(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2011-524099
(P2011-524099A)
(43)公表日　平成23年8月25日(2011.8.25)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
H04L 9/32	(2006.01)	H04L	9/00	601E	5K067
H04W 12/04	(2009.01)	H04L	9/00	675A	
H04W 92/08	(2009.01)	H04Q	7/00	182	
		H04Q	7/00	685	

審査請求 有　予備審査請求 有　（全 32 頁）

(21)出願番号　特願2011-504132 (P2011-504132)
(86)(22)出願日　平成21年4月7日 (2009.4.7)
(85)翻訳文提出日　平成22年12月7日 (2010.12.7)
(86)国際出願番号　PCT/US2009/039805
(87)国際公開番号　WO2009/126647
(87)国際公開日　平成21年10月15日 (2009.10.15)
(31)優先権主張番号　61/043,007
(32)優先日　平成20年4月7日 (2008.4.7)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/081,756
(32)優先日　平成20年7月18日 (2008.7.18)
(33)優先権主張国　米国 (US)

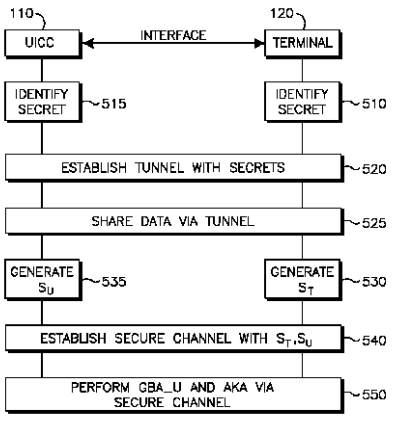
(71)出願人　510030995
インターデイジタル　パテント　ホールディングス　インコーポレイテッド
アメリカ合衆国　１９８１０　デラウェア州　ウィルミントン　シルバーサイド　ロード　３４１１　コンコルド　プラザ　ヘイグリー　ビルディング　スイート　１０５
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　ルイス　ジェイ．グッチョーネ
アメリカ合衆国　１０７０９　ニューヨーク州　イースト　チェスター　リンカーン　プレイス　２１１

最終頁に続く

(54)【発明の名称】セキュリティ保護されたセッション鍵生成

(57)【要約】
無線通信におけるＵＩＣＣ（汎用ＩＣカード）と端末との間のインタフェースをセキュリティ保護するための方法および装置が開示される。ＡＫＡ（認証と鍵の合意）手続き、およびアプリケーションレベルのＧＢＡ＿Ｕ（ＵＩＣＣベースの拡張を伴うＧＢＡ（汎用ブートストラッピングアーキテクチャ））手続きのセキュリティが向上する。セキュリティ保護された共有セッション鍵を使用して、ＵＩＣＣと端末の間の通信が暗号化される。このセキュリティ保護された共有セッション鍵は、認証手続きまたは匿名手続きを使用して生成される。

FIG. 5



【特許請求の範囲】
【請求項１】
ＵＩＣＣ（汎用ＩＣカード）と端末の間の通信をセキュリティ保護するための方法であって、
セキュリティ保護された共有セッション鍵を生成すること、および
前記ＵＩＣＣと前記端末の間の通信を前記セキュリティ保護された共有セッション鍵で暗号化すること
を含むことを特徴とする方法。
【請求項２】
前記セキュリティ保護された共有セッション鍵を生成することは、共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すことを含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すことは、秘密から共有される秘密を生成することを含むことを特徴とする請求項２に記載の方法。
【請求項４】
前記セキュリティ保護された共有セッション鍵を導き出すことは、前記共有される秘密を使用してＰＲＦ（擬似乱数関数）を実行することを含むことを特徴とする請求項２に記載の方法。
【請求項５】
前記通信を暗号化することは、安全な通信路を確立することを含むことを特徴とする請求項１に記載の方法。
【請求項６】
前記安全な通信路を使用して、アプリケーションレベルのＧＢＡ＿Ｕ（ＵＩＣＣベースの拡張を伴うＧＢＡ（汎用ブートストラッピングアーキテクチャ））手続き、またはＡＫＡ（認証と鍵の合意）手続きの少なくともいずれかを実行することをさらに含むことを特徴とする請求項５に記載の方法。
【請求項７】
前記ＵＩＣＣと前記端末の間のインタフェース上でトンネルを作成することをさらに含むことを特徴とする請求項１に記載の方法。
【請求項８】
前記セキュリティ保護された共有セッション鍵を生成することは、
前記ＵＩＣＣと前記端末の間にセキュリティ保護された共有セッション鍵が存在するかどうかを判定すること、および
前記セキュリティ保護された共有セッション鍵が存在していないという条件で、新たなセキュリティ保護された共有セッション鍵を生成することを含むことを特徴とする請求項１に記載の方法。
【請求項９】
前記セキュリティ保護された共有セッション鍵を生成することは、
生成されるべき鍵ネゴシエーションパラメータを生成し、該生成された鍵ネゴシエーションパラメータを前記ＵＩＣＣに報告すること、
受け取られるべき鍵ネゴシエーションパラメータを受け取ること、
前記生成された鍵ネゴシエーションパラメータ、および前記受け取られた鍵ネゴシエーションパラメータを使用して、前記セキュリティ保護された共有セッション鍵を作成することを含むことを特徴とする請求項１に記載の方法。
【請求項１０】
前記作成することは、
前記生成された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるかどうかを判定すること、および

前記生成された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるという条件で、セキュリティ保護された共有セッション鍵を導き出すことを含むことを特徴とする請求項９に記載の方法。
【請求項１１】
前記生成することは、
ＲＡＮＤ（ランダムチャレンジ）およびＳＱＮ（シーケンス番号）を選択すること、
ＡＫ（匿名鍵）、ＭＡＣ（メッセージ認証コード）、ＸＲＥＳ（想定される応答）、およびＸＳＱＮ（想定されるシーケンス）を計算すること、および
前記ＲＡＮＤ、前記ＭＡＣ、および前記ＸＳＱＮを組み合わせて、前記生成されるべき鍵ネゴシエーションパラメータを生成することを含むことを特徴とする請求項９に記載の方法。
【請求項１２】
前記計算することは、
共有される秘密および前記ＲＡＮＤを使用して前記ＡＫを計算すること、
前記共有される秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＭＡＣを計算すること、
前記共有される秘密および前記ＲＡＮＤを使用して前記ＸＲＥＳを計算すること、および
前記ＳＱＮおよび前記ＡＫを使用して前記ＸＳＱＮを計算することを含むことを特徴とする請求項１１に記載の方法。
【請求項１３】
前記生成することは、
ノンスを選択すること、
Ｔａｇ（認証値）を計算すること、および
前記ノンスと前記Ｔａｇを組み合わせて、前記生成されるべき鍵ネゴシエーションパラメータを生成することを含むことを特徴とする請求項９に記載の方法。
【請求項１４】
前記生成することは、
セッション鍵を選択すること、
暗号化されたセッション鍵を計算すること、および
前記暗号化されたセッション鍵を使用して、前記鍵ネゴシエーションパラメータを生成することを含むことを特徴とする請求項９に記載の方法。
【請求項１５】
前記セキュリティ保護された共有セッション鍵を生成することは、
受け取られるべき鍵ネゴシエーションパラメータを受け取ること、
生成されるべき鍵ネゴシエーションパラメータを生成すること、
前記生成された鍵ネゴシエーションパラメータを前記端末に報告すること、および
前記受け取られた鍵ネゴシエーションパラメータ、および前記生成された鍵ネゴシエーションパラメータを使用して、前記セキュリティ保護された共有セッション鍵を作成すること
を含むことを特徴とする請求項１に記載の方法。
【請求項１６】
前記作成することは、
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるかどうかを判定すること、および
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるという条件で、セキュリティ保護された共有セッション鍵を導き出すこと
を含むことを特徴とする請求項１５に記載の方法。
【請求項１７】

前記生成することは、
前記受け取られた鍵ネゴシエーションパラメータからＲＡＮＤ（ランダムチャレンジ）、ＭＡＣ（メッセージ認証コード）、およびＸＳＱＮ（想定されるシーケンス）を抽出すること、
ＡＫ（匿名鍵）、ＸＭＡＣ（想定されるメッセージ認証コード）、およびＳＱＮ（シーケンス番号）を計算すること、
前記ＸＭＡＣが前記ＭＡＣと同一であるかどうかを判定すること、および
前記ＸＭＡＣが前記ＭＡＣと同一であるという条件で、共有される秘密および前記ＲＡＮＤを使用してＲＥＳ（応答）を計算すること
を含むことを特徴とする請求項１５に記載の方法。

【請求項１８】
前記計算することは、
前記共有される秘密および前記ＲＡＮＤを使用して前記ＡＫを計算すること、
前記ＸＳＱＮおよび前記ＡＫを使用して前記ＳＱＮを計算すること、および
前記共有される秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＸＭＡＣを計算すること
を含むことを特徴とする請求項１７に記載の方法。

【請求項１９】
前記生成することは、
前記受け取られた鍵ネゴシエーションパラメータからノンスおよびＴａｇを抽出すること、
前記Ｔａｇを検証すること、
前記Ｔａｇが妥当であるという条件で、セッション鍵を導き出し、ＸＴａｇ（想定される認証値）を計算すること、および
前記ＸＴａｇを使用して、前記生成されるべき鍵ネゴシエーションパラメータを生成すること
を含むことを特徴とする請求項１５に記載の方法。

【請求項２０】
前記生成することは、前記受け取られる鍵ネゴシエーションパラメータから前記暗号化されたセッション鍵を抽出することを含み、さらに該セッション鍵を導き出すことは、前記暗号化されたセッション鍵を解読することを含むことを特徴とする請求項１９に記載の方法。

【請求項２１】
前記セキュリティ保護された共有セッション鍵を生成することは、
事前鍵ネゴシエーションパラメータを生成すること、および
前記事前鍵ネゴシエーションパラメータを前記端末に報告すること
を含むことを特徴とする請求項１に記載の方法。

【請求項２２】
前記セキュリティ保護された共有セッション鍵を生成することは、
前記ＵＩＣＣから事前鍵ネゴシエーションパラメータを受け取ることを含むことを特徴とする請求項１に記載の方法。

【請求項２３】
前記生成することは、ディフィーヘルマン鍵交換プロトコルを実行することを含むことを特徴とする請求項１に記載の方法。

【請求項２４】
セキュリティ保護された共有セッション鍵を生成し、
前記セキュリティ保護された共有セッション鍵で通信を暗号化し、
前記暗号化された通信を送信し、さらに
前記セキュリティ保護された共有セッション鍵を使用して、受信される暗号化された通信を解読するように構成されたＵＩＣＣ（汎用ＩＣカード）と、

前記セキュリティ保護された共有セッション鍵を生成し、
前記セキュリティ保護された共有セッション鍵で通信を暗号化し、
前記暗号化された通信を送信し、さらに
前記セキュリティ保護された共有セッション鍵を使用して、受信される暗号化された通信を解読するように構成された端末と
を備えることを特徴とするＷＴＲＵ（無線送信／受信ユニット）。
【請求項２５】
前記ＵＩＣＣは、共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すことによって、前記セキュリティ保護された共有セッション鍵を生成するように構成され、さらに
前記端末は、前記共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すことによって、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項２６】
前記ＵＩＣＣは、第１の秘密から前記共有される秘密を生成することによって、前記共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すように構成され、さらに
前記端末は、第２の秘密から前記共有される秘密を生成することによって、前記共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すように構成されることを特徴とする請求項２５に記載のＷＴＲＵ。
【請求項２７】
前記ＵＩＣＣは、前記共有される秘密を使用してＰＲＦ（擬似乱数関数）を実行することによって、前記セキュリティ保護された共有セッション鍵を導き出すように構成され、さらに
前記端末は、前記共有される秘密を使用してＰＲＦ（擬似乱数関数）を実行することによって、前記セキュリティ保護された共有セッション鍵を導き出すように構成されることを特徴とする請求項２５に記載のＷＴＲＵ。
【請求項２８】
前記ＵＩＣＣは、前記端末と安全な通信路を確立するように構成され、さらに前記端末は、前記ＵＩＣＣと安全な通信路を確立するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項２９】
前記安全な通信路を介して手続きを実行することは、アプリケーションレベルのＧＢＡ＿Ｕ（ＵＩＣＣベースの拡張を伴うＧＢＡ（汎用ブートストラッピングアーキテクチャ））手続き、またはＡＫＡ（認証と鍵の合意）手続きの少なくともいずれかを実行することを含むことを特徴とする請求項２８に記載のＷＴＲＵ。
【請求項３０】
前記端末は、
生成されるべき鍵ネゴシエーションパラメータを生成し、
前記生成された鍵ネゴシエーションパラメータを前記ＵＩＣＣに報告し、
前記ＵＩＣＣから、受け取られるべき鍵ネゴシエーションパラメータを受け取り、さらに
前記生成された鍵ネゴシエーションパラメータ、および前記受け取られた鍵ネゴシエーションパラメータを使用して、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項３１】
前記端末は、
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるかどうかを判定し、さらに
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーショ

ンパラメータと同一であるという条件で、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項３０に記載のＷＴＲＵ。
【請求項３２】
前記端末は、
ＲＡＮＤ（ランダムチャレンジ）およびＳＱＮ（シーケンス番号）を選択し、
ＡＫ（匿名鍵）、ＭＡＣ（メッセージ認証コード）、ＸＲＥＳ（想定される応答）、およびＸＳＱＮ（想定されるシーケンス）を計算し、さらに
前記ＲＡＮＤ、前記ＭＡＣ、および前記ＸＳＱＮを使用して、前記生成される鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項３０に記載のＷＴＲＵ。
【請求項３３】
前記端末は、
共有される秘密と前記ＲＡＮＤを使用して前記ＡＫを計算し、
前記共有される秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＭＡＣを計算し、
前記共有される秘密および前記ＲＡＮＤを使用して前記ＸＲＥＳを計算し、さらに
前記ＳＱＮおよび前記ＡＫを使用して前記ＸＳＱＮを計算するように構成されることを特徴とする請求項３２に記載のＷＴＲＵ。
【請求項３４】
前記端末は、
ノンスを選択し、
Ｔａｇ（認証値）を計算し、さらに
前記ノンスと前記Ｔａｇを使用して、前記生成されるべき鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項１０に記載のＷＴＲＵ。
【請求項３５】
前記端末は、
セッション鍵を選択し、
暗号化されたセッション鍵を計算し、さらに
前記暗号化されたセッション鍵を使用して、前記生成されるべき鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項３０に記載のＷＴＲＵ。
【請求項３６】
前記ＵＩＣＣは、
前記端末から、受け取られる鍵ネゴシエーションパラメータを受け取り、
生成されるべき鍵ネゴシエーションパラメータを生成し、
前記生成された鍵ネゴシエーションパラメータを前記端末に報告し、さらに
前記受け取られた鍵ネゴシエーションパラメータ、および前記生成された鍵ネゴシエーションパラメータを使用して、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項３７】
前記ＵＩＣＣは、
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるかどうかを判定し、さらに
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるという条件で、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項３６に記載のＷＴＲＵ。
【請求項３８】
前記ＵＩＣＣは、
前記受け取られた鍵ネゴシエーションパラメータからＲＡＮＤ（ランダムチャレンジ）、ＭＡＣ（メッセージ認証コード）、およびＸＳＱＮ（想定されるシーケンス）を抽出し、

ＡＫ（匿名鍵）、ＸＭＡＣ（想定されるメッセージ認証コード）、およびＳＱＮ（シーケンス番号）を計算し、
前記ＸＭＡＣが前記ＭＡＣと同一であるかどうかを判定し、
前記ＸＭＡＣが前記ＭＡＣと同一であるという条件で、共有される秘密および前記ＲＡＮＤとを使用してＲＥＳ（応答）を計算し、さらに
前記ＲＥＳを使用して、前記生成される鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項３６に記載のＷＴＲＵ。
【請求項３９】
前記ＵＩＣＣは、
前記共有される秘密および前記ＲＡＮＤを使用して前記ＡＫを計算し、
前記ＸＳＱＮおよび前記ＡＫを使用して前記ＳＱＮを計算し、さらに
前記共有される秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＸＭＡＣを計算するように構成されることを特徴とする請求項３８に記載のＷＴＲＵ。
【請求項４０】
前記ＵＩＣＣは、
前記受け取られる鍵ネゴシエーションパラメータからノンスおよびＴａｇを抽出し、
前記Ｔａｇを検証し、
ＸＴａｇ（想定される認証値）を計算し、さらに
前記ＸＴａｇを使用して、前記生成される鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項３６に記載のＷＴＲＵ。
【請求項４１】
前記ＵＩＣＣは、
前記受け取られた鍵ネゴシエーションパラメータから暗号化されたセッション鍵を抽出し、
前記暗号化されたセッション鍵を解読し、さらに
前記解読されたセッション鍵を使用して、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項４０に記載のＷＴＲＵ。
【請求項４２】
前記ＵＩＣＣは、
事前鍵ネゴシエーションパラメータを生成し、さらに
前記事前鍵ネゴシエーションパラメータを前記端末に報告するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項４３】
前記端末は、
事前鍵ネゴシエーションパラメータを前記ＵＩＣＣから受け取るように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項４４】
前記ＵＩＣＣは、ディフィーヘルマン鍵交換プロトコルを実行するように構成され、さらに前記端末は、ディフィーヘルマン鍵交換プロトコルを実行するように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、無線通信に関する。
【背景技術】
【０００２】
ＡＫＡ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ａｇｒｅｅｍｎｔ：認証と鍵の合意）手続き（プロシージャ）が、３ＧＰＰ（第３世代パートナーシッププロジェクト：第３世代移動体通信システムの標準化団体）通信ネットワークにおいてＷＴＲＵ（無線送信／受信ユニット）に関する認証、および共有秘密鍵を確立するために使用される。

ＡＫＡは、２つの当事者間でセキュリティ保護された（安全な、セキュアな）相互認証をもたらす。さらに、ＡＫＡ手続きに基づく、アプリケーションレベルのＧＢＡ＿Ｕ（ＵＩＣＣベースの拡張を伴うＧＢＡ（汎用ブートストラッピングアーキテクチャ））が、アプリケーションセキュリティを可能にする手段を提供する。しかし、ＡＫＡ手続き、およびアプリケーションレベルのＧＢＡ＿Ｕ（ＵＩＣＣベースの拡張を伴うＧＢＡ（汎用ブートストラッピングアーキテクチャ））手続きは、ＵＩＣＣ（汎用ＩＣカード）とＷＴＲＵの端末（Ｔｅｒｍｉｎａｌ）を接続するインタフェースのセキュリティを保護しない。クリティカルキー（重要鍵）関連資料が、ＡＫＡプロセス中、およびＧＢＡ＿Ｕプロセス中にＵＩＣＣから端末に送られる。その結果、セッション鍵（例えば、ＣＫ／ＩＫおよびＫｓ＿ｅｘｔ＿ＮＡＦ）が、販売間際の端末の導入準備作業中、ローカル鍵がまだ確立されていないときや、あるいは確立されたローカル鍵が期限切れになったときに開示される。

【０００３】

ＵＩＣＣと端末の間の接続を保護するように設計された既存のプロトコルは、ＡＫＡプロセスおよびＧＢＡ＿Ｕプロセスが完了するまで、開始され得ない。その結果、これらのプロトコルは、鍵を盗聴することを可能にする。ＡＫＡプロセスおよびＧＢＡ＿Ｕプロセスの後、無線ネットワーク構成要素との対話、および無線ネットワーク構成要素による参加を介して他のアプリケーションレベルのプロセスに関して、端末とＵＩＣＣの間のリンクをセキュリティ保護しようとする試みでは、これらの欠陥を解決しない。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

したがって、端末とＵＩＣＣの間の通信をセキュリティ保護するための改良された方法および装置の必要性が存在している。

【課題を解決するための手段】

【０００５】

無線通信におけるＵＩＣＣ（汎用ＩＣカード）と端末との間のインタフェースをセキュリティ保護するための方法および装置が開示される。ＡＫＡ手続き、およびアプリケーションレベルのＧＢＡ＿Ｕ（ＵＩＣＣベースの拡張を伴うＧＢＡ（汎用ブートストラッピングアーキテクチャ））手続きのセキュリティが向上する。セキュリティ保護された共有セッション鍵を使用して、ＵＩＣＣと端末の間の通信が暗号化される。このセキュリティ保護された共有セッション鍵は、認証手続きまたは匿名手続き（ｎｏｎ－ａｕｔｈｅｎｔｉｃａｔｉｎｇ　ｐｒｏｃｅｄｕｒｅ）を使用して生成される。

【０００６】

より詳細な理解は、添付の図面と併せて例示として与えられている、以下の説明から得ることができる。

【図面の簡単な説明】

【０００７】

【図１】セキュリティ保護されたセッション鍵生成を実行するための無線送信／受信ユニットの例を示す図である。

【図２】無線通信を実行するためのハンドセット（携帯電話）として構成された端末の例を示す図である。

【図３】コネクテッド・デバイスと連携してセキュリティ保護されたセッション鍵の生成を実行するための無線送信／受信ユニットの例を示す図である。

【図４】無線通信を実行するためのネットワークの例を示す図である。

【図５】汎用ＩＣカードと端末の間の通信をセキュリティ保護するためのセッション鍵の生成の例を示す図である。

【図６】ＡＫＡ手続き（プロシージャ）を使用する明示的な相互認証の例を示す図である。

【図７】ワンタイム（一時的な、１回限りの）認証付暗号化機能を使用する明示的な相互認証の例を示す図である。

【図８】ワンタイム認証付暗号化機能および再生保護を使用する明示的な相互認証の例を示す図である。
【図９】暗黙の相互認証の例を示す図である。
【図１０】再生保護を伴う暗黙の相互認証の例を示す図である。
【図１１】認証なしの共有秘密鍵の例を示す図である。
【発明を実施するための形態】
【０００８】
以降、言及する場合、「ＷＴＲＵ（無線送信／受信ユニット）」という用語には、ＵＥ（ユーザ機器）、移動局、固定加入者ユニットもしくは移動加入者ユニット、ポケットベル、セルラ電話機、ＰＤＡ（携帯情報端末）、コンピュータ、または無線環境において動作することができる他の任意のタイプのユーザデバイスが含まれるが、以上には限定されない。以降、言及する場合、「基地局」という用語には、ノードＢ、サイトコントローラ、ＡＰ（アクセスポイント）、または無線環境において動作することができる他の任意のタイプのインタフェースデバイスが含まれるが、以上には限定されない。「ＷＴＲＵ」という用語と「基地局」という用語は、相互排除的ではない。
【０００９】
図１は、セキュリティ保護されたセッション鍵生成を実行するためのＷＴＲＵ（無線送信／受信ユニット）１００の例示的なブロック図である。ＷＴＲＵ１００は、ＵＩＣＣ（汎用ＩＣカード）１１０および端末１２０を含む。ＵＩＣＣは、インタフェース１３０を介して端末と通信する。ＷＴＲＵ１００は、例示のためにＵＩＣＣ１１０および端末１２０を含むものとして示されている。ＵＩＣＣ１１０または端末１２０は、本明細書で説明されるとおりに通信することができる限り、任意の仕方で構成されることが可能である。例えば、図３は、端末（Ｔｅｒｍｉｎａｌ）１２０が、コネクテッド・デバイス（連結デバイス）内に配置された例を示す。
【００１０】
図２は、無線通信を実行するためのハンドセット（携帯電話）として構成された端末１２０の拡大図の例示的なブロック図である。端末１２０は、プロセッサ２１０、アンテナ２２０、ユーザインタフェース２３０、および表示部（ディスプレイ）２４０を含む。
【００１１】
図３は、コネクテッド・デバイス（連結デバイス）３００と連動してセキュリティ保護されたセッション鍵生成を実行するためのＷＴＲＵ（無線送信／受信ユニット）１００の例示的なブロック図である。ＷＴＲＵ１００内のＵＩＣＣ１０は、コネクテッド・デバイス３００内の端末１２０とインタフェース１３０を介して通信する。コネクテッド・デバイス３００は、ＰＣ（パーソナルコンピュータ）であることが可能であり、あるいは端末１２０として構成された他の任意のデバイスであることが可能である。インタフェース１３０は、有線インタフェースまたは無線インタフェースであることが可能である。本明細書で説明される方法および装置は、ＵＩＣＣ１１０と端末１２０の他の任意の組合せまたは構成を含む。オプションとして、端末１２０は、内部ＵＩＣＣ読み取り装置または外部ＵＩＣＣ読み取り装置を含むことが可能である。
【００１２】
例えば、コネクテッド・デバイス３００は、ラップトップコンピュータであることが可能である。このラップトップは、イーサネット（登録商標）接続を介してインターネットに接続されることが可能である。また、このラップトップは、Ｂｌｕｅｔｏｏｔｈインタフェース１３０を介してＷＴＲＵ１００に接続されることも可能である。その場合、ＷＴＲＵ１００内のＵＩＣＣ１１０は、セキュリティ保護された接続を要求する通信を実行するためにラップトップ内の端末１２０を使用することが可能である。代替として、ラップトップ内の端末１２０が、セキュリティ保護された接続を要求する通信を実行するためにＷＴＲＵ１００内のＵＩＣＣ１１０を使用してもよい。
【００１３】
図４は、無線通信を実行するためのネットワーク４００の例示的なブロック図である。

ネットワーク４００は、ＷＴＲＵ１００、ＲＡＮ（無線アクセスネットワーク）４１０、およびＣＮ（コアネットワーク）４２０を含む。ＲＡＮ４１０は、基地局４３０およびＲＮＣ（無線ネットワークコントローラ（制御装置））４４０を含む。ＣＮ４２０は、ＶＬＲ（ビジタロケーションレジスタ（在圏網加入者管理レジスタ、あるいは訪問者位置登録装置とも称されている））４５０およびＨＬＲ（ホームロケーションレジスタ（現在所在地登録装置とも称されている））４６０を含む。また、ネットワーク４００は、ＥＶＥ（イーブズドロッパ：盗聴者）４９０も含む。基地局４３０は、ＲＡＮ４１０に関するネットワークのエントリ（入り口）点の役割をする。ＲＮＣ４４０は、無線リソース管理、移動性管理機能、および暗号化機能などの無線通信における様々な機能を実行する。ＶＬＲ４５０が、無線通信のために使用される、ユーザサービスプロファイルのコピーや、デバイスロケーションエリアなどの、ＷＴＲＵ１００についての情報を格納する。ユーザサービスプロファイルのマスタコピーを格納するＨＬＲ４６０が、スイッチング機能を実行し、ＷＴＲＵ１００とネットワーク４００の間の無線通信を管理する。

【００１４】

図５は、ＵＩＣＣ１１０と端末１２０の間のインタフェース１３０をセキュリティ保護するためのセッション鍵生成の例である。５１０で、端末１２０が、ＵＩＣＣ１１０との通信を暗号化するのに使用され得る秘密（ｓｅｃｒｅｔ）を識別する。５１５で、同様に、ＵＩＣＣが、端末１２０との通信を暗号化するのに使用され得る秘密を識別する。オプションとして、これらの識別される秘密は、事前に準備された共有秘密である。５２０で、これらの秘密を使用してインタフェース１３０上でトンネル（ｔｕｎｎｅｌ：公衆回線網上のある２点間を結ぶ閉じられた仮想的な直結通信回線）が確立され、したがって、ＵＩＣＣ１１０と端末１２０の間の通信路が、それぞれの秘密を使用してセキュリティ保護される。５２５で、このトンネルが、セキュリティ保護された共有セッション鍵（ｓｅｃｕｒｅ ｓｈａｒｅｄ ｓｅｓｓｉｏｎ ｋｅｙ：セキュアな共有セッション鍵とも称されている）を導き出す際に使用するためのデータを共有するのに使用される。

【００１５】

次に、５３０で、端末１２０が、端末１２０の秘密からセキュリティ保護された共有セッション鍵S_Tを導き出す。同様に、５３５で、ＵＩＣＣ１１０が、ＵＩＣＣ１１０の秘密からセキュリティ保護された共有セッション鍵S_Uを導き出す。オプションとして、５３０、５３５で、ＵＩＣＣ１１０と端末１２０は、相互認証も実行する。５４０で、セキュリティ保護された共有セッション鍵S_T、S_Uが、ＵＩＣＣ１１０と端末１２０の間で安全な通信路（ｓｅｃｕｒｅ ｃｈａｎｎｅｌ）を確立するのに使用され、したがって、この安全な通信路を通過する情報の機密性および完全性が保護される。次に、５５０で、ＵＩＣＣ１１０と端末１２０が、この安全な通信路を介してＡＫＡ３００手続き（プロシージャ）およびＧＢＡ＿Ｕ４００手続き（プロシージャ）を実行する。

【００１６】

一部の実施形態において、共有される秘密Ｋが、ＳＨＡ－２５６ ＨＭＡＣセキュリティ関数、暗号化ＡＥＳ－１２８ ＣＢＣ ＭＡＣセキュリティ関数、またはＡＫＡセキュリティ関数などの、任意の長さの入力に対応することができる鍵付きＰＲＦ（擬似乱数関数）を実行するのに使用される。共有される秘密Ｋおよび、および入力ｘを使用するＰＲＦは、f_K（ｘ）と表されることが可能である。同様に、f_K（ｘ，ｙ）という表記は、ＰＲＦが、示される引数の連結に対して実行されることを示す。ＰＲＦファミリは、可変ビット長の値が固定長（すなわち、１２８または２５６）のビット系列に変換される、関連する不可逆な一方向ＰＲＦのセットである。例えば、ＰＲＦファミリにおける第１のＰＲＦが、f_K（０，Ｙ，Ｚ）と表されることが可能であり、ＰＲＦファミリにおける第２のＰＲＦが、f_K（１，Ｙ，Ｚ）と表されることが可能であり、したがって、先頭の０を有するＰＲＦは、先頭の１を有するＰＲＦとは異なる結果をもたらす。

【００１７】

一部の実施形態において、端末１２０は、ＲＡＮＤ（ランダムチャレンジ）、ＡＫ（匿名鍵）、およびＳＱＮ（シーケンス番号）を生成するように構成される。また、端末１２

０は、ＭＡＣ（メッセージ認証コード）、ＸＲＥＳ（想定される応答）、およびＸＳＱＮ（想定されるシーケンス番号）、またはＴａｇ（認証値）を計算するようにも構成される。同様に、ＵＩＣＣ１１０が、ＲＥＳ（応答）またはＸＴａｇ（想定される認証値）を生成するように構成される。ＲＡＮＤ、ＡＫ、ＳＱＮ、ＭＡＣ、およびＸＲＥＳは、当技術分野で知られている、それぞれのいくつかの関数のいずれに従って生成されてもよいことが、当業者には認識されよう。オプションとして、これらの関数は、３ＧＰＰ（第３世代パートナーシッププロジェクト）によって定義される鍵生成関数であってもよい。また、端末１２０は、計算された値をＵＩＣＣ１１０に送るようにも構成される。また、端末１２０は、ＵＩＣＣ１１０から応答（ＲＥＳ）を受信し、さらにＵＩＣＣ１１０の認証のために、計算された値と受け取った値とを比較するようにも構成される。同様に、ＵＩＣＣ１１０が、端末１２０にそれらの値を送り、さらにＵＩＣＣ１１０の認証のために、計算された値と受け取った値とを比較するように構成される。また、端末１２０とＵＩＣＣ１１０は、共有セッション鍵や匿名鍵などの共有値を単独で導き出すようにも構成される。簡明のため、ＵＩＣＣ１１０において生成された値は、下付き文字Ｕで示されることが可能であり、端末１２０において生成された値は、下付き文字Ｔで示されることが可能である。例えば、ＵＩＣＣ１１０におけるAK_Uは、端末１２０におけるAK_Tと同一の値を有する。

【００１８】

図６は、明示的相互認証－セッション鍵生成方法６００の例を示す。最初に、６１０で、端末１２０が、ＲＡＮＤおよびSQN_Tを生成する。６２０で、端末１２０が、ＭＡＣ、ＸＲＥＳ、AK_T、およびＸＳＱＮを計算する。ＭＡＣは、共有される秘密Ｋ、ＲＡＮＤ，およびSQN_Tに基づいて計算される。ＸＲＥＳは、認証コードを表し、共有される秘密Ｋ、およびＲＡＮＤを使用して計算される。AK_Tは、共有される秘密Ｋ、およびＲＡＮＤを使用して生成される。オプションとして、AK_Tは、SQN_Tと同一のサイズである。ＸＳＱＮは、ＳＱＮとAK_Tのビット単位の排他的論理和（ＸＯＲまたは

【００１９】

【数１】

【００２０】

）を実行することによって計算される。

【００２１】

次に、６３０で、端末１２０が、インタフェース１３０を介してＵＩＣＣ１１０にそのＭＡＣ、そのＲＡＮＤ、およびそのＸＳＱＮを送る。６４０で、ＵＩＣＣ１１０が、AK_U、SQN_U、およびＸＭＡＣ（想定されるＭＡＣ）を計算する。AK_Uは、共有される秘密Ｋ、および受け取られたＲＡＮＤを使用して計算される。SQN_Uは、AK_UとＸＳＱＮのビット単位の排他的論理和を実行することによって計算される。ＸＭＡＣは、共有される秘密Ｋ、ＲＡＮＤ、およびSQN_Uを使用して計算される。オプションとして、ＵＩＣＣ１１０においてAK_Uを計算するのに使用される関数は、端末１２０においてAK_Tを計算するのに使用される関数と同一である。

【００２２】

次に、６５０で、ＵＩＣＣ１１０が、ＸＭＡＣをＭＡＣと比較する。ＸＭＡＣとＭＡＣが等しくない場合、６５５で、認証プロセスは、失敗し、失敗状態で終了する。オプションとして、認証プロセスは、所定の間隔で再スタートされてもよい。ＸＭＡＣとＭＡＣが等しい場合、６６０で、端末１２０は、検証され、ＵＩＣＣ１１０が、共有される秘密Ｋ、およびＲＡＮＤを使用してＲＥＳを計算する。６７０で、ＵＩＣＣ１１０が、このＲＥＳを端末１２０に送り、６８０で、共有セッション鍵S_Uを導き出す。例えば、共有セッション鍵は、ＲＡＮＤ、および共有される秘密Ｋを使用して導き出される。

【００２３】

最後に、６９０で、端末１２０が、ＲＥＳをＸＲＥＳと比較する。ＲＥＳとＸＲＥＳが

等しくない場合、６９１で、認証プロセスは、失敗し、失敗状態で終了する。オプションとして、認証プロセスは、所定の間隔で再スタートされてもよい。ＲＥＳとＸＲＥＳが等しい場合、６９２で、ＵＩＣＣ１１０は、検証され、端末１２０が、共有セッション鍵S_Tを導き出す。次に、ＵＩＣＣ１１０と端末１２０は、共有セッション鍵S_U、S_Tを使用して、ＧＢＡ＿Ｕ４００手続きおよびＡＫＡ３００手続きを実行する。

【００２４】

図７は、ワンタイム認証付暗号化機能を使用する明示的相互認証およびセッション鍵生成方法７００の例を示す。７０５で、端末１２０が、セッション鍵S_Tおよびノンス（ｎｏｎｃｅ:セッションをユニークにするためのランダムな値）Ｒを生成する。オプションとして、ノンスＲは、カウンタを使用して選択され、このカウンタは、インクリメントされる。７１０で、端末１２０は、共有される秘密Ｋ、ノンスＲを使用してセッション鍵S_Tの暗号化されたセッション鍵ｅを計算し、さらにノンスＲと暗号化されたセッション鍵ｅのタプル（ｔａｐｌｅ:１件分のデータ）Ｅを計算する。タプルＥは、以下のベクトル式による暗号化プロセスによって生成される。すなわち、

【００２５】

【数２】

$$E = (R,\ e = f_K(0,R) \oplus S_T)$$

式（１）

【００２６】

次に、７２０で、端末１２０が、共有される秘密Ｋ、ノンスＲ、および暗号化されたセッション鍵ｅを使用して認証値Ｔａｇを、以下の式に従って計算する。すなわち、

$Tag = f_K(0, R, e)$　　式（２）

【００２７】

次に、７３０で、端末１２０が、インタフェース１３０を介してＵＩＣＣ１１０にタプルＥおよび認証値Ｔａｇを送る。７４０で、ＵＩＣＣ１１０が、共有される秘密Ｋ、および受け取られたタプルＥを使用して、受け取られた認証値Ｔａｇを検証する。この検証は、以下のとおり表されることが可能である。すなわち、

$Tag == f_K(0, R, e)$　　式（３）

【００２８】

受け取られた認証値Ｔａｇが妥当であると確認されなかった場合、７４５で、認証プロセスは、失敗し、失敗状態で終了する。オプションとして、認証プロセスは、所定の間隔の後に再スタートされてもよい。受け取られた認証値Ｔａｇが妥当であると確認された場合、７５０で、端末１２０は認証され、ＵＩＣＣが、セッション鍵S_Uを、以下の式に従って解読する。すなわち、

【００２９】

【数３】

$$S_U = f_K(0,R) \oplus e$$

式（４）

【００３０】

次に、７６０で、ＵＩＣＣ１１０が、ＸＴａｇ（想定される認証値）を計算する。この計算は、以下のとおり表されることが可能である。すなわち、

$XTag = f_K(1, R)$　　式（５）

【００３１】

７７０で、ＵＩＣＣ１１０が、インタフェース１３０を介して端末１２０に想定される認証値ＸＴａｇを送る。７８０で、端末１２０が、共有される秘密Ｋ、およびノンスＲを使用して、受け取られたＸＴａｇを検証（妥当性確認）する。この検証は、以下のとおり表されることが可能である。

$XTag == f_K(1, R)$　　式（６）

【００３２】
ＸＴａｇが妥当であると確認された場合、７９０で、ＵＩＣＣ１１０は認証される。ＸＴａｇが妥当であると確認されなかった場合、７９１で、認証プロセスは、失敗し、失敗状態で終了する。オプションとして、認証プロセスは、所定の間隔の後に再スタートされてもよい。
【００３３】
図８は、ワンタイム認証付暗号化機能および再生保護を使用する明示的相互認証およびセッション鍵生成方法８００の例を示す。８０５で、ＵＩＣＣ１１０が、ノンスＮを生成する。ノンスが図８に示されるものの、任意の適切な事前鍵ネゴシエーションパラメータが使用されることが可能である。オプションとして、ノンスＮは、カウンタを使用して生成され、このカウンタは、インクリメントされる。次に、８１０で、ＵＩＣＣ１１０が、インタフェース１３０を介してノンスＮを端末１２０に送る。
【００３４】
８２０で、端末１２０が、セッション鍵S_TおよびノンスＲを生成する。オプションとして、ノンスＲは、カウンタを使用して生成され、このカウンタは、インクリメントされる。８３０で、端末１２０が、式１に従って、共有される秘密Ｋ、およびノンスＲを使用してセッション鍵S_Tの暗号化されたセッション鍵ｅを計算する。次に、８４０で、端末１２０が、共有される秘密Ｋ、ノンスＲ、暗号化されたセッション鍵ｅ、およびノンスＮを使用して認証値Ｔａｇを計算する。この計算は、以下のとおり表されることが可能である。すなわち、
$Tag = f_K(0, R, e, N)$　　式（７）
【００３５】
次に、８５０で、端末１２０が、インタフェース１３０を介してＵＩＣＣ１１０に認証値Ｔａｇ、およびノンスＲと暗号化されたセッション鍵ｅのタプルＥを送る。８６０で、ＵＩＣＣ１１０が、共有される秘密Ｋ、受け取られたタプルＥ、およびノンスＮを使用して、受け取られた認証値Ｔａｇを検証する。この検証は、以下のとおり表されることが可能である。すなわち、
$Tag = = f_K(0, R, e, N)$　　式（８）
【００３６】
受け取られた認証値Ｔａｇが妥当であると確認されなかった場合、８６５で、認証プロセスは、失敗し、失敗状態で終了する。オプションとして、認証プロセスは、所定の間隔の後に再スタートされてもよい。受け取られた認証値Ｔａｇが妥当であると確認された場合、８７０で、ＵＩＣＣが、セッション鍵S_Uを、式４に従って解読する。次に、８８０で、ＵＩＣＣ１１０が、式５に従って想定される認証値ＸＴａｇを計算する。
【００３７】
８９０で、ＵＩＣＣ１１０が、インタフェース１３０を介して端末１２０にＸＴａｇを送信する。８９２で、端末１２０が、式６に従って、ノンスＲを使用して受け取られたＸＴａｇを検証する。ＸＴａｇが妥当であると確認された場合、８９４で、ＵＩＣＣ１１０は認証される。ＸＴａｇが妥当であると確認されなかった場合、８９６で、認証プロセスは、失敗し、失敗状態で終了する。オプションとして、認証プロセスは、所定の間隔の後に再スタートされてもよい。
【００３８】
図９は、暗黙の相互認証、およびセッション鍵生成の例を示す。９００で、端末１２０が、ノンスＲを生成する。オプションとして、ノンスＲは、カウンタを使用して生成され、このカウンタは、インクリメントされる。次に、９１０で、端末１２０は、共有される秘密Ｋ、およびノンスＲを使用して認証値Ｔａｇを計算する。この計算は、以下のとおり表されることが可能である。すなわち、
$Tag = f_K(0, R)$　　式（９）
【００３９】
次に、９２０で、端末１２０が、インタフェース１３０を介してＵＩＣＣ１１０にノン

スＲおよび認証値Ｔａｇを送る。９３０で、ＵＩＣＣ１１０が、共有される秘密Ｋ、およびノンスＲを使用して、受け取られた認証値Ｔａｇを検証する。この検証は、以下のとおり表されることが可能である。すなわち、

$Tag = f_K(0, R)$　　式（１０）

【００４０】

受け取られた認証値Ｔａｇが妥当であると確認されなかった場合、９３５で、認証プロセスは、失敗し、失敗状態で終了する。オプションとして、認証プロセスは、所定の間隔の後に再スタートされてもよい。受け取られた認証値Ｔａｇが妥当であると確認された場合、９４０で、端末１２０は認証され、ＵＩＣＣ１１０が、共有される秘密Ｋ、およびノンスＲを使用してセッション鍵S_Uを計算する。このセッション鍵計算は、以下のとおり表されることが可能である。すなわち、

$S_U = f_K(2, R)$　　式（１１）

【００４１】

次に、９５０で、ＵＩＣＣ１１０が、式５に従って想定される認証値ＸＴａｇを計算する。９６０で、ＵＩＣＣ１１０が、インタフェース１３０を介して端末１２０に想定される認証値ＸＴａｇを送る。９７０で、端末１２０が、式６に従って、ノンスＲを使用して、受け取られた想定される認証値ＸＴａｇを検証する。受け取られた想定される認証値ＸＴａｇが妥当であると確認されなかった場合、９７５で、認証プロセスは、失敗し、失敗状態で終了する。オプションとして、認証プロセスは、所定の間隔の後に再スタートされてもよい。受け取られた想定される認証値ＸＴａｇが妥当であると確認された場合、９８０で、ＵＩＣＣ１１０は認証され、端末１２０が、共有される秘密Ｋ、およびノンスＲを使用してセッション鍵S_Tを計算する。このセッション鍵計算は、以下のとおり表されることが可能である。すなわち、

$S_T = f_K(2, R)$　　式（１２）

【００４２】

図１０は、再生保護を伴う暗黙の相互認証、およびセッション鍵生成の例を示す。１００５で、ＵＩＣＣ１１０が、ノンスＮを生成する。オプションとして、ノンスＮは、カウンタを使用して生成され、このカウンタは、インクリメントされる。次に、１０１０で、ＵＩＣＣ１１０が、インタフェース１３０を介して端末１２０にノンスＮを送る。

【００４３】

１０２０で、端末１２０が、ノンスＲを生成する。オプションとして、ノンスＲは、カウンタを使用して生成され、このカウンタは、インクリメントされる。次に、１０３０で、端末１２０が、ノンスＲおよびノンスＮを使用して認証値Ｔａｇを計算する。この計算は、以下のとおり表されることが可能である。すなわち、

$Tag = f_K(0, R, N)$　　式（１３）

【００４４】

次に、１０４０で、端末１２０が、インタフェース１３０を介してＵＩＣＣ１１０にノンスＲおよび認証値Ｔａｇを送る。１０５０で、ＵＩＣＣ１１０が、共有される秘密Ｋ、ノンスＲ、およびノンスＮを使用して、受け取られた認証値Ｔａｇを検証する。この検証は、以下のとおり表されることが可能である。すなわち、

$Tag = f_K(0, R, N)$　　式（１４）

【００４５】

受け取られた認証値Ｔａｇが妥当であると確認されなかった場合、１０５５で、認証プロセスは、失敗し、失敗状態で終了する。オプションとして、認証プロセスは、所定の間隔の後に再スタートされてもよい。受け取られた認証値Ｔａｇが妥当であると確認された場合、１０６０で、端末１２０は認証され、ＵＩＣＣ１１０が、式１１に従って、共有される秘密Ｋ、およびノンスＲを使用してセッション鍵S_Uを計算する。次に、１０７０で、ＵＩＣＣ１１０が、式５に従って想定される認証値ＸＴａｇを計算する。１０８０で、ＵＩＣＣ１１０が、インタフェース１３０を介して端末１２０に想定される認証値ＸＴａｇを送る。

【００４６】
次に、１０９０で、端末１２０が、式６に従って、ノンスＲを使用して、受け取られた想定される認証値ＸＴａｇを検証する。受け取られた想定される認証値ＸＴａｇが妥当であると確認されなかった場合、１０９１で、認証プロセスは、失敗し、失敗状態で終了する。オプションとして、認証プロセスは、所定の間隔の後に再スタートされてもよい。受け取られた想定される認証値ＸＴａｇが妥当であると確認された場合、１０９２で、ＵＩＣＣ１１０は認証され、端末１２０が、共有される秘密Ｋ、およびノンスＲを使用してセッション鍵S_Tを計算する。このセッション鍵計算は、以下のとおり表されることが可能である。すなわち、

$S_T = f_K(2, R)$　　式（１５）

【００４７】
図１１は、ディフィーヘルマン鍵交換プロトコルを使用する、認証なしの共有秘密鍵確立の例を示す。最初に、１１００で、ＵＩＣＣ１１０と端末１２０が、非常に大きい素数ｐ、および生成作用素ｇについて合意する。使用される代数構造は、体F_pから導き出された乗法群

【００４８】
【数４】

$$F_p^*$$

【００４９】
である。

【００５０】
【数５】

$$F_p^*$$

【００５１】
は、巡回群であり、生成元ｇを含み、したがって、

【００５２】
【数６】

$$F_p^*$$

【００５３】
の任意の元のａに関して、$a = g^n \mod p$であるような整数ｎが見出されることが可能である。値ｐおよびｇは、公に知られており、鍵ペアの公開鍵部分を表す。

【００５４】
次に、１１１０で、端末１２０が、秘密鍵$RAND_i$を、秘密鍵$RAND_i$が非常に大きい素数ｐと比べて、少なくとも１（一）小さく、２（二）を超えて小さくはないようにランダムに選択する。１１２０で、端末１２０が、秘密鍵$RAND_i$からg_{RANDi}を計算する。この計算は、以下のとおり表されることが可能である。すなわち、

$g_{RANDi} \equiv g^{RANDi} \mod p$　　式（１６）

【００５５】
１１３０で、同様に、ＵＩＣＣ１１０が、秘密鍵ＦＲＥＳＨを、秘密鍵ＦＲＥＳＨが非常に大きい素数ｐと比べて、少なくとも１（一）小さく、２（二）を超えて小さくはないように選択する。次に、１１４０で、ＵＩＣＣ１１０が、秘密鍵ＦＲＥＳＨからg_{FRESH}を計算する。この計算は、以下のとおり表されることが可能である。

$g_{FRESH} \equiv g^{FRESH} \mod p$　　式（１７）

【００５６】

次に、１１５０で、ＵＩＣＣ１１０と端末１２０が、インタフェース１３０を介してg_{RANDi}およびg_{FRESH}を交換する。

【００５７】

次に、１１６０で、端末１２０が、秘密鍵ＲＡＮＤｉおよび受け取られたg_{FRESH}を使用して、共有される秘密Ｋを計算する。この計算は、以下のとおり表されることが可能である。すなわち、

【００５８】

【数７】

$$K \equiv g_{FRESH}^{RAND_i} \bmod p$$

式（１８）

【００５９】

１１７０で、同様に、ＵＩＣＣ１１０が、秘密鍵ＦＲＥＳＨおよび受け取られたg_{RAND_i}を使用して、共有される秘密Ｋ’を計算する。この計算は、以下のとおり表されることが可能である。すなわち、

【００６０】

【数８】

$$K' \equiv g_{RAND_i}^{FRESH} \bmod p$$

式（１９）

【００６１】

次に、１１６５、１１７５で、端末１２０およびＵＩＣＣ１１０が、セキュリティ保護された秘密セッション鍵Ｓを計算するのに次に使用される、共有される秘密Ｋ’＝Ｋを処理する。１１８０で、セキュリティ保護された秘密セッション鍵Ｓが、ＧＢＡ＿Ｕ手続きおよびＡＫＡ手続きを実行するのに使用される。

【００６２】

特徴および要素は、前段で、特定の組合せで説明されているものの、各特徴または各要素は、その他の特徴および要素なしに単独で、または他の特徴および要素を伴って、または伴わずに様々な組合せで使用されることが可能である。本明細書で与えられる方法またはフローチャートは、汎用コンピュータまたはプロセッサによって実行されるようにコンピュータ可読記憶媒体に組み込まれたコンピュータプログラム、ソフトウェア、またはファームウェアにおいて実施されることが可能である。コンピュータ可読記憶媒体の例には、ＲＯＭ（読み取り専用メモリ）、ＲＡＭ（ランダムアクセスメモリ）、レジスタ、キャッシュメモリ、半導体メモリデバイス、内部ハードディスクやリムーバブルディスクなどの磁気媒体、光磁気媒体、およびＣＤ－ＲＯＭディスクやＤＶＤ（ＤＶＤ）などの光媒体が含まれる。

【００６３】

適切なプロセッサには、例として、汎用プロセッサ、専用プロセッサ、従来のプロセッサ、ＤＳＰ（デジタルシグナルプロセッサ）、複数のマイクロプロセッサ、ＤＳＰコアに関連する１つまたは複数のマイクロプロセッサ、コントローラ、マイクロコントローラ、ＡＳＩＣ（特定用途向け集積回路）、ＦＰＧＡ（フィールドプログラマブルゲートアレイ）回路、他の任意のタイプのＩＣ（集積回路）、および／または状態マシンが含まれる。

【００６４】

（実施形態）

１．ＵＩＣＣ（汎用ＩＣカード）と端末の間の通信をセキュリティ保護するための方法。

２．通信をセキュリティ保護することは、セキュリティ保護された共有セッション鍵を生成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。

３．通信をセキュリティ保護することは、ＵＩＣＣと端末の間の通信をセキュリティ保護

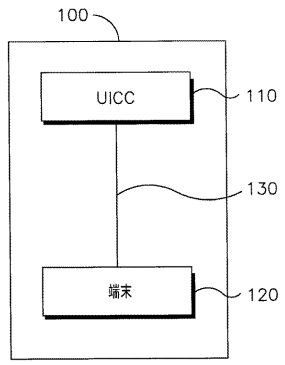
された共有セッション鍵で暗号化することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
４．セキュリティ保護された共有セッション鍵を生成することは、共有される秘密からセキュリティ保護された共有セッション鍵を導き出すことを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５．共有される秘密からセキュリティ保護された共有セッション鍵を導き出すことは、秘密から共有される秘密を生成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
６．セキュリティ保護された共有セッション鍵を導き出すことは、共有される秘密を使用してＰＲＦ（擬似乱数関数）を実行することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
７．通信を暗号化することは、安全な通信路を確立することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
８．安全な通信路を使用して、アプリケーションレベルのＧＢＡ＿Ｕ（ＵＩＣＣベースの拡張を伴うＧＢＡ（汎用ブートストラッピングアーキテクチャ））手続きを実行することをさらに含む前述の実施形態のいずれか１つにおけるとおりの方法。
９．安全な通信路を使用して、ＡＫＡ（認証と鍵の合意）手続きを実行することをさらに含む前述の実施形態のいずれか１つにおけるとおりの方法。
１０．ＵＩＣＣと端末の間のインタフェース上でトンネルを作成することをさらに含む前述の実施形態のいずれか１つにおけるとおりの方法。
１１．セキュリティ保護された共有セッション鍵を生成することは、ＵＩＣＣと端末の間にセキュリティ保護された共有セッション鍵が存在するかどうかを判定することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
１２．セキュリティ保護された共有セッション鍵を生成することは、セキュリティ保護された共有セッション鍵が存在しないという条件で、新たなセキュリティ保護された共有セッション鍵を生成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
１３．セキュリティ保護された共有セッション鍵を生成することは、生成される鍵ネゴシエーションパラメータを生成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
１４．セキュリティ保護された共有セッション鍵を生成することは、生成される鍵ネゴシエーションパラメータをＵＩＣＣに報告することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
１５．セキュリティ保護された共有セッション鍵を生成することは、受け取られる鍵ネゴシエーションパラメータを受け取ることを含む前述の実施形態のいずれか１つにおけるとおりの方法。
１６．セキュリティ保護された共有セッション鍵を生成することは、生成される鍵ネゴシエーションパラメータ、および受け取られる鍵ネゴシエーションパラメータを使用してセキュリティ保護された共有セッション鍵を作成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
１７．作成することは、鍵ネゴシエーションパラメータが、受け取られる鍵ネゴシエーションパラメータと同一であるかどうかを判定することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
１８．作成することは、生成される鍵ネゴシエーションパラメータが、受け取られる鍵ネゴシエーションパラメータと同一であるという条件で、セキュリティ保護された共有セッション鍵を導き出すことを含む前述の実施形態のいずれか１つにおけるとおりの方法。
１９．生成することは、ＲＡＮＤ（ランダムチャレンジ）およびＳＱＮ（シーケンス番号）を選択することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
２０．生成することは、ＡＫ（匿名鍵）を計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
２１．生成することは、ＭＡＣ（メッセージ認証コード）を計算することを含む前述の実

施形態のいずれか１つにおけるとおりの方法。
２２．生成することは、ＸＲＥＳ（想定される応答）を計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
２３．生成することは、ＸＳＱＮ（想定されるシーケンス番号）を計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
２４．生成することは、ＲＡＮＤ、ＭＡＣ、およびＸＳＱＮを組み合わせて、生成される鍵ネゴシエーションパラメータを生成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
２５．計算することは、共有される秘密およびＲＡＮＤを使用してＡＫを計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
２６．計算することは、共有される秘密、ＲＡＮＤ、およびＳＱＮを使用してＭＡＣを計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
２７．計算することは、共有される秘密およびＲＡＮＤを使用してＸＲＥＳを計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
２８．計算することは、ＳＱＮおよびＡＫを使用してＸＳＱＮを計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
２９．生成することは、ノンスを選択することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
３０．生成することは、Ｔａｇ（認証値）を計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
３１．生成することは、ノンスとＴａｇを組み合わせて、生成される鍵ネゴシエーションパラメータを生成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
３２．生成することは、セッション鍵を選択することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
３３．生成することは、暗号化されたセッション鍵を計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
３４．生成することは、暗号化されたセッション鍵を使用して、鍵ネゴシエーションパラメータを生成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
３５．セキュリティ保護された共有セッション鍵を生成することは、受け取られる鍵ネゴシエーションパラメータを受け取ることを含む前述の実施形態のいずれか１つにおけるとおりの方法。
３６．セキュリティ保護された共有セッション鍵を生成することは、生成される鍵ネゴシエーションパラメータを生成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
３７．セキュリティ保護された共有セッション鍵を生成することは、生成される鍵ネゴシエーションパラメータを端末に報告することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
３８．セキュリティ保護された共有セッション鍵を生成することは、受け取られる鍵ネゴシエーションパラメータ、および生成される鍵ネゴシエーションパラメータを使用してセキュリティ保護された共有セッション鍵を作成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
３９．作成することは、生成される鍵ネゴシエーションパラメータが、受け取られる鍵ネゴシエーションパラメータと同一であるかどうかを判定することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
４０．作成することは、生成される鍵ネゴシエーションパラメータが、受け取られる鍵ネゴシエーションパラメータと同一であるという条件で、セキュリティ保護された共有セッション鍵を導き出すことを含む前述の実施形態のいずれか１つにおけるとおりの方法。
４１．生成することは、受け取られる鍵ネゴシエーションパラメータからＲＡＮＤ（ランダムチャレンジ）を抽出することを含む前述の実施形態のいずれか１つにおけるとおりの方法。

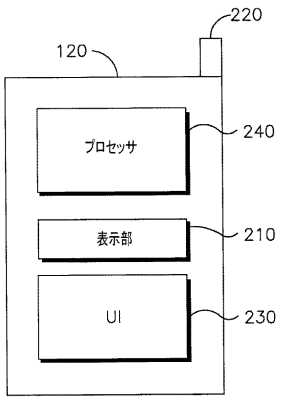
４２．生成することは、受け取られる鍵ネゴシエーションパラメータからＭＡＣ（メッセージ認証コード）を抽出することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
４３．生成することは、受け取られる鍵ネゴシエーションパラメータからＸＳＱＮ（想定されるシーケンス）を抽出することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
４４．生成することは、ＡＫ（匿名鍵）を計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
４５．生成することは、ＸＭＡＣ（想定されるメッセージ認証コード）を計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
４６．生成することは、ＳＱＮ（シーケンス番号）を計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
４７．生成することは、ＸＭＡＣがＭＡＣと同一であるかどうかを判定することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
４８．生成することは、ＸＭＡＣがＭＡＣと同一であるという条件で、共有される秘密およびＲＡＮＤを使用してＲＥＳ（応答）を計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
４９．計算することは、共有される秘密およびＲＡＮＤを使用してＡＫを計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５０．計算することは、ＸＳＱＮおよびＡＫを使用してＳＱＮを計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５１．計算することは、共有される秘密、ＲＡＮＤ、およびＳＱＮを使用してＸＭＡＣを計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５２．生成することは、受け取られる鍵ネゴシエーションパラメータからノンスおよびＴａｇを抽出することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５３．生成することは、Ｔａｇを検証することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５４．生成することは、Ｔａｇが妥当であるという条件で、セッション鍵を導き出し、ＸＴａｇ（想定される認証値）を計算することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５５．生成することは、ＸＴａｇを使用して、生成される鍵ネゴシエーションパラメータを生成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５６．生成することは、受け取られる鍵ネゴシエーションパラメータから暗号化されたセッション鍵を抽出することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５７．セッション鍵を導き出すことは、暗号化されたセッション鍵を解読することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５８．セキュリティ保護された共有セッション鍵を生成することは、事前鍵ネゴシエーションパラメータを生成することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
５９．セキュリティ保護された共有セッション鍵を生成することは、事前鍵ネゴシエーションパラメータを端末に報告することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
６０．セキュリティ保護された共有セッション鍵を生成することは、ＵＩＣＣから事前鍵ネゴシエーションパラメータを受け取ることを含む前述の実施形態のいずれか１つにおけるとおりの方法。
６１．生成することは、ディフィーヘルマン鍵交換プロトコルを実行することを含む前述の実施形態のいずれか１つにおけるとおりの方法。
６２．前述の実施形態のいずれか１つの少なくとも一部を実行するように構成されたＷＴＲＵ（無線送信／受信ユニット）。
６３．前述の実施形態のいずれか１つの少なくとも一部を実行するように構成された基地

局。
６４．前述の実施形態のいずれか１つの少なくとも一部を実行するように構成された集積回路。
【００６５】
ソフトウェアに関連するプロセッサが、ＷＴＲＵ（無線送信／受信ユニット）、ＵＥ（ユーザ機器）、端末、基地局、ＲＮＣ（無線ネットワークコントローラ）、または任意のホストコンピュータにおいて使用するための無線周波数トランシーバを実施するのに使用されることが可能である。ＷＴＲＵは、カメラ、ビデオカメラモジュール、テレビ電話機、スピーカフォン、振動デバイス、スピーカ、マイクロフォン、テレビトランシーバ、ハンズフリーハンドセット、キーボード、Ｂｌｕｅｔｏｏｔｈ（登録商標）モジュール、ＦＭ（周波数変調）無線ユニット、ＬＣＤ（液晶表示部）表示部ユニット、ＯＬＥＤ（有機発光ダイオード）表示部ユニット、デジタル音楽プレーヤ、メディアプレーヤ、ビデオゲームプレーヤモジュール、インターネットブラウザ、および／またはＷＬＡＮ（無線ローカルエリアネットワーク）モジュールもしくはＵＷＢ（ウルトラワイドバンド（超広帯域））モジュールなどの、ハードウェアおよび／またはソフトウェアで実施されるモジュールと連携して使用されることが可能である。

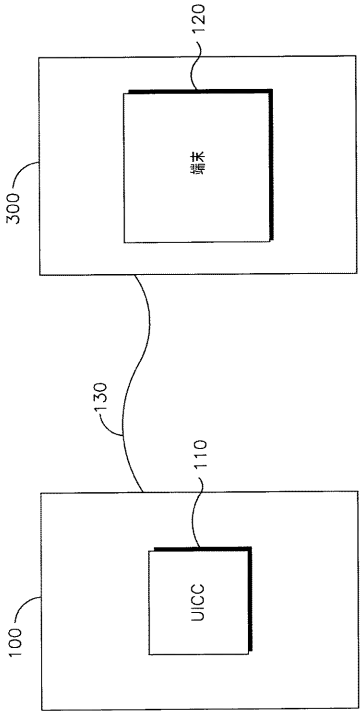
【図１】



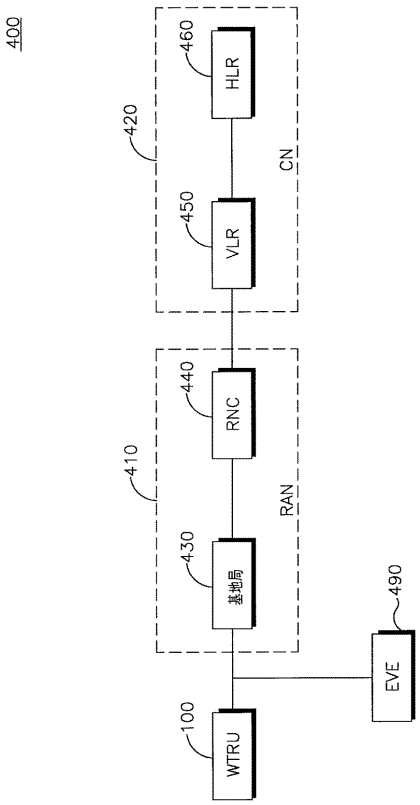
【図２】



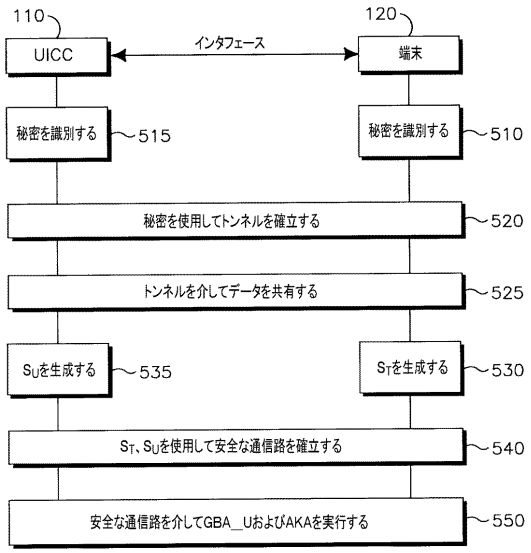
【図３】


120
端末
300
130
110
UICC
100

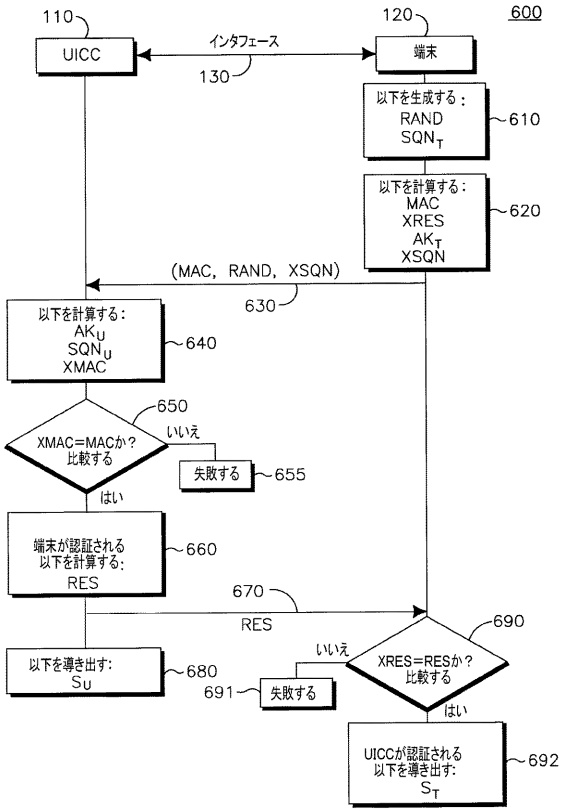
【図４】


400
460
HLR
420
CN
450
VLR
440
RNC
410
RAN
430
基地局
490
EVE
100
WTRU

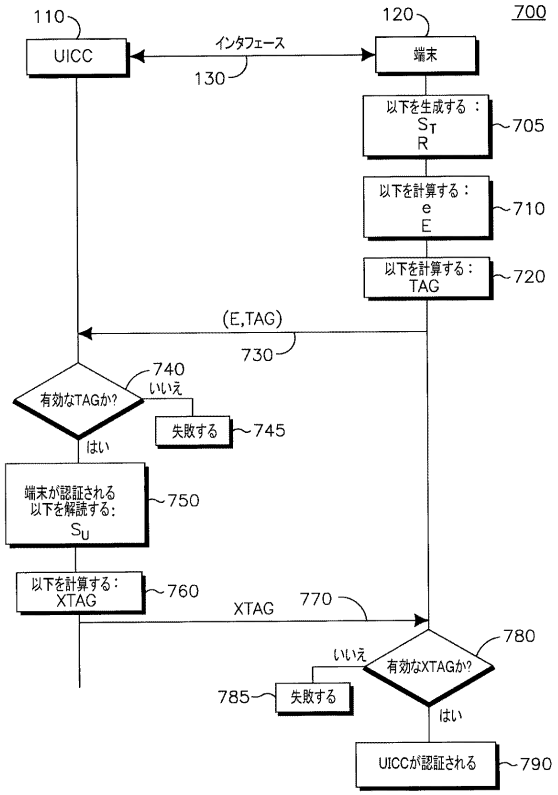
【図５】


110
UICC
インタフェース
120
端末
秘密を識別する
515
秘密を識別する
510
秘密を使用してトンネルを確立する
520
トンネルを介してデータを共有する
525
SIを生成する
535
STを生成する
530
ST、SUを使用して安全な通信路を確立する
540
安全な通信路を介してGBA_UおよびAKAを実行する
550

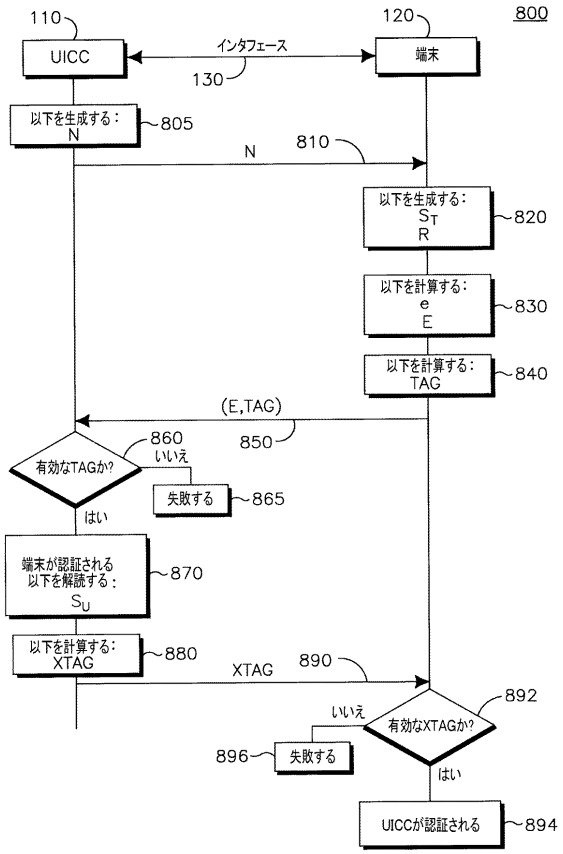
【図６】


600
110
UICC
インタフェース
130
120
端末
以下を生成する：
RAND
SQNT
610
以下を計算する：
MAC
XRES
AKT
XSQN
620
(MAC, RAND, XSQN)
630
以下を計算する：
AKU
SQNU
XMAC
640
650
XMAC=MACか？
比較する
いいえ
失敗する
655
はい
端末が認証される
以下を計算する：
RES
660
670
RES
690
以下を導き出す：
SU
680
691
失敗する
いいえ
XRES=RESか？
比較する
はい
UICCが認証される
以下を導き出す：
ST
692

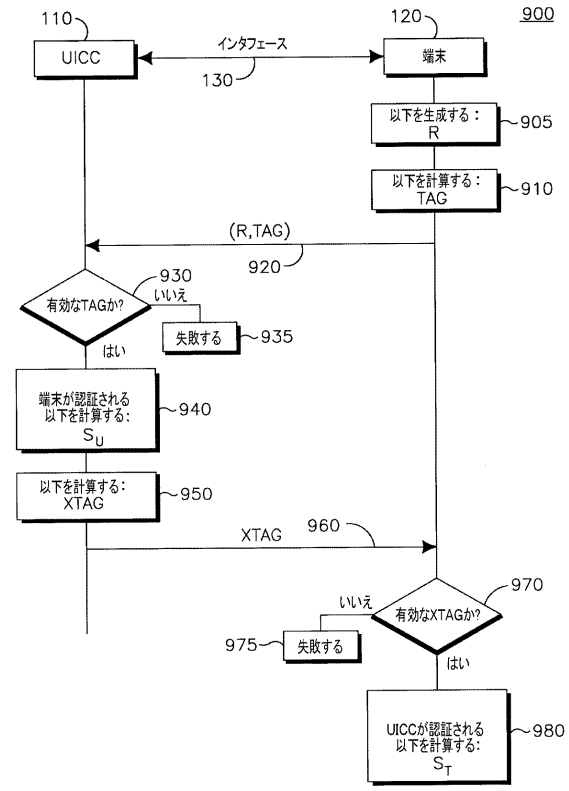
【図７】


700
110
UICC
インタフェース
130
120
端末
以下を生成する：
S_T
R
705
以下を計算する：
e
E
710
以下を計算する：
TAG
720
(E,TAG)
730
有効なTAGか?
740
いいえ
失敗する
745
はい
端末が認証される
以下を解読する：
S_U
750
以下を計算する：
XTAG
760
XTAG
770
有効なXTAGか?
780
いいえ
785
失敗する
はい
UICCが認証される
790

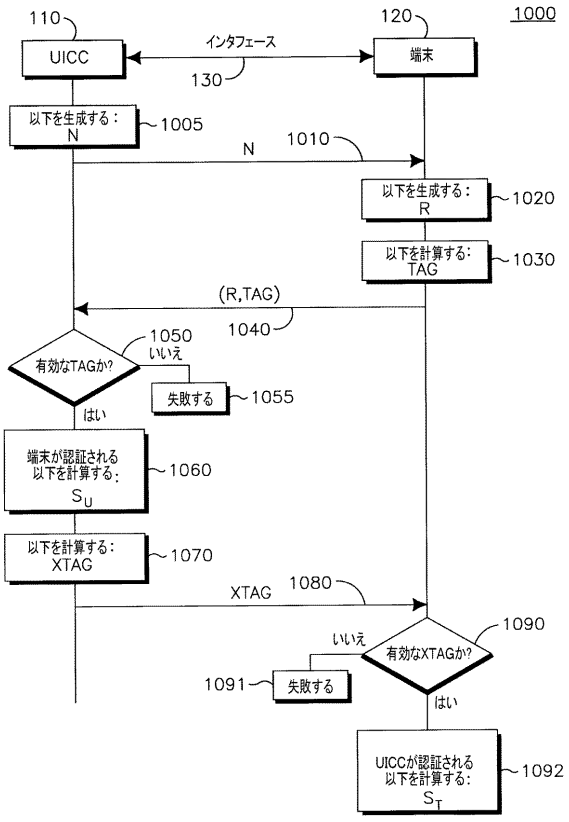
【図８】


800
110
UICC
インタフェース
130
120
端末
以下を生成する：
N
805
N
810
以下を生成する：
S_T
R
820
以下を計算する：
e
E
830
以下を計算する：
TAG
840
(E,TAG)
850
有効なTAGか?
860
いいえ
失敗する
865
はい
端末が認証される
以下を解読する：
S_U
870
以下を計算する：
XTAG
880
XTAG
890
有効なXTAGか?
892
いいえ
896
失敗する
はい
UICCが認証される
894

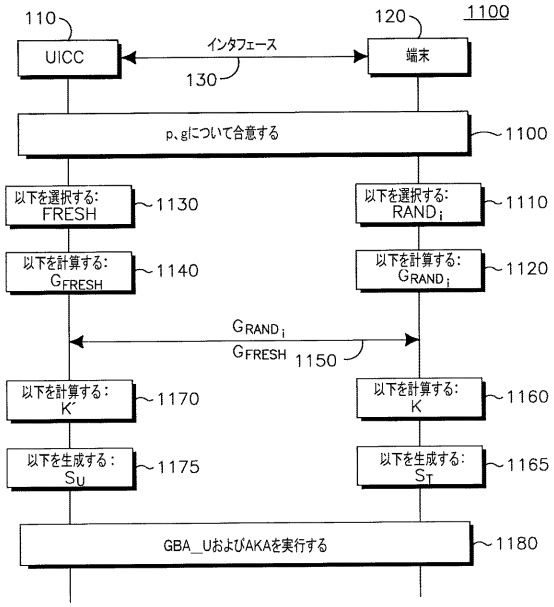
【図９】


900
110
UICC
インタフェース
130
120
端末
以下を生成する：
R
905
以下を計算する：
TAG
910
(R,TAG)
920
有効なTAGか?
930
いいえ
失敗する
935
はい
端末が認証される
以下を計算する：
S_U
940
以下を計算する：
XTAG
950
XTAG
960
有効なXTAGか?
970
いいえ
975
失敗する
はい
UICCが認証される
以下を計算する：
S_T
980

【図１０】


1000
110
UICC
インタフェース
130
120
端末
以下を生成する：
N
1005
N
1010
以下を生成する：
R
1020
以下を計算する：
TAG
1030
(R,TAG)
1040
有効なTAGか?
1050
いいえ
失敗する
1055
はい
端末が認証される
以下を計算する：
S_U
1060
以下を計算する：
XTAG
1070
XTAG
1080
有効なXTAGか?
1090
いいえ
1091
失敗する
はい
UICCが認証される
以下を計算する：
S_T
1092

【図１１】



【手続補正書】
【提出日】平成22年12月7日(2010.12.7)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ＵＩＣＣ（汎用ＩＣカード）と端末の間の通信をセキュリティ保護するための方法であって、
セキュリティ保護された共有セッション鍵を生成すること、
前記ＵＩＣＣと前記端末の間の通信を前記セキュリティ保護された共有セッション鍵で暗号化して、安全な通信路を確立すること、および
前記安全な通信路を介して手続き（プロシージャ）を実行することを含むことを特徴とする方法。
【請求項２】
前記セキュリティ保護された共有セッション鍵を生成することは、共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すことを含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すことは、秘密から共有される秘密を生成することを含むことを特徴とする請求項２に記載の方法。
【請求項４】

前記セキュリティ保護された共有セッション鍵を導き出すことは、前記共有される秘密を使用してＰＲＦ（擬似乱数関数）を実行することを含むことを特徴とする請求項２に記載の方法。
【請求項５】
前記手続きを実行することは、アプリケーションレベルのＧＢＡ＿Ｕ（ＵＩＣＣベースの拡張を伴うＧＢＡ（汎用ブートストラッピングアーキテクチャ））手続き、またはＡＫＡ（認証と鍵の合意）手続きの少なくともいずれかを実行することを含むことを特徴とする請求項１に記載の方法。
【請求項６】
前記ＵＩＣＣと前記端末の間のインタフェース上でトンネルを作成することをさらに含むことを特徴とする請求項１に記載の方法。
【請求項７】
前記セキュリティ保護された共有セッション鍵を生成することは、
前記ＵＩＣＣと前記端末の間にセキュリティ保護された共有セッション鍵が存在するかどうかを判定すること、および
前記セキュリティ保護された共有セッション鍵が存在していないという条件で、新たなセキュリティ保護された共有セッション鍵を生成することを含むことを特徴とする請求項１に記載の方法。
【請求項８】
前記セキュリティ保護された共有セッション鍵を生成することは、
生成されるべき鍵ネゴシエーションパラメータを生成し、該生成された鍵ネゴシエーションパラメータを前記ＵＩＣＣに報告すること、
受け取られるべき鍵ネゴシエーションパラメータを受け取ること、
前記生成された鍵ネゴシエーションパラメータ、および前記受け取られた鍵ネゴシエーションパラメータを使用して、前記セキュリティ保護された共有セッション鍵を作成することを含むことを特徴とする請求項１に記載の方法。
【請求項９】
前記作成することは、
前記生成された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるかどうかを判定すること、および
前記生成された鍵ネゴシエーションパラメータが、前記受信された鍵ネゴシエーションパラメータと同一であるという条件で、セキュリティ保護された共有セッション鍵を導き出すことを含むことを特徴とする請求項８に記載の方法。
【請求項１０】
前記生成することは、
ＲＡＮＤ（ランダムチャレンジ）およびＳＱＮ（シーケンス番号）を選択すること、
ＡＫ（匿名鍵）、ＭＡＣ（メッセージ認証コード）、ＸＲＥＳ（想定される応答）、およびＸＳＱＮ（想定されるシーケンス）を計算すること、および
前記ＲＡＮＤ、前記ＭＡＣ、および前記ＸＳＱＮを組み合わせて、前記生成されるべき鍵ネゴシエーションパラメータを生成することを含むことを特徴とする請求項８に記載の方法。
【請求項１１】
前記計算することは、
共有される秘密および前記ＲＡＮＤを使用して前記ＡＫを計算すること、
前記共有される秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＭＡＣを計算すること、
前記共有される秘密および前記ＲＡＮＤを使用して前記ＸＲＥＳを計算すること、および
前記ＳＱＮおよび前記ＡＫを使用して前記ＸＳＱＮを計算することを含むことを特徴とする請求項１０に記載の方法。

【請求項１２】
前記生成することは、
ノンスを選択すること、
Ｔａｇ（認証値）を計算すること、および
前記ノンスと前記Ｔａｇを組み合わせて、前記生成されるべき鍵ネゴシエーションパラメータを生成することを含むことを特徴とする請求項８に記載の方法。
【請求項１３】
前記生成することは、
セッション鍵を選択すること、
暗号化されたセッション鍵を計算すること、および
前記暗号化されたセッション鍵を使用して、前記鍵ネゴシエーションパラメータを生成することを含むことを特徴とする請求項８に記載の方法。
【請求項１４】
前記セキュリティ保護された共有セッション鍵を生成することは、
受け取られるべき鍵ネゴシエーションパラメータを受け取ること、
生成されるべき鍵ネゴシエーションパラメータを生成すること、
前記生成された鍵ネゴシエーションパラメータを前記端末に報告すること、および
前記受け取られた鍵ネゴシエーションパラメータ、および前記生成された鍵ネゴシエーションパラメータを使用して、前記セキュリティ保護された共有セッション鍵を作成すること
を含むことを特徴とする請求項１に記載の方法。
【請求項１５】
前記作成することは、
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるかどうかを判定すること、および
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるという条件で、セキュリティ保護された共有セッション鍵を導き出すこと
を含むことを特徴とする請求項１４に記載の方法。
【請求項１６】
前記生成することは、
前記受け取られた鍵ネゴシエーションパラメータからＲＡＮＤ（ランダムチャレンジ）、ＭＡＣ（メッセージ認証コード）、およびＸＳＱＮ（想定されるシーケンス）を抽出すること、
ＡＫ（匿名鍵）、ＸＭＡＣ（想定されるメッセージ認証コード）、およびＳＱＮ（シーケンス番号）を計算すること、
前記ＸＭＡＣが前記ＭＡＣと同一であるかどうかを判定すること、および
前記ＸＭＡＣが前記ＭＡＣと同一であるという条件で、共有される秘密および前記ＲＡＮＤを使用してＲＥＳ（応答）を計算すること
を含むことを特徴とする請求項１４に記載の方法。
【請求項１７】
前記計算することは、
前記共有される秘密および前記ＲＡＮＤを使用して前記ＡＫを計算すること、
前記ＸＳＱＮおよび前記ＡＫを使用して前記ＳＱＮを計算すること、および
前記共有される秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＸＭＡＣを計算すること
を含むことを特徴とする請求項１６に記載の方法。
【請求項１８】
前記生成することは、
前記受け取られた鍵ネゴシエーションパラメータからノンスおよびＴａｇを抽出するこ

と、
前記Ｔａｇを検証すること、
前記Ｔａｇが有効であるという条件で、セッション鍵を導き出し、ＸＴａｇ（想定される認証値）を計算すること、および
前記ＸＴａｇを使用して、前記生成されるべき鍵ネゴシエーションパラメータを生成すること
を含むことを特徴とする請求項１４に記載の方法。
【請求項１９】
前記生成することは、前記受け取られる鍵ネゴシエーションパラメータから前記暗号化されたセッション鍵を抽出することを含み、さらに該セッション鍵を導き出すことは、前記暗号化されたセッション鍵を解読することを含むことを特徴とする請求項１８に記載の方法。
【請求項２０】
前記セキュリティ保護された共有セッション鍵を生成することは、
事前鍵ネゴシエーションパラメータを生成すること、および
前記事前鍵ネゴシエーションパラメータを前記端末に報告すること
を含むことを特徴とする請求項１に記載の方法。
【請求項２１】
前記セキュリティ保護された共有セッション鍵を生成することは、
前記ＵＩＣＣから事前鍵ネゴシエーションパラメータを受け取ることを含むことを特徴とする請求項１に記載の方法。
【請求項２２】
前記生成することは、ディフィーヘルマン鍵交換プロトコルを実行することを含むことを特徴とする請求項１に記載の方法。
【請求項２３】
セキュリティ保護された共有セッション鍵を生成し、前記セキュリティ保護された共有セッション鍵で通信を暗号化するように構成されたＵＩＣＣ（汎用ＩＣカード）と、
前記セキュリティ保護された共有セッション鍵を生成し、前記セキュリティ保護された共有セッション鍵で通信を暗号化し、安全な通信路を確立し、かつ前記安全な通信路を介して手続き（プロシージャ）を実行するように構成された端末と
を具備することを特徴とするＷＴＲＵ（無線送信／受信ユニット）。
【請求項２４】
前記ＵＩＣＣは、共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すことによって、前記セキュリティ保護された共有セッション鍵を生成するように構成され、さらに
前記端末は、前記共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すことによって、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項２３に記載のＷＴＲＵ。
【請求項２５】
前記ＵＩＣＣは、第１の秘密から前記共有される秘密を生成することによって、前記共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すように構成され、さらに
前記端末は、第２の秘密から前記共有される秘密を生成することによって、前記共有される秘密から前記セキュリティ保護された共有セッション鍵を導き出すように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項２６】
前記ＵＩＣＣは、前記共有される秘密を使用してＰＲＦ（擬似乱数関数）を実行することによって、前記セキュリティ保護された共有セッション鍵を導き出すように構成され、さらに
前記端末は、前記共有される秘密を使用してＰＲＦ（擬似乱数関数）を実行することによ

って、前記セキュリティ保護された共有セッション鍵を導き出すように構成されることを特徴とする請求項２４に記載のＷＴＲＵ。
【請求項２７】
前記ＵＩＣＣは、前記端末と前記安全な通信路を確立するように構成されることを特徴とする請求項２３に記載のＷＴＲＵ。
【請求項２８】
前記安全な通信路を介して手続きを実行することは、アプリケーションレベルのＧＢＡ＿Ｕ（ＵＩＣＣベースの拡張を伴うＧＢＡ（汎用ブートストラッピングアーキテクチャ））手続き、またはＡＫＡ（認証と鍵の合意）手続きの少なくともいずれかを実行することを含むことを特徴とする請求項２７に記載のＷＴＲＵ。
【請求項２９】
前記端末は、
生成されるべき鍵ネゴシエーションパラメータを生成し、
前記生成された鍵ネゴシエーションパラメータを前記ＵＩＣＣに報告し、
前記ＵＩＣＣから、受け取られるべき鍵ネゴシエーションパラメータを受け取り、さらに
前記生成された鍵ネゴシエーションパラメータ、および前記受け取られた鍵ネゴシエーションパラメータを使用して、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項２３に記載のＷＴＲＵ。
【請求項３０】
前記端末は、
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるかどうかを判定し、さらに
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるという条件で、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項２９に記載のＷＴＲＵ。
【請求項３１】
前記端末は、
ＲＡＮＤ（ランダムチャレンジ）およびＳＱＮ（シーケンス番号）を選択し、
ＡＫ（匿名鍵）、ＭＡＣ（メッセージ認証コード）、ＸＲＥＳ（想定される応答）、およびＸＳＱＮ（想定されるシーケンス）を計算し、さらに
前記ＲＡＮＤ、前記ＭＡＣ、および前記ＸＳＱＮを使用して、前記生成される鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項２９に記載のＷＴＲＵ。
【請求項３２】
前記端末は、
共有される秘密と前記ＲＡＮＤを使用して前記ＡＫを計算し、
前記共有される秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＭＡＣを計算し、
前記共有される秘密および前記ＲＡＮＤを使用して前記ＸＲＥＳを計算し、さらに
前記ＳＱＮおよび前記ＡＫを使用して前記ＸＳＱＮを計算するように構成されることを特徴とする請求項３１に記載のＷＴＲＵ。
【請求項３３】
前記端末は、
ノンスを選択し、
Ｔａｇ（認証値）を計算し、さらに
前記ノンスと前記Ｔａｇを使用して、前記生成されるべき鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項２９に記載のＷＴＲＵ。
【請求項３４】
前記端末は、

セッション鍵を選択し、
暗号化されたセッション鍵を計算し、さらに
前記暗号化されたセッション鍵を使用して、前記生成されるべき鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項２９に記載のＷＴＲＵ。
【請求項３５】
前記ＵＩＣＣは、
前記端末から、受け取られる鍵ネゴシエーションパラメータを受け取り、
生成されるべき鍵ネゴシエーションパラメータを生成し、
前記生成された鍵ネゴシエーションパラメータを前記端末に報告し、さらに
前記受け取られた鍵ネゴシエーションパラメータ、および前記生成された鍵ネゴシエーションパラメータを使用して、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項２３に記載のＷＴＲＵ。
【請求項３６】
前記ＵＩＣＣは、
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるかどうかを判定し、さらに
前記生成された鍵ネゴシエーションパラメータが、前記受け取られた鍵ネゴシエーションパラメータと同一であるという条件で、前記セキュリティ保護された共有セッション鍵を生成するように構成されることを特徴とする請求項３５に記載のＷＴＲＵ。
【請求項３７】
前記ＵＩＣＣは、
前記受け取られた鍵ネゴシエーションパラメータからＲＡＮＤ（ランダムチャレンジ）、ＭＡＣ（メッセージ認証コード）、およびＸＳＱＮ（想定されるシーケンス）を抽出し、
ＡＫ（匿名鍵）、ＸＭＡＣ（想定されるメッセージ認証コード）、およびＳＱＮ（シーケンス番号）を計算し、
前記ＸＭＡＣが前記ＭＡＣと同一であるかどうかを判定し、
前記ＸＭＡＣが前記ＭＡＣと同一であるという条件で、共有される秘密および前記ＲＡＮＤとを使用してＲＥＳ（応答）を計算し、さらに
前記ＲＥＳを使用して、前記生成される鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項３５に記載のＷＴＲＵ。
【請求項３８】
前記ＵＩＣＣは、
前記共有される秘密および前記ＲＡＮＤを使用して前記ＡＫを計算し、
前記ＸＳＱＮおよび前記ＡＫを使用して前記ＳＱＮを計算し、さらに
前記共有される秘密、前記ＲＡＮＤ、および前記ＳＱＮを使用して前記ＸＭＡＣを計算するように構成されることを特徴とする請求項３７に記載のＷＴＲＵ。
【請求項３９】
前記ＵＩＣＣは、
前記受け取られた鍵ネゴシエーションパラメータからノンスおよびＴａｇを抽出し、
前記Ｔａｇを検証し、
ＸＴａｇ（想定される認証値）を計算し、さらに
前記ＸＴａｇを使用して、前記生成されるべき鍵ネゴシエーションパラメータを生成するように構成されることを特徴とする請求項３５に記載のＷＴＲＵ。
【請求項４０】
前記ＵＩＣＣは、
前記受け取られた鍵ネゴシエーションパラメータから暗号化されたセッション鍵を抽出し、
前記暗号化されたセッション鍵を解読し、さらに
前記解読されたセッション鍵を使用して、前記セキュリティ保護された共有セッション

鍵を生成するように構成されることを特徴とする請求項３９に記載のＷＴＲＵ。
【請求項４１】
前記ＵＩＣＣは、
事前鍵ネゴシエーションパラメータを生成し、さらに
前記事前鍵ネゴシエーションパラメータを前記端末に報告するように構成されることを特徴とする請求項２３に記載のＷＴＲＵ。
【請求項４２】
前記端末は、
事前鍵ネゴシエーションパラメータを前記ＵＩＣＣから受け取るように構成されることを特徴とする請求項２３に記載のＷＴＲＵ。
【請求項４３】
前記ＵＩＣＣは、ディフィーヘルマン鍵交換プロトコルを実行するように構成され、さらに前記端末は、ディフィーヘルマン鍵交換プロトコルを実行するように構成されることを特徴とする請求項２３に記載のＷＴＲＵ。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/039805

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06

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)
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 practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Key establishment between a UICC and a terminal; (Release 7); 3GPP TS 33.110" ETSI STANDARDS, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, no. V1.0.0, 1 June 2006 (2006-06-01), XP014035038 ISSN: 0000-0001 page 8 - page 12	1-44
X	WO 2006/094838 A1 (ERICSSON TELEFON AB L M [SE]; GEHRMANN CHRISTIAN [SE]) 14 September 2006 (2006-09-14) page 4, line 1 - line 10 page 5, line 17 - page 8, line 9; figure 3	1-44

☐ 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 document 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
3 February 2010	10/02/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Raposo Pires, João

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2009/039805

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006094838 A1	14-09-2006	EP 1856836 A1	21-11-2007
		KR 20070112260 A	22-11-2007
		US 2006206710 A1	14-09-2006

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

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

(72)発明者 エフゲニー ドディス
アメリカ合衆国 １００１２ ニューヨーク州 ニューヨーク ワシントン スクエア ヴィレッジ ナンバー１２エイチ ２
(72)発明者 ヨゲンドラ シー. シャー
アメリカ合衆国 １９３４１ ペンシルベニア州 エクストン リージェンシー コート １０
(72)発明者 インヒョク チャ
アメリカ合衆国 １９０６７ ペンシルベニア州 ヤードリー サウスリッジ サークル ５１０

Ｆターム(参考) 5J104 AA07 AA16 EA15 EA18 KA02 KA04 NA02 NA35 PA01
5K067 AA21 BB04 BB21 DD27 EE02 FF02 FF32 HH36