Security in the Evolved Packet System

Security is a fundamental building block of wireless telecommunications systems. It is also a process – new threats are discovered over time, forcing communication systems to evolve.

ROLF BLOM, KARL NORRMAN, MATS NÄSLUND, STEFAN ROMMER AND BENGT SAHLIN

Wireless telecommunications systems must live up to user and network service provider expectations regarding trust and privacy. Besides the obvious need for authentication and encryption (to enable reliable charging, and to hinder eavesdropping), new architectures require more sophisticated protection mechanisms.

The authors provide an overview of the security architecture and security features of the Evolved Packet System for LTE and non-3GPP accesses.

Background

The fundamental needs for authentication and encryption were addressed in the design of the Global System for Mobile Communication (GSM), which mitigated problems in earlier wireless telecommunication systems and helped to make GSM a widely successful system.

The design of the Universal Mobile Telecommunications System (UMTS) retained the good security features of GSM and introduced new ones[1], including

- public review of encryption algorithms by the security community;
- the MILENAGE algorithm set, which was specified by 3rd Generation Partnership Project (3GPP) as an example authentication algorithm to be used by network service providers who did not want to design their own algorithm;
- 128-bit encryption key length (increased from 64 bits);
- mutual authentication and mandatory integrity protection of signaling between wireless terminals and the network – this feature was added to protect against a false base station; and
- encryption from the terminal to a node beyond the base station.

In 2004, 3GPP started work on the next-generation radio technology, called Long Term Evolution (LTE). The main drivers of this work were the needs to increase capacity and throughput, and to decrease latency. Work was also started on the Evolved Packet Core (EPC), with the aim of simplifying the core network, and to integrate non-3GPP access technologies with the EPC.

Work on EPS security began in 2005. It was based on the strong security from UMTS, but has in fact improved security even further[2-3].

Long Term Evolution

The trust model in LTE **(Figure 1)** is similar to that of UMTS. It can roughly be described as a secure core network while radio access nodes and interfaces between the core network and the radio access nodes are vulnerable to attack.

The system architecture for LTE is flatter than that of UMTS, having no node that corresponds to the radio network controller (RNC) in UMTS. Therefore, the user equipment (UE) user plane security must either be terminated in the LTE base station (eNB) or in a core network node. For reasons of efficiency, it has been terminated in the eNB. However, because eNBs and backhaul links might be deployed in locations that are vulnerable to attacks, some new security mechanisms have been added.

Security over the LTE air interface is provided through strong crypto-

BOX A Terms and abbreviations

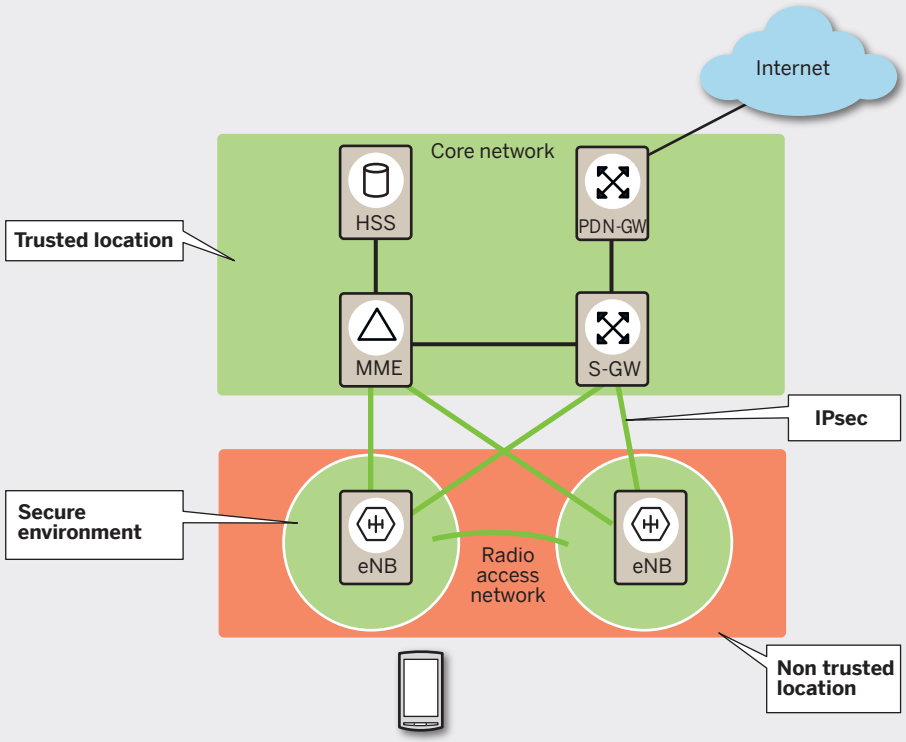
3GPP	3rd Generation Partnership Project
AAA	authentication, authorization and accounting
AES	advanced encryption standard
AKA	authentication and key agreement
BBF	Broadband Forum
CDMA	code division multiple access
CMAC	cipher-based message authentication code
DSMIPv6	dual-stack mobile IPv6
EAP	extensible authentication protocol
EPC	3GPP Evolved Packet Core
EPS	3GPP Evolved Packet System
eNB	eNodeB (base station)
ePDG	evolved packet data gateway
GERAN	GSM/EDGE Radio Access Network
GSM	Global System for Mobile Communication
HRPD	high-rate packet data
HSGW	HRPD Serving Gateway
HSS	home subscriber server
IETF	Internet Engineering Task Force
IKE	internet key exchange
IP	Internet Protocol
IPsec	IP security protocol
LTE	3GPP Long Term Evolution
MIP	Mobile IP
MME	mobility management entity
PDN-GW	packet data network gateway
QoS	quality of service
RNC	radio network controller
S-GW	serving gateway
SIM	subscriber identity module
UE	user equipment
UMTS	Universal Mobile Telecommunications System
USIM	universal SIM
UTRAN	Universal Terrestrial Radio Access Network
VPLMN	Visited Public Land Mobile Network
WLAN	Wireless Local Area Network

graphic techniques. The backhaul link from the eNB to the core network makes use of internet key exchange (IKE) and the IP security protocol (IPsec) when cryptographic protection is needed. Strong cryptographic techniques provide end-to-end protection for signaling between the core network and UE. Therefore, the main location where user traffic is threatened by exposure is in the eNB.

Moreover, to minimize susceptibility to attacks, the eNB needs to provide a secure environment that supports the execution of sensitive operations, such as the encryption or decryption of user data, and the storage of sensitive data like keys for securing UE communication, long-term cryptographic secrets and vital configuration data. Likewise, the use of sensitive data must be confined to this secure environment.

Even with the above security measures in place, one must consider attacks on an eNB, because, if successful, they could give attackers full control of the eNB and its signaling to UEs and other nodes. To limit the effect of a successful attack on one eNB, attackers must not be able to intercept or manipulate user and signaling plane traffic that traverses another eNB – for example, after handover.

FIGURE 1 **LTE trust model.**



User authentication, key agreement and key generation

The subscriber-authentication function in LTE/3GPP Evolved Packet System (EPS) is based on the UMTS authentication and key agreement (UMTS AKA) protocol. It provides mutual authentication between the UE and core network, ensuring robust charging and guaranteeing that no fraudulent entities can pose as a valid network node. Note that GSM Subscriber Identity Modules (SIMs) are not allowed in LTE because they do not provide adequate security.

EPS AKA provides a root key from which a key hierarchy is derived. The keys in this hierarchy are used to protect signaling and user plane traffic between the UE and network. The key hierarchy is derived using cryptographic functions. For example, if key_2 and key_3 (used in two different eNBs) are keys derived from key_1 by a mobility management entity (MME), an attacker who gets hold of, say, key_2, still cannot deduce key_3 or key_1, which is on a higher layer in the key hierarchy. Furthermore, keys are bound to where, how and for which purpose they are used. This ensures, for example, that keys used for one access network cannot be used in another access network, and that the same key is not used for multiple purposes or with different algorithms. Because GSM does not have this feature, attackers who can break one algorithm in GSM can also compromise the offered security when other algorithms use the same key.

Further, the key hierarchy and bindings also make it possible to routinely and efficiently change the keys used between a UE and eNBs (for example, during handover) without changing the root key or the keys used to protect signaling between the UE and core network.

Signaling and user-plane security

For radio-specific signaling, LTE provides integrity, replay protection, and encryption between the UE and eNB. IKE/IPsec can protect the backhaul signaling between the eNB and MME. In addition, LTE-specific protocols provide end-to-end protection of signaling between the MME and UE.

For user-plane traffic, IKE/IPsec can similarly protect the backhaul from the eNB to the serving gateway (S-GW). Support for integrity, replay protection and encryption is mandatory in the eNB. The user-plane traffic between the UE and eNB is only protected by encryption as integrity protection would result in expensive bandwidth overhead. Notwithstanding, it is not possible to intelligently inject traffic on behalf of another user: attackers are essentially blind in the sense that any traffic they try to inject would almost certainly decrypt to garbage.

Handover in LTE

When handover occurs between two eNBs, the source eNB needs to transfer security parameters to the target eNB **(Figure 2)**. At the same time, there might be a need to

restore security should the source

FIGURE 2 **Security during handover.**

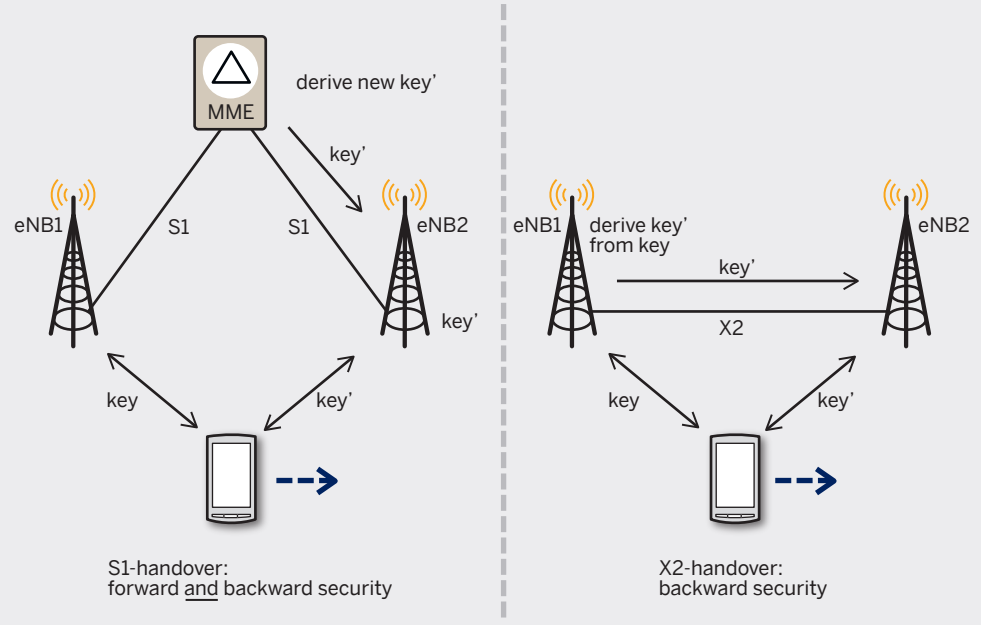
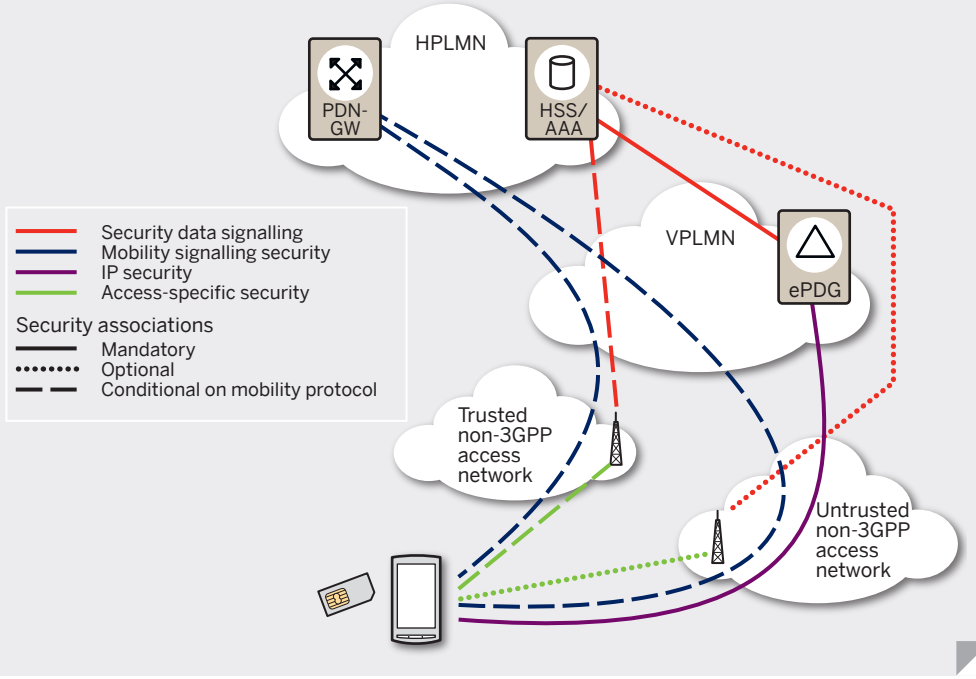


FIGURE 3 **Overview of security architecture for non-3GPP access to EPC.**



- eNB have been compromised (forward security); or
- keep previous traffic secure should the target eNB have been compromised (backward security).

In either case, the core network can provide the target eNB with a new key, unknown in the source eNB, to be used after handover. An attacker who has compromised one of the eNBs and obtained its key will not know which key will be (or has been) used in the other eNB. The UE, on the other hand, has all the information it needs to deduce the correct keys.

A simpler procedure also used in LTE, which ensures only backward security, is to have the source eNB derive a new key from the current key via a cryptographic function. Only the derived key is transferred to the target eNB.

Handover to legacy systems

When a UE moves between LTE and other 3GPP radio access technologies, the security context may also be transferred in much the same way as when a UE moves between GSM/EDGE Radio Access Network (GERAN) and Universal Terrestrial Radio Access Network (UTRAN). LTE also includes the caching of security contexts. This saves on the number of times a subscriber must be authenticated when a UE rapidly moves back and forth between LTE and UTRAN.

Non-3GPP access

3GPP Rel-6-enabled access through interworking Wireless Local Area Network (WLAN) technology gives users internet access via a (U)SIM-based subscription. To enable the use of (U) SIM cards, the AKA protocol is carried by the extensible authentication protocol (EAP) and IEEE 802.1X. Knowing that legacy WLAN technology (such as IEEE 802.11b) has sub-optimal security, 3GPP has also allowed user traffic to be tunneled across the access network using IKE/IPsec.

EPS/3GPP Rel-8 takes this concept one step further, enabling end users to use common security and mobility protocols based on Internet Engineering Task Force (IETF) specifications to access the EPC over basically any non-3GPP wireless or wireline access technology. Rel-8 also defines optimized handover

between LTE and high-rate packet data (HRPD) access developed by 3GPP2.

The disparity between the security solutions offered for the different access technologies was an immediate challenge. Wireline accesses (xDSL), for example, employ a security model that relies on the physical security of the wire, thus omitting user-specific credentials and cryptographic protection.

A heterogeneous patchwork of security solutions needed to be avoided, as did a "one-size-fits-all" approach, since this might overprotect accesses with good security and lead to sub-optimal performance. Instead, a common framework has been introduced with a simple security classification for different accesses.

Principles

The common denominator for any non-3GPP access to EPC is the use of a USIM card. EAP AKA-based mutual authentication is always performed between a UE (USIM) and the authentication, authorization and accounting (AAA) server. The AAA server fetches credentials from the home subscriber server (HSS). EAP AKA authentication also provides cryptographic keys for data integrity and encryption between the UE and network at the access layer, at the Internet Protocol (IP) layer, or both. The EAP AKA protocol has been extended to support keys that are bound to the identity of the access network[4]. This limits the risk of key misuse, as discussed above.

Next, a given non-3GPP access can be treated either as a trusted non-3GPP access or as an untrusted non-3GPP access. An access is trusted if it can provide all necessary security itself. Untrusted accesses need IPsec tunneling (similar to the Rel-6 interworking WLAN solution). The issue of trust is not solely a matter of access technology, however; network service provider A, for example, might trust a given access network, whereas network service provider B might not. **Figure 3** gives an overview of the architecture for non-3GPP access to EPC.

The access-level authentication or security association is optional for untrusted access. Since the access is not trusted, it is not clear whether the security provided by the access would add anything. Instead, mandatory EAP AKA authentication provides an IKE/IPsec security association between the evolved Packet Data Gateway (ePDG) and UE, protecting all traffic across the entire access network.

EAP AKA is used for trusted access to create an access-level security association between the UE and the non-3GPP access network. However, this access-level authentication is optional when mobility is based on the dual-stack mobile IPv6 protocol (DSMIPv6). This is because DSMIPv6 always uses EAP AKA authentication between the UE and MIP home agent (the packet data network gateway, PDN-GW), which adequately fulfills the authentication needs.

Because the security procedures for trusted and untrusted accesses differ, the UE needs to know the "trust value" of the access. This can be made available via the authentication signaling. If no signaling is received, the UE inspects a configuration file on the USIM to determine the trust value. If the UE does not find the access network identity there either, it reverts to a default and assumes the access is untrusted.

CDMA2000

HRPD is one non-3GPP access that has been treated in a special way in 3GPP standardization in order to fulfill strict performance requirements for mobility between LTE and HRPD.

A delay-optimized handover between LTE and HRPD could be handled in the same manner as handover between LTE and GERAN/UTRAN – for example, by transferring the security parameters in use. However, since HRPD in CDMA is not part of the 3GPP family of accesses, the mapping of security parameters between HRPD and LTE is not straightforward.

Another option is to perform new security procedures every time the UE enters a new access. But if the UE in question is only able to operate one radio at a time, this option suspends all traffic while the UE performs security procedures in the target access.

One straightforward approach to reduce the delays is that before attaching to the LTE access, the UE performs HRPD access attachment procedures (including security procedures) directly over the HRPD radio access. The UE can then attach to LTE over LTE radio access and continue using LTE. In this case the security context in HRPD access is prepared and cached and a later handover from LTE to HRPD can be performed more efficiently.

Another alternative is for the UE to perform attach-and-security signaling with the target HRPD access while it is still active in LTE access. In this case the LTE access network transparently forwards HRPD-specific signaling (including EAP-AKA) between the UE and HRPD access network **(Figure 4)**. The LTE network needs not be aware of HRPD-specific messages or parameters (and vice versa). Also in this case the target HRPD access network is prepared when the UE executes a handover to HRPD. This alternative is however more complex and requires additional functionality in the LTE and HRPD access networks.

Summary and future outlook

EPS security has adopted UMTS security as a baseline, drawing on the successful concepts of UMTS to build an even more secure and flexible solution. The most prominent components are

- the EPS AKA procedure with a key hierarchy, in which keys are bound to their use;
- prepared for stronger 256-bit cryptography;
- a new key-updating mechanism for intra-LTE handovers;
- backhaul security;
- resistance to attacks on eNBs; and
- integration of security for non-3GPP accesses.

These features address attacks from a false eNB, and confine the consequences of a compromised eNB to itself. The use of cryptographic algorithms means that signaling and user traffic is strongly protected over the air interface and backhaul.

Future 3GPP security work will focus on LTE Advanced. But because no big changes are anticipated with respect to core LTE functionality, the basic security mechanisms will continue to prevail. From a security point of view, the main new development will be relay nodes, and work in this area is already under way.

Other developments will include the introduction of home base stations, ▸▸

BOX B

Key sizes and algorithms in LTE

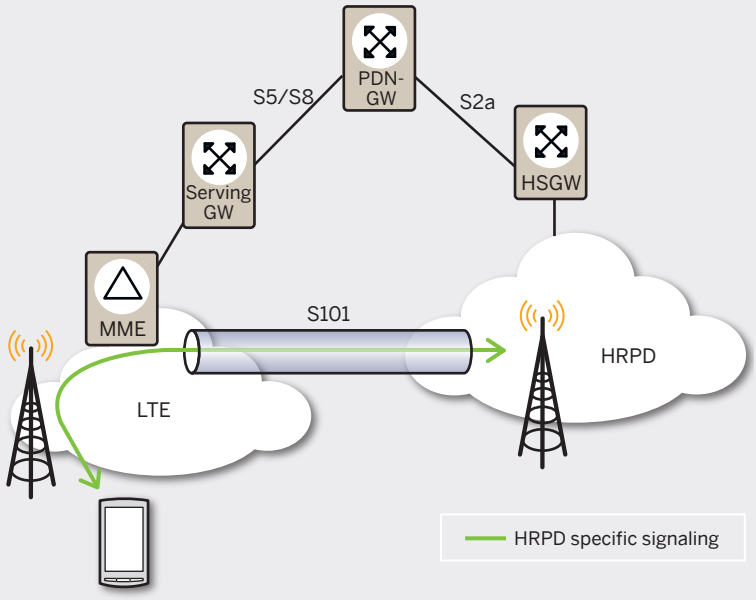
At present, the integrity protection and encryption algorithms use 128-bit keys. However, the system is prepared to use algorithms with 256-bit keys. LTE uses the following encryption algorithms:

1. 128-EEA1 based on the SNOW 3G algorithm. It is identical to UEA2 as specified for UMTS.
2. 128-EEA2 based on the advanced encryption standard (AES) in counter mode.

Likewise, LTE uses the following integrity-protection algorithms:

1. 128-EIA1 based on SNOW 3G. This algorithm is identical to UIA2 in UMTS.
2. 128-EIA2 based on Advanced Encryption Standard (AES) in cipher-based message authentication code (CMAC) mode[5].

FIGURE 4 **Preparation (pre-registration) of HRPD access while the UE is still active in LTE using the S101 interface to forward HRPD specific signaling.**



machine-to-machine communication, local IP access, and selected IP traffic offload. Home base stations require new security solutions for authentication with the core network and authorization of end-user access to the radio cell. Home base stations will also be deployed in environments where it is easy to launch attacks on the physical hardware. Accordingly, the network must be able to detect such tampering. The first versions of related standards have already been released.

Local IP access will allow users to access local residential or corporate networks from a 3GPP device. Selected IP traffic offload deals with achieving a more optimal traffic path for user internet traffic which is not intended to reach services in the operator's core network.

In addition there is work ongoing in 3GPP as well as in the Broadband Forum (BBF) for providing a more optimized interworking of BBF fixed access networks with the EPC. This work may result in additional security work to be done in 3GPP and BBF.

Rolf Blom

is an Expert in Mobile Communications Security at Ericsson Research in Kista, Sweden. He first joined Ericsson in 1984 and worked until 1995, mainly with the development of crypto and crypto-based products for defense communications. After a period of work abroad, he returned to Ericsson in 1998, and since then he has been active in establishing and leading security research activities. He holds an MSc in Electrical Engineering from the Royal Institute of Technology in Stockholm, Sweden, and a PhD in Information Theory from Linköping University, Sweden.

Stefan Rommer,

who joined Ericsson in 2001, is a Senior Specialist in IP mobile networks at Business Unit Networks, Product Development Unit Packet Core. He has also contributed to various wireless LAN and mobile packet core projects. Since 2006, he has been working with packet core standardization in 3GPP (SA2 working group). Stefan holds an MSc in Engineering Physics and a PhD in Theoretical Physics, both from Chalmers University of Technology, Gothenburg, Sweden.

Karl Norrman

joined Ericsson Research in Kista, Sweden in 2001. His main areas of interest are security protocols and architectures. He holds an MSc in Computer Science from Stockholm University in Sweden, and is currently Ericsson's standardization coordinator for security in 3GPP (SA3 working group).

Mats Näslund

worked for Ericsson since 1999, when he joined the then newly formed Communication Security Lab, now Research Area Security. His research interests cover most aspects of fixed and mobile network security, and in 2009 he received Ericsson's Inventor of the Year award. Mats holds a PhD in Computer Science from the Royal Institute of Technology (KTH) in Stockholm, Sweden.

Bengt Sahlin

joined Ericsson Finland in 2001. He has worked in the area of security ever since, and is currently Section Manager for the Network Security Section at Ericsson Research NomadicLab. Bengt holds an MSc in Computer Science from Helsinki University of Technology (TKK) in Finland, and is a certified information systems security professional (CISSP). He is also the current chairperson of 3GPP SA3.

References

1. Boman, K., Horn, G., Howard, P. and Niemi, V.: UMTS security. Electronics & Communication Engineering Journal, Oct 2002, pp. 191-204.
2. TS 33.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture.
3. TS 33.402, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security aspects of non-3GPP accesses.
4. IETF RFC 5448: Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA').
5. Algorithm descriptions can be found at: http://gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm#nav-