

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第6533203号
(P6533203)

(45) 発行日 令和1年6月19日(2019.6.19)

(24) 登録日 令和1年5月31日(2019.5.31)

(51) Int.Cl. F I
HO4L 9/08 (2006.01) HO4L 9/00 601F

請求項の数 20 外国語出願 (全 30 頁)

(21) 出願番号	特願2016-200282 (P2016-200282)	(73) 特許権者	503260918
(22) 出願日	平成28年10月11日 (2016.10.11)		アップル インコーポレイテッド
(62) 分割の表示	特願2014-557779 (P2014-557779) の分割		Apple Inc.
原出願日	平成25年2月14日 (2013.2.14)		アメリカ合衆国 95014 カリフォル ニア州 クパチーノ アップル パーク ウェイ ワン One Apple Park Way, Cupertino, Californ ia 95014, U. S. A.
(65) 公開番号	特開2017-50875 (P2017-50875A)	(74) 代理人	100076428
(43) 公開日	平成29年3月9日 (2017.3.9)		弁理士 大塚 康徳
審査請求日	平成28年10月26日 (2016.10.26)	(74) 代理人	100115071
(31) 優先権主張番号	61/598,819		弁理士 大塚 康弘
(32) 優先日	平成24年2月14日 (2012.2.14)	(74) 代理人	100112508
(33) 優先権主張国	米国 (US)		弁理士 高柳 司郎
(31) 優先権主張番号	13/767,593		
(32) 優先日	平成25年2月14日 (2013.2.14)		
(33) 優先権主張国	米国 (US)		
前置審査			最終頁に続く

(54) 【発明の名称】 複数のアクセス制御クライアントをサポートするモバイル装置、及び対応する方法

(57) 【特許請求の範囲】

【請求項 1】

モバイル装置に含まれる電子ユニバーサル集積回路カード (eUICC) に関連付けられた、侵害されたデジタル証明書を交換する様に構成された eUICC 管理サーバであって、

それぞれが各 eUICC に関連付けられている複数のデジタル証明書に関連付けられた署名権限が侵害されたことを判定することと、

前記複数のデジタル証明書の各デジタル証明書について、

失効リストに前記デジタル証明書を追加することであって、前記失効リストは、(i) 前記 eUICC が、前記 eUICC 管理サーバに前記デジタル証明書を含む要求を送信し、(ii) 更新デジタル証明書が前記デジタル証明書より新しい場合に、前記デジタル証明書に関連付けられた前記各 eUICC が前記デジタル証明書を前記更新デジタル証明書に交換する原因となる、前記追加することと、を含むステップを、前記 eUICC 管理サーバに実行させる様に構成されたプロセッサを含む、eUICC 管理サーバ。

【請求項 2】

前記更新デジタル証明書に含まれる第 2 エポックのプロパティが、前記デジタル証明書に含まれる第 1 エポックのプロパティを超えていると、前記更新デジタル証明書が前記デジタル証明書より新しい、請求項 1 に記載の eUICC 管理サーバ。

【請求項 3】

前記ステップは、

(i) 前記 e U I C C に対応し、かつ、(i i) 前記デジタル証明書に関連付けられている公開鍵 (P K e U I C C) を識別することと、

前記更新デジタル証明書を取得することと、
をさらに含み、

前記更新デジタル証明書は、前記 P K e U I C C と、前記署名権限に対応する更新された秘密鍵 (S K U p d a t e d _ S A) と、に基づく、請求項 1 に記載の e U I C C 管理サーバ。

【請求項 4】

前記複数のデジタル証明書の各デジタル証明書について、前記 P K e U I C C を識別することは、最初に前記デジタル証明書を生成させた証明書署名要求 (C S R) を取得することを含む、請求項 3 に記載の e U I C C 管理サーバ。

10

【請求項 5】

前記複数のデジタル証明書の各デジタル証明書について、前記デジタル証明書及び前記更新デジタル証明書は、(i) 前記 P K e U I C C と、(i i) 前記 P K e U I C C に対応する秘密鍵 (S K e U I C C) と、に関連付けられている、請求項 4 に記載の e U I C C 管理サーバ。

【請求項 6】

前記複数のデジタル証明書の各デジタル証明書について、前記デジタル証明書は、前記署名権限に対応する元の秘密鍵 (S K O r i g i n a l _ S A) を使用してデジタル的に署名され、前記 S K O r i g i n a l _ S A は、侵害されている、請求項 3 に記載の e U I C C 管理サーバ。

20

【請求項 7】

前記 S K U p d a t e d _ S A は、前記 S K O r i g i n a l _ S A の改変に回答して前記署名権限により生成される、請求項 6 に記載の e U I C C 管理サーバ。

【請求項 8】

モバイル装置に含まれる電子ユニバーサル集積回路カード (e U I C C) に関連付けられた、侵害されたデジタル証明書を交換する方法であって、

e U I C C 管理サーバにおいて、

それぞれが各 e U I C C に関連付けられている複数のデジタル証明書に関連付けられた署名権限が侵害されたことを判定することと、

30

前記複数のデジタル証明書の各デジタル証明書について、

失効リストに前記デジタル証明書を追加することであって、前記失効リストは、(i) 前記 e U I C C が、前記 e U I C C 管理サーバに前記デジタル証明書を含む要求を送信し、(i i) 更新デジタル証明書が前記デジタル証明書より新しい場合に、前記デジタル証明書に関連付けられた前記各 e U I C C が前記デジタル証明書を前記更新デジタル証明書に交換する原因となる、前記追加することと、
を含む、方法。

【請求項 9】

前記更新デジタル証明書に含まれる第 2 エポックのプロパティが、前記デジタル証明書に含まれる第 1 エポックのプロパティを超えていると、前記更新デジタル証明書が前記デジタル証明書より新しい、請求項 8 に記載の方法。

40

【請求項 10】

(i) 前記 e U I C C に対応し、かつ、(i i) 前記デジタル証明書に関連付けられている公開鍵 (P K e U I C C) を識別することと、

前記更新デジタル証明書を取得することと、
をさらに含み、

前記更新デジタル証明書は、前記 P K e U I C C と、前記署名権限に対応する更新された秘密鍵 (S K U p d a t e d _ S A) と、に基づく、請求項 8 に記載の方法。

【請求項 11】

50

前記複数のデジタル証明書の各デジタル証明書について、前記 P K e U I C C を識別することは、最初に前記デジタル証明書を生成させた証明書署名要求 (C S R) を取得することを含む、請求項 1 0 に記載の方法。

【請求項 1 2】

前記複数のデジタル証明書の各デジタル証明書について、前記デジタル証明書及び前記更新デジタル証明書は、(i) 前記 P K e U I C C と、(i i) 前記 P K e U I C C に対応する秘密鍵 (S K e U I C C) と、に関連付けられている、請求項 1 1 に記載の方法。

【請求項 1 3】

前記複数のデジタル証明書の各デジタル証明書について、前記デジタル証明書は、前記署名権限に対応する元の秘密鍵 (S K O r i g i n a l _ S A) を使用してデジタル的に署名され、前記 S K O r i g i n a l _ S A は、侵害されている、請求項 1 0 に記載の方法。

10

【請求項 1 4】

前記 S K U p d a t e d _ S A は、前記 S K O r i g i n a l _ S A の改変に回答して前記署名権限により生成される、請求項 1 3 に記載の方法。

【請求項 1 5】

モバイル装置に含まれる電子ユニバーサル集積回路カード (e U I C C) に関連付けられた、侵害されたデジタル証明書を交換する様に構成された e U I C C 管理サーバであって、

それぞれが各 e U I C C に関連付けられている複数のデジタル証明書に関連付けられた署名権限が侵害されたことを判定し、

20

前記複数のデジタル証明書の各デジタル証明書について、

失効リストに前記 デジタル証明書 を追加する様に構成され、

前記失効リストは、(i) 前記 e U I C C が、前記 e U I C C 管理サーバに前記デジタル証明書を含む要求を送信し、(i i) 更新デジタル証明書が前記デジタル証明書より新しい場合に、前記デジタル証明書に関連付けられた前記各 e U I C C が前記デジタル証明書を前記更新デジタル証明書に交換する原因となる、e U I C C 管理サーバ。

【請求項 1 6】

(i) 前記 e U I C C に対応し、かつ、(i i) 前記デジタル証明書に関連付けられている公開鍵 (P K e U I C C) を識別し、

30

前記更新デジタル証明書を取得する様にさらに構成され、

前記更新デジタル証明書は、前記 P K e U I C C と、前記署名権限に対応する更新された秘密鍵 (S K U p d a t e d _ S A) と、に基づく、請求項 1 5 に記載の e U I C C 管理サーバ。

【請求項 1 7】

前記複数のデジタル証明書の各デジタル証明書について、前記 P K e U I C C を識別することは、最初に前記デジタル証明書を生成させた証明書署名要求 (C S R) を取得することを含む、請求項 1 6 に記載の e U I C C 管理サーバ。

【請求項 1 8】

前記複数のデジタル証明書の各デジタル証明書について、前記デジタル証明書及び前記更新デジタル証明書は、(i) 前記 P K e U I C C と、(i i) 前記 P K e U I C C に対応する秘密鍵 (S K e U I C C) と、に関連付けられている、請求項 1 7 に記載の e U I C C 管理サーバ。

40

【請求項 1 9】

前記複数のデジタル証明書の各デジタル証明書について、前記デジタル証明書は、前記署名権限に対応する元の秘密鍵 (S K O r i g i n a l _ S A) を使用してデジタル的に署名され、前記 S K O r i g i n a l _ S A は、侵害されている、請求項 1 6 に記載の e U I C C 管理サーバ。

【請求項 2 0】

前記 S K U p d a t e d _ S A は、前記 S K O r i g i n a l _ S A の改変に回答して

50

前記署名権限により生成される、請求項 19 に記載の e U I C C 管理サーバ。

【発明の詳細な説明】

【技術分野】

【0001】

(優先権)

本出願は、2013年2月14日に本出願と同時出願された米国特許出願第13/767,593号「METHODS AND APPARATUS FOR LARGE SCALE DISTRIBUTION OF ELECTRONIC ACCESS CLIENTS」に対する優先権を主張し、これは更に、2012年2月14日に本出願と同時出願された米国特許出願第61/598,819号「METHODS AND APPARATUS FOR LARGE SCALE DISTRIBUTION OF ELECTRONIC ACCESS CLIENTS」に対する優先権を主張し、上記のそれぞれは、参照によりその全体が本明細書に組み込まれる。

10

【0002】

(関連出願)

本出願は、共同出願で同時係属の米国特許出願第13/457,333号(2012年4月26日出願)「ELECTRONIC ACCESS CLIENT DISTRIBUTION APPARATUS AND METHODS」、同第13/464,677号(2012年5月4日出願)「METHODS AND APPARATUS FOR PROVIDING MANAGEMENT CAPABILITIES FOR ACCESS CONTROL CLIENTS」、同第13/095,716号(2011年4月27日出願)「APPARATUS AND METHODS FOR DISTRIBUTING AND STORING ELECTRONIC ACCESS CLIENTS」、同第13/080,558号(2011年4月5日出願)「APPARATUS AND METHODS FOR CONTROLLING DISTRIBUTION OF ELECTRONIC ACCESS CLIENTS」、同第12/952,082号(2010年11月22日出願)「WIRELESS NETWORK AUTHENTICATION APPARATUS AND METHODS」、同第12/952,089号(2010年11月22日出願)「APPARATUS AND METHODS FOR PROVISIONING SUBSCRIBER IDENTITY DATA IN A WIRELESS NETWORK」、同第13/183,023号(2011年7月14日出願)「VIRTUAL SUBSCRIBER IDENTITY MODULE DISTRIBUTION SYSTEM」、同第12/353,227号(2009年1月13日出願)「POSTPONED CARRIER CONFIGURATION」、同第13/093,722号(2011年4月25日出願)「APPARATUS AND METHODS FOR STORING ELECTRONIC ACCESS CLIENTS」、同第13/109,851号(2011年5月17日出願)「METHODS AND APPARATUS FOR ACCESS CONTROL CLIENT ASSISTED ROAMING」、同第13/079,614号(2011年4月4日出願)「MANAGEMENT SYSTEMS FOR MULTIPLE ACCESS CONTROL ENTITIES」、同第13/111,801号(2011年5月19日出願)「METHODS AND APPARATUS FOR DELIVERING ELECTRONIC IDENTIFICATION COMPONENTS OVER A WIRELESS NETWORK」、同第13/080,521号(2011年4月5日出願)「METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS」、同第13/078,811号(2011年4月1日出願)「ACCESS DATA PROVISIONING APPARATUS AND METHODS」、同第13/287,874号(2011年11月2日出願)「METHODS AND APPARATUS FOR ACCESS DATA RECOVERY FROM A MALFUNCTIONING DEVICE」、同第13/080,533号(2011年4月5日出願)「SIMULACRUM OF PHYSICAL SECURITY DEVICE AND METHODS」、及び同第13/294,631号(2011年11月11日出願)「APPARATUS AND METHODS FOR RECORDATION OF DEVICE HISTORY ACROSS MULTIPLE SOFTWARE EMULATION」に関連し、上記のそれぞれは、参照によりその全体が本明細書に組み込まれる。

20

30

40

【0003】

本開示は、一般的に、無線通信及びデータネットワークの分野に関する。より具体的には、本発明は特に、電子アクセス制御クライアントの大規模配信のための方法及び装置に関する。

【背景技術】

【0004】

アクセス制御は、従来技術の無線通信システムの多くにおいて、セキュアな通信のために必要である。一例として、1つの単純なアクセス制御方式は、(i)通信者のアイデン

50

ティティを確認すること、及び(i i)その確認されたアイデンティティに対応するアクセスレベルを与えること、を含み得る。例示的なセルラーシステム(例えば、ユニバーサル移動体通信システム(UMTS))のコンテキストにおいて、アクセス制御は、物理的なユニバーサル集積回路カード(UICC)(「SIMカード」とも呼ばれる)の上で実行されるユニバーサル加入識別モジュール(USIM)と呼ばれるアクセス制御クライアントによって管理される。USIMアクセス制御クライアントは、UMTSセルラーネットワークに対する加入者を認証する。認証が成功した後、その加入者はセルラーネットワークに対するアクセスが認められる。本明細書で以下に使用される用語「アクセス制御クライアント」は一般に、ネットワークに対する第1の装置のアクセスを制御するのに適した、ハードウェア又はソフトウェア内のいずれかで実現された論理エンティティを指す。10
アクセス制御クライアントの一般的な例としては、上述のUSIM、CDMA加入者識別モジュール(CSIM)、IPマルチメディアサービス識別モジュール(ISIM)、加入者識別モジュール(SIM)、除去可能ユーザ識別モジュール(RUIM)などが挙げられる。

【0005】

従前のSIMカードに基づいたアプローチは、数多くの問題を抱えている。例えば、従来のUICCは単一のUSIM(又はより一般的には「SIM」)アクセス制御クライアントのみをサポートしている。別のSIMを使用してセルラーネットワークへの認証を受けたい場合は、ユーザは機器のSIMカードを別のSIMカードと物理的に交換しなければならない。一部の機器は2枚のSIMカードを同時に収容するように設計されている(デュアルSIM電話)。しかしながら、そのようなデュアルSIM電話はSIMカード機器の基本的な物理的制限に対処するものではない。例えば、一方のSIMカード内に記憶されている情報を、もう一方のSIMカード内に記憶されている情報と統合することは容易にはできない。既存のデュアルSIM機器は、両方のSIMカードの内容に同時にアクセスすることはできない。20

【0006】

更に、SIMカードにアクセスするには、ユーザが知覚できる長さの時間を必要とする。SIMカードを切り替えて情報を移すのは望ましくなく、従来型及びデュアルSIM機器の両方において問題である。

【0007】

加えて、既存のSIMカード発行者とアクチベーションエンティティは一般にネットワークごとに固有であり、別のネットワークの別のユーザにとってはユビキタスではない。具体的には、所与のネットワーク内の所与のユーザは、自分の電話をアクチベートするか、又は、SIM発行を認定されたごく特定されたエンティティから交換用SIMカードを入手する必要がある。これは、例えば、他のネットワークを経たローミング、電話機の交換などの場合に、有効なアクセス特権をユーザが迅速に取得する可能性を大幅に制限する可能性がある。30

【0008】

最近では、例えば本明細書の譲受人により、電子SIM(eSIMと呼ばれる)が開発されている。この電子SIMは、別のeSIMとの交換、別の機器への転送などに関して、強化された柔軟性を提供する。しかしながら、SIMの配信とアクチベーションを行うための既存のネットワークのインフラストラクチャはこの進歩に追いついていない。40

【0009】

したがって、電子アクセスクライアント(例えば、eSIM)により提供される強化された柔軟性を推進するため、及び、電子アクセスクライアントのセキュアでユビキタスな配信をサポートするために、新しいソリューションとインフラストラクチャが必要とされている。

【発明の概要】

【0010】

本開示は特に、電子アクセス制御クライアントの大規模配信を提供する。50

【 0 0 1 1 】

第1に、電子アクセス制御クライアントの大規模配信のための方法が開示される。例示的な一実施形態において、この方法には、1つ以上の電子アクセス制御クライアントの所有権を確立することと、1つ以上の電子アクセス制御クライアントが以前に複製されていないかどうかを判定することと、1つ以上の電子アクセス制御クライアントを、第2の機器への転送のために暗号化することと、その暗号化された1つ以上の電子アクセス制御クライアントを交換することとが含まれる。

【 0 0 1 2 】

電子アクセス制御クライアントの大規模配信のための装置が更に開示される。例示的な一実施形態において、この装置は、プロセッサと、永続的コンピュータ可読媒体とを含み、このコンピュータ可読媒体は、このプロセッサによって実行されたときに、1つ以上の電子アクセス制御クライアントの所有権を確立し、1つ以上の電子アクセス制御クライアントが以前に複製されていないかどうかを判定し、1つ以上の電子アクセス制御クライアントを、第2の機器への転送のために暗号化し、その暗号化された1つ以上の電子アクセス制御クライアントを交換する、命令を含む。

【 0 0 1 3 】

電子アクセス制御クライアントのトランザクションのためのモバイル機器が更に開示される。一実施形態において、この機器は、無線ネットワークと通信するように構成された無線インタフェースと、このインタフェースとデータ通信するプロセッサと、このインタフェースとデータ通信するセキュアエレメントとを含む。一変異において、このセキュアエレメントは、セキュアプロセッサと、そのセキュアプロセッサとデータ通信し、少なくともその中に記憶されたネットワークとの認証のために有用な複数のアクセス制御クライアントを有する、セキュア記憶装置と、そのセキュアプロセッサとデータ通信する論理であって、この論理は、複数のアクセス制御クライアントを記憶し、これにアクセスし、装置へ転送し又は装置から転送するように構成されている、論理と、少なくともこのセキュアエレメントと通信を行い、その装置のユーザが、記憶されている複数のアクセス制御クライアントのうちの1つを選択することができるように構成され、その装置をそのネットワークに対して認証して、その中での通信を可能にする、ユーザインタフェース論理とを含む。

【 0 0 1 4 】

無線システムが更に開示される。

【 0 0 1 5 】

加えて、コンピュータ可読装置が開示される。一実施形態において、この装置は、その上に配置されたコンピュータプログラムを有する記憶媒体を含み、このプログラムは、実行されたときに、電子アクセス制御クライアントを配信するように構成されている。

【 0 0 1 6 】

加えて、電子アクセスクライアントを備えた無線モバイル機器を提供するためのネットワークアーキテクチャが開示される。一実施形態において、このアーキテクチャには、複数のブローカーと、その複数のブローカーとデータ通信する複数のメーカーとが含まれる。一変異において、所与のユーザモバイル機器は、複数のブローカーによってサービスを受けることができ、このブローカーのいずれも、1つ以上のメーカーに、電子アクセスクライアントを注文することができる。

【 0 0 1 7 】

1つ以上のモバイル機器に電子アクセスクライアントを提供する装置が更に開示される。一実施形態において、この装置は、少なくとも1つのプロセッサと、その少なくとも1つのプロセッサとデータ通信する、この装置にアクセスクライアントの暗号化及び暗号復号を実行させるように構成されている、第1の論理と、その少なくとも1つのプロセッサとデータ通信する、この装置に対し、このアクセスクライアントが複製されていないことを確実にさせるように構成されている、第2の論理と、その少なくとも1つのプロセッサとデータ通信する、この装置に対し、このアクセスクライアントのユーザの信用、所有権

10

20

30

40

50

、及び/又は検証のうちの少なくとも1つを確立させるように構成されている、第3の論理と、を含む。

【0018】

電子アクセス制御クライアントの失効手順が更に開示される。一実施形態において、この手順には、証明書を記憶する1つ以上の装置に関連付けられている、証明書を発行した証明書署名権限が侵害されているかどうかを判定することと、証明書の初期要求が生成されたときに、生成されたその証明書サービス要求を1つ以上の装置で判定することと、その判定された証明書サービス要求を使用して新しい証明書を要求することと、その要求に基づいて新しい証明書を発行することと、が含まれる。一変異において、1つ以上の装置が、以前使用された秘密鍵を、この要求の一部として使用することができ、新しい証明書は、以前の秘密鍵に対応する以前の公開鍵を含んで発行される。

10

【0019】

他の特徴及び有利点は、添付図面、及び以下に記載されるような例示的实施形態の詳細な説明を参照することで、当業者によって即座に認識されるであろう。

【図面の簡単な説明】

【0020】

【図1】本開示の様々な態様に関連して有用な、1つの例示的な電子ユニバーサル集積回路カード(eUICC)の論理ブロック図である。

【図2】本開示の様々な態様に関連して有用な、1つの例示的な電子加入者識別モジュール(eSIM)ディレクトリ構造の論理ブロック図である。

20

【図3】本開示の様々な態様に関連して有用な、加入者識別モジュール(SIM)専用ファイル(SDF)のための、1つの例示的なステートマシンを表わす論理ブロック図である。

【図4】本開示の様々な態様に関連して有用な、eSIM動作のための、1つの例示的なステートマシンを表わす論理ブロック図である。

【図5】本開示の様々な実施形態に関連して有用な、1つの例示的なeSIMブローカーネットワークの図である。

【図6】本開示の様々な実施形態に関連して有用な、1つの例示的な階層セキュリティプロトコルの論理ブロック図である。

【図7】本開示の様々な態様に関連して有用な、3つの要素を含む1つの例示的なデータ構造の図である。

30

【図8】本開示の様々な態様に関連して有用な、1つの例示的なOEM認証階層の図である。

【図9A】パーソナライズなしでeSIMを機器に配信するための、1つの例示的な論理シーケンスの初期段階を表わす論理フロー図である。

【図9B】パーソナライズなしでeSIMを機器に配信するための、1つの例示的な論理シーケンスの最終段階を表わす論理フロー図である。

【図10A】事前パーソナライズを伴ってeSIMを機器に配信するための、1つの例示的な論理シーケンスの初期段階を表わす論理フロー図である。

【図10B】事前パーソナライズを伴ってeSIMを機器に配信するための、1つの例示的な論理シーケンスの中間段階を表わす論理フロー図である。

40

【図10C】事前パーソナライズを伴ってeSIMを機器に配信するための、1つの例示的な論理シーケンスの最終段階を表わす論理フロー図である。

【図11A】eSIMのバッチを機器に配信するための、1つの例示的な論理シーケンスの初期段階を表わす論理フロー図である。

【図11B】eSIMのバッチを機器に配信するための、1つの例示的な論理シーケンスの最終段階を表わす論理フロー図である。

【図12】電子ユニバーサル集積回路カード(eUICC)装置の論理図である。

【図13】電子加入者識別モジュール(eSIM)デポ装置の論理図である。

【図14】1つの代表的なユーザ装置を示す論理フロー図である。

50

【図15】電子アクセス制御クライアントの大規模配信のための方法の一実施形態を示す論理フロー図である。

【0021】

全ての図は、2012年から2013年に作成され、その全ての著作権はApple Inc. が保持している。

【発明を実施するための形態】

【0022】

ここで図面を参照するが、全体を通して、同様の番号は同様の部分を指す。

【0023】

例示的实施形態の説明

本開示の例示的实施形態及び態様が、ここに詳しく記述される。これらの実施形態及び態様は主に、GSM（登録商標）、GPRS/EDGE、又はUMTSセルラーネットワークの加入者識別モジュール（SIM）のコンテキストで主に議論されるが、当業者には、本開示がそのように限定されないことが理解されよう。実際、本開示の様々な特徴は、アクセス制御クライアントを機器に記憶及び配信することで利益が得られる可能性がある任意のネットワーク（無線セルラー又はその他かどうかを問わず）において有用である。

【0024】

本明細書で使用される用語「クライアント」及び「UE」には、無線使用可能な携帯電話、スマートホン（例えばiPhone（商標）など）、無線使用可能なパーソナルコンピュータ（PC）、モバイル機器（例えばハンドヘルドコンピュータ、PDA、パーソナルメディア装置（PMD）、無線タブレット（例えばiPad（商標）など）、いわゆる「ファブレット」、又はこれらの任意の組み合わせが挙げられるが、これらに限定されない。

【0025】

本明細書で以下に使用される用語「加入者識別モジュール（SIM）」、「電子SIM（eSIM）」、「プロファイル」、及び「アクセス制御クライアント」は、一般に、ネットワークに対する第1の装置のアクセスを制御するのに適した、ハードウェア又はソフトウェア内のいずれかで実現された論理エンティティを指す。アクセス制御クライアントの一般的な例としては、上述のUSIM、CDMA加入者識別モジュール（CSIM）、IPマルチメディアサービス識別モジュール（ISIM）、加入者識別モジュール（SIM）、除去可能ユーザ識別モジュール（RUIM）など、又はこれらの任意の組み合わせが挙げられる。

【0026】

用語「加入者識別モジュール」が本明細書で使用される時（例えばeSIM）、この用語は、下記であるかどうかを必ずしも意味せず又は必要ともしないことが理解されよう。（i）本質的に加入者による使用（すなわち、本開示の様々な機能が、加入者又は非加入者によって実践し得る）、（ii）単一個人の識別（すなわち、本開示の様々な特徴が、家族などの個人集団、あるいは企業などの無形又は架空のエンティティのために実践され得る）、あるいは（iii）任意の有形の「モジュール」装置又はハードウェア。

【0027】

例示的なeUICC及びeSIMの動作

ここで、本開示の様々な特徴及び機能が、1つの例示的な実装に関して議論される。本開示の例示的な実施形態のコンテキストにおいて、従来技術におけるような物理的なUICCを使用する代わりに、UICCが、例えばソフトウェアアプリケーションのような仮想又は電子エンティティ（以下、電子ユニバーサル集積回路カード（eUICC）と呼ばれる）としてエミュレートされ、これは、UE内のセキュアエレメント（例えばセキュアなマイクロプロセッサ又は記憶装置）内に収容される。eUICCは、以下、電子加入者識別モジュール（eSIM）として呼ばれる、複数のSIM要素を記憶及び管理することができる。各eSIMは、典型的なUSIMのソフトウェアシミュレーションであり、相似プログラミング及びそれに関連するユーザデータを含む。eUICCは、eSIMのI

10

20

30

40

50

CC-IDに基づいてeSIMを選択する。eUICCが所望のeSIMを選択すると、UEは、eSIMの対応するネットワークオペレータから無線ネットワークサービスを取得するための認証手順を開始することができる。

【0028】

eUICCソフトウェアアーキテクチャ

ここで図1を参照し、本開示に関連して有用な、1つの例示的な電子ユニバーサル集積回路カード(eUICC)が示されている。例示的なeUICCの例は、前記で参照により全体が本明細書に組み込まれた、同出願で同時係属の米国特許出願第13/093,722号(2011年4月25日出願)「APPARATUS AND METHODS FOR STORING ELECTRONIC ACCESS CLIENTS」に記述されており、ただし他のものも本開示に一貫して使用し得ることが理解されよう。

10

【0029】

図1は、1つの例示的なJava Card(登録商標)eUICCアーキテクチャである。スマートカードに利用するための他のオペレーティングシステム(OS)の例としては、MULTOS及び独自仕様のOSが挙げられ(これらに限定されない)、Java Cardは単に説明目的である。OSは、アプリケーションソフトウェアとハードウェアの間のインタフェースを提供する。一般に、OSは、入力出力(I/O)、ランダムアクセスメモリ(RAM)、リードオンリーメモリ(ROM)、不揮発性メモリ(NV)(EEPROM、フラッシュ)などのために構成されたサービス及び機能を含む。OSは更に、高次の層、メモリ及びファイル管理、並びに通信プロトコルに使用される暗号サービスを提供し得る。

20

【0030】

例示的なJava実装は、次の3つの部分から成る。Javaカード仮想マシン(JCVM)(バイトコードインタプリタ)、Javaカードランタイム環境(JCRE)(カードリソース、アプレット実行、及びその他のランタイム特徴を管理する)、及びJavaアプリケーションプログラミングインタフェース(API)(スマートカードアプリケーションをプログラミングするための一組のカスタマイズされたクラス)。

【0031】

JCVMはカード上の構成要素(バイトコードインタプリタ)と、カード外の相対物(コンバータ)とを有する。カードリソースの制限により、コンバータがいくつかのコンパイルタスクを実施することができる。最初、Javaコンパイラは、ソースコードからクラスファイルを作成する。コンバータは、クラスファイルをプリプロセスし、CAPファイルを作成する。コンバータは、Javaクラスのロードイメージが良好に形成されていることを確認し、Javaカードの言語サブセット違反をチェックし、更に他のいくつかのタスクを実行する。CAPファイルはJavaパッケージ内のクラスの実行可能バイナリ表現を含む。コンバータは更に、エクスポートファイルを生成し、これは公開API情報を含む。CAPファイルのみが、カードにロードされる。もう1つの広く使用されるフォーマットがIJCであり、これはCAPファイルからコンバートすることができる。IJCファイルは、CAPファイルに比べ、大きさがやや小さい可能性がある。

30

【0032】

典型的に、カードにアプレットをダウンロードするには、CAPファイルの内容をカードの永続性メモリにロードするために、アプリケーションプロトコルデータ単位(APDU)交換が必要である。このオンカードインストーラは更に、CAPファイルのクラスをカード上の他のクラスとリンクさせ得る。その後、インストールプロセスはアプレットのインスタンスを生成し、JCREでインスタンスを登録する。アプレットは、選択されるまで、サスペンド状態に維持される。

40

【0033】

上述の手順は、1つ以上のセキュリティ層を追加で実施し得る。例示的な一実施形態において、グローバルプラットフォーム(GP)はアプリケーションを管理するためのセキュアプロトコルを提供する。GPはセキュアな発行者セキュリティドメイン内で動作し、

50

これはカード発行者のオンカード表現である。カードは更に、例えばアプリケーションプロバイダのために、他のセキュリティドメインを実行し得る。

【0034】

例示的な一実施形態において、eUICCは取り外しができない機器コンポーネントである。動作中、eUICCはセキュアなブートストラップOSを実行する。ブートストラップOSは、eUICCがセキュアであることを確実にし、その中のセキュリティプロトコルの実施を管理する。セキュアなブートストラップOSの例は、共同出願で同時係属の米国特許出願第13/080,521号(2011年4月5日出願)「METHODS AND APPARATUS FOR STORAGE AND EXECUTION OF ACCESS CONTROL CLIENTS」に記述されており、これは上記で参照によりその全体が組み込まれている。更に、様々な移動体通信事業者(MNO)が、eSIMをカスタマイズして、様々な度合のサービス差別化をサポートし得ることが理解されよう。カスタマイズの一般的な例には、独自仕様のファイル構造及び/又はソフトウェアアプリケーションが挙げられるがこれらに限定されない。eSIMの構成可能性により、eSIMはその大きさが顕著に変化し得る。

10

【0035】

従来技術のSIMカードとは異なり、eSIMは、セキュアなトランザクションにより機器間で自由に交換することができる。加入者は、機器間でSIMを移動するのに「物理的なカード」を必要としない。ただし、eSIMの実際のトランザクションは、例えば特定のセキュリティプロトコルを介して、確実なセキュリティで保護されなければならない。例示的な一実施形態において、eSIMは、特定の受信者に対して暗号化されてから配信される。いくつかの変異において、暗号化された内容に加え、各eSIMが、平文であるメタデータ部分を含み得る。更に暗号化署名を使用して、平文内容の完全性を確保することができる。このメタデータ部分は、非セキュアな記憶装置などを支援するため、(セキュアでないエンティティに対してであっても)自由に提供し得る。

20

【0036】

eSIMソフトウェアアーキテクチャ

ここで図2を参照し、例示的なeUICC内に実施されている、1つの例示的な電子加入者識別モジュール(eSIM)ディレクトリ構造が開示されている。図示のように、eSIMディレクトリ構造は、eSIMにより提供される柔軟性をサポートするよう改変されている。例えば、このeSIMディレクトリ構造は特に次のものを含む。(i)インストールされているeSIMのリストを含むEFeSimDir、(ii)eUECCをグローバル、一意に特定するカードシリアル番号を含むEFcsn、(iii)1つ以上のeUICC証明書に対応するセキュリティ関連データ及び秘密鍵を記憶するDFsecurity。そのような一変異において、DFsecurity情報には次のものが含まれる。(i)eUICCプラットフォームレベルPCFを含むDFepcf、(ii)ルート証明書及びOEM一般名を含むEFoemcert(OEM認証情報は、例えば工場リファビッシュなどの特殊な操作に使用され得る)、(iii)eUICCの証明書であるEFeUICCcert、(iv)サーバL1アプライアンスのルート証明書であるEFsL1cert、(v)サーバL2アプライアンスのルート証明書であるEFsL2cert、及び、(vi)サーバL3アプライアンスのルート証明書であるEFsL3cert。

30

40

【0037】

例示的な一実施形態において、このディレクトリ構造は更に、あるeSIMに固有のファイル構造を含むSIM専用ファイル(SDF)を含む。各SDFはMFの直下に位置する。各SDFは名前属性と、例えば、集積回路カード識別子(ICCID)などのSID(eSIM ID)を有する。図示のように、各SDFは更に、DFprofiles及びDFcodesを含む。更に、一変異において、すべてのプロファイルPCF関連EFは、DFppcfの下に記憶され、DFppcfはDFprofileの下に記憶される。

【0038】

50

例示的な一実施形態において、DFprofile情報には次のものが含まれる。(i)eSIMの記述であるEFname(eSIMの名前とバージョンなど)、(ii)eSIMのタイプを記述するEFtype(例えば、レギュラー、ブートストラップ、及びテストなど)。ソフトウェアアプリケーションは、この情報を、例えば、ブートストラップeSIMが使用中のときにアイコンを表示するために使用することができる。(iii)eSIMをサポートするのに必要なeUICCソフトウェアの最小バージョン番号であるEFsys_ver、(iv)eSIMが必要とする不揮発性メモリの最小量を示すEFnv_min、(v)必要な揮発性メモリの最小量を示すEFram_min、(vi)オーバザエアートランザクション(OTA)のために確保される不揮発性メモリの量を示すEFnv_rsvd、及び(vii)OTAのために確保される揮発性メモリの量を示すEFram_rsvd。

10

【0039】

例示的な一実施形態において、DFcode情報は各eSIMの一組の鍵を含む。これらの値は、多くの状況において、eUICCから読み出すことができない。1つの例外的な使用例が、eSIM全体を暗号的にラップしエクスポートするエクスポート動作である。eSIM全体が暗号化されているため、鍵の値はセキュアに保たれる。例示的な一実施形態において、DFcode情報は次のものを含む。(i)グローバルPIN(個人識別番号)及びPUK(PINロック解除鍵)を含むExEFgPinx/gPukx、(ii)ユニバーサルなPIN及びPUKを含むEFuPin/uPuk、(iii)ADM INコードを含むEFadminx、及び(iv)OTAコードを含むEFotax。いくつの変異において、更に、次のような追加の要素を含むADFusimが存在し得る。(i)K(128ビットの共有認証鍵)を記憶するEFk、(ii)加入者鍵及びオペレータ変異体アルゴリズム構成フィールドOPから導出されるOPcを記憶するEFop c(一部の变異体はOPcではなくOPを記憶し得る)、(iii)RESの長さを特定するEFauthpar、(iv)ネットワーク認証アルゴリズム(例えばMilena ge)を特定するEFalgid、(v)SQNを記憶するEFsan、及び(vi)ローカルPINのためにPIN及びPUKを記憶するEFlpinx/lpukx。

20

【0040】

本開示を読む当業者には、上記のファイル、構造、又は要素が単に例示であり、所望の機能又は構造を所有する他のものに置き換え得ることが理解されよう。

30

【0041】

ここで図3を参照すると、SDF動作のための1つの例示的なステートマシンが示されている。図示されているように、このSDFステートマシンは次のステートを含む。作成、初期化、動作(アクチベーション済み)、動作(アクチベーション解除済み)、及び終了。

【0042】

eSIMが最初にインストールされると、SDFが作成され(作成)、次にそのeSIMに含まれているファイル構造データで初期化される(初期化)。eSIMがインストールされると、SDFはアクチベーション解除済みステートに移行する。アクチベーション解除済みステート中は、利用できるファイルはない。eSIMが選択されると、SDFがアクチベーション解除済みステートからアクチベーション済みステートに移行する。このアクチベーション済みステートにより、SDFのファイルへのアクセスが可能になる。eSIMが(暗示的又は明示的のいずれでも)選択解除されると、SDFはアクチベーション済みステートからアクチベーション解除済みステートに戻る。

40

【0043】

ここで図4を参照すると、eSIM動作のための1つの例示的なステートマシンが示されている。図示されているように、このeSIMステートマシンは次のステートを含む。インストール済み、選択済み、ロック済み、アクチベーション解除済み、エクスポート済み、及び削除済み。

【0044】

50

e S I Mのインストール中に（インストール済み）、e S I Mのためのエントリがe U I C Cレジストリに作成される。このエントリは、1つ以上の関連するS D F及びアプリケーションを示す。インストール済みステート中に、S D Fがアクチベーション解除済みステートに設定され、アプリケーションはインストール済みステートに設定される。

【 0 0 4 5 】

e S I Mが選択されると、このe S I Mが選択済みステートに移行する。選択済みステート中に、S D Fはアクチベーション済みステートに移行し、アプリケーションは選択可能ステートに移行される。e S I Mが選択解除されると、このe S I Mはインストール済みステートに戻る。

【 0 0 4 6 】

特定の条件下において、e S I Mはロック済みステートになり得る。例えば、e U I C C P C Fが変更されて、インストール済みe S I Mがもはや使用できなくなった場合、e S I Mはロック済みステートに移行する。ロック済みステート中に、S D Fがアクチベーション解除済みステートに設定され、アプリケーションはロック済みステートに設定される。その他の種々のステートには、エクスポート済みステート（すなわち、e S I Mがエクスポートされ、もはや選択できない状態）、及び削除済みステート（すなわち、e S I Mが削除されている状態）が挙げられる。

【 0 0 4 7 】

ネットワーク認証アルゴリズム

ネットワーク認証アルゴリズム（N A A）は、一般に、移動体通信事業者（M N O）の動作に必須である。N A Aの様々な実装が存在するが、その機能は実質的に異なるものではない。特定の実施形態において、e U I C CはN A Aの共通パッケージを含み得る。e S I Mインストール中に、各N A Aアプリケーションのインスタンスを、事前ロード済みパッケージから各e S I Mについて作成することができ、これによってe S I Mの全体のロード時間が短縮され、e U I C Cの不必要なメモリ消費が低減され得る。

【 0 0 4 8 】

N A Aの一般的な例としては、M i l e n a g e、C O M P 1 2 8 V 1、C O M P 1 2 8 V 2、C O M P 1 2 8 V 3、a n d C O M P 1 2 8 V 4、及び特定の独自仕様アルゴリズムが挙げられるが、これらに限定されない。今も使用されている数多くの独自仕様アルゴリズムがある（C O M P I 2 8 V Iに対する攻撃が知られているため）。一実施形態において、ネットワーク認証は、周知の認証及び鍵合意（A K A）プロトコルに基づく。

【 0 0 4 9 】

N A Aが損われるという可能性の低い事態が生じた場合、代替のN A A方式には、ソフトウェアの更新が必要となり得る。そのような事態において、e S I Mは、例えば、セキュアなソフトウェア更新を介して、代替アルゴリズムでパッチを行うことができる。これ以降、M N Oは既存のO T A機構を介して代替アルゴリズムを使用可能にすることができる。

【 0 0 5 0 】

例示的なe S I Mブローカーネットワーク

図5は、本開示の様々な態様に関連して有用な、1つの例示的なe S I Mブローカーネットワークの高レベル図である。例示的な一実施形態において、このブローカーネットワークは、ブローカーとメーカーの分散ネットワークを含み、これにより機器は複数のブローカーによってサービスを受けることができ、ブローカーは複数のe S I Mメーカーにe S I Mを注文することができる。いくつかの実施形態において、機器が特定のe S I M動作で通信可能とする、ブローカー群を制限するような、e U I C C及び/又はe S I Mプロファイルポリシーが存在し得る。例えば、M N Oは、そのM N Oにより補助されている機器が、そのM N Oが所有するブローカーとのみ通信することを義務付けることがある。

【 0 0 5 1 】

そのような一変異において、プライマリブローカーは機器に対しディスカバリーサービ

10

20

30

40

50

スを提供し、これにより機器は適切なブローカーを特定することができる。これ以降、その機器はeSIM動作(例えば、購入、インストール、エクスポート、及びインポート)に関して、特定されたブローカーと直接通信することができる。

【0052】

関連するネットワーク分野の当業者には、図5に示されているもののような大規模配信ネットワークの動作中に、複数の実際的な問題が生じることが理解されよう。具体的には、大規模配信ネットワークは、プロビジョニングトラフィックの大きなバースト(例えば、所与のモバイルユーザ機器のいわゆる「発売日」に起こり得る)を取り扱えるよう、スケラブルでなければならない。ネットワークトラフィック全体を低減するための1つの提案される方式は、発売日以前の、事前パーソナライズeSIMを伴う(可能な場合)。

例えば、いわゆる「SIMイン」ユニットは、出荷時にeSIMが既に割り当てられている。この事前割り当てされたeSIMは、例えば、ユニットのeUICCに固有の鍵で、対応するeSIMプロファイルを暗号化することによって、そのユニットの事前パーソナライズを行うことができる。

10

【0053】

その他の考慮事項には、システム信頼性が挙げられる。例えば、ブローカーネットワークは様々な装置故障から回復することが可能でなければならない。1つの解決策は、様々な地域にわたって複数のデータセンターが重複コンテンツを有する、地理的冗長性である。しかしながら、データセンターのネットワークは、eSIMクローニングを回避するため、能動的に互いに同期し得る。そのようなネットワーク同期には、非常に大きなネットワーク帯域を必要とし得る。別の解決策として、各データセンターが別のeSIMセットを有することができる。しかしながら、これには多大なeSIMオーバーヘッドが必要である。

20

【0054】

理想的には、ブローカーネットワークは柔軟に、様々なビジネスモデルに適合し得る。具体的には、様々な法的及び反トラストの理由から、上記のブローカーネットワークの様々な構成要素が、異なる当事者により取り扱われる可能性がある。したがって、eSIMトラフィックのセキュリティ面は、注意深い監視と評価が必要になる。各eSIMは、大切なユーザ情報及びMNO情報を含む。例えば、eSIMは共有認証鍵(U SIM用のK、及びS IM用のK_i)を含む可能性があり、もし侵害されると、SIMクローニングに

利用される可能性がある。同様に、eSIMは更に、銀行口座情報などのセンシティブなユーザデータを有している可能性があるアプリケーションを含み得る。

30

【0055】

加えて、eUICCソフトウェアは機器リカバリのために更なる対策を必要とすることが理解されよう。物理的SIMとは異なり、eUICCソフトウェアが回復不能な状態になった場合、機器全体を交換する必要がある(これは、SIMカードを交換するよりはるかに高価につく)。したがって、例示的な解決策は、そのような苛酷な手段をあらかじめ除外するために、機器リカバリを取り扱うことが可能であるべきである。

【0056】

最後に、ネットワーク動作は「良好な」ユーザエクスペリエンスを提供すべきである。長すぎる応答時間、信頼性の低い動作、過剰なソフトウェアクラッシュなどは、全体的なユーザエクスペリエンスに大きなマイナスとなり得る。

40

【0057】

例示的なセキュリティプロトコル

したがって、本明細書において、上記の様々な問題に対処するため、階層セキュリティソフトウェアプロトコルが開示される。例示的な一実施形態において、サーバeUICC及びクライアントeUICCソフトウェアは、いわゆる、ソフトウェア層の「スタック」を含む。各ソフトウェア層は、一組の階層的機能を担当し、これらに対応するピアソフトウェア層と交渉される。更に、各ソフトウェア層はその層自体と通信する。場合によっては、機器アプリケーションプロセッサ(AP)が侵害される可能性がある(例えば「ジェ

50

イルブレイク」されるなど)ことが更に理解されよう。したがって、クライアント e U I C C と対応するサーバ e U I C C (又はその他のセキュアなエンティティ)との間に信頼関係が存在することが認識される。すなわち、その A P は信頼されない。

【 0 0 5 8 】

例示的な一実施形態において、3階層システムが開示される。図6に示すように、セキュリティソフトウェアプロトコルは、レベル1(L1)、レベル2(L2)、及びレベル3(L3)を含む。L1セキュリティは、e S I Mデータの暗号化及び暗号復号を実施する。L1動作は、実行環境(例えば、e U I C C又はハードウェアセキュリティモジュール(HSM))をセキュアにすることに限定される。L1内で、e S I Mデータは論理L1バウンダリ内に平文で(すなわち、暗号化されていない状態で)記憶することができる。L1バウンダリの外では、e S I Mデータは常にセキュアに暗号化される。L2セキュリティにより、e S I Mが複製できないよう確実にする。L2バウンダリにより、e S I Mの唯一のコピーが1つだけ存在するよう確実にする。L2バウンダリ内には、複数のコピーが存在する可能性がある。加えて、L2セキュリティは更に、暗号化されたe S I Mペイロードにチャレンジを埋め込む可能性がある。e S I Mの受け取り側は、e S I Mをインストールするより前に記憶されたチャレンジと、受信したチャレンジとを比較して、そのe S I Mが陳腐化していないことを(すなわち現行の唯一のe S I Mであることを)確認する。L3セキュリティは、ユーザの信頼、所有、及び検証の確立を担当する。各e S I Mについて、e U I C Cは、e S I Mに関連付けられた所有権を示す情報を記憶し得る。

10

20

【 0 0 5 9 】

1つの例示的な実施において、いわゆる「チャレンジ」は、特定のe S I Mインスタンスをe U I C Cと関連付けるのに使用される重要なリソースである。具体的には、各e U I C Cは各プロファイルエージェントについて特定の数のチャレンジを保持し、このプロファイルエージェントは、L2セキュリティを保持する論理エンティティである。チャレンジが有効であることを検証することによって、e U I C Cはそのe S I Mが陳腐化したe S I M(すなわち、無効な複製)ではないことを確認できる。パーソナライズされる各e S I Mについて、数多くのチャレンジが作成される。e U I C Cは、合致するe S I Mを受信すると、チャレンジを削除する。

【 0 0 6 0 】

下記の事前パーソナライズシナリオを考慮する。e U I C Cが、ネットワークに提供される数多くのチャレンジを作成し(又は与えられ)、このチャレンジは更に、e U I C Cの不揮発性メモリに保存される。したがって、これ以降、ネットワークは、事前生成されたチャレンジに拘束されたe U I C Cのためのe S I Mを生成することができる。e U I C Cが後で機器アクチベーションの際にe S I Mを受信すると、e U I C Cはその受け取ったe S I Mが適切なチャレンジを含んでいることを検証することができる。

30

【 0 0 6 1 】

しかしながら、上記の方式の欠点の1つは、固定数のチャレンジは容易に、サービス拒否(DOS)攻撃で侵害される可能性があることである。DOS攻撃では、e U I C Cがチャレンジを生成するよう連続的にトリガされ、ついにはチャレンジリソースすべてが枯渇する。したがって、そのような一変異において、e U I C Cは追加として、プロファイルサーバ/エージェントの認証を行うためのハンドシェイクセッションを実施してから、チャレンジを生成するようe U I C Cをトリガする要求を処理する。加えて、リソースが枯渇し、e U I C Cが新たなチャレンジを生成できなくなるという、可能性の低い場合において、e U I C Cは、別のチャレンジセットを解放するよう特別に指定された、別個の確保されたチャレンジセットを記憶することができる。場合によっては、e U I C Cは更に、相手先ブランド名製造者(OEM)認証情報を含めることができ、OEMはこれを使用して更にチャレンジ操作を制御することができる。

40

【 0 0 6 2 】

ここで図7を参照して、e S I Mのための1つの例示的なデータ構造が図示されている

50

。図示されているように、例示的なデータ構造は、3つの部分を含み、このそれぞれが、L1、L2、及びL3セキュリティレベルである。セキュリティ構成要素を別個のレベルに分離することによって、全体的なネットワーク動作を、幅広いオプションにより、複数のエンティティにわたって分散することができる。例えば、様々なネットワークエンティティが、セキュリティ層を1つ又は2つだけ実施することができる（例えば、eSIM業者はL2のみを取り扱うことができるなど）。この柔軟性により、事実上、任意のビジネス構成に容易、有利に適合させることができる。

【0063】

図7に示すように、非対称暗号化（すなわち、各エンティティが異なる一意の鍵を有する）は対称動作（エンティティが鍵を共有）よりもずっと遅いため、各eSIMプロファイル構成要素702は対称鍵で暗号化され、この対称鍵は、予定されたeSIM受信者のL1公開鍵で暗号化される。このeSIMは更に、メタデータ（例えば、ICCIDの文字列）のための平文部分を含み得る。暗号化された対称鍵、メタデータ、及び暗号化されたeSIMコンテンツは、「供与側」L1エンティティの公開鍵でハッシュされ、署名される。関連するL1証明書が、検証のために、（例えば、末尾に）添付される。

【0064】

図7のバッチ記述子構成要素704は、eSIMのL2情報を含む。これは、グローバル意識別子（GUID）、予定されたeSIM受信者に対するチャレンジ、そのeSIM受信者の一意のID、プロファイルを取得するためのURL、及びインストール結果をポストするためのURLを含む平文部分を有する。このバッチ記述子は更に、次のものからなる要素の配列の平文部分を含む。各プロファイルのICCID、及びプロファイルのハッシュされた部分（メタデータ部分及び暗号化されたeSIMコンテンツ）。一実施形態において、このハッシュは対称鍵を含まず、これによってバッチ記述子を、実際のプロファイルが生成されるのを待たずに生成することができる。機器側の動作のために、バッチ記述子は、1つのICCIDとプロファイルハッシュを含むだけである。サーバ間バッチ移動のためには、ずっと大きな配列が期待される。バッチ記述子のデータコンテンツはL2公開鍵でハッシュ及び署名され、関連するL2証明書が末尾に添付される。

【0065】

L3所有者構成要素706は、そのeSIMのためのL3情報を含む。このプリンシパルフィールドは、eSIMに関連付けられているユーザアカウント（例えばabc@me.com）を特定し、サービス名は、これでユーザアカウントを認証するサービスプロバイダを特定する。バッチ記述子のハッシュは、L2及びL3データ構造を関連付けるために含まれる。このデータは、L3公開鍵でハッシュ及び署名され、平文内に記憶される。L3証明書は末尾に添付される。

【0066】

本明細書で使用される場合、証明書には、eUICC証明書、サーバアプライアンス証明書、及びOEM証明書の3つのタイプがある。一実施形態において、信頼されるサードパーティが、認証されたeUICCに対する証明書を発行する。各eUICCは、このエンティティ、又はこのエンティティに従属する鍵権限者によって発行された、公開鍵及び関連付けられた証明書を含む。いくつかの実施形態において、1つの信頼されるサードパーティが、認証されたL1、L2、及びL3アプライアンスに対する証明書を発行し得る。またあるいは、別のサードパーティエンティティが、L1、L2、又はL3アプライアンスに対する証明書を発行し得る。複数のサードパーティが存在する場合、eUICCは、サードパーティのルート証明書認証局（CA）を事前ロードし（又は信頼されるエンティティからのOTAを供給され得る）、適切なCAに基づいてサーバアプライアンスから受け取ったメッセージを検証することができる。

【0067】

ここで図8を参照し、1つの例示的なOEM証明書階層が示されている。ルート証明書認証局（CA）は、タスクのサブセット（例えば、iOSなどの発行、又は匹敵する機器証明書の発行）を実行する一組の中間CAを有する。図示のように、eUICC CAに

10

20

30

40

50

はeSIM固有の動作が搭載されている。eUICC CAは一組のサーバに対して証明書を発行できる。図示のように、この証明書には例えば、eUICC保守のための工場リファビッシュサーバ、及びeUICC PCFに署名するアクチベーションサーバが含まれる。ルートCAは、eUICC CAの共通名と合わせて、クライアントeUICCによって使用され、OEM署名のメッセージを検証する。

【0068】

上記に従い、例示的な一実施形態において、各クライアントeUICCは次のセキュリティ関連データを記憶する。(i) eUICC L1、L2、及びL3動作に使用されるeUICC証明書(各eUICCはL1、L2、及びL3セキュリティ関連動作両方に使用される証明書を記憶する)、(ii) eUICC証明書に関連付けられているeUICC秘密鍵、(iii) OEMのルート証明書及びOEM eUICC CAの共通名を含む、OEM認証情報、並びに(iv) サーバアプライアンスを認証できるサードパーティのルート証明書。いくつかの変異において、eUICCの証明書は、CA署名が侵害された場合に交換する必要があるあり得る。例えば、eUICC CA又はサーバCAが侵害された場合(例えば、秘密鍵が侵害/紛失した場合)、2つの失効手順が下記に記述される。

【0069】

第1の例示的な失効手順により、eUICC証明書を発行する署名CAが侵害された場合、影響を受けたeUICC内に記憶されているeUICC証明書は交換されるべきである。具体的には、そのeUICCに対して初期証明書要求が生成されたとき、その証明書署名要求(CSR)が保存されている。署名CAが侵害された場合、初期CSRを使って、そのeUICCに対して新しい証明書を要求することができる。同じCSRを保持することにより、eUICCは同じ秘密鍵を使用することができ、同じeUICC公開鍵を含んだ新しい証明書が発行される。OEMは、そのOEMの秘密鍵を使って、新しい証明書を署名できる。eUICCがサーバブローカーに要求を送ると、ブローカーは不良eUICC CAの失効リストをチェックし、その証明書を交換する必要がある旨を示した特定のエラーをもってその要求を却下することができる。APは、既存のOEMサービスを介して新しいeUICC証明書を取得し、その新しい証明書をeUICCに送ることができる(APはこのシナリオにおいて信頼されている必要はない)。

【0070】

この後、eUICCはOEM署名を検証し、受け取った公開鍵が、前にeUICCに記憶された公開鍵に合致していることを確認する。いくつかの変異において、サービス拒否(DOS)攻撃又はリプレイ攻撃を防ぐために、eUICCは更にeUICC証明書を含む。一変異において、新しい証明書が発行されると、このエポックが増加する。eUICCは、受け取った証明書のeUICCエポックが、現行の証明書のそれよりも高いことを検証してから、新しい証明書を記憶することができる。

【0071】

残念ながら、様々なeUICCリソースの制限により、eUICCにおいてサーバ証明書を失効させるのは困難であり得る。すなわち、大きな失効リストの処理は、1つのeUICCには対処できない可能性がある。失効リストの保守を回避するため、第2の失効方式においては、各サーバ証明書が追加として1つのエポックに関連付けられる。CAが侵害されたとき、ルートCAが正当なすべてのエンティティに対して証明書を再発行し、新しい証明書のそれぞれのエポックを増加させる。サーバ証明書の数は大きくならないため、証明書の再発行は既存のシステムで扱うことができる。クライアントeUICCにおいて、このeUICCは、サーバL1、L2、及びL3証明書の予期されるエポックを、不揮発性メモリに保存する。受信した証明書が高いエポックを含む場合、eUICCは対応するNVエポックを更新しなければならず、より低いエポックの証明書を今後却下しなければならない。すなわちeUICCは、CAが侵害されて以来署名していない不良サーバを却下する。いくつかの変異において、このサーバは更に、侵害されたeUICCに関するeUICCブラックリストを保守し得る。一実施形態において、ブラックリストに掲載されたeUICCからの要求は、サーバにより却下される。

10

20

30

40

50

【 0 0 7 2 】

ポリシー制御機能

上記のセキュリティ解決策のコンテキストにおいて、(i) e U I C C プラットフォームレベル、及び(i i) プロファイルレベルの、2つのレベルのポリシー制御機能(P C F)がある。例示的な一実施形態において、e U I C C P C FはO E Mによってのみ更新することができ、一方、プロファイルP C FはM N Oによって制御され、e S I Mの一部である。そのような1つの変異において、e S I Mがエクスポート及び/又はインポートされた場合、プロファイルP C Fはエクスポート/インポートパッケージの一部として含まれる。

【 0 0 7 3 】

ここでe U I C C P C Fを参照して、e U I C C P C Fは次のものを含み得る。(i) e U I C C がアクチベーションし得るe S I Mのタイプを特定するS I Mロックポリシー、(i i) e U I C C 内のすべてのe S I Mの削除を承認するのに使用することができる秘密のコード、(i i i) e U I C C が通信し得るサーバアプライアンスのクラスタを特定するサーバ(L 1、L 2、及びL 3)の共通名のリスト(例えば、ビジネス検討事項又は方法に基づく)(すなわち、包含リスト)、(i v) e U I C C が通信することができないサーバアプライアンスのクラスタを特定するサーバ(L 1、L 2、及びL 3)の共通名のリスト(すなわち、除外リスト)。

【 0 0 7 4 】

同様に、プロファイルP C Fは次のものを含み得る。(i) e U I C C がe S I Mをエクスポートし得るデポのクラスタを特定するサーバ(L 1、L 2、及びL 3)の共通名のリスト(包含)、(i i) e U I C C がe S I Mをエクスポートできないデポのクラスタを特定するサーバ(L 1、L 2、及びL 3)の共通名のリスト(除外)、(i i i) 特定されたe S I M動作の完了時に通知が送られるU R Lを特定する、通知U R L及び動作タイプ、(i v) プロファイルが失効になったときにA Pがe S I Mを削除し得る場合の、自動失効パラメータ、(v) 実施されるセキュリティレベルを示す別のクラスが割り当てられ得るサーバアプライアンス(L 1、L 2、及びL 3)のクラス(プロファイルは、特定のレベルを超えるサーバ構成要素とのみ通信するように選択することができる)、(v i) インストール中にチェックされるサーバ証明書(L 1、L 2及びL 3)のエポック(例えば、e U I C C サーバ証明書のエポックが指定されたエポック以上である場合にのみ、e U I C C はプロファイルをインストールする)、(v i i) L 3 認証が使用し得るL 3 サービス名、及び/又は、L 3 認証が使用できないサービス名のリスト、(v i i i) e U I C C システムの最少バージョン(指定された最少バージョン以上のe U I C C システムにのみ、e S I Mがインストールされ得る)、(i x) そのe S I Mに必要な最小R A Mサイズ(O T A 動作を含まない)、(x) O T A のために確保される最小R A Mサイズ、(x i) e S I Mのために必要な最小の不揮発性(N V)メモリサイズ(O T A のために用いられるスペースを除く)、(x i i) O T A のために確保される最小N V サイズ。

【 0 0 7 5 】

例示的な動作

上記の構成要素(例えば、e U I C C、e S I M、ブローカーネットワーク、セキュリティプロトコルなど)のコンテキスト内で、下記の例示的なメッセージングシーケンスが開示される。以下のシーケンス図において、ブローカー、プロファイルエージェント、及びプロファイルロッカーの3つのエンティティが表わされ、これはそれぞれL 3、L 2、L 1セキュリティを担当するエンティティを表わす。ただし、これらは論理エンティティであって、別のネットワークトポロジーを包含することが可能であり、また、それらの上記機能を更に差別化することが可能であることが理解されよう。

【 0 0 7 6 】

クライアントe U I C Cは、図示の実施形態において、3つのセキュリティレベルすべてを担当している。ただし、明確さのため、クライアントe U I C Cは、そのe U I C C

10

20

30

40

50

内での機能的要件を捕捉するため、3つの論理エンティティに分けられている。加えて、クライアントeUICC内のL1、L2、及びL3のための別の認証情報セットがあってもよいが、クライアント機器は単一の機器であるため、同じ（すなわち、1つの認証情報）が使用され得ることが理解されよう。

【0077】

eSIM配信、パーソナライズなし

図9は、パーソナライズなしでeSIMを機器に配信するための、1つの例示的な論理シーケンスを示す。最初に、機器は発見プロセス（図示なし）を介してサーバブローカーを特定する。機器がサーバブローカーと通信を試みた後、次の3つの主な動作がある。（i）機器が、利用可能なeSIMオプションについてサーババックエンドにクエリを行う、（ii）要求したeSIMが事前パーソナライズされていない場合、サーバがeSIMをパーソナライズするよう、機器が要求する、及び、（iii）機器が実際のeSIMをダウンロードし、これをインストールする。

10

【0078】

第1段階で、機器がgetProfileOptionsを使用し、使用可能なeSIMオプションについてサーババックエンドにクエリを行う。機器に関連付けられているeUICCは、UniqueIdにより特定され、これは、例えば、カードのシリアル番号であり得る。ブローカーは、機器に利用できる1つ以上のeSIMオプションを決定するため、販売情報を利用する。ロック解除された機器については、利用可能なeSIMの非常に大きなセットがある可能性がある。よって、いくつかの実施形態において、ユーザが選択する可能性が高い一般的なオプションが表示される（例えば、ロケーション、費用などに基いて）。サーバは、その機器に有効なプロファイルプロバイダ（MNO）及びプロファイルタイプ（例えば、プリペイド/ポストペイド）のアレイを返す。

20

【0079】

いくつかのシナリオにおいて、ユーザが利用できるeSIMのタイプは、プライベート情報と考えられ得るため、いくつかの変異において、getProfileOptionsAPIが更に機器のeUICCL3に対しeUICCの一意の識別子に署名し、その署名された識別子をAPIに含めるように要求する。サーバブローカー（又はブローカーサーバ）は、署名を検証してからその要求を処理することができる。これにより、なりすまされた要求を送信することによって悪意ある者がユーザのプロファイルオプションを取得するのを妨げる。いくつかの変異において、機器ブローカーとサーバブローカーの間の通信にはセキュリティプロトコル（例えば、トランスポート層セキュリティ（TLS））を使用して、取得及びリプレイ攻撃を防ぐ。

30

【0080】

一実施形態において、getProfileOptionsは、eSIMの現行及び新しい所有権を検証するため、2つのL3トークンを含む。現行L3トークンは一意の識別子、又はいわゆる「偽カード」スクラッチコードであり得る。新しいL3トークンは、ユーザアカウントをeSIMと関連付けるのに使用される情報であり得、例えば、iCloudアカウントのためのサインオントークンであり得る（例えば、機器がトークンを取得するためにユーザアカウントにログインされている場合）。両方のL3トークンが、eUICCL3により署名される。サーバブローカーは、関連付けられた認証サービスを使用してL3トークンを認証する。例えば、ネットワークサーバ（例えば譲受人のiCloudサーバ）、又はサードパーティサービスと通信して、サインオントークンを検証することができる。

40

【0081】

性能を最適化し、重複の認証を避けるため、機器により渡されたトークンを認証した後、サーバブローカーは、ワンタイムコード（OTC）を生成し、そのOTCを機器に戻し渡す。機器は、サーバが既にL3認証を実施した証明としてこのOTCを使用することができる。完全なデータのバイナリラージオブジェクト（BLOB）は、生成されたOTC、一意の機器識別子（例えば、カードのシリアル番号（CSN））、プリンシパル、サー

50

ビスプロバイダ、及びそのOTCの有効性を示すタイムスタンプを含み得る。このBLOBは、ブローカーにハッシュされ、署名される。一変異において、ハッシュは、全体の性能を改善するために対称鍵で実施される。getProfileOptionsがeSIMのアレイを返した場合、ユーザには選択を行うプロンプトが提示される。

【0082】

第2段階において、機器はpersonalizeProfileを呼び出し、eSIMをパーソナライズするようサーババックエンドに要求する。機器がパーソナライズの要求をサーバに送る前に、認証のため、eUICCプロファイルエージェントとサーバプロファイルエージェントとの間でハンドシェイクセッションがある。機器ブローカー及びeUICCは、ユーザが選択したプロファイルオプション、及びサーバブローカーから送られた現行のL3コード及び新しいL3コードに基づいて、セッションを作成する。eUICCはこの情報を保存して、以後これにより送られるプロファイル要求を満たすことができる。eUICCプロファイルエージェントは、セッションIDを作成し、これは以後、これに対する認証のために、サーバエージェントによりエコーバックされる。

10

【0083】

機器ブローカーはこれで、eUICCにより生成された要求セッションを、サーバブローカーに渡すことができる。サーバブローカーは、この要求をチェックすることができる。例えば、サーバブローカーは、一意のIDにより表わされたeUICCの要求がサービス可能であるかどうかを判定する。一意の識別子は平文に含まれているため、サーバプロファイルエージェントによって、より徹底した要求検証が実施されるけれども、サーバブローカーはこの情報を取得することができる。

20

【0084】

要求が適切な場合、サーバブローカーはその要求をプロファイルエージェントに渡す。プロファイルエージェントは、eUICC L2証明書を検証し、eUICC L2公開鍵を使用してL2署名を検証することによって、その要求を暗号により検証する。検証が合格すると、サーバプロファイルエージェントはSessionResponseを作成し、これには次のものを含む平文部分が含まれる。受信したセッション識別子及び一意の識別子、L2署名(平文部分のハッシュと、サーバプロファイルエージェントの秘密鍵を使ってそのハッシュに署名することによって生成)、及びサーバプロファイルエージェントの証明書。

30

【0085】

セッション応答はサーバプロファイルエージェントからサーバブローカーに送られ、これは次に、セッション応答を機器ブローカーに転送する。機器ブローカーはこの応答を、prepareProfileRequestメッセージ内でeUICCに渡す。eUICC L2は、サーバプロファイルエージェントの証明書及びL2署名を検証することにより、sessionResponseを検証する。eUICC L2は更に、セッション識別子及び一意の識別子が、eUICC内の情報に合致することを検証する。検証が合格したら、eUICCはパーソナライズされたプロファイル要求に対するチャレンジを作成する。このチャレンジは不揮発性メモリに記載される。eUICCは次に、L1、L2及びL3関連情報を含むプロファイル要求BLOBを作成する。詳細な構造は本明細書の付録Aに記載されており、参照により本明細書に組み込まれる。

40

【0086】

次に、プロファイル要求BLOBがサーババックエンドに送られる。サーバブローカーはL3検証を行い、eSIMを関連付けるためのL3所有者情報(例えば、プリンシパル及びサーバプロバイダ)を含む。このサーバプロファイルエージェントは、バッチ記述子を作成し、サーバプロファイルブローカーはそのeUICCのためのeSIMをパーソナライズする。パーソナライズされたeSIMは、性能最適化のため、コンテンツ配信ネットワーク(CDN)に分散され得る。

【0087】

機器ブローカーは、プロファイル記述子及び関連するL3所有者情報を受け取った後、

50

受け取ったGUID（グローバル意識別子）を提供することにより、getProfileを介して、関連付けられたプロファイルを取得する。

【0088】

機器ブローカーがプロファイル記述子及びプロファイルを取得すると、クライアントeUICCに対し、eSIMをインストールするよう指示を行う。この呼び出しフローは3つの異なる呼び出し、processL3Owner、processProfileDescriptor、及びinstallProfileを示しているが、ただし、実際の実装においては、これら3つの論理呼び出しは、単一のトランザクション内に組み合わせることができることが理解されよう。eUICCはL3、L2、及びL1検証を実施し、検証された後、eSIMがインストールされる。関連付けられたチャレンジは削除される。L3所有者情報は、適切な所有権を示すため、eSIMと一緒に保存される。L3所有者情報は、ユーザがeSIMをエクスポートした場合、後の時点で提供することができる。

10

【0089】

プロファイルがインストールされると、eUICCはインストール結果をサーバに返す。サーバインフラストラクチャは、コンテンツ配信ネットワーク(CDN)内のキャッシュされたコンテンツのページをトリガする通知を使用することができる。場合によっては、この情報は更に、例えば、インストール成功、部分的インストール、インストール失敗などを示す通知サービスのために使用することもできる。

【0090】

eSIM配信、事前パーソナライズ

図10は、事前パーソナライズを伴ってeSIMを機器に配信するための、1つの例示的な論理シーケンスを示す。図9の方式と同様、事前パーソナライズされたeSIMの配信には3つの段階が必要である。

20

【0091】

最初に、クライアント機器の製造中に、工場ブローカーがeUICCに対し、eSIM事前パーソナライズに対するチャレンジを後で作成するよう指示を行う。ただし、図9の方式とは異なり、機器はまだMNOにも、またeSIMタイプにも関連付けられていない。代わりに、これらのフィールドは特別な値が入れられ、選択が後で行われることを示す。プロファイル要求BLOBの完全なコンテンツは、後でのパーソナライズ使用のために保存される。

30

【0092】

第2段階は、例えば、出荷通知、機器販売などにより自動的にトリガされる。配信センターL2（クライアントプロファイルエージェント）は、クライアントeUICC L2のためのプロキシとして機能する。eUICCプロファイル要求BLOBはMNO及びeSIMタイプを含んでいないが、クライアントプロファイルエージェントは、これらのフィールドを更新情報で置き換えることにより、BLOBを再生成することができる。クライアントプロファイルエージェントは、それ自体のチャレンジを生成し、eUICCチャレンジを置換することができる。クライアントプロファイルエージェントはそれ自体の秘密鍵でコンテンツの署名を行う（そうでなければ、すべてのL2が一意的なチャレンジを必要とすることになる）。BLOBはeUICCのL1署名を含み、このeUICCは依然として、パーソナライズされたeSIMの暗号を復号する必要がある。新しいプロファイル要求BLOBは、既存のpersonalizeProfile要求を使用して、サーバブローカーに送られる。これ以降の手順は、図9の手順と違いはない。

40

【0093】

加えて、MNOがそれ自体のブローカーシステムをサポートしたい場合であっても、本開示の事前パーソナライズプロセスは同じインタフェースを使用できることが理解されよう。サーバブローカーは、バッチ記述子をクライアントに返し、eSIMをパーソナライズする。クライアントプロファイルエージェントはeUICCのチャレンジで新しいバッチ記述子を作成し、これは、eUICCがプロファイルを後で要求したときに使用される

50

【0094】

最後に、最終段階で、ユーザが機器の電源を入れると、機器が `getProfileOptions` を実行して、使用できる `eSIM` オプションをチェックする。`eSIM` がすでに事前パーソナライズされているため、この応答には有効なバッチ記述子が含まれ、機器はもはや `personalizeProfile` を呼び出す必要はない。これは、`getProfile` 要求を介して `eSIM` を直接取得するための記述子内の情報を使用し得る。

【0095】

`eSIM` 配信、バッチ配信

図11は、例えば、2つのエンティティの間で多数の(バッチ) `eSIM` を配信するための1つの例示的な論理シーケンスを示す。一実施形態において、クライアントブローカー及びサーバブローカーは、例えば、仮想プライベートネットワーク(VPN)を介したセキュアな通信を有するセキュアなエンティティである。「バッチ化」は、クライアントが大量の `eSIM` を注文できるようサポートされる。

【0096】

このシナリオにおいて、プロファイルエージェントがプロファイルをパーソナライズする要求を受信した場合、このプロファイルは、バッチ記述子が返されている場合はパーソナライズする必要はない。むしろ、クライアントは所望に応じて後の段階で実際のプロファイルを要求することができる。バッチ記述子動作において、プロファイルコンテンツのハッシュは、暗号化されたプロファイル(対称鍵でラップされている)及びプロファイルメタデータを用いて計算され、これらのいずれも、プロファイルをパーソナライズする必要はない。また、L1が `eUICC` ごとに対称鍵を記憶する必要もない。これは、記憶する必要がある場合は、充足するのが難しい追加記憶容量要件によってL1の大きな負担となり得る。一実施形態において、暗号化 `eSIM` (対称鍵でラップされている)は、外部記憶装置に記憶することができる。対称鍵はL1 RFS(リモートファイルシステム)鍵でラップされてもよく、このラップされた鍵は、暗号化された `eSIM` と一緒に外部記憶装置に保存することができる。

【0097】

`eSIM` エクスポート

最後に、`eSIM` がクライアント機器に記憶されると、ユーザは選択により、機器外に `eSIM` をエクスポートし、後でこの `eSIM` を同じ又は異なる機器にインポートすることができる。目的の1つは、`eSIM` のスワップをサポートすることである。もう1つの目的は、追加の `eSIM` を記憶するために `eUICC` メモリのスペースを解放することである。エクスポートする際は、次の3つの可能なシナリオがある。(i)クラウドにエクスポートする、(ii)AP(オフボード記憶装置用)にエクスポートする、及び(iii)機器間 `eSIM` 転送を行う。同様に、ユーザは、クラウド、AP、又はその他の機器からインポートすることができる。

【0098】

`eSIM` インストール中、ユーザアカウント情報は `eSIM` に関連付けられる(ユーザがオプトアウトしない限り)。アカウント情報には、L3認証のための十分な情報が含まれる。例えば、これには、認証のための、プリンシパル(例えば、`x2z@yahoo.com`)、及びそれに関連付けられたサービスプロバイダが含まれ得る。`eSIM` に関連付けられたアカウント情報がない場合は、ユーザは他の認証方法と共に `eSIM` をエクスポートすることができる。そのような一実施形態は、機器の物理的な所有を証明する `eUICC` にセキュアに接続されている物理的なボタンを含む。別の実施形態において、各 `eSIM` は一意のパスワードを含み、ユーザは自らの所有権を証明するパスワードを有しなければならない。OEM認証情報を使用することも更に別のオプションである。

【0099】

ユーザが `eSIM` をエクスポートする場合、APは `eUICC` から、インストールされ

10

20

30

40

50

たプロファイルのリストを取得する。各プロファイルについて、eUICCは更に、関連付けられたプリンシパルと、リプレイ防止のために生成されたノンスとを返す。ユーザがプロファイルをエクスポートすることを選択した場合、APはプリンシパルに含まれる情報を使用して、サービスプロバイダからシングルサインオン(SSO)トークンを取得し、ユーザには、この目的のためにユーザ名とパスワードを入力するようプロンプトが提示され得る。SSOトークンは、エクスポート要求において、プリンシパル及びノンスと一緒にサーバブローカーに渡される。サーバブローカーは、機器により供給されたSSOトークンを使用して、サービスプロバイダと共に認証を処理することができる。認証が合格すると、フローは機器へのeSIM配信を反映するが、ただしクライアントとサーバの役割は逆転する。高レベルにおいて、サーバブローカーはeUICCとのセッションを開始し、そのエクスポートのための要求BLOBを作成する。この要求には、動作がL3認証に合格したことを示すための、eUICCが生成したノンスが含まれる。eUICCは要求BLOBを検証し、サーバエージェントの公開鍵を使ってeSIMを暗号化し、そのeSIMのためのパッチ記述子及びL3所有者情報を作成する。L3及びL2情報と共にeSIMは、サーバに送られ得る。

【0100】

eUICCがエクスポートのためにeSIMを暗号化すると、eUICCはそのeSIMの所有権を放棄し、そのeSIMをもはや使用しないか、あるいはそのeSIMを任意の他のエンティティにエクスポートしない。いくつかの場合において、eUICCは暗号化されたコピーを保存して、接続喪失(すなわち、暗号化eSIMがサーバに全く到達しない場合)からのリカバリに役立てることができる。あるいは、APは、接続障害の場合に再送信を行うため、暗号化されたeSIMのコピーを保存し得る。サーバは承認を返すことができ、これによりAPをトリガして、記憶されたコピーを除去する。

【0101】

いくつかの実施形態において、エクスポートは、ウェブポータルから開始することもできる。ユーザが自分の機器を紛失した場合は、ウェブポータルを使用して、自分の機器からeSIMをエクスポートすることができる。この場合、ウェブポータルはその機器と通信を行って、エクスポート動作を開始し得る。このフローは同様であるが、ただし、ユーザはAPの代わりにウェブポータルを使用して、所有権検証のためにSSOトークンを取得し得る。

【0102】

装置

上述の方法に関連して有用な様々な装置が、ここで詳しく記述される。

【0103】

eUICCアプライアンス

図12は、本開示によるeUICCアプライアンス1200の例示的な一実施形態を示す。eUICCアプライアンスは、スタンドアロンのエンティティを含み得、又は、例えばサーバなどの他のネットワークエンティティを組み込み得る。図示のように、eUICCアプライアンス1200は一般に、通信ネットワークとのインタフェースのためのネットワークインタフェース1202、プロセッサ1204、及び1つ以上の記憶装置1206を含む。ネットワークインタフェースはMNOインフラストラクチャに接続した状態で示されており、これにより、他のeUICCアプライアンスへのアクセス、及び1つ以上のモバイル機器への直接的又は間接的なアクセスが提供されているが、ただし、他の構成及び機能に置換することもできる。

【0104】

一構成において、このeUICCアプライアンスは次のことが可能である。(i)他のeUICC(eUICCアプライアンス又はクライアント機器)との通信を確立する、(ii)eSIMをセキュアに記憶する、(iii)セキュアに記憶されたeSIMを取得する、(iv)他の特定のeUICCに配信するために、eSIMを暗号化する、及び(v)eSIMデポとの間で複数のeSIMの送信のやりとりを行う。

10

20

30

40

50

【 0 1 0 5 】

e S I M デポ

図 1 3 は、本開示による e S I M デポ 1 3 0 0 の例示的な一実施形態を示す。e S I M デポ 1 3 0 0 は、スタンドアロンエンティティとして実施することができ、あるいは、他のネットワークエンティティ（例えば、e U I C C アプライアンス 1 2 0 0）を組み込み得る。図示のように、e S I M デポ 1 3 0 0 は一般に、通信ネットワークとのインタフェースのためのネットワークインタフェース 1 3 0 2、プロセッサ 1 3 0 4、及び記憶装置 1 3 0 6 を含む。

【 0 1 0 6 】

図 1 3 に図示される実施形態において、e S I M デポ 1 3 0 0 は次のことが可能である。
 (i) e S I M のインベントリ管理（例えば関連付けられているメタデータを介して）、
 (i i) 暗号化された e S I M のための（例えば、他の e S I M デポ及び/又は e U I C C アプライアンス 1 2 0 0 からの）要求に対する応答、
 (i i i) e S I M のための加入者要求の管理。

10

【 0 1 0 7 】

例えば、ある e S I M がユーザにより e S I M デポ 1 3 0 0 に記憶されているとき、その e S I M は意図された行先と共に記憶することができ（例えば、他の機器への転送を促進するため）、又は無期限に駐留させることができる。いずれの場合でも、e S I M デポは、セキュアな記憶、及び行先装置向けのその後の暗号化のために、e S I M を e U I C C アプライアンスに提供することができる。

20

【 0 1 0 8 】

ユーザ装置

ここで図 1 4 を参照して、本開示の様々な態様による例示的なユーザ装置 1 4 0 0 が図示されている。

【 0 1 0 9 】

図 1 4 の例示的な U E 装置は、プロセッササブシステム 1 4 0 2（例えば、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は 1 つ以上の基板に搭載された複数の処理構成要素）を備えた無線機器である。この処理サブシステムはまた、内部キャッシュメモリも含み得る。この処理サブシステムは、メモリサブシステム 1 4 0 4 と通信しており、メモリサブシステムには例えば、S R A M、フラッシュ、及び/又は S D R A M 構成要素を含み得るメモリが含まれる。このメモリサブシステムは、当該技術分野において周知のようにデータアクセスを促進するために、1 つ以上の D M A タイプのハードウェアを実装することができる。このメモリサブシステムは、プロセッササブシステムにより実行可能な、コンピュータ実行可能命令を含む。

30

【 0 1 1 0 】

例示的な一実施形態において、この機器は、1 つ以上の無線ネットワークに接続するよう適合された、1 つ以上の無線インタフェース 1 4 0 6 を含む。複数の無線インタフェースは、例えば、G S M、C D M A、U M T S、L T E / L T E - A、W i M A X、W L A N、B l u e t o o t h（登録商標）などの異なる無線技術を、無線技術分野で周知である適切なアンテナ及びこの種の現行のサブシステムを実装することによりサポートし得る。

40

【 0 1 1 1 】

ユーザインタフェースサブシステム 1 4 0 8 は、任意の数の周知の I / O を含み、これには、キーパッド、タッチスクリーン（例えば、マルチタッチインタフェース）L C D ディスプレイ、バックライト、スピーカー、及び/又はマイクロホンが挙げられるがこれらに限定されない。しかしながら、特定の適用例では、これらの構成要素のうちの 1 つ以上が不要となり得ることが認識されよう。例えば、P C M C I A カードタイプクライアントの実施形態は、ユーザインタフェースが欠如する場合がある（それらは、物理的及び/又は電氣的に結合されるホスト機器のユーザインタフェースを、便乗して利用することが可能であるため）。

50

【 0 1 1 2 】

図示の実施形態において、機器には、e U I C Cアプリケーションを含み動作するセキュアエレメント1410が含まれる。このe U I C Cは、ネットワークオペレータとの認証に使用するための、複数のアクセス制御クライアントを記憶し、これにアクセスすることができる。セキュアエレメントには、セキュアな媒体に記憶されているソフトウェアを実行するセキュアプロセッサが含まれる。このセキュアな媒体は、他の構成要素（セキュアプロセッサ以外）に対してはアクセス不可である。更に、例示的なセキュアエレメントは、前述のように、改ざんを防止するために更に硬化することができる（例えば、樹脂に封入）。例示的なセキュアエレメント1410は、1つ以上のアクセス制御クライアントを受信し記憶することができる。一実施形態において、セキュアエレメントは、ユーザに関連付けて（例えば、1つを仕事用、1つを個人用、いくつかをローミングアクセス用、など）、及び/又は他の論理方式又は関係に従って（例えば、1つを家族又は事業エンティティの複数の各メンバー用、1つを家族メンバーの個人と仕事用それぞれに、など）、e S I Mのアレイ又は複数のe S I Mを記憶する。各e S I Mには小さなファイルシステムが含まれ、これにはコンピュータ可読命令（e S I Mプログラム）及び関連データ（例えば、暗号鍵、完全性鍵など）が含まれる。

10

【 0 1 1 3 】

このセキュアエレメントは更に、モバイル機器との間のe S I Mの転送を可能にするよう適合することができる。一実施形態において、モバイル機器はG U Iベースの承認を提供して、e S I Mの転送を開始する。

20

【 0 1 1 4 】

モバイル機器のユーザがe S I Mのアクチベーションを行うことを決めると、そのモバイル機器は、アクチベーションサービスにアクチベーションの要求を送る。モバイル機器は、標準の認証及び鍵合意（A K A）交換のためにe S I Mを使用することができる。

【 0 1 1 5 】

方法

上述の方法に関連して有用な様々な方法が、ここで詳しく記述される。

【 0 1 1 6 】

図15は、電子アクセス制御クライアントの大規模配信のための方法の一実施形態を示す。

30

【 0 1 1 7 】

ステップ1502で、第1の機器が、1つ以上の電子アクセス制御クライアントの所有権を確立する。

【 0 1 1 8 】

ステップ1504で、この第1の機器が、1つ以上の電子アクセス制御クライアントが以前に複製されていないかどうかを判定する。

【 0 1 1 9 】

ステップ1506で、この第1の機器が、第2の機器への転送のために、1つ以上の電子アクセス制御クライアントを暗号化する。

【 0 1 2 0 】

ステップ1508で、第1の機器及び第2の機器が、暗号化された1つ以上の電子アクセス制御クライアントの交換又は転送を行う。

40

【 0 1 2 1 】

本開示により、当業者には、電子アクセス制御クライアントの大規模配信のための、他の無数の方式が認識されよう。

【 0 1 2 2 】

本開示の特定の態様が、特定の方法の具体的なステップのシーケンスの観点から説明されているが、これらの説明は、本開示のより広範な方法の例示に過ぎないものであり、具体的な適用によって、必要に応じて修正することができる点が、認識されるであろう。特定のステップは、特定の状況下では、不必要又は任意選択とすることができる。更には、

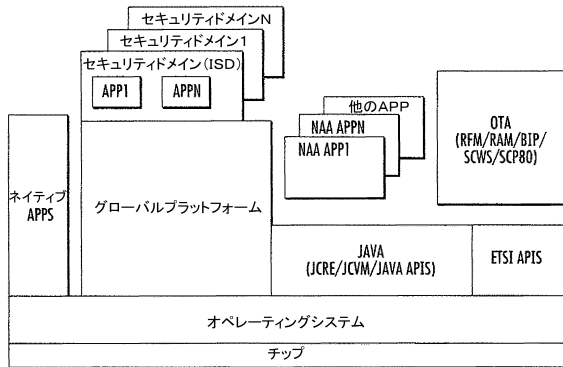
50

特定のステップ又は機能性を、開示される実施形態に追加することができ、あるいは2つ以上のステップの実行の順序を、置き換えることもできる。全てのそのような変更形態は、本明細書で開示され特許請求される、本開示の範囲内に包含されると見なされる。

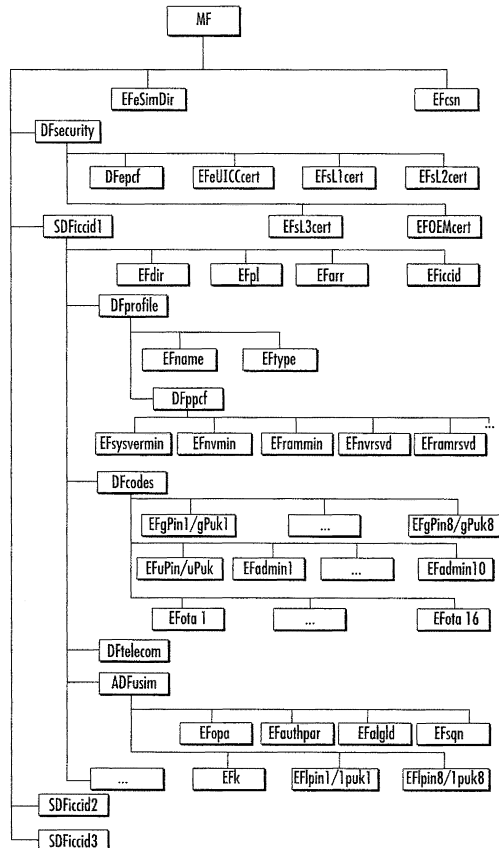
【 0 1 2 3 】

上記の発明を実施するための形態は、様々な実施形態に適用されるような、本開示の新規の機構を示し、説明し、指摘しているが、例示された機器又はプロセスの形態及び詳細の様々な省略、置換、並びに変更を、本開示から逸脱することなく当業者によって実施することができる点が理解されるであろう。上記の説明は、本開示の実施について現時点で想到される最適な例である。本説明は、限定することを決して意図するものではなく、むしろ、本開示の一般的原理の例示として解釈されるべきである。本開示の範囲は、特許請求の範囲に準拠して決定されるべきである。

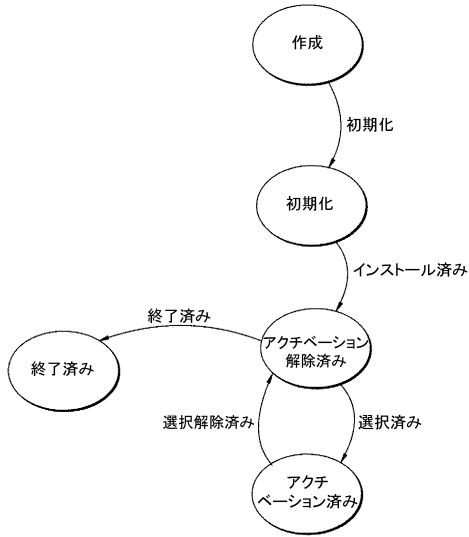
【 図 1 】



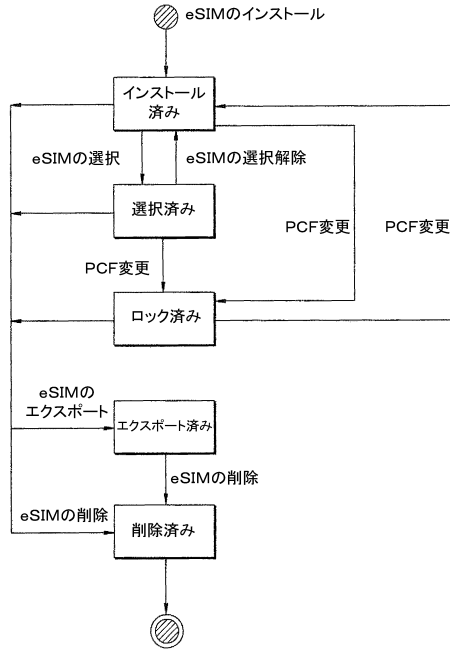
【 図 2 】



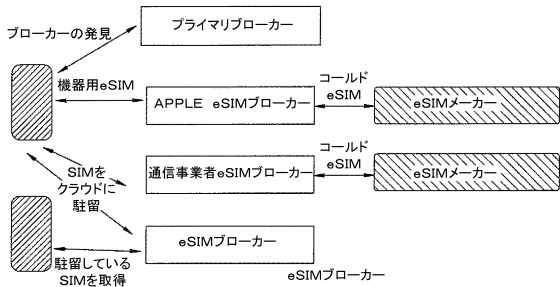
【図3】



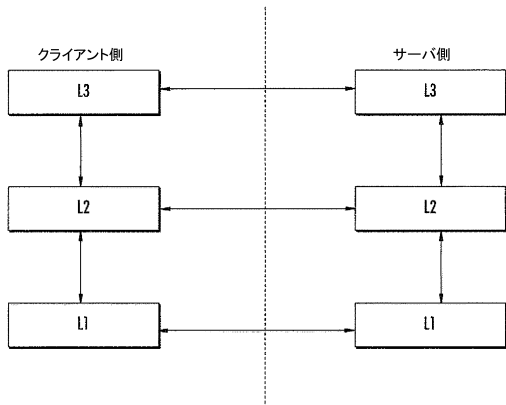
【図4】



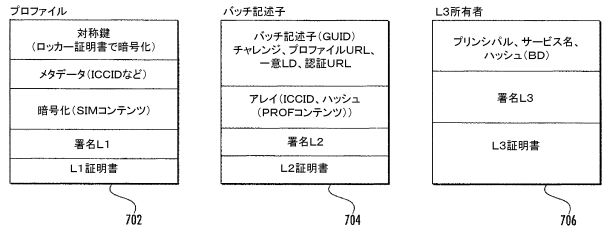
【図5】



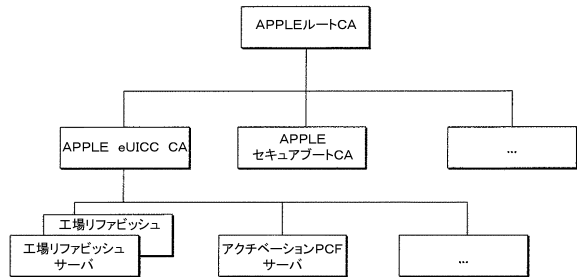
【図6】



【図7】



【図8】



【図9A】

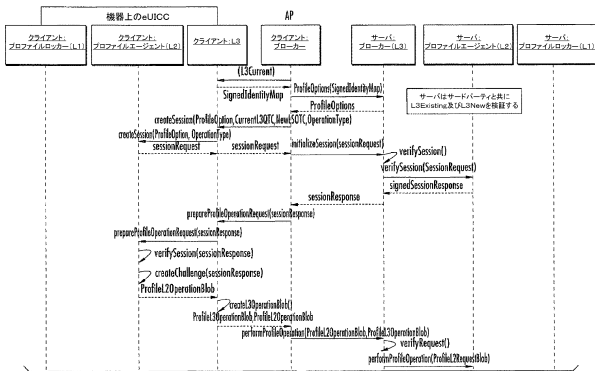
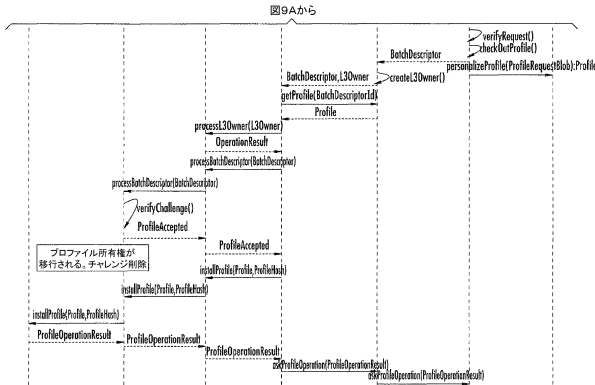


図9Bへ続く

【図9B】



【図10A】

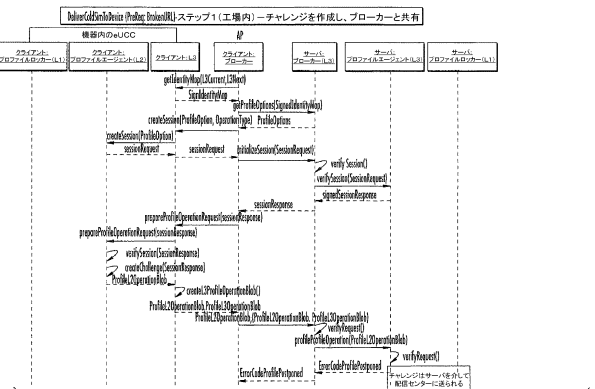


図10Bへ

【図10B】

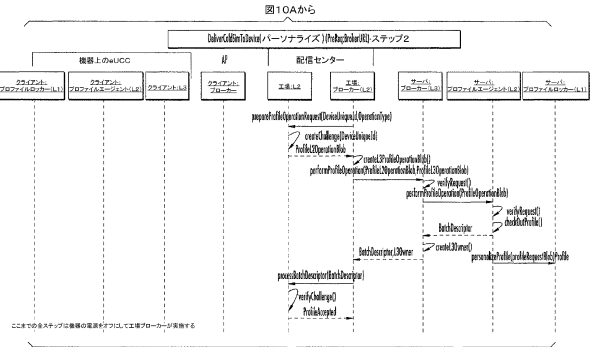
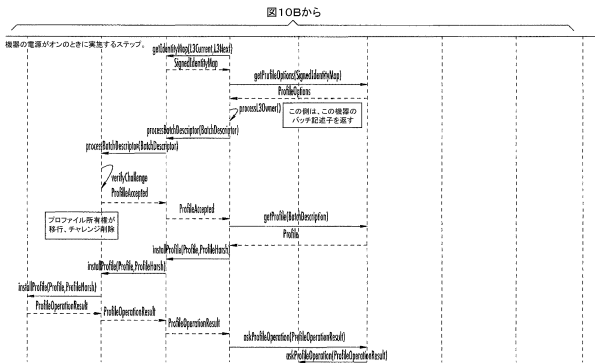
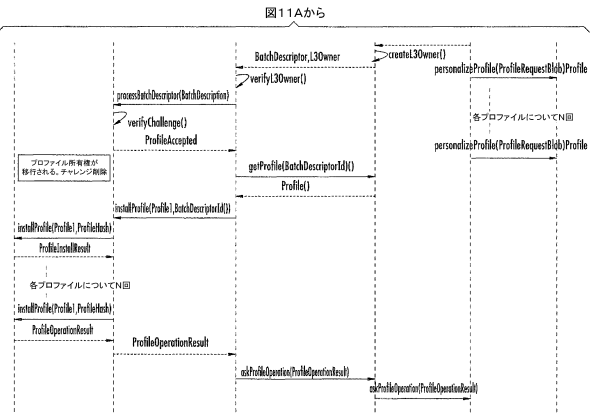


図10Cへ

【図10C】



【図11B】



【図11A】

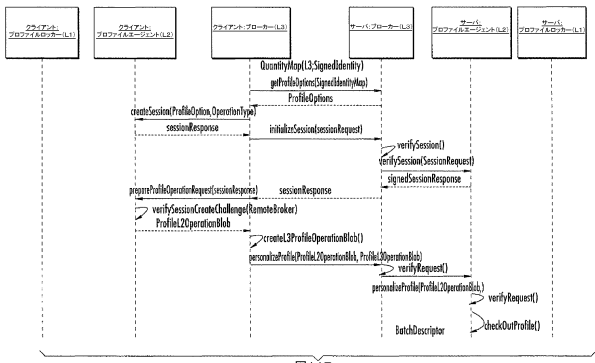
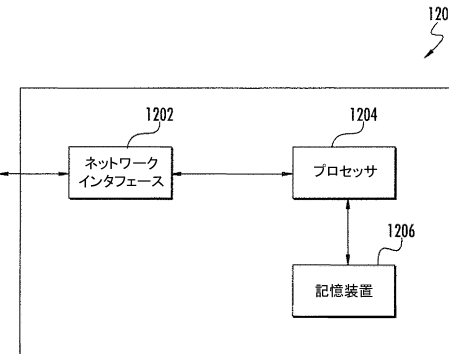


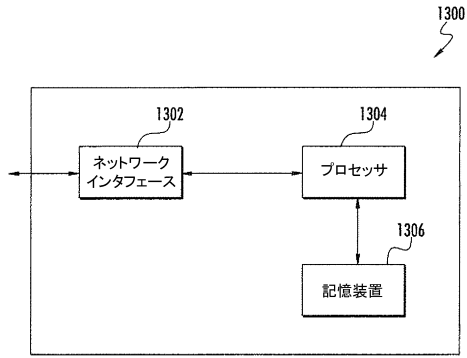
図11Bへ

【図12】

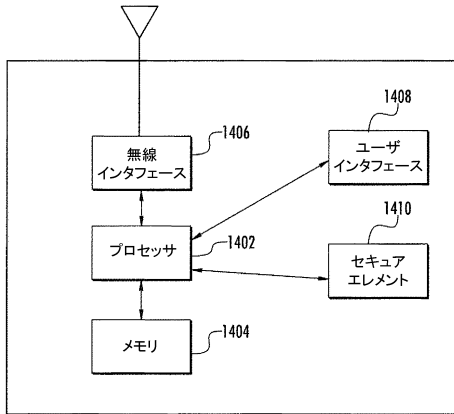


1200

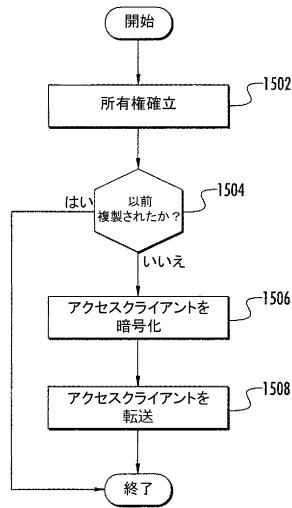
【図13】



【図14】



【図15】



フロントページの続き

- (74)代理人 100116894
弁理士 木村 秀二
- (74)代理人 100130409
弁理士 下山 治
- (74)代理人 100134175
弁理士 永川 行光
- (72)発明者 ハガティ, デーヴィッド
アメリカ合衆国 カリフォルニア州 95014, クパチーノ, インフィニット ループ 1
, エム/エス 87-2シージーエス
- (72)発明者 ハウク, ジェロルド
アメリカ合衆国 カリフォルニア州 95014, クパチーノ, インフィニット ループ 1
, エム/エス 111-エイチオーエム
- (72)発明者 ジュアン, ベン
アメリカ合衆国 カリフォルニア州 95014, クパチーノ, インフィニット ループ 1
, エム/エス 302-1アイオーエス
- (72)発明者 リ, リ
アメリカ合衆国 カリフォルニア州 95014, クパチーノ, インフィニット ループ 1
, エム/エス 302-1アイオーエス
- (72)発明者 マティアス, アルン
アメリカ合衆国 カリフォルニア州 95014, クパチーノ, インフィニット ループ 1
, エム/エス 302-2アイオーエス
- (72)発明者 マクラフリン, ケヴィン
アメリカ合衆国 カリフォルニア州 95014, クパチーノ, インフィニット ループ 1
, エム/エス 302-4オーエス4
- (72)発明者 ナラシムハン, アヴィナシュ
アメリカ合衆国 カリフォルニア州 95014, クパチーノ, インフィニット ループ 1
, エム/エス 302-2アイオーエス
- (72)発明者 シャープ, クリス
アメリカ合衆国 カリフォルニア州 95014, クパチーノ, インフィニット ループ 1
, エム/エス 87-2シージーエス
- (72)発明者 ヴェイド, ユーセフ
アメリカ合衆国 カリフォルニア州 95014, クパチーノ, インフィニット ループ 1
, エム/エス 302-2アイオーエス
- (72)発明者 ヤン, シャンイン
アメリカ合衆国 カリフォルニア州 95014, クパチーノ, インフィニット ループ 1
, エム/エス 302-2アイオーエス

審査官 青木 重徳

- (56)参考文献 特開2004-326800(JP, A)
特表2008-507154(JP, A)
米国特許出願公開第2012/0011345(US, A1)
宇根 正志, 金融分野におけるPKI, 日本銀行金融研究所ディスカッション・ペーパー・シリーズ(2002年収録分), 日本, 日本銀行金融研究所, 2002年12月27日, pp. 38-39
ETSI TC SCP, Liaison Statement on new Work Item for Eucc[online], 3GPP TSG-SA WG1 54 S1-111191, 2011年

(58)調査した分野(Int.Cl. , DB名)

H04L 9/08