

Access Security in 3GPP-based Mobile Broadband Systems

GEIR M. KØIEN



Geir M. Køien is a postdoctoral (researcher) at the University of Agder, Norway

In this article we shall take a brief look at access security in the 3GPP-based mobile broadband systems. We shall mainly look at access security in UMTS and LTE, but will also briefly look at the latest status of GERAN access security. Furthermore, we shall see that the GSM SIM is not an acceptable platform for supporting true mobile broadband subscribers.

1 Overview

1.1 Access Security Goals

The primary goal of access security is to authenticate the subscribers and to ensure that access to the system is protected. To be able to do this the subscriber must have a unique identity and a set of security credentials. In the early days (1G, 2G) the authentication was one-way, ie. only the subscriber was authenticated. Later on, authentication became mutual and included indirect verification of the network. While the modern access security architectures offer solid protection it is worth noting that there are limitations to the scope and range of the offered protection. Even if the protection may be pervasive and strong for the access channel, it is nevertheless limited in scope to the access network. That is, the access security schemes do not provide end-to-end protection.

In the 3GPP-based systems one now has three different security architectures: a) Access security for the 2G systems (GSM/GPRS); b) Access security for the 3G system (UMTS); and c) Access security for the new LTE system. Now, GSM/GPRS based communication cannot reasonably be called broadband, but we cover it here since fallback to EDGE-based services is a realistic scenario for mobile broadband services in suburban/rural areas.

1.2 Access Security Concepts

The following is a brief security primer on some terms used in access security in 3GPP-based systems. Some of the definitions are partly taken from TS 33.102 [5]. The basis for all access security in 3GPP is the use of symmetric key cryptography.

- **Entity Authentication:** The provision of assurance of the claimed identity of an entity.
In plain English: Entity authentication is the process of verifying a claimed identity. In 3GPP this amounts to verifying the IMSI of a subscriber.
- **Challenge-Response (part of the AKA protocol)**
This is the entity authentication scheme used in the 3GPP systems. The network challenges the sub-

scriber with a RANDom challenge. If, and only if the subscriber is the claimed subscriber will it be able to compute, by use of a cryptographic one-way function and the authentication secret, the correct RESponse. The challenge may itself be authenticated (UMTS AKA and EPS-AKA).

- **Authentication and Key Agreement (AKA) protocol**

An AKA protocol is a structured scheme with the aim of verifying the identity of one (the subscriber) or both of the part-taking entities. During the process one also agrees on keys (or key material) for subsequent use in protecting the access link.

- **Cryptographic One-way function (keyed)**

A keyed cryptographic one-way function is designed to be computationally infeasible to reverse and to provide an apparently total de-correlation between the input and the output. The output is required to be uniformly distributed and unpredictable. For example, for the function $f_K(X) \Rightarrow Y$, we require that it be computationally infeasible to derive K from knowledge of $f()$, X and Y . Or to derive X from knowledge of $f()$ and Y . We also require it to be computationally infeasible to derive Y from knowledge of $f()$ and X . The essential property is that one must have access to K in order to compute Y from X .

- **Pseudo-Random Function (prf)**

A cryptographic prf() function algorithmically produces an apparently random looking output. It is based on an internal state (the starting state commonly needs to be secret) and produces uniformly distributed output. The output should be unpredictable and not repeat for the given context. The prf() is used to generate RANDom challenge data.

- **GSM AKA**

The AKA protocol used in GSM and GPRS. It provides only assurance of the subscriber (no network or challenge verification). The Key Agreement provides on 64 bit key (K_c).

- **UMTS AKA**

The AKA protocol used in UMTS. It provides assurance of the subscriber and indirect verification of the network (through verification of the challenge). The Key Agreement provides two 128 bit keys (CK, IK). UMTS AKA may be run over GERAN.

- **EPS-AKA**

The AKA protocol used in LTE is called EPS-AKA, and for authentication it is very similar to UMTS AKA and provides roughly the same level of identity assurance. The Key Agreement is based on the CK, IK keys which is transformed into the 256 bit wide K_{ASME} master key. From this basis a full key hierarchy is derived.

- **Data Confidentiality**

The property that information is not made available or disclosed to unauthorised individuals, entities or processes. In plain English: Data confidentiality is the security service that prevents eavesdropping on the exchanged data, through the use of data encryption (A5, GEA, f8, EEA functions)

- **Data Integrity**

The property that data has not been altered in an unauthorised manner. In plain English: Data integrity is the security service that detects willful manipulation of the exchanged data. The services cannot prevent unauthorised alterations, but alterations will be detected and so the receiving party will not be fooled by an attacker. A closely related concept is ‘data origin authentication’ in which one provides data integrity for the identity of the sending party. In both cases one computes a cryptographic integrity checksum over the data and appends the result to the data (f9 function in UMTS, EIA function in LTE).

- **Attacker, Adversary, Intruder**

This is a party with a ‘malicious’ intent to break the security of the system or to get access beyond its own authorization. The attacker/adversary concept is often associated with real-life miscreants. The Intruder is a concept more often used in security modelling.

- **Subscriber Security Credentials**

The basic security credentials would include the identity (IMSI) and an authentication secret (called K_i in GSM/GPRS, and K in UMTS/LTE). Additionally, and associated with the subscription, we have a set of authentication algorithms (AKA functions).

- **Tamper Resistant Module**

Security in 3GPP is based on the subscriber having a tamper resistant module, a piece of hardware which protects the subscriber security credentials and provides a protected execution environment for the AKA functions. The protection must include data integrity and data confidentiality. In GSM/GPRS the tamper resistant module is the SIM card and in UMTS and LTE the module is the UICC. We note that the module is not required to be *tamper proof*, since that goal is unattainable in practice. Instead we require that the module should be tamper resistant to the extent that the effort involved in breaking the security of the module is substantial, ie. that the security of the module is not the weakest link.

2 Access Security in 2G Systems (GSM/GPRS)

2.1 Background

In the early days of the 1G systems (up to ca. 1985) there was not much in terms of access security. One example is the NMT system, which initially only had a 3-digit ‘secret’ password system¹⁾. This inevitably led to problems and it became apparent that one needed proper subscriber authentication. NMT itself got its NMT-SIS extension, which provided a hardware based security element in the phone and a one-way challenge-response mechanism to verify the user identity. In GSM, one took the concept further and added the now ubiquitous SIM card. The SIM card, which is a smartcard, contains the authentication credentials, including the subscriber identity (the IMSI number). Since the GSM system was designed to be all-digital from day one it was possible to provide data confidentiality. The data confidentiality is provided by the A5-family of stream cipher functions. To do its business, the A5 cipher needs a 64-bit symmetric key (K_c)²⁾. So it was clear that the GSM authentication scheme would also need to produce a session key for use with the A5 cipher. Thus was born the GSM AKA protocol. GSM then has the following:

- An authentication protocol to verify the subscriber identity;
- A cipher mechanism to protect the over-the-air transmission.

The GPRS system is overlaid on top of GSM, and so the GSM AKA protocol is also used for GPRS. The

¹⁾ The ‘password’ was not known to the user, but it was in fact sent in plaintext over-the-air.

²⁾ Symmetric key: The same key is used for both encryption and decryption.

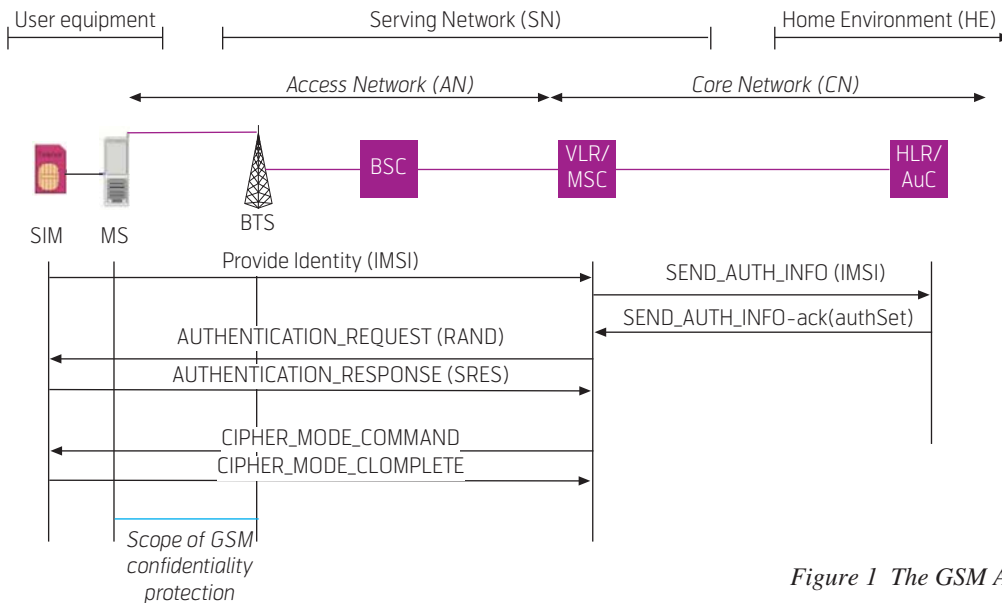
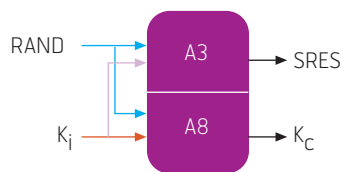


Figure 1 The GSM AKA Protocol



A3/A8 are operator specific functions. Widely used "example" algorithms exists:

- COPM128 (very bad)
- COMP128-2 (ok, but only 54 bit)
- COMP128-3 (ok, all 64 bits)
- GSM milenage (very good)

Figure 2 The A3/A8 authentication and key derivation algorithms

key K_c is likewise used in GPRS, but here it is input to the GEA-family of data confidentiality algorithms. A notable difference between GSM and GPRS is that while GSM over-the-air protection is between the MS and the BTS, the GPRS protection is between the MS and the SGSN.

2.2 The GSM AKA Protocol

The GSM AKA protocol is executed in two phases. One starts by forwarding of the so-called triplet (also known as an *authentication set*) from the HLR/AuC to the VLR/SGSN.

GSM triplet = {RAND,SRES, K_c }

The second phase consists of running the GSM challenge-response protocol [1].

Figure 1 depicts the message sequence. The outline of the challenge-response scheme is as follows: The VLR/MSC sends the *random challenge* (RAND) to

the MS/SIM. The SIM computes a *signed response* (SRES) and a session key (K_c) based on the RAND and an authentication secret (K_i). The 128 bit wide key K_i is only known to the SIM and the AuC of the home environment (which generated the *challenge* and the corresponding *response* in the first place). When the MS/SIM forwards the SRES to the VLR/MSC, the VLR/MSC will compare it with the SRES it received from the HLR/AuC. If the two match then it is taken as proof that the MS/SIM is the entity it claims to be.

In GSM AKA we have two algorithms which compute the session key and the signed response. The A3/A8 algorithms, Figure 2, are interface definitions; the implementations are operator specific, but most operators use one of the COMP128 algorithms (see [4] for recommendations on algorithm use).

2.3 The A5 and GEA Algorithms

The A5 and GEA algorithm families are used in GSM and GPRS respectively. The A5 family consists of the following 64-bit stream-cipher algorithms:

- **A5/1 – The original (default) A5 algorithm**
A5/1 is implemented in all GSM handsets and in all GSM base stations (BTSes). By now it is showing its age. The obvious replacement is the A5/3 algorithm.
- **A5/2 – The very weak export-control algorithm**
A5/2 was internationally weakened to permit export to 'hostile' countries. It has been officially deprecated (should not be used in any network!).
- **A5/3 – This algorithm is based on the KASUMI cipher (used in UMTS)**
A5/3 has no known weaknesses and it is the new

recommended algorithm for use in GSM. It will gradually replace A5/1.

The A5/3 algorithm is not completely future proof. This is due to the inherent limitation in the length of the key Kc, which is only 64-bit wide. The 3GPP has therefore recently approved a new algorithm called A5/4 [2,3]. This new algorithm is internally identical to A5/3, but it has a new interface and it now accepts a 128 bit key (Kc₁₂₈). To use A5/4 one must also use a UICC/USIM and execute the UMTS AKA protocol (that is, one runs UMTS AKA over GERAN). Based on the CK,IK key-pair one then derives the new 128 bit key (Kc₁₂₈) (see [6]). The A5/4 algorithm is expected to be future proof for the lifetime of GSM networks. A corresponding 128-bit GPRS algorithm also exists (GEA4). The other GEA algorithms all use the 64-bit Kc key. The original GEA algorithm is effectively only a 54 bit algorithm, while GEA2 and GEA3 are full 64 bit algorithms.

3 Access Security in 3G Systems (UMTS)

3.1 Background for the 3G Systems

The 2G systems did a good job in protecting its customers and its operators from harm, but they were not perfect. An important shortcoming was the lack of network authentication. The 3G system, like UMTS and/or CDMA2000, therefore have *mutual* entity authentication [5]. Furthermore, it was also decided that 64 bit cipher algorithms were inadequate for the 3G systems. So, the key size was extended to 128 bits, and one decided to provide separate keys for

data confidentiality and for data integrity. The idea of using a smartcard (the SIM card) was retained in the guise of the UICC smartcard. The USIM security application is executed by the UICC. Backwards compatibility dictated that one had to be able to access the 3G system (UMTS) with a 2G subscription (SIM card), but one then essentially only gets the GSM security level in UMTS.

3.2 The UMTS AKA Protocol

The UMTS AKA protocol is based on the GSM AKA message exchange (Figure 3), but this time the challenge is authenticated by signing it with a message authentication code (MAC-A) [5]. To avoid replay of earlier (valid) challenges a unique sequence number is added to the challenge data (it is authenticated too). This allows the USIM to verify that *a*) the challenge was generated by the HE (AuC), and *b*) that the challenge has not been used before. Thus, the USIM has assurance of the validity of the challenge and takes this to be proof of network validity³⁾. In the UMTS AKA protocol, like its 2G cousin, the home environment (HE) delegates execution of the challenge-response scheme to the serving network (SN). To do so, the HE forwards an Authentication Vector (AV) to the SN.

$$\text{UMTS AV} = \{\text{RAND}||\text{XRES}||\text{CK}||\text{IK}||\text{AUTN}\}^4)$$

The UMTS AKA protocol also includes derivation of two 128-bit wide session keys (CK and IK). The 3GPP has provided a default set of AKA functions called the MILENAGE algorithm set [6]. Formally, MILENAGE, which is based on the AES crypto-primitive [7], is an example set. MILENAGE contains all

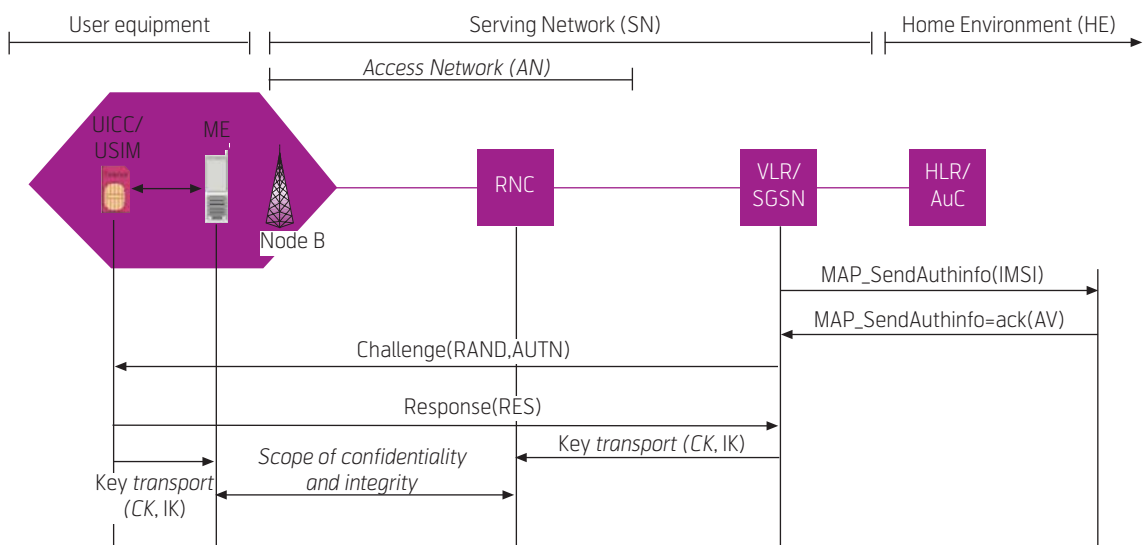


Figure 3 The UMTS Authentication and Key Agreement Protocol

³⁾ But it does not prove that the HLR/AuC is online and it does not actually verify the SN (only that the SN possesses a valid challenge).

⁴⁾ The symbol || is used to denote concatenation.

AKA functions, with exception of the f0 function (pseudo-random function).

3.3 The KASUMI and SNOW-3G Cipher (f8/f9 Functions)

KASUMI was the original algorithm for the f8 (data confidentiality) and the f9 (data integrity)⁵⁾ functions in UMTS [8]. Figure 3 depicts the range of the UMTS link layer protection. The KASUMI cipher was designed from the MISTY1 cipher, and uses a 64-bit internal block length under control of a 128-bit key. Subsequently, the 3GPP has adopted a second cipher suite for use with UMTS, called SNOW-3G (based on SNOW 2.0). The SNOW-3G cipher is a stream cipher [9]. It was designed to be a companion cipher to the KASUMI cipher for use with UMTS⁶⁾. Internally, the SNOW-3G cipher is a true 128-bit cipher. The SNOW-3G cipher is also adopted for use with LTE. For more information on the f8/f9 functions please see TS 33.102 [5].

3.4 Summary of 3G Access Security

The UMTS access security architecture has been very successful. It builds on the 2G model and extends it with mutual entity authentication. The use of a smart-card as the basis for subscriber security was retained. With respect to session key generation, UMTS has a system where one only generates new keys when the UMTS AKA protocol is executed. Ideally, one would have wanted to be able to generate new keys more often, for instance in conjunction with handover events etc. The session keys produced in UMTS are 128 bit wide and this seems sufficient for the foreseeable future. Another point worth noting is that in UMTS one terminates access security in the RNC, which is situated relatively deep inside the access network. This, together with the lack of separation between signalling (control plane) traffic and user plane traffic means that the UMTS architecture has a few inherent limitations when it comes to providing responsive high-bandwidth services.

4 Access Security in 4G Systems (LTE)

4.1 Background for the 4G Systems

The LTE architecture is not formally a 4G architecture, but LTE-Advanced will be a full 4G architecture. In terms of access security architecture, there will not be any significant differences between LTE and LTE-Advanced. The LTE security architecture

(also known as the SAE/EPS security architecture) is quite different from its 2G and 3G cousins. This reflects changes in the LTE systems architecture (with respect to 2G/3G) and improvements to the access security. The handling of backwards compatibility is very important in an evolved architecture. So, for LTE it was decided that (subscriber-side):

- The GSM SIM would be *insufficient* for accessing LTE;
- The UMTS UICC/USIM would be retained as an essential part of the LTE architecture. No replacement for the UICC/USIM was deemed necessary;
- The mobile equipment (ME) will derive the LTE keys. The UICC/USIM does not know about LTE specific security features. Thus, the LTE key hierarchy has to be derived by the ME.

Figure 4 depicts the E-UTRAN architecture. The EPS-AKA is executed between the UE and the MME. The access protection in LTE is divided into separate protection for the control plane and the user plane. Furthermore, one distinguishes between AS protection (the LTE-Uu interface) and NAS protection (UE – MME). The eNB plays an important part in the security architecture. See [10,11] for an extensive discussion of the LTE security architecture. TS 33.401 [12] is the primary source for the security architecture.

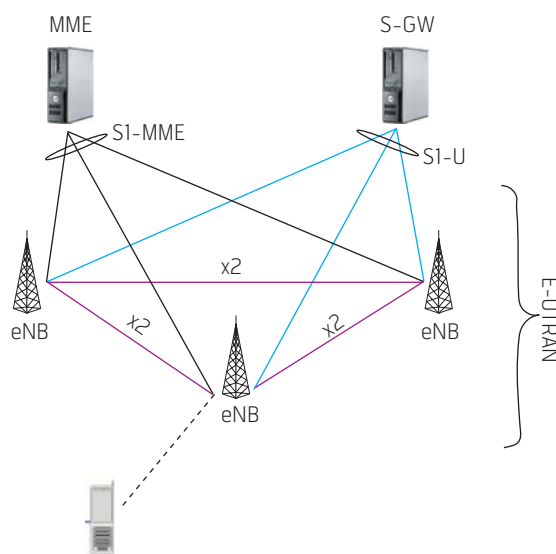


Figure 4 Overview over the E-UTRAN Architecture

5) The integrity protection only applies to control plane (signalling) data.

6) SNOW-3G is not a replacement for KASUMI as such, and importantly KASUMI is still safe to use. However, KASUMI (with its 64-bit block length limitation) was not considered a suitable choice for LTE.

4.2 The EPS-AKA Protocol

The authentication part of the EPS-AKA protocol consists mainly of the UMTS AKA protocol with some minor additions. One change is the fact that the EPS-AKA protocol is executed between UE and the MME instead of between the USIM and the VLR/SGSN. Secondly, one has amended the protocol to include indication that the protocol is run in an EPS/LTE context and not in a 3G context. With respect to the UICC/USIM the protocol execution is exactly identical to the execution of the UMTS AKA protocol.

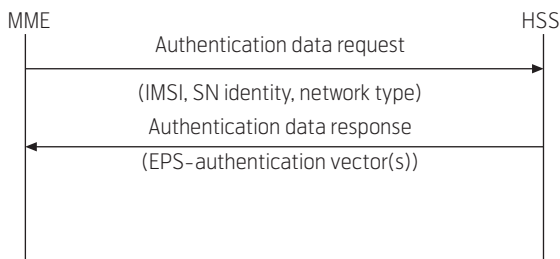


Figure 5 EPS-AV Distribution over the Diameter based S6a Interface

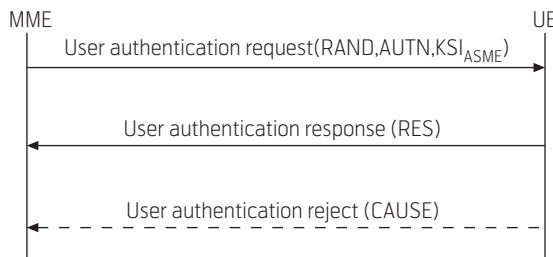


Figure 6 EPS-AKA (distinct from UMTS AKA by use of a 'separation bit') in AUTN (AMF part)

Another interesting change to the authentication is that the EPS Authentication Vector (EPS-AV) is generated for the specific target network through inclusion of the 'SN Identity' (Figure 5) in the AV derivation. The UE (USIM/ME) will use the beacons 'SN Identity' when computing the AV. Technically speaking, the 'SN Identity' is part of the input when computing the master key K_{ASME} , using the concatenated UMTS AKA keys (CK||IK) as the controlling key (see Annex A in TS 33.401 [12] for more information).

$$EPS-AV = \{K_{ASME}, RAND, AUTN, XRES\}$$

The so-called 'separation bit' in the AUTN part of the EPS-AKA challenge is set to indicate that the executed AKA is EPS-AKA and not UMTS AKA. This is verified by the ME (the USIM is oblivious to the difference between EPS-AKA and UMTS AKA; although it does verify that AUTN is valid it has no knowledge of EPS/LTE as such⁷⁾). Figure 6 depicts the EPS-AKA message exchange between the UE and the MME. The KSI_{ASME} is an index to the generated security context.

4.3 The LTE Key Hierarchy

The LTE architecture is substantially different from its 3G antecedent in that one needs many more keys and that one now separates the *control plane* from the *user plane*, both with respect to termination points and with respect to the actual keys used. The consequence is that one needs more keys and that the keys are needed at different places. To ensure that all needs are covered an extensive key hierarchy has been designed. The master key for the duration of the EPS-AKA context is the 256-bit wide K_{ASME} . This key is constructed from the CK,IK key-pair that is

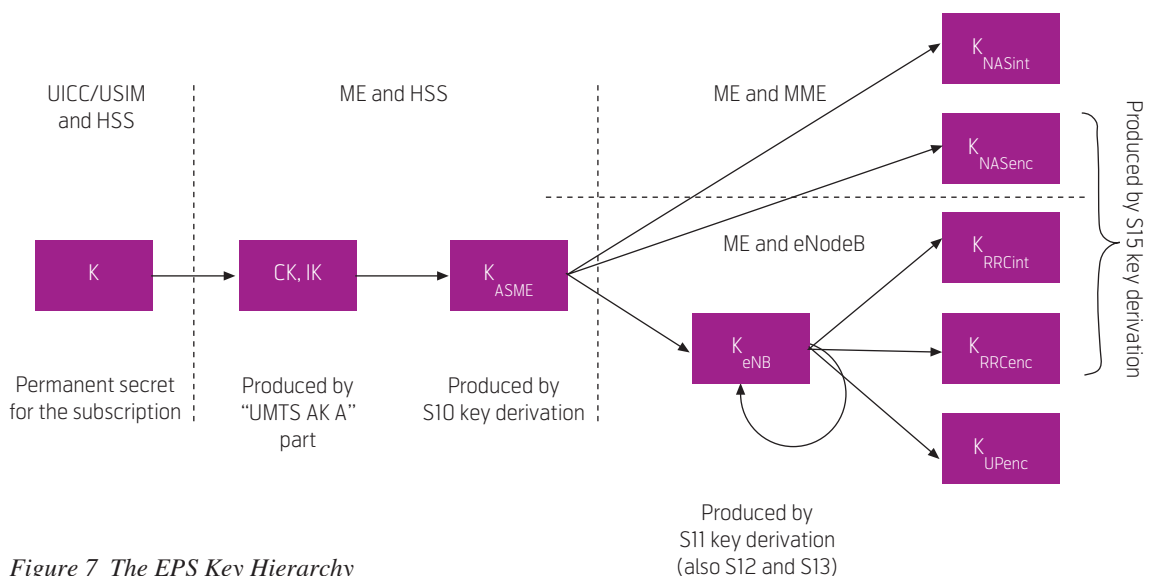


Figure 7 The EPS Key Hierarchy

⁷⁾ A Release 99 USIM is sufficient for an LTE capable ME to access E-UTRAN.

natively produced by running the UMTS AKA. The K_{ASME} master key is not used directly, but is instead the basis for deriving the 128-bit wide NAS keys, used for data protection between the UE and the MME, and the 256-bit wide K_{eNB} root key. The K_{eNB} root key is the basis for deriving all keys that are used between the UE and the eNodeB (eNB). The K_{eNB} itself is bounded to a specific eNB. Thus, a handover event will cause derivation of a new K_{eNB} , including regenerating all dependent keys.

Figure 7 depicts the LTE key hierarchy. We shall not go into the details of the key derivations, which are fairly complex. More details of the key derivations can be found in [10,11,12].

We note that one may create EPS contexts from so-called *legacy* contexts (created by UMTS AKA) and that the EPS context can be used for generating UMTS contexts. One may also use an EPS context to generate a GSM/GPRS context (transformation via a UMTS context), but that it is strictly prohibited to use a GSM/GPRS context to derive an EPS context.

4.4 LTE Summary

Access security in LTE is quite different from the architecture found in 3G/UMTS. One still uses the USIM, and the EPS-AKA is very similar to the UMTS AKA, but there are significant differences:

- Use of USIM is required (GSM SIM will not work).
- The eNodeB is now a very important security element (and it must be protected).
- Separation of control plane and user plane (EPS-AKA terminates in MME, but user plane traffic does not go to MME).
- Full key hierarchy, with frequent key changes independent of EPS-AKA (ie. during handover).

5 Concluding Remarks

Access security in mobile broadband is coming of age with the new LTE access security architecture [10,11,12], where one has a mature architecture which separates between control plane and user plane and where one is able to generate new session keys independently of carrying out a full AKA sequence (ie. very fast re-keying for local handovers). Ideally, it would have been beneficial to have the HE being online during the EPS challenge-response sequence. In the absence of that, it is reassuring that one can now cryptographically bind the EPS-AV to specific serving networks.

Access security in UMTS still gets the job done, but it is a bit inflexible and not really adapted for mobile broadband. The restrictions and limitations are mostly theoretical, but the UMTS architecture was not really designed for high-bandwidth mobile broadband services and this is beginning to show.

In this article we have also briefly presented access security in the GSM/GPRS system, which definitively is not a mobile broadband system. However, mobile broadband subscribers cannot expect pervasive 4G coverage. In fact they cannot even expect the 3G (UMTS) coverage to be pervasive and so they may have to use 2G (EGDE) services from time to time. In this respect it is worth noting that support for 128-bit encryption over-the-air is becoming available to GERAN users too through the new A5/4 and GEA4 ciphers. The prerequisites are that the ME and the networks support A5/4 (BTS) and GEA (SGSN), and that the subscriber has a UICC/USIM. The serious network provider would anyhow issue UICC/USIM to its mobile broadband subscribers (and of course UICC/USIM is a prerequisite for access to LTE/LTE-Advanced networks).

Acknowledgements

Some of this material was written while the author was employed by Telenor. Some of the figures in this article are from the book *Entity Authentication and Personal Privacy in Future Cellular Systems* [11], by kind permission of River Publishers.

References

- 1 3GPP. *Security related network functions (Release 9)*. Sophia Antipolis, France, December 2009. (3GPP TS 43.020)
- 2 3GPP. *3G Security; Specification of the A5/4 Encryption Algorithms for GSM and ECSD, and the GEA4 Encryption Algorithm for GPRS (Release 6)*. Sophia Antipolis, France, February 2004. (3GPP TS 55.226) (Only an unofficial version presented to the SA3 workgroup is currently available)
- 3 Kjøien, G M. *Mobile Access Security; Introducing 128-bit cipher algorithms in GSM/GPRS*. Fornebu, Telenor GBD&R, 2009. (R&I N 25/2009)
- 4 Johannessen, T H, Kjøien, G M, Lupetti, S (ed). *Access and OTA Security*. Fornebu, Telenor GBD&R, 2009. (R&I N 22/2009)

- 5 3GPP. *3G Security; Security architecture (Release 9)*. Sophia Antipolis, France, December 2009. (3GPP TS 33.102)
- 6 3GPP. *3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions $f1$, $f1^*$, $f2$, $f3$, $f4$, $f5$ and $f5^*$; Document 1: General (Release 9)*. Sophia Antipolis, France, December 2009. (3GPP TS 35.205)
- 7 NIST. *Advanced Encryption Standard (AES)*. FIPS-197, November 2001.
- 8 3GPP. *3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: $f8$ and $f9$ Specification (Release 9)*. Sophia Antipolis, France, December 2009. (3GPP TS 35.201)
- 9 3GPP. *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications (Release 9)*. Sophia Antipolis, France, December 2009. (3GPP TS 35.215)
- 10 Kjøien, G M. *Mobile Access Security; An Introduction to Access Security in LTE*. Fornebu, Telenor GBD&R, 2009 (R&I N 27/2009)
- 11 Kjøien, G M. *Entity Authentication and Personal Privacy in Future Cellular Systems*. Aalborg, Denmark, River Publishers, 2009. (ISBN 978-87-92329-32-5)
- 12 3GPP. *3GPP System Architecture Evolution (SAE): Security architecture; (Release 9)*. Sophia Antipolis, France, December 2009 (3GPP TS 33.401)

Geir M. Kjøien is a postdoctor (researcher) at the University of Agder, Norway, where he works with cellular security, personal privacy and similar topics. He holds a BSc.hons in Computing Science from the University of Newcastle upon Tyne, England, an MSc in IT from the Norwegian University of Science and Technology (NTNU, then NTH), and a PhD from Aalborg University (AAU). Kjøien has previously worked for Telenor and participated in security standardization in 3GPP during 1999–2009 as the Telenor delegate. He has worked extensively with access security in GSM/GPRS, UMTS and LTE.

email: geir.koien@uia.no