USIM LTE Conformance Test

Technology Reports

Special Articles on SAE Standardization Technology

USIM File Extension and Creation of Conformance Test Specification toward LTE Deployment

With the deployment of LTE, a variety of parameters generated at the time of network authentication will be saved in the USIM. To simplify authentication when a USIM is removed from one mobile terminal and inserted into another or when a mobile terminal crosses into a new area, USIM files have been extended. In addition, a WI has been established in 3GPP CT WG6 to create a conformance test specification to test the operation of the interface between an LTE-capable mobile terminal and the USIM prior to the launch of LTE services.

Communication Device Development Department **Motoi Minami**†

1. Introduction

Network authentication in Long Term Evolution (LTE)[*1] differs from that of 3G in that the parameters that are generated and saved at the time of authentication are different. If these parameters were to be stored in Elementary Files (EFs) within the Universal Subscriber Identity Module (USIM)[*2] used for mobile communications, and if those parameters were then used for subsequent authentication processes, the amount of authentication processing required could be reduced and access to the network speeded up. For this reason, the files for storing these parameters have been specified within TS31.102 [1], a technical specification that prescribes USIM core specifications such as file structure, by 3GPP Core Network and Terminals Working Group 6 (3GPP CT WG6), which drafts USIM application specifications. Furthermore, as the operation of an LTE-capable mobile terminal at the time of authentication differs from 3G operation, test items to check for correct mobile terminal operation must be drawn up, and a Work Item (WI) for this purpose has been established in CT WG6.

This article describes the conformance test[*3] specification now being created to check the operation of the interface between an LTE-capable mobile terminal and USIM.

2. Extension of USIM Files

2.1 Background to Extension

In standard specifications prior to

† Currently R&D Strategy Department

*1 **LTE**: Extended standard for the 3G mobile communications system studied by 3GPP. It is equivalent to "3.9G" or Super3G as proposed by NTT DOCOMO.

*2 **USIM**: An IC card used to store information such as the phone number from the subscribed mobile operator.

*3 **Conformance test**: A standard test for checking a communications device for proper operation based on standard functions and specifications established by a standards body.

the deployment of LTE (3GPP Release 8), provision was made for an EF_Location Information (LOCI) file and an EF_Packet Switched Location Information (PSLOCI) file for 3G-authentication use in the Circuit Switched (CS) and Packet Switched (PS) domains, respectively. Each of these files can store the Temporary Mobile Subscriber Identity (TMSI)[*4] and other information. These files made for smooth authentication when inserting a USIM into a different terminal or when crossing into a new area. These elements could just as well be stored in a mobile terminal's non-volatile memory, and for LTE authentication, the need for introducing a file similar to EF_LOCI and EF_PSLOCI in the USIM was discussed. Eventually, however, a new file named EF_Evolved Packet System Location Information (EPSLOCI) was specified, which brings us to the present state of deployment. In addition to this file, another new file named EF_EPS Non-Access-Stratum Security Context (EPSNSC) was specified for storing security context such as a cipher key. Referring to these files when moving a USIM from one terminal to another, for example, makes it unnecessary to re-execute the Authentication and Key Agreement (AKA)[*5] process from the beginning. This can shorten the time required for authentication (time for becoming attached to the network) and increase user convenience while also reducing network traffic.

2.2 Data Structure

The data structure of the EF_EPSLOCI file is shown in **Table 1** and described here. The LTE Globally Unique Temporary Identifier (GUTI)[*6] corresponds to TMSI in 3G. The last visited registered Tracking Area Identity (TAI)[*7] stores the last visited network and tracking area[*8], while the EPS update status stores values that indicate whether the last attach[*9] or detach[*10] process completed normally. These elements are described in detail in 3GPP TS 24.301 [2]. The data structure of the EF_EPSNSC file is shown in **Table 2**.

The EPS Non-Access-Stratum (NAS)[*11] security context element stores the K_{ASME} key value for cipher. Details on the use of K_{ASME} can be found in [3]. The detailed data structure is specified in 3GPP TS 31.102 [1] and details on each of the security parameters are specified in TS 33.401 [4].

3. Creation of Conformance Test Specification

For LTE, a test is needed to confirm that mobile-terminal operation is appropriate given the addition of new files to the USIM and the need for a mobile terminal to generate a cipher key in an authentication process different from that of 3G. For this reason, a WI for creating a conformance test was established at the CT WG6 meeting held in November 2008. As a supporting company, NTT DOCOMO is actively involved in the creation of test items, and it created a draft version of the test specification at the first ad hoc meeting for this purpose held in March 2009. This draft version was submitted to the CT WG6 meeting held in May 2009 for approval. It consists, in particular, of updates made to TS 31.121 [5], the test specification for interface operation between the mobile terminal and

Table 1 EF_EPSLOCI structure

Element	Stored Data	Length
GUTI	Temporary authentication ID	12 bytes
Last visited registered TAI	Last visited network and tracking area	5 bytes
EPS update status	Attach/detach completion status (normal/abnormal)	1 byte

Table 2 EF_EPSNSC structure

Element	Stored Data	Length
EPS NAS security context	K_{ASME}, etc.	12 bytes

*4 **TMSI**: A temporary ID used for user authentication by the network.
*5 **AKA**: An authentication process combined with key agreement. The USIM computes a cipher key and integrity key based on parameters supplied by the network and checks the validity of those parameters.
*6 **GUTI**: Information consisting of a Globally Unique MME Identifier (GUMMEI) and TMSI. This is a temporary ID used to uniquely identify a mobile terminal instead of using the mobile terminal's or user's (USIM) permanent ID.
*7 **TAI**: Information consisting of the Mobile Country Code (MCC) identifying the operator's country code, Mobile NW Code (MNC) identifying the operator's network code, and Tracking Area (see*8) Code (TAC).
*8 **Tracking area**: An area consisting of one or more cells and used as a unit for managing the positions of mobile terminals on the network; TAC is the code given to a tracking area by the operator.
*9 **Attach**: Procedure to register a terminal on the network when, for example, its power is switched on.
*10 **Detach**: Procedure to remove registration of a terminal from the network when, for example, its power is switched off.

USIM, and to TS 31.124 [6], the test specification for the Universal Subscriber Identity Module Application Toolkit (USAT)[*12] function.

4. Conclusion

This article described an extension to the USIM file in conjunction with LTE deployment and the creation of a conformance test specification for interface operation between an LTE-capable mobile terminal and LTE-capable USIM. This extension is expected to speed up the authentication process when moving a USIM from one mobile terminal to another or when crossing into a new area. The conformance test specification will enable the interface between the mobile terminal and USIM to be checked for proper operation based on established standard specifications before the launch of LTE services. Final specifications are scheduled to be completed in September 2009.

Looking forward, we plan to create test specifications for USAT and other functions.

REFERENCES

[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) Stage 3," 2009.
[3] A. Zugenmaier et. al: "Security Technology for SAE/LTE," NTT DOCOMO Technical Journal, Vol. 11, No. 3, pp. 27-30, Dec. 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.

*11 **NAS**: A functional layer between the mobile terminal and core network.
*12 **USAT**: A standard function specified by 3GPP TS31.111 enabling the use of USAT commands to provide a variety of functions and services between the network and USAT-function-capable USIMs and mobile terminals.