(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4705021号
(P4705021)
(45)発行日　平成23年6月22日(2011.6.22)　(24)登録日　平成23年3月18日(2011.3.18)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601C
G09C 1/00 (2006.01)　　G09C 1/00 640E

請求項の数 17　(全 31 頁)

(21)出願番号　特願2006-509665 (P2006-509665)
(86)(22)出願日　平成16年4月2日(2004.4.2)
(65)公表番号　特表2006-522571 (P2006-522571A)
(43)公表日　平成18年9月28日(2006.9.28)
(86)国際出願番号　PCT/US2004/010304
(87)国際公開番号　WO2004/091176
(87)国際公開日　平成16年10月21日(2004.10.21)
審査請求日　平成19年3月30日(2007.3.30)
(31)優先権主張番号　60/460,257
(32)優先日　平成15年4月2日(2003.4.2)
(33)優先権主張国　米国(US)

(73)特許権者　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】ＣＤＭＡネットワークとＧＳＭネットワークとの間の暗号化

(57)【特許請求の範囲】
【請求項１】
第１ネットワークで加入された移動局（ＭＳ）が第２ネットワークを使用し通信することを可能とする、前記第１ネットワークと前記第２ネットワークとの間の無線通信方法であって、
前記移動局の識別情報を、第２ネットワークにおいて保存手段によって、保存することと；
前記移動局の前記識別情報に基づき前記第１ネットワークから認証情報を、第２ネットワークにおいて、入手することと、なお前記第１ネットワークはＧＳＭネットワークであり、前記第２ネットワークはＣＤＭＡネットワークである；
キーを作成するために前記第１ネットワークからの前記認証情報を、前記移動局によって使用することと、なお、前記キーは前記第１ネットワークにおいても作成され、前記作成されたキーは前記第１ネットワークから前記汎用グローバルゲートウェイにおいて受信される；
前記移動局を認証するために第１アルゴリズムで使用される認証キーの代わりに前記キーを、前記汎用グローバルゲートウェイにおいて、用いることと；そして
前記移動局と前記第２ネットワークとの間のメッセージを暗号化するために第２アルゴリズムで使用される暗号化キーの代わりに前記キーを、前記移動局において、用いることと；
を備え、

前記汎用グローバルゲートウェイは、前記第１および第２ネットワーク間を相互連携動作する相互連携動作相互運用性の機能を有しており、前記移動局に対しては、前記第２ネットワークへのビジッタロケーションレジスタとして機能し、また、ショートメッセージサービスセンタとして機能し、そして前記第２ネットワークにおいては認証コントローラとして動作する、

無線通信方法。

【請求項２】

前記第１アルゴリズムは前記第２ネットワーク中で実行される、請求項１に記載の方法。

【請求項３】

前記認証キーはＳＳＤ－Ａである、請求項１に記載の方法。

【請求項４】

前記暗号化キーはＳＳＤ－Ｂである、請求項１に記載の方法。

【請求項５】

前記第１アルゴリズムはＣＡＶＥアルゴリズムである、請求項１に記載の方法。

【請求項６】

前記第２アルゴリズムはＣＡＶＥアルゴリズムである、請求項１に記載の方法。

【請求項７】

前記ＧＳＭネットワークは汎用パケット無線サービス（ＧＰＲＳ）である、請求項１に記載の方法。

【請求項８】

前記ＧＳＭネットワークはユニバーサルモバイルテレコミュニケーションシステム（ＵＭＴＳ）である、請求項１に記載の方法。

【請求項９】

前記ＧＳＭネットワークは広帯域－ＣＤＭＡ（Ｗ－ＣＤＭＡ）である、請求項１に記載の方法。

【請求項１０】

前記ＣＤＭＡネットワークはｃｄｍａ２０００－１ｘである、請求項１に記載の方法。

【請求項１１】

前記ＣＤＭＡネットワークはｃｄｍａ２０００－１ｘＥＶ－ＤＯである、請求項１に記載の方法。

【請求項１２】

移動局の識別情報を、第２ネットワークにおいて、保存するための手段と；

前記移動局の前記識別情報に基づき第１ネットワークから認証情報を入手するための手段と、なお前記第１ネットワークはＧＳＭネットワークであり、前記第２ネットワークはＣＤＭＡネットワークである；

キーを作成するために前記第１ネットワークからの前記認証情報を使用するための手段と、なお、前記キーは前記第１ネットワークにおいても作成され、前記作成されたキーは前記第１ネットワークから前記汎用グローバルゲートウェイにおいて受信される；

前記移動局を認証するために第１アルゴリズムで使用される認証キーの代わりに前記キーを用いるための手段と、なお、前記キーは、前記移動局を認証するために前記第１アルゴリズムで使用される前記認証キーの代わりに用いられる；そして

前記移動局と前記第２ネットワークとの間のメッセージを暗号化するために第２アルゴリズムで使用される暗号化キーの代わりに前記キーを用いるための手段と；

を備え、なお、前記汎用グローバルゲートウェイは、前記第１および第２ネットワーク間を相互連携動作する相互連携動作相互運用性の機能を有しており、前記移動局に対しては、前記第２ネットワークへのビジッタロケーションレジスタとして機能し、また、ショートメッセージサービスセンタとして機能し、そして前記第２ネットワークにおいては認証コントローラとして動作する、

移動局。

【請求項１３】
前記ＧＳＭネットワークは汎用パケット無線サービス（ＧＰＲＳ）である、請求項１２に記載の移動局。
【請求項１４】
前記ＧＳＭネットワークはユニバーサルモバイルテレコミュニケーションシステム（ＵＭＴＳ）である、請求項１２に記載の移動局。
【請求項１５】
前記ＧＳＭネットワークは広帯域－ＣＤＭＡ（Ｗ－ＣＤＭＡ）である、請求項１２に記載の移動局。
【請求項１６】
前記ＣＤＭＡネットワークはｃｄｍａ２０００－１ｘである、請求項１２に記載の移動局。
【請求項１７】
前記ＣＤＭＡネットワークはｃｄｍａ２０００－１ｘＥＶ－ＤＯである、請求項１２に記載の移動局。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願の相互参照）
本出願は、２００３年４月２日に出願されたシリアル番号第６０／４６０，２５７号の米国仮特許出願の優先権を主張する。
本発明は、概して無線通信システムに関し、特に、ＣＤＭＡネットワークとＧＳＭネットワークとの間の暗号化を可能とするシステムに関する。
【背景技術】
【０００２】
符号分割多元接続方式（ＣＤＭＡ）は、比較的より大きな帯域幅容量を本質的に有している、即ち、他の無線通信技術よりも、周波数帯域あたりより多くの通話のサービスを本質的に可能とするデジタル無線技術である。更に、ＣＤＭＡのスペクトル拡散原理は安全確実な通信を本質的に提供できる。引用により本願に組み込まれる米国特許第４,９０１,３０７号には、音声通話及び非音声コンピュータデータの両方を送信するのに使用できるＣＤＭＡシステムの詳細が記載されている。
【０００３】
ＣＤＭＡの利点にもかかわらず、他の原理を使用する他の無線システムが存在する。例えば、世界の多くで、時分割多元接続方式の一種を使うＧＳＭが使用されている。
ＣＤＭＡ原理が使用されていようと、或いは他の無線原理が使用されていようと、無線通信システムは、二つの主要要素、即ち、無線接続方式ネットワーク（ＲＡＮ）とコアインフラストラクチャ（ｃｏｒｅ　ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）とを有しているようなものと考えられ得ることができ、前記コアインフラストラクチャは、ＲＡＮと通信し、公衆交換電話網（ＰＳＴＮ）やインターネット（特にデータ通話専用ではないが）等のような外部システムと通信する。種々さまざまな無線技術に関連するコアインフラストラクチャは、ハードウエアの面で、又、特定化された、典型的なシステム特定の（system-specific）通話切り替え、加入及び付随の認証及び通話監視、及び請求をサポートする通信プロトコルの開発の面で、非常に高価となることがある。従って、一つの無線システムの通信プロトコル（ＧＳＭの場合は、ＧＳＭプロトコル、又ｃｄｍａ２０００－１ｘのようなＣＤＭＡの場合は、ＩＳ－４１プロトコル）は、一つの或いは他のシステムのコアインフラストラクチャにおいて費用を掛けた非常に高価な変更無しでは他のシステムのプロトコルと互換性が無い。
【０００４】
ＧＳＭが世界の多くで現存するので、ＣＤＭＡネットワークとＧＳＭネットワークとの間を相互接続し、そうすることで、付随する利点を備えたままでのＣＤＭＡ対応ＲＡＮの

利用を可能とし、且つ、ＧＭＳ対応コアインフラストラクチャの利用を可能とすることが望ましいであろう。

【０００５】

このように、二重モード移動局は、例えば欧州においてはＧＳＭコアインフラストラクチャと便利にインターフェースすることが可能となり、又、例えば米国においてはＣＤＭＡインフラストラクチャを使用することが可能となるかもしれない。

【発明の開示】

【発明を解決するための手段】

【０００６】

本発明の一面は、

第１ネットワークで加入された移動局（ＭＳ）が第２ネットワークを使用し通信することを可能にする、前記第1ネットワークと前記第２ネットワークとの間の無線通信方法であって、

前記移動局の識別情報を保存し、

前記移動局の前記識別情報に基づき前記第１ネットワークから認証情報を入手し、

キーを作成するために前記第１ネットワークからの前記認証情報を使用し、

前記移動局を認証するために第１アルゴリズムで使用されるＳＳＤ－Ａ（共有秘密データ－Ａ）の代わりに前記キーを用い、そして

前記移動局と前記第２ネットワークとの間のメッセージを暗号化するために第２アルゴリズムで使用されるＳＳＤ－Ｂ（共有秘密データ－Ｂ）の代わりに前記キーを用いることを含む、

無線通信方法である。

【０００７】

本発明による種々さまざまな実施例が示され実例として説明されている以下の詳細な説明から、本発明の他の実施例が当業者に容易に明らかになることが分かる。理解されるとおり、本発明の精神及び範囲を逸脱せずに、本発明は他の異なる実施例が可能であり、いくつかの細部は種々さまざまな別の点で修正が可能である。従って、図面及び詳細な記述は、本質的に例示として見なされるべきものであり、限定的なものとして見なされるべきでない。

【発明を実施するための最良の詳細】

【０００８】

頭字語（ａｃｒｏｎｙｍｓ）

３ＧＰＰ２　－　第３世代パートナーシッププロジェクト２（3rd Generation Partnership Project2）

Ａｃｋ　－　受け取り通知（Acknowledgement）

ＡＣＭ－　アドレス完全メッセージ　（Address Complete Message）

ＡＮＭ　－　アンサーメッセージ（Answer Message）

Ａｓｓｉｇｎ　－　割当（Assignment）

ＡｕＣ　－　認証センタ（Authentication Center）

Ａｕｔｈ　－　認証（Authentication）

ＡＵＴＨＲ　－　認証レスポンス（Authentication Response）

ＢＳ　－　基地局（Base Station）

ＢＳＣ　－　基地局コントローラ（Base Station Controller）

ＢＴＳ　－　基地局トランシーバーサブシステム（Base station Transceiver Subsystem）

【０００９】

ＣＡＶＥ　－　移動電話認証及び音声暗号化（Cellular Authentication and Voice Encryption）

ＣＤＭＡ　－　符号分割多元接続方式（Code Division Multiple Access）

ＣＤＭＡ２０００　－　第３世代ＣＤＭＡ（Third Generation CDMA）

ＣＨ － チャンネル（Channel）
ＣＭ － 移動電話メッセージ（Cellular Message）
ＣＭＥＡ － 移動電話メッセージ暗号化アルゴリズム（Cellular Message Encryption Algorithm）
ＥＣＭＥＡ － 高度ＣＭＥＡ（Enhanced CMEA）
ＥＳＮ － 電子シリアル番号（Electronic Serial Number）
ＧＳＭ － 汎ヨーロッパデジタル移動通信システム（Global System for Mobile communications）
ＧＳＭＩｘ － ＧＳＷ－ＭＡＰのＣＤＭＡ２０００との収斂（Convergence of GSM-MAP with CDMA2000）

【００１０】
ＨＬＲ － ホームロケーションレジスタ（Home Location Register）
ＩＡＭ － 初期アドレスメッセージ（Initial Address Message）
ＩＭＳＩ － 国際モバイル加入者識別情報（International Mobile Subscriber Identity）
ＩＳＵＰ － ＩＳＤＮユーザーパート（ISDN User Part）
Ｉｎｆｏ － 情報（Information）
ＩＯＳ － 相互運用可能性仕様（Inter Operability Specification）
ＩＰ － インターネットプロトコル（Internet Protocol）
Ｋｃ － 暗号化キー（Ciphering Key）
Ｋｉ － 個人加入者認証キー（Individual Subscriber Authentication Key）
ＭＡＰ － モバイル申請パート（Mobile Application Part）
ＭＩＮ － モバイルＩＤ番号（Mobile Identification Number）
ＭＯ － モバイルが起点の（Mobile Originated）
ＭＳ － 移動局（Mobile Station）
ＭＳＮ － モバイル交換ノード（Mobile Switching Node）
ＭＴ － モバイルが終点の（Mobile Terminated）

【００１１】
ＰＤＳＮ － パケットデータサービスノード（Packet Data Service Node）
ＰＬＣ － プライベートロングコード（Private Long Code）
ＰＬＣＭ － ＰＬＣマスク（PLC Mask）
Ｐｒｉｖ － プライバシ（Privacy）
ＰＳＴＮ － 公衆交換電話網（Public Switched Telephone Network）
ＲＡＮ － 無線接続方式ネットワーク（Radio Access Network）
ＲＡＮＤ － ランダムチャレンジデータ（Random Challenge Data）
Ｒｅｑ － リクエスト（Request）
Ｒｅｓｐ － レスポンス（Response）
ＳＩＭ － 加入者ＩＤモジュール（Subscriber Identity Module）
ＳＭＳ － ショートメッセージサービス（Short Message Service）
ＳＭＳＣ － ショートメッセージサービスセンタ（Short Message Service Center）
ＳＲＥＳ － 署名入りレスポンス（Signed Response）
ＳＳＤ － 共有秘密データ（Shared Secret Data）
ＳＳ７ － 信号方式７（Signaling System 7）
ＴＣＨ － 通信チャンネル（Traffic Channel）
ＶＰ － 音声プライバシ（Voice Privacy）
ＶＰＭ － ＶＰマスク（VP Mask）

【００１２】
システムアーキテクチャ（System Architectures）
一実施例において、本システムはＣＤＭＡ ＲＡＮをＧＳＭコアネットワークに統合する。これは、ＧＳＭ加入の移動局（ＭＳ）とＧＳＭネットワークエンティティを使用する

ことにより達成される。前記ＧＳＭネットワークエンティティ用のオプションのうちの２つは、

（１）モバイル交換ノード（ＭＳＮ）、と

（２）相互連携動作相互運用可能性機能（ＩＩＦ）、である。

【００１３】

モバイル交換ノード（ＭＳＮ）は、標準ＩＯＳ準拠ＣＤＭＡ ＲＡＮとＧＳＭコアネットワークとの間の通信をサポートするネットワークスイッチング要素である。ＧＳＭ ＭＳＮは、ＨＬＲ、ＡｕＣ、ＳＭＳＣのようなＧＳＭコアーネットワークエンティティと共に動作する。ＭＳＮを使用したＧＳＭシステムアーキテクチャは図１に示される。

【００１４】

汎用グローバルゲートウェイ（ＧＧＧ）は、ＣＤＭＡとＧＳＭとのコアーネットワーク間を相互連携動作する相互連携動作相互運用可能性機能（ＩＩＦ）である。用語、「相互連携動作」（"interworks"）、「インターネットワーク」（"internetworks"）、は置き換え可能である。実施例において、ＧＧＧはＧＳＭ１ｘグローバルゲートウェイと呼ばれることもある。ＧＧＧは、Ｊ－ＳＴＤ－０３８ＩＩＩが進化したものであり、認証及びＳＭＳ機能性を強化している。このＧＧＧ解決法では、ＣＤＭＡ ＲＡＮに加え、標準ＣＤＭＡ ＭＳＣ／ＶＬＲを使用する。ＧＧＧは、これらの要素とＨＬＲ、ＡｕＣ、ＧＭＳＣ、ＳＭＳＣのような標準ＧＳＭネットワーク要素との間を相互連携動作する。ＧＧＧ使用のＧＳＭシステムアーキテクチャは図２に示される。

【００１５】

ＭＳＮアーキテクチャ（MSN Architecture）

図１は、一実施例による、ＭＳＮ使用のシステムアーキテクチャ１００のブロック図を示す。システム１００は、移動局１０２とＣＤＭＡネットワーク１０４とＧＳＭネットワーク１０６とＭＳＮ１０８とＰＤＳＮ１１０とＩＰネットワーク１１２とＰＳＴＮ１１４とを備える。

【００１６】

ＣＤＭＡネットワーク１０４は、ＢＴＳｓとＢＳＣｓとを備える。ＣＤＭＡネットワーク１０４はＰＤＳＮ１１０とインターフェースをとり、ＰＤＳＮ１１０はＩＰネットワーク１１２とインターフェースをとる。一実施例においては、ＣＤＭＡネットワーク１０４とＰＤＳＮ１１０との間のインターフェースはＩＳＯ ４．ｘに従う。一実施例においては、ＰＤＳＮ１１０とＩＰネットワーク１１２との間のインターフェースはＩＰを使用する。

【００１７】

ＣＤＭＡネットワーク１０４はＧＳＭ ＭＳＮ１０８とインターフェースをとる。一実施例においては、ＣＤＭＡネットワーク１０４とＧＳＭ ＭＳＮ１０８との間のインターフェースはＩＳＯ ４．ｘに従う。

ＧＳＭ ＭＳＮ１０８はＰＳＴＮ１１４とインターフェースをとる。一実施例においては、ＧＳＭ ＭＳＮ１０８とＰＳＴＮ１１４とのインターフェースはＩＳＵＰ経由で行われる。

【００１８】

ＧＳＭ ＭＳＮ１０８はＧＳＭネットワーク１４とインターフェースをとる。一実施例においては、ＧＳＭネットワーク１４は、ＧＳＭ ＳＳ７ １１６とＧＳＭ ショートメッセージセンタ（ＧＳＭ ＳＭＳＣ）１１８とＧＳＭ ホームロケーションレジスタ（ＧＳＭ ＨＬＲ）１２０とＧＳＭ認証センタ（ＧＳＭ ＡｕＣ）１２２とを備える。

【００１９】

ＧＧＧアーキテクチャー（GGG Architecture）

図２は、一実施例による無線通信システム１０のブロック図を示し、この無線システム１０は、ＣＤＭＡネットワーク１２とＧＳＭネットワーク１４と汎用グローバルゲートウェイ（ＧＧＧ）１６と移動局１８、２０、２２、２４とを備える。ＧＳＭ移動局２０は加入者ＩＤモジュール（ＳＩＭ）２６を含む。ＣＤＭＡ移動局２４はＳＩＭ２８を含む。Ｓ

ＩＭ２６、２８は、本技術分野で知られた原理に従い、夫々、無線局２０、２４に連動し取り外し可能である。

【００２０】

ＧＧＧ１６は、ＣＤＭＡネットワーク１２とＧＳＭネットワーク１４との間を相互接続する。ＧＧＧはトランシーバ（開示せず）を含んでおり、このトランシーバは、ＧＧＧに、ＣＤＭＡネットワーク１２及びＧＳＭネットワーク１４への、及び、からの、メッセージの送受信を許可する。

【００２１】

一実施例においては、ＣＤＭＡネットワークはＡＮＳＩ－４１ネットワークである。ＣＤＭＡネットワーク１２は、ｃｄｍａ２０００－１ｘやｃｄｍａ２０００－１ｘＥＶ－ＤＯに限定はされないがこれらを含む種々様々なＣＤＭＡネットワークの任意のものでよいことは当業者には明らかであろう。又、ＧＳＭネットワーク１４は、汎用パケット無線サービス（ＧＰＲＳ）やユニバーサルモバイルテレコミュニケーションシステム(Universal Mobile Telecommunication System)（ＵＭＴＳ）や広帯域－ＣＤＭＡ（Ｗ－ＣＤＭＡ）に限定されるものではないがこれらを含む種々様々なＧＳＭネットワーク又は後継ネットワークの任意のものでよいということも又、当業者には明らかであろう。

【００２２】

ＧＳＭネットワーク１４は、ＧＳＭコア３０とＧＳＭ無線接続方式ネットワーク３２とを備える。ＧＳＭコア３０は、ＧＳＭホームロケーションレジスタ（ＧＳＭ　ＨＬＲ）３４とＧＳＭ認証センタ（ＧＳＭ　ＡｕＣ）３６とＧＳＭショートメッセージセンタ（ＧＳＭ　ＳＭＳＣ）３８とＧＳＭゲートウェイモバイル交換センタ（ＧＳＭ　ＧＭＳＣ）４０とを備える。ＣＤＭＡネットワーク１２は、ＣＤＭＡホームロケーションレジスタ（ＣＤＭＡ　ＨＬＲ）４２とＣＤＭＡ認証センタ（ＣＤＭＡ　ＡｕＣ）４４とＣＤＭＡ　ＭＳＣ４６と関連ＣＤＭＡ無線接続方式ネットワーク（ＣＤＭＡ　ＲＡＮ）４８とを備える。

【００２３】

ＣＤＭＡコアに加入のＧＳＭ移動局２０関しては、ＧＧＧ１６はＧＭＳネットワーク１４に対するビジッタロケーションレジスタ（ＶＬＲ）５０として機能する。ＧＳＭコアに加入のＣＤＭＡ移動局２４関しては、ＧＧＧ１６はＣＤＭＡネットワーク１２に対するビジッタロケーションレジスタ（ＶＬＲ）５２として機能する。

【００２４】

移動局１８、２０、２２、２４は両方のコアインフラストラクチャ１２、１４に加入する必要はなく、コアインフラインストラクチャ１２，１４の一方のみに加入してもよい。

ＣＤＭＡコアに加入のＧＳＭ移動局２０とＧＳＭコアに加入のＣＤＭＡ移動局２４の両方に関し、ＧＧＧ１６はショートメッセージサービスセンタ（ＳＭＳＣ）として機能する。ＧＧＧ１６はＳＭＳＣ５４を含むことが出来或いはＳＭＳＣ５４と通信することが出来る、ということは当業者にとっては明らかであろう。

【００２５】

移動局１８，２０は、ＧＳＭ信号伝達プロトコル、ＧＳＭ認証手続き、ＧＳＭショートメッセージサービスをサポートする。同様に、移動局２２，２４は、ＣＤＭＡ信号伝達プロトコル、ＣＤＭＡ認証手続き、ＣＤＭＡショートメッセージサービスをサポートする。

【００２６】

ＧＳＭコアに加入のＣＤＭＡ移動局２４の登録の期間、ＧＧＧはＣＤＭＡネットワークにおいて認証コントローラとして作動するが、ＧＳＭ認証機構を使用し移動局２４を認証する。同様に、前記ＣＤＭＡコアに加入のＧＳＭ移動局２０の登録の期間、ＧＧＧはＧＳＭネットワークにおいて認証コントローラとして作動するが、ＣＤＭＡ認証機構を使用し前記移動局２０を認証する。

【００２７】

ＧＧＧは、ショートメッセージサービスセンタ５４を介しメッセージセンタとして働く。ＣＤＭＡネットワークにおいては、ＳＭＳメッセージは、ＣＤＭＡ　ＳＭＳ機構を使い移動局２４に、及びから、転送される。即ち、ＣＤＭＡネットワークにおいては、ＧＳＭ

メッセージは、ＣＤＭＡ　ＳＭＳ機構を使い移動局２４に、及びから、通り抜けていく（are tunneled）。ＧＳＭメッセージはＣＤＭＡ　ＳＭＳメッセージとしてインターフェースがとられる（encapsulated within）。

【００２８】

同様に、ＧＳＭネットワークにおいては、ＳＭＳメッセージは、ＧＳＭ　ＳＭＳ機構を使い移動局２０に、及びから、転送される。即ち、ＧＳＳＭネットワークにおいては、ＣＤＭＡメッセージは、ＧＭＳ　ＳＭＳ機構を使い移動局２０に、及びから、通り抜けていく（tunneled）。前記ＣＤＭＡメッセージはＧＳＭ　ＳＭＳメッセージとしてインターフェースがとられる（encapsulated within）。

【００２９】

登録されたＧＳＭ加入者２４への入呼（incoming call）は、加入者のホームＧＳＭネットワーク１４のＧＳＭゲートウェイＭＳＣ（ＧＳＭ　ＧＭＳＣ）４０に到着する。ＧＭＳＣ４０は、ＣＤＭＡネットワーク１２の中にある加入者２４のロケーションを決定するため、ＧＳＭ　ＬＲ５０を調べる。加入者２４のロケーションは、ＧＳＭ　ＬＲ５０から見ると、ＧＧＧ１６の中にあり、ＧＳＭ　ＶＬＲとして見える。ＧＳＭ　ＬＲ５０がＧＧＧ１６に経路情報（routing information）を要求する時、ＧＧＧ１６はサービスを行っているＣＤＭＡ　ＬＲ５２に経路情報を要求し、このようにして呼（call）がＣＤＭＡ　ＭＳＣ４６に転送される。

【００３０】

同様に、登録されたＣＤＭＡ加入者２０への入呼は、加入者のホームＣＤＭＡネットワーク１２のＣＤＭＡ　ＭＳＣ４６に到着する。ＣＤＭＡ　ＭＳＣ４６は、ＧＳＭネットワーク１４の中にある加入者２０のロケーションを決定するため、ＣＤＭＡ　ＬＲ５２を調べる。ＣＤＭＡ加入者２０のロケーションは、ＣＤＭＡ　ＬＲ５２から見ると、ＧＧＧ１６の中にあり、ＣＤＭＡ　ＶＬＲとして見える。ＣＤＭＡ　ＬＲ５０がＧＧＧ１６に経路情報を要求する時、ＧＧＧ１６はサービスを行っているＧＳＭ　ＬＲ５０に経路情報を要求し、このようにして呼がＧＳＭ　ＧＭＳＣ４０に送られる。

【００３１】

ＣＤＭＡを基地とした移動局２２，２４は、本技術分野で知られたＣＤＭＡ原理に従い、ＣＤＭＡ無線接続方式ネットワーク（ＲＡＮ）４８を使用してＣＤＭＡモバイル交換センタ（ＭＳＣ）４６と通信する。一実施例においては、ＣＤＭＡ　ＭＳＣ４６はＩＳ－４１　ＭＳＣである。

【００３２】

同様に、ＧＳＭを基地とした移動局１８、２０は、本技術分野で知られたＧＳＭ原理に従い、ＧＳＭ　ＲＡＮ３２を使用してＧＳＭモバイル交換センタ（ＧＳＭ　ＧＭＳＣ）４０と通信する。

本技術分野で知られたＣＤＭＡ原理に従い、ＣＤＭＡ　ＲＡＮ４８は基地局及び基地局コントローラを含んでいる。一実施例においては、図２で示されるＣＤＭＡ　ＲＡＮ２４はｃｄｍａ２０００を使用しており、特に、ｃｄｍａ２０００　１ｘ、ｃｄｍａ２０００　３ｘ、又は、ｃｄｍａ２０００高データ率（ＨＤＲ）原理を使用する。

【００３３】

本技術分野で知られたＧＳＭ原理に従い、ＧＳＭ　ＲＡＮ３２は基地局及び基地局コントローラを含んでいる。一実施例においては、ＧＳＭ　ＲＡＮ３２はＧＳＭ、ＧＰＲＳ、ＥＤＧＥ、ＵＭＴＳ、又はＷ－ＣＤＭＡ原理を使用する。

ＣＤＭＡ　ＭＳＣ４６とＣＤＭＡ　ＲＡＮ４８とを備えたＣＤＭＡコアインフラストラクチャは、加入者移動局２２を認証するため、又、特別のＣＤＭＡコアインフラストラクチャにより要求されるような経理及び請求の情報を収集するため、本技術分野で知られたＣＤＭＡ原理に従い、ＣＤＭＡ認証センタ（ＣＤＭＡ　ＡＵＣ）４４とＣＤＭＡホームロケーションレジスタ（ＣＤＭＡ　ＨＬＲ）４２とを含むことが出来、或いは、これらにアクセスすることが出来る。

【００３４】

同様に、ＧＳＭコア３０は、加入者移動局１８を認証するため、又、特別のＧＳＭコアインフラにより要求されたような経理及び請求の情報を収集するため、本技術分野で知られたＧＳＭ原理に従い、ＧＳＭ認証センタ（ＧＳＭ　ＡＵＣ）３６とＧＳＭホームロケーションレジスタ（ＧＳＭ　ＨＬＲ）３４とを含むことが出来、或いは、これらにアクセスすることが出来る。

【００３５】

ＣＤＭＡ　ＭＳＣ４６は、ＧＳＭネットワーク１４と通信するためＧＧＧ１６を使用する。ＧＳＭネットワーク１４は、加入者移動局２４を認証するため、又、特別のＧＳＭコア３０により要求されるような経理及び請求の情報を収集するため、本技術分野で知られたＧＳＭ原理に従い、ＧＳＭ認証センタ３６とＧＳＭホームロケーションレジスタ（ＨＬＲ）３４とを含めることが出来、或いは、これらにアクセスすることが出来る。

【００３６】

同様に、ＧＳＭ　ＧＭＳＣ４０は、ＣＤＭＡネットワーク１２と通信するためＧＧＧ１６を使用する。ＣＤＭＡネットワーク１２は、加入移動局２０を認証するため、又、特別のＣＤＭＡネットワーク１２により要求されるような経理及び請求の情報を収集するため、本技術分野で知られたＣＤＭＡ原理に従い、ＣＤＭＡ認証センタ４４とＣＤＭＡホームロケーションレジスタ（ＨＬＲ）４２とを含めることが出来、或いは、これらにアクセスすることが出来る。

【００３７】

ＧＳＭコア３０とＣＤＭＡコアインフラストラクチャの両方は、例えば、公共交換電話網（ＰＳＴＮ）及び／又はインターネットプロトコル（ＩＰ）ネットワークなどのネットワークと通信できる。

ＧＳＭコア３０で加入のＣＤＭＡ移動局２４に関しては、ＧＧＧ１６はＧＳＭネットワーク１４に対しＶＬＲ５０として機能する。ＧＧＧはＶＬＲ５０用ＧＳＭプロトコル要件を満足する。ＧＧＧは、ＧＧＧ１６がＣＤＭＡネットワーク１２に入呼を転送する（routes incoming calls）ことを除き、ＧＳＭ仕様に従い、ＧＳＭ　ＨＬＲ３４やＧＳＭ　ＳＭＳＣ３８のようなＧＳＭコアネットワーク要素と相互に作用する。ＧＳＭ　ＬＲ５０は又、移動局がＣＤＭＡネットワーク１２に登録する時、ＧＳＭネットワーク１４でのロケーションを更新する。この意味で、ＧＧＧはＣＤＭＡネットワーク１２全体に対しＶＬＲとして働く。

【００３８】

ＣＤＭＡネットワーク１２で加入のＧＳＭ移動局２０に関しては、ＧＧＧ１６はＣＤＭＡネットワーク１２に対しＶＬＲ５２として機能する。ＧＧＧはＶＬＲ５２用ＣＤＭＡプロトコル要件を満足する。ＧＧＧは、ＧＧＧ１６がＣＤＭＡネットワーク１２に入呼を転送することを除き、ＣＤＭＡ仕様に従い、ＣＤＭＡ　ＨＬＲ４２やＣＤＭＡ　ＭＳＣ４６のようなＣＤＭＡコアネットワーク要素と相互に作用する。ＣＤＭＡ　ＬＲ５２は又、移動局がＧＳＭネットワーク１４に登録する時、ＣＤＭＡネットワーク１２でのロケーションを更新する。この意味で、ＧＧＧはＧＳＭネットワーク１４全体に対しＶＬＲとして働く。

【００３９】

ＣＤＭＡネットワーク１２の中にある移動局がＧＳＭネットワーク１４から呼び出される時、呼は、標準仕様に従いＧＧＧ１６の中にあるＣＤＭＡ　ＬＲ５２に転送される（routed）。ＧＧＧ１６はこの呼をＣＤＭＡネットワーク１２に転送する。ＣＤＭＡネットワーク１２は結果として、移動局にサービスを提供するＣＤＭＡ　ＭＳＣ４６にこの呼を転送する。同様に、ＳＭＳがＧＳＭネットワーク１４からＣＤＭＡネットワーク１２に転送される場合、ＧＧＧ１６はＣＤＭＡネットワーク１２内のメッセージセンタ（示されておらず）に前記メッセージを転送する。

【００４０】

ＧＳＭネットワーク１４の中にある移動局がＣＤＭＡネットワーク１２から呼び出される時、呼は、標準仕様に従いＧＧＧ１６の中にあるＧＳＭ　ＬＲ５０に転送される。ＧＧ

Ｇ１６は、この呼をＧＳＭネットワーク１４に転送する。ＧＳＭネットワーク１４は結果として、移動局にサービスを提供するＧＳＭ　ＧＭＳＣ４０にこの呼を転送する。同様に、ＳＭＳがＣＤＭＡネットワーク１２からＧＭＳネットワーク１０に転送される場合、ＧＧＧ１６はＧＳＭネットワーク１４内のＧＳＭ　ＳＭＳＣ３８に前記メッセージを転送する。

【００４１】

移動局がＣＤＭＡネットワーク１２に登録する時、ＣＤＭＡネットワーク１２はＧＳＭネットワーク１４にロケーション更新指示（a location update indication）を送る。ＧＳＭ　ＬＲ５０はそのあと、ＧＳＭコアネットワーク１４で、標準仕様に従いロケーションを更新する。

【００４２】

移動局がＧＳＭネットワーク１４に登録する時、ＧＳＭネットワーク１４はＣＤＭＡネットワーク１２にロケーション更新指示を送る。前記ＣＤＭＡ　ＬＲ５２はそのあと、ＣＤＭＡネットワーク１２で、標準仕様に従いロケーションを更新する。

ＧＳＭコア３０で加入のＣＤＭＡ移動局２４に関しては、ＧＧＧ１６はＣＤＭＡネットワーク１２におけるＨＬＲ５２として働く。ＣＤＭＡ　ＬＲ５２は、ＧＳＭがＣＤＭＡローミングを行う（CDMA roaming）ＨＬＲプロトコル要件を満足する必要がある。ＨＬＲ５０が保持する情報の重要な一つは、移動局２４にサービス提供するＣＤＭＡ　ＭＳＣ４６のアドレスである。ＧＧＧ１６の中のＧＳＭ　ＬＲ５０がＧＤＭＡ側１２に呼を転送する時、ＣＤＭＡ　ＬＲ５２は更にそれを、サービス提供を行うＭＳＣ４６に転送する。

【００４３】

ＣＤＭＡネットワーク１２で加入のＧＳＭ移動局２０に関しては、ＧＧＧ１６はＧＳＭネットワーク１４におけるＨＬＲ５０として働く。ＧＳＭ　ＬＲ５０は、ＣＤＭＡがＧＳＭローミングを行う（GSM roaming）ＨＬＲプロトコル要件を満足する必要がある。ＨＬＲが保持する情報の重要な一つは、移動局２０に前記サービス提供するＧＳＭ　ＧＭＳＣ４０のアドレスである。ＧＧＧ１６の中のＣＤＭＡ　ＬＲ５２がＧＳＭ側１４に呼を転送する時、ＧＳＭ　ＬＲ５０は更にそれを、サービス提供を行うＭＳＣ４０に転送する。

【００４４】

ＧＧＧは、ＧＳＭ加入者２４に対しては、ＣＤＭＡネットワークにおける認証コントローラ（ＡＵＣ）として働く。ＣＤＭＡネットワーク１２の中のＡＵＣ４４は、移動局の認証及びネットワークリソースへのアクセスの許可／拒否に責任を持つ。ＧＧＧにおけるＡＬＵの機能は、ＧＧＧ又はＭＳでのＡ－キープロビジョニング（A-key provisioning）を必要としない。その代わりＧＧＧは、移動局２４を認証するのに、ＧＳＭ認証資格証明情報とＧＳＭ信号方式によるＧＳＭ認証手法を使用する。ＧＧＧは、ＣＤＭＡ　ＡＬＵ４４によって受領されることのある有効メッセージに応答する。

【００４５】

ＧＧＧは、ＣＤＭＡ加入者２０に対しては、ＧＳＭネットワークにおける認証コントローラ（ＡＵＣ）として働く。ＣＤＭＡネットワーク１４の中のＡＵＣ３６は、移動局の認証及びネットワークリソースへのアクセスの許可／拒否に責任を持つ。ＧＧＧにおける前記ＡＬＵの機能は、ＧＧＧ又はＭＳでのＡ－キープロビジョニングを必要としない。その代わりＧＧＧは、移動局２０を認証するのに、ＣＤＭＡ認証資格証明情報とＣＤＭＡ信号方式によるＣＤＭＡ認証手法を使用する。ＧＧＧは、ＧＳＭ　ＡＬＵ３６によって受領されることのある有効メッセージに応答する。

【００４６】

ＧＧＧ１６は、ＣＤＭＡネットワーク１２でのメッセージセンタ（ＭＣ）として働き、ＧＳＭ　ＳＭＳ機構を使用しＣＤＭＡ移動局２４とＧＳＭ　ＧＭＳＣ４０との間でＳＭＳメッセージを転送する。

同様に、ＧＧＧ１６は、ＧＳＭネットワーク１４でのメッセージセンタ（ＭＣ）として働き、ＣＤＭＡ　ＳＭＳ機構を使用しＧＳＭ移動局２０とＣＤＭＡ　ＭＳＣ４６との間でＳＭＳメッセージを転送する。

【００４７】
ＣＤＭＡ　ＭＳ２４はＣＤＭＡネットワークにおける有効識別情報(a valid identity)を持つことを要求される。もしこの識別情報がＧＳＭ国際モバイル加入者識別情報（ＩＭＳＩ）と異なるならば（即ち、もしＣＤＭＡネットワークが真のＩＭＳＩを使用しないならば）、そのときは、ＧＧＧはＣＤＭＡ識別情報とＧＳＭ　ＩＭＳＩとの間のマッピング（mapping）を提供する。移動局２４を特有の方法で識別するのに、本技術分野で知られた任意の技術／方法が使用され得ることは当業者にとっては明らかであろう。
【００４８】
ＧＳＭ　ＭＳ２０はＧＳＭネットワークにおける有効識別情報を持つことを要求される。一実施例においては、この識別情報はＧＳＭ　ＩＭＳＩである（即ち、もしＣＤＭＡネットワークが真のＩＭＳＩを使用しないならば）。もしＧＳＭネットワークにおける識別情報がＣＤＭＡネットワークにおける識別情報と異なるならば、そのときは、ＧＧＧはＧＳＭ識別情報とＣＤＭＡ識別情報との間のマッピングを提供する。移動局２０を特有の方法で識別するのに、本技術分野で知られた任意の技術／方法が使用され得ることは当業者にとって明らかであろう。
【００４９】
限定しない実施例においては、移動局１８、２０は、京セラ、三星、或いは他の製造業者により製造された、ＧＳＭ原理及びＧＳＭ放送（ＯＴＡ）通信エアーインターフェース（GSM over-the-air(OTA)communication air interface）を使用した移動電話である。限定しない実施例においては、移動局２２、２４は、京セラ、三星、或いは他の製造業者により製造された、ＣＤＭＡ原理及びＣＤＭＡ放送（ＯＴＡ）通信エアーインターフェース（CDMA over-the-air(OTA)communication air interface）を使用した移動電話である。本発明は、しかしながら、例えば、ラップトップコンピュータ、無線送受話器或いは電話、データトランシーバ、或いはページング及び位置決定レシーバ（paging and position determination receivers）、などの他の移動局にも適用できる。地上局は、所望に応じ、手で持てるサイズであり得、或いは、車両（自動車、トラック、ボート、飛行機、列車を含む）に搭載されるように持ち運び出来るものであり得る。しかしながら、無線通信装置は一般に移動式であるように見られるのであるが、本発明はある実施のもとでは「固定」ユニット（”fixed” units）に適用され得ることが理解されるべきである。又、本発明は、音声及び／又はデジタル化されたビデオ情報を含むはデータの情報を転送するのに使用される、データモジュール或いはモデムに適用され、又、有線或いは無線のリンクを使用する他の装置と通信できる。更に、多重通信チャンネルで情報を転送するように、所定の調整のされた或いは関連付けのされた方法で、モデム或いはモジュールを動作させるようにコマンドが使用されてもよい。無線通信装置は又、時には、ユーザターミナル、移動局、モバイルユニット、加入者ユニット、モバイルラジオ或いは無線電話、無線ユニット、と呼ばれることがあり、或いは、ある通信システムにおいては単純に「ユーザーズ」、又「モバイル」と言われる。（”users” and ”mobiles”）
【００５０】
ＳＳＤ不使用による認証（Authentication without using SSD）
図３Ａ及び３Ｂは、ＳＳＤを使用しない一実施例による、ＧＳＭネットワーク１４で加入のＣＤＭＡ移動局２４を認証するフローチャートを示す。図３Ａ及び３Ｂは、図６の記述内容を伝えるように記述されている。
【００５１】
ステップ２０２において、移動局２４（ＭＳ）はＣＤＭＡエリアにローミングして入り（roam into）、制御フローはステップ２０４に進む。ステップ２０４において、移動局２４は、ＣＤＭＡ　ＲＡＮ４８経由でＣＤＭＡ　ＭＳＣ４６への登録システムアクセスを開始し、制御フローはステップ２０６に進む。
【００５２】
登録システムアクセスは、ＣＤＭＡ　ＲＡＮ４８経由のＣＤＭＡ　ＭＳＣ４６へのメッセージであり、このメッセージは移動局２４の識別情報（an identity）を含む。一実施

例においては、移動局２４の識別情報はＳＩＭ２８から提供されることもある。一実施例においては、移動局２４の識別信号はＩＭＳＩである。一実施例においては、前記移動局24の識別信号はモバイルＩＤ番号（ＭＩＮ）である。

【００５３】

ステップ２０６において、ＣＤＭＡ　ＭＳＣ４６は、移動局識別情報に基づき、移動局２４がＧＳＭ加入者であるかどうかを決定する。一実施例においては、移動局２４の識別情報はＩＭＳＩであり、ＩＭＳＩは他の情報の中で、移動局が加入している国及びネットワークを表すコードを含んでいるので、ＭＳＣ４６はこれを決定出来る。

【００５４】

ＣＤＭＡ加入移動局２２がテスト中の移動局である場合には、制御フローはステップ２０８に進む。ステップ２０８において、移動局２２は、ＣＤＭＡ　ＨＬＲ４２及びＣＤＭＡ　ＡＵＣ４４を使用するＣＤＭＡコアインフラストラクチャによりＣＤＭＡ原理を使って認証される。

【００５５】

ＧＳＭネットワークで加入のＣＤＭＡ移動局２４がテスト中の移動局である場合には、制御フローはステップ２１０に進む。ステップ２１０においては、一実施例に従い、ＣＤＭＡ　ＭＳＣ４６は、ＧＧＧ１６の中のＣＤＭＡ　ＬＲ５２に認証リクエストを送ることによりＧＧＧ１６をアクセスし、制御フローはステップ２１２に進む。別の実施例では、制御フローはステップ２１４に進む。

【００５６】

一実施例においては、移動局２４の識別信号は、認証リクエストの一部分としてＣＤＭＡ　ＬＲ５２に送られる。あるいは、移動局２４の識別信号は、認証リクエストに追加してＣＤＭＡ　ＬＲ５２に送られる。

一実施例においては、認証リクエストはパラメータＭＩＮ、ＥＳＮ及びＣＯＵＮＴを含むことが出来る。ＥＳＮは電子シリアル番号である。

【００５７】

一実施例においては、認証リクエストはパラメータＭＩＮ、ＥＳＮ及びＣＯＵＮＴを含むことが出来る。ＥＳＮは電子シリアル番号である。ＣＯＵＮＴは、ＧＧＧ１６と移動局２４との間で相互合意された、所定の事象のカウント（count）を表す。一実施例においては、ＧＧＧ１６は、ＧＧＧ１６と相互作用するノード（node）と共にＣＯＵＮＴの更新を共有する。別のノードと更新機能を共有することにより、ＧＧＧ１６とその他のノードとの間のメッセージ量（message traffic）は軽減されることも可能である。例えば、もしＧＧＧ１６がＣＤＭＡ　ＭＳＣ４６とＣＯＵＮＴ更新機能を共有すれば、そのときは、ＧＧＧ１６とＣＤＭＡ　ＭＳＣ４６との間のメッセージ量は軽減されることも可能である。

【００５８】

一実施例においては、ＣＯＵＮＴは、移動局２４がＧＳＭネットワーク１４をアクセスしようと試みた回数を表す。移動局２４がＧＳＭネットワークをアクセスする毎に、ＧＧＧは特定の移動局２４用のＣＯＵＮＴを更新する。移動局２４は又、それがＧＳＭネットワーク１４をアクセスする回数用のそれ自身のＣＯＵＮＴを更新する。ＧＧＧ１６は、ＥＳＮの数値（value）を記憶する。別の実施例においては、ＣＯＵＮＴは、移動局による認証リクエストの数を表す。カウントされ得る多くの事象があり、移動局２４とＧＧＧ１６はそれらの事象をカウントできる、ということは、当業者にとっては明らかであろう。

【００５９】

ステップ２１２において、ＧＧＧ１６はＣＯＵＮＴの数値とＧＧＧデータベース中のカウント値とを比較する。ＣＯＵＮＴの数値がＧＧＧデータベースの中のカウント値と等しい場合は、そのときは、制御フローはステップ２１４に進む。ＣＯＵＮＴの数値がＧＧＧデータベースの中のカウント値と等しくない場合は、そのときは、制御フローはステップ２１６に進む。応用に応じて、種々様々の基準（criteria）が、認証リクエストが許可されるかどうかを決定するのに適用されることは当業者にとって明らかであろう。

【００６０】
ステップ２１４においては、認証リクエストリターン結果（ＡＲＲＲ）が真（true）とセットされ、制御フローはステップ２１８に進む。認証リクエストリターン結果メッセージは認証リクエストの結果を示す。
ステップ２１６においては、認証リクエストリターン結果（ＡＲＲＲ）が偽（false）とセットされ、制御フローはステップ２２０に進む。
【００６１】
真の認証リクエストリターン結果に応答し、ＧＧＧ１６は、ＧＳＭネットワーク１４にアクセスし、ＧＳＭ　ＨＬＲ３４とＧＳＭ　ＡｕＣ３６とから必要な認証情報を入手する。ステップ２１８においては、一実施例に従い、ＧＧＧ１６は、対応するＧＳＭ　ＩＭＳＩを入手するためにそのデータベースの中のＭＩＮを調べ、移動局２４のＩＭＳＩと共にＧＳＭ　ＨＬＲ認証メッセージをＧＳＭ　ＨＬＲ／ＡｕＣ３４、３６に送ることによりＧＳＭネットワーク１４にアクセスする。制御フローはステップ２２０に進む。
【００６２】
方法の複数のステップは、本発明の範囲を逸脱せずに入れ替え可能である。従って、ステップ２１８はステップ２２０の必ずしも前に実行される必要はないことは当業者にとって明らかであろう。
ステップ２２０において、ＧＧＧ１６は認証リクエストリターン結果をＣＤＭＡ　ＭＳＣ４６に送り、制御フローはステップ２２２に進む。ステップ２２２においては、認証リクエストリターン結果がテストされる。もし、認証リクエストリターン結果が真であれば、そのあとステップ２２４において、ＧＧＧ１６はタイマ、Ｔ　ＲＥＧをスタートさせ、制御フローはステップ２２６に進む。
【００６３】
もし、認証リクエストリターン結果が偽であれば、制御フローはステップ２２８に進む。ステップ２２８において、ＣＤＭＡ　ＭＳＣ４６は、移動局２４が認証されないことを示す移動局認証メッセージを移動局２４に送る。移動局はアップリケーションに応じ認証を再度試みることも出来る、ということは当業者には明らかであろう。
【００６４】
ＧＧＧはプログラムロジックを実行するロジックユニット（示されておらず）を含む。ロジックユニットは汎用プロセッサ、特定目的用プロセッサ、及び／又はファームウェアを含むことも出来る、ということは当業者には明らかであろう。
ステップ２２６において、ＣＤＭＡ　ＭＳＣ４６は、成功認証を示す認証リクエストリターン結果を受領すると、ＧＧＧ１６の中のＣＤＭＡ　ＬＲ５２に登録通知を送る。制御フローはステップ２３０に進む。
【００６５】
ステップ２３０においては、Ｔ　ＲＥＧが終了する前にＧＧＧ１６が登録通知を受領したかどうかがチェックされる。もしＧＧＧ１６がＴ　ＲＥＧ終了前に登録通知を受領したのであれば、そのときは、制御フローはステップ２３２に進み、そうでなければ制御フローはステップ２３４に進む。ステップ２３２においては、Ｔ　ＲＥＧが終了しなかったことを示すように登録通知リターン結果がセットされ、制御フローはステップ２３６に進む。ステップ２３４においては、Ｔ　ＲＥＧが終了したことを示すように登録通知リターン結果がセットされ、制御フローはステップ２３６に進む。
【００６６】
ステップ２３６において、ＧＧＧ１６は、Ｔ　ＲＥＧが終了したかどうかを示す登録通知リターン結果付の登録通知に応答する。登録通知リターン結果は前記ＧＧＧ１６からＣＤＭＡ　ＭＳＣ４６に送られる。
一実施例においては、ＧＧＧ１６は、ＳＭＳオンリーモード／状態（SMS only mode/status）を示す登録通知リターン結果を付けて或いはその範囲内でメッセージを送る。「ＳＭＳオンリー」とは、移動局２４はデータ及び／又は音声メッセージを送受信するのではなく、ＳＭＳメッセージのみを送受信することを意味する。制御フローはステップ２３８

に進む。

【００６７】

ステップ２３８において、ＣＤＭＡ　ＭＳＣ４６は、登録通知リターン結果を受領すると登録許可メッセージを移動局２４に送る。登録通知リターン結果のように、登録許可メッセージはＴ　ＲＥＧが終了したかどうかを示す。制御フローはステップ２４０に進む。

【００６８】

ステップ２４０においては、移動局２４は、登録許可メッセージが許可された登録を示しているかどうかを、即ちＴ　ＲＥＧが終了しなかったことを示しているかどかを決定する。もしＴ　ＲＥＧが終了したのであれば、そのあと、制御フローはステップ２４２に進み、そうでなければ制御フローはステップ２４４に進む。

【００６９】

ステップ２４２においては、移動局２４は登録を再試行するかもしれないし、しないかもしれない。移動局アップリケーション（a mobile station application）に応じ、移動局が再試行するかもしれないかしないかもしれないかは、当業者には明らかであろう。

【００７０】

方法の複数のステップは、本発明の範囲内で入れ替え可能である。従って、ステップ２４４はステップ２４２の必ずしも後で実行される必要がないことは当業者にとって明らかであろう。

ステップ２４４は、ステップ２１８のＧＳＭ　ＨＬＲ認証メッセージがＧＳＭ　ＨＬＲ／ＡｕＣ３４、３６に送られた後に実行さえすればよい。ステップ２４４において、ＧＳＭ　ＨＬＲ／ＡｕＣ３４、３６は、認証パラメータを含むＧＧＧ認証メッセージをＧＧＧ１６に送り、制御フローはステップ２４６に進む。

【００７１】

ＧＧＧ１６が首尾よく登録通知リターン結果をＣＤＭＡ　ＭＳＣ４６に送り、ＧＧＧ認証メッセージをＧＳＭ　ＨＬＲ／ＡｕＣ３４から受領した後、ステップ２４６において、ＧＧＧ１６はＧＳＭ認証リクエストメッセージをＣＤＭＡ　ＭＳＣ４６に送る。制御フローはステップ２４８に進む。ステップ２４８においては、ＣＤＭＡ　ＭＳＣ４６はＧＳＭ認証リクエストメッセージを移動局２４に転送し、制御フローはステップ２５０に進む。

【００７２】

一実施例においては、ステップ２１０のオリジナルの認証リクエストに適用された基準（criteria）に加え、アプリケーションは移動局を認証するためのもっと多くの基準を持ち得る。従って、一実施例においては、ＣＤＭＡ　ＭＳＣ４６はＧＧＧ１６に第二認証リクエスト（示されず）を送り、ＧＧＧ１６は第二認証リクエスト（示されず）に応答する。

【００７３】

ステップ２５０において、移動局２４は、ＧＳＭ認証方法を使用して例えば暗号化キーなどの認証パラメータを決定し、認証パラメータを含む認証レスポンスをＣＤＭＡ　ＭＳＣ４６に送ることにより、ＧＳＭ認証リクエストメッセージに応答する。一実施例においては、認証レスポンスはＩＳ－６３７ＳＭＳトランスポートを使って送られる。制御フローはステップ２５２に進む。

【００７４】

ステップ２５２においては、ＣＤＭＡ　ＭＳＣ４６は認証レスポンスをＧＧＧ１６に転送し、ＧＧＧ１６は、認証パラメータをステップ２４４においてＧＳＭ　ＨＬＲ／ＡｕＣ３４、３６から受信の数値に合わせることにより、認証パラメータを有効にする。制御フローはステップ２５４に進む。

【００７５】

ステップ２５４において、ＧＧＧ１６は、移動局２４のロケーションを更新するためにＧＳＭ　ＨＬＲ３４に更新ロケーションメッセージを送り、制御フローはステップ２５６に進む。ステップ２５６において、ＧＳＭ　ＨＬＲ３４は、移動局２４のＧＳＭ加入者プロファイルをＧＧＧ１６の中のＧＳＭ　ＬＲ５０に送る。制御フローはステップ２５８に

進む。

【００７６】

ステップ２５８において、ＧＧＧ１６はＧＳＭ加入者プロファイルをＣＤＭＡ加入者プロファイルに関連付けし、資格ディレクティブ（a Qualification Directive）中のＣＤＭＡプロファイルをＣＤＭＡ　ＭＡＣ４６に送り、制御フローはステップ２６０に進む。資格ディレクティブは、移動局２４が資格を与えられたこと、即ちＧＳＭ　ネットワーク１４と通信する権限を与えられたことを示す。もし、前記移動局２４が資格を与えられなければ、そのときは移動局２４はＧＳＭネットワーク１４（示されておらず）と通信する権限を与えられない。一実施例において、ＧＧＧ１６はＣＤＭＡ　ＭＳＣ４６に「全プロファイル」（”full profile”）を示し、これは、同様に移動局２４に転送され、移動局２４に対し、移動局２４がＳＭＳメッセージを、これに限定されないが、送受信できることを示す。

【００７７】

ステップ２６０において、ＣＤＭＡ　ＭＳＣ４６は資格ディレクティブに応答し、資格ディレクティブ応答をＣＤＭＡ　ＬＲ５２に送り、制御フローはステップ２６２に進む。

ステップ２６２においては、ＧＳＭ加入者プロファイルデータを受信するＧＳＭ　ＬＲ５０に応答し、ＧＧＧ１６は、ＧＳＭ加入者プロファイルデータレスポンスをＧＳＭ　ＨＬＲ／ＡｕＣ３４，３６に送る。

【００７８】

ステップ２６４においては、ステップ２５４におけるＧＧＧ１６からの更新ロケーションメッセージを受信するＧＳＭ　ＨＬＲ３４に応答し、ＧＳＭ　ＨＬＲ３４は、更新ロケーションメッセージに答え、更新ロケーションメッセージレスポンスをＧＳＭ　ＬＲ５０に送るが、この更新ロケーションメッセージレスポンスは、移動局２４のロケーションがＧＳＭ　ＬＲ５０において更新されていることを示している。

【００７９】

認証キー（Authentication Keys）

ＧＧＧがＪ－ＳＴＤ－０３８　ＩＩＦと最も異なるのは、認証のエリアの中においてである。Ｊ－ＳＴＤ－０３８　ＩＩＦでは、ローミング加入者（the roaming subscriber）は二重の加入　－　一つはＡＮＳＩ－４１用で、他はＧＳＭ用　－　が要求されるので、ＡＮＳＩ－４１外国モードにおける加入者を認証するのに標準ＡＮＳＩ－４１技術を使う。それとは違って、ＧＧＧ解決法においては、ＡＮＳＩ－４１外国モードのローミングサービス利用者（roamer）に完全なＡＮＳＩ－４１加入を要求しない。とりわけ、ＭＳかＧＧＧかの何れかがＡＮＳＩ－４１　Ａ－キーを供給されることが必要である。以下では先ず標準ＡＮＳＩ－４１認証機構を説明する。その後ＡＮＳＩ－４１方法の変形例が説明される。

【００８０】

標準ＡＮＳＩ－４１認証（Standard ANSI-41 Authentication）

認証キーを作成する標準ＡＮＳＩ－４１アプローチが図４に描かれている。キー（これは移動局と認証センタのみに知られた秘密のデータである）とＲＡＮＤＳＳＤと呼ばれるランダムな数字とがＣＡＶＥアルゴリズムを使用し処理され、秘密共有データ（ＳＳＤ）と呼ばれる１２８－ビット数字が作成される。この処理は移動局と認証センタとで実行される。ＳＳＤは、認証に使用される６４－ビットＳＳＤ－Ａキーと暗号化に使用される６４－ビットＳＳＤ－Ｂキーとから成る。夫々のシステムアクセスがあると（On each system access）、移動局は、ＳＳＤ－Ａ、ＥＳＮ、ＭＩＮ、認証データ（ＡＵＴＨ＿ＤＡＴＡ　－　システムアクセスのタイプに依存するがＩＭＳＩ＿Ｓかダイアルされたデジット）、それにオーバーヘッドメッセージでＲＡＮによりブロードキャストされたランダムな数字（ＲＡＮＤ）を処理することにより、認証レスポンス（ＡＵＴＨＲ）を生成する。処理は、ＣＡＶＥアルゴリズムを実行することにより再度行われる。移動局は、システムアクセスにおいてＡＵＴＨＲを送信し、認証センター（又は任意に前記ＭＳＣ／ＶＬＲ）が独自に同じ計算を行いその結果と受信されたものとを比較する時に認証を受ける。

【００８１】

ＳＳＤ－ＡとしてのＫｃの使用（Using Kc as SSD-A）

ＧＭＳ認証資格証明情報を使用したＡＮＳＩ－４１ネットワークにおけるＧＳＭ加入者を認証するという目的は、ＳＳＤ－ＡとしてＫｃを使用することにより達成される。一実施例によるＳＳＤ－Ａキー及びＡＵＴＨＲを発生する新方法は図５に示される。ＧＳＭ認証が移動局で又ＧＳＭ　ＡｕＣで実行される時、秘密キーＫｉ（加入者のＳＩＭ及びＧＳＭ　ＡｕＣのみに知られている）とランダムな数字（ＧＳＭ＿ＲＡＮＤ）がＳＲＥＳ及び暗号化キーＫｃを作成するのに使用される。Ｋｃは丁度ＳＳＤ－Ａのように６４ビット長である。従って、Ｋｃは、ＣＡＶＥアルゴリズム使用のＡＵＴＨＲの標準ＡＮＳＩ－４１計算において、ＳＳＤ－Ａ値の代わりに使用され得る。

【００８２】

ＧＧＧは、認証リクエストＩＮＶＯＫＥにおいて、ＧＳＭ　ＡｕＣとＲＡＮＤ、ＥＳＮ、ＭＩＮ及びＡＵＴＨ＿ＤＡＴＡからＧＳＭ認証トリプレット（即ち、ＧＳＭ＿ＲＡＮＤ、ＳＲＥＳ及びＫｃ）を獲得するので、それからは、ＧＧＧは、地上局がＧＳＭ＿ＲＡＮＤを使用し初めて認証された後に、ＡＮＳＩ＿４１方法を使用して地上局を認証するのにＫｃ値をＳＳＤ－Ａ値として使用できる。即ち、ＧＧＧでのＧＳＭ＿ＲＡＮＤ値を使用して地上局がＧＳＭ認証手続きを実行した後は、ＧＧＧと地上局とは共通のＫｃ値を持つ。このＧＳＭ認証は、ＩＳ－６３７ＳＭＳ伝送を使って信号を送るＧＳＭを使用の前記ＡＮＳＩ－４１／ＣＤＭＡ２０００ネットワークにおいて、実行されうる。移動局とＧＧＧとが一度同一のＫｃを持てば、その後はこの値はＳＳＤ－Ａとして使用され得、標準ＡＮＳＩ－４１方法は移動局を認証するものとして使用され得る。ＡＮＳＩ－４１認証技術を使用する利点は、よりよい送信効率である。このアプローチは又、ＧＳＭ資格証明情報を使用するＡＮＳＩ－４１ネットワークにおいて移動局を認証するという目的を満たす、ということに注目して下さい。

【００８３】

ＳＳＤ共有付認証（Authentication with SSD sharing）

図３の動作シナリオの期間、ＧＧＧにおけるＡＮＳＩ－４１は認証責任を保有する。サービスを行うＭＳＣ／ＶＬＲは、ＧＧＧにおけるＡＮＳＩ－４１　ＨＬＲ／ＡＣへの認証リクエストＩＮＶＯＫＥを用いた各異動局のアクセス試み（例：登録、発信、ページリスポンス及びフラッシュ）に対し応答する責任を負う。このアプローチは最大のセキュリティを提供するが、このトレードオフとしてＡＮＳＩ－４１　ＭＳＣ／ＶＬＲとＧＧＧとの間の送信通話量がより多くなる。

【００８４】

ＭＳＣ／ＶＬＲ－ＨＬＲ／ＡＣ送信通話量を軽減するため、サービスを行うＭＳＣ／ＶＬＲにＡＣが認証責任を分配することを許可する方法が下記に説明される。図４を参照して説明されたように、もしＫｃ値がＳＳＤ－Ａの代わりに使用されるのであれば、ＧＧＧによるＧＳＭ１ｘ解決に対しＳＳＤ共有が適用される。本セクションの残りの部分で、ＳＳＤ共有がどのように行われるかが説明される。

【００８５】

ＳＳＤ更新（SSD update）

図６は、一実施例に従い、ＧＧＧが、サービスを行うＭＳＣ／ＶＬＲと共有されるＳＳＤを更新する、成功したＳＳＤ更新手続の情報フローを示している。このシナリオの初期条件は、ＧＧＧがサービスを行うＭＳＣ／ＶＬＲとこれまでにＳＳＤを共有しており、又、ＭＳがシステムアクセスを実行する時にＭＳＣ／ＶＬＲがＭＳを認証することである。

【００８６】

次の手続きは、この情報フローを説明する：

ステップ５０１において、ＧＧＧは、ＭＩＮ、ＥＳＮ、及びＮＯＳＳＤのパラメータと共にＡＮＳＩ－４１　ＭＳＣ／ＶＬＲへの認証ディレクティブ（ＩＳ４１＿ＡＵＴＨＤＩＲ）を呼び出すことにより、ＳＳＤの更新を始める。

【００８７】

ステップ５０２において、ＭＳＣ／ＶＬＲは、指定ＭＳ用に所有するＳＳＤを棄て、ＧＧＧへの認証ディレクティブリターンリクエストを呼び出すことにより応答する。ＭＳＣ／ＶＬＲは今、このＭＳの各システムアクセスに対し、ＧＧＧにおけるＨＬＲ／ＡＣへの認証リクエストを呼び出す。

【００８８】

ステップ５０３において、ＧＧＧは、ＭＳ用の呼経歴カウント（ＣＯＵＮＴ）パラメータの現在の数値をリクエストするため、ＭＳＣ／ＶＬＲへのカウントリクエスト（ＩＳ４１＿ＣＯＵＮＴＲＥＱ）を呼び出す。

ステップ５０４において、ＭＳＣ／ＶＬＲは、リクエストされたＣＯＵＮＴパラメータを含んだカウントリクエストリターン結果を使って応答する。

【００８９】

ステップ５０５において、もし、ＧＧＧがＭＳ用の追加のＧＳＭ認証トリプレット（triplets）を有さないのであれば、そのときは、ＧＧＧはＧＳＭ　ＨＬＲへのＭＡＰ＿ＳＥＮＤ＿ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ＿ＩＮＦＯを呼び出す。ＭＳが次回にシステムをアクセスする時、次のステップが起こる。

【００９０】

ステップ５０６において、ＧＳＭ　ＨＬＲは、１セット（少なくとも１つ）の認証トリプレットを含むＭＡＰ＿ｓｅｎｄ＿ａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｉｎｆｏで応答する。

ステップ５０７において、ＭＳが次回にシステムをアクセスする時、次のステップが起こる。

【００９１】

ステップ５０８において、ＳＳＤはもはや共有されていないので、ＭＳＣ／ＶＬＲは、ＭＳシステムアクセスを認証するため、ＧＧＧへの認証リクエスト（ＩＳ４１＿ＡＵＴＨＲＥＱ）を呼び出す。

ステップ５０９において、ＧＧＧのＡＣは、前のステップで受信されたパラメータとＭＳ用に保存されたＫｃの数値（ＳＳＤ－Ａ）とが付与されたＡＮＳＩ－４１認証を実行する。ＡＣは、そのあと、成功したＡＮＳＩ－４１認証を示すため、ＭＳＣ／ＶＬＲへの認証リクエストリターン結果（ＩＳ４１＿ａｕｔｈｒｅｑ）を呼び出す。

【００９２】

ステップ５１０において、ＧＧＧは、ＩＳ４１＿ＳＭＤＰＰ伝送を使うＧＳＭ１ｘ認証リクエストを呼び出すことにより、ＧＳＭ１ｘ認証プロセスを開始する。

ステップ５１１において、ＭＳＣはこのＳＭＳをＭＳに転送する。

ステップ５１２において、ＭＳは、ＧＳＭ認証方法を使用してＳＲＥＳとＫｃとを計算することにより、又、ＩＳ－６３７ＳＭＳ伝送でレスポンス（ＧＳＭ１ｘ　Ａｕｔｈ　Ｒｓｐ）を送ることにより、ＧＳＭ１ｘ認証リクエストに応答する。

【００９３】

ステップ５１３において、ＭＳＣはＳＭＳをＧＧＧに転送し、ＧＧＧは、ＧＳＭ１ｘ中のＳＲＥＳがＧＳＭ　ＨＬＲ／ＡｕＣから受信の数値に一致する（match）ことを確認する（validate）。このステップでＭＳへのＳＳＤ更新が完了する。

ステップ５１４において、ＭＳによる次のシステムアクセスがあると、ＭＳＣ／ＶＬＲはＧＧＧへの認証リクエスト（ＩＳ４１＿ＡＵＴＨＲＥＱ）を呼び出す。

【００９４】

ステップ５１５において、ＧＧＧにおけるＡＣは、前のステップで受信したパラメータと該ＭＳ用に保存されたＫｃ（ＳＳＤ－Ａ）の数値とが付与されたＡＮＳＩ－４１認証を実行する。ＡＣはそのあと、成功したＡＮＳＩ－４１認証を示すため、ＭＳＣ／ＶＬＲへの認証リクエストリターン結果を呼び出す。ＳＳＤパラメータは又、ＭＳＣ／ＶＬＲとＳＳＤを共有するように含まれている。

【００９５】

ＳＳＤ共有付初期登録（Initial registration with SSD sharing）

図７は、一実施例に従う、ＳＳＤ共有用に修正された初期登録シナリオを示す。図７で示される情報フローは、ステップ６１９まで、図３Ａ及び３Ｂのフローチャートで示される情報フローと似ている。

【００９６】

ステップ６０１において、初期登録シナリオは、ＭＳが登録システムアクセスを実施する時に始まる。

ステップ６０２において、ＡＮＳＩ－４１　ＭＳＣ／ＶＬＲは、ＧＧＧ中のＨＬＲ（ＧＳＭ１ｘ　ＭＳ用ＨＬＲ）への認証リクエスト（ＩＳ４１＿ＡＵＴＨＲＥＱ）を呼び出す。このＡＵＴＨＲＥＱ中の関連パラメータはＭＩＮ、ＥＳＮ、及びＣＯＵＮＴである。ＧＧＧはＥＳＮの数値を保存し、ＣＯＵＮＴの数値をデータベース中の数値と比較する。

【００９７】

ステップ６０３において、ＧＧＧは、対応するＧＳＭ　ＩＭＳＩを入手するためそのデータベース中のＭＩＮを調べ、ＧＳＭ　ＨＬＲ／ＡｕＣへのＭＡＰ＿ＳＥＮＤ＿ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ＿ＩＮＦＯを呼び出す。

ステップ６０４においては、ＧＧＧは、成功した認証を示すＭＳＣ／ＶＬＲへの認証リクエストリターン結果（ＩＳ４１＿ａｕｔｈｒｅｑ）を呼び出し、タイマ、ＴＲＥＧをスタートさせる。

【００９８】

ステップ６０５においては、成功した認証を示すＩＳ４１＿ａｕｔｈｒｅｑを受信すると、ＭＳＣ／ＶＬＲは、ＧＧＧ中のＨＬＲへの登録通知（ＩＳ４１＿ＲＥＧＮＯＴ）を呼び出す。

ステップ６０６において、もしＧＧＧがＴＲＥＧの終了する前に（このシナリオにおけるように）ＩＳ４１＿ＲＥＧＮＯＴを受信すれば、そのときそれは、ＳＭＳのみ（SMS only）を許可するプロファイル マクロ命令付き（with a profile macro）の登録通知リターン結果（ＩＳ４１＿ｒｅｇｎｏｔ）により応答する。ＳＭＳのみは下記のとおり特定される。

【００９９】

ＳＭＳ＿ＯｒｉｇｉｎａｔｉｏｎＲｅｓｔｒｉｃｔｉｏｎ＝「全許可」（”allow all”）

ＳＭＳ＿ＴｅｒｍｉｎａｔｉｏｎＲｅｓｔｒｉｃｔｉｏｎ＝「全許可」

ＯｒｉｇｉｎａｔｉｏｎＩｎｄｉｃａｔｏｒ＝「単一デレクトリ番号」（"single directory number" （例、発表を行う）

ステップ６０７において、ＩＳ４１＿ｒｅｇｎｏｔを受信すると、ＭＳＣ／ＶＬＲはＭＳに登録許可を送る。

【０１００】

ステップ６０８において、ＧＧＧはＧＳＭ　ＨＬＲ／ＡｕＣから、一又はそれ以上の認証トリプレットを含んだＭＡＰ＿ｓｅｎｄ＿ａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｉｎｆｏを受け取る。

ステップ６０９において、ＧＧＧがＭＳＣ／ＶＬＲ（６）にＩＳ４１＿ｒｅｇｎｏｔを送るのに成功し、又ＧＳＭ　ＨＬＲ／ＡｕＣ（８）からＭＡＰ＿ｓｅｎｄ＿ａｕｔｈｅｎｔｉｃａｔｉｏｎ＿ｉｎｆｏを受け取るのに成功した後に、それはＩＳ４１＿ＳＭＤＰＰ伝送を使用して前記ＧＳＭ１ｘ認証リクエスト（ＧＳＭ１ｘ　Ａｕｔｈ　Ｒｅｑ）メッセージを送る。

【０１０１】

ステップ６１０において、ＭＳＣはこのＳＭＳをＭＳに転送する。

ステップ６１１において、ＭＳは、ＧＳＭ認証方法を使用しＳＲＥＳ及びＫｃを計算することにより、又、ＩＳ－６３７　ＳＭＳ伝送を使用しレスポンス（ＧＳＭ１ｘ　Ａｕｔｈ　Ｒｓｐ）を送ることにより、ＧＳＭ１ｘ認証リクエストに応答する。

【０１０２】

ステップ６１２において、ＭＳＣはＳＭＳをＧＧＧに転送し、ＧＧＧは、ＧＳＭ１ｘ

Ａｕｔｈ　Ｒｓｐ中のＳＲＥＳがＧＳＭ　ＨＬＲ／ＡｕＣから受領の数値と合うことを確証する（validate）。

ステップ６１３において、ＧＧＧは、ＭＳのロケーションを更新するため、ＧＳＭ　ＨＬＲへのＭＡＰ＿ＵＰＤＡＴＥ＿ＬＯＣを呼び出す。

【０１０３】

ステップ６１４において、ＧＳＭ　ＨＬＲは、加入者プロファイルを送るため、ＧＧＧ中のＧＳＭ　ＶＬＲへのＭＡＰ＿ＩＮＳＥＲＴ＿ＳＵＢ＿ＤＡＴＡを呼び出す。

ステップ６１５において、ＧＧＧは、ＧＳＭ加入者プロファイルのＡＮＳＩ－４１加入者プロファイルへの関連付けを行い（map）、クオリケーションディレクティブ（ＩＳ４１＿ＱＵＡＬＤＩＲ）を呼び出すことによりこのＡＮＳＩ－４１プロファイルをＭＳＣ／ＶＬＲに送る。

【０１０４】

ステップ６１６において、ＭＳＣ／ＶＬＲはステップ６１５のクオリケーションディレクティブに応答する。

ステップ６１７において、ＧＧＧはステップ６１４のＭＡＰ＿ＩＮＳＥＲＴ＿ＳＵＢ＿ＤＡＴＡに応答する。

ステップ６１８において、ＧＳＭ　ＨＬＲはステップ６１３のＭＡＰ＿ＵＰＤＡＴＥ＿ＬＯＣに応答する。

【０１０５】

ステップ６１９において、ＭＳによる次のシステムアクセスがあると、以下のステップが発生する。

ステップ６２０において、ＭＳＣ／ＶＬＲ　ＶＬＲは、ＧＧＧへの認証リクエスト（ＩＳ４１＿ＡＵＴＨＲＥＱ）を呼び出す。

ステップ６２１において、ＧＧＧ中のＡＣは、前のステップで受信されたパラメータと該ＭＳ用に保存されたＫｃ（ＳＳＤ－Ａ）の数値とが付与されたＡＮＳＩ－４１認証を実行する。ＡＣはその後、成功したＡＮＳＩ－４１認証を示すため、ＭＳＣ／ＶＬＲへの認証リクエストリターン結果（ＩＳ４１＿ａｕｔｈｒｅｑ）を呼び出す。ＳＳＤパラメータは又、ＭＳＣ／ＶＬＲとＳＳＤを共有するために含まれる。

【０１０６】

共有ＳＳＤ付の新ＭＳＣ／ＶＬＲでの登録（Registration at new MSC/VLR with SSD sharing）

図８は、一実施例に従う、ＳＳＤ共有が許可される時の新しいＭＳＣ／ＶＬＲでの成功した登録用の情報フローを示す。

【０１０７】

ステップ７１５において、ＭＳによる次のシステムアクセスがあると、以下のステップが発生する。

ステップ７１６において、ＭＳＣ／ＶＬＲ　ＶＬＲは、ＧＧＧへの認証リクエスト（ＩＳ４１＿ＡＵＴＨＲＥＱ）を呼び出す。

ステップ７１７においては、ＧＧＧ中のＡＣは、前のステップで受信されたパラメータと該ＭＳ用に保存されたＫｃ（ＳＳＤ－Ａ）の数値とが付与されたＡＮＳＩ－４１認証を実行する。ＡＣはその後、成功したＡＮＳＩ－４１認証を示すため、ＭＳＣ／ＶＬＲへの認証リクエストリターン結果（ＩＳ４１＿ａｕｔｈｒｅｑ）を呼び出す。ＳＳＤパラメータは又、ＭＳＣ／ＶＬＲとＳＳＤを共有するために含まれる。

【０１０８】

暗号化（Ciphering）

ＧＳＭ暗号化は成功したＧＳＭ認証に基づく。認証のためにＭＳＮによりＭＳに送られたＲＡＮＤ値は、ＧＳＭ　Ｋｃの生成においても又使用される。ＲＡＮＤ値は、Ｋｃ数値を生成するためＳＩＭに送られる。一実施例においては、本技術分野において知られているＧＳＭ　Ａ８　アルゴリズムがＫｃ数値を生成するために使用される。ＳＩＭは、大量暗号化（Ａ８を使用）のためＫｃをＭＳに戻す。Ａ３とＡ８は認証及びキー発生機能であ

る。

【０１０９】

認証手続きの概要（Outline of Authentication Procedure）

図９は、一実施例に従う、ＧＳＭ移動局用認証手続きの概要を示す。図９は、ＧＳＭ移動局によって使用される認証プロセスの概要である。

ＭＳＮ９０２はランダム数字ＲＡＮＤと共に認証リクエスト９０４をＭＳ９０６に送る。ＲＡＮＤは、ＭＳ９０６によってＧＳＭ　ＳＩＭカード９０８に送られる。図９のＲＡＮＤは図４の中で示されるＧＳＭ＿ＲＡＮＤと同じであることに注意して下さい。

【０１１０】

ＭＳ９０６はＧＳＭ　ＳＩＭカード９０８とインターフェースがとられている。実施例において、ＧＳＭ　ＳＩＭカードは取り外し可能である。或いは、ＧＳＭカードはＭＳ９０６に一体化される。一実施例においては、ＧＳＭ　ＳＩＭ９０８は、ＭＳＮ９０２に送られるＳＲＥＳを計算するためにＧＳＭ認証アルゴリズムを使用する。

【０１１１】

一実施例においては、ＭＳ９０６は、ＧＳＭ認証方法を使用してＳＲＥＳとＫｃを計算することにより、又、ＳＲＥＳ付きの認証レスポンスをＭＳＮ９０２に送ることにより、認証リクエスト９０４に応答する。

ＭＳＮ９０２は、ＧＳＭ　ＳＩＭ９０８からＭＳＮ９０２に戻されたＳＲＥＳをベリファイする（verify）。ＭＳＮは、ＧＳＭ　ＳＩＭカード９０８により戻されたＳＲＥＳがＧＳＭ　ＡｕＣ（示されておらず）によってそれに提供されたＳＲＥＳと一致することをベリファイする。

【０１１２】

キー生成（Key Generation）

図１０は、ＧＳＭネットワーク中のＧＳＭ　ＭＳでのＧＳＭキー生成を示す。図１１は、ＣＤＭＡネットワーク中のＣＤＭＡ　ＭＳでのＣＤＭＡキー生成を示す。

一実施例に従い、システムは、ＣＤＭＡ　ＲＡＮをＧＳＭコアネットワークにシームレスに統合する（seamlessly integrate）。これは、ＣＤＭＡ　ＲＡＮをＧＳＭコアネットワークに結合するＧＳＭ　ＭＳＮを使用することにより達成される。暗号化デザインがＧＳＭとＣＤＭＡ　Ｋｅｙ生成の両アルゴリズムを組み合わせる。一実施例においては、音声通話をスクランブルするためＰＬＣのような拡散符号系列（spreading sequence）を使用する。一実施例においては、ＧＳＭキー生成はＡ５／１－暗号化アルゴリズムを使用する。一実施例においては、ＧＳＭキー生成はＡ５／２を使用する。

【０１１３】

一実施例においては、ＧＳＭネットワークの中で加入の移動局、即ち、ＧＳＭネットワークからＫｉへのアクセス権を有する移動局、がＣＤＭＡネットワークの中でローミング出来、ＧＳＭ契約に従い認証されることが出来、又、移動局により送受信されるメッセージが暗号化されることが出来るように、システムは、図１０のＧＳＭキー生成を図１１のＣＤＭＡキー生成に結合させる。従って、ＧＳＭ　ＳＩＭを備えた移動局はＣＤＭＡネットワークにおいてスムーズに（seamlessly）動作する。

【０１１４】

一実施例に従い、図１０は、ＧＳＭ認証及びプライバシ（privacy）のために使用されるＧＳＭキー生成プロセスを示す。図１０は、ＧＳＭの状況のもとで、どのようにＧＳＭ認証及び暗号化が機能するかを説明する。

ＲＡＮＤ１００２とＫｉ１００４は２つのアルゴリズム、Ａ３　１００６とＡ８　１００８に入力される。これら２つの要素は２つの他の要素、ＳＲＥＳ１０１０とＫｃ１０１２を生成する。ＳＲＥＳ１０１０は認証パラメータである。認証プロセスの間に、ネットワークは、ＳＩＭ又は認証センタから戻ってくる、ＳＲＥＳを有するレスポンスを入手する。ネットワークはＳＲＥＳに基づき移動局を認証する。

【０１１５】

ＧＳＭプライバシは音声パケットの暗号を意味する。ボイストラフィック（voice traf

fic）１０１４から、全ての音声フレームが暗号化され、他の装置が音声フレームをデコードするのを禁止する。他の装置はＫｃへのアクセス権を有さないので前記音声フレームをデコードできない。

【０１１６】

Ａ８　１００８は暗号化キーであるＫｃを生成する。Ｋｃは音声暗号化（voice ciphering）を行うのに使用される。Ｋｃとスピーチ符号化（speech encoding）用の多数のビットを提供するボイストラフィック要素１０１４とは、アルゴリズムＡ５／１又はＡ５／２　１０１６を使用しお互いに結合される。Ａ５／１又はＡ５／２アルゴリズム１０１６はＧＳＭプライバシ用のＧＭＳ暗号化を可能にする。

【０１１７】

図１１は一実施例に従うＣＤＭＡキー生成を示す。

ＣＤＭＡ認証プロセスは止められる（turned off）。然しながら、ＧＳＭ　ＭＳＮとＭＳは、音声プライバシ（ＶＰ）用の音声プライバシマスク（ＶＰＭ）を生成する。ＧＳＭ　ＭＳとＭＳＮは、信号プライバシ用の高度移動電話メッセージ暗号化アルゴリズム（ＥＣＭＥＡ）キーを生成する。

【０１１８】

ＭＳＮとＭＳは、ＶＰ用のＶＰＭと信号プライバシ用のＥＣＭＥＡキーとを計算するプロセスにおいて、次の要素を取り替える。

ＳＳＤ－ＡがＫｃに取り替えられる。

ＳＳＤ－ＢがＫｃに取り替えられる。

ＥＳＮがＩＭＳＩに取り替えられる。

ネットワークと移動局の両方は、ネットワーク上では決して送られないＡ－キーを有する。ＥＳＮ１１０４、Ａ－キー１１０２、及びＲＡＮＤ１１０６がＣＡＶＥアルゴリズム１１０８に入力される。図１１のこのＲＡＮＤ１１０６は図４のＲＡＮＤと同じである。ＣＡＶＥアルゴリズム１１０８はＳＳＤ１１１０を生成する。ＳＳＤ１１１０は１２８ビットであり、２つの部分、ＳＳＤ－Ａ１１１２とＳＳＤ－Ｂ１１１４とに分割される。ＳＳＤ－Ａ１１１２とＳＳＤ－Ｂ１１１４は、ＣＡＶＥアルゴリズム１１１６、１１１８の２つの他ラング（rung）への入力となる。ラング１１１６の一つは、認証情報、ＡＵＴＨＲ１１２０を計算するのに使用される。これらの認証ビットは全てのアクセスに対し送られる連続したビットであり、それゆえネットワークは、共有された秘密情報を有する移動局以外の他の装置は認証ＡＵＴＨＲを生成出来なかったであろうと判定することが可能である。そのようにして、ネットワークは、移動局が認証されるかどうかを判定することが可能である。同様に、ネットワークは常にＲＡＮＤを送り、これにより移動局はネットワークを判定することが出来る。認証にとって重要なことは、ネットワークが正しい移動局と交信していることを確かめることである。

【０１１９】

ＳＳＤ－Ｂ１１１４はＣＡＶＥアルゴリズム１１１８の別の例示に進む。ＣＡＶＥアルゴリズム１１１８への他の入力は、ＥＳＮ１１１４、認証データ例えばＭＩＮ又は最後にダイアルされたデジット（last dialed digits）１１２２、それにＳＳＤ－Ａを使用して実行されたＣＡＶＥアルゴリズム１１１６の出力を含む。ＣＡＶＥアルゴリズム１１１８は、ＶＰＭＡＳＫ１１２４とＣＭＥＡキー１１２６を生成するため、これらの入力を処理する。ＶＰＭＡＳＫとＣＭＥＡキーはＣＤＭＡパケットを暗号化するのに使用される。丁度、ＧＳＭキー生成によりＫｃが提供され、アルゴリズムＡ５／１及びＡ５／２がＫｃを用いて実行されたように、ＣＤＭＡキー生成によりＳＳＤ－Ｂが提供され、ＣＡＶＥアルゴリズムがＳＳＤ－Ｂを用いて実行される。両ケースにおいて、暗号コード（ciphers）が暗号化（encryption）のために使用される。

【０１２０】

一実施例において、システムは、図１０のＧＳＭキー生成と図１１のＣＤＭＡキー生成とを結び付ける。図１０におけるのと丁度同じように、ランダムな数字がＧＳＭ　ＳＩＭを備えた移動局に送られ、移動局はＫｃを生成する。図１１のＣＤＭＡキー生成において

、ＫｃがそのあとＳＳＤ－Ａ及びＳＳＤ－Ｂの代わりに使われる。その後、移動局は、図１１のＣＤＭＡキー生成において示されるのとまさに同じように動作する。

【０１２１】

このように、動作のハイブリッドモード、即ち、ＣＤＭＡネットワークにローミングするＧＳＭ　ＳＩＭを備えた移動局においては、移動局はランダム数字を使用するＫｃ及びＳＲＥＳを生成する。一度Ｋｃが生成されると、ＫｃはＳＳＤ－Ａ及びＳＳＤ－Ｂの代わりに使われ、ネットワークと移動局の両方が有効な認証データ及び暗号を持つことを可能にする。

【０１２２】

登録の間のメッセージフロー（Message Flow During Registration）

図１２－１４は、ハイブリッド認証モード、即ち、ＣＤＭＡネットワークにローミングするＧＳＭ　ＳＩＭを有する移動局、のための実施例に従うメッセージフローを示す。ＭＳＮは、ＣＤＭＡネットワークにおけるＭＳＣと同じレベルにある。別の実施例においては、ＧＧＧを備えたネットワークにおいて同一の手続きが続く。ＧＧＧ構成において、ネットワークは、ＭＳＮの代わりにＣＤＭＡ　ＭＳＣを有し、又、ネットワークは図６－８において示されたのとまさに同じようにＧＧＧを含む。

【０１２３】

図１２は、実施例に従う、登録の間のメッセージフローを示す。図１２は、移動局が初めて認証される時のメッセージフローを描写する。

図１２は、移動局が丁度スイッチを入れられていたことを前提としている。移動局は登録メッセージ１２０２を送り、この登録メッセージは、ロケーションアップデートリクエスト１２０４の一部分としてＭＳＮに送られる。登録メッセージは、ＢＴＳ／ＢＳＣとＭＳＮとの間のインターフェース上でロケーションアップデートリクエストに変換される。ＢＴＳ／ＢＳＣとＭＳＮとの間のインターフェースは、ＣＤＭＡ２０００標準規格により定義されるＡ－インターフェースと呼ばれる。。

【０１２４】

ロケーションアップデートリクエストがＭＳＮにより受信されて後、ＭＳＮはＭＡＰ＿ＳＥＮＤ＿ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ　Ｉｎｆｏ１２０６をＧＳＭ　ＨＬＲ／ＡｕＣ１２０６に送る。ＭＳＮは、移動局用の認証情報を取得するために、ＭＡＰ＿ＳＥＮＤ＿ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ　Ｉｎｆｏ１２０６をＧＳＭ　ＨＬＲ／ＡｕＣ１２０６に送る。ＭＳＮは、ＭＡＰ＿ＳＥＮＤ＿ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ　ＲＥＳＰＯＮＳＥ　１２０８の中で要求されているような、ＳＲＥＳ、ランダム数字、Ｋｃ、及び他の認証パラメータを、ＧＳＭ　ＨＬＲ／ＡｕＣから取得する。その後に続く認証に対しては、ＭＳＮは異なる認証パラメータを取得できる。

【０１２５】

トリプレット（ＳＲＥＳ、ランダム数字、及びＫｃ）がＭＳＮに保存される。ＭＳＮは、そのとき、ＧＳＭ認証リクエスト１２１０をＢＴＳ／ＢＳＣに送る。ＳＭＳは、前に説明したように、ランダム数字を封入する（encapsulate）のに使用される。ランダム数字は、データバーストメッセージ（data burst message）、Ａｕｔｈ リクエストデータバースト１２１２を通して移動局に伝わる。移動局は、Ａｕｔｈ　レスポンスデータバーストを備えたＡｕｔｈ リクエストデータバースト１２１２に応答する。

【０１２６】

ランダム数字は、移動局によりＳＩＭに送られる。ＳＩＭは、そのあと、ＳＲＥＳを戻し、Ｋｃを計算する。ＳＲＥＳは、認証レスポンス１２１６の中でＭＳＮに戻される。ＭＳＮは、そのあと、ＡｕＣから受信されたＳＲＥＳをモバイルが送るＳＲＥＳと比較でき、又、もし、２つのＳＲＥＳが合えば、そのときは、ＭＳＮは、移動局は本物であると判定し、移動局は認証される。

【０１２７】

ＭＳＮは、アップデートロケーションリクエスト１２１８によりＧＳＭ　ＨＬＲを更新する。ＧＳＭ　ＨＬＲは、アップデートロケーションレスポンス１２２０によりアップデ

ートロケーションリクエスト１２１８に応答する。アップデートロケーションレスポンス１２２０を受信後、ＭＳＮは、ロケーションアップデートアクセプト１２２２をＢＴＳ／ＢＳＣに送る。ＢＴＳ／ＢＳＣは登録許可命令を移動局に送り、移動局はＧＳＭネットワークを使用することを許可される。

【０１２８】

図１２のメッセージフローの終わりにおいて、移動局は、ＡｕＣがＭＳＮに送るＫｃと同じＫｃを有する。ＭＳＮと移動局の両方が同一のＫｃを有し、両方は暗号化の準備が出来ている。図１３及び図１４は、暗号化を可能とするコールフロー（the call flows）である。

【０１２９】

一実施例において、最適プライバシを提供するために、ＧＳＭ認証は登録後直ちに実行される。一実施例においては、ＭＳが認証プロセスをパスした後、モバイルが終点の（ＭＴ）コール（a mobile terminated (MT) Call）用のページレスポンスの中で、或いは、モバイルが起点の（ＭＯ）コール（a mobile originated (MO) Call）用のオリジネーションメッセージの中で、音声及び通信プライバシが要求される。

【０１３０】

もし、電源が入れられ、登録が完了する前に発信又は受信が行われる場合は、次の二つのケースが存在する。

【０１３１】

モバイル起点コール中のメッセージフロー（Message Flow During Mobile Originated Call[）

図１３は、一実施例に従う、ＭＯコール中のメッセージフローを示す。ＥＮＣＲＹＰＴＩＯＮ＿ＩＮＦＯＲＭＡＴＩＯＮフィールドのＰＲＩＶＡＣＹ＿ＭＯＤＥ＿ＲＥＱＵＥＳＴメッセージにおけるコールセットアップ中に（during call setup）、ＭＳＮに、ＶＰＭ及びＥＣＭＥＡキーをＢＴＳまで送らせることが必要である。

【０１３２】

図１３は２つの部分に分けられることが可能である。認証手続きの上側の部分はＣＤＭＡコールセットアップである。モバイルは開始（an origination）１３０２を送り、ＢＴＳ／ＢＳＣは、ＢＴＳ／ＢＳＣが開始メッセージを受信したことを示す、確認命令（an acknowledgment order）１３０４を送る。開始メッセージは必ずしも確実に送られないかもしれないので、確認命令１３０４は必要とされる。

【０１３３】

ＢＴＳ／ＢＳＣは、コールを始めるため、ＭＳＮにＣＭ＿Ｓｅｒｖｉｃｅ＿Ｒｅｑｕｅｓｔ１３０６を送る。このリクエストの結果、ＭＳＮは、モバイルに割り当てられたチャンネルを入手するため、割当リクエスト１３０８をＢＴＳ／ＢＳＣに送る。ＢＴＳ／ＢＳＣはＣＨ割当１３１０を移動局に送る。

【０１３４】

移動局は、通信チャンネル（ＴＣＨ）プリアムブル（a traffic channel (TCH) preamble）１３１２をＢＴＳ／ＢＳＣに送る。ＴＣＨプリアムブル１３１２は、移動局がノイズを作りつつある、ことを意味する。ＢＴＳ／ＢＳＣは移動局に注意して聞き、移動局を捕らえるように試みる（attempts to acquire the mobile station）。ＢＴＳ／ＢＳＣは、移動局を捕らえ次第、フォーワード（ＦＷ）Ａｃｋ命令（a forward (FW) Ack Order）１３１４を移動局に送る。ＦＷ　Ａｃｋ命令１３１４は、ＢＴＳ／ＢＳＣがＴＣＨプリアムブル１３１２を受領したこと示す。

【０１３５】

サービス接続１３１６がＢＴＳ／ＢＳＣから移動局に送られる。ＢＴＳ／ＢＳＣからのサービス接続は、移動局に、移動局は今サービス中にあり準備が出来ていることを示す。移動局は、ＢＴＳ／ＢＳＣへのサービス接続完了１３１８によりサービス接続を確認し、このＢＴＳ／ＢＳＣはこのあと、ＢＴＳ／ＢＳＣからＭＳＮへの割当完了１３２０の形に変える（translate）。この時点で、ＭＳＮはモバイルへの通信チャンネルを有する。

【０１３６】
ＩＡＭ１３２２とＡＣＭ１３２４は、ＰＳＴＮと共に反対側にリンクをセットアップする電話ネットワークに信号を送るＳＳ７である。移動局はコールしている（making a call）。ＩＡＭメッセージはコールされた装置を「鳴らす」。ＡＣＭは、ＳＳ７コールのセットアップ完了である。
通信チャンネルがセットアップされた後、ＧＳＭ認証手続はオプションとして実行されることが可能である。オプションとしてのＧＳＭ認証手続きは、オーバーヘッドチャンネル若しくは通信チャンネルで実行できる。モバイルが起点のコールに対し、ＭＳＮは、オプショナルとして認証手続きを実行することを決定できる。しかし、たとえＭＳＮが認証手続きを実行しなくとも、そのときは、移動局が生成した最後のＫｃはＭＳＮ　Ｋｃと同じＫｃである。Ｋｃは、ＧＳＭ認証手続きが実行される時のみ変わる。
【０１３７】
一度ユーザがコールの他端で答えると、ＰＳＴＮはＡＮＭ１３２６をＭＳＮに送る。ＡＮＭ１３２６は、コールされた装置が取り上げられたということを合図する、ＳＳ７によるアンサーメッセージである。ユーザがコールの他端で答えた後、ＭＳＮは、ＢＴＳ／ＢＳＣに対し、プライバシモードメッセージで、暗号化を開始するように指示する、計算されたロングコードマスクである、プライバシモード１３２８を動作することを決定できる。ＭＳＮは、ＢＴＳに対し、ＶＰＭ　Ｍａｓｋ及びＣＭＥＡキーを使用するように指示し、又、プライバシーモードメッセージでこれらのキーを送っている。
【０１３８】
ＶＰＭ　Ｍａｓｋ及びＣＭＥＡキーは、ＣＤＭＡ２０００標準規格において説明されているように使用される。それらは音声パケットを暗号化するのに使用される。プライバシーモードメッセージ１３２８において、ＭＳＮは地上局に暗号化を開始するように指示し、モバイルはリクエストプライバシロングコードトランジションレスポンス（a Request Privacy Long Code Transition Response）１３３２により確認応答する。
【０１３９】
ＢＴＳ／ＢＳＣはＭＳにリクエストプライバシロングコードトランジションオーダ（a Request Privacy Long Code Transition Order）１３３０を送り、移動局はリクエストプライバシロングコードトランジションレスポンス１３３２で応答する。
【０１４０】
リクエストプライバシロングコードトランジションレスポンス１３３２を受信後、ＢＴＳ／ＢＳＣはプライバシモード完了１３３４をＭＳＮに送る。プライバシモードが完了した後は、移動局は、音声フレームが暗号化されていることを意味するスクランブルされた通話状態にある。
【０１４１】
モバイル終点コール中のメッセージフロー（Message Flow During Mobile Terminated Call[）
図１４は、一実施例に従う、モバイルが終点となる（ＭＴ）コール中のメッセージフローを示す。ＭＳＮに、ＥＮＣＲＹＰＴＩＯＮ＿ＩＮＦＯＲＭＡＴＩＯＮフィールドのＰＲＩＶＡＣＹ＿ＭＯＤＥ＿ＲＥＱＵＥＳＴメッセージにおけるコールセットアップ中に（during call setup）、ＶＰＭ及びＥＣＭＥＡキーをＢＴＳに送らせることが必要である。
【０１４２】
図１４は、コールがＰＳＴＮ側で起こるときのプライバシモードの例である。このコールは、この移動局をコールする別の移動局が関係することもあるであろう。ＭＳＮとＰＳＴＮとの間のメッセージは、開始及び終了メッセージをＰＳＴＮに送るのに使用されるＳＳ７メッセージとして規則正しく定義される。
【０１４３】
ＩＡＭ１４０２は、移動局へのコールが開始されている、ということをＭＳＮに示すリクエストである。ＩＡＭに応答してＭＳＮは、モバイルが図１２で定義されたように前に登録されているので、モバイルをさがす（page）。ＭＳＮは、ページングリクエスト１４

０４をＢＴＳ／ＢＳＣに送る。ＧＳＭ認証を使って予め認証されているので、この時点では、モバイルは既にＫｃを有している。

【０１４４】

ＭＳＮからページングリクエストを受信すると、ＢＴＳ／ＢＳＣはジェネラルページ（general page）１４０６を移動局に送る。移動局は、ＢＴＳ／ＢＳＣに送られたページリスポンス１４０８により、ページに対し応答する。ＢＴＳ／ＢＳＣは、ページレスポンス１４１０をＭＳＮに送る。一度ページレスポンス１４１０がＭＳＮにより受信されると、ＭＳＮは、モバイルがそこにありコールを受信できる準備が出来ていることを知る。ＭＳＮはそのあとＢＴＳ／ＢＳＣに割当リクエスト１４１２を送る。割当リクエスト１４１２は、ＢＴＳ／ＢＳＣにモバイル用のチャンネルをセットアップするように示しており、ＢＴＳ／ＢＳＣはモバイルにチャンネルを割り当て、移動局にチャンネル割当１４１４を送る。

【０１４５】

移動局はＴＣＨプリアムブル１４１６をＢＴＳ／ＢＳＣに送る。ＴＣＨプリアムブル１４１６は、ＢＴＳ／ＢＳＣが移動局を確保できるように、モバイルがフォーワードチャンネルに何らかのノイズを作りつつあることを示す。ＢＴＳ／ＢＳＣは、ＴＣＨプリアムブルを受信後に、ＦＷ　Ａｃｋ命令１４１８を移動局に送る。

【０１４６】

ひとたびＢＴＳ／ＢＳＣが移動局を確保すれば、そこにはサービス接続１４２０及びサービス接続完了１４２２が存在する。ＢＴＳ／ＢＳＣはサービス接続１４２０を移動局に送り、移動局は、サービス接続１４２０に対しサービス接続完了１４２２で応答する。

【０１４７】

ＢＴＳ／ＢＳＣは移動局に、Ｉｎｆｏ付きの呼び出し（Ａｌｅｒｔ）１４２４を送る。Ｉｎｆｏ付きの呼び出しは、移動局にベルを鳴らすことを求めるリクエストである。移動局がベルを鳴らすことを開始した後に、割当完了１４２６がＢＴＳ／ＢＳＣからＭＳＮに送られる。割当完了は、ＭＳＮに対し、移動局がベルを鳴らしており、チャンネルが移動局に割り当てられたことを示す。移動局がベルを鳴らしていることをＰＳＴＮに示すＡＣＭ１４２８が、ＭＳＮからＰＴＳＮに送られる。

【０１４８】

ある時点で、ユーザはコールされた移動局を取り、接続命令が移動局からＢＴＳ／ＢＳＣに送られる。その後、ＢＴＳ／ＢＳＣは接続１４３２をＭＳＮに送る。

一度接続が確立されてしまうと、ＧＳＭ認証手続きがオプショナルとして実行されることがある。いつＧＳＭ認証手続きを実行するかはオプショナルであり、従って、例えば、５回のコール毎に一度、或いは１０回のコール毎に一度認証手続きが実行されるということを、認証ポリシは決定出来る（dictate）。ＡｕＣが認証ポリシをＭＳＮに指示し、そのあとは、ＭＳＮはポリシに従うことが出来る。

【０１４９】

認証手続きが実行される時、前述したように同期が取られるであろうＫｃの新しい数値が決定される。プライバシモードリクエスト１４３４、リクエストプライバシロングコードトランジションオーダ１４３６、リクエストプライバシロングコードトランジションリスポンス１４３８、プライバシモード完了１４４０、及びＡＮＭ１４４２が、図１３において説明されたように動作する。ＡＮＭ１４４２がＭＳＮからＰＳＴＮに送られた後に、ＭＳＮは、スクランブルモードで実行するコールを開始する。ＡＮＭは前述同様にアンサーメッセージである。

【０１５０】

ＧＳＭネットワークにおいては、ＧＳＭ　ＭＳＣがいつ認証すべきかを、認証センタがＧＳＭ　ＭＳＣに伝えることに注意してください。ＣＤＭＡネットワークにおいては、ＡｕＣがＭＳＣに対しいつ認証を行うべきかを示すようなマッピング（mapping）は無い。然しながら、混合移動局（a mixed mobile station）、即ち、ＣＤＭＡネットワークの中でローミングを行うＧＳＭ　ＳＩＭを備えた移動局、に対しては、ＧＳＭ認証手続きが、

ＭＳＮがそれを実行することを必要とする時はいつでも、即ち、ＭＳＮの認証ポリシに従い、実行されることがありえる。このように、ＭＳＮは、ＡｕＣによって用意されたポリシを実行することが出来る。

【０１５１】

ここで示され又詳細に説明された特定のＣＤＭＡネットワークとＧＳＭネットワークとの間の暗号化は、この発明の上記説明の目的を達成するのに十分可能であるが、それは本発明の現在好ましい実施例であり、従って本発明により広く考えられた代表的な主題であり、本発明の範囲は、当業者に明らかとなる他の実施例を十分包含し、又、本発明の範囲は、従って、添付の特許請求の範囲以外によっては限定されず、特許請求の範囲においては、要件の単数での参照は明白に記載されなければ「１つ及び唯一１つ」を意味することを意図されておらす、寧ろ「１若しくはそれ以上」を意味するように意図されている、ということが、理解されるべきである。当業者に知られ、又、後で知られるようになる、上記説明された好ましい実施例の要件の全ての構成上の及び機能上の均等物は、参照することにより明らかにここに含まれ、本発明特許請求の範囲により包含されるべく意図されている。更に、本開示における要素、部品、或いは方法ステップは、該要素、部品、或いは方法ステップが特許請求の範囲中で明白に列挙されているかどうかに関係なく、公共に捧げられるべく意図されてはいない。語句「・・・ための手段」を使用して構成要件が明らかに記載されているのでなければ、或いは方法の特許請求の範囲の場合においては、構成要件が「動作」の代わりに「ステップ」として記載されているのでなければ、ここでの特許請求の範囲の要件は、米国特許法３５Ｕ．Ｓ．Ｃ．第１１２条第６パラグラフの規定のもとで解釈されるべきでない。

【０１５２】

方法ステップは、本発明の範囲を逸脱しないで、交換することが可能である。

以下に、本願発明の当初の［特許請求の範囲］に記載された発明を付記する。

［１］

第１ネットワークで加入された移動局（ＭＳ）が第２ネットワークを使用し通信することを可能とする、前記第1ネットワークと前記第２ネットワークとの間の無線通信方法であって、

前記移動局の識別情報を保存し、

前記移動局の前記識別情報に基づき前記第１ネットワークから認証情報を入手し、

キーを作成するために前記第１ネットワークからの前記認証情報を使用し、

前記移動局を認証するために第１アルゴリズムで使用されるＳＳＤ－Ａ（共有秘密データ－Ａ）の代わりに前記キーを用い、そして

前記移動局と前記第２ネットワークとの間のメッセージを暗号化するために第２アルゴリズムで使用されるＳＳＤ－Ｂ（共有秘密データ－Ｂ）の代わりに前記キーを用いることを含む無線通信方法。

【図面の簡単な説明】

【０１５３】

【図１】図１は、一実施例による、モバイル交換ノード（ＭＳＮ）を使用するシステムアーキテクチャのブロック図を示す。

【図２】図２は、一実施例による、ＣＤＭＡネットワークとＧＳＭネットワークと汎用グローバルゲートウェイ（ＧＧＧ）と移動局とを備える、無線通信システムのブロック図を示す。

【図３Ａ】図３Ａは、秘密共有データ（ＳＳＤ）を使用しない一実施例による、ＧＳＭネットワークで加入のＣＤＭＡ移動局を認証するためのフローチャートを示す。

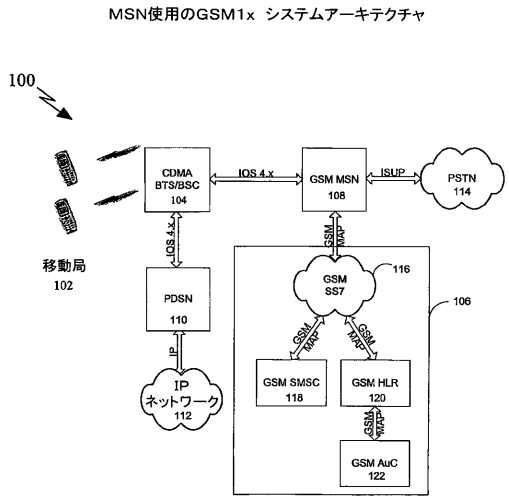
【図３Ｂ】図３Ｂは、秘密共有データ（ＳＳＤ）を使用しない一実施例による、ＧＳＭネットワークで加入のＣＤＭＡ移動局を認証するフローチャートを示す。

【図４】図４は、認証を実現する標準規格ＡＮＳＩ－４１アプローチを描く。

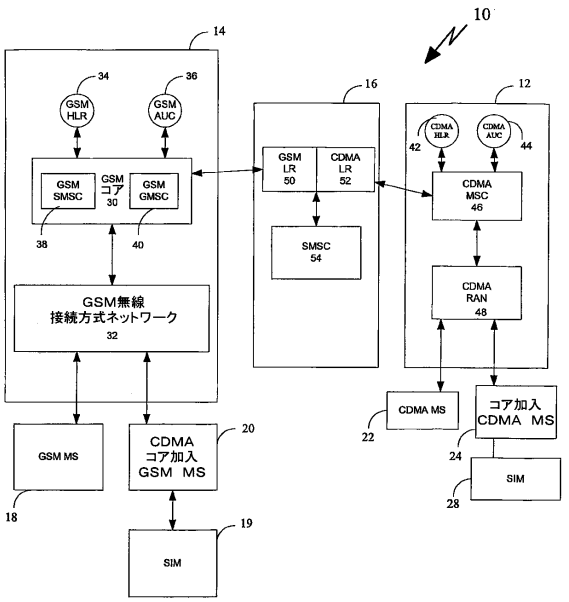
【図５】図５は、一実施例による、ＡＮＳＩ－４１ネットワークにおけるＧＳＭ加入者の認証を示し、ＳＳＤ－ＡとしてＫｃを使用することによりＳＭ認証資格証明情報を使用す

る。
【図６】図６は、一実施例による、成功したＳＳＤ更新手続きのための情報フローを示し、手続きにおいて、ＧＧＧが、サービスを行うＭＳＣ／ＶＬＲと共有するＳＳＤを更新する。
【図７】図７は、一実施例による、ＳＳＤ共有用に修正された初期登録シナリオを示す。
【図８】図８は、一実施例による、ＳＳＤ共有が許可される時の新ＭＳＣ／ＶＬＲへの成功した登録用の情報フローを示す。
【図９】図９は、一実施例による、ＧＳＭ移動局用の認証手続きの概要を示す。
【図１０】図１０は、ＧＳＭネットワークにおけるＧＳＭ　ＭＳでのＧＳＭ キー生成を説明する。
【図１１】図１１は、ＣＤＭＡネットワークにおけるＣＤＭＡ　ＭＳでのＧＳＭ キー生成を説明する。
【図１２】図１２は、実施例による、登録中のメッセージフローを示す。
【図１３】図１３は、実施例による、モバイル起点コール（ＭＯ）中のメッセージフローを示す。
【図１４】図１４は、実施例による、モバイル終点コール（ＭＴ）中のメッセージフローを示す。

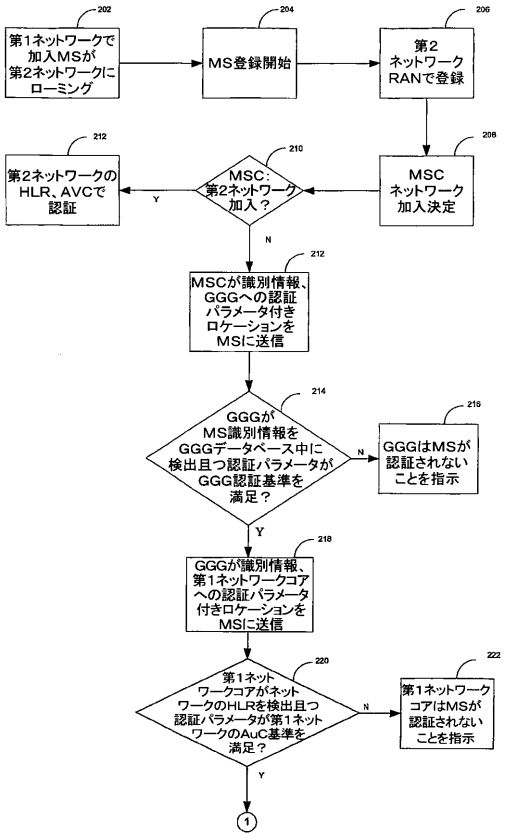
【図１】



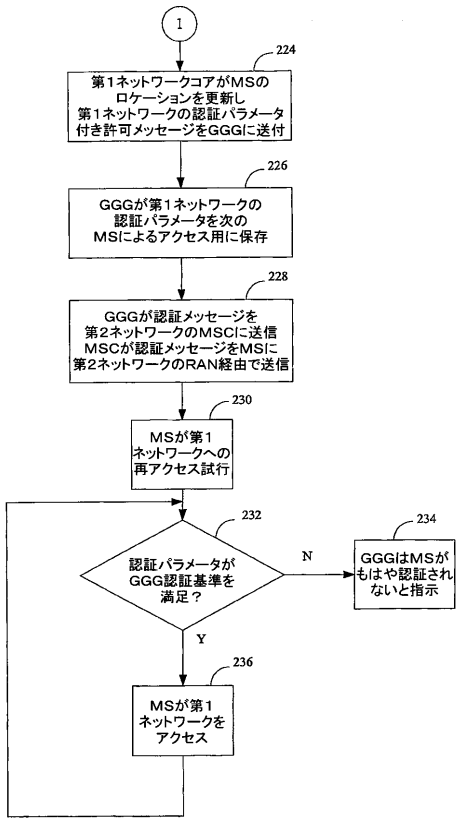
【図２】



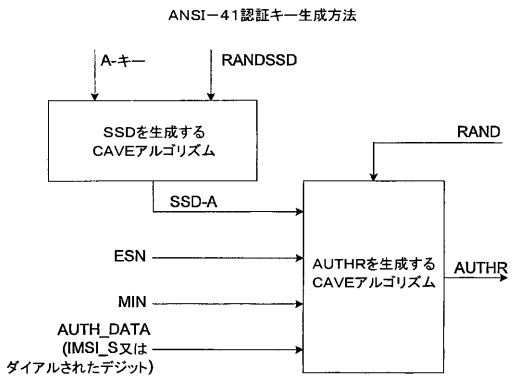
【図３Ａ】



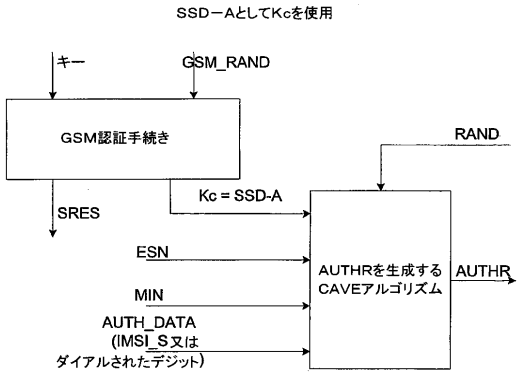
【図３Ｂ】



【図４】

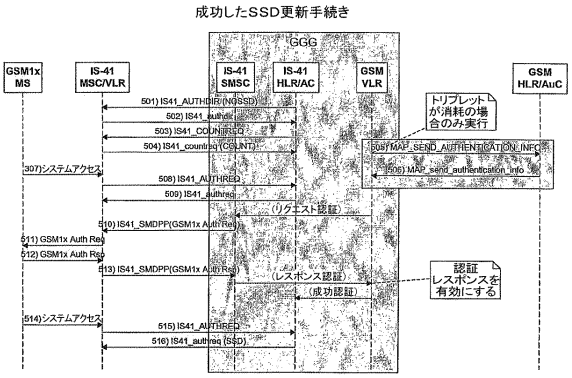


【図５】

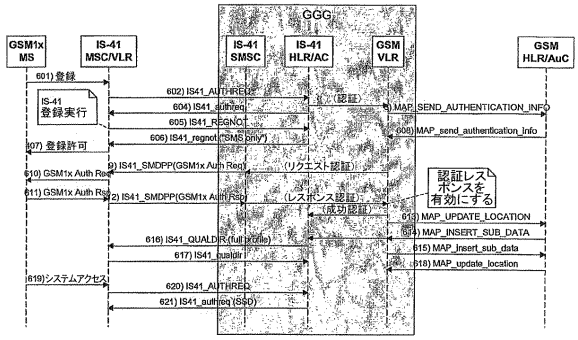


STRES

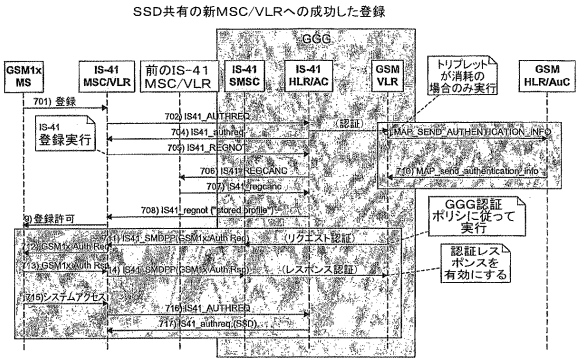
【図６】



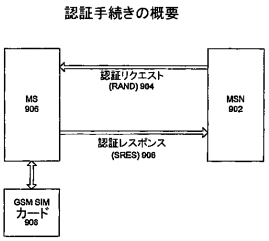
【図７】



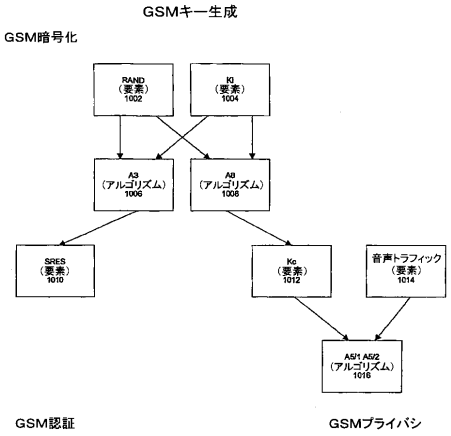
【図８】



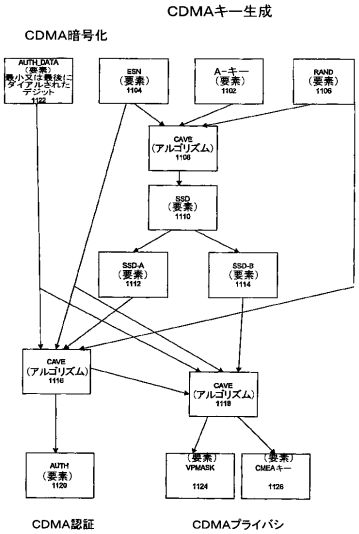
【図９】



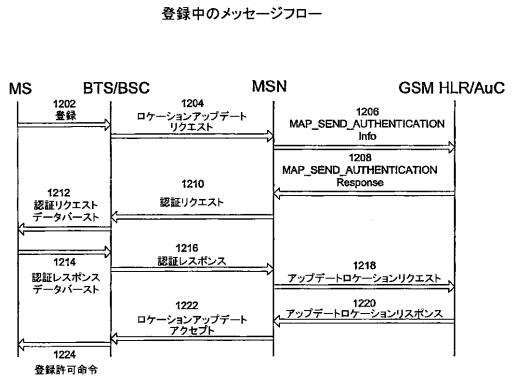
【図１０】



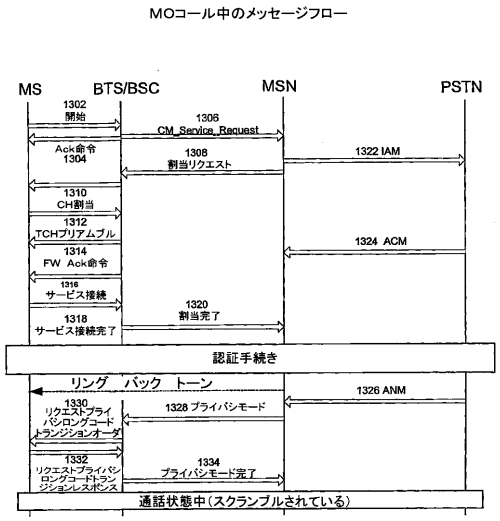
【図１１】



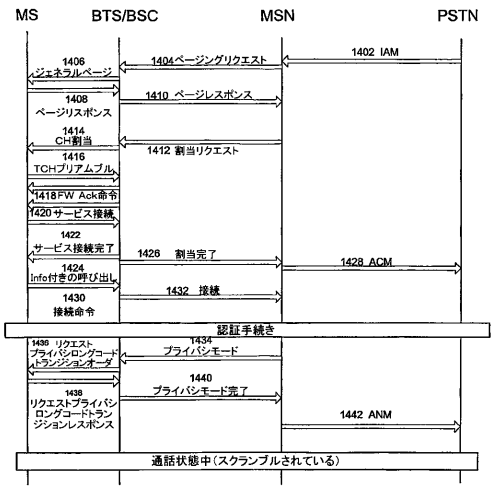
【図１２】


登録中のメッセージフロー
MS
BTS/BSC
MSN
GSM HLR/AuC
1202 登録
1204 ロケーションアップデートリクエスト
1206 MAP_SEND_AUTHENTICATION Info
1208 MAP_SEND_AUTHENTICATION Response
1210 認証リクエスト
1212 認証リクエストデータバースト
1214 認証レスポンスデータバースト
1216 認証レスポンス
1218 アップデートロケーションリクエスト
1220 アップデートロケーションリスポンス
1222 ロケーションアップデートアクセプト
1224 登録許可命令

【図１３】


MOコール中のメッセージフロー
MS
BTS/BSC
MSN
PSTN
1302 開始
1306 CM_Service_Request
Ack命令 1304
1308 割当リクエスト
1322 IAM
1310 CH割当
1312 TCHプリアムブル
1324 ACM
1314 FW Ack命令
1316 サービス接続
1320 割当完了
1318 サービス接続完了
認証手続き
リング バック トーン
1326 ANM
1330 リクエストプライバシロングコードトランジションオーダ
1328 プライバシモード
1332 リクエストプライバシロングコードトランジションレスポンス
1334 プライバシモード完了
通話状態中（スクランブルされている）

【図１４】


MTコール中のメッセージフロー
MS
BTS/BSC
MSN
PSTN
1402 IAM
1404ページングリクエスト
1406 ジェネラルページ
1410 ページレスポンス
1408 ページリスポンス
1414 CH割当
1412 割当リクエスト
1416 TCHプリアムブル
1418 FW Ack命令
1420 サービス接続
1422 サービス接続完了
1426 割当完了
1428 ACM
1424 Info付きの呼び出し
1432 接続
1430 接続命令
認証手続き
1436 リクエストプライバシロングコードトランジションオーダ
1434 プライバシモード
1440 プライバシモード完了
1438 リクエストプライバシロングコードトランジションレスポンス
1442 ANM
通話状態中（スクランブルされている）

フロントページの続き

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100092196
弁理士 橋本 良郎
(74)代理人 100100952
弁理士 風間 鉄也
(72)発明者 ジャイン、ニクヒル、
アメリカ合衆国、カリフォルニア州 ９２１３０、サン・ディエゴ、フェダーマン・レーン ４２９１
(72)発明者 コリンズ、ブルース
アメリカ合衆国、カリフォルニア州 ９２１３１、サン・ディエゴ、アンジェリク・ストリート １１７３０
(72)発明者 ナガライ、サディ・エム.
アメリカ合衆国、カリフォルニア州 ９２１３１、サン・ディエゴ、サイプレス・キャニョン・ロード １１８２０－２

審査官 新田 亮

(56)参考文献 特開２０００－０１３８７３（ＪＰ，Ａ）
特開２００１－００５７８２（ＪＰ，Ａ）
特開平０６－０６９８８２（ＪＰ，Ａ）
特表２００２－５３３０３５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/08
G09C 1/00