審決

不服２０１４－　２４７０４

アメリカ合衆国 カリフォルニア ９２１２１ サン ディエゴ モアハウス ドライブ ５７７５
請求人　　クアルコム，インコーポレイテッド

東京都千代田区丸の内一丁目９番２号 グラントウキョウサウスタワー 特許業務法人 志賀国際特許事務所
代理人弁理士　　村山 靖彦

東京都千代田区丸の内一丁目９番２号 グラントウキョウサウスタワー 特許業務法人 志賀国際特許事務所
代理人弁理士　　黒田 晋平

特願２０１３－５１５５２６「通信システムにおいて加入者認証とデバイス認証とをバインドするための方法および装置」拒絶査定不服審判事件〔平成２３年１２月２２日国際公開，ＷＯ２０１１／１５９９５２，平成２５年９月　５日国内公表、特表２０１３－５３４７５４〕について，次のとおり審決する。

結　論

本件審判の請求は，成り立たない。

理　由

１．手続の経緯

本件請求に係る出願（以下「本願」という。）は，２０１０年６月１６日（以下「優先日」という。）のアメリカ合衆国における出願，及び，２０１１年６月１５日のアメリカ合衆国における出願を基礎とするパリ条約による優先権主張を伴った，２０１１年６月１６日を国際出願日とする出願であって，その手続の経緯の概略は以下のとおりである。

平成２４年１２月１４日	：国内書面の提出
平成２４年１２月２０日	：国際出願翻訳文提出書， 出願審査請求書の提出
平成２５年１２月　２日付け	：拒絶理由の通知
平成２６年　４月　８日	：意見書，手続補正書の提出
平成２６年　７月２５日付け	：拒絶査定（同年８月４日謄本送達）
平成２６年１２月　３日	：審判請求書，手続補正書の提出
平成２６年１２月２５日	：前置報告
平成２７年　４月　７日	：上申書の提出
平成２７年　８月３１日付け	：拒絶理由の通知（当審）
平成２７年１２月　７日	：意見書，手続補正書の提出

２．本願発明

本願の請求項１に記載された発明（以下，「本願発明」という。）は，上記平成２７年１２月７日付け手続補正書により補正された特許請求の範囲，明細書及び図面の記載からみて，その特許請求の範囲の請求項１に記載された以下のとおりのものと認める。

「デバイスにおいて動作可能な方法であって，

サブスクリプションを認証するための鍵に基づいてネットワークエンティティとの加入者認証を実行し，第１の鍵を取得するステップと，
質問応答交換に基づいて前記ネットワークエンティティとの前記デバイスのデバイス認証を実行し，第２の鍵を含むデバイス認証データを取得するステップであって，前記第２の鍵は前記ネットワークエンティティから取得され，前記デバイス認証のための質問は暗号化された前記第２の鍵を含む，デバイス認証データを取得するステップと，
前記第１の鍵と前記デバイス認証データとに基づいて，前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成するステップと，
前記デバイスとサービングネットワークとの間の通信をセキュアにするために前記セキュリティ鍵を使用するステップと
を含む，方法。」

３．引用文献

（１）引用文献１に記載されている技術的事項および引用発明１

本願優先日前に頒布され，上記平成２７年８月３１日付けで当審より通知した拒絶理由通知（以下，「当審拒絶理由」という。）において引用された，特表２００８－５４７３５０号公報（平成２０年１２月２５日公表。以下，「引用文献１」という。）には，図面とともに，以下の技術的事項が記載されている。（当審注：下線は，参考のために当審で付与したものである。）

Ａ．「【０００５】
図１を参照すると，IEEE 802.16e通信システムは，移動端末機（Mobile Station；以下，‘ＭＳ’と称する）ＭＳ１００と，基地局（ＢＳ：Base Station）１４０と，権限・認証・アカウンティング（Authorization, Authentication and Accounting；以下，‘ＡＡＡ’と称する）サーバー１８０を含む。IEEE 802.16e通信システムにおいては，EAP-in-EAP方式を使用するので，２回のＥＡＰ方式に従う認証が遂行される。以下，説明の便宜のため，ＥＡＰ方式に基づいた認証を‘ＥＡＰ認証’と称する。上記２回のＥＡＰ認証のうち，第１のＥＡＰ認証１２０は機器認証であり，第２のＥＡＰ認証１６０は第１のＥＡＰ認証が成功した後のユーザ認証である。」

Ｂ．「【００３７】
前述した目的を達成するために本発明は，移動端末機と，基地局と，権限・認証・アカウンティング（ＡＡＡ：Authorization, Authentication and Accounting）サーバーを含む広帯域無線接続通信システムにおける拡張可能認証プロトコル（ＥＡＰ：Extensible Authentication Protocol）方式を使用して認証を遂行する方法であって，移動端末機と，基地局とＡＡＡサーバーは，EAP-in-EAP方式を使用して上記移動端末機に対する機器認証である第１のＥＡＰ認証を遂行して第１のマスターセッションキー（ＭＳＫ：Master Session Key）を獲得する過程と，上記第１のＥＡＰ認証を遂行した後に，上記移動端末機と上記基地局と上記ＡＡＡサーバーは，上記EAP-in-EAP方式を使用して上記移動端末機に対するユーザ認証である第２のＥＡＰ認証を遂行して第２のＭＳＫを獲得する過程とを含むことを特徴とする。
・・・（中略）・・・
【００４１】
図４は，本発明の実施形態に従うIEEE 802.16e通信システムにおける二重ペアワイズマスターキー（Pairwise Master Key；以下，‘ＰＭＫ’と称する）を使用するEAP-in-EAP方式の認証に対する信号の流れを示す信号流れ図である。」

Ｃ．「【００５３】
ＡＡＡサーバー４８０は，基地局４４０へ，ＥＡＰ認証に成功したことを表すRADIUS ACCEPTメッセージを送信する（ステップＳ４７３）。基地局４４０は，ＭＳ４００へPKM_EAP/EAP-SUCCESSメッセージを送信する（ス

テップＳ４７５）。ユーザ認証４６０を通じて，基地局４４０は，ＭＳＫ２から第２のＰＭＫ（すなわち，ＰＭＫ２）を生成し，ＰＭＫとＰＭＫ２とを使用して権限キー（Authorization Key；以下，‘ＡＫ’と称する）を生成する（ステップＳ４７７）。ＭＳ４００及び基地局４４０が，ＰＭＫとＰＭＫ２とから，ＡＫを生成する動作については，下記の図５の説明で詳しく後述するので，ここでは，その詳細な説明を省略する。

【００５４】

図５は，本発明に従うIEEE 802.16e通信システムにおけるＡＫを生成する過程を示すフローチャートである。

【００５５】

この過程は，基地局での生成及びＭＳ全てで遂行され，ここでは，基地局がＡＫを生成する場合を説明することにする。

【００５６】

図５を参照すると，ステップＳ５１１で，基地局は，第１のＥＡＰ認証，即ち機器認証を通じてＭＳＫを獲得し，ステップＳ５１３で，一般にＭＳＫを使用してＥＩＫとＰＭＫとを生成する。具体的には，基地局は，ＭＳＫを除去（truncation）して所定のビット，一例としては，１６０ビットのＥＩＫと１６０ビットのＰＭＫで，ＥＩＫとＰＭＫとを生成する。

【００５７】

ステップＳ５１５で，基地局は，第２のＥＡＰ認証，即ちユーザ認証を通じて第２のＭＳＫ（すなわち，ＭＳＫ２）を獲得し，ステップＳ５１７で，第２のＰＭＫ（すなわち，ＰＭＫ２），一例としては，ＭＳＫ２の除去により１６０ビットであるＰＭＫ２を生成する。

【００５８】

基地局は，ＰＭＫとＰＭＫ２をＡＫ生成関数に適用してＡＫを生成する。具体的には，基地局は，一例として，Dot16KDF関数にＰＭＫとＰＭＫ２とを適用する。Dot16KDF関数は，下記数式３または数式４のような関数で表すことができる。

【００５９】

【数３】

AK=Dot16KDF(PMK (+) PMK2,SSID|BSID|'AK',160)

【００６０】

数式３において，ＳＳＩＤはＥＡＰ認証が遂行されるＭＳの識別子（ＩＤ）を表し，ＢＳＩＤは基地局の識別子（ＩＤ）を表し，‘ＡＫ’はDot16KDF関数により生成されるＡＫであることを表し，１６０はＡＫの長さが１６０ビットであることを表す。したがって，Dot16KDF関数は，ＰＭＫとＰＭＫ２との排他的論理和（ＸＯＲ）と，ＳＳＩＤとＢＳＩＤを連接（concatenation）したパラメータを使用して，１６０ビットのＡＫを生成する。

【００６１】

【数４】

AK=Dot16KDF(PMK,SSID|BSID|PMK2|'AK',160)

【００６２】

数式４において，ＳＳＩＤは，ＥＡＰ認証が遂行されるＭＳの識別子（ＩＤ）を表し，ＢＳＩＤは基地局の識別子（ＩＤ）を表し，‘ＡＫ’は上記Dot16KDF関数により生成されるＡＫであることを表し，１６０はＡＫの長さが１６０ビットであることを表す。したがって，Dot16KDF関数は，ＰＭＫとＳＳＩＤ，ＢＳＩＤ及びＰＭＫ２を連接したパラメータを使用して，１６０ビットのＡＫを生成する。

【００６３】

前述したように，本発明の実施形態に従うIEEE 802.16e通信システムにおいて，二重ＰＭＫを使用するEAP-in-EAP方式を使用して認証を遂行する場合に，第１のＥＡＰ認証で生成されたＰＭＫと，第２の認証で生成されたＰＭＫ２を使用して，ＡＫが生成される。したがって，一般的なIEEE 802.16e通信システムで発生していた中間者攻撃の発生を除去することができる。」

ここで，上記引用文献１に記載されている事項を検討する。

（ア）上記Ａの「IEEE 802.16e通信システムは，移動端末機（Mobile

Station；以下，‘ＭＳ’と称する）ＭＳ１００と，基地局（ＢＳ：Base Station）１４０と，権限・認証・アカウンティング（Authorization, Authentication and Accounting；以下，‘ＡＡＡ’と称する）サーバー１８０を含む。」との記載，上記Ｂの「本発明は，移動端末機と，基地局と，権限・認証・アカウンティング（ＡＡＡ：Authorization, Authentication and Accounting）サーバーを含む広帯域無線接続通信システムにおける拡張可能認証プロトコル（ＥＡＰ：Extensible Authentication Protocol）方式を使用して認証を遂行する方法であって」との記載からすると，

引用文献１には，

“通信システムは，移動端末機ＭＳと，基地局及び認証サーバであるＡＡＡサーバとを含”むことが記載されていると認められる。

（イ）上記Ｂの「移動端末機と，基地局とＡＡＡサーバーは，EAP-in-EAP方式を使用して上記移動端末機に対する機器認証である第１のＥＡＰ認証を遂行して第１のマスターセッションキー（ＭＳＫ：Master Session Key）を獲得する過程」，「ペアワイズマスターキー（Pairwise Master Key；以下，‘ＰＭＫ’と称する）」との記載，上記Ｃの段落【００５５】の「この過程は，基地局での生成及びＭＳ全てで遂行され，ここでは，基地局がＡＫを生成する場合を説明することにする。」，段落【００５６】の「基地局は，第１のＥＡＰ認証，即ち機器認証を通じてＭＳＫを獲得し，ステップＳ５１３で，一般にＭＳＫを使用してＥＩＫとＰＭＫとを生成する。」との記載からすると，

引用文献１には，

“ＭＳは，ＡＡＡサーバと機器認証を実行し，獲得したマスターセッションキーＭＳＫからペアワイズマスターキーＰＭＫを生成”することが記載されていると認められる。

（ウ）上記Ｂの「上記移動端末機と上記基地局と上記ＡＡＡサーバーは，上記EAP-in-EAP方式を使用して上記移動端末機に対するユーザ認証である第２のＥＡＰ認証を遂行して第２のＭＳＫを獲得する過程」，「ペアワイズマスターキー（Pairwise Master Key；以下，‘ＰＭＫ’と称する）」との記載，上記Ｃの段落【００５５】の「この過程は，基地局での生成及びＭＳ全てで遂行され，ここでは，基地局がＡＫを生成する場合を説明することにする。」，段落【００５７】の「基地局は，第２のＥＡＰ認証，即ちユーザ認証を通じて第２のＭＳＫ（すなわち，ＭＳＫ２）を獲得し，ステップＳ５１７で，第２のＰＭＫ（すなわち，ＰＭＫ２），一例としては，ＭＳＫ２の除去により１６０ビットであるＰＭＫ２を生成する。」との記載からすると，

引用文献１には，

上記「ＭＳ」は“ＡＡＡサーバとユーザ認証を実行し，獲得したマスターセッションキーＭＳＫ２からペアワイズマスターキーＰＭＫ２を生成”することが記載されていると認められる。

（エ）上記Ｃの段落【００５３】の「ユーザ認証４６０を通じて，基地局４４０は，ＭＳＫ２から第２のＰＭＫ（すなわち，ＰＭＫ２）を生成し，ＰＭＫとＰＭＫ２とを使用して権限キー（Authorization Key；以下，‘ＡＫ’と称する）を生成する」との記載，段落【００５８】の「基地局は，ＰＭＫとＰＭＫ２をＡＫ生成関数に適用してＡＫを生成する。具体的には，基地局は，一例として，Dot16KDF関数にＰＭＫとＰＭＫ２とを適用する。」，段落【００６３】の「IEEE 802.16e通信システムにおいて，二重ＰＭＫを使用するEAP-in-EAP方式を使用して認証を遂行する場合に，第１のＥＡＰ認証で生成されたＰＭＫと，第２の認証で生成されたＰＭＫ２を使用して，ＡＫが生成される。」との記載からすると，引用文献１には，

上記「ＭＳ」は“ＰＭＫとＰＭＫ２とに基づいて，Ｄｏｔ１６ＫＤＦ関数により権限キーＡＫを生成”することが記載されていると認められる。

（オ）以上，（ア）～（エ）で検討した事項を踏まえると，引用文献１には，次の発明（以下，「引用発明１」という。）が記載されているものと認める。

「通信システムは，移動端末機ＭＳと，基地局及び認証サーバであるＡＡＡサーバとを含み，
　前記ＭＳは，前記ＡＡＡサーバと機器認証を実行し，獲得したマスターセッションキーＭＳＫからペアワイズマスターキーＰＭＫを生成し，
　前記ＭＳは，前記ＡＡＡサーバとユーザ認証を実行し，獲得したマスターセッションキーＭＳＫ２からペアワイズマスターキーＰＭＫ２を生成し，
　前記ＭＳは，前記ＰＭＫと前記ＰＭＫ２とに基づいて，Ｄｏｔ１６ＫＤＦ関数により権限キーＡＫを生成する通信システム。」

（２）引用文献２に記載されている技術的事項および引用発明２

　本願優先日前に頒布され，当審拒絶理由において引用された，国際公開第２００９／１４１９１９号（２００９年１１月２６日公開，以下，「引用文献２」という。）には，以下の技術的事項が記載されている。（当審注：下線は，参考のために当審で付与したものである。また，日本語訳は，引用文献の翻訳文である特表２０１１－５２３１０５号公報の記載を用いた。）

Ｄ．「[0078] After successful user authentication, device authentication and key establishment are performed as shown in Fig. 8.
[0079] In step S801, the remote ISIM server 204 verifies that the remote ISIM client 208 is trusted, and vice versa.
[0080] In step S802, the remote ISIM client 208 and the remote ISIM server 204 establishes an encryption key between them. After that, a secure transmission channel (e.g., a Transport Layer Security (TLS) session) is set up between them using the established key.
Therefore, according to the present embodiment, successful pairing results in establishment of a TLS session between the remote ISIM client 208 and the remote ISIM server 204.
[0081] According to the present embodiment, the remote ISIM client 208 and the remote ISIM server 204 perform the device authentication and key establishment based on a mechanism defined by 3GPP. Using this mechanism, a shared secret key (called Ks_local_device) is established between the remote ISIM client 208 and the remote ISIM server 204. Then, the remote ISIM client 208 and the remote ISIM server 204 establish the TLS session using the established Ks_local_device .」
（当審訳：「【００７８】
　ユーザ認証の成功後，デバイス認証及び鍵確立が，図８に示すように実行される。
【００７９】
　ステップＳ８０１で，リモートＩＳＩＭサーバ２０４は，リモートＩＳＩＭクライアント２０８が「信頼された」ものであることを検証する。その反対も行われる。
【００８０】
　ステップＳ８０２で，リモートＩＳＩＭクライアント２０８及びリモートＩＳＩＭサーバ２０４は，両者の間で暗号鍵を確立する。その後，確立された鍵を使用して，両者の間でセキュア伝送チャネル（例えば，トランスポート・レイヤ・セキュリティ（ＴＬＳ）セッション）がセットアップされる。それゆえ，本実施形態によれば，ペアリングの成功は，リモートＩＳＩＭクライアント２０８とリモートＩＳＩＭサーバ２０４との間のＴＬＳセッションの確立という結果をもたらす。
【００８１】
　本実施形態によれば，リモートＩＳＩＭクライアント２０８及びリモートＩＳＩＭサーバ２０４は，３ＧＰＰによって規定されるメカニズムに基づいて，デバイス認証及び鍵確立を行う。このメカニズムを使用すると，（Ks_local_deviceと呼ばれる）共有秘密鍵が，リモートＩＳＩＭクライアント２０８とリモートＩＳＩＭサーバ２０４との間で確立される。次いで，リモートＩＳＩＭクライアント２０８及びリモートＩＳＩＭサーバ２０４は，確立されたKs_local_deviceを使用してＴＬＳセッションを確立する。」）

ここで，上記引用文献２に記載されている事項を検討する。

（ア）上記Ｄの段落【００７８】の「ユーザ認証の成功後，デバイス認証及び鍵確立が，図８に示すように実行される。」，段落【００７９】の「リモートＩＳＩＭサーバ２０４は，リモートＩＳＩＭクライアント２０８が「信頼された」ものであることを検証する。その反対も行われる。」，段落【００８１】の「リモートＩＳＩＭクライアント２０８及びリモートＩＳＩＭサーバ２０４は，３ＧＰＰによって規定されるメカニズムに基づいて，デバイス認証及び鍵確立を行う。」旨の記載からすると，
引用文献２には，
“端末とサーバ間で，ユーザ認証の後にデバイス認証を実行”することが記載されていると認められる。

（イ）上記Ｄの段落【００８０】の「リモートＩＳＩＭクライアント２０８及びリモートＩＳＩＭサーバ２０４は，両者の間で暗号鍵を確立する。その後，確立された鍵を使用して，両者の間でセキュア伝送チャネル（例えば，トランスポート・レイヤ・セキュリティ（ＴＬＳ）セッション）がセットアップされる。」，段落【００８１】の「リモートＩＳＩＭクライアント２０８及びリモートＩＳＩＭサーバ２０４は，３ＧＰＰによって規定されるメカニズムに基づいて，デバイス認証及び鍵確立を行う。」旨の記載からすると，
引用文献２には，
“鍵を確立し，セキュアなセッションを確立”することが記載されていると認められる。

（ウ）以上，（ア）～（イ）で検討した事項を踏まえると，引用文献２には，次の発明（以下，「引用発明２」という。）が記載されているものと認める。

「端末とサーバ間で，ユーザ認証の後にデバイス認証を実行し，
鍵を確立し，セキュアなセッションを確立する方法。」

（３）引用文献３に記載されている技術的事項および引用発明３

本願優先日前に頒布され，当審拒絶理由において引用された，国際公開第２００９／１４８２６１号（２００９年１２月１０日公開，以下，「引用文献３」という。）には，以下の技術的事項が記載されている。（当審注：下線は，参考のために当審で付与したものである。また，日本語訳は，引用文献の翻訳文である特表２０１１－５２６０９７号公報の記載を用いた。）

Ｅ．「Encryption is applied to the MAC PDU payload requested by a selected ciphersuite. Generally, the mobile station and the base station need a key to perform encryption. Accordingly, in the IEEE 802.16 standard, a traffic encryption key (TEK) is defined. The TEK is generated as a random number by the base station. The base station can transfer an encrypted TEK to the mobile station through a corresponding TEK encryption algorithm.
・・・（中略）・・・
A data service flow through a broadband wireless access network has a series of quality of service (QoS) parameters, and encryption and decryption are performed through a traffic encryption key (TEK). The IEEE 802.16 standard which supports one of broadband wireless access systems defines a traffic encryption key (TEK) to protect a unicast data service.」（３頁２２行～４頁１５行）
（当審訳：「暗号化は，選択された暗号化スイートにより要請されるＭＡＣＰＤＵペイロードに適用される。移動局及び基地局で通常的に暗号化を行うにあってはキー（Ｋｅｙ）が必要とされ，このために，ＩＥＥＥ８０２．１６標準ではトラフィック暗号化キー（ＴＥＫ：Ｔｒａｆｆｉｃ Ｅｎｃｒｙｐｔｉｏｎ Ｋｅｙ）を定義する。ＴＥＫは基地局で乱数

（Ｒａｎｄｏｍ　Ｎｕｍｂｅｒ）として生成される。基地局は，対応するＴＥＫ暗号化アルゴリズムに基づいて暗号化されたＴＥＫを移動局に伝達することができる。
・・・（中略）・・・
　広帯域無線接続網を介したデータサービスの流れは、一連のサービス品質（ＱｏＳ：Ｑｕａｌｉｔｙ　ｏｆ　Ｓｅｒｖｉｃｅ）パラメータを有し、ＴＥＫを用いて暗号化及び複号化が行われる。広帯域無線接続システムのうちの一つを支援するＩＥＥＥ　８０２．１６標準は、ユニキャストデータサービスの保護のためにトラフィック暗号化キー（ＴＥＫ）を定義している。」）

Ｆ．「In one aspect of the present invention, a method of generating a traffic encryption key (TEK) comprises the steps of obtaining a key parameter during an authentication procedure with a base station; deriving the authentication key (AK) using the key parameter; receiving, by a mobile station from the base station, a first nonce and first security materials for deriving the traffic encryption key (TEK) ; and deriving the traffic encryption key (TEK) using one or more of the first nonce, the authentication key (AK) , and the first security materials.
…（中略）…
Also, the nonce is generated using a random number generator by the base station.
The key parameter includes one or more of a pre- authentication key (PAK) , a pair-wise master key (PMK) , and a pair-wise master key2 (PMK2) .」（７頁１４～２３行，８頁４～８行）
（当審訳：「本発明の一様態であって，トラフィック暗号化キー（ＴＥＫ）生成方法は，基地局との認証過程でキーパラメータを獲得する段階と，前記キーパラメータを用いて認証キー（ＡＫ）を生成する段階と，前記基地局から前記トラフィック暗号化キー（ＴＥＫ）を生成するための第１保安材料及び第１ノンスを受信する段階と，前記第１ノンス，前記ＡＫ及び前記第１保安材料のうち一つ以上を用いて前記ＴＥＫを生成する段階と，を含むことができる。
・・・（中略）・・・
　また，ノンス値は基地局で乱数生成器（Ｒａｎｄｏｍ　Ｎｕｍｂｅｒ　Ｇｅｎｅｒａｔｏｒ）を用いて任意に生成することができ，前記パラメータは，事前認証キー（ＰＡＫ），ペアワイズマスターキー（ＰＭＫ）及びペアワイズマスターキー２（ＰＭＫ２）のうち一つ以上を含むことができる。」）

Ｇ．「Table 1 illustrates a method of generating a TEK. [Table 1]

Referring to Table 1, the authentication key (AK) can be generated using one or more of PAK, PMK and PMK2. Also, the CMAC key and the HMAC key can be generated using MAC address of the mobile station and base station identifier (BS ID) . Moreover, the base station can generate a TEK using a random number and encrypt the TEK using a KEK.」（２０頁１１行～２１頁７行）
（当審訳：「下記の表１は，ＴＥＫを生成する方法を表す。

　表１を参照すると，認証キー（ＡＫ：Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｋｅｙ）は，ＰＡＫ，ＰＭＫ及びＰＭＫ２のうち一つ以上を用いて生成することができる。また，ＣＭＡＣキー及びＨＭＡＣキーは，ＡＫ，移動局のＭＡＣアドレス及び基地局識別子（ＢＳＩＤ）を用いて生成することができる。また，基地局は，乱数を用いてＴＥＫを生成し，ＫＥＫを用いてＴＥＫを暗号化することができる。」）

Ｈ．「The following Equation 1 represents an example of a method of generating a TEK, which can be used in the embodiments of the present invention.

[Equation 1]
(Old,New)TEK=Dot16KDF(AK,(Old,New)Nonce|SAID|TEK,128)
In the Equation 1, new TEK and old TEK represent TEKs generated during an initial network entry procedure of the mobile station or a location update procedure of the mobile station. At this time, the mobile station and the base station can use an AK, Nonce, and SAID when generating a TEK.
Referring to the Equation 1, in the embodiments of the present invention, the AK is used when the TEK is generated. This method is different from a general method of generating a TEK using a random number in a base station. The reason that an AK is used in generating a TEK is to allow the base station and the mobile station to flexibly and efficiently process a network operation such as handoff and support a unified method of generating and updating a TEK.」（２７頁１～２０行）
（当審訳：「下記の数学式１は，本発明の実施例で用いることができるＴＥＫ生成方法の一例を表す。
【数１】
(Old,New)TEK=Dot16KDF(AK,(Old,New)Nonce|SAID|TEK,128)
　数学式１で，新ＴＥＫ（Ｎｅｗ　ＴＥＫ），旧ＴＥＫ（Ｏｌｄ　ＴＥＫ）は，移動局の初期ネットワーク進入時に，位置更新時等に生成されるＴＥＫを表す。このＴＥＫ生成時に移動局及び基地局はＡＫ，ノンス及びＳＡＩＤを使用することができる。
　数学式１を参照すると，本発明の実施例では，ＴＥＫ生成にＡＫを用いる。これは，基地局が任意の乱数を用いてＴＥＫを生成することとは相違することである。ＴＥＫの生成にＡＫを使用することは，ハンドオフのようなネットワーク動作に柔軟で効率的に対処するためである。すなわち，一元化したＴＥＫ生成及び更新を支援するためである。」）

　ここで，上記引用文献３に記載されている事項を検討する。

（ア）上記Ｆの「基地局との認証過程でキーパラメータを獲得する段階」，「前記パラメータは，事前認証キー（ＰＡＫ），ペアワイズマスターキー（ＰＭＫ）及びペアワイズマスターキー２（ＰＭＫ２）のうち一つ以上を含むことができる。」旨の記載からすると，
　引用文献３には，
“移動局は，基地局との認証過程で，パラメータであるペアワイズマスターキーＰＭＫ及びＰＭＫ２を獲得”することが記載されていると認められる。

（イ）上記Ｆの「前記キーパラメータを用いて認証キー（ＡＫ）を生成する段階」，「前記パラメータは，事前認証キー（ＰＡＫ），ペアワイズマスターキー（ＰＭＫ）及びペアワイズマスターキー２（ＰＭＫ２）のうち一つ以上を含むことができる。」旨の記載，上記Ｇの「認証キー（ＡＫ：Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｋｅｙ）は，ＰＡＫ，ＰＭＫ及びＰＭＫ２のうち一つ以上を用いて生成することができる。」旨の記載，及び，表１の「AK=Dot16KDF(PMK(+)PMK2,SS MAC Address|BSID|AK,160)」との記載からすると，
　引用文献３には，
“ＰＭＫとＰＭＫ２とに基づいて，Ｄｏｔ１６ＫＤＦ関数により認証キーＡＫを生成”することが記載されていると認められる。

（ウ）上記Ｈの「このＴＥＫ生成時に移動局及び基地局はＡＫ，ノンス及びＳＡＩＤを使用することができる。」，「本発明の実施例では，ＴＥＫ生成にＡＫを用いる。」旨の記載，数学式１の「(Old,New)TEK=Dot16KDF(AK,(Old,New)Nonce|SAID|TEK,128)」との記載，及び，上記Ｅの「移動局及び基地局で通常的に暗号化を行うにあってはキー（Ｋｅｙ）が必要とされ，このために，ＩＥＥＥ　８０２．１６標準ではトラフィック暗号化キー（ＴＥＫ：Ｔｒａｆｆｉｃ　Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ）を定義する。」，「広帯域無線接続システムのうちの一つを支援するＩＥＥＥ８０２．１６標準は、ユニキャストデータサービスの保護のためにトラフィック暗号化キー（ＴＥＫ）を定義している。」旨の記載からすると，

引用文献３には，
“認証キーＡＫを用いて生成したトラフィック暗号化キーＴＥＫを使用して，移動局と基地局間のデータサービス通信を暗号化する”することが記載されていると認められる。

（エ）以上，（ア）～（ウ）で検討した事項を踏まえると，引用文献３には，次の発明（以下，「引用発明３」という。）が記載されているものと認める。

「移動局は，基地局との認証過程で，パラメータであるペアワイズマスターキーＰＭＫ及びＰＭＫ２を獲得し，
ＰＭＫとＰＭＫ２とに基づいて，Ｄｏｔ１６ＫＤＦ関数により認証キーＡＫを生成し，
認証キーＡＫを用いて生成したトラフィック暗号化キーＴＥＫを使用して，移動局と基地局間のデータサービス通信を暗号化する方法。」

４．対比

本願発明と引用発明１とを対比する。

（１）引用発明１の「移動端末機ＭＳ」は，ユーザ認証及び機器認証を実行する装置であるから，本願発明の「デバイス」に相当する。
引用発明１の「移動端末機ＭＳ」，「基地局」及び「ＡＡＡサーバ」は，ネットワーク上の装置であるから，本願発明の「ネットワークエンティティ」に相当する。
引用発明１の「ユーザ認証」，「機器認証」は，それぞれ本願発明の「加入者認証」，「デバイス認証」に相当することは明らかである。
引用発明１の「ＰＭＫ」は，機器認証（デバイス認証）により取得される鍵であるから，本願発明の「デバイス認証データ」に相当する。
引用発明１の「ＰＭＫ２」は，ユーザ認証（加入者認証）により取得される鍵であるから，本願発明の「第１の鍵」に相当する。
引用発明１の「ＡＫ」は，ユーザ認証（加入者認証）により取得された鍵，及び，機器認証（デバイス認証）により取得された鍵の両方の鍵から生成される鍵であるから本願発明の「セキュリティ鍵」に相当する。

（２）引用発明１の「前記ＭＳは，前記ＡＡＡサーバとユーザ認証を実行し，マスターセッションキーＭＳＫ２からペアワイズマスターキーＰＭＫ２を生成」することと，本願発明の「デバイスにおいて動作可能な方法であって」，「サブスクリプションを認証するための鍵に基づいてネットワークエンティティとの加入者認証を実行し，第１の鍵を取得するステップ」とを対比すると，上記（１）の検討結果からすると，後記する点で相違するものの，
“ネットワークエンティティとの加入者認証を実行し，第１の鍵を取得するステップ”である点で共通しているといえる。

（３）引用発明１の「前記ＭＳは，前記ＡＡＡサーバと機器認証を実行し，マスターセッションキーＭＳＫからペアワイズマスターキーＰＭＫを生成」することと，本願発明の「質問応答交換に基づいて前記ネットワークエンティティとの前記デバイスのデバイス認証を実行し，第２の鍵を含むデバイス認証データを取得するステップであって，前記第２の鍵は前記ネットワークエンティティから取得され，前記デバイス認証のための質問は暗号化された前記第２の鍵を含む，デバイス認証データを取得するステップ」とを対比すると，上記（１）の検討結果からすると，後記する点で相違するものの，
“前記ネットワークエンティティとの前記デバイスのデバイス認証を実行し，デバイス認証データを取得するステップ”である点で共通しているといえる。

（４）上記（１）において検討したとおり，引用発明１の「ＰＭＫ２」は本願発明の「第１の鍵」に相当し，引用発明１の「ＰＭＫ」は本願発明の「デバイス認証データ」に相当し，引用発明１の「ユーザ認証」，「機器認証」は，それぞれ本願発明の「加入者認証」，「デバイス認証」に相当するの

で，引用発明１において「ＰＭＫ２」（第１の鍵）と「ＰＭＫ」（デバイス認証データ）とに基づいて「ＡＫ」を生成することは，「ＰＭＫ２」を得るための「加入者認証」（ユーザ認証）と，「ＰＭＫ」を得るための「機器認証」（デバイス認証）とを“結び付ける”こと，すなわち，“バインド”することに他ならない。
　よって，引用発明１の「前記ＭＳは，前記ＰＭＫと前記ＰＭＫ２とに基づいて，Ｄｏｔ１６ＫＤＦ関数により権限キーＡＫを生成」することは，本願発明の「前記第１の鍵と前記デバイス認証データとに基づいて，前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成するステップ」に相当する。

（５）以上から，本願発明と引用発明１とは，以下の点で一致し，また，以下の点で相違する。

（一致点）

「デバイスにおいて動作可能な方法であって，
　ネットワークエンティティとの加入者認証を実行し，第１の鍵を取得するステップと，
　前記ネットワークエンティティとの前記デバイスのデバイス認証を実行し，デバイス認証データを取得するステップと，
　前記第１の鍵と前記デバイス認証データとに基づいて，前記加入者認証と前記デバイス認証とをバインドするセキュリティ鍵を生成するステップ
を含む，方法。」

（相違点１）
　本願発明では，「加入者認証」と「デバイス認証」の順序で実行されているのに対して，
　引用発明１では，「機器認証」（デバイス認証）と「ユーザ認証」（加入者認証）の順序で実行されている点。

（相違点２）
　本願発明では，「前記デバイスとサービングネットワークとの間の通信をセキュアにするために前記セキュリティ鍵を使用する」のに対して，
　引用発明１では，ＡＫを用いて通信をセキュアにする処理は特定されていない点。

（相違点３）
　「加入者認証」に関して，
　本願発明では，「サブスクリプションを認証するための鍵」に基づいて実行するのに対して，
　引用発明１では，「サブスクリプションを認証するための鍵」を用いる点は特定されていない点。

（相違点４）
　「デバイス認証データ」を取得する「デバイス認証」に関して，
　本願発明では，「質問応答交換」に基づいて実行し，その「質問」はネットワークエンティティから取得される「暗号化された第２の鍵」を含み，取得される「デバイス認証データ」は前記「第２の鍵」を含むのに対して，
　引用発明１では，そのような点は特定されていない点。

５．当審の判断

　上記相違点１～相違点４について検討する。

（１）相違点１について

　引用発明１は，装置間でユーザ認証及びデバイス認証の両方を実行するところ，

引用発明２のような，「端末とサーバ間で，ユーザ認証の後にデバイス認証を実行し，鍵を確立し，セキュアなセッションを確立する方法」は，本願優先日前に公知であった。
引用発明１と引用発明２とは，いずれも，認証技術の技術分野に属し，いずれもユーザ認証及びデバイス認証を実行する点で共通の機能を備える発明であるから，引用発明１に引用発明２を適用し，「ユーザ認証」及び「デバイス認証」の順序で実行すること，すなわち，相違点１に係る構成とすることは，当業者が容易に想到し得たことである。

（２）相違点２について
引用発明１は，ペアワイズマスターキーＰＭＫ及びＰＭＫ２とに基づいて，Ｄｏｔ１６ＫＤＦ関数により権限キーＡＫを生成するところ，
引用発明３のような「移動局は，基地局との認証過程で，パラメータであるペアワイズマスターキーＰＭＫ及びＰＭＫ２を獲得し，
ＰＭＫとＰＭＫ２とに基づいて，Ｄｏｔ１６ＫＤＦ関数により認証キーＡＫを生成し，
認証キーＡＫを用いて生成したトラフィック暗号化キーＴＥＫを使用して，移動局と基地局間のデータサービス通信を暗号化する方法」は，本願優先日前に公知であった。
引用発明１と引用発明３とは，いずれも，認証技術の技術分野に属し，いずれも認証時に生成された２つのペアワイズマスターキーに基づいてＤｏｔ１６ＫＤＦ関数で鍵ＡＫを生成する点で共通の機能を備える発明であるから，引用発明１に引用発明３を適用し，「ＡＫ」に基づいて生成した鍵で通信を暗号化することで，「ＡＫ」を用いてデータサービス通信をセキュアにすること，すなわち，相違点２に係る構成とすることは，当業者が容易に想到し得たことである。

（３）相違点３について
ユーザ認証において，加入者キー（subscriber key）を用いることは，認証技術の技術分野における常とう手段である。（必要であれば，例えば本願優先日前に頒布された特表２００５－５２９５６９号公報の段落【００３９】～【００４５】，図２を参照されたい。）
前記「加入者キー（subscriber key）」を用いたユーザ認証は，加入者（subscriber）のサブスクリプション（subscription）を認証するものであるから，前記「加入者キー（subscriber key）」は「サブスクリプションを認証するための鍵」といえる。
してみると，引用発明１において，ユーザ認証において「サブスクリプションを認証するための鍵」を用いること，すなわち，上記相違点３に係る構成とすることは，当業者が容易に想到し得たことである。

（４）相違点４について
装置間のデバイス認証において，片方で生成した乱数を暗号化して通信するチャレンジアンドレスポンス方式の認証を実行し，該乱数を鍵とすることは，認証技術の技術分野における常とう手段である。（必要であれば，例えば本願優先日前に頒布された特表２００５－５２９５６９号公報の段落【００３４】，【００５１】，【０１１３】～【０１１４】を参照されたい。）
してみると，引用発明１において，ネットワークエンティティ側から取得される暗号化された乱数（暗号化された第２の鍵）で「チャレンジアンドレスポンス」（質問応答交換）方式のデバイス認証を実行し，該乱数をデバイス認証で生成される鍵とすること，すなわち，上記相違点４に係る構成とすることは，当業者が容易に想到し得たことである。

（５）小括

上記で検討したごとく，上記相違点１～相違点４は格別のものではなく，そして，これらの相違点を総合的に勘案しても，本願発明の奏する作用効果は，上記引用発明１～引用発明４，前記常とう手段の奏する作用効果から予測される範囲内のものにすぎず，格別顕著なものということはできない。

６．むすび

以上のとおり，本願の請求項１に係る発明は，特許法第２９条第２項の規定により特許を受けることができないものであるから，その余の請求項に係る発明について検討するまでもなく，本願は拒絶すべきものである。

よって，結論のとおり審決する。

平成２８年　２月２４日

審判長　特許庁審判官　石井 茂和
特許庁審判官　戸島 弘詩
特許庁審判官　辻本 泰隆

（行政事件訴訟法第４６条に基づく教示）
この審決に対する訴えは、この審決の謄本の送達があった日から３０日（附加期間がある場合は、その日数を附加します。）以内に、特許庁長官を被告として、提起することができます。

〔審決分類〕Ｐ１８　．１２１－ＷＺ　（Ｈ０４Ｌ）

出訴期間として９０日を附加する。

審判長	特許庁審判官	石井　茂和	8837
	特許庁審判官	辻本　泰隆	8945
	特許庁審判官	戸島　弘詩	2957