(19)日本国特許庁(JP)　　(12)公表特許公報(A)　　(11)公表番号
特表2025-519087
(P2025-519087A)
(43)公表日　令和7年6月24日(2025.6.24)

(51)国際特許分類			FI		テーマコード（参考）
H04W	*8/20*	*(2009.01)*	H04W	8/20	5K067
H04L	*67/51*	*(2022.01)*	H04L	67/51	
H04W	*92/08*	*(2009.01)*	H04W	92/08	
H04W	*12/37*	*(2021.01)*	H04W	12/37	
H04W	*4/50*	*(2018.01)*	H04W	4/50	

審査請求　未請求　予備審査請求　未請求　（全28頁）　最終頁に続く

(21)出願番号　特願2024-568984(P2024-568984)
(86)(22)出願日　令和5年5月11日(2023.5.11)
(85)翻訳文提出日　令和6年11月25日(2024.11.25)
(86)国際出願番号　PCT/EP2023/062659
(87)国際公開番号　WO2023/227386
(87)国際公開日　令和5年11月30日(2023.11.30)
(31)優先権主張番号　2204935
(32)優先日　令和4年5月23日(2022.5.23)
(33)優先権主張国・地域又は機関
フランス(FR)
(81)指定国・地域　AP(BW,CV,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
最終頁に続く

(71)出願人　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　110002077
園田・小林弁理士法人
(72)発明者　ヴィシニェフスカ， カタジナ
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， シー／オー アイデミア フランス
(72)発明者　ウォズニアック， トマーシュ
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， シー／オー アイデミア フランス
(72)発明者　カルピンスキ， パウェル
最終頁に続く

(54)【発明の名称】　セキュアエレメントのサービスプロファイルを管理する方法

(57)【要約】
本発明は、セキュアエレメントのサービスプロファイルを管理する新規な方法であって、中央集中プロファイル管理装置によって実施され、及び複数の処理装置から、同一のサービスに対応するプロファイルデータを受信することと、前記サービスに関連付けられる、受信されたプロファイルデータのうちのプロファイルデータをメモリに保存することと、前記サービスのためのセキュアエレメントのサービスプロファイルの更新をトリガするイベントを検出することと、前記イベントの検出時、前記サービスに関連付けられた保存されたプロファイルデータのうちの最新のプロファイルデータをホスト端末に送信することとを含む方法を提案する。
【選択図】図３

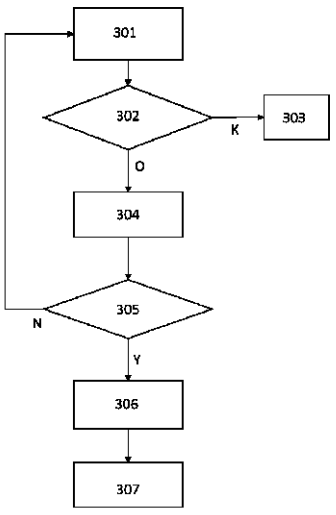

Figure 3

【特許請求の範囲】
【請求項１】
ホスト端末のセキュアエレメントのサービスプロファイルを管理する方法であって、前記ホスト端末の外部の中央集中プロファイル管理装置によって実施され、及び
－　複数の処理装置から、同一のサービスに対応し、且つ前記セキュアエレメントに対して意図されるプロファイルデータを受信することと、
－　前記受信されたプロファイルデータのうちのプロファイルデータをメモリに保存することであって、それぞれの保存されたプロファイルデータは、前記サービスに関連付けて保存される、保存することと、
－　前記サービスのための前記セキュアエレメントのサービスプロファイルの更新をトリガするイベントを検出することと、
－　前記イベントの検出時、前記サービスに関連付けられた前記保存されたプロファイルデータのうちの最新のプロファイルデータを前記ホスト端末に送信することと
を含む方法。
【請求項２】
前記中央集中プロファイル管理装置は、少なくとも１つの他のセキュアエレメントに対して意図される他のプロファイルデータをさらに受信し、各プロファイルデータは、それが意図されるセキュアエレメントの識別子と共に受信され、それぞれの保存されたプロファイルデータは、それが意図される前記セキュアエレメントの前記識別子に関連付けてさらに保存され、前記サービスに関連付けられた前記保存されたプロファイルデータのうちの前記最新のプロファイルデータは、それが意図される前記セキュアエレメントの前記識別子と共に送信される、請求項１に記載の方法。
【請求項３】
それぞれの保存されたプロファイルデータは、それぞれバージョンデータに関連付けられ、前記バージョンデータは、前記中央集中プロファイル管理装置による受信時間又は前記プロファイルデータに関連付けられたプロファイルのバージョン番号であり、前記送信されたプロファイルデータは、前記サービスに関連付けられた前記保存されたプロファイルデータのうち、最新のバージョンデータを有する前記プロファイルデータに対応する、請求項１又は２に記載の方法。
【請求項４】
各プロファイルデータは、それぞれのサービス識別データと共に受信され、前記方法は、
－　受信され、且つメモリに保存された各プロファイルデータについて、前記プロファイルデータと共に受信された前記それぞれのサービス識別データ基づいて、対応するサービスを特定し、且つ前記プロファイルデータを、前記特定された対応するサービスに関連付けて保存すること
をさらに含む、請求項１～３の何れか一項に記載の方法。
【請求項５】
前記受信されたサービス識別データのうちのサービス識別データは、
－　前記処理装置であって、前記プロファイルデータがそれから受信された前記処理装置の識別子、
－　前記処理装置であって、前記関連するプロファイルデータがそれから受信された前記処理装置のネットワークアドレス、
－　前記受信されたプロファイルデータに関連付けられたサービスを管理するサービスプロバイダの識別子、又は
－　前記受信されたプロファイルデータに関連付けられたサービスの識別子
である、請求項４に記載の方法。
【請求項６】
前記サービスに関連付けられたそれぞれの受信されたプロファイルデータについて、
－　前記プロファイルデータに関連付けられたサービスプロバイダを特定し、且つ前記プ

ロファイルデータを、前記特定されたサービスプロバイダに関連付けて保存すること、
－　前記イベントの検出時、データベースに基づいて、前記サービスのための前記セキュアエレメントに関連付けられた現在のサービスプロバイダを特定すること
をさらに含み、前記送信されたプロファイルデータは、前記サービスと、前記サービスのための前記セキュアエレメントに関連付けられた前記現在のサービスプロバイダとに関連付けられた前記保存されたプロファイルデータのうちの最新のプロファイルデータである、請求項１～５の何れか一項に記載の方法。
【請求項７】
前記セキュアエレメントの前記サービスプロファイルの前記更新をトリガする前記イベントの前記検出は、
－　前記ホスト端末又は前記ホスト端末を管理するための管理プラットフォームから、前記所与のサービスに関する識別情報を含む問合せリクエストを受信すること
を含む、請求項１～６の何れか一項に記載の方法。
【請求項８】
前記複数の処理装置のうちの各処理装置は、それぞれの第一の非対称鍵ペアを有し、それぞれの第一の非対称鍵ペアは、秘密鍵及び公開鍵を含み、前記公開鍵は、前記処理装置と前記中央集中プロファイル管理装置との間で共有され、それぞれの受信されたプロファイルデータは、前記発行元の処理装置の前記秘密鍵で署名され、前記方法は、それぞれの受信されたプロファイルデータについて、
－　前記中央集中プロファイル管理装置が前記プロファイルデータの前記署名を前記発行元の処理装置の前記公開鍵に基づいてチェックすることと、
－　前記チェックが成功した場合にのみ、前記受信されたプロファイルデータを前記中央集中プロファイル管理装置の前記メモリに保存することと
をさらに含む、請求項１～７の何れか一項に記載の方法。
【請求項９】
前記中央集中プロファイル管理装置は、第二の非対称鍵ペアを有し、前記第二の非対称鍵ペアは、前記中央集中プロファイル管理装置の秘密鍵と、前記中央集中プロファイル管理装置の公開鍵とを含み、前記第二の非対称鍵ペアの前記公開鍵は、前記中央集中プロファイル管理装置と前記セキュアエレメントとの間で共有され、それぞれの保存されたプロファイルデータについて、前記プロファイルデータは、前記中央集中プロファイル管理装置の前記秘密鍵を使用して署名される、請求項１～８の何れか一項に記載の方法。
【請求項１０】
ホスト端末のセキュアエレメントの通信プロファイルを管理するための中央集中プロファイル管理装置であって、前記ホスト端末の外部にあり、
－　複数の処理装置から、同一のサービスに対応し、且つ前記セキュアエレメントに対して意図されるプロファイルデータを受信することと、
－　前記受信されたプロファイルデータのうちのプロファイルデータをメモリに保存することであって、それぞれの保存されたプロファイルデータは、前記サービスに関連付けて保存される、保存することと、
－　前記サービスのための前記セキュアエレメントのサービスプロファイルの更新をトリガするイベントを検出することと、
－　前記イベントの検出時、前記サービスに関連付けられた前記保存されたプロファイルデータのうちの最新のプロファイルデータを前記ホスト端末に送信することと
を行うように構成される中央集中プロファイル管理装置。
【請求項１１】
セキュアエレメントを有するホスト端末と、前記ホスト端末の外部の中央集中プロファイル管理装置と、複数の処理装置とを含むシステムであって、前記中央集中プロファイル管理装置は、
－　複数の処理装置から、同一のサービスに対応し、且つ前記セキュアエレメントに対して意図されるプロファイルデータを受信すること、

－　前記受信されたプロファイルデータのうちのプロファイルデータをメモリに保存することであって、それぞれの保存されたプロファイルデータは、前記サービスに関連付けて保存される、保存すること、
－　前記サービスのための前記セキュアエレメントのサービスプロファイルの更新をトリガするイベントを検出すること、
－　前記イベントの検出時、前記サービスに関連付けられた前記保存されたプロファイルデータのうちの最新のプロファイルデータを前記ホスト端末に送信すること
を行うように構成され、前記セキュアエレメントは、
－　前記中央集中プロファイル管理装置によって送信された前記プロファイルデータを受信することと、
－　前記受信されたプロファイルデータに基づいて前記サービスプロファイルを更新することと
を行うように構成される、システム。
【請求項１２】
　前記複数の処理装置のうちの各処理装置は、それぞれの第一の非対称鍵ペアを有し、それぞれの第一の非対称鍵ペアは、秘密鍵及び公開鍵を含み、前記公開鍵は、前記処理装置と前記中央集中プロファイル管理装置との間で共有され、それぞれの受信されたプロファイルデータは、前記発行元の処理装置の前記秘密鍵で署名され、前記中央集中プロファイル管理装置は、それぞれの受信されたプロファイルデータについて、
－　前記プロファイルデータの前記署名を前記発行元の処理装置の前記公開鍵に基づいてチェックすることと、
－　前記チェックが成功した場合にのみ、前記受信されたプロファイルデータをメモリに保存することと
を行うようにさらに構成される、請求項１１に記載のシステム。
【請求項１３】
　前記中央集中プロファイル管理装置は、第二の非対称鍵ペアを有し、前記第二の非対称鍵ペアは、前記中央集中プロファイル管理装置の秘密鍵と、前記中央集中プロファイル管理装置の公開鍵とを含み、前記第二の非対称鍵ペアの前記公開鍵は、前記中央集中プロファイル管理装置と前記セキュアエレメントとの間で共有され、それぞれの保存されたプロファイルデータについて、前記プロファイルデータは、前記ホスト端末に送信される前に前記中央集中プロファイル管理装置の前記秘密鍵を使用して署名される、請求項１１又は１２に記載のシステム。
【請求項１４】
　前記複数の処理装置のうちの各処理装置の前記公開鍵は、前記セキュアエレメントと共有され、前記セキュアエレメントは、
－　前記署名されたプロファイルデータの受信時、前記プロファイルデータを発行した前記処理装置の前記公開鍵と、前記中央集中プロファイル管理装置の前記公開鍵とを使用して、前記関連する署名をチェックすることと、
－　前記チェックが成功した場合にのみ、前記受信されたプロファイルデータに基づいて前記サービスプロファイルを更新することと
を行うように構成される、請求項１２に記載のシステム。
【請求項１５】
　コンピュータプログラム製品であって、前記プログラムがプロセッサによって実行されるとき、請求項１～９の何れか一項に記載の方法を実施するための命令を含むコンピュータプログラム製品。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、ホスト端末のセキュアエレメントにおけるサービスプロファイルの管理に関する。

【背景技術】
【０００２】
セキュアエレメント、ＳＥは、ホスト端末（典型的には移動端末）で使用され、信頼できる当局が設定したセキュリティ規則及び要求事項に則してアプリケーション及びデータを安全にホストすることができる、耐タンパー性を有するハードウェアコンポーネント又はプラットフォーム（典型的にはチップ又はチップカード）である。
【０００３】
一層普及しつつあるＳＥの１つのフォームファクタは、組み込み型セキュアエレメント、ｅＳＥである。この組み込み型セキュアエレメントは、一般に、ホスト端末にはんだ付けされる。より最近の１つのフォームファクタは、統合型セキュアエレメント、ｉＳＥである。したがって、セキュアエレメントは、メインプロセッサの一体部分を（例えば、プロセッサの他のコアに追加されるセキュアコアとして）形成する。
【０００４】
セキュアエレメントは、所望のアプリケーションに従ってプログラムされる。
【０００５】
例えば、ｅＳＥ又はｉＳＥは、ホスト移動端末によって実施されるＮＦＣ（近距離無線通信）通信に基づく様々な用途又はサービスに必要なセキュアエレメントを形成し得る。例えば、ＮＦＣの支払サービスでは、ユーザの秘密の銀行情報が必要となり、これは、有利には、あらゆる好ましくないアクセスから保護されるｅＳＥに保存される。これは、公共交通サービスにも当てはまり、ｅＳＥによって入口ゲートでユーザを識別することが可能となる。
【０００６】
セキュアエレメントの他の例は、組み込み型ＵＩＣＣ（ユニバーサル集積回路カード）であり、これは、特に様々な事業者を介した１つ以上の移動電話ネットワーク上で自らを認証するための加入者の資格情報を提供する。例えば、これは、ＳＩＭ（加入者識別モジュール）カードとして構成される。続いて、ｅＵＩＣＣ（組み込み型ＵＩＣＣの略）又はｉＵＩＣＣ（統合型ＵＩＣＣの略）に言及する。ｅＵＩＣＣカードの主な仕様は、ＧＳＭＡ（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ａｓｓｏｃｉａｔｉｏｎ）グループにより、２０１７年６月２７日付の「Ｒｅｍｏｔｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ Ｅｍｂｅｄｄｅｄ ＵＩＣＣ－Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ－Ｖｅｒｓｉｏｎ３．２」という名称のＧＳＭＡ規格ＳＧＰ．０２ｖ３．２で定義されている。
【０００７】
これらのセキュアエレメントの主な利点は、同一のセキュアエレメントを使用して複数のサービスを提供することである。したがって、複数のサービスプロバイダは、データ及び／又はアプリケーションを同じセキュアエレメントにロードして、ユーザがそれぞれのサービスにアクセスできるようにしなければならない。あるユーザのサービスプロバイダに特有のこれらのデータ及び／又はアプリケーションは、サービスプロファイル（以下では単に「プロファイル」ともいう）を形成し、それがセキュアエレメント内に保存される。特に、２０１７年９月１日付のＧＳＭＡ　ＲＳＰ技術仕様バージョン２．２（以下ではＧＳＭＡ　ＳＧＰ．２２）の意味における、モバイル事業者（サービスプロバイダ）に関連付けられ、ユーザに関する情報を含み、それらが前記モバイル事業者の移動電話サービスにアクセスできるようにするプロファイルが知られている。Ｇｌｏｂａｌ Ｐｌａｔｆｏｒｍ Ｃａｒｄ Ｓｐｅｃｉｆｉｃａｔｉｏｎ規格（２０１５年１０月のバージョン２．３）の意味における、公共機関（サービスプロバイダ）に関連付けられ、ユーザに関する情報を含み、それらが前記当局のそれぞれのサービスにアクセスできるようにする構成も知られている。
【０００８】
ＧＳＭＡ規格によれば、これらのプロファイルは、ＬＰＡ（ローカルプロファイル管理）と呼ばれるエンティティによって管理される。ＬＰＡは、ホスト端末のオペレーティン

グシステム又はホスト端末のセキュアエレメント内にあり、通信ネットワーク上でプロファイル管理オペレータ（例えば、ＳＭ－ＤＰ＋、サブスクリプションマネージャデータ準備＋、サブスクリプション管理サーバ）のデータセキュアエレメントとそのエンティティとの間のインタフェースを形成する。これにより、ホスト端末のユーザは、例えば、新規のプロファイルをセキュアエレメントにインストールするか、又はセキュアエレメント内にすでにインストールされているプロファイルをイネーブル、ディスエーブル若しくは削除することが可能となる。

【０００９】

近年、新たなサービスに関連付けられたプロファイルを保存するセキュアエレメントを含む、何万又はさらに何十万もの接続されたデバイスを表すモノのインターネット（ＩｏＴ）の発展に伴い、このようなプロファイルの有効なリモート管理のための解決策を考えることが必要となっている。

【００１０】

特に図１によるシステムが提案されており、サービスプロファイルのリモート管理のための機能は、ホスト端末の外部の、通信ネットワーク内にあるデバイスであるＣＬＰＡ¡によって実施される。

【００１１】

より正確には、図１は、セキュアエレメント１０２、例えばｅＵＩＣＣ及び通信エージェント１０３を含むホスト端末１０１を示す。ホスト端末１０１は、例えば、移動電話機、自動車に組み込まれてその自動車のメーカの情報システムによって遠隔的に管理されるデバイス又は他の任意の種類の接続オブジェクトでもあり得る。セキュアエレメント１０２は、典型的には、１つ以上のプロファイルを保存する。通信エージェント１０３は、ホスト端末１０１のオペレーティングシステム又はホスト端末１０１のセキュアエレメント１０２内にあり、以下で詳述するように、セキュアエレメント１０２と、各種の外部プロファイル管理装置ＣＬＰＡ¡、１０５ａ、１０５ｂ、１０５ｃとの間のインタフェースを形成する。

【００１２】

図１のシステムは、モバイルネットワークのＳＭ－ＤＰ＋（サブスクリプションマネージャデータ準備）サーバ１０４も含み、このサーバは、セキュアエレメント１０２に送信される複数のプロファイルを保存又は受信する。様々な種類のリモートサーバが使用され得、例えばＳＭ－ＤＰ＋サーバ１０４を２つのＳＭ－ＤＰ及びＳＭ－ＳＲサーバの代わりに使用し得る。

【００１３】

セキュアエレメント１０２上に保存されるプロファイルは、複数の外部プロファイル管理装置ＣＬＰＡ¡ １０５ａ、１０５ｂ、１０５ｃによって管理され、これらは、ホスト端末１０１内にあるのではなく、ネットワーク内のリモートデバイス（又はサーバ）である。これに関して、外部プロファイル管理装置ＣＬＰＡ¡ １０５ａ、１０５ｂ、１０５ｃは、それらにそれぞれ関連付けられたサービスのために、２０１６年１０月１４日付の「ＲＳＰ Ｔｅｃｈｎｉｃａｌ Ｓｐｅｃｉｆｉｃａｔｉｏｎ－Ｖｅｒｓｉｏｎ２．０」という名称のＧＳＭＡ規格ＳＧＰ．２２ ｖ２．０で定義されているＬＰＡエンティティの代わりにプロファイル管理機能を実施する。

【００１４】

外部プロファイル管理装置ＣＬＰＡ¡ １０５ａ、１０５ｂ、１０５ｃの各々は、そのため、一方ではＳＭ－ＤＰ＋サーバ１０４と通信して、セキュアエレメント１０２のプロファイルの管理に関する１つ（以上）のコマンド（例えば、プロファイルをインストール又は削除するコマンド）を取得し、他方ではホスト端末１０１の通信エージェント１０３と通信して、前記プロファイル管理コマンドをそれに送信するように構成される。通信エージェント１０３は、プロファイル管理コマンドをセキュアエレメント１０２に送信するようにさらに構成される。

【００１５】

このようなシステムは、仏国特許出願第３１１１０４２号明細書に詳細に記載されている。

【００１６】

しかしながら、同一のセキュアエレメントに関連付けられたサービスの数が増え続け、したがって外部プロファイル管理装置の数も一層増えることを考えると、このようなシステムは、完全に満足できるものではない。

【００１７】

実際に、外部プロファイル管理装置は、ホスト端末と（直接又は端末を管理する他の管理プラットフォームを介して）通信するため、セキュアエレメントに安全にアクセスするために、外部プロファイル管理装置をホストするプレミスが認証機関によって認証される必要がある。しかしながら、このような認証は、無視できないほどのコストがかかり、必ずしも全てのサービスプロバイダがそれに投資することを望むわけではない。

【００１８】

さらに、このシステムでは、あるサーバのための外部プロファイル管理装置の展開（例えば、使用されなくなったか、又はプロファイルの更新、外部プロファイル管理装置の交換などができない外部プロファイル管理装置）を有効に管理することができない。例えば、所与のサービスに関して、新たなサービスプロバイダへの移行は、このサービスに関連付けられたプロファイル管理装置の変更を伴う。セキュアエレメントには、この展開が知らされず、新しいプロファイル管理装置のアドレスがわからない。現在、既存のサービスに関する新たな外部プロファイル管理装置の切り換えを可能にするメカニズムは、提供されていない。

【発明の概要】

【００１９】

したがって、セキュアエレメント内に保存されたサービスプロファイルの管理を改良する必要がある。

【００２０】

本発明の第一の態様は、ホスト端末のセキュアエレメントのサービスプロファイルを管理する方法であって、ホスト端末の外部の中央集中プロファイル管理装置によって実施される方法に関する。この方法は、

－　複数の処理装置から、同一のサービスに対応し、且つそのセキュアエレメントに対して意図されるプロファイルデータを受信することと、

－　受信されたプロファイルデータのうちのプロファイルデータをメモリに保存することであって、それぞれの保存されたプロファイルデータは、前記サービスに関連付けて保存される、保存することと、

－　前記サービスのためのセキュアエレメントのサービスプロファイルの更新をトリガするイベントを検出することと、

－　前記イベントの検出時、前記サービスに関連付けられた保存されたプロファイルデータのうちの最新のプロファイルデータをホスト端末に送信することと

を含み得る。

【００２１】

「プロファイルデータ」は、プロファイルをセキュアエレメントにインストールするか又は更新するための、サービスプロファイルに関連付けられた１つ以上のデータを意味すると理解されたい。「処理装置」は、サービスプロバイダによって管理され、サービスプロバイダによって管理される１つ以上のサービスに関連付けられたプロファイルデータがそれに保存される外部デバイス又はサーバであり得る。以下では、処理装置は、「プロファイル管理装置」とも呼ばれる。「サービスプロファイルの更新をトリガするイベント」は、中央集中プロファイル管理装置２０６に保存されたプロファイルデータのうちのプロファイルデータを検索し、送信することにつながるあらゆるイベントを意味すると理解されたい。例えば、中央集中プロファイル管理装置は、セキュアエレメントから問合せリクエストを受信し得る（「プルモード」）か、又は所定の時間にプロファイルデータが入手

可能であるか否かをチェックして、適切な場合にそれをセキュアエレメントに送信するように構成され得る。

【００２２】

上述の方法により、有利には、同一のサービスに対応する複数のプロファイルデータが少なくとも２つの異なる処理装置から受信される事例を管理することが可能となり、これは、図１のアーキテクチャでは不可能であった。さらに、中央集中管理装置が、ホスト端末の通信相手となる唯一のエンティティとして存在することにより、認証の問題を排除することができる。

【００２３】

１つ以上の実施形態では、送信されたプロファイルデータは、中央集中プロファイル管理装置によってホスト端末の通信エージェントに送信され得、通信エージェントは、前記プロファイルデータをセキュアエレメントに転送するように構成される。

【００２４】

１つ以上の実施形態では、中央集中プロファイル管理装置は、少なくとも１つの他のセキュアエレメントに対して意図される他のプロファイルデータをさらに受信し得、各プロファイルデータは、それが意図されるセキュアエレメントの識別子と共に受信され、それぞれの保存されたプロファイルデータは、それが意図されるセキュアエレメントの識別子に関連付けてさらに保存され、前記サービスに関連付けられた保存されたプロファイルデータのうちの最新のプロファイルデータは、それが意図されるセキュアエレメントの識別子と共に送信される。

【００２５】

換言すれば、中央集中プロファイル管理装置は、同じホスト端末に属するか又は属さない複数のセキュアエレメントのプロファイルを管理するように構成され得る。この場合、処理装置から受信された各プロファイルデータは、それが意図されるセキュアエレメントの識別子を含み得る。

【００２６】

さらに、それぞれの保存されたプロファイルデータは、それぞれバージョンデータに関連付けられ得、バージョンデータは、中央集中プロファイル管理装置による受信時間を表すか、又はプロファイルデータに関連付けられたプロファイルのバージョン番号であり、送信されたプロファイルデータは、前記サービスに関連付けられた保存されたプロファイルデータのうち、最新のバージョンデータを有するプロファイルデータに対応する。

【００２７】

１つ以上の実施形態では、各プロファイルデータは、それぞれのサービス識別データと共に受信され得、この方法は、

－　受信され、且つメモリに保存された各プロファイルデータについて、前記プロファイルデータと共に受信されたそれぞれのサービス識別データ基づいて、対応するサービスを特定し、且つプロファイルデータを、特定された対応するサービスに関連付けて保存すること

をさらに含み得る。

【００２８】

例えば、受信されたサービス識別データのうちのサービス識別データは、

－　処理装置であって、プロファイルデータがそれから受信された処理装置の識別子、

－　処理装置であって、プロファイルデータがそれから受信された処理装置のネットワークアドレス、

－　受信されたプロファイルデータに関連付けられたサービスを管理するサービスプロバイダの識別子、又は

－　受信されたプロファイルデータに関連付けられたサービスの識別子

であり得る。

【００２９】

各プロファイルデータは、このように、それが対応するサービスを特定できるようにす

る情報と共に受信される。そのため、プロファイルデータを保存する際、前記データと、対応するサービスとを関連付けることが可能となる。

【００３０】

１つ以上の実施形態では、この方法は、サービスに関連付けられたそれぞれの受信されたプロファイルデータについて、

－　そのプロファイルデータに関連付けられたサービスプロバイダを特定し、且つそのプロファイルデータを、特定されたサービスプロバイダに関連付けて保存すること、

－　前記イベントの検出時、データベースに基づいて、前記サービスのためのセキュアエレメントに関連付けられた現在のサービスプロバイダを特定すること

をさらに含み、送信されたプロファイルデータは、前記サービスと、前記サービスのためのセキュアエレメントに関連付けられた現在のサービスプロバイダとに関連付けられた保存されたプロファイルデータのうちの最新のプロファイルデータである。

【００３１】

「現在のサービスプロバイダ」は、トリガイベントが検出された時点でのサービスのプロバイダを意味すると理解されたい。実際に、プロファイルデータの少なくとも幾つかが受信されてからトリガイベントが検出されるまでの間、対象のサービスプロバイダは、変わっている場合がある。この場合、端末に送信されるプロファイルデータは、中央集中プロファイル管理装置内に保存され、サービスの現在のプロバイダに関連付けられたプロファイルデータのうちから選択される。

【００３２】

１つ以上の実施形態では、セキュアエレメントのサービスプロファイルの更新をトリガするイベントの検出は、

－　ホスト端末又はホスト端末を管理するための管理プラットフォームから、前記所与のサービスに関する識別情報を含む問合せリクエストを受信すること

を含み得る。

【００３３】

このような実施形態は、「プル」モードに対応する。ホスト端末は、所与のサービスに対応する、そのサービスに関連付けられたプロファイルの新バージョンが入手可能であるか否かを尋ねるリクエストを送信し、可能な場合にそれを取得する。図１のシステムでは、問合せリクエストの送信先の処理装置のネットワークアドレスが変更されると、このリクエストは、失われるか又は誤ったエンティティに送信される。実際に、ネットワークアドレス又はプロバイダの変更を動的に管理するものは何も提供されていない。本発明では、この問題がもはや生じず、なぜなら、全ての問合せリクエストは、そのネットワークアドレスが固定されている同一のエンティティに送信されるためである。

【００３４】

問合せリクエストは、セキュアエレメントの識別子をさらに含み得る。

【００３５】

１つ以上の実施形態では、複数の処理装置のうちの各処理装置は、それぞれの第一の非対称鍵ペアを有し得、それぞれの第一の非対称鍵ペアは、秘密鍵及び公開鍵を含み、公開鍵は、処理装置と中央集中プロファイル管理装置との間で共有される。それぞれの受信されたプロファイルデータは、発行元の処理装置の秘密鍵で署名され得る。この方法は、それぞれの受信されたプロファイルデータについて、

－　中央集中プロファイル管理装置がプロファイルデータの署名を発行元の処理装置の公開鍵に基づいてチェックすることと、

－　チェックが成功した場合にのみ、受信されたプロファイルデータを中央集中プロファイル管理装置のメモリに保存することと

をさらに含み得る。

【００３６】

発行元の処理装置は、プロファイルデータがそれから受信された処理装置を意味すると理解されたい。処理装置の署名のこのようなチェックにより、プロファイルデータが、実

際に正規の信頼できるエンティティによって発行されたことと、その送信と受信との間にそれらが破壊されていないこととをチェックすることができる。幾つかの実施形態では、処理装置の公開鍵は、デジタル証明書において中央集中プロファイル管理装置にブロードキャストされ得る。

【００３７】

さらに、中央集中プロファイル管理装置は、第二の非対称鍵ペアを有し得、第二の非対称鍵ペアは、中央集中プロファイル管理装置の秘密鍵と、中央集中プロファイル管理装置の公開鍵とを含み、第二の非対称鍵ペアの公開鍵は、中央集中プロファイル管理装置とセキュアエレメントとの間で共有される。それぞれの保存されたプロファイルデータについて、前記プロファイルデータは、中央集中プロファイル管理装置の秘密鍵を使用して署名され得る。

【００３８】

この署名は、上述の第一の署名に追加され得る。この実施形態によれば、したがって、プロファイルデータは、二重に、すなわち第一に発行元の処理装置の秘密鍵で、第二に中央集中プロファイル管理装置の秘密鍵で署名される。第二の非対称鍵ペアの公開鍵（したがって中央集中プロファイル管理の公開鍵）は、第二のデジタル証明書においてセキュアエレメントに送信され得る。この実施形態では、処理装置の公開鍵もセキュアエレメントに通信されなければならない（例えば、各処理装置の証明書は、中央集中プロファイル管理装置からセキュアエレメントに送信され得、この証明書は、場合により中央集中プロファイル管理装置の秘密鍵を使用して署名され得る）。これにより、セキュアエレメントは、それがプロファイルデータを受信したとき、それが処理装置によって送信されて以降、変更されていないことをチェックし、その経路（発行元の処理装置－中央集中プロファイル管理装置－セキュアエレメント）を「追跡」することができる。

【００３９】

本発明の他の態様は、ホスト端末のセキュアエレメントの通信プロファイルを管理するための中央集中プロファイル管理装置であって、ホスト端末の外部にある中央集中プロファイル管理装置に関する。中央集中プロファイル管理装置は、

－　複数の処理装置から、同一のサービスに対応し、且つそのセキュアエレメントに対して意図されるプロファイルデータを受信することと、

－　受信されたプロファイルデータのうちのプロファイルデータをメモリに保存することであって、それぞれの保存されたプロファイルデータは、前記サービスに関連付けて保存される、保存することと、

－　前記サービスのためのセキュアエレメントのサービスプロファイルの更新をトリガするイベントを検出することと、

－　前記イベントの検出時、前記サービスに関連付けられた保存されたプロファイルデータのうちの最新のプロファイルデータをホスト端末に送信することと

を行うように構成され得る。

【００４０】

本発明の他の態様は、セキュアエレメントを有するホスト端末と、ホスト端末の外部の中央集中プロファイル管理装置と、複数の処理装置とを含むシステムに関し、中央集中プロファイル管理装置は、

－　複数の処理装置から、同一のサービスに対応し、且つそのセキュアエレメントに対して意図されるプロファイルデータを受信することと、

－　受信されたプロファイルデータのうちのプロファイルデータをメモリに保存することであって、それぞれの保存されたプロファイルデータは、前記サービスに関連付けて保存される、保存することと、

－　前記サービスのためのセキュアエレメントのサービスプロファイルの更新をトリガするイベントを検出することと、

－　前記イベントの検出時、前記サービスに関連付けられた保存されたプロファイルデータのうちの最新のプロファイルデータをホスト端末に送信することと

を行うように構成され得る。
【００４１】
セキュアエレメントは、
－　中央集中プロファイル管理装置によって送信されたプロファイルデータを受信することと、
－　受信されたプロファイルデータに基づいてサービスプロファイルを更新することと
を行うように構成され得る。
【００４２】
さらに、複数の処理装置のうちの各処理装置は、それぞれの第一の非対称鍵ペアを有し得、それぞれの第一の非対称鍵ペアは、秘密鍵及び公開鍵を含み、公開鍵は、処理装置と中央集中プロファイル管理装置との間で共有される。それぞれの受信されたプロファイルデータは、発行元の処理装置の秘密鍵で署名され得、中央集中プロファイル管理装置は、それぞれの受信されたプロファイルデータについて、
－　プロファイルデータの署名を発行元の処理装置の公開鍵に基づいてチェックすることと、
－　チェックが成功した場合にのみ、受信されたプロファイルデータをメモリに保存することと
を行うようにさらに構成され得る。
【００４３】
１つ以上の実施形態では、中央集中プロファイル管理装置は、第二の非対称鍵ペアを有し得、第二の非対称鍵ペアは、中央集中プロファイル管理装置の秘密鍵と、中央集中プロファイル管理装置の公開鍵とを含み、第二の非対称鍵ペアの公開鍵は、中央集中プロファイル管理装置とセキュアエレメントとの間で共有される。それぞれの保存されたプロファイルデータについて、前記プロファイルデータは、ホスト端末に送信される前に中央集中プロファイル管理装置の秘密鍵を使用して（場合により第一の署名に加えて）署名され得る。
【００４４】
複数の処理装置のうちの各処理装置の公開鍵は、セキュアエレメントと共有され得、セキュアエレメントは、
－　署名されたプロファイルデータの受信時、そのプロファイルデータを発行した処理装置の公開鍵と、中央集中プロファイル管理装置の公開鍵とを使用して、関連する署名をチェックすることと、
－　チェックが成功した場合にのみ、受信されたプロファイルデータに基づいてサービスプロファイルを更新することと
を行うように構成され得る。
【００４５】
本発明の他の態様は、コンピュータプログラム製品であって、このプログラムがプロセッサによって実行されるとき、上記の方法を実施するための命令を含むコンピュータプログラム製品に関する。
【００４６】
本発明の他の態様は、非一時的コンピュータ可読媒体であって、中央集中プロファイル管理装置のプロセッサによって実行されるとき、中央集中プロファイル管理装置に上記の方法を実施させるプログラムを記憶する非一時的コンピュータ可読媒体に関する。
【００４７】
本発明による方法の少なくとも幾つかは、コンピュータによって実施され得る。その結果、本発明は、完全にハードウェアの形態の実施形態、完全にソフトウェア（ファームウェア、常駐ソフトウェア、マイクロコード等を含む）の形態の実施形態又はソフトウェア及びハードウェアの態様を含む実施形態の形態をとり得、これらの全てを本明細書では「回路」、「モジュール」又は「システム」と呼び得る。本発明は、媒体に組み込まれたコンピュータによって使用可能なプログラムコードも有する何れの有形表現媒体にも組み込

まれるコンピュータプログラム製品の形態をさらにとり得る。
【００４８】
本発明は、ソフトウェアで実施され得ることを考えると、本発明は、任意の適切な媒体上でプログラム可能装置に供給されるコンピュータ可読コードの形態で組み込まれ得る。有形又は非一時的媒体は、ハードドライブリーダ、磁気テープデバイス又は半導体メモリデバイスなどの記憶媒体を含み得る。一時媒体は、信号、例えば電気信号、電子信号、光信号、音響信号、磁気信号又は電磁信号、例えばマイクロ波又はＲＦ（無線周波数）信号を含み得る。
【００４９】
本発明の他の特定の具体的な特徴及び利点は、本発明の幾つかの限定的な例示的実施形態を示す添付図によって図解される以下の説明からより明確に明らかになるであろう。
【図面の簡単な説明】
【００５０】
【図１】外部プロファイル管理装置を含む先行技術の通信システムの一例を示す。
【図２】本発明の１つ以上の実施形態による中央集中プロファイル管理装置を含む通信システムの一例を示す。
【図３】本発明の１つ以上の実施形態によるサービスプロファイルの管理方法のフローチャートの一例を示す。
【図４】本発明の１つの特定の実施形態によるサービスプロファイル管理方法のステップを示す。
【図５】図４に示される実施形態の１つの代替的実施形態を示す。
【図６】本発明の１つ以上の実施形態によるトランザクションを実施するための中央集中プロファイル管理装置の一例を示す。
【発明を実施するための形態】
【００５１】
本発明は、プロファイルデータを様々なサービスプロバイダから受信し、セキュアエレメントを組み込むホスト端末に再送信するように構成され、プロファイルデータは、このセキュアエレメントの各種のサービスに対応するプロファイルをインストール又は更新するものである外部プロファイル管理装置（又はサーバ）を組み込むように先行技術のアーキテクチャを改良することを提案する。換言すれば、プロファイルデータは、様々なプロバイダに関連付けられたサーバからホスト端末に直接送信されることがなくなり、代わりに中央集中プロファイル管理装置と呼ばれるものに送信され、それが前記プロファイルデータの少なくとも幾つかをホスト端末に再送信する。後に詳述するように、このようなアーキテクチャにより、同一のサービスに対応するデータが複数のサーバによって（例えば、サービスプロバイダの変更に関して）送信される状況を効率的に管理することが可能となる。提案されるシステムによれば、さらに、各プロバイダがサービスの存在するプレミスの各々についての証明書を有する必要性をなくすことができる。実際に、データは、中央集中プロファイル管理装置から送信されるため、それをホストするプレミスのみに証明書が必要となる。
【００５２】
図２は、本発明の１つ以上の実施形態による中央集中プロファイル管理装置を含む通信システムの一例を示す。
【００５３】
図２に示されるシステムは、ホスト端末２０１を含み、これは、セキュアエレメント２０２、例えばｅＵＩＣＣ及び通信エージェント（図２ではＤＡＧで示される）２０３を含む。ホスト端末２０１は、例えば、移動電話、自動車に搭載され、その自動車のメーカの情報システムによって遠隔的に管理されるデバイス又は他の何れかの種類の接続されたオブジェクトであり得る。セキュアエレメント２０２は、典型的には、１つ以上のプロファイル（「サービスプロファイル」又は「サブスクリプション」とも呼ばれる）を保存する。各プロファイルは、「サービスプロバイダ」と呼ばれる事業者によって提供される所与

のサービスに関連付けられる。各サービスプロバイダは、プロファイル管理装置（又はサーバ）ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃ（ＤＰＡは、遠隔プロファイルアドミニストレータの略であるが、他の何れの用語も使用され得る）を有し得、このサービスに関連付けられたプロファイルがそれに保存される。例えば、プロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃは、対象のサービスに関するプロファイルの最新のバージョンと、場合によりこのプロファイルの過去のバージョンとを保存し得る（例えば、サービスプロファイルの入手可能な新バージョンの各々が過去のバージョンに加えて又はその代わりにプロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃに保存され得る）。

【００５４】

通信エージェント２０３は、ホスト端末２０１のオペレーティングシステム内又はホスト端末２０１のセキュアエレメント２０２内にあり、セキュアエレメント２０２と、後に詳述する機能を有する中央集中プロファイル管理装置（図２ではＴＳで示される）との間のインタフェースを形成する。代替形態として、ホスト端末は、端末を管理するためのリモート管理プラットフォーム２０４（デバイス管理プラットフォームの略のＤＭＰで示される）によって管理され得る。この場合、通信エージェント２０３は、セキュアエレメント２０２と、端末を管理するためのリモート管理プラットフォーム２０４との間のインタフェースを形成する。

【００５５】

図２のシステムは、中央集中プロファイル管理装置ＴＳ　２０６をさらに含む。この中央集中プロファイル管理装置２０６は、外部のプロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃから、それにより準備されたサービスプロファイルに関連付けられたデータ（「プロファイルデータ」と呼ばれる）を受信するように構成される。プロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃによって送信されるプロファイルデータは、完全なプロファイル（すなわちプロファイルを構成するデータセット）、例えばインストールされる新規プロファイル又はすでにセキュアエレメント２０２にインストールされているプロファイルを更新するためのデータであり得る。単純化するために、プロファイルの「更新」という用語は、以下では、セキュアエレメント２０２への新プロファイルのインストール及びセキュアエレメント２０２にすでにインストールされているプロファイルの更新の両方を指すために使用される。

【００５６】

例えば、各外部プロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃは、中央集中プロファイル管理装置２０６に対し、それらが実施するサービスのための１つ以上のプロファイルに対応するプロファイルデータを送信し得る。

【００５７】

１つ以上の実施形態では、プロファイルデータは、プロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃにより、それらが意図されるセキュアエレメント２０２の識別子に関連付けられた中央集中プロファイル管理装置２０６に送信され得る。実際には、図２には１つのセキュアエレメント２０２のみが示されているが、中央集中プロファイル管理装置２０６は、複数のホスト端末のセキュアエレメント及び／又は同一のホスト端末の複数のセキュアエレメントのためのプロファイルデータを受信し得る。この場合、中央集中プロファイル管理装置２０６は、それが受信するプロファイルデータが意図されるサービスエレメントを知る必要がある。

【００５８】

さらに、１つ以上の実施形態では、プロファイルデータは、プロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃによって中央集中プロファイル管理装置２０６にサービス識別データに関連付けて送信され得る。このサービス識別データにより、中央集中プロファイル管理装置２０６は、受信されたプロファイルデータが対応するサービスを特定することができる。サービス識別データは、例えば、

－　そのプロファイルデータの送信元である外部プロファイル管理装置ＤＰＡ¡　２０５

ａ、２０５ｂ、２０５ｃの識別子、
－　そのプロファイルデータの送信元である外部プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃのネットワークアドレス（例えば、ＩＰアドレス）、
－　そのプロファイルデータの送信元である外部プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃを管理するサービスプロバイダの識別子、又は
－　受信されたプロファイルデータに関連付けられたサービスの識別子
であり得る。

【００５９】

最初の３つの例では、中央集中プロファイル管理装置２０６は、識別子又はアドレスを受信されたプロファイルデータに関連付けられたサービスの識別子に関連付けるテーブル（例えば、中央集中プロファイル管理装置２０６のメモリ内に保存されている）又はデータベースへのアクセスをさらに有し得る。中央集中プロファイル管理装置２０６は、このテーブルを使用して、受信されたデータに関連付けられたサービスを、受信されたサービス識別データに基づいて特定することができる。当然のことながら、サービス識別データによって受信されたプロファイルデータに関連付けられたサービスを特定できるのであれば、上述のもの以外の例も考えられる。

【００６０】

中央集中プロファイル管理装置２０６は、プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃからプロファイルデータを受信すると、それをそれが関連付けられるサービスに関連付けてメモリ内に保存する。１つ以上の実施形態では、この関連付けは、サービス識別子に基づいて実施され得る。

【００６１】

同一のサービスについて、複数のプロファイルデータが異なるプロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃから受信され得る点に留意されたい。このような状況は、例えば、ユーザがサービスプロバイダを変更したときに起こり得る。例えば、プロバイダの変更前に、第一のプロファイル管理装置（例えば、ＤＰＡ$_1$　２０５ａ）は、所与のサービスに関連付けられた第一のプロファイルデータを送信し得、プロバイダの変更後、第二のプロファイル管理装置（例えば、ＤＰＡ$_2$　２０５ｂ）は、同じサービスに関連付けられた第二のプロファイルデータを送信し得る。

【００６２】

１つ以上の実施形態では、各プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃは、それぞれの非対称鍵ペアを有し、各ペアは、公開鍵$K_{CPA,pub,i}$及び秘密鍵$K_{CPA,priv,i}$で形成される。各プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃの公開鍵$K_{CPA,pub,i}$は、中央集中プロファイル管理装置２０６と共有される（すなわち、中央集中プロファイル管理装置２０６には、各プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃの公開鍵$K_{CPA,pub,i}$がわかる）。幾つかの実施形態では、プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃの公開鍵$K_{CPA,pub,i}$は、認証機関によって発行されたデジタル証明書においてプロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃに送信され得る。プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃは、その後、中央集中プロファイル管理装置２０６に対して、プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃの秘密鍵$K_{CPA,priv,i}$を使用して生成された署名で署名されたプロファイルデータを送信し得る。中央集中プロファイル管理装置２０６は、プロファイルデータを受信すると、その署名をチェックするが、これは、すなわち、このデータ及びそれがそのプロファイルデータをそれから受信したプロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃの公開鍵$K_{CPA,pub,i}$に基づいて署名を計算し、その後、２つの署名を比較する。２つの署名が一致すると、これは、プロファイルデータが実際に「正規の」エンティティから送信されたことを示し、そのデータが中央集中プロファイル管理装置２０６のメモリに保存される。２つの署名が一致しなければ、そのプロファイルデータが削除され、中央集中プロファイル管理装置２０６のメモリに保存されない。これにより

、受信データの完全性及び出所（トレーサビリティ）をチェックすることが可能となる。

【００６３】

次に、中央集中プロファイル管理装置２０６は、それがメモリ内に保存したプロファイルデータのうちの１つ以上のプロファイルデータを通信エージェント２０３に直接送信し得る（例えば、エージェント２０３から中央集中プロファイル管理装置２０６への直接リクエスト後）か、又は変形形態として、端末を管理するためのリモート管理プラットフォーム２０４に送信し得る（このリモート管理プラットフォームは、これらを通信エージェント２０３に送信する）。通信エージェント２０３は、その後、１つ以上のプロファイルデータをセキュアエレメント２０２に転送し、それが１つ以上の対応するプロファイルをインストール又は更新し得る。プロファイルデータは、セキュアエレメントが、更新されるプロファイルを特定することができようにサービス識別データに関連付けて（詳細に前述したとおり）、且つ／又はそのプロファイルデータがそれから送信されたプロファイル管理装置ＤＰＡ$_i$ ２０５ａ、２０５ｂ、２０５ｃに関連付けて送信され得る（これは、データが後述のように発行元のプロファイル管理装置の秘密鍵$K_{CPA,priv,i}$を使用して署名されているときに特に有利であり、それにより、セキュアエレメントは、発行元のプロファイル管理装置の公開鍵$K_{CPA,pub,i}$を使用して署名をチェックすることができる）。代替的又は追加的に、プロファイルデータはセキュアエレメントの識別子に関連付けて送信され得る（これは、端末が複数のセキュアエレメント２０２を含むときに特に有利であり、それにより、通信エージェント２０３は、このデータを、更新が関わるプロファイルを含むセキュアエレメント２０２に送信する）。

【００６４】

前述のように、中央集中プロファイル管理装置２０６は、同一のサービスに関連付けられる、複数のそれぞれのプロファイル管理装置ＤＰＡ$_i$ ２０５ａ、２０５ｂ、２０５ｃから受信された複数のプロファイルデータを保存し得る。したがって、中央集中プロファイル管理装置２０６は、所与のサービスについて、このサービスに関連付けられた何れのプロファイルデータを通信エージェント２０３又は端末を管理するためのリモート管理プラットフォーム２０４に送信すべきかがわかっている必要があり得る。１つ以上の実施形態では、所与のサービスについて送信されるのは、このサービスに関連付けられた保存されたプロファイルデータのうちの最新のプロファイルデータである。例えば、それぞれの保存されたプロファイルデータについて、中央集中プロファイル管理装置２０６によるその受信日又はこの日付を表す何れかの情報を記録することが可能であり、送信されるプロファイルデータは、その受信日が最新のもの（すなわち最後に受信されたプロファイルデータ）である。代替形態として、それぞれの保存されたプロファイルデータは、対応するプロファイルのバージョン番号と共に記録され得、送信されるプロファイルデータは、最新バージョンに対応するものである。

【００６５】

中央集中プロファイル管理装置２０６が複数のセキュアエレメントのためのプロファイルを管理する場合、プロファイルデータは、そのプロファイルデータが意図されるサービスエレメントの識別子に関連付けてさらに保存され得、送信されるプロファイルデータは、このサービス及びセキュアエレメント２０２の識別子に関連付けられた保存されたプロファイルデータのうちの最新のプロファイルであり得る。代替形態として、プロファイルデータは、関連するサービスのプロバイダの識別子と共に送信され得、中央集中プロファイル管理装置２０６は、セキュアエレメントを、ユーザがサブスクリプションを登録したサービスプロバイダのリストに関連付けるテーブル又はデータベースへのアクセスを有し得る。送信されるプロファイルデータは、所与のサービスについて保存され、セキュアエレメント２０２に関連付けられたこのサービスのプロバイダによって提供されるプロファイルデータのうちの最新のプロファイルデータであり得る。他の代替形態によれば、中央集中プロファイル管理装置２０６のメモリは、サービスプロバイダに従ってメモリエリアに仕切られ得、各メモリエリアは、それぞれのプロバイダに対応し、セキュアエレメントがそのプロファイルの１つの更新を検索するリクエストを送信すると（後に詳述する「プ

ル」モード）、これは、それに応答して、ホスト端末２０１のユーザがサブスクリプションを登録したサービスプロバイダに関連付けられたメモリエリア内に保存されたプロファイルデータのうちのプロファイルデータを受信する。この目的のために、ホスト端末２０１のユーザがサブスクリプションを登録したサービスプロバイダに関連付けられたメモリエリアのそれぞれのアドレスを指し示すポインタを使用することが可能である。

【００６６】

１つ以上の実施形態では、中央集中プロファイル管理装置２０６は、非対称鍵ペアを有し、このペアは、公開鍵$K_{TS,pub}$及び秘密鍵$K_{TS,priv}$で形成される。中央集中プロファイル管理装置２０６の公開鍵$K_{TS,pub}$は、セキュアエレメント２０２と共有される。幾つかの実施形態では、中央集中プロファイル管理装置２０６の公開鍵$K_{TS,pub}$は、認証機関によって中央集中プロファイル管理装置２０６に対して発行されるデジタル証明書において送信され得る。中央集中プロファイル管理装置２０６は、その後、プロファイルデータを（場合により発行元のプロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃの秘密鍵$K_{CPA,priv,i}$を使用して事前に署名されている）をその秘密鍵$K_{TS,priv}$で署名して、署名された（場合により二重に署名された）データを、端末を管理するための管理プラットフォーム２０４又は端末２０１の通信エージェント２０３に送信し得る。セキュアエレメント２０２がプロファイルデータを受信すると、それは、したがって、署名をチェックし、すなわち、それは、このデータ及び中央集中プロファイル管理装置２０６の公開鍵$K_{TS,pub}$に基づいて署名を計算し、その後、２つの署名を比較する。これらが一致すれば、セキュアエレメントの対象のプロファイルは、受信されたデータに基づいて更新される。一致しなければ、プロファイルが更新されず、受信されたプロファイルデータが削除される。さらに、セキュアエレメント２０２が受信したデータが二重に署名されている（すなわち発行元のプロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃの秘密鍵$K_{CPA,priv,i}$に基づく署名及び中央集中プロファイル管理装置２０６の秘密鍵$K_{TS,priv}$に基づく署名）場合、セキュアエレメントは、発行元のプロファイル管理装置ＤＰＡ$_I$　２０５ａ、２０５ｂ、２０５ｃの公開鍵$K_{CPA,pub,i}$も知っている必要がある。幾つかの実施形態では、プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５、２０５ｃの公開鍵$K_{CPA,pub,i}$は、中央集中プロファイル管理装置２０６によってセキュアエレメント２０２に（端末を管理するための管理プラットフォーム２０４を介して又は端末２０１の通信エージェント２０３に）送信され得る。さらに、プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃの公開鍵$K_{CPA,pub,i}$は、中央集中プロファイル管理装置２０６によってそのデジタル証明書において送信され得、これは、場合により、中央集中プロファイル管理装置２０６によってその秘密鍵$K_{TS,priv}$を使用して署名される。データが二重に署名されている場合、セキュアエレメント２０２は、２つの署名、すなわち発行元のプロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃの公開鍵$K_{CPA,pub,i}$に基づく一方と、中央集中プロファイル管理装置２０６の公開鍵$K_{TS,pub}$に基づく他方とをチェックする。両方のチェックが成功すれば、セキュアエレメントの対象のプロファイルは、受信データに基づいて更新される。成功しなければ、このプロファイルが更新されず、受信されたプロファイルデータが削除される。この二重チェックにより、第一に、プロファイルデータが「正規の」エンティティからのものであること、第二に、それが発行元の外部プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃに送信されてから変更されていないことをチェックすることが可能となる。

【００６７】

外部プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃは、ホスト端末２０１又は端末を管理するための管理プラットフォーム２０４と直接通信しないことに留意されたい。プロファイルは、外部プロファイル管理装置ＤＰＡ$_i$　２０５ａ、２０５ｂ、２０５ｃから中央集中プロファイル管理装置２０６に送信され、それがこれらをホスト端末２０１に転送する。ホスト端末２０１（又は端末を管理するためのリモート管理プラットフォーム２０４）は、このように、１つのエンティティのみからプロファイルを受信し

、それにより前述のような認証の問題を解決し、サービスプロバイダの変更の管理を容易にする。

【００６８】

実際に、外部プロファイル管理装置ＤＰＡ｛　２０５ａ、２０５ｂ、２０５ｃが存在する全てのプレミスを認証する必要がなくなり、中央集中プロファイル管理装置２０６が存在するプレミスのみを認証すればよく、なぜなら、それがセキュアエレメント２０２にデータを送信する唯一のエンティティであるためである。

【００６９】

さらに、幾つかの実施形態によれば、プロファイルは、「プル」モードにおいて、すなわちセキュアエレメント２０２の要求に応じて取得される。これらの実施形態では、セキュアエレメント２０２は、通信エージェント２０３を介して、プロファイルデータ（新規プロファイル又はあるプロファイルの新バージョンに対応）が入手可能であるか否かを確認する問合せリクエストを送信する。図１のシステムでは、このリクエストは、対象のプロファイルに関連付けられたサービスプロバイダの外部プロファイル管理装置ＣＬＰＡ｛１０５ａ、１０５ｂ、１０５ｃに送信される。しかしながら、ユーザがサービスプロバイダを変更する場合又はサービスプロバイダが外部プロファイル管理装置ＣＬＰＡ｛　１０５ａ、１０５ｂ、１０５ｃを変更する場合があり得る。このような場合、問合せリクエストは、正しい外部プロファイル管理装置ＣＬＰＡ｛　１０５ａ、１０５ｂ、１０５ｃに送信されない場合がある。実際に、セキュアエレメント２０２において、サービスプロバイダの変更又は所与のサービスのサービスプロバイダのサーバのアドレスを動的に管理するためのメカニズムは、提供されない。図２のシステムでは、この問題が生じなくなり、なぜなら、（図４及び５に関して詳述するように）問合せリクエストは、そのネットワークアドレスが固定されている中央集中プロファイル管理装置２０６に送信されるためである。プロバイダは、端末２０１にとって明白に変更され、問合せリクエストが誤ったエンティティに送信されることがあり得ない。

【００７０】

図３は、本発明の１つ以上の実施形態によるサービスプロファイルの管理方法のフローチャートの一例を示す。第一のステップ３０１では、中央集中プロファイル管理装置２０６は、所与のサービスに関するプロファイルデータを受信する。

【００７１】

任意選択により、このプロファイルデータは、そのプロファイルデータがそれから受信されたプロファイル管理装置ＤＰＡ｛　２０５ａ、２０５ｂ、２０５ｃの秘密鍵$K_{CPA,priv,i}$を使用して署名される。署名は、その後、そのプロファイルデータがそれから受信されたプロファイル管理装置ＤＰＡ｛　２０５ａ、２０５ｂ、２０５ｃの公開鍵$K_{CPA,pub,i}$を使用してチェックされ得る（ステップ３０２）。チェックが失敗であれば（ステップ３０２、図３の矢印「Ｋ」）、データが削除される（ステップ３０３）。チェックが成功すれば（ステップ３０２、図３の矢印「Ｏ」）、データは、中央集中プロファイル管理装置２０６のメモリ内に対象のサービスに関連付けて保存される（ステップ３０４）。対象のサービスに関連付けられたセキュアエレメントのプロファイルの更新をトリガするイベントが検出されない限り（ステップ３０５、矢印「Ｎ」）、中央集中プロファイル管理装置２０６は、引き続き対象のサービスに関するプロファイルデータを受信し（ステップ３０１）、場合によりこれらをチェックし（ステップ３０２）、それを削除する（ステップ３０３）か、それらをメモリに保存する（ステップ３０４）。対象のサービスに関連付けられたセキュアエレメントのプロファイルの更新をトリガするイベントが検出された場合（ステップ３０５、矢印「Ｙ」）、対象のサービスに関連付けられた保存されたプロファイルデータのうちの最新のプロファイルデータが通信エージェント２０３又は端末を管理するためのリモート管理プラットフォーム２０４に送信される（ステップ３０７）。任意選択により、プロファイルデータは、前述のように、ステップ３０７で送信される前に中央集中プロファイル管理装置２０６の秘密鍵$K_{TS,priv}$を使用して署名され得る（ステップ３０６）。

【００７２】
セキュアエレメントのプロファイルの更新をトリガするイベントは、最新のプロファイルデータが中央集中プロファイル管理装置２０６によって通信エージェント２０３又は端末を管理するためのリモート管理プラットフォーム２０４に送信されるようにするあらゆるイベントであり得る。幾つかの実施形態では、このトリガイベントは、中央集中プロファイル管理装置２０６が、セキュアエレメント２０２から通信エージェント２０３を介して送信された、所与のサービスに関連付けられたプロファイルデータが利用可能であるか否かを確認するための問合せリクエスト（このような問合せリクエストは、特に対象のサービスの識別子を含む）を受信することであり得る。これらの実施形態は、「プルモード」に対応し、幾つかの例が図４及び５に詳細に示されている。代替形態として、このトリガイベントは、そのデータを送信するプロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃから、プロファイルができるだけ早く又はプロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃからのデータの受信時に更新されなければならないという受信に対応し得る。他の代替形態によれば、トリガイベントは、プロファイルが更新されなければならない所定のタイミング（例えば、定期的）に対応する（例えば、毎週又はホスト端末が再起動されるたび等）。

【００７３】
図４は、本発明の１つの特定の実施形態によるサービスプロファイルの管理方法のステップを示す。

【００７４】
この実施形態は、「プル」モードに対応し、このモードでは、ホスト端末２０１の通信エージェント２０３は、中央集中プロファイル管理装置２０６に（場合により端末を管理するためのリモート管理プラットフォーム２０４を介して）問合せリクエストを送信し、引き換えとしてホスト端末２０１のセキュアエレメント２０２のプロファイルを更新するためにプロファイルデータを検索するように構成される。さらに、図４の実施形態では、ホスト端末が端末を管理するためのリモート管理プラットフォーム２０４によって管理されると仮定される。

【００７５】
ステップ４０１では、プロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃは、プロファイルデータを中央集中プロファイル管理装置２０６（図４ではＴＳで示される）に送信する（「プッシュする」）。すでに詳述したように、このプロファイルデータは、署名され得る。この場合、プロファイルデータの署名は、チェックされ（ステップ４０２）、チェックが成功した場合にのみ中央集中プロファイル管理装置２０６のメモリに保存され得る。プロファイルデータは、対応するサービス及びバージョンデータ（例えば、受信されたプロファイルデータに関連付けられたプロファイルのバージョン番号又はプロファイルデータの受信日）に関連付けて保存される。さらに、プロファイルデータは、場合により、２回目として中央集中プロファイル管理装置２０６の秘密鍵$K_{TS,priv}$を使用して署名され得る（ステップ４０３）。署名された／二重に署名されたプロファイルデータは、その後、パケットにカプセル化され（ステップ４０４）、それが中央集中プロファイル管理装置２０６に保存される。１つ以上の実施形態では、パケットは、サービス識別データ及び／又はそれが意図されるセキュアエレメントの識別子をさらに含み得る。任意選択のステップ４０５では、中央集中プロファイル管理装置２０６は、プロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃに対して、それ以前に受信されたプロファイルデータに対して行われた処理（ステップ４０２～４０３）の結果を知らせる通知を送信する。ある意味では、これは、受信されたプロファイルデータの受信及び保存を承認する。

【００７６】
ステップ４０１～４０５は、各種のプロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃから受信された複数のプロファイルデータ及び各種のサービスについて反復され得る。ステップ４０１～４０５の数回のイテレーション後、中央集中プロファイル管

理装置２０６は、メモリ内において、同一のセキュアエレメント２０２に対して意図される複数のパケットを有し得、その少なくとも２つのパケットは、同一のサービスに関連付けられ、２つの異なるプロファイル管理装置ＤＰＡ｟　２０５ａ、２０５ｂ、２０５ｃから発せられる。

【００７７】

ステップ４０６では、ホスト端末（図４ではＴＥＲＭで示される）の通信エージェント２０３は、端末を管理するためのリモート管理プラットフォーム２０４（図４ではＤＭＰで示される）に問合せクエストを送信し、これは、ステップ４０７で中央集中プロファイル管理装置２０６に転送される。問合せリクエストは、これらの実施形態によれば、セキュアエレメントの識別子及び／又はそれについて更新が入手可能であるか否かが尋ねられるサービスの識別子を含み得る。問合せリクエストは、例えば、定期的（例えば、毎週）又はホスト端末２０１のユーザの動作後に送信され得る。

【００７８】

１つ以上の実施形態では、問合せリクエストは、セキュアエレメントの秘密鍵$K_{SE,priv}$を使用して署名され得、秘密鍵$K_{SE,priv}$は、セキュアエレメント２０２に関連付けられた秘密鍵$K_{SE,priv}$及び公開鍵$K_{SE,pub}$で形成される非対称鍵ペア（$K_{SE,priv}$，$K_{SE,pub}$）の一部を形成する。セキュアエレメント２０２の公開鍵$K_{SE,pub}$は、中央集中プロファイル管理装置２０６と共有され得る。問合せリクエストを受け取ると（ステップ４０７）、中央集中プロファイル管理装置２０６は、セキュアエレメント２０２の公開鍵$K_{SE,pub}$によるステップ４０８のリクエストの署名をチェックし得る。チェックが失敗に終わると、この問合せリクエストは、無視される。チェックが成功した場合、中央集中プロファイル管理装置２０６は、端末を管理するためのリモート管理プラットフォーム２０４に対して、中央集中プロファイル管理装置２０６に保存された対象のサービスに関連付けられたプロファイルデータのうちの最新のプロファイルデータを送信する（ステップ４０９）。対象のサービスは、例えば、問合せリクエストに含まれるサービス識別子に基づいて特定され得る。代替形態として、問合せリクエストは、サービス識別子を含まず、ステップ４０９で中央集中プロファイル管理装置２０６は、それについてそれがプロファイルデータを保存する各サービスのために、このサービスに関連付けられた最新のプロファイルデータを送信する。換言すれば、中央集中プロファイル管理装置２０６は、複数のプロファイルデータを送信し、その各々が所与のサービスに関する最新のプロファイルデータである。ステップ４１０では、１つ以上のプロファイルデータが端末を管理するためのリモート管理プラットフォーム２０４から端末２０１の通信エージェント２０３に送信され、これは、その後、セキュアエレメント２０２に転送される。セキュアエレメントは、その後、１つ以上の受信されたプロファイルデータに対応する１つ以上のプロファイルを、この１つ以上の受信されたプロファイルデータに関連付けられた１つ以上の署名が有効であることを条件として更新し得る。

【００７９】

図５は、図４に示される実施形態の１つの代替的な実施形態を示す。この実施形態によれば、ホスト端末は、端末を管理するためのリモート管理プラットフォーム２０４によって管理されず、通信エージェント２０３は、中央集中プロファイル管理装置２０６と直接通信する。

【００８０】

ステップ４０１～４０５及び４０８は、図４と同じである。ステップ５０６及び５０９は、一方では図４のステップ４０６～４０７及び他方では４０９～４１０にそれぞれ対応する。換言すれば、ステップ５０６では、問合せリクエストがホスト端末２０１（図５ではＴＥＲＭで示される）の通信エージェント２０３から中央集中プロファイル管理装置２０６（図５ではＴＳで示される）に直接送信され、ステップ５０９では、１つ以上のプロファイルデータが中央集中プロファイル管理装置２０６からホスト端末２０１の通信エージェント２０３に直接送信される。図４と同様に、通信エージェント２０３が受信した１つ以上のプロファイルデータは、その後、セキュアエレメント２０２に転送される。セキ

ュアエレメントは、その後、１つ以上の受信されたプロファイルデータに対応する１つ以上のプロファイルを、この１つ以上の受信されたプロファイルデータに関連付けられた１つ以上の署名が有効であることを条件として更新し得る。

【００８１】

図６は、本発明の１つ以上の実施形態によるトランザクションを実施する他の中央集中プロファイル管理装置の一例を示す。

【００８２】

この実施形態では、デバイス６００は、方法が実施されるようにする命令、受信されたプロファイルデータ及び前述の方法の各種のステップを実施するための一時的データを保存するためのメモリ６０５（図６ではＭＥＭで示される）を含む。

【００８３】

このデバイスは、回路６０４（図６ではＰＲＯＣで示される）をさらに含む。この回路は、例えば、

－　コンピュータプログラムの形態の命令を解釈できるプロセッサ、

－　本発明の方法のステップがシリコン中で説明される電子カード、又は

－　ＦＰＧＡ（フィールドプログラマブルゲートアレイ）チップ、例えばＳＯＣ（システムオンチップ）又は他にＡＳＩＣ（特定用途集積回路）等のプログラム可能な電子チップであり得る。

【００８４】

ＳＯＣ、すなわちシステムオンチップは、電子システムのコンポーネントの全部を１つのチップに統合した埋込型システムである。ＡＳＩＣは、あるアプリケーションに合わせてカスタム化された機能を１つにまとめた専用の電子回路である。ＡＳＩＣは、一般に、これらが製造され、ユーザによるシミュレートのみが可能である場合に構成される。フィールドプログラマブルゲートアレイ（ＦＰＧＡ）プログラマブルロジック回路は、ユーザによって再構成可能な電子回路である。

【００８５】

デバイス６００は、プロファイル管理装置ＤＰＡ¡　２０５ａ、２０５ｂ、２０５ｃからプロファイルデータを受信するための少なくとも１つの入力インタフェース６０３（図６ではＩＮＰで示される）と、プロファイルデータを、端末を管理するための管理プラットフォーム２０４又は端末２０１の通信エージェント２０３に提供するための１つの出力インタフェース６０６（図６ではＯＵＴで示される）とを含む。最後に、中央集中デバイスは、ユーザと容易にやり取りできるようにするためのスクリーン６０１及びキーボード６０２を含み得る。当然のことながら、キーボードは、特に例えばタッチスクリーンタブレットの形態の中央集中デバイスに関して任意選択である。

【００８６】

実施形態に応じて、デバイス６００は、コンピュータ、コンピュータネットワーク、電子コンポーネント又はメモリに動作的に連結されるプロセッサを含む他の装置及びまた選択された実施形態に応じて、データ保存ユニット並びにネットワークインタフェース及びリムーバブル記憶媒体を読み出し、そのような媒体に書き込むための媒体リーダ（図示せず）等の他の関連するハードウェア要素であり得る。リムーバブル記憶媒体は、例えば、コンパクトディスク（ＣＤ）、デジタルビデオ／バーサタイルディスク（ＤＶＤ）、フラッシュディスク、ＵＳＢキー等であり得る。

【００８７】

実施形態に応じて、メモリ、データ記憶ユニット又はリムーバブル記憶媒体は、命令を含み、それは、これらが制御回路６０４によって実行されるとき、この制御回路６０４に、入力インタフェース６０３、出力インタフェース６０６、メモリ６０５内のデータ保存及び／又は提案される方法の本明細書に記載の例示的実施形態のデータ処理部を実行又は制御させる。

【００８８】

制御回路６０４は、デバイス６００のユニット６０３、６０５及び６０６を制御するコ

ンポーネントであり得る。

【００８９】

さらに、デバイス６００は、プロセッサによって実行可能なプログラムの形態をとるソフトウェアの形態、又は特定用途集積回路（ＡＳＩＣ）、システムオンチップ（ＳＯＣ）等の形態、又はハードウェアの要素とソフトウェアの要素との組合せの形態、例えば前述の電子コンポーネント（例えば、ＦＰＧＡ、プロセッサ）にロードされ、そこで実行されることが意図されるソフトウェアプログラムの形態をとる。デバイス６００は、ハイブリッドアーキテクチャ、例えばＣＰＵ＋ＦＰＧＡ、ＧＰＵ（グラフィクス処理ユニット）又はＭＰＰＡ（多目的プロセッサアレイ）に基づくアーキテクチャも使用し得る。

【００９０】

さらに、図３に示されるブロック図は、幾つかの命令が前述の中央集中デバイスで実行され得るプログラムの１つの典型例である。これに関して、図３は、本発明の意味におけるコンピュータプログラムの一般的アルゴリズムのフローチャートに対応し得る。

【００９１】

上記で本発明を具体的な実施形態に関して説明したが、本発明は、これらの具体的な実施形態に限定されず、本発明の範囲内に含まれる改良形態が当業者に自明であろう。

【００９２】

例としてのみ提供され、本発明の範囲を限定しない前述の例示的な実施形態を参照することで、他の多くの改良形態及び変更形態が当業者に明らかとなり、前記範囲は、付属の特許請求項によってのみ定義される。特に、各種の実施形態の様々な特徴は、適切な場合に入れ替えられ得る。

【図面】

【図１】

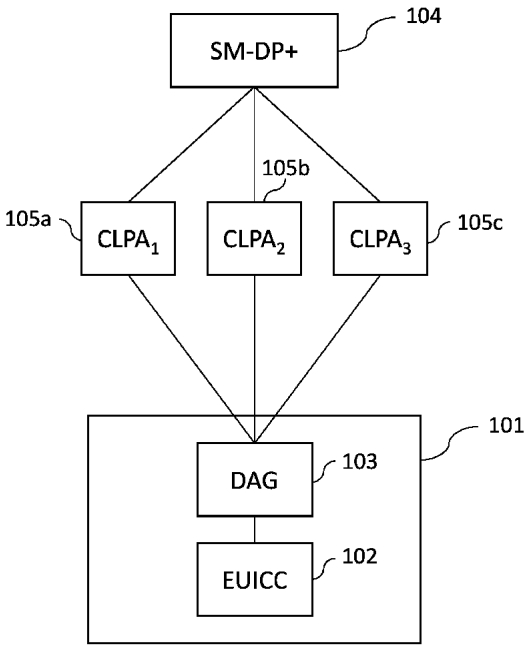

Figure 1

【図２】

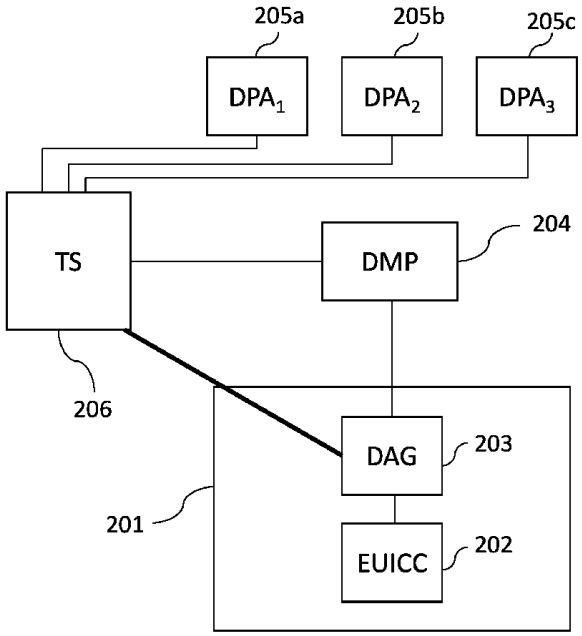

Figure 2

【図３】

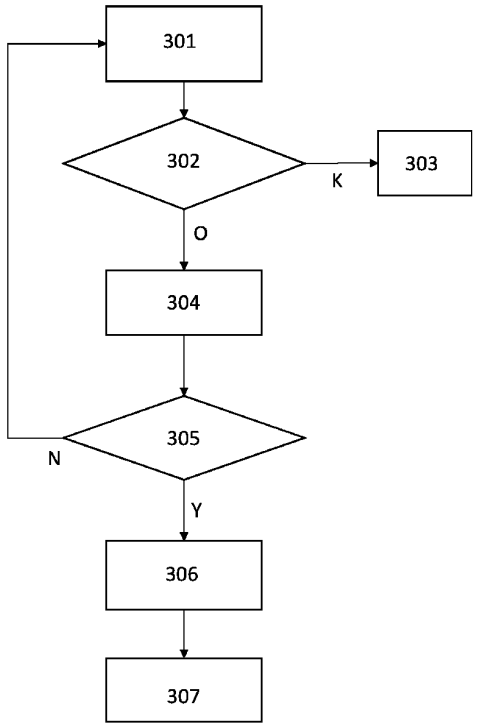

Figure 3

【図４】

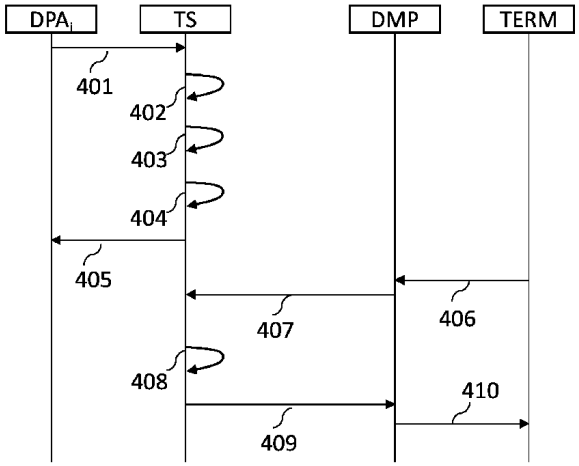

Figure 4

【図５】

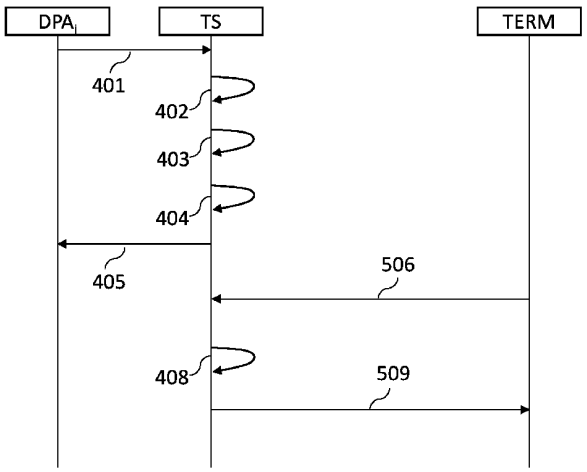

Figure 5

【図６】

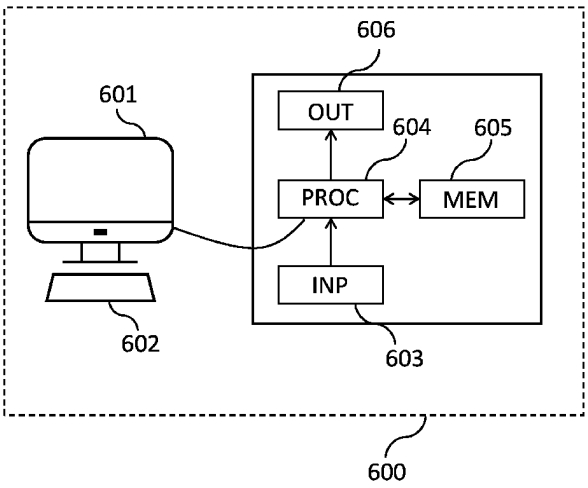

Figure 6

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2023/062659

A. CLASSIFICATION OF SUBJECT MATTER

H04W 4/50(2018.01)i; ***H04W 8/20***(2009.01)i; ***H04W 12/30***(2021.01)i; ***H04L 67/303***(2022.01)i; ***H04L 67/51***(2022.01)i; ***H04W 8/18***(2009.01)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)

H04W; H04L

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)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020396593 A1 (VIKBERG JARI [SE] ET AL) 17 December 2020 (2020-12-17) paragraphs [0008] - [0009], [0045] - [0046], [0050] - [0052], [0058] - [0059], [0074] - [0078] figures 2, 3, 5, 7	1-15
A	US 2018070224 A1 (PARK JONG-HAN [KR] ET AL) 08 March 2018 (2018-03-08) paragraphs [0002], [0074] - [0075], [0096] - [0103], [0119] - [0127], [0167] - [0171] figures 2, 4, 7	1-15
A	US 9020479 B1 (SOMAYAJULA SIVA RAMA KUMAR [US] ET AL) 28 April 2015 (2015-04-28) column 2, line 1 - column 2, line 66 column 4, line 30 - column 6, line 44 column 10, line 9 - column 11, line 23 figures 1, 2, 7, 8	1-15

☐ 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
24 July 2023	**01 August 2023**
Name and mailing address of the ISA/EP **European Patent Office** **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	Authorized officer **Volpato, Gian Luca** Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2023/062659

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2020396593 A1	17 December 2020	EP 3677058 A1	08 July 2020
		US 2020396593 A1	17 December 2020
		WO 2019042541 A1	07 March 2019
US 2018070224 A1	08 March 2018	CN 107660346 A	02 February 2018
		CN 113207118 A	03 August 2021
		EP 3277002 A1	31 January 2018
		KR 20160115832 A	06 October 2016
		KR 20220137593 A	12 October 2022
		US 2018070224 A1	08 March 2018
		WO 2016153281 A1	29 September 2016
US 9020479 B1	28 April 2015	NONE	

Form PCT/ISA/210 (patent family annex) (January 2015)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2023/062659

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04W4/50 H04W8/20 H04W12/30 H04L67/303 H04L67/51
H04W8/18
ADD.
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04W H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2020/396593 A1 (VIKBERG JARI [SE] ET AL) 17 décembre 2020 (2020-12-17) alinéas [0008] - [0009], [0045] - [0046], [0050] - [0052], [0058] - [0059], [0074] - [0078] figures 2, 3, 5, 7	1-15
A	US 2018/070224 A1 (PARK JONG-HAN [KR] ET AL) 8 mars 2018 (2018-03-08) alinéas [0002], [0074] - [0075], [0096] - [0103], [0119] - [0127], [0167] - [0171] figures 2, 4, 7	1-15

-/--

[x] Voir la suite du cadre C pour la fin de la liste des documents

[x] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
24 juillet 2023	01/08/2023

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Volpato, Gian Luca

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2023/062659

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 9 020 479 B1 (SOMAYAJULA SIVA RAMA KUMAR [US] ET AL) 28 avril 2015 (2015-04-28) colonne 2, ligne 1 - colonne 2, ligne 66 colonne 4, ligne 30 - colonne 6, ligne 44 colonne 10, ligne 9 - colonne 11, ligne 23 figures 1, 2, 7, 8	1-15

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2023/062659

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2020396593 A1	17-12-2020	EP 3677058 A1	08-07-2020
		US 2020396593 A1	17-12-2020
		WO 2019042541 A1	07-03-2019
US 2018070224 A1	08-03-2018	CN 107660346 A	02-02-2018
		CN 113207118 A	03-08-2021
		EP 3277002 A1	31-01-2018
		KR 20160115832 A	06-10-2016
		KR 20220137593 A	12-10-2022
		US 2018070224 A1	08-03-2018
		WO 2016153281 A1	29-09-2016
US 9020479 B1	28-04-2015	AUCUN	

Formulaire PCT/ISA/210 (annexe familles de brevets) (avril 2005)

フロントページの続き

(51)国際特許分類		FI			テーマコード（参考）
H04L	*9/32 (2006.01)*	H04L	9/32	200B	

,MC,ME,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,CV,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IQ,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,MG,MK,MN,MU,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

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， シー／オー アイデミア フランス

(72)発明者 マカウダ， ヤツェク

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， シー／オー アイデミア フランス

(72)発明者 コチェツキ， マレク

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， シー／オー アイデミア フランス

Ｆターム（参考） 5K067 AA30 DD17 EE02 EE16