

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3854148号

(P3854148)

(45) 発行日 平成18年12月6日(2006. 12. 6)

(24) 登録日 平成18年9月15日(2006. 9. 15)

(51) Int. Cl.		F I			
H04Q	7/34	(2006.01)	H04Q	7/04	C
G06F	21/20	(2006.01)	G06F	15/00	330B
H04L	9/32	(2006.01)	H04L	9/00	675B
H04Q	7/38	(2006.01)	H04B	7/26	109R

請求項の数 24 (全 13 頁)

(21) 出願番号	特願2001-534904 (P2001-534904)	(73) 特許権者	398012616
(86) (22) 出願日	平成11年11月3日 (1999. 11. 3)		ノキア コーポレイション
(65) 公表番号	特表2003-513572 (P2003-513572A)		フィンランド エフイーエンーO2150
(43) 公表日	平成15年4月8日 (2003. 4. 8)		エスプー ケイララーデンティエ 4
(86) 国際出願番号	PCT/EP1999/008422	(74) 代理人	100059959
(87) 国際公開番号	W02001/033883		弁理士 中村 稔
(87) 国際公開日	平成13年5月10日 (2001. 5. 10)	(74) 代理人	100067013
審査請求日	平成14年5月1日 (2002. 5. 1)		弁理士 大塚 文昭
		(74) 代理人	100082005
			弁理士 熊倉 禎男
		(74) 代理人	100065189
			弁理士 穴戸 嘉一
		(74) 代理人	100096194
			弁理士 竹内 英人

最終頁に続く

(54) 【発明の名称】 識別確認情報を選択する方法及び装置

(57) 【特許請求の範囲】

【請求項 1】

ユーザ認識を確認するのに使用される識別確認情報を選択するための方法であって、

a) 識別確認情報をレジスタから要求し、

b) 上記レジスタから得られた識別確認情報の形式に基づいて、上記レジスタから得られた上記識別確認情報を使用すべきか又はユーザデータベース(1)からの識別確認情報を使用すべきか判断し、そして

c) 上記判断段階の結果に応答して上記ユーザデータベースからの上記識別確認情報を検索する、

という段階を含み、上記識別確認情報は、セキュリティ及び／又は認証関連データより成ることを特徴とする方法。 10

【請求項 2】

上記レジスタはビジター位置レジスタ(21-23)であり、上記ユーザデータベースはホーム位置レジスタ(1)であり、そして上記選択は、位置更新手順の間に行われる請求項 1 に記載の方法。

【請求項 3】

上記識別確認情報は、公開キー暗号に使用される暗号情報である請求項 1 に記載の方法。

【請求項 4】

上記識別確認情報の形式は、ネゴシエーション結果に基づいて決定される請求項 1 又は 20

2に記載の方法。

【請求項 5】

上記ネゴシエーションは、MAPバージョンネゴシエーションである請求項4に記載の方法。

【請求項 6】

上記識別確認情報は、上記ネゴシエーションが、識別確認情報をサポートしないMAPバージョンの使用を導く場合に、上記ユーザデータベースから検索される請求項5に記載の方法。

【請求項 7】

ユーザ装置のSIM形式を指示するパラメータが上記識別確認情報に追加され、そして
上記判断段階は、このパラメータに基づいて実行される請求項 1 ないし 6 のいずれかに記載の方法。 10

【請求項 8】

上記SIM形式パラメータが、上記ユーザ装置にUSIMが与えられることを指示する場合に、UMTS認証ベクトルが認証に使用される請求項7に記載の方法。

【請求項 9】

上記SIM形式パラメータは、上記レジスタから受け取ったMAP SEND IDENTIFICATION応答メッセージに含まれる請求項 7 又は 8 に記載の方法。

【請求項 10】

上記SIM形式パラメータは、上記ユーザデータベースから受け取ったMAP SEND AUTHENTICATION INFO応答メッセージに含まれる請求項 7 ないし 9 のいずれかに記載の方法。 20

【請求項 11】

上記SIM形式パラメータは、要求されたMAPバージョンが上記レジスタ及び上記ユーザデータベースに向かってサポートされない場合に、不定値にセットされる請求項 7 ないし 10 のいずれかに記載の方法。

【請求項 12】

ユーザ認識を確認するのに使用される識別確認情報を選択するための方法であって、

a) 識別確認情報をレジスタから要求し、

b) 上記レジスタから得られた識別確認情報の形式に基づいて、上記レジスタから得られた上記識別確認情報を使用すべきか又はユーザデータベース(1)からの識別確認情報を使用すべきか判断し、そして 30

c) 上記判断段階の結果に応答して上記ユーザデータベースからの上記識別確認情報を検索する、

という段階を含み、上記識別確認情報は、公開キー暗号に使用される暗号情報であることを特徴とする方法。

【請求項 13】

ユーザ認識を確認するのに使用される識別確認情報を選択するための方法であって、

a) 識別確認情報をレジスタから要求し、

b) 上記レジスタから得られた識別確認情報の形式に基づいて、上記レジスタから得られた上記識別確認情報を使用すべきか又はユーザデータベース(1)からの識別確認情報を使用すべきか判断し、そして 40

c) 上記判断段階の結果に応答して上記ユーザデータベースからの上記識別確認情報を検索する、

という段階を含み、ユーザ装置のSIM形式を指示するパラメータが上記識別確認情報に追加され、そして上記判断段階は、このパラメータに基づいて実行されることを特徴とする方法。

【請求項 14】

ユーザ認識を確認するのに使用される識別確認情報の選択を実行する装置であって、

a) レジスタとの通信を実行するための通信手段(203)と、 50

b) 上記レジスタから受信した識別確認情報の形式に基づいて、ユーザ装置の上記識別確認情報のソースについて判断するための判断手段(205)と、

c) 上記判断手段(205)の判断結果に基づき、上記レジスタ又はユーザデータベース(1)のいずれかから上記識別確認情報を検索するための検索手段(203)と、
を備え、識別確認情報の上記形式は、上記レジスタとのネゴシエーションに基づいて決定されることを特徴とする装置。

【請求項 15】

該装置は、レジター位置レジスタ(21-23)である請求項 14 に記載の装置。

【請求項 16】

上記レジスタは、レジター位置レジスタ(21-23)であり、そして上記ユーザデータベースは、ホーム位置レジスタ(1)である請求項 14 に記載の装置。

【請求項 17】

上記ネゴシエーションは、MAPバージョンネゴシエーションである請求項 14 に記載の装置。

【請求項 18】

上記判断手段(205)は、上記ネゴシエーションの結果が、識別確認情報をサポートしないMAPバージョンである場合に、上記ユーザデータベース(4)を上記識別確認情報のソースとして判断するよう構成された請求項 17 に記載の装置。

【請求項 19】

上記識別確認情報からSIM形式指示情報を抽出するための抽出手段(204)を更に備え、上記判断手段(205)は、上記SIM形式指示情報に基づいて判断を行うように構成された請求項 14 ないし 18 のいずれかに記載の装置。

【請求項 20】

上記判断手段(205)は、要求されたMAPバージョンが上記レジスタ及び上記ユーザデータベース(1)に向かってサポートされない場合に上記SIM形式指示情報を不定値にセットするように構成された請求項 19 に記載の装置。

【請求項 21】

上記判断手段(205)は、上記抽出されたSIM形式の指示情報が不定である場合には、上記ユーザデータベース(4)から検索された識別確認情報に基づいて上記SIM形式指示情報をセットするように構成される請求項 19 又は 20 に記載の装置。

【請求項 22】

ユーザ認識を確認するのに使用される識別確認情報の選択を実行する装置であって、

a) レジスタとの通信を実行するための通信手段(203)と、

b) 上記レジスタから受信した識別確認情報の形式に基づいて、ユーザ装置の上記識別確認情報のソースについて判断するための判断手段(205)と、

c) 上記判断手段(205)の判断結果に基づき、上記レジスタ又はユーザデータベース(1)のいずれかから上記識別確認情報を検索するための検索手段(203)と、

を備え、上記識別確認情報からSIM形式指示情報を抽出するための抽出手段(204)を更に備え、上記判断手段(205)は、上記SIM形式指示情報に基づいて判断を行うように構成されたことを特徴とする装置。

【請求項 23】

上記判断手段(205)は、要求されたMAPバージョンが上記レジスタ及び上記ユーザデータベース(1)に向かってサポートされない場合に上記SIM形式指示情報を不定値にセットするように構成された請求項 22 に記載の装置。

【請求項 24】

上記判断手段(205)は、上記抽出されたSIM形式の指示情報が不定である場合には、上記ユーザデータベース(4)から検索された識別確認情報に基づいて上記SIM形式指示情報をセットするように構成される請求項 22 又は 23 に記載の装置。

【発明の詳細な説明】

【0001】

10

20

30

40

50

【技術分野】

本発明は、少なくとも2つのソース間で識別確認情報を選択する方法及び装置に係る。本発明は、例えば、UMTS（ユニバーサル移動テレコミュニケーションシステム）ネットワークのようなセルラーネットワークの古い位置エリアから新しい位置エリアに入るユーザ装置の位置更新手順であって、ビジター位置レジスタ及びホーム位置レジスタ間で認証又はセキュリティパラメータの選択が行われる位置更新手順に適用することができる。

【0002】**【背景技術】**

加入者が移動ネットワーク内をローミングする間に、移動ターミナルは、位置更新手順を使用することによりその位置を更新する。この手順は、無線アクセスネットワークにより専用のシステム情報としてブロードキャスト又は送信される現在位置エリア識別子が増加するときに開始される。このプロセスでは、例えば、エアインターフェイスにおいてセキュリティ、認証又は暗号化手順を可能にするために使用される認証又はセキュリティパラメータが、新たな接続岐路についても必要とされる。

10

【0003】

位置エリアが増加するときには、それにサービスするビジター位置レジスタ（VLR）も増加する。このような状態では、新たなVLRが、セキュリティ又は認証パラメータ及び国際移動加入者認識（IMSI）のような識別確認情報を、以前の即ち古いVLRから受信する。次いで、移動ターミナルに割り当てられた古い「一時的移動加入者認識（TM-SI）」とIMSIとの間の関係が古いVLRにおいて失われる。更に、位置更新手順の一部として、HLRは、適切なコール取り扱いのために新たなVLRを知る必要のある加入者パラメータを送信する。

20

【0004】

より詳細には、移動ターミナルの位置及び加入者の管理に関連したデータが、HLRとVLRとの間で交換される。移動加入者に提供される主たるサービスは、全サービスエリア内でコールを設定するか又は受信する能力である。これをサポートするために、位置レジスタは、データを交換しなければならない。HLRは、移動加入者へのサービスをサポートするのに必要な全てのデータをVLRへ送信する。次いで、HLRは、その加入者の位置登録を打ち消すように以前のVLRに命令する。データの交換は、移動加入者が特定のサービスを受け取るとき、移動加入者が自分の契約に付随するあるデータを変更したいとき、又は契約のあるパラメータが管理手段により変更されるときに行われる。従って、HLRは、移動加入者の管理を担当するデータベースである。

30

【0005】

移動ネットワークは、加入者の数、装置の容量及びネットワークの編成に基づいて1つ又は多数のHLRを含む。HLRには、2種類の情報が記憶され、即ち加入者情報と、移動ターミナルが位置するところの移動交換センター（MSC）に向かうコールのルーティング及び課金を可能にするある位置情報とである。各移動契約には2つの形式の番号が付随されてHLRに記憶され、それらは、IMSIと、1つ以上の移動ステーション国際ISDN番号（MSISDN）である。IMSI又はMSISDNは、移動契約に対しデータベース内の情報にアクセスするためのキーとして使用されてもよい。

40

【0006】

VLRは、IMSI、MSISDN、進行中のコールをもつ移動ターミナルのための移動ステーションローミング番号、もし適用できればTM-SI、もし使用されればローカル移動ステーション認識、及び移動ステーションが登録されそしてステーションをコールするのに使用される位置エリアを含むデータベースを備えている。上記情報は、GSM仕様書03.12に記載された手順によりVLRとHLRとの間に通される。加入者データの編成は、GSM仕様書03.08に要約されている。

更に、認証センター（AuC）が、HLRに組み合わされ、関連HLRに登録された各移動加入者の認識を記憶する。このキーは、IMSIを認証するのに使用されるデータを発生するのに使用され、そして移動ターミナルと移動ネットワークとの間の無線経路に沿っ

50

た通信を暗号化するのに使用されるキーである。認証及び暗号化に使用される手順は、GSM仕様書03.20に記載されている。

【0007】

第3世代のUMTSネットワークの開発は、新規な形式の加入者認識モジュール（SIM）がUMTS加入者認識モジュール（USIM）として導入され、そして新たなセキュリティパラメータがそれに関連されるようなリリース99GSM/UMTSシステムを導出した。GSM SIMに関連したセキュリティ機能は、GSM認証ベクトル（AVs）、即ちGSMトリプレットを使用する。UMTS USIMに関連した新たなセキュリティ機能は、UMTSネットワークに必要とされる付加的な認証パラメータより成るUMTSクイントプレットで構成されるUMTS AVsを使用する。

10

しかしながら、USIM移動ターミナルが非UMTSケーパブルGSM MSC/VLR（リリース98MSC/VLR）からUMTSケーパブルGSM MSC/VLR（リリース99MSC/VLR）へローミングするときには、次の理由で問題が発生する。

【0008】

最初に、リリース98MSC/VLRは、加入者データと、加入者のためのセキュリティパラメータとを含む。加入者の移動のために、次の筋書きが実行される。UEは、位置エリアの変化に気付く、そして「L3-MM LOCATION UPDATE REQUEST（位置更新要求）」メッセージを移動ネットワークに送信することにより位置更新手順を開始する。新たなMSC/VLRは、UEが到来するところの古い位置エリアが別のMSC/VLRにより制御されることを識別する。これは、MAP（移動アプリケーションパート）バージョン3ネゴシエーションを古いMSC/VLRに向かって開始し、そして古いリリース98MSC/VLRはMAPバージョン2しかサポートしないので、MAPバージョン2への後退が行われる。新たなMSC/VLRは、古い位置エリア識別子及びTMSIを古いMSC/VLRへ送信して、IMSI及び認証パラメータを検索する。これに回答して、古いリリース98MSC/VLRは、加入者のIMSI及びGSMトリプレット（GSM AVs）を返送する。ここで、新たなリリース99MSC/VLRは、加入者が移動ターミナルにUSIMを有するかどうかそしてUMTS AVsを使用しなければならないかどうかを知らないので、問題が発生する。

20

【0009】

新規なMAPバージョン3のオペレーションにおいては、VLR間に使用される「SEND IDENTIFICATION（識別送信）」メッセージと、VLRとHLRとの間に使用される「SEND AUTHENTICATION INFO（認証情報送信）」メッセージが、UMTS AVsの送信をサポートするためにリリース99GSM-UMTSに既に規定されている。しかしながら、その仕様においてそれらが使用される仕方は、上記問題に対処するものではない。

30

更に、UMTSとGSMネットワークとの間のシステム間オペレーションを達成するためのメカニズムが、GSMユーザ（SIM）に対する両ネットワーク間の機密相互オペレーションを許すために示唆されている。この示唆されたメカニズムによれば、MSC/VLRは、標準的な変換機能により、受信したGSM認証ベクトルからUMTS認証ベクトルを導出し、UMTSセキュリティパラメータをUMTS無線アクセスネットワークに与えることができる。移動ターミナル側では、移動ターミナルがUMTS無線アクセスネットワークに位置するときに、UEは、標準的な変換機能によりGSM認証パラメータからUMTS認証パラメータを導出する。

40

しかしながら、この場合にも、新たなMSC/VLRが、移動ターミナルに設けられたSIM形式を知らない場合に上記の問題が発生する。

【0010】

【発明の開示】

本発明の目的は、セキュリティを改善することのできる識別確認情報を選択するための方法及び装置を提供することである。

この目的は、ユーザ認識を確認するのに使用される識別確認情報を選択するための方法で

50

あって、識別確認情報をレジスタから要求し、上記レジスタから得られた識別確認情報の形式に基づいて、上記レジスタから得られた上記識別確認情報を使用すべきか又はユーザデータベースからの識別確認情報を使用すべきか判断し、そして上記判断段階の結果に回答して上記ユーザデータベースからの上記識別確認情報を検索するという段階を含む方法によって達成される。

【0011】

更に、上記目的は、ユーザ認識を確認するのに使用される識別確認情報の選択を実行する装置であって、レジスタとの通信を実行するための通信手段と、上記レジスタから受信した識別確認情報の形式に基づいて、ユーザ装置の上記識別確認情報のソースについて判断するための判断手段と、上記判断手段の判断結果に基づき、上記レジスタ又はユーザデータベースのいずれかから上記識別確認情報を検索するための検索手段とを備えた装置によって達成される。

10

従って、レジスタとの通信が、所望の識別確認情報の送信がサポートされないという結果を招き、例えば、その識別確認情報又は異なる形式の識別確認情報をサポートしないプロトコルバージョンへの後退が決定されたときには、識別確認情報がユーザデータベースから検索され、これにより、所望の識別確認情報が使用されるよう保証する。

【0012】

識別確認情報の形式は、ネゴシエーション結果に基づいて決定することができ、ネゴシエーションは、MAPバージョンネゴシエーションである。この場合、判断手段は、ネゴシエーションの結果が、識別確認情報をサポートしないMAPバージョンである場合に、ユーザデータベースを識別確認情報のソースとして判断するように構成される。

20

更に、装置及び／又はレジスタは、ビジター位置レジスタであり、そしてユーザデータベースは、ホーム位置レジスタであり、選択は、位置更新手順の間に行われる。

識別確認情報は、セキュリティ及び／又は認証関連データ、例えば、認証ベクトルを含む。

【0013】

好ましくは、識別確認情報は、ユーザ装置のSIM形式を指示するパラメータを含み、上記判断段階は、このパラメータに基づいて行われる。従って、識別確認情報からSIM形式指示情報を抽出するための抽出手段が設けられ、上記判断手段は、このSIM形式指示情報に基づいて判断を行うように構成される。この場合に、上記SIM形式パラメータが、ユーザ装置にUSIMが設けられていることを指示する場合には、UMTS認証ベクトルが認証に使用される。より詳細には、古い位置レジスタから受け取られたMAP SEND IDENTIFICATION（識別送信）応答メッセージにSIM形式のパラメータが含まれる。更に、ユーザデータベースから受け取られたMAP SEND AUTHENTICATION INFO（認証情報送信）応答メッセージにもSIM形式のパラメータが含まれる。SIM形式のパラメータは、要求されたMAPバージョンネゴシエーションがユーザデータベースに向かってサポートされない場合には、不定値にセットされる。

30

【0014】

従って、位置レジスタ又はユーザデータベースは、IMSIにより識別されるユーザ装置に関連した識別確認情報の形式を装置に明確に指示することができる。従って、売主が能力のサブセットしか実施しない場合でも、SIM形式の指示を得ることができ、SIM形式は、少なくとも未知であるとして指示され、新たな位置レジスタは、それに対応する識別確認情報をユーザデータベースから要求することができる。

40

或いは又、ユーザ装置のクラスマーク情報を判断段階に使用して、ユーザ装置のSIM形式を指示することもできる。

判断手段は、抽出されたSIM形式指示情報が不定である場合には、ユーザデータベースから受け取られた識別確認情報に基づいてSIM形式指示情報をセットし、或いは要求されたMAPバージョンがユーザデータベースに向かってサポートされない場合には、SIM形式指示情報を不定値にセットするように構成される。

50

【0015】

【発明を実施するための最良の形態】

以下、添付図面を参照して、本発明の好ましい実施形態を詳細に説明する。

異なる能力、即ちリリースバージョンをもつ異なる種類のレジスタを備えた移動ネットワークの位置エリアをローミングするUSIMに基づいて好ましい実施形態を以下に説明する。

最初に、本発明の好ましい実施形態による位置更新手順を、対応するフローチャートである図1を参照して説明する。ここに述べる位置更新手順は、レジスタ、汎用パケット無線サービス(GPRS)ネットワークのサービングGPRSサポートノード(SGSN)、又はネットワークのスイッチング要素により使用される他のレジスタにおいて実行されて、そのエリアに現在位置するローミング中のユーザ装置への又はそこからのコールを取り扱うための情報を検索することができる。

10

【0016】

この手順は、ステップS101において、各位置エリアをローミング中のユーザ装置から位置更新要求が受け取られたときにスタートする。位置更新要求が受け取られた場合には、バージョンのネゴシエーション、例えば、MAPバージョンネゴシエーションが、位置更新要求メッセージに指示された古いVLRで実行される(ステップS102)。次いで、識別確認情報、例えばセキュリティ及び／又は認証パラメータの要求が古いVLRへ発生される(ステップS103)。

【0017】

20

その後、通信に使用されるMAPバージョンがステップS104においてチェックされる。要求されたMAPバージョン、例えば、完全な識別確認情報を送信するのに必要なMAPバージョン3が、古いVLRによりサポートされる場合には、SIM形式指示パラメータが、受信された識別確認情報から抽出される(ステップS105)。次いで、SIM形式指示パラメータにより指示されたSIM形式がステップS106においてチェックされる。GSM SIMが指示された場合には、手順がステップS107へ分岐し、そこで、受信器のGSM認証ベクトルが新たなVLRにより認証に使用される。ステップS106で決定されたSIM形式がUMTS USIMを指示する場合には、手順がステップS111へ分岐し、そこで、受信された識別確認情報(例えば、セキュリティ又は認証パラメータ)の形式がチェックされる。受信されたパラメータがUMTS形式(例えば、UMTS クイントプレット)である場合には、受信されたUMTS 認証ベクトル又はパラメータが新たなVLRにおいて認証に使用される(S112)。さもなければ、受信されたパラメータがGSM形式(例えば、GSMトリプレット)の場合には、ユーザ装置のクラスマーク情報がステップS113においてチェックされる。クラスマークが、ユーザ装置がGSM形式であることを指示する場合には、受信されたGSMパラメータが使用される(S116)。さもなければ、クラスマークが、ユーザ装置がより高い形式であることを指示する場合には、新たな認証情報(認証ベクトル)に対する要求がHLRへ発生される(S114)。次いで、HLRから受信された新たな認証ベクトルが認証に使用される(S115)。これにより、SIM形式指示パラメータにより「USIM」が指示されるが新たな認証ベクトルをHLRから検索しなければならないケースがカバーされる。このようなケースの一例として、古いVLRそれ自体が、「USIM」にセットされたSIM形式指示パラメータを受信してもよいし、受信したUMTS 認証ベクトル全部を使用してもよいし、新たなGSM認証ベクトルしか受信できないようにされてもよい。というのは、HLRに向かうMAPバージョン2しかサポートしないからである。従って、新たなVLRが、再び、HLRから新たな認証ベクトルを要求する。

30

40

【0018】

SIM形式指示パラメータが不定値、例えば、「未知」にセットされた場合には、手順がステップS108に分岐し、そこで、新たな認証情報の要求がHLRへ発生される。次いで、新たなVLRに使用されるSIM形式指示パラメータは、HLRから受信された新たな識別確認情報(認証ベクトル)に基づいてセットされる(ステップS109)。次いで

50

、H L Rから受信された認証ベクトルが、ステップS 1 1 0において、新たな位置エリアに入るユーザ装置を認証するために使用される。

【0019】

ステップS 1 0 4において、要求されたM A Pバージョン3が古いV L Rによりサポートされないと決定された場合には、手順がステップS 1 1 7へ分岐し、そこで、H L Rに向かって新たなV L RによりサポートされるM A Pバージョンがチェックされる。全識別確認情報（例えば、U M T S A V s）を送信するには充分でないM A Pバージョン、即ちM A Pバージョン2がサポートされる場合には、手順がステップS 1 2 0へ分岐し、そこで、新たなV L Rに使用されるS I M形式指示パラメータが不定値（「未知」）にセットされる。一方、M A Pバージョン3がH L Rに向かってサポートされる場合には、手順が
10
ステップS 1 1 8へ分岐し、そこで、新たな識別確認情報（認証ベクトル）がH L Rから要求される。次いで、S I M形式指示パラメータが、ステップS 1 1 9において、識別確認情報（認証ベクトル）の受信形式に基づいてセットされる。

【0020】

従って、本発明の好ましい実施形態によれば、V L R間で不十分なM A Pバージョンへの後退がなされたときに、リリース99 M S C/V L Rが、H L R/A u Cからセキュリティ又は認証ベクトルを検索し、正しい認証パラメータが使用されるように保証する。

しかしながら、売主は、通常、リリース98及びリリース99 V L Rを厳密に実施せず、即ち特定のV L Rは、リリース99 M A Pオペレーションのサブセットしか実施しない。

従って、あるV L Rは、M A P S E N D I D E N T I F I C A T I O NメッセージのM A Pバージョン3を実施するが、M A P S E N D A U T H E N T I F I C A T I O N I N F OメッセージのM A Pバージョン2しか実施しない状態が生じ得る。それ故、S I M形式指示パラメータが与えられて、3つの異なる値、即ち「S I M」、「U S I M」又は「未知」にセットすることができる。新たなS I M形式指示パラメータは、M A P S E N D I D E N T I F I C A T I O N応答メッセージに組み込むことができ、そして任意であるが、M A P S E N D A U T H E N T I F I C A T I O N I N F Oメッセージにも組み込むことができる。従って、V L R及び任意であるがH L Rは、新たな位置エリアに入るユーザ装置の所与のI M S Iに関連したS I Mの形式を新たなV L Rに指示することができる。
20

【0021】

或いは又、新たなV L Rは、H L Rから明確な指示を受け取らずに、H L Rから受信したセキュリティ又は認証パラメータ又は加入者データの形式に基づいてこのパラメータをセットしてもよい。これにより、新たなV L Rにおいてユーザ装置に対し正しい識別確認情報が使用されることが保証される。

以下、図2に示すブロック図及び図3に示す対応するメッセージ流れ図を参照して、異なる種類のV L RをローミングしているU S I Mを示す例示的筋書きを説明する。

【0022】

図2を参照すれば、移動ネットワークは、各M S C/V L R A、B及びC 21ないし23に接続されたH L R（又はH L R/A u C）1を備え、ここで、V L Rは、関連M S Cにより制御されるエリアをローミング中の移動加入者（U E）に対する位置及び管理の
40
データベースである。M S Cは、そのエリアに現在位置する所与のU E 4に関連したデータを必要とするときに、それに対応するV L Rに質問する。U E 4が、M S C/V L R A、B及びC 21ないし23の1つとの位置更新手順を開始すると、それに対応するM S Cが当該情報を記憶するV L Rに通知する。この手順は、U E 4が、M S C/V L R A、B及びC 21ないし23の各1つによってサービスされる位置エリアA、B及びCの別の1つにローミングするとき生じる。U E 4とM S C/V L R A、B及びC 21ないし23との間の通信は、位置エリアA、B及びCの各1つにおいてU E 4に無線接続された各無線アクセスネットワーク（R A N）A、B及びC 31ないし33を経て実行される。R A N A、B及びC 31ないし33は、ベースステーションサブシステム、U M T S無線アクセスネットワーク等より成る。
30
50

【0023】

図2に示すように、MSC/VLR A 21は、HLR1及びMSC/VLR B 22に向かうMAPバージョン2をサポートする。更に、MSC/VLR B 22は、HLR1に向かうMAPバージョン2、及びMSC/VLR A 21に向かうMAPバージョン3をサポートする。最終的に、MSC/VLR C 23は、HLR1及びMSC/VLR B 22に向かうMAPバージョン3をサポートする。従って、MSC/VLR A 21は、非UMTSケーパブルMSC/VLR（リリース98 GSM MSC/VLR）であり、MSC/VLR B 22は、ハイブリッドMSC/VLRであり、そしてMSC/VLR C 23は、UMTSケーパブルMSC/VLR（リリース99 MSC/VLR）である。

10

【0024】

以下、UE4が位置エリアAから位置エリアBへローミングし、そしてその後に、位置エリアCへローミングするケースについて、図3を参照して説明する。

UE4が位置エリアAにおいてアクチベートされると仮定すれば、IMSIアタッチ手順がUE4によりそのアクチベーションの際にMSC/VLR A 21に向かって実行される。それに応答して、MSC/VLR A 21は、UE4のIMSIをHLR1に送信し、そしてGSM認証ベクトル（トリプレット）をHLR1から受信する。MSC/VLR A 21は、リリース98 MSC/VLRであるから、GSM認証ベクトルしかMSC/VLR A 21に送信されないことに注意されたい。

【0025】

20

UE4が位置エリアAを出て位置エリアBに入ると、各TMSIを含む位置更新要求をハイブリッドMSC/VLR B 22へ発生する。これに応答して、MSC/VLR B 22は、MSC/VLR A 21とのMAPバージョンネゴシエーションを実行し、これは、MAPバージョン2の確立を招く。次いで、MSC/VLR B 22は、MSC/VLR A 21から識別確認情報を要求し、そしてGSM認証ベクトル及びUE4のIMSIを受信する。MAPバージョンネゴシエーションはMAPバージョン2を導くので、MSC/VLR B 22は、HLR1から新たなセキュリティ又は認証パラメータを要求する。しかしながら、ここに示すケースでは、これは任意のものである。というのは、MSC/VLR B 22は、要求を開始するアプリケーションが、MAPバージョン2しかHLR1に向かってサポートされないのを知っている場合に、HLR1からパラメータを要求しないと判断するからである。

30

【0026】

パラメータ要求に応答して、HLR1は、GSM認証ベクトルをMSC/VLR B 22へ送信する。以前のMSC/VLR B 22は、MAPバージョン2をMSC/VLR A 21及びHLR1に向かって使用していた。従って、SIM指示パラメータを「未知」にセットする。というのは、UE4に与えられるSIM形式を知らないからである。

UE4は、位置エリアBを出て位置エリアCに入るときに、古いMSC/VLR B 22のTMSIより成る位置更新要求を新たなMSC/VLR C 23へ送信する。次いで、MSC/VLR C 23は、MSC/VLR B 22に向かってMAPバージョンネゴシエーションをスタートし、これは、MAPバージョン3の確立を招き、そしてMSC/VLR B 22から加入者IMSI及びセキュリティ認証パラメータを求める。これに応答して、IMSI及びセキュリティ認証パラメータは、SIM形式指示パラメータと共に、新たなMSC/VLR C 23へ送信される。MSC/VLR C 23は、SIM形式指示パラメータに基づき、UE4のSIM形式が未知であり即ち不定であることに気付くので、HLR1へ発生された対応要求により、要求されたUMTS認証ベクトルを検索する。HLR1からUMTS認証ベクトルを受信すると、MSC/VLR C 23は、UE4の加入者に関連したSIM形式指示パラメータを「USIM」にセットする。従って、UMTS MSC/VLR C 23に正しい認証ベクトルが使用される。

40

50

【0027】

図4は、上記の位置更新手順を実行するための装置、例えば、VLRユニット、GSGN等の基本的なブロック図である。図4によれば、HLR1、又は装置が割り当てられた各MSCとの間で情報及びメッセージを送信／受信するためにトランシーバユニット（TRX）201が設けられる。更に、シグナリング制御ユニット203が設けられ、これは、HLR1又は割り当てられたMSCで実行されるシグナリングを制御して、加入者データメモリ202と必要なデータ交換を行い、このデータメモリには、例えば、そのエリアに現在位置するローミング中の移動ステーションとの間のコールを取り扱うための加入者情報が記憶される。更に、シグナリング制御ユニット203は、割り当てられたMSCを経て他の対応装置との各バージョンネゴシエーション（例えば、MAPバージョンネゴシエーション）を実行するように構成される。

10

【0028】

好ましい実施形態によれば、位置更新手順の間にシグナリング制御ユニット203から供給される識別確認情報からSIM形式パラメータを抽出するためのSIM形式抽出器204が設けられる。更に、検索判断ユニット205が設けられ、これには、確立されたMAPバージョンを指示する情報がシグナリング制御ユニット203から供給されると共に、SIM形式抽出器204により抽出されたSIM形式パラメータが供給される。MAPバージョン及びSIM形式パラメータに基づき、検索判断ユニット105は、図1に示すフローチャートに基づいて説明したように、HLR1から新たな識別確認情報（セキュリティ又は認証パラメータ）を要求するようにシグナリング制御ユニット203を制御する。

20

【0029】

識別確認情報の選択は、必ずしも、位置レジスタで実行されたネゴシエーションの結果に基づかなくてもよい。受信した識別確認情報の形式は、情報のフォーマット又は構造、例えば、トリプレット、クイントレット又は他の種類のベクトルに基づいて決定されてもよい。更に、識別確認情報のソースとしてユーザデータベースを選択するのを判断するのに必要なユーザ装置の種類又はバージョンを識別するために、クラスマーク情報を直接使用してもよい。

図2及び4の基本的ブロック図は、本発明に必要とされる機能を遂行するのに重要な要素しか示していないことに注意されたい。図示されたネットワークエンティティの他の要素は、簡単化のために省略されている。更に、図4に示す各ブロックの機能は、各装置に配置された処理ユニット（例えば、CPU）を制御する制御プログラムの対応サブルーチンによって実行されてもよいことに注意されたい。

30

【0030】

本発明は、検索されるべきいかなる種類のセキュリティ関連情報にも適用できる。例えば、本発明は、PGP公開キー暗号化方法においてメッセージを暗号化又は暗号解読するのに使用される暗号化パラメータの選択にも使用でき、この場合、レジスタは、受信器又は送信器関連データを記憶するデータベースである。

更に、本発明は、GSM/UMTSネットワークにおいて認証パラメータを与えることに限定されないことを指摘しておく。異なるリリースバージョン又は能力を有する各ネットワークエンティティに識別確認情報を使用して、所望の識別確認情報の使用を保証するようないかなるテレコミュニケーションネットワークにも適用できる。従って、好ましい実施形態の上記説明及び添付図面は、本発明を単に例示するものに過ぎない。本発明の好ましい実施形態は、特許請求の範囲内で種々変更し得るものである。

40

【図面の簡単な説明】

【図1】 本発明の好ましい実施形態による位置更新手順のフローチャートである。

【図2】 異なる位置更新能力をもつビジター位置レジスタを備えた移動ネットワークの主たるブロック図である。

【図3】 図2の移動ネットワークにおいて位置更新手順に関連したメッセージ送信図である。

【図4】 本発明の好ましい実施形態により位置更新を遂行するための装置を示す基本的

50

ブロック図である。

【図 1】

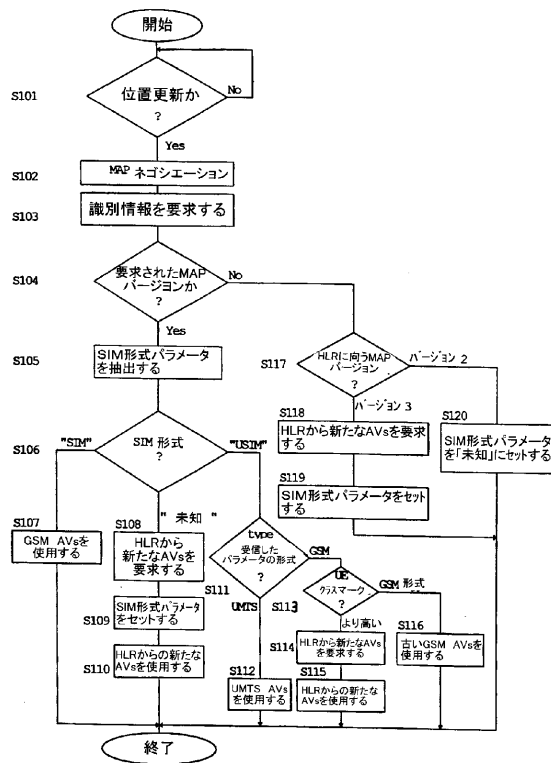


Fig. 1

【図 2】

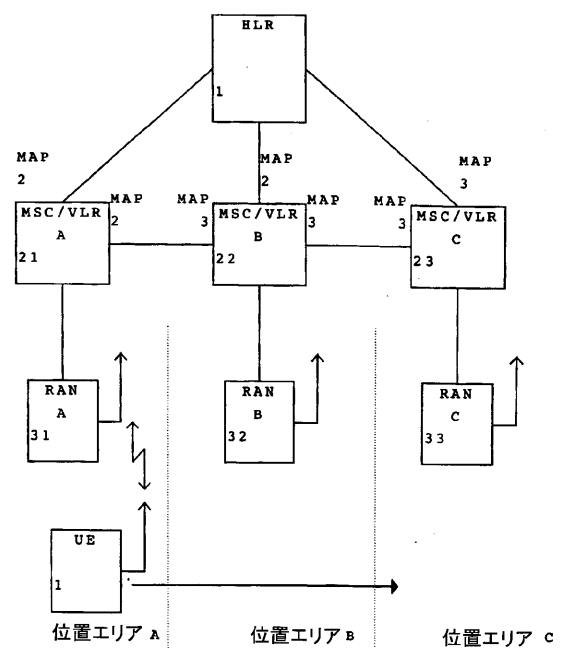


Fig. 2

【図 3】

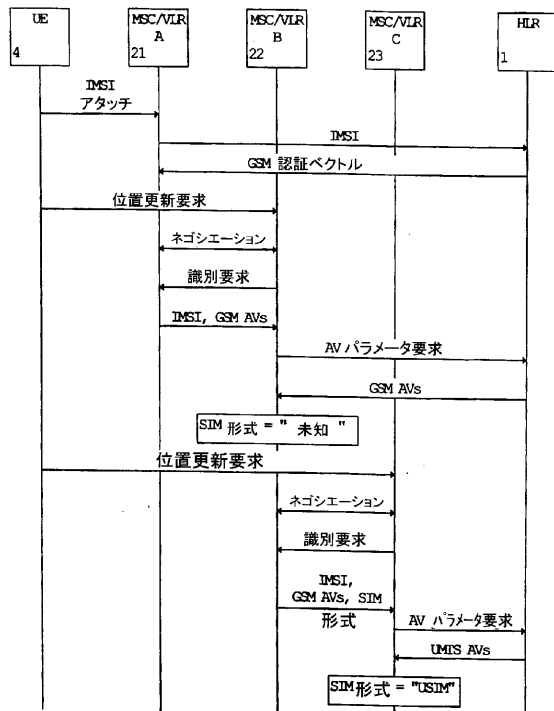


Fig. 3

【図 4】

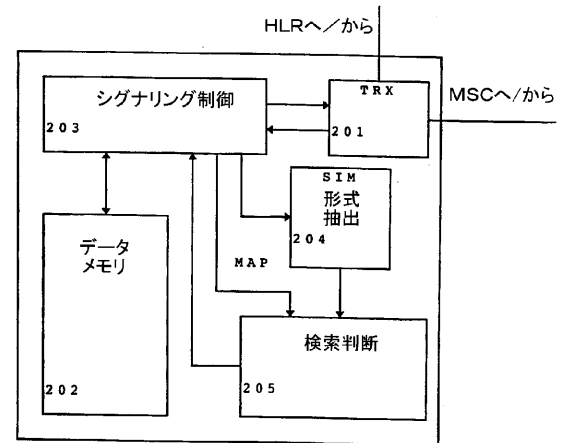


Fig. 4

フロントページの続き

- (74)代理人 100074228
弁理士 今城 俊夫
- (74)代理人 100084009
弁理士 小川 信夫
- (74)代理人 100082821
弁理士 村社 厚夫
- (74)代理人 100086771
弁理士 西島 孝喜
- (74)代理人 100084663
弁理士 箱田 篤
- (72)発明者 ベック ユハ
フィンランド エフイーエンー02150 エスプー ケイララーデンティエ 4 ノキア ネットワークス オサケ ユキチュア
- (72)発明者 フルッコネン トニ
フィンランド エフイーエンー02150 エスプー ケイララーデンティエ 4 ノキア ネットワークス オサケ ユキチュア
- (72)発明者 メキネン テーム
フィンランド エフイーエンー02150 エスプー ケイララーデンティエ 4 ノキア ネットワークス オサケ ユキチュア
- (72)発明者 サリン ハンヌーペッカ
フィンランド エフイーエンー02150 エスプー ケイララーデンティエ 4 ノキア ネットワークス オサケ ユキチュア

審査官 桑江 晃

- (56)参考文献 特開平06-141366 (JP, A)
特開平06-069880 (JP, A)
特開平07-030953 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
H04B 7/24 - 7/26
H04Q 7/00 - 7/38