Access Security Authentication Encryption

Special Articles on SAE Standardization Technology

Security Technology for SAE/LTE

For a smooth transition from 3G to 4G, we have studied the requirements for new security functions to be introduced for LTE. Of those, security functions that have the same level as in the previous 3G or higher and functions for defense against current attacks from the Internet are particularly important. We therefore introduced a key hierarchy, separated security into an access stratum and a non-access stratum, and expanded the forwarding security functions during handover as the main new security functions for LTE.

DOCOMO Communications Laboratories Europe GmbH **Alf Zugenmaier**
Services & Solutions Development Department **Hiroshi Aono**

1. Introduction

The Long Term Evolution (LTE) architecture design is greatly different from the scheme used by the existing FOMA network (3G). That difference brings with it a need to adapt and improve the security functions. The most important requirement is that at least the same level of security as exists in the 3G network must be guaranteed in LTE. The main changes and additions made to satisfy that requirement are listed below [1][2].

- Introduction of a hierarchical key system in which keys can be changed for different purposes
- Separation of the security functions for the Non-access Stratum (NAS)[*1], in which processing is done for communication between a core network node and a mobile terminal (UE), from those functions for the Access Stratum (AS)[*2], which encompasses communication between the network edge (evolved Node B (eNB)[*3]) and the UE.
- Introduction of the concept of forward security, which limits the scope of harm when a compromised[*4] key is used
- Addition of security functions for interconnection between a 3G network and an LTE network

In this article, we describe the main new security functions for LTE to which NTT DOCOMO contributed in 3GPP Service and System Aspects (SA) WG3: introduction of a key hierarchy, separation of the NAS security functions from AS security and expansion of forward security functions for handover.

2. LTE Security Requirements

Currently, the security functions for 3G services [3] are in wide use, providing the 3G network with confidentiality of user IDs, authentication, confidentiality of the User Plane (U-Plane)[*5] and the Control Plane (C-Plane)[*6] as well as C-Plane integrity protection[*7] at a security level in conformance with other

[*1] **NAS**: The functional layer in the Universal Mobile Telecommunications System (UMTS) protocol stack between the core network and the UE.

[*2] **AS**: The functional layer in the UMTS protocol stack between the eNB (see *3) and the UE.

[*3] **eNB**: A base station for the LTE radio access system.

[*4] **Compromised**: A security relevant item (such as a key) is compromised, if it is known to or can be accessed by an unauthorized party.

international standards.

There are four main requirements for security functions in LTE:

- Provide at least the same level of security as the 3G network without affecting user convenience.
- Provide defense against current attacks from the Internet.
- The security functions provided by LTE shall not affect the step-wise transition from 3G to LTE.
- Allow continued used of the Universal Subscriber Identity Module (USIM)[*8].

The latter two are satisfied by re-using the 3GPP Authentication and Key Agreement (3GPP AKA)[*9] mechanism.

The security requirements for the evolved packet core, i.e., the LTE core network, can be satisfied by applying Network Domain Security (NDS)[*10] on the IP layer as standardized in TS33.210 [4], in the same way as for 3G.

However, because some of the Radio Network Controller (RNC) functions are integrated into the eNB in LTE, the 3G security architecture cannot be re-used as-is for the radio access network in LTE. Specifically, eNB stores the key for encryption and integrity protection only while the UE is in the connected state. Thus, for example, the key for acting on the signal message is not stored when the UE is not connected, unlike in 3G.

Furthermore, the eNBs in LTE may be installed in exposed locations to ensure coverage for indoor areas such as offices and sufficient wireless capacity, a measure that is expected to increase the risk of unauthorized access to eNB. Therefore, the measures described below are specified to minimize the harm that may result when a key is stolen from an eNB.

3. Key Hierarchy

For data encryption, LTE uses a stream encryption method in which data is encrypted by taking an exclusive OR (XOR)[*11] of the data and key stream[*12] in the same way as is done in 3G. It is very important in that method that the key stream will never be re-used. The algorithms used in 3G and LTE [5][6] generate a key stream of finite length. Therefore, to prevent re-use of the key stream, the key used to generate the key stream is changed regularly, e.g. when connecting to a network or during handovers, etc. In the 3G network, execution of AKA is necessary to generate that key. Executing AKA may take several hundreds of milliseconds for key computation on the USIM and for connection to the Home Subscriber Server (HSS)[*13], so a function that allows key updating without executing AKA must be added to achieve a higher data rate as in LTE.

In addition, to minimize the harm that may result if one of the keys used for encryption or integrity protection becomes compromised, it is desirable that the same key isn't stored and used at multiple locations on the network. To solve that issue in LTE, we introduced a hierarchical key system (**Figure 1**).

In the same way as for the 3G network, the USIM and Authentication Center (AuC)[*14] share secret information (key K) in advance.

- When AKA is executed for mutual

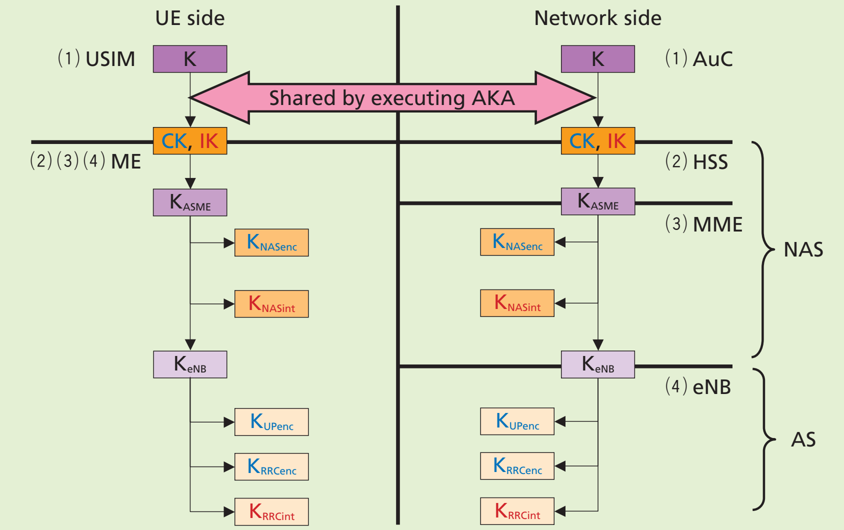

Figure 1 Hierarchical keys and method for key generation between entities in LTE

[*5] **U-Plane**: The protocol for transmitting user data.

[*6] **C-Plane**: The protocol for transmitting control signals.

[*7] **Integrity protection**: Security technology against communication data tempering.

[*8] **USIM**: An application on an IC card to persistently store subscriber information such as configuration and authentication data as well as subscriber defined information such as phone numbers.

[*9] **3GPP AKA**: A 3GPP protocol for mutually authenticating network and USIM and for sharing temporary keys for encryption and integrity protection.

[*10] **NDS**: Security between the nodes within a network domain.

authentication by the network and user, key CK for encryption and key IK for integrity protection are generated and respectively passed from USIM to Mobile Equipment (ME) and from AuC to HSS.

- ME and HSS generate K_{ASME} from the key pair CK and IK using a key generation function that is based on the ID of the visited network. By establishing the correspondence of that key, HSS guarantees that this K_{ASME} can be used only by the visited network. K_{ASME} is transferred from the HSS to the Mobility Management Entity (MME)[*15] of the visited network to serve as basic information on the key hierarchy.
- The K_{NASenc} key for NAS protocol encryption between the UE and the MME and the K_{NASint} key for integrity protection are generated from the K_{ASME}.
- When the UE is connected to the network, MME generates the K_{eNB} key and passes it to the eNB. From this K_{eNB}, the K_{UPenc} key for U-Plane encryption, the K_{RRCenc} key for Radio Resource Control (RRC) encryption and the K_{RRCint} key for integrity protection are generated.

4. Separation of AS and NAS Security Functions

Because it is assumed that a large volume of data can be transmitted only when the UE is connected, the LTE network establishes security associations[*16] between the UE and eNB only for UEs that are connected. Accordingly, for UEs in idle mode, there is no need to preserve state in an eNB. Because NAS messages are exchanged with idle mode UEs, NAS security associations are established between the UE and core network nodes, i.e. the MME.

After UE authentication, the MME retains the K_{ASME}, which is the topmost key of the key hierarchy in the visited network. The NAS security mode command negotiates the encryption and integrity protection algorithms for NAS communication using K_{NASenc} and K_{NASint} keys. At this point, the MME must determine from which UE the authentication request message arrived in order to find the correct keys to use for decryption and to verify the data integrity. However, the UE ID (International Mobile Subscriber Identity (IMSI)) should be protected in the radio area, so a temporary ID called the Global Unique Temporary Identity (GUTI)[*17] was introduced in the LTE to identify the UE instead of using the IMSI. This GUTI is changed periodically, so it is not possible to trace which GUTI the UE is using.

As soon as the UE enters the connected state, the eNB switches on the AS protection functions with the AS security mode command. Afterwards, AS security is applied to all communication between the UE and the eNB. The algorithm used for AS is negotiated independently from the algorithm used for NAS. In countries that do not allow encryption, it is possible to negotiate a mode that does not provide security through encryption.

In the LTE, encryption and integrity protection algorithms based on Snow 3G[*18] and Advanced Encryption Standard (AES)[*19] are standardized. While those two algorithms each provide full security, two standard algorithms that differ in basic structure are used in 3GPP so that even if one algorithm is broken, the other can be used for continued secure use of the LTE system.

5. Handover Security

Installation of an eNB in an exposed location creates a high risk of unauthorized access to it, so adequate security is required. To achieve that, the concept of forward security was introduced to LTE. Here, forward security means that, without knowledge of K_{ASME}, even with knowledge of the K_{eNB} that is shared by the UE and the current eNB, computational complexity prevents guessing the future K_{eNBs} which will be used between the UE and eNBs to which the UE will connect in the future. Thus, the encryption will not be broken.

The model for key transmission at handover in LTE is shown in **Figure 2**. When the initial AS security context is shared by UE and eNB, MME and UE must respectively generate the K_{eNB} and the Next-hop parameter[*20] (hereinafter referred to as "NH"). K_{eNB} and NH are

[*11] **XOR**: A logical computational operation in which the value of the given input is taken as true when there is an odd number of true bits and false when there is an even number of true bits.

[*12] **Key stream**: In stream encryption, encryption is done by performing a bit-wise XOR of the plaintext data with a pseudo-random number. The pseudo-random number generated by stream encryption is called a key stream.

[*13] **HSS**: A subscriber information database in a 3GPP mobile communication network; it manages authentication information and network visiting information.

[*14] **AuC**: A logical node in 3GPP for storing user authentication data and other data related to security.

[*15] **MME**: A logical node for mobility management and control.

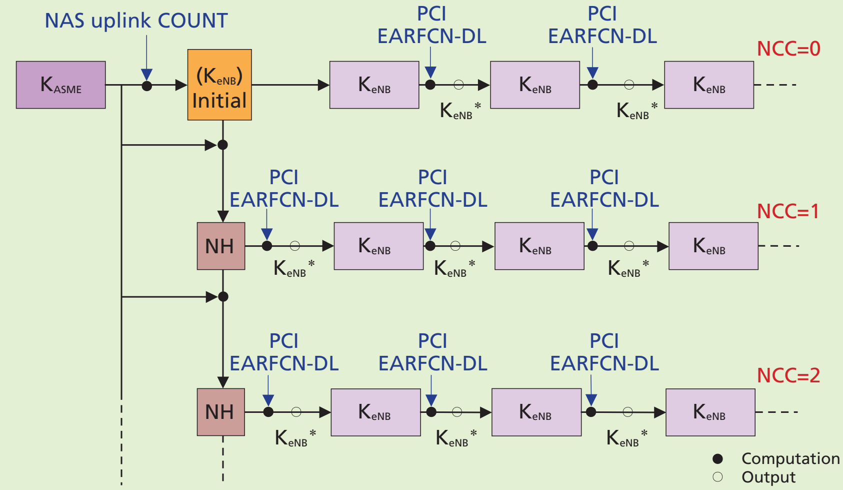

Figure 2 Key chain model for handover

generated from K_{ASME}, and there is a K_{eNB} and NH for each NH Chaining Counter (NCC)[*21]. Those respective K_{eNB} are generated from the NH value for each NCC. In the initial setting, K_{eNB} is generated directly from K_{ASME} and the NAS uplink COUNT, resulting in an NCC=0 key chain. With the initial setting, the derived NH value is also used for a key chain of NCC=1 or less.

K_{eNB} is used as the base key for securing communication between UE and eNB. For handover directly between eNBs, $K_{eNB}{}^*$, the new key, is generated from the active K_{eNB} or from the NH. In the figure, a horizontal key derivation depicts generation of $K_{eNB}{}^*$ from the existing K_{eNB},; vertical key derivation depicts generation of $K_{eNB}{}^*$ from the NH. In handovers using vertical key derivation, $K_{eNB}{}^*$ is generated from NH with additional inputs of the connection's E-UTRAN Absolute Radio Frequency Channel Number-Down Link (EARFCN-DL) and its target Physical Cell Identity (PCI). In handover using horizontal key derivation, the $K_{eNB}{}^*$ is generated from current K_{eNB} using the target PCI and its EARFCN-DL as additional parameters.

Because NH can be calculated only by UE and MME, this use of NH provides a method that achieves forward security in handovers across multiple eNBs. In that case, the n-hop forward security at the time of vertical key delivery means that the future K_{eNB} to be used when UE connects to another eNB after n (where n is 1 or 2) or more handovers cannot be guessed because of computational complexity. This function can limit the scope of harm, even if a key is leaked, because future keys will be generated without using the current K_{eNB} in case of vertical key delivery.

6. Conclusion

LTE security functions must provide at least the same level of security as provided by 3G security functions, and still minimize the effect on the previous architecture. The current 3GPP Release 8 has standardized the security functions that satisfy those requirements. In the future, we will continue to develop new security functions such as Home eNB security and Machine to Machine (M2M) security for standardization in Release 9.

References

[1] 3GPP TS33.401 V8.4.0: "3GPP System Architecture Evolution (SAE); Security architecture," 2009.

[2] 3GPP TR33.821 V8.0.0: "Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE)," 2009.

[3] 3GPP TS33.102 V8.3.0: "3G security; Security architecture," 2009.

[4] 3GPP TS33.210 V8.3.0: "3G Security; Network Domain Security; IP network layer security," 2009.

[5] 3GPP TS35.201 V8.0.0: "Specification of the 3GPP confidentiality and integrity algorithm; Document 1: f8 and f9 specification," 2008.

[6] 3GPP TS35.216 V8.0.0: "Specification of the 3GPP confidentiality and integrity algorithm; Document 1: UEA2 and UIA2 specification," 2008.

*16 **Security association**: Establishes a secure communication path by exchanging or sharing information such as encryption methods and encryption keys before communication begins.

*17 **GUTI**: A temporary ID used to distinguish users in SAE/LTE.

*18 **Snow 3G**: A stream encryption method used in LTE.

*19 **AES**: A symmetric key encryption method that has been adopted as a new encryption standard by the U.S.A. It is also one of the cryptosystems used in 3GPP.

*20 **Next-hop parameter**: A key generated by UE and MME to implement forward security. It's value is changed when NCC (see *21) is incremented.

*21 **NCC**: The next-hop counter, which is incremented when a vertical handover is executed.