USIM　LTE　コンフォーマンス試験

Technology Reports

SAE標準化技術特集

LTE導入に向けたUSIMファイル拡張とコンフォーマンス試験仕様の策定

LTE導入に伴い，NW認証時に生成される各種関連パラメータをUSIMに保存し，移動端末間でUSIMを差し替えるときやエリアをまたがるときに認証をスムーズに行うことが可能となるように，USIMのファイル拡張を行った．また，LTEサービス開始に先んじたLTE対応移動端末とUSIM間のインタフェース動作確認のためのコンフォーマンス試験仕様を策定するために，3GPP CT WG6会合にてWIを立ち上げた．

移動機開発部　南本（みなみ もとい）†

1. まえがき

LTE（Long Term Evolution）[*1]におけるNW認証は3Gの認証とは異なり，認証時に生成，保存されるパラメータが異なる．これらパラメータを移動通信用加入者識別モジュールであるUSIM（Universal Subscriber Identity Module）[*2]内の基本ファイル（EF：Elementary File）に格納し，次回認証時にそれらのパラメータを利用することによって，USIMの差替え時に不要な認証処理がされなくなり，NWアクセスの高速化が実現できる．このため，USIMのアプリケーション仕様の策定を行っている3GPP CT WG（Core Network and Terminals Working Group）6会合において，USIMのコア仕様でありファイル構造などを規定しているTS31.102[1]仕様中に，それらのパラメータを保存するファイルの規定を行った．また，認証時における移動端末の動作は3Gの動作とは異なるため，移動端末の動作の正常性を確認するための試験項目の策定が必要であり，それを実現するためのWI（Work Item）をCT WG6会合にて立ち上げた．

本稿では，現在策定中であるLTE対応移動端末とUSIMとの間のインタフェース動作確認のためのコンフォーマンス試験仕様について解説する．

2. USIMファイルの拡張

2.1 導入背景

LTE導入（3GPP Release 8）以前の標準仕様では，3G認証用にEF_LOCI（Location Information），EF_PSLOCI（Packet Switched Location Information）というファイルがそれぞれ回線交換（CS：Circuit Switched）／パケット交換（PS：Packet Switched）ドメインでの認証用に用意されており，これらファイルの中にTMSI（Temporary Mobile Subscriber Identity）[*3]などを保存することができた．これによってUSIMの差替え時やエリアをまたがる際に，スムーズな認証が可能となっていた．これらの要素は移動端末

† 現在，研究開発推進部

＊1 **LTE**：3GPPで検討されている第3世代移動通信方式の拡張規格．ドコモがSuper3Gとして提唱したもので「3.9G」と位置付けられる．

＊2 **USIM**：携帯電話会社と契約した電話番号などを記録しているICカード．

＊3 **TMSI**：NWによるユーザの認証に用いられる一時的なID．

の不揮発メモリに格納することも考えられるが，LTE認証においてもUSIMにEF_LOCIやEF_PSLOCIと同様のファイルを導入することの必要性が議論され，最終的にEF_EPSLOCI（Evolved Packet System Location Information）というファイルを新規に規定し，今回の導入に至った．また，それとは別に秘匿鍵などのセキュリティコンテクストを格納するEF_EPSNSC（EPS Non-Access-Stratum Security Context）というファイルを新規に規定した．これらのファイルを参照することにより，例えばUSIMを別の移動端末に差し替えた場合に再度AKA（Authentication and Key Agreement）[*4]プロセスを最初から実行する必要がなくなり，認証時間（在圏できるまでの時間）を短縮でき，ユーザ利便性が向上するとともに，NWのトラフィックも軽減することができる．

2.2 データ構造

EF_EPSLOCIのデータ構造を**表1**に示す．

ここで，LTEのGUTI（Globally Unique Temporary Identifier）[*5]は3GのTMSIに相当するものである．また，Last visited registered TAI（Tracking Area Identity）[*6]には，移動端末が最後に在圏したNWとTracking Area[*7]が格納される．EPS update statusには，前回のアタッチ[*8]やデタッチ[*9]が正常に終了したかなどを意味する値が格納される．これらの詳細はいずれも，3GPP TS 24.301[2]に規定されている．

続いて，EF_EPSNSCのデータ構造を**表2**に示す．

EPS NAS（Non-Access-Stratum）[*10]セキュリティコンテクストには，秘匿に使われる鍵値K_{ASME}などが格納される．K_{ASME}の利用の詳細については[3]を参照されたい．詳細なデータ構造は3GPP TS 31.102[1]に，それぞれのセキュリティパラメータの詳細はTS 33.401[4]に規定されている．

3. コンフォーマンス試験仕様の策定

LTEでは，USIMに新規にファイルが追加されたことや，3G認証と異なり移動端末が秘匿鍵を生成する必要があることなどにより，移動端末の動作の正当性を確認するための試験が必要になる．このため，2008年11月に開催されたCT WG6会合において，コンフォーマンス試験[*11]を策定するためのWIを立ち上げた．ドコモもサポーティングカンパニーとして試験項目策定に積極的にかかわり，2009年3月に第1回アドホック会合を開催し，試験仕様のドラフト版を策定した．この内容は2009年5月開催のCT WG6会合に入力され，承認されている．具体的にはUSIMと移動端末との間のインタフェース動作の試験仕様であるTS 31.121[5]およびUSAT（Universal Subscriber Identity Module Application Toolkit）[*12]機能のテスト仕様であるTS 31.124[6]の更新を行っている．

4. あとがき

本稿では，LTE導入に伴いUSIMに新規に拡張したファイルについて解説した．また，LTE対応移動端末とLTE対応USIM間のインタフェース動作を試験するコンフォーマンス試験仕様の策定について解説した．これらにより，USIMの差替え時やエリアをまたがる際の認証の高速化が期待される．また，LTEサービス開始に先立って標準仕様に基づき移動端末，USIMそれぞれの動作の正当性の確認を行うことが可能となる．最終的な仕様完成のターゲット時期を2009年9月とした．

今後はさらに，USATなどの試験仕様の作成を行っていく予定である．

表1　EF_EPSLOCI構造

要素	格納データ	長さ
GUTI	一時的な認証ID	12bytes
Last visited registered TAI	最後の在圏NW，Tracking Area	5bytes
EPS update status	アタッチ，デタッチの正常または異常終了	1byte

表2　EF_EPSNSC構造

要素	格納データ	長さ
EPS NAS セキュリティコンテクスト	K_{ASME} など	12bytes

＊4 **AKA**：認証（Authentication）と鍵生成（Key Agreement）を用いた認証処理の総称．USIMは，NWより払い出されたパラメータを基に秘匿鍵，完全性検査鍵を生成するとともに，それらのパラメータの正当性を確認する．

＊5 **GUTI**：GUMMEI（Globally Unique MME Identifier）とTMSIから構成される情報．移動端末やユーザ（USIM）の恒久IDを使用せずに移動端末を一意に認識するために用いられる一時的なID．

＊6 **TAI**：事業者の国コードであるMCC（Mobile Country Code），事業者のネットワークコードであるMNC（Mobile NW Code），TAC（Tracking Area（＊7参照）Code）から構成される情報．

＊7 **Tracking Area**：1つまたは複数のセルから構成され，NW上で管理される移動端末の位置を示すセル単位．Tracking Areaを各事業者がコード化したものがTAC．

＊8 **アタッチ**：通信網へ在圏すること．

＊9 **デタッチ**：通信網の在圏状態を終了すること．

文　献

[1] 3GPP TS31.102 V8.6.0：“Characteristics of the Universal Subscriber Identity Module (USIM) application，”2009.
[2] 3GPP TS24.301 V8.2.1：“Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS) Stage3，”2009.
[3] Zugenmaier，ほか：“SAE/LTEを実現するセキュリティ技術，”本誌，Vol.17, No.3, pp.27-30, Oct. 2009.
[4] 3GPP TS33.401 V8.4.0：“3GPP System Architecture Evolution (SAE) Security architecture，”2009.
[5] 3GPP TS31.121 V8.1.0：“UICC-terminal interface; Universal Subscriber Identity Module (USIM) application test specification，”2009.
[6] 3GPP TS31.124 V6.10.0：“Universal Subscriber Identity Module Application Toolkit (USAT) conformance test specification，”2009.

＊10 **NAS**：移動端末とコアNWとの間の機能レイヤ．
＊11 **コンフォーマンス試験**：標準化団体で規定される，標準機能仕様に基づいて作成された通信機器の正当性を確認するための標準試験．
＊12 **USAT**：USAT機能は，3GPP TS31.111で規定されている標準機能であり，USATコマンドを用いることによって，USAT機能対応のUSIM，移動端末，NW間でさまざまな機能やサービスの提供が可能となる．