項５】
前記スマートカードアプリケーションが外部との前記サービス処理を実行するときに、前記現在のサービスの前記関連データを取得する前記ステップは：
前記仮想スマートカードアプリケーションが前記ＮＦＣコントローラと通信するときに、前記仮想スマートカードアプリケーションにおける前記両者間の通信を監視し、前記現在のサービスの前記関連データを取得するステップを更に備える、
請求項１に記載のセキュリティ検証方法。
【請求項６】
前記現在のサービスの前記関連データとセキュリティパラメータとを特定する前記ステップの前に：
ユーザにより入力されたセキュリティパラメータを受信し、格納するステップと；
ユーザの関連データに基づく解析を通してサーバにより得られたセキュリティパラメータを受信し、格納するステップと；を更に備える、
請求項１に記載のセキュリティ検証方法。
【請求項７】
スマートカードアプリケーションのためのセキュリティ検証デバイスであって：
前記スマートカードアプリケーションが外部とのサービス処理を実行するときに、現在のサービスの関連データを取得するように構成された取得ユニットと；
前記現在のサービスの前記関連データとセキュリティパラメータとを特定するように構成された特定ユニットと；
前記現在のサービスの前記関連データが前記セキュリティパラメータと一致しない場合、前記現在のサービスを終了するように構成された処理ユニットと；を備える、
セキュリティ検証デバイス。
【請求項８】
前記処理ユニットは、前記現在のサービスの前記関連データが前記セキュリティパラメ

ータと一致する場合、前記現在のサービスの継続を許可するように更に構成される、
請求項７に記載のセキュリティ検証デバイス。
【請求項９】
前記現在のサービスの前記関連データは、現在地情報、現在時刻情報、及び取引情報のうちの少なくとも１つ、又はこれらの組み合わせを含む、
請求項７に記載のセキュリティ検証デバイス。
【請求項１０】
前記取得ユニットは、埋め込み型セキュリティチップに組み込まれたスマートカードアプリケーションとＮＦＣコントローラとの間の通信を監視し、前記現在のサービスの前記関連データを取得する、
請求項７に記載のセキュリティ検証デバイス。
【請求項１１】
前記取得ユニットは、仮想スマートカードアプリケーションに組み込まれ、前記仮想スマートカードアプリケーションとＮＦＣコントローラとの間の通信において前記現在のサービスの前記関連データを取得する、
請求項７に記載のセキュリティ検証デバイス。
【請求項１２】
セキュリティパラメータ受信ユニットを更に備え、前記セキュリティパラメータ受信ユニットは：
ユーザが入力したセキュリティパラメータを受信し、格納するように構成される；又は
サーバがユーザの関連データに基づく解析を通して取得したセキュリティパラメータを受信し、格納するように構成される；
請求項７に記載のセキュリティ検証デバイス。

【発明の詳細な説明】
【技術分野】
【０００１】
本願は、２０１６年１月５日に提出され「スマートカードアプリケーションのためのセキュリティ検証方法及びデバイス」と題された中国特許出願第２０１６１０００６０６２．２号の優先権を主張し、上記中国特許出願は参照によってその全体が本願に組み込まれる。
【０００２】
本願は情報セキュリティ技術の分野に関し、特に、スマートカードセキュリティ検証方法及びデバイスに関する。
【背景技術】
【０００３】
モバイルインターネット技術の発展に伴い、インテリジェント端末上のスマートカードアプリケーションを用いて実施できるサービスの数は増え続けている。例えば、モバイル決済、公共交通機関の利用、職場エリアへの立入等、インテリジェント端末によるスマートカードアプリケーションの実施を、近距離通信チップにより支援することができる。人々の生活の中でインテリジェント端末が重要な役割を果たすようになるにつれて、インテリジェント端末を紛失したり悪用されたりした場合に、ユーザ、企業、又は公共機関は多大な損害を被る可能性がある。現在、スマート端末用のスマートカードアプリケーションのセキュリティを高めるための技術的解決策が求められている。
【発明の概要】
【０００４】
スマート端末の盗難後にスマートカードアプリケーションのセキュリティを確保できない既存の技術における問題を解決するために、スマートカードアプリケーションの使用をユーザ設定又はユーザの習慣に基づいて制約するように、スマートカードアプリケーショ

ンのためのセキュリティ検証方法及びデバイスを提案する。これにより、スマートカードのアプリケーションのセキュリティを確保できる。

【０００５】

本願の一実施形態は、スマートカードアプリケーションが外部とのサービス処理を実行するときに、現在のサービスの関連データを取得するステップと；前記現在のサービスの前記関連データとセキュリティパラメータとを特定するステップと；前記現在のサービスの前記関連データが前記セキュリティパラメータと一致しない場合、前記現在のサービスを終了するステップと；を含むスマートカードアプリケーションのためのセキュリティ検証方法を提供する。

【０００６】

本願の一実施形態は、スマートカードアプリケーションが外部とのサービス処理を実行するときに、現在のサービスの関連データを取得するように構成された取得ユニットと；前記現在のサービスの前記関連データとセキュリティパラメータとを特定するように構成された特定ユニットと；前記現在のサービスの前記関連データが前記セキュリティパラメータと一致しない場合、前記現在のサービスを終了するように構成された処理ユニットと；を含むスマートカードアプリケーションのためのセキュリティ検証デバイスを提供する。

【０００７】

本願の実施の技術的解決策の説明から分かることは、スマートカードアプリケーションを用いてサービス実行のセキュリティを確保するために、サービスの地理的位置、時刻、取引情報等が特定されるということである。加えて、異なるタイプのスマートカードアプリケーション（ｅＳＥチップ、ＨＣＥ等）に基づき、これらの異なるタイプのスマートカードアプリケーションに適用できるセキュリティ検証方法が設計されるということである。例えば、検証のためにｅＳＥチップ中のスマートカードアプリケーションと通信モジュールとの間のサービス処理が得られ、又はＨＣＥに組み込まれたスマートカードアプリケーションにおけるセキュリティ検証方法を用いてサービスセキュリティ検証が実行される。

【０００８】

当然ながら、本願の任意の製品又は方法を実施することは、上で述べた全ての利点を同時に満たす必要はない。

【図面の簡単な説明】

【０００９】

本願の実施における、又は、既存技術における技術的解決策をより明瞭に説明するために、各実施又は既存技術を説明する添付の図面について以下簡単に述べる。以下の説明における添付の図面は、本願のいくつかの実施態様を示しているに過ぎず、当業者は、創造的な努力無しに、これらの添付の図面から他の図面を導けることは明らかである。

【００１０】

【図１】図１は、本願の実施に係るスマートカードアプリケーションのためのセキュリティ検証方法を示すフローチャートである。

【００１１】

【図２】図２は、本願の実施に係るスマートカードアプリケーションのためのセキュリティ検証デバイスを示す概略構造図である。

【００１２】

【図３】図３は、本願の実施に係るスマートカードアプリケーションのためのセキュリティ検証方法を示すフローチャートである。

【００１３】

【図４】図４は、本願の実施に係る、ｅＳＥチップにスマートカードアプリケーションをインストールするシステム構造を示す図である。

【００１４】

【図５】図５は、本願の実施に係る、スマートカードアプリケーションのための別のセキ

ュリティ検証方法を示すフローチャートである。
【００１５】
【図６】図６は、本願の実施に係る、スマートフォンにスマートカードアプリケーションをインストールするシステム構造を示す図である。
【発明を実施するための形態】
【００１６】
本願の実施は、スマートカードアプリケーションのためのセキュリティ検証方法及びデバイスを提供する。
【００１７】
当業者が本願の技術的解決策をより深く理解できるように、本願の実施の添付図面を参照しつつ、本願の実施における技術的解決策を明瞭且つ十分に以下説明する。記載の実施態様は本願の全ての実施態様を示すものではなく、そのうちのいくつかを示すに過ぎないことは明らかである。当業者により本願の実施に基づいて創造的な努力無しに得られる他の実施は、本願の保護範囲内に含まれるものである。
【００１８】
本願におけるスマートカードアプリケーションは、例えば、アクセス制御アプリケーション、交通カードアプリケーション、及び銀行カードアプリケーションを含む。スマートカードアプリケーションは、インテリジェント端末に搭載されたｅＳＥ（ｅｍｂｅｄｄｅｄ　Ｓｅｃｕｒｅ　Ｅｌｅｍｅｎｔ、埋め込み型セキュリティエレメント）チップにインストールできる、又は、スマートカードアプリケーションは、ＨＣＥ（Ｈｏｓｔ　Ｃａｒｄ　Ｅｍｕｌａｔｉｏｎ）技術を用いて実装できる。ここでは、アプリケーションの詳細は述べない。
【００１９】
図１に示すように、同図は、本願の実施に係るスマートカードアプリケーションのためのセキュリティ検証方法を示すフローチャートである。この実施では、インテリジェント端末が取引端末とサービス処理を実行するときに、インテリジェント端末は、現在のサービスが安全であるかどうかを所定のルールに基づいて特定する。安全でない場合、サービスは中断する。安全な場合、サービスは継続を許可される。所定のルールは、位置情報、時刻情報、サービス内容等に基づくルールであってもよく、また、ユーザによって自発的に設定されても、システムによって統計解析された後にインテリジェント端末に提供されてもよい。スマートカードアプリケーションは、デバイス紛失により生じる損害を回避するように安全に制御できる。
【００２０】
この方法はステップ１０１を含む。ステップ１０１では、スマートカードアプリケーションが外部のサービス処理を実行するときに、現在のサービスの関連データを取得する。
【００２１】
ステップ１０２：現在のサービスの関連データとセキュリティパラメータとを特定する。
【００２２】
ステップ１０３：現在のサービスの関連データがセキュリティパラメータと一致しない場合には、現在のサービスを終了する。
【００２３】
本願の実施によれば、この方法は、現在のサービスの関連データがセキュリティパラメータと一致する場合、現在のサービスを継続することを可能とする。スマートカードアプリケーションで実行されている現在のサービスのセキュリティを確保するために、現在のサービスの関連データを特定することにより、現在のサービスを終了又は承認できる。
【００２４】
本願の実施によれば、現在のサービスの関連データは、現在地情報、現在時刻情報、又は取引情報のうちの少なくとも１つ、若しくはこれらの組み合わせを含む。現在地情報と、セキュリティパラメータ内で設定された位置情報とを特定できる。現在地が、セキュリ

ティパラメータ内で設定された位置範囲を外れる場合、サービスの継続は許可されない。例えば、スマートカードアプリケーションが、現在、エリアＡ内でサービスを実行しており、ユーザによってセキュリティパラメータ内で設定された位置範囲がエリアＢである場合、スマートカードアプリケーションで現在実行されているサービスは安全でないとみなされる。スマートカードアプリケーションにより現在実行中のサービスが１０００ＲＭＢ（人民元）であり、ユーザがセキュリティパラメータ内で設定した取引情報が８００ＲＭＢである場合、スマートカードアプリケーションで現在実行されているサービスは安全でないとみなされる。

【００２５】

現在のサービスの関連データに関し、インテリジェント端末のＧＰＳモジュールを用いて又は基地局測位を介して、現在地情報を入手でき、システムクロック又はネットワーククロックを用いて、現在時刻情報を入手でき、取引注文を用いて、取引情報を入手できる。具体的な測位方法については、既存の測位技術を参照できる。現在時刻情報は、既存技術における特定の解決策を参照して入手できる。簡略化のために、ここでは詳細について述べない。

【００２６】

本願の実施によれば、スマートカードアプリケーションが外部とのサービス処理を実行するときに現在のサービスの関連データを入手するステップは：この両者間の通信を監視するステップと；ｅＳＥチップに組み込まれたスマートカードアプリケーションがＮＦＣ（Ｎｅａｒ　Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ、近距離通信）コントローラと通信するときに、現在のサービスの関連データを入手するステップと；を更に含む。

【００２７】

このステップのこの実施において、本願のこの実施における方法は、ソフトウェア方法又はハードウェアモジュール方法にて実施できる。この方法は、現在のサービスの関連データを入手するステップと、後続の工程、例えば解析及び特定の工程、を含む。この方法は、ｅＳＥチップ内のスマートカードアプリケーションとＮＦＣコントローラ（又は、別のスマートカードアプリケーションに用いられる類似の通信モジュール）との間の通信を監視することによって実行される。或いは、ＮＦＣコントローラは、サービス実行時に、本願におけるセキュリティ検証アプリケーションに通知することができる。言い換えれば、ｅＳＥチップ内のスマートカードアプリケーションとＮＦＣコントローラとの間でサービス処理が実行されるかどうかを、本願のこの実施におけるセキュリティ検証方法に基づいて監視する。セキュリティ検証は、サービス処理が生じると開始する。

【００２８】

この実施では、スマートカードアプリケーションとＮＦＣコントローラとの通信中はいつでも、現在のサービスの関連データを入手でき、後続のステップを実行できる。例えば、セキュリティ検証は、ＮＦＣコントローラがスマートカードアプリケーションにサービス命令を転送する前に実行される。

【００２９】

本願の実施によれば、スマートカードアプリケーションが外部とのサービス処理を実行するときに現在のサービスの関連データを入手するステップは：仮想ＨＣＥスマートカードアプリケーションがＮＦＣコントローラと通信するときに、仮想スマートカードアプリケーションにおける両者間の通信を監視するステップと；現在のサービスの関連データを入手するステップと；を更に含む。

【００３０】

このステップのこの実施では、ＨＣＥスマートカードアプリケーションを用いてスマートカードアプリケーションを実施するときに、このアプリケーションに本願のセキュリティ検証方法を適用することができ、本願のこの実施におけるセキュリティ検証方法を、ＨＣＥによりサービスを実行する工程に含まれているステップの前又は後に実行できる。セキュリティ検証に成功した場合、サービス工程を継続できる。失敗した場合、サービス工程は終了する。

【００３１】
本願の実施によれば、現在のサービスの関連データとセキュリティパラメータとを特定するステップの前に、本方法は、ユーザにより入力されたセキュリティパラメータを受信し、格納するステップを含む、又は、サーバにより、ユーザの関連データに基づく解析を通して入手されたセキュリティパラメータを受信し、格納するステップを含む。
【００３２】
このステップのこの実施において、セキュリティパラメータはユーザにより任意に設定できる、又は、セキュリティパラメータはユーザの動作履歴の解析に基づいてサーバにより特定できる。例えば、統計解析が、ユーザが過去に一度もエリアＡ内に出現していないものの、現在のサービスの位置情報がエリアＡであることを示す場合、そのサービスは危険であるとみなされ、ユーザの現在のサービスは拒否される。更に、この実施では、例えばサービスがアクセス制御に関する認証であり、ユーザがエリアＡへの進入を過去に一度も求めたことがない場合にあって、エリアＡへの進入の現在要求がなされると、アクセス制御スマートカードアプリケーションを搭載したモバイルフォンを紛失し、他人に誤用された可能性がある。
【００３３】
スマートカードアプリケーションを用いたサービスの実行のセキュリティを確保するために、本願のこの実施における方法に基づいて、サービスの地理的位置、時刻、取引情報等が特定される。加えて、異なるタイプのスマートカードアプリケーション（ｅＳＥチップ、ＨＣＥ等）に基づいて、異なるタイプのスマートカードアプリケーションに適したセキュリティ検証方法が設計される。例えば、ｅＳＥチップ内のスマートカードアプリケーションと通信モジュールとの間のサービス工程が検証のために得られる、又は、ＨＣＥに組み込まれたスマートカードアプリケーションにおけるセキュリティ検証方法を用いてサービスセキュリティ検証が実行される。
【００３４】
図２に示すように、同図は、本願の実施に係るスマートカードアプリケーションのためのセキュリティ検証デバイスを示す概略構造図である。この実施におけるデバイスはインテリジェント端末に組み込まれ、インテリジェント端末上を走る。インテリジェント端末には、例えばスマートフォン又はタブレットコンピュータが含まれる。スマートカードアプリケーションのための検証デバイスは、プログラマブル論理デバイス（ＦＰＧＡ）のような専用チップを用いて、又は、ＨＣＥスマートカードアプリケーション内のソフトウェアを用いて実施できる。
【００３５】
同図は、スマートカードアプリケーションが外部とのサービス処理を実行するときに、現在のサービスの関連データを入手するように構成された取得ユニット２０１と；現在のサービスの関連データとセキュリティパラメータとを特定するように構成された特定ユニット２０２と；現在のサービスの関連データがセキュリティパラメータと一致しない場合、現在のサービスを終了するように構成された処理ユニット２０３と；を含む。
【００３６】
本願の実施によれば、処理ユニットは、現在のサービスの関連データがセキュリティパラメータと一致する場合、現在のサービスの継続を許可するように更に構成される。
【００３７】
本願の実施によれば、現在のサービスの関連データは、現在地情報、現在時刻情報及び取引情報のうち少なくとも１つ、又はこれらの組み合わせを含む。
【００３８】
現在地情報は、インテリジェント端末に組み込まれたＧＰＳモジュールを用いて入手できる。現在時刻情報は、ネットワーク通信モジュールを用いて、又はインテリジェント端末に組み込まれたクロック発振器を用いて入手できる。取引情報は、インテリジェント端末の取引注文を用いて入手できる。
【００３９】

本願の実施によれば、取得ユニットは、ｅＳＥチップに組み込まれたスマートカードアプリケーションとＮＦＣコントローラとの間の通信を監視し、現在のサービスの関連データを入手する。

【００４０】

本願の実施によれば、取得ユニットは仮想スマートカードアプリケーションに組み込まれており、仮想ＨＣＥスマートカードアプリケーションとＮＦＣコントローラとの間の通信における現在のサービスの関連データを入手する。

【００４１】

本願の実施によれば、本デバイスはセキュリティパラメータ受信ユニット２０４を更に含む。セキュリティパラメータ受信ユニット２０４は、ユーザが入力したセキュリティパラメータを受信し格納するように、又はサーバがユーザの関連データに基づく解析により入手したセキュリティパラメータを受信し格納するように、構成される。

【００４２】

本願のこの実施におけるデバイスによれば、スマートカードアプリケーションを用いたサービス実行時のセキュリティを確保するために、サービスの地理的位置、時刻、取引情報等が特定される。加えて、異なるタイプのスマートカードアプリケーション（ｅＳＥチップ、ＨＣＥ等）に基づき、異なるタイプのスマートカードアプリケーションに適用可能なセキュリティ検証方法が設計される。例えば、検証のためにｅＳＥチップ内のスマートカードアプリケーションと通信モジュールとの間のサービス工程が得られる、又は、ＨＣＥ内に組み込まれたスマートカードアプリケーションにおけるセキュリティ検証方法を用いてサービスセキュリティ検証を実行される。

【００４３】

図３に示すように、同図は、本願の実施に係るスマートカードアプリケーションのためのセキュリティ検証方法を示すフローチャートである。同図のスマートカードアプリケーションはｅＳＥチップに組み込まれる。この実施では、インテリジェント端末はスマートフォンであってよく、カードリーダはＰＯＳ（Ｐｏｉｎｔ　ｏｆ　ｓａｌｅ、販売時点情報管理）デバイスにインストールされたＮＦＣカードリーダであってよく、ＮＦＣコントローラは、決済サービスを行うためにＰＯＳデバイスのＮＦＣカードリーダと通信するように構成された、スマートフォン上の１つのハードウェアであってよい。本願のこの実施における、スマートフォンに組み込まれた装置を用いることにより、又はこの方法に基づくソフトウェアを用いることにより、決済サービスのセキュリティ検証を実施するべく、スマートカードアプリケーションとＮＦＣコントローラとの間の決済サービス処理を監視できる。

【００４４】

ステップ３０１：ｅＳＥチップに組み込まれた決済アプリケーションをＮＦＣコントローラに登録し、決済アプリケーションの識別子はＮＦＣコントローラに記憶される。

【００４５】

この実施では、スマートカードアプリケーション管理端末を用いて、又はネットワーク上でエアカード（航空券）発行ユニット（スマートフォンのｅＳＥチップに組み込むことができる）を用いて、スマートカードアプリケーションをｅＳＥチップにインストールすることができる。図４に特定のシステム構造図を示す。ＰＯＳデバイス上のＮＦＣカードリーダは、ＮＦＣを介してスマートフォンのＮＦＣコントローラと通信する。スマートカードアプリケーション管理端末は、ＮＦＣを介してスマートフォンのｅＳＥチップにスマートカードアプリケーションをインストールすることができる、又はエアカード発行ユニットを用いてスマートカードアプリケーションを遠端から入手し、ｅＳＥチップにインストールすることができる。ｅＳＥチップとＮＦＣコントローラとの間の通信を監視するために、本願でのセキュリティ検証アプリケーショもスマートフォンに組み込まれている。セキュリティ検証アプリケーションは、ＮＦＣコントローラ内の通信インターフェースを用いて、ｅＳＥチップとＮＦＣコントローラとの間の通信を監視できる。

【００４６】

このステップにおいて、又はこのステップの前に、ユーザは、タッチスクリーン及びボタンのようなスマートフォンに搭載された入力デバイスから、本願による、スマートフォンに組み込まれたセキュリティ検証アプリケーションへセキュリティパラメータを入力できる。スマートカード決済アプリケーション中のセキュリティパラメータは、例えば、位置限定、範囲限定、取引金額閾値であってよい。セキュリティパラメータの数は実際の必要性に基づいて設定できる。この実施では、位置限定は、例えば、エリアＡ、エリアＢ、エリアＣであってよく、この場合、スマートカード決済アプリケーションはこの３つのエリア内で許可され、他のエリアでは許可されない。取引金額閾値は、例えば１０００ＲＭＢであってよく、この場合には、位置に関係なく、１０００ＲＭＢを超える消費は許可されない。当然ながら、当業者は、本開示に基づいてその他のセキュリティパラメータの組み合わせ（例えば、取引金額と位置限定の組み合わせ）を考慮できる。例えば、限定位置エリアでの取引金額を限定せず、位置限定外のエリアでの取引金額の上限を１００ＲＭＢとすることができる。時刻パラメータをセキュリティパラメータと見なした場合、より多くの可能なセキュリティパラメータの組み合わせを取得できる。本願のこの実施では、種々の可能な組み合わせを記載し尽くすことはできないので、簡素化のために詳細は述べない。

【００４７】

ステップ３０２：ＰＯＳデバイスのＮＦＣカードリーダが、スマートフォンのＮＦＣコントローラを用いＮＦＣを介して決済サービスを実行する。

【００４８】

このステップでは、ＮＦＣカードリーダとＮＦＣコントローラとの間の決済サービス処理について既存技術における解決策を参照できる。例えば、ＮＦＣカードリーダは、ＮＦＣコントローラに登録された決済アプリケーションの識別子を選択し、その後、対応のスマートカード決済サービス手順を実行する。

【００４９】

ステップ３０３：ＮＦＣコントローラは、セキュリティ検証アプリケーションを開始するために、決済サービスのプロンプトをセキュリティ検証アプリケーションへ送信する。

【００５０】

ステップ３０４：スマートフォンに組み込まれたセキュリティ検証アプリケーションが決済サービスの関連データを入手する。

【００５１】

このステップでは、セキュリティ検証アプリケーションは、ＮＦＣコントローラのインターフェースを用いて決済サービスの関連データを入手できる。このような場合、決済アプリケーションが決済サービスの関連データを入手することはない。

【００５２】

決済サービスの関連データは、現在地情報と現在の取引金額とを含む。セキュリティ検証アプリケーションは、スマートフォンに組み込まれたＧＰＳモジュールによって現在地情報を入手する、又は基地局測位やネットワーク測位によって現在地情報を入手する、更に、阻止されたサービス処理結果を用いて現在の取引金額を入手できる。

【００５３】

ステップ３０５：現在地情報と現在の取引金額とを、セキュリティパラメータに基づいて検証する。

【００５４】

この実施では、阻止された位置情報はエリアＤであり、取引金額は２，０００ＲＭＢである。決済サービスの関連データを、セキュリティパラメータ内の位置情報及び取引金額閾値と比較し、決済サービスの関連データがセキュリティパラメータと一致しないという特定結果を導く。

【００５５】

ステップ３０６：セキュリティ検証アプリケーションは現在の決済サービスを終了し、現在の決済サービスの失敗メッセージをＮＦＣコントローラへ送信する。

【００５６】
このステップでは、セキュリティ検証結果をスマートフォン画面上でユーザに対しプロンプト表示することができる。
【００５７】
ステップ３０５での特定結果が、決済サービスの関連データがセキュリティパラメータと一致する場合には、現在の決済サービスは継続を許可され（つまり、妨害されない）、ＮＦＣコントローラとｅＳＥチップ内のスマートカードアプリケーションとの間の決済サービスは妨害されない。図３では、決済サービスが継続を許可された場合に決済アプリケーションによるサービス処理を実行する工程を破線で示す。ＮＦＣコントローラは、ｅＳＥチップに組み込まれた決済アプリケーションへ決済サービス命令を転送する。決済アプリケーションはサービス処理を実行し、ＮＦＣコントローラを用いてサービス処理結果をＮＦＣカードリーダへ返す。決済アプリケーションは、決済サービス手順の実行を成功させるために、何度でもＮＦＣカードリーダと通信することができる。この部分の詳細については既存技術を参照することができるので、簡略化のためにここでは述べない。
【００５８】
ステップ３０７：ＮＦＣコントローラは、現在の決済サービスの失敗メッセージをＰＯＳデバイスのＮＦＣカードリーダへ送信し、現在の決済は失敗となる。
【００５９】
この実施では、スマートカードアプリケーションは、ユーザが設定したセキュリティパラメータに基づく本願の技術的解決策にて管理できる。未承認の（セキュリティパラメータと一致しない）サービスを実行すると、ユーザプロパティと情報のセキュリティとを確保するために、スマートカードアプリケーションの安全でないサービス処理は適切なタイミングで終了され、これにより、インテリジェント端末紛失時の悪用による損害を防ぐ。
【００６０】
図５に示すように、同図は、本願の実施に係る、スマートカードアプリケーションのための別のセキュリティ検証方法を示すフローチャートである。この実施では、本願の技術的解決策を説明するために、仮想スマートカードアプリケーションを例にとる。仮想スマートカードは、ｅＳＥチップが組み込まれていないインテリジェント端末に主として用いられ、インテリジェント端末によるスマートカードアプリケーションのサポートを支援する。本願におけるセキュリティ検証方法又はデバイスは、仮想スマートカードアプリケーションが仮想スマートカードアプリケーションのセキュリティ検証を行えるよう、仮想スマートカードアプリケーションに組み込むことができる。この実施では、やはり決済サービスを例に説明する。インテリジェント端末はスマートフォンであり、ＰＯＳデバイスカードリーダはＮＦＣカードリーダである。スマートフォンは、ＮＦＣコントローラを用いてＮＦＣカードリーダと通信する。当然ながら、他の実施では、別のＮＦＣ技術を用いて通信を行うことができる。ここでは何の制限もかけられるものではない。
【００６１】
ステップ５０１：仮想スマートカードアプリケーションは、ＮＦＣコントローラに決済アプリケーション識別子を登録する。
【００６２】
この実施では、スマートカードアプリケーション管理端末を用いて、仮想スマートカードアプリケーションをスマートフォンのメモリへロードすることができる。図６に具体的なシステム構造図を示す。ＰＯＳデバイス上のＮＦＣカードリーダは、ＮＦＣを介してスマートフォンのＮＦＣコントローラと通信する。スマートカードアプリケーション管理端末が、ＮＦＣを介して、仮想スマートカードアプリケーションをスマートフォンのメモリにインストールする、又は仮想スマートカードアプリケーションを、スマートフォンのインターネット機能を用いて遠端（リモートエンド）から入手し、スマートフォンにインストールすることができる。本願のセキュリティ検証アプリケーションは、仮想スマートカードアプリケーションに組み込むことができる。
【００６３】

ステップ５０２：決済サービスを実行するために、ＰＯＳデバイスのＮＦＣカードリーダがＮＦＣコントローラと通信し、仮想スマートカードアプリケーションの識別子を選択する。

【００６４】

ステップ５０３：ＮＦＣコントローラが、決済サービスを実行させる命令を仮想スマートカードアプリケーションへ送信する。

【００６５】

ステップ５０４：仮想スマートカードアプリケーション内のセキュリティ検証アプリケーションが、現在地情報と現在時刻情報とを入手する。

【００６６】

現在地情報は、スマートフォンに組み込まれたＧＰＳモジュールを用いて、又は基地局測位若しくはネットワーク測位によって入手できる。現在時刻情報は、スマートフォンのシステム時刻を用いて、又はスマートフォンのインターネット機能を用いてインターネットから入手できる。

【００６７】

ステップ５０５：スマートフォンの通信モジュールを用いて、リモートサーバからユーザのセキュリティパラメータを入手する。

【００６８】

このステップにおけるセキュリティパラメータは、インターネットを介してリモートサーバから入手できる。リモートサーバは、ユーザの履歴データを解析することにより、又はユーザに関連するビッグデータを解析することにより、対応のセキュリティパラメータを入手する。例えば、ユーザのセキュリティパラメータは、決済取引の傾向、１日の決済取引金額、位置、時刻、ユーザの商品カテゴリ等のデータを解析して入手でき、現在の取引のセキュリティリスクを、ユーザデータに基づき、電子取引分野の各方法を用いて特定できる。特定のセキュリティパラメータ計算方法は既存の技術を参照でき、参照により本明細書に援用される。

【００６９】

この実施におけるセキュリティパラメータの入手方法と、図３に示した実施におけるユーザによるセキュリティパラメータの設定方法とは差替えることができる。

【００７０】

ステップ５０６：現在の決済サービスの現在地情報と現在時刻情報とを、セキュリティパラメータに基づいて検証する。

【００７１】

セキュリティパラメータ内の位置情報が現在地情報と合致しない場合、及びセキュリティパラメータ内の時刻情報が現在時刻情報と異なる場合、ユーザは、通常、現在時刻又は現在位置にて決済サービスを実行しないことを意味するので、その決済サービスはユーザによって実施されていない可能性があり、危険を伴う。

【００７２】

ステップ５０７：現在の決済サービスを終了し、対応のサービス処理結果を生成し、このサービス処理結果をＮＦＣコントローラへ転送する。

【００７３】

ステップ５０６での特定結果が安全な決済サービスである場合には、仮想スマートカードアプリケーションの決済サービス手順は継続し、この期間中に、ＮＦＣコントローラは、決済サービス手順を完了するように、ＰＯＳデバイスのＮＦＣカードリーダとの間で１回以上通信することができる。

【００７４】

ステップ５０８：ＮＦＣコントローラが、決済サービス処理結果をＰＯＳデバイスのＮＦＣカードリーダへ送信する。

【００７５】

本願の実施における方法及びデバイスに基づき、スマートカードアプリケーションを用

いてサービスを実行する上でセキュリティを確保するために、サービスの地理的位置、時刻、取引情報等を特定できる。加えて、異なるタイプのスマートカードアプリケーション（ｅＳＥチップ、ＨＣＥ等）に基づいて、異なるタイプのスマートカードアプリケーションに適用可能なセキュリティ検証方法が設計される。例えば、検証のためにｅＳＥチップ内のスマートカードアプリケーションと通信モジュールとの間のサービス工程を取得する、又は、ＨＣＥに組み込まれたスマートカードアプリケーションにおけるセキュリティ検証方法を用いてサービスセキュリティ検証を実行する。

【００７６】

技術の改良がハードウェアの改良（例えば、ダイオード、トランジスタ、スイッチのような回路構造の改良）であるか、ソフトウェアの改良（方法の手順の改良）であるかは明白に区別できる。しかし、技術の発達と共に、現在の方法の手順の改良の多くは、ハードウェア回路構造の直接的な改良とみなされ得る。設計者は、通常、ハードウェア回路に、改良した方法の手順をプログラムすることにより、対応するハードウェア回路構造を取得する。したがって、実体的なハードウェアモジュールは方法の手順を改良できる。例えば、プログラマブル論理デバイス（Ｐｒｏｇｒａｍｍａｂｌｅ Ｌｏｇｉｃ Ｄｅｖｉｃｅ、ＰＬＤ）（例えば、フィールドプログラマブル回路アレイ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ、ＦＰＧＡ））はそのような集積回路であり、プログラマブル論理デバイスの論理機能は、デバイスプログラミングを介してユーザにより特定される。設計者は、アプリケーション特化集積回路チップ２の設計及び製造をチップ製造業者に依頼することなく、デジタルシステムをＰＬＤに「統合させる」ためにプログラミングを実行する。加えて、プログラミングは、集積回路チップを手作りするのではなく、「論理コンパイラ（ｌｏｇｉｃ ｃｏｍｐｉｌｅｒ）」ソフトウェアを修正して実施されることがほとんどである。これは、プログラムの開発及び構成に使用するソフトウェアコンパイラと類似する。コンパイル前のオリジナルコードも特定のプログラミング言語で書かれる必要があり、これはハードウェア記述言語（Ｈａｒｄｗａｒｅ Ｄｅｓｃｒｉｐｔｉｏｎ Ｌａｎｇｕａｇｅ、ＨＤＬ）と呼ばれる。しかし、ＨＤＬは多様である。例えば、ＡＢＥＬ（Ａｄｖａｎｃｅｄ Ｂｏｏｌｅａｎ Ｅｘｐｒｅｓｓｉｏｎ Ｌａｎｇｕａｇｅ）、ＡＨＤＬ（Ａｌｔｅｒａ Ｈａｒｄｗａｒｅ Ｄｅｓｃｒｉｐｔｉｏｎ Ｌａｎｇｕａｇｅ）、Ｃｏｎｆｌｕｅｎｃｅ、ＣＵＰＬ（Ｃｏｒｎｅｌｌ Ｕｎｉｖｅｒｓｉｔｙ Ｐｒｏｇｒａｍｍｉｎｇ Ｌａｎｇｕａｇｅ）、ＨＤＣａｌ、ＪＨＤＬ（Ｊａｖａ（登録商標）Ｈａｒｄｗａｒｅ Ｄｅｓｃｒｉｐｔｉｏｎ Ｌａｎｇｕａｇｅ）、Ｌａｖａ、Ｌｏｌａ、ＭｙＨＤＬ、ＰＡＬＡＳＭ、ＲＨＤＬ（Ｒｕｂｙ Ｈａｒｄｗａｒｅ Ｄｅｓｃｒｉｐｔｉｏｎ Ｌａｎｇｕａｇｅ）がある。現在、ＶＨＤＬ（Ｖｅｒｙ－Ｈｉｇｈ－Ｓｐｅｅｄ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ ＨａｒｄｗａｒｅＤｅｓｃｒｉｐｔｉｏｎ Ｌａｎｇｕａｇｅ）とＶｅｒｉｌｏｇ２が最も普及している。当業者は、この方法の手順では、記載したいくつかのハードウェア記述言語を用いて論理プログラミングを実行するだけでよく、また、この方法の手順は集積回路にプログラムされており、それにより、論理方法手順を実施するハードウェア回路を容易に入手できることを更に理解するはずである。

【００７７】

コントローラは任意の適切な方法で実施できる。例えば、コントローラはマイクロプロセッサ又はプロセッサを使用でき、コンピュータ読み取り可能媒体、論理ゲート、スイッチ、アプリケーション特化集積回路（Ａｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ、ＡＳＩＣ）、プログラマブル論理コントローラ、更に、（マイクロ）プロセッサにより実行し得る、コンピュータ読み取り可能プログラムコード（例えば、ソフトウェア又はハードウェア）といった、埋め込み型マイクロコントローラのような形態を格納できる。コントローラの例には、以下のマイクロコントローラ：ＡＲＣ６２５Ｄ、Ａｔｍｅｌ ＡＴ９１ＳＡＭ、Ｍｉｃｒｏｃｈｉｐ ＰＩＣ１８Ｆ２６Ｋ２０、Ｓｉｌｉｃｏｎｅ Ｌａｂｓ Ｃ８０５１Ｆ３２０が非限定的に含まれる。メモリコントローラもメモリの制御論理の一部として実施できる。

【００７８】
当業者は、コントローラを、純粋な、コンピュータ読み取り可能なプログラムコード方法で実施することに加えて、方法ステップを用いて、論理プログラミングを完全に実行でき、これにより、コントローラが同じ機能を、論理ゲート、スイッチ、アプリケーション特化集積回路、プログラマブル論理コントローラ、埋め込み型マイクロプロセッサ等の形態にて実施できるようになることも理解している。そのため、コントローラはハードウェアコンポーネントとみなすことができ、様々な機能を実施するための装置はハードウェアコンポーネント内の構造とみなすことができる。或いは、様々な機能を実施するように構成された装置を、本方法を実施できる、ソフトウェアモジュール、又はハードウェアコンポーネント内の構造とみなすことができる。
【００７９】
上記の実施で述べたシステム、装置、モジュール、ユニットは、コンピュータチップ又はエンティティにより実施でき、又は機能を有する製品により実施できる。
【００８０】
説明を容易にするために、記載の装置は、機能毎に様々なユニットに分割して述べられている。当然ながら、本願を実施する場合には、これらのユニットの機能を１つ以上のソフトウェア及び／又はハードウェアにて実施できる。
【００８１】
上記の実施の説明に基づけば、当業者は、本願をソフトウェア及び必須の汎用ハードウェアプラットフォームにより実施できることを明確に理解できる。このような理解に基づき、本質的に又は部分的に既存の技術に寄与する本願の技術的解決策は、ソフトウェア製品の形態にて実施できる。コンピュータソフトウェア製品は、ＲＯＭ／ＲＡＭ、磁気ディスク、光学ディスクのような記録媒体に格納でき、更に、本願の実施又はそのいくつかの部分に記載された方法を実行するようにコンピュータデバイス（パーソナルコンピュータ、サーバ、ネットワークデバイスであってよい）に命令するためのいくつかの命令を含む。
【００８２】
本明細書における実施は全て順を追って説明されている。複数の実施において同一又は類似する部分については、それらの実施を参照されたい。各実施は、他の実施との違いに焦点を置いている。特に、システムの実施は方法の実施と基本的に類似しているため、簡潔に述べられている。関連する部分については、方法の実施についての記載を部分的に参照されたい。
【００８３】
本願は多くの汎用又は専用コンピュータシステムの環境又は構成、例えば、パーソナルコンピュータ、サーバコンピュータ、ハンドヘルド型デバイス若しくはポータブルデバイス、フラットタイプデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、セットトップボックス、プログラマブル民生用デジタルデバイス、ネットワークＰＣ、小型コンピュータ、メインフレームコンピュータ、及び、記載のシステム又はデバイスのいずれかを含む分散型計算環境に適用できる。
【００８４】
本願は、プログラムモジュールのような、コンピュータにより実行される、コンピュータで実行可能な命令の一般的な文脈にて説明できる。一般に、プログラムモジュールは、特定のタスクを実行する、又は特定のアブストラクトデータタイプを実施する、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造等を含む。本願は、分散型計算環境にて実施することも可能である。これらの分散型計算環境において、タスクは、通信ネットワークを用いて接続したリモートの処理デバイスによって実行される。分散型計算環境では、格納デバイスを設けたローカル又はリモートのコンピュータ格納媒体内にプログラムモジュールを配置できる。
【００８５】
本願は実施を用いて表されているが、当業者は、本願がその主旨から逸脱しない多くの

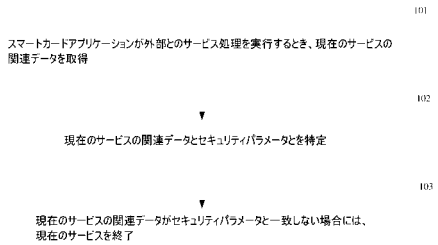
変形及び変更を含み、添付の特許請求の範囲が本願の主旨から逸脱しないこれらの変形及び変更を含むことを理解する。

【符号の説明】

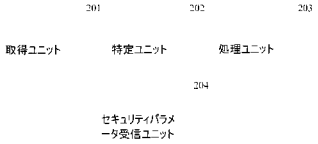
【００８６】

２０１　取得ユニット
２０２　特定ユニット
２０３　処理ユニット
２０４　セキュリティパラメータ受信ユニット

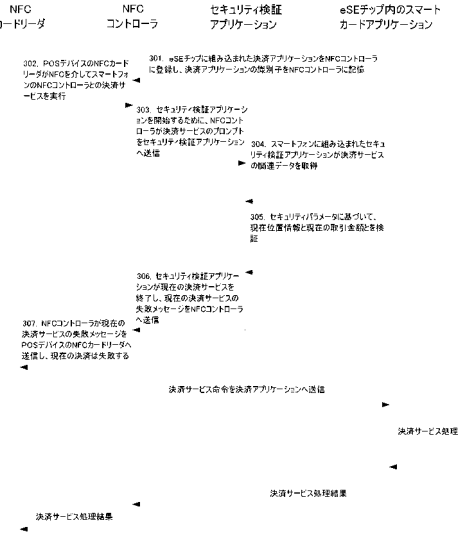
【図１】



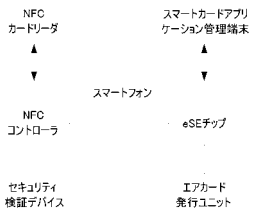
【図２】



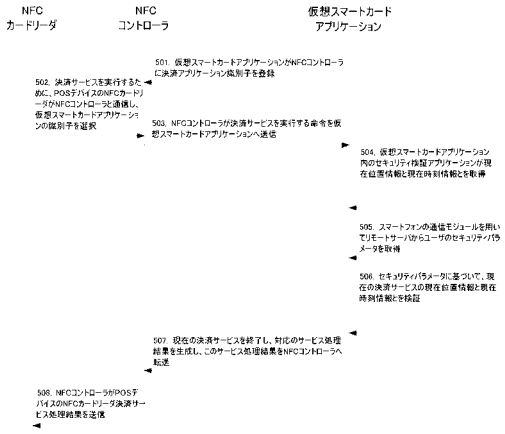
【図３】



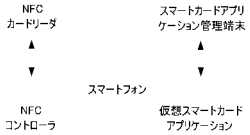
【図４】



【図５】


NFC
カードリーダ
NFC
コントローラ
仮想スマートカード
アプリケーション
501. 仮想スマートカードアプリケーションがNFCコントローラに決済アプリケーション識別子を登録
502. 決済サービスを実行するために、POSデバイスのNFCカードリーダがNFCコントローラに通信し、仮想スマートカードアプリケーションの識別子を選択
503. NFCコントローラが決済サービスを実行する命令を仮想スマートカードアプリケーションへ送信
504. 仮想スマートカードアプリケーション内のセキュリティ強靭アプリケーションが現在位置情報と現在時刻情報を取得
505. スマートフォンの通信モジュールを用いてリモートサーバからユーザのセキュリティパラメータを取得
506. セキュリティパラメータに基づいて、現在の決済サービスの現在位置情報と現在時刻情報とを検証
507. 現在の決済サービスを終了し、対応のサービス処理結果を生成し、このサービス処理結果をNFCコントローラへ転送
508. NFCコントローラがPOSデバイスのNFCカードリーダ決済サービス処理結果を送信

【図６】


NFC
カードリーダ
スマートカードアプリケーション管理端末
スマートフォン
NFC
コントローラ
仮想スマートカード
アプリケーション

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/112265

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/34 (2013.01) i

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)

G06F

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 practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, IEEE: security chip, virtual smart card, terminate, mobile, pay, security, safe, location, operation, transaction, smart, card, terminal, eSE, HCE, limit, quota, virtual

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104751329 A (SHENZHEN ZTE MOBILE TECHNOLOGY CO., LTD.) 01 July 2015 (01.07.2015) description, paragraphs [0078]-[0114]	1-12
X	CN 103065240 A (ZTE CORPORATION) 24 April 2013 (24.04.2013) description, paragraphs [0005] and [0041]-[0073]	1-12
A	CN 104504568 A (WANGYIBAO CO., LTD.) 08 April 2015 (08.04.2015) the whole document	1-12
A	CN 102855560 A (NATIONZ TECHNOLOGIES INC.) 02 January 2013 (02.01.2013) the whole document	1-12
A	US 2010145819 A1 (PANTECH CO., LTD.) 10 June 2010 (10.06.2010) the whole document	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family 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 application or patent 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
09 March 2017	31 March 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LIU, Changyong Telephone No. (86-10) 53318983

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/112265

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104751329 A	01 July 2015	None	
CN 103065240 A	24 April 2013	None	
CN 104504568 A	08 April 2015	None	
CN 102855560 A	02 January 2013	WO 2013000351 A1	03 January 2013
US 2010145819 A1	10 June 2010	KR 20060041346 A	11 May 2006
		US 2006100966 A1	11 May 2006

Form PCT/ISA /210 (patent family annex) (July 2009)

国际检索报告

国际申请号
PCT/CN2016/112265

A. 主题的分类
G06F 21/34(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)
G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)
CNPAT,WPI,EPODOC,CNKI,IEEE:移动，支付，安全，额度，位置，业务，交易，安全芯片，虚拟智能卡，智能卡，终止，mobile，pay，security，safe，location，operation，transaction，smart，card，terminal，eSE，HCE，limit，quota，virtual

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 104751329 A (深圳市中兴移动通信有限公司) 2015年 7月 1日 (2015-07-01) 说明书第[0078]-[0114]段	1-12
X	CN 103065240 A (中兴通讯股份有限公司) 2013年 4月 24日 (2013-04-24) 说明书第[0005]，[0041]-[0073]	1-12
A	CN 104504568 A (网易宝有限公司) 2015年 4月 8日 (2015-04-08) 全文	1-12
A	CN 102855560 A (国民技术股份有限公司) 2013年 1月 2日 (2013-01-02) 全文	1-12
A	US 2010145819 A1 (PANTECH CO., LTD.) 2010年 6月 10日 (2010-06-10) 全文	1-12

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：
"A" 认为不特别相关的表示了现有技术一般状态的文件
"E" 在国际申请日的当天或之后公布的在先申请或专利
"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）
"O" 涉及口头公开、使用、展览或其他方式公开的文件
"P" 公布日先于国际申请日但迟于所要求的优先权日的文件
"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2017年 3月 9日	2017年 3月 31日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 刘长勇 电话号码 (86-10)010-53318983

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/112265

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	104751329	A	2015年 7月 1日	无			
CN	103065240	A	2013年 4月 24日	无			
CN	104504568	A	2015年 4月 8日	无			
CN	102855560	A	2013年 1月 2日	WO	2013000351	A1	2013年 1月 3日
US	2010145819	A1	2010年 6月 10日	KR	20060041346	A	2006年 5月 11日
				US	2006100966	A1	2006年 5月 11日

表 PCT/ISA/210（同族专利附件）（2009年7月）

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ

(74)代理人 100100398
弁理士 柴田 茂夫
(72)発明者 シュ，チャオ
中華人民共和国 ３１００９９，ハンヂョウ，ナンバー１８ ワンタン ロード，フアンロン タイムズ プラザ，ビルディング ビー １７エフ，アンツ パテント チーム内
(72)発明者 ワン，レイ
中華人民共和国 ３１００９９，ハンヂョウ，ナンバー１８ ワンタン ロード，フアンロン タイムズ プラザ，ビルディング ビー １７エフ，アンツ パテント チーム内
(72)発明者 シ，チェンジェ
中華人民共和国 ３１００９９，ハンヂョウ，ナンバー１８ ワンタン ロード，フアンロン タイムズ プラザ，ビルディング ビー １７エフ，アンツ パテント チーム内