

Cisco ITP MAP Gateway による パブリック WLAN の SIM 認証および許可

概要

高速ワイヤレス データ サービスの必要性を認識する Global System for Mobile Communications (GSM) モバイル事業者が増えています。これらの事業者は、既存の 2.5G および将来の第 3 世代携帯電話 (3G) アクセスおよびサービスを補完するものとして、自社のサービスおよびアクセス ポートフォリオへの Wireless LAN (WLAN; ワイヤレス LAN) テクノロジーの導入を決定しています。

このようなサービスへのアクセスには、適切なユーザ認証が不可欠です。このため、シスコシステムズでは、実績ある既存の GSM ベースのユーザ認証と既存の GSM プロビジョニング ファシリティを使用した WLAN 加入者認証の実現に向けた取り組みを開始しました。

認証プロセスは、あらゆるユーザ トランザクションにとって重要です。市場に投入された初期の WLAN システムでは、ユーザ名とパスワードに基づく認証プロセスが使用されていました。当初は Secure Hypertext Transfer Protocol (HTTPS) Web ページを通じて証明書を入力していましたが、これらは後に Extensible Authentication Protocol (EAP; 拡張認証プロトコル) (RFC 2284)、つまり 802.1X ベースのソリューションへと進化しています。EAP (802.1X) を使用することにより、たとえば、GSM ネットワーク内で現在使用されている同様の技術に比べ、より高いエントロピーを持つ共有秘密鍵および暗号鍵交換をサポートする認証方式への移行が促進されます。

WLAN 技術で使われている認証および許可メカニズムと、既存の GSM ベースの認証およびプロビジョニング モデルとを橋渡しする必要性を認識したシスコシステムズは、Cisco IP Transfer Point (ITP) Mobile Application Part (MAP) Gateway 機能を開発しました。Cisco ITP MAP Gateway 機能を使用すると、既存の GSM サービス プロバイダーは Subscriber Identity Mobile (SIM) カードを使用して、802.11 テクノロジーを既存の GSM ネットワークに完全に統合できます。この場合、Cisco ITP MAP Gateway は、シスコのパブリック WLAN ソリューション アーキテクチャの一部となります。

Cisco ITP MAP Gateway 機能によって WLAN SIM 認証および許可が可能になるだけでなく、MAP ベースの付加機能 (ITP Multi-layer Router [MLR]) を導入すれば「SMS ルーティング」なども使用可能になります。ITP Multi-layer Router に関する詳細については、該当するホワイトペーパーを参照してください。



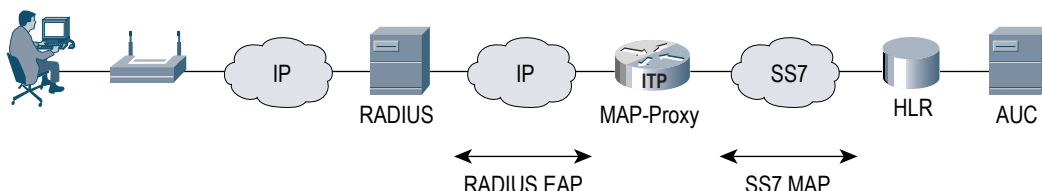
Cisco ITP MAP Gateway ソリューションの概要

Cisco ITP MAP Gateway では、WLAN EAP (802.1X) と GSM SIM 認証メカニズムがトランスペアレントに融合され、モバイル ノードでは、標準的な EAP Remote Access Dial-In User Service (RADIUS) ベースの認証を使用して、GSM Authentication Center (AUC) に対する SIM 認証が実行できるようになります。これによって得られる利点は、GSM 事業者がネットワークに WLAN ホット スポットを導入する場合、すでに GSM サービスに対して提供しているものと同じ加入者プロビジョニング、認証、およびサービス許可の仕組みをそのまま利用できることです。

WLAN クライアントが SIM カードと SIM カードリーダーを備えていれば、Cisco ITP MAP Gateway によって、WLAN ネットワークで使用されている RADIUS ベース認証と GSM ネットワークで使用されている SIM 認証がトランスペアレントに相互接続されます (図 1 を参照)。

- GSM Home Location Register (HLR) 側から見た場合、Cisco ITP は Signaling System 7 (SS7) ネットワーク内の別のノードとして動作します (通常、Home Public Land Mobile Network [HPLMN] ベースの Visitor Location Register [VLR] に相当します。この資料の別項を参照してください)。
- RADIUS サーバ側から見た場合、Cisco ITP は別の RADIUS サーバとして動作します。

図 1
Cisco ITP MAP Gateway により WLAN および GSM の認証を融合

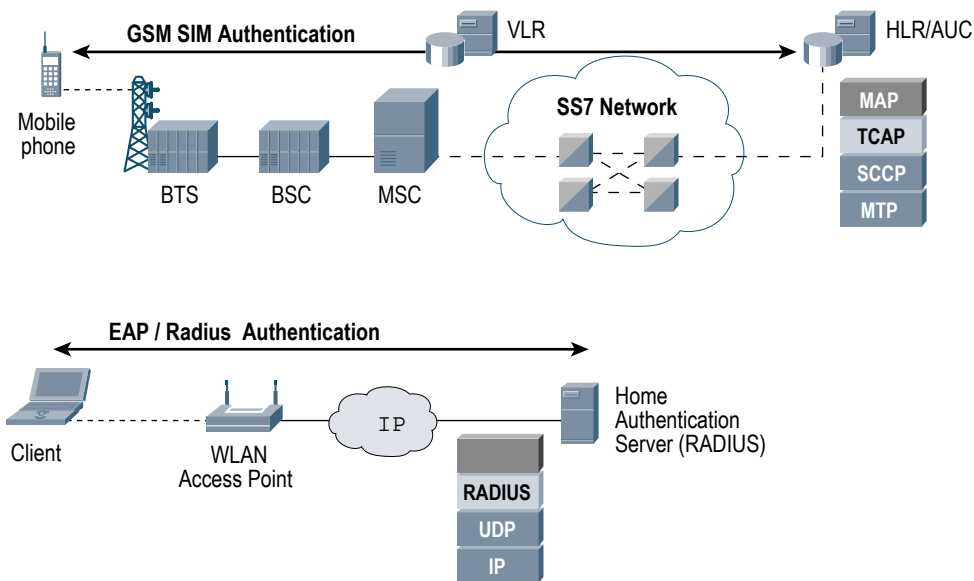


Cisco ITP MAP Gateway の利点

GSM および WLAN のテクノロジーを、同一のサービス プロバイダー ネットワーク内のそれぞれ異なる地域で同時に使用する場合を想定します。

図 2 に示すように、MAP ゲートウェイ ソリューションを使用しないと、WLAN と GSM の両方を使用するサービス プロバイダーは、2つの認証シグナリング プロセスを個別に維持する必要があります。このため、個別のプロビジョニング費用が必要となり、2つの認証サービス間でサービス品質に差が生じます。GSM ユーザは MAP SS7 ベースの HLR と AUC に対して認証されますが、WLAN ユーザ (同じ GSM ユーザが WLAN サービスの領域に移動した場合など) は複合的なメカニズム (802.1X [EAP] および RADIUS ベースなど) を使用して認証されます。

図 2
WLAN および GSM の認証シグナリング プロセス : 本来は個別に動作



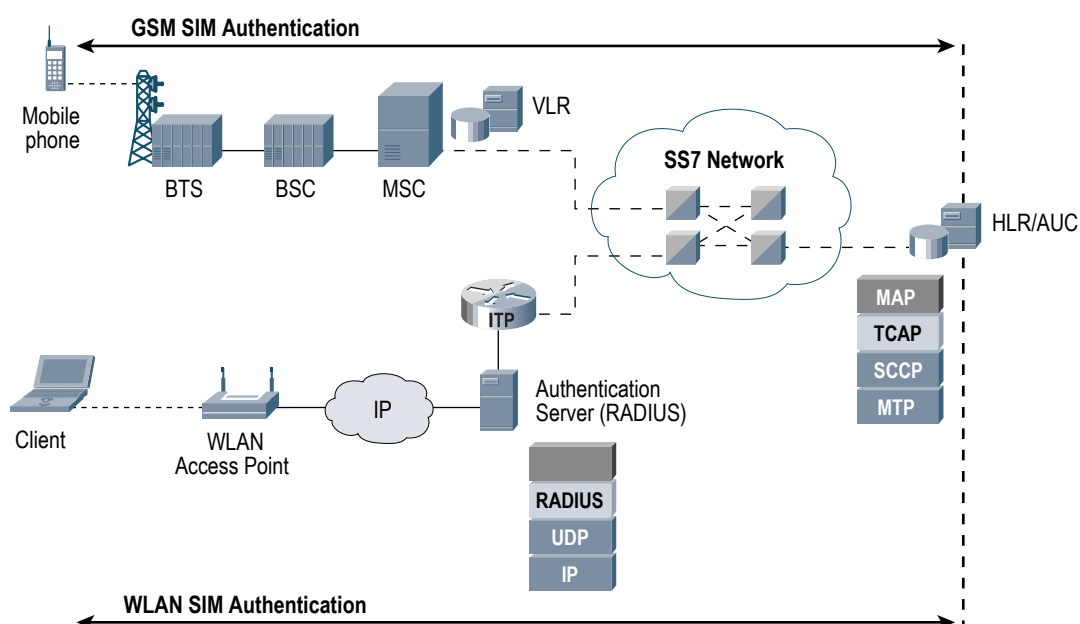


MAP ゲートウェイ機能を携帯電話ネットワークに導入すると (図 3 を参照)、サービスプロバイダーは WLAN と GSM のテクノロジーを 1 つのセキュリティメカニズムに統合できます。これには、次のような数多くの利点があります。

- **均質でよりセキュアな認証** — Cisco ITP MAP Gateway の機能を使用すると、SIM カードを利用した WLAN 認証が可能になります。SIM カードでは、加入者 ID とエントロピーの高い秘密鍵が、不正開封が防止されるメモリに保存されます。SIM ベースの認証は、従来の WLAN ネットワークで使用されているユーザ名とパスワードによる認証よりもハッキングに対する強度が優れています。SIM 認証は、携帯電話ネットワークで現在最も多く使用されている認証メカニズムであるため、不正行為やクローニングのリスクはほとんどありません。
- **すでに GSM ネットワークで利用されている既存のプロビジョニングシステムの再利用** — MAP ゲートウェイを使用すると、事業者はサービスのプロビジョニングとアクセス許可に既存の GSM の HLR/AUC を活用し、GSM ベースのサービスで使われている既存のプロセスを再利用できます。Cisco ITP MAP Gateway による SIM ベースの認証プロセスを使用しない場合、WLAN サービスにアクセスするために別の独立したプロセスが必要になるため、事業者は既存の HLR と AUC のほかに専用のデータベースを導入し、運用する必要があります。

図 3

Cisco ITP MAP Gateway により WLAN および GSM のアクセスセキュリティを融合



Cisco ITP MAP Gateway が提供する機能を理解するためには、WLAN と GSM の認証で使用されているセキュリティメカニズムそれぞれについて理解しておくことが有効です。ここからは、WLAN ベースおよび GSM ベースのネットワークに使用されている認証機能について個別に詳しく説明していきます。さらに、MAP ゲートウェイがどのようにこれらの機能を WLAN および GSM ネットワークに最適な共通の機能として統合しているかについて説明します。

802.11 および RADIUS と EAP を組み合わせた従来の認証方式

IEEE 802.1X は、ポートベースのネットワーク アクセス制御を行うための規格です。IEEE 802.1X を使用すると、認証されたユーザだけが WLAN アクセス ポイントを経由してネットワークにアクセスできます。IEEE 802.1X 規格は、イーサネット、トークンリング、および 802.11 WLAN などの IEEE 802 メディアへの認証アクセスを実現するために設計されました。802.1X 規格では、WLAN の認証フレームワークを規定しており、HPLMN などを使用した一元的なユーザ認証を可能にします。ただし、ユーザが認証されているかどうかを判断するための特定のアルゴリズムは規定されておらず、複数のオプションを使用できます。

802.1X は EAP をサポートします。EAP は複数の認証メカニズムをサポートしている一般的な認証プロトコルであり、イーサネット、トークンリング、または WLAN 上で動作します。802.1X を使用している WLAN では、ユーザ (要求元) はアクセス ポイント (認証者) へのアクセスを要求します。

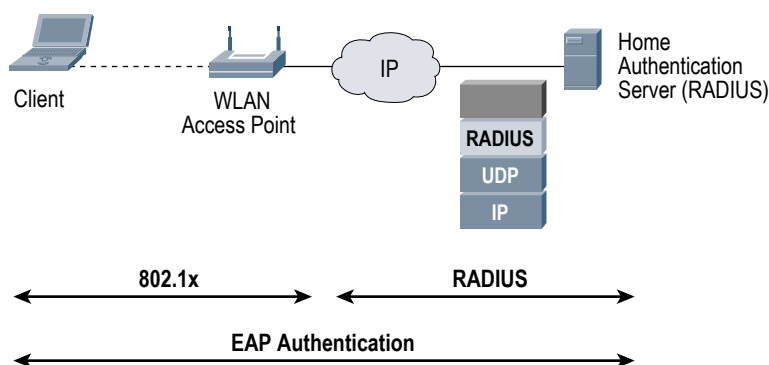
認証サーバは、多くの場合、サーバとアクセス ポイント上の認証ピア間で RADIUS プロトコルを使用します。この場合、EAP 要求元とバックエンドの認証サーバ間での通信を可能にするために、EAP メッセージは RADIUS プロトコルを使用してカプセル化されます。



図 4 に示すように、この複合型 EAP 認証プロセスには 3 つの要素が含まれています。

1. WLAN サービスへのアクセスを要求する **クライアント デバイス** — Microsoft Windows XP オペレーティング システムで提供しているような 802.1X 準拠のクライアント ソフトウェアが稼働している必要があります。
2. クラアイントを実際に認証する **RADIUS 認証サーバ** — 認証サーバはクラアイントの ID を確認し、WLAN サービスへのアクセスを許可するかどうかをアクセス ポイントに通知します。アクセス ポイントはプロキシとして機能するため、認証サービスはクライアントに対してトランスペアレントです。
3. クラアイントの認証状態に基づいてネットワークへの物理アクセスを制御する **アクセス ポイント** — アクセス ポイントはクライアントと認証サーバ間の仲介装置 (プロキシ) として機能し、クライアントの ID 情報要求、認証サーバでの ID 情報確認、およびクライアントへの応答中継を行います。アクセス ポイントには RADIUS クラアイントが存在し、EAP フレームのカプセル化とカプセル化解除、および認証サーバとのやりとりを行います。

図 4
802.1X および RADIUS 認証と EAP との組み合わせによる認証方式



EAP およびその他の非 SIM ベース認証メカニズムの限界

WLAN アクセスでは、すでに多様な認証アプリケーションが開発されており、実際に使用されています。一般的に専門家は、クライアントとサーバ間で認証のために使用される長期秘密鍵の種類および保管場所によってセキュリティレベルを判断します。現在使用されている方式には、次の 3 つがあります。

- 長期秘密鍵として、クライアントとユーザ間で英数字パスワードの交換を行う方式。この方式は、エントロピーが最も低く、辞書攻撃などによる攻撃が容易です。
- より複雑な構造を持つ長期秘密鍵をユーザ デバイス (PC や Personal Digital Assistant [PDA; 携帯情報端末] など) のハードドライブに保管する方式。この方法では、実際に使用するメカニズム (EAP または非 EPA) が何であろうと、長期秘密鍵を容易に調べ出すことができます。デバイスの OS (オペレーティング システム) 自体に不正アクセスを防止する仕組みがなく、ハードディスク上の情報へのアクセスが可能であるためです。
- 長期秘密鍵をスマートカードなどの不正開封が防止される環境に保管する最も安全で強力な方式。この方式は不正アクセスを防止することができ、アプリケーション レベルのセキュリティを実現できるため、銀行や民間企業がユーザ デバイスへの導入を進めています。スマートカードを使用すると、秘密鍵やパスワードなどの重要情報、健康管理データなどの個人情報などを安全に保管できます。また、公開鍵または秘密鍵による暗号化などのセキュア プロセスを安全に実行できます。

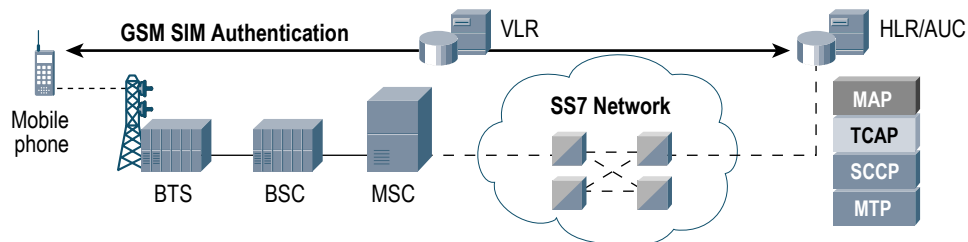
GSM ネットワークでの SIM ベース認証

GSM ネットワークでは、スマートカード ベースのユーザ認証およびデータ暗号化方式が使用されています。SIM カードはユーザの携帯電話機に挿入されるスマートカードで、International Mobile Subscriber Identity (IMSI) という ID 番号を使用してユーザを一意に認識します。

SIM 認証は、ユーザとユーザ データベース (HLR) 内にある AUC との間のエンドツーエンドのメカニズムです (図 5 を参照)。



図 5
GSM の SIM 認証アーキテクチャ



GSM 認証プロセスは 3 つのコンポーネントで構成されています。

1. **モバイル端末** — モバイル端末には SIM カードが装着されており、ここに AUC と共有する IMSI と秘密鍵 (Ki)、および認証アルゴリズム (A3) と鍵交換アルゴリズム (A8) が保管されています。
2. **Mobile Switching Center (MSC; 移動通信交換局) および VLR** — これらは個別のコンポーネントになっている場合がありますが、簡素化するために 1 つのコンポーネントとして示します。
3. **HLR および AUC** — これらは個別のコンポーネントになっている場合がありますが、簡素化するために 1 つのコンポーネントとして示します。

GSM 認証は、チャレンジ/レスポンス方式に基づいています。SIM 上で実行される認証アルゴリズムは、128 ビットの乱数 RAND をチャレンジとして使用します。次に、SIM は事業者固有の機密アルゴリズム (A3) を実行します。A3 では SIM に保管されている RAND と秘密鍵 (Ki) を入力として使用し (Ki は加入時に IMSI とともに割り当てられる)、32 ビットの応答用 Secret Response (SRES) を生成します。さらに、もう 1 つのアルゴリズム (A8) を使用して、Ki と RAND から 64 ビットの鍵 (Kc) を計算します。この鍵 Kc は、無線インターフェイス上の暗号鍵として使用することを目的としています。

SIM と AUC によって算出された SRES 値は、AUC によって比較されて、値が一致した場合に認証が許可されます。

Cisco ITP を使用した複合型 EAP SIM 認証

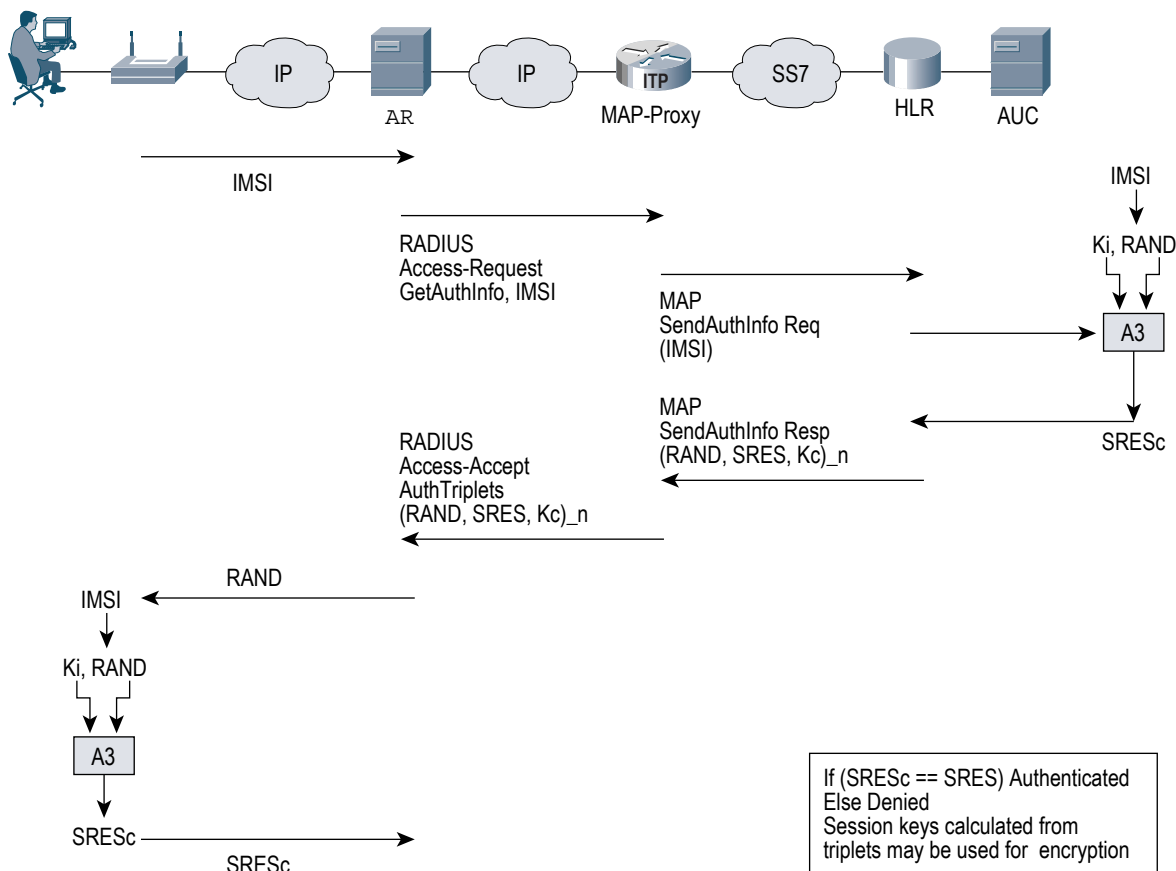
すでに説明したように、Cisco ITP MAP Gateway によって RADIUS サーバと HLR/AUC が融合されて、SIM に類似した認証を GSM の HLR/AUC に対して実現できます。

- HLR 側から見た場合、Cisco ITP は VLR として動作します。
- RADISU サーバ側から見た場合、Cisco ITP は別の RADIUS サーバとして動作します。

図 6 は、クライアント、RADIUS サーバ (ここでは Cisco Access Registrar)、Cisco ITP、および HLR/AUC の間に発生するデータフローの概略を示しています。



図 6
Cisco ITP を使用した EAP SIM 認証のデータ フロー



注：これはデータ フローの一部であり、IMSI に関連する部分のみを示しています。

GSM SIM 認証との相違点

複数の RAND チャレンジを使用して複数の 64 ビット鍵 Kc を生成し、それらを組み合わせて特定の 802.11 暗号スイートに必要なセッション鍵を作成するという点で、EAP SIM は GSM と異なります。

また、EAP SIM はネットワーク認証を使用して、GSM の基本認証メカニズムを強化しています。GSM 認証が定義された時点では、違法な Base Transceiver Station (BTS; 無線基地局) はセキュリティ上の脅威とは見なされていませんでした。EAP SIM ではネットワークのクライアント チャレンジが定義されており、メッセージ認証コードを使って RAND チャレンジを実行することで、相互認証を可能にしています。

EAP SIM プロセス：相互認証

ネットワーク認証

最初に、クライアントは、要求元によって生成された Nonce と呼ばれる 16 バイト (128 ビット) 乱数を送信することにより、EAP、SIM、または Start 要求に応答します。次に、RADIUS サーバは、その乱数とユーザの IMSI、Ki、および 2 つまたは 3 つの GSM 乱数 RAND[n] を使用して、SIM または EAP チャレンジ パケットに格納される 20 バイトの MAC (メディア アクセス制御) である MAC_RAND を計算し、クライアントに返します。また、チャレンジ パケットにも、セッション鍵の生成に使用される 2 つまたは 3 つの乱数 RAND[n] が含まれています。クライアントが最初にチャレンジ (すなわち、ネットワーク) を認証します。この認証では、クライアントが固有の MAC_RAND を計算し、それをネットワークから受信した MAC_RAND と比較します。これらが一致すれば、クライアントはユーザの AUC と接続されている認証サーバと通信していると判断します。これは、ユーザの HPLMN と WLAN のアクセスポイント事業者との間に信頼関係が確立されていることを示しています。



クライアント認証

次に、クライアントは RAND[n] と GSM の A3 および A8 アルゴリズムを使用して、一致する SRES[i] と Kc[n] をそれぞれ計算します。IMSI、Ki、および SRES[n] は、応答として返される別の MAC (MAC_SRES) を計算するために使われます。ネットワークは MAC_SRES を使用してクライアントを認証します。SRES[n] が無線を経由して直接返されることはないため、RAND または SRES のペアを使用しても、秘密鍵 (Ki) を不正に入手することはできません。

利点：認証メカニズムの安全性向上

総合的に見ると、Cisco ITP MAP Gateway を使用することによって、GSM や Universal Telecommunications System (UMTS) 携帯電話ネットワークと同じレベルの保護を実現することができます。MAC_RANDOM または MAC_SRES の計算に使用されるデータ暗号鍵 Kc[n] が無線経由で送信されることはありません。ネットワークとクライアントは、Kc[n]、IMSI、Nonce、およびバージョン情報を使用して、無線リンク上でのデータの暗号化に使用する暗号鍵 (Kc) を計算します。SRES も無線経由で送信されることはありません。EAP または SIM に攻撃を加えることによって、GSM のトリプレット (RAND、SRES、Kc) のすべてを入手する方法は発見されていません。

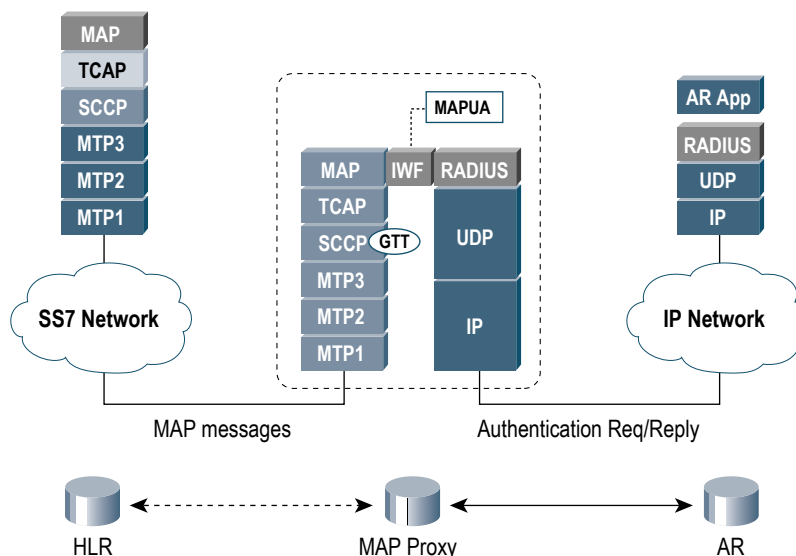
Cisco ITP MAP Gateway Protocol の適合性とインターオペラビリティ

既存の標準との適合性

図 7 は、Cisco ITP MAP Gateway、RADIUS サーバ、および従来の Time Division Multiplexing (TDM; 時分割多重) ベースの SS7 HLR 間のインターフェイス部分の詳細を示しています。Cisco ITP MAP Gateway は、モバイル ネットワークにおける業界の主要な HLR および Signaling Transfer Point (STP) サプライヤとのインターオペラビリティを確保しています。また、RADIUS (Cisco Access Registrar) とのインターオペラビリティもすでに確保されています。

図 7

シスコの RADIUS サーバおよび従来の SS7 HLR とのインターフェイスを提供する Cisco ITP MAP Gateway



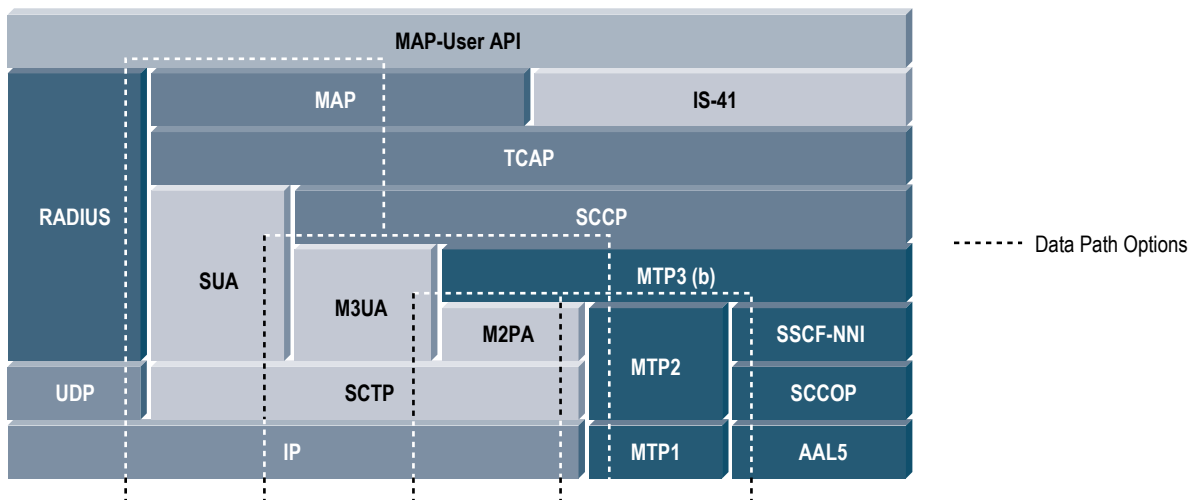
さらに、Cisco ITP MAP Gateway は、Internet Engineering Task Force (IETF) の SIGTRAN M3UA および SIGTRAN SCCP User Adaptation (SUA) ベースの HLR を含めた、従来型とは異なる SS7 エンド ノードとのインターオペラビリティも有しています。SIGTRAN は SS7-over-IP (SS7oIP) アプリケーションに関する IETF ベースの規格であり、UMTS ネットワークなどに向けて設計されたものです。

図 8 に示すように、Cisco ITP は SS7 ネットワークとのインターフェイスを確保するために、次のような多様な実装形態をサポートしています。

- ITU または ANSI の MTP1、MTP2、および MTP3 上での従来の SS7 プロトコル リンク
- ATM Adaptation Layer 5 (AAL5)、Service Specific Connection Oriented Protocol (SSCOP)、および Service Specific Coordination Function (SSCF) の Node-to-Network Interface (NNI) プロトコル上での高速 ATM ベース リンク
- IETF SIGTRAN M2PA Peer-to-Peer Protocol for MTP3 over IP
- IP ネイティブ SS7 HLR アプリケーションに対する IETF SIGTRAN Client Server M3UA for SCCP over IP および SUA for MAP over IP プロトコル



図 8
Cisco ITP MAP Gateway のプロトコル スタック



今後の標準適合性

シスコのソリューションは、SIM EAP に準拠しています。SIM EAP とは、認証メカニズムとして EAP のメカニズムを使用しながら、鍵の配布に GSM の SIM を利用する方式のことです。SIM EAP は将来的に IETF の正式な標準となる予定です。

設定可能な Cisco ITP MAP Gateway 機能

EAP SIM ベースの認証

認証要求が RADIUS サーバに送信されると、RADIUS サーバは認証要求を Cisco ITP に転送します。Cisco ITP は、MAP SendAuthInfo 要求を AUC に送信して認証トリプレットを取得し、これを認証応答に埋め込んで RADIUS サーバに返します。その後、RADIUS サーバは、クライアントに対する標準的な認証応答を実行します。

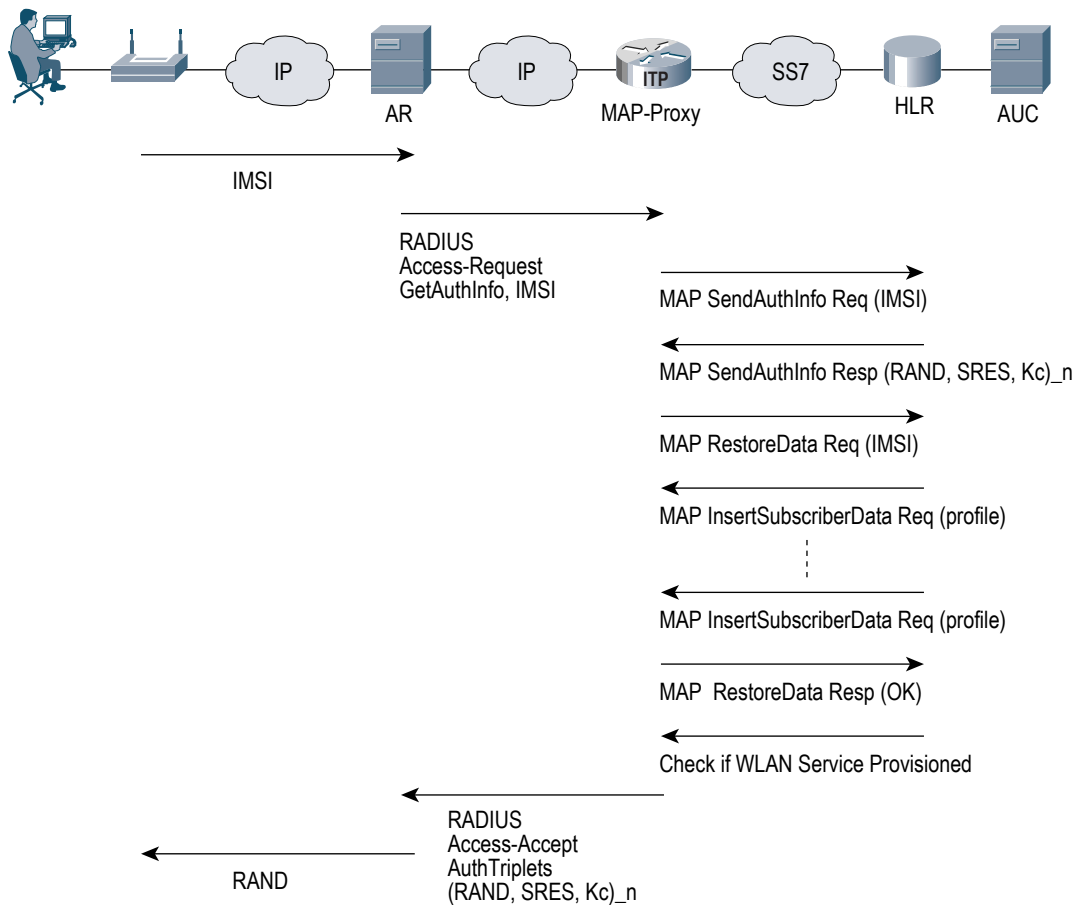
SIM ベースの許可

この機能を使用すると、EAP SIM 認証が完了済みだと仮定した場合、事業者は加入者が WLAN サービスの契約を結んでいる場合にのみ接続を許可することができます（図 9 を参照）。

一般的に、許可サービスは HLR の加入者プロファイルに記載されています。しかし、大半の HLR には WLAN サービス専用のフィールドが存在しません。これは、WLAN サービスが European Telecommunication Standards Institute (ETSI) の勧告事項に含まれていなかったためです。現在、標準化団体がこの機能の実装に取り組んでいます。正式な標準化が制定されるまでの間は、使用頻度の少ないサービス フィールドを WLAN 用として使用することができます。Cisco ITP では、ベアラ サービス (BS) とテレサービス (TS) の 2 つのフィールドをサポートしています。HLR 加入者プロファイル内の既存の BS または TS サービスはいずれも使用でき、設定変更が可能です（一般的に、事業者は BS 31 を使用）。



図 9
認証および許可プロセスのデータフローの概要



トリプレットのキャッシング

Cisco ITP MAP Gateway は、設定変更可能な数のトリプレットを HLR からキャッシュして、必要に応じてローカルで認証を実行できます。

また、Cisco ITP のコンフィギュレーションでは、事業者の実装ポリシーに応じて、同じユーザの認証プロセスが複数回行われる場合にトリプレットを再利用することができます。

さらに、トリプレットを Cisco ITP MAP Gateway のキャッシュ メモリに保管する時間を設定することができます。

性能およびキャパシティ

表 1 は、Cisco ITP の主な特長を示しています。

表 1 Cisco ITP の特長

カテゴリ	内容
Cisco 7513 シャーシの寸法 (高さ×幅×奥行)	85.73 × 44.45 × 55.88 cm (33.75 × 17.5 × 22 インチ) — 高さ 3 フィート未満
Cisco 7206VXR シャーシの寸法 (高さ×幅×奥行)	13.34 × 42.67 × 43.18 cm (5.25 × 16.8 × 17 インチ)
リンク キャパシティ	最大 720 の SS7 リンク (Cisco 7513) 最大 24 の SS7 リンク (Cisco 7206VXR)
認証数	最大 1800/ 秒
認証および許可数	最大 400/ 秒



Cisco ITP MAP Gateway のトポロジー

実際にどのようなトポロジーを採用するかはネットワーク設計者が選択するものであり、ネットワークの仕様に大きく左右されます。ここでは、Cisco ITP 機能を集中配置また分散配置することにより、冗長性の向上とコスト削減を可能にする Cisco ITP ベースのトポロジーの例について説明します。

- 分散型トポロジーでは、Cisco ITP MAP Gateway ノードは各地域の RADIUS サーバに隣接して配置（同じデータセンター内に配置）されます。この場合、ローカル RADIUS サーバと同じ数の MAP ゲートウェイが配備されます。すべての MAP ゲートウェイは、中央の HLR または AUC と SS7 接続されています。
- 中央集中型アーキテクチャでは、MAP ゲートウェイは 1 つだけで、通常、HLR または AUC とともに配置されます。この場合、ローカル RADIUS サーバとの間に複数の RADIUS 接続が確立されます。長距離リンクは IP ベースで、トポロジーに応じて既存の IP ネットワークを利用することにより、伝送コストを削減できます。Cisco ITP と RADIUS サーバ間の IP リンク上で IP Security (IPSec) を使用すると、重要なシグナリングトラフィックを保護できます。
- そのほかに、Cisco ITP の SIGTRAN IP ベース M2PA バックホール機能を利用するトポロジーがあります。このトポロジーでは、各ローカルデータセンターにリモート MAP ゲートウェイを配置し、中央集中型 MAP ゲートウェイを HLR クラスタとともに配置します。中央の MAP ゲートウェイは、SIGTRAN M2PA という IETF 標準の SS7oIP ピアツーピアプロトコルを使用して、リモート MAP ゲートウェイと通信します。

Cisco ITP MAP Gateway の信頼性と冗長性

ノードおよびアーキテクチャの冗長性

Cisco ITP MAP Gateway 製品は、実績のある Cisco 7500 または Cisco 7200VXR シリーズ ルータのハードウェアプラットフォームに組み込む設計になっています。Cisco 7500 および 7200VXR シリーズ ルータは、通信、医療、銀行、証券、航空、および官公庁などの、高い信頼性とアベイラビリティが要求される業界で幅広く使用されています。シスコの Customer Advocacy 部門では、Cisco 7500 シリーズのハードウェアとソフトウェアの Mean Time Between Failure (MTBF; 平均故障間隔) と Mean Time To Repair (MTTR; 平均復旧時間) をモニタしています。お客様の使用実績によると、単一の Cisco ITP で「シックス ナイン」(99.9999%) のアベイラビリティが実現されています。これを年間の停止時間に換算すると約 1 秒になります。

完全に冗長な Cisco ITP プラットフォームを使用すると、リンク、ポート アダプタ、または中央処理装置に障害が発生した場合のスイッチオーバーが可能になり、サービスの停止時間を最小限に抑えることができます。スイッチオーバーの際にトラフィックが中断されると、パケットが消失するため、RADIUS サーバは再送を行います。リンクが再度確立されると、HLR と RADIUS サーバからのパケットは MAP ゲートウェイで再度処理されます。

また、アーキテクチャそのものを冗長構成にして、負荷分散やバックアップ用に複数の ITP を使用することもできます。特に、Cisco Access Registrar を使用すると、複数の ITP MAP ゲートウェイを定義できます。この場合、MAP ゲートウェイに障害が発生すると、トラフィックはバックアップ ITP にリダイレクトされます。複数の ITP をラウンドロビン方式で使用するよう RADIUS サーバを設定することもできます。

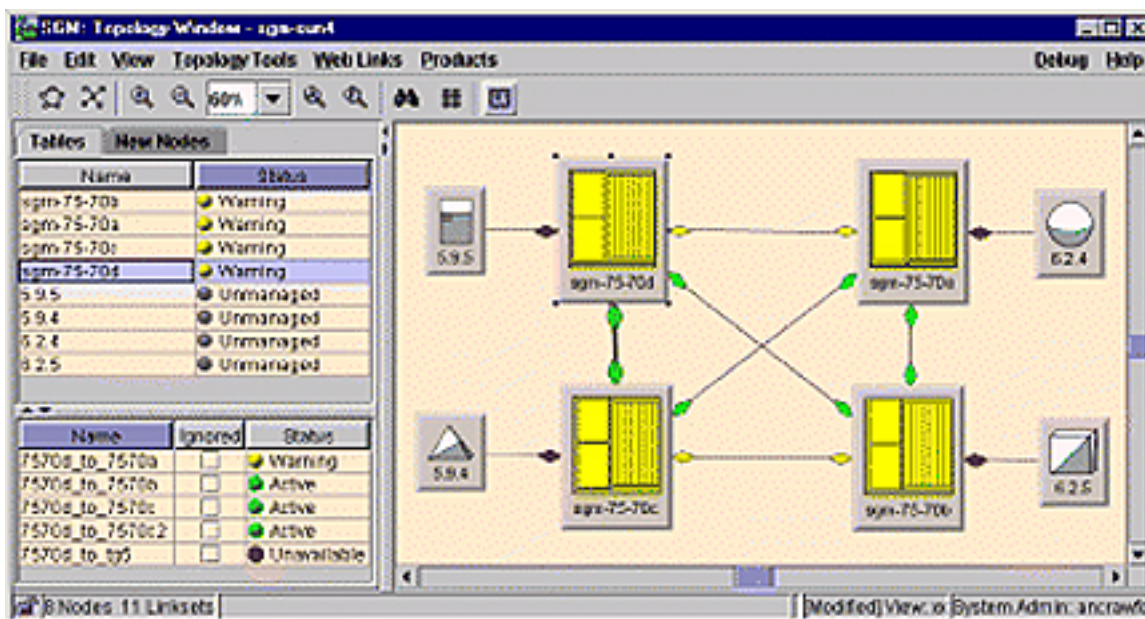
ネットワーク管理

Cisco ITP のネットワーク管理ソリューションは、Cisco Signaling Gateway Manager (SGM) と既存のシスコ製およびサードパーティ製の IP ネットワーク管理製品を融合させます。Cisco SGM を CiscoWorks、CiscoView、および Agilent acceSS7 や HP OpenView などのエコシステム パートナー製品と併せて使用すると、Cisco ITP SS7 ネットワークのエンドツーエンドの管理スイートを実現できます。これにより、ネットワーク管理者は Cisco ITP ネットワークの検出、管理、およびトラブルシューティングを行うことができます。市販の SS7 ネットワーク管理アプリケーション（エンドツーエンドのコールトレース、パケット分析、および長期トレンド分析など）の主要ベンダーとの連携により、この管理ソリューションでは、既存の SS7 管理アプリケーションとの迅速な統合が可能となっています。

Cisco SGM は、ネットワーク管理者が Cisco ITP ネットワークの SS7oIP レイヤを管理できるようにするソフトウェアアプリケーションです。Cisco SGM はクライアント / サーバアーキテクチャで、Windows、Solaris、および Web ベースクライアントをサポートしています。図 10 は、Cisco SGM による SS7oIP ネットワークのトポロジー表示の画面です。



図 10
Cisco SGM のトポロジー表示



まとめ

ネットワークに Cisco ITP MAP Gateway の機能を導入すると、モバイル事業者は既存の GSM アーキテクチャに WLAN テクノロジーを容易に統合し、高レベルで均質なセキュリティとサービスアクセス許可を実現できます。さまざまな中央集中型または分散型のオプションが用意されているため、Cisco ITP MAP Gateway は柔軟な実装が可能です。また、Cisco ITP は、ITU、ANSI、および IETF SS7oIP の各種標準をサポートしているため、さまざまな方法で GSM 事業者の HLR とのインターフェイスを確保できます。

Cisco ITP MAP Gateway は、Cisco 7200VXR シリーズおよび Cisco 7500 シリーズ上で提供されるため、使用状況に合わせてリンク密度、性能、および冗長性を柔軟に選択できます。Cisco ITP MAP Gateway を Cisco 7500 シリーズに導入して高い処理能力を得ることにより、ネットワークとトラフィックを同一プラットフォーム上で拡張できます。Cisco ITP MAP Gateway を使用すれば、モバイル事業者は新たな技術を容易に導入することができます。

略語の解説

AUC : GSM Authentication Center (認証センター)

AP : WLAN Access Point (アクセスポイント)

CAR : Cisco CNS Access Registrar (シスコの EAP 対応 RADIUS 製品)

EAP : Extensible Authentication Protocol (RFC 2284)

GSM : Global System for Mobile Communications (第 2 世代携帯電話 [2G] ネットワークの ETSI 規格)

HLR : Home Location Register (GSM ネットワークの加入者データベース)

IMSI : International Mobile Subscriber Identity

HPLMN : Home Public Land Mobile Network

ITP : Cisco IP Transfer Point (SS7 および IP ネットワークのシグナリングゲートウェイ)

MAP : Mobile Application Part (携帯電話ネットワーク内でのモビリティ管理シグナリングの ETSI GSM 規格)

MS : Mobile Station (モバイル端末)、GSM ネットワーク内では携帯電話機に相当

RADIUS : Remote Access Dial-In User Service

SIM : Subscriber Identity Mobile (GSM 加入者を一意に識別する)

UMTS : Universal Telecommunications System (第 3 世代携帯電話システムの 3GPP 規格)

VLR : Visitor Location Register (加入者の HLR プロキシとして機能するローカル GSM データベース)

WLAN : Wireless LAN (IETF 802.11 規格より)

©2004 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。
この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>
問合せ URL: <http://www.cisco.com/jp/go/contactcenter/>
〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL: 03-6670-2992

お問合せ先

電話でのお問合せは、以下の時間帯で受付けております。
平日 10:00 ~ 12:00 および 13:00 ~ 17:00