Tampere University of Technology
Telecommunications laboratory

8309700 Advanced Topics in Telecommunications
Report, 3rd April, 2000
(Revised 24th May, 2000)

150105 Antti Vähä-Sipilä, avs@iki.fi

Ciphering in GPRS and UMTS

Encryption in 3G Packet Data Networks

Revised

Acronyms and Abbreviations

3G Third generation

3G- UMTS version of (usually a GSM or GPRS) term

3GPP Third generation partnership project, the standardisation body for UMTS

A3 GSM authentication algorithm

A5 GSM confidentiality (encryption) algorithm

A8 GSM key generation algorithm

AK Authentication key (see text)

AMF Authentication management field (see text)

AMPS American mobile phone system, an analog mobile phone system in the Americas

AUTN Authentication information (see text)

AV Authentication vector (see text)

AuC Authentication centre, an entity that contains the security (authentication) related subscriber data at the network side

BSC Base station controller, a unit that controls BTSes

BTS Base tranceiver station, a base station that serves mobile phones

CKSN Ciphering key sequence number (see text)

CK (or C_k) Ciphering key (see text)

Core network See: GPRS backbone

ECB Electronic codebook, a block cipher mode where each encrypted block is independent of previous and subsequent blocks

ETSI European telecommunications standards institute, the standardisation body responsible for GSM/GPRS standards development. http://www.etsi.org/

f2 UMTS authentication algorithm

f3 UMTS key generation algorithm

f8 UMTS confidentiality algorithm

f9 UMTS integrity algorithm

FCS Frame check sequence

GEA GPRS encryption algorithm

GEA2 GPRS encryption algorithm version 2

GGSN Gateway GPRS support node, a GPRS network element that routes packets from the GPRS core network to interconnected networks, e.g. the Internet

GPRS- GPRS version of (usually a GSM) term

GPRS backbone The private network that handles the packet traffic inside the operator's domain, user packets are tunneled through it between the mobile phone and interconnected networks

GPRS Generic packet radio system, a packet radio system built on GSM principles

GSM Global system for mobile communications, a widely-deployed digital (second-generation) mobile phone system

GTP GPRS tunneling protocol, tunnels data between SGSN and GGSN

HE Home environment

HLR Home location register, a unit that contains subscriber data at the network side

I frames LLC frames for confirmed information transfer

IK Integrity key (see text)

IMSI International mobile subscriber identity, an unique identification of the subscriber

IOV Input offset (see text)

IPSec Internet protocol security services

IP Internet protocol

KI (or K_i) A subscriber-specific shared secret between the SIM and the network (see text)

KSI Key set identifier (see text)

LIG Legal interception gateway, a back door for the authorities

LLC Logical link control layer, a lowest common communications layer between a mobile phone and a SGSN in a GPRS network

MAC-A Message authentication code (see text)

MAC Message authentication code (see text), or medium access control layer

MSC Mobile switching centre

MS Mobile station, usually the mobile phone plus its accessories and the SIM card

Mobile IP Internet protocol with mobility management functions

NMT Nordic mobile telephone, an analog mobile phone system in the Nordic countries and some other European countries

Node B A part of UTRAN

PDCP Packet data convergence protocol layer

PHY Physical layer (voltage changes on wire, modulated radio waves, etc.)

QoS Quality of service

RAND A random value (see text)

RES A response message (see text)

RLC Radio link control protocol

RNC Radio network controller (controlling RNC or serving RNC)

RRC Radio resource control

SAGE Security algorithms group of experts

SGSN Serving GPRS support node, a GPRS network element that serves the mobile phone as it connects to the packet network

SIM card Subscriber identity module, a smart card containing subscriber information and some cryptographic algorithms

SMG ETSI's working group

SNDCP Subnetwork dependent convergence protocol

SQN Sequence number (see text)

SRES A response value (see text)

SSH Secure shell, a cryptographic protocol over TCP

SSL Secure sockets layer, a cryptographic protocol over TCP

TCP Transmission control protocol, provides connection-oriented services over IP

TLS Transport layer security, a cryptographic protocol over TCP

UEA UMTS encryption algorithm (UEA0 and UEA1 have been defined)

UIA UMTS integrity algorithm (UIA1 has been defined)

UI frames LLC frames for unconfirmed information transfer

UMTS Universal mobile telephone system, also known as a third generation mobile phone system

USIM A SIM in UMTS

UTRAN UMTS terrestial radio access network, the part of UMTS that handles radio access (base station subsystem etc.)

VLR Visitor location register, a unit that contains subscriber data of visiting mobile users

VPN Virtual private network, a private network implemented over a public network using a cryptographic tunnel

WCDMA Wideband code division multiplexing access, the air interface technology for UMTS (compare with time/frequency division multiplexing of GSM)

XRES An expected response value (see text)

1 Introduction

GPRS (Generic Packet Radio Service) extends the current GSM (Global System for Mobile Communications) mobile phone system to allow the transport of packet data in addition to circuit-switched data calls. As data transfer is becoming more widespread in digital mobile phone networks, packet data transfer is seen as a solution which will enable several users to share network resources more effectively. In circuit-switched data, a fixed-bandwidth communications channel is reserved solely for a single terminal. This is mostly suited for speech, whereas data transfers are bursty by nature, with alternating periods of data transfer and silence. In a packet data network, a single channel can be shared between several users.

UMTS (Universal Mobile Telephone System) is the third generation mobile phone system (GSM being of the second generation, and analog networks such as AMPS (American Mobile Phone System) and NMT (Nordic Mobile Telephone) being of the first generation). UMTS is on the evolutionary path from GSM and GPRS, but employs a different radio interface. It is envisaged that UMTS is mostly a data transfer network, and speech is just one kind of data with a certain quality of service (QoS) requirement.

In this paper, I try to describe the encryption (ciphering) solutions used on the radio interface, also called the air interface, of GPRS and UMTS networks.

This report has been written for the course *8309700 Advanced Topics in Telecommunications* held in Tampere University of Technology, Finland, in spring 2000 as a part of my postgraduate studies. The author can be reached at <avs@iki.fi>. Please send me any corrections that you might have.

2 Overview of the GPRS Network

As the GPRS network is built on the existing GSM network (see figure 1), the main network elements are quite similar. The mobile phone is called the MS (*mobile station*), which contains a SIM card (*subscriber identity module*). GSM

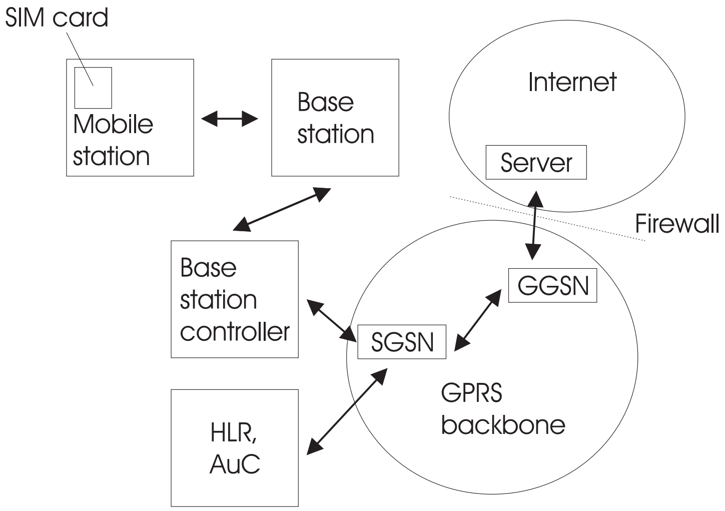

Figure 1: GPRS network elements: a simplified picture

(and GPRS) phones are not subscriber-specific. The subscriber is identified by the SIM smart card, which is responsible for the authentication of the user. The phone number is tied to the SIM card, not the phone.

The MS talks to a *base station*, also known as the BTS (Base Tranceiver Station). BTSes are responsible for radio transmission from and to the mobile phone. Base stations are controlled by a BSC, Base Station Controller, which handles the management of radio resources (channels) and handovers (changing of a base station when a call is in progress).

The switching of the call (routing it to the correct destination) is first done in an MSC (*mobile switching centre*, not shown in the simplified picture above). An MSC is responsible for creating calls and routing the calls to other telephone networks. Other noteworthy elements are the *location registers* (HLR, for home location register, and VLR, for visitor location register), which contain the subscriber information and the current location of the mobile user. They handle mobility management. HLR contains a network entity called the *authentication centre* (AuC), which is used for key management and subscriber authentication purposes.

All of the above components can be found in a conventional GSM network as well as in a GPRS network. To enable packet data transmission, a GPRS network has two types of network elements, called the SGSN (*serving GPRS support node*) and GGSN (*gateway GPRS support node*). If the reader is familiar with Mobile IP, SGSN is roughly the counterpart of a foreign agent and GGSN is the home agent [Häm96]. The SGSN serves the mobile station and the GGSN routes the packets to and from an external network, such as the Internet. SGSN and GGSN are located in the network operator's private IP network, called the *GPRS backbone* or the *core network*.

When the mobile station wants to use the packet data services, it performs a *GPRS attach*, during which it associates itself with a SGSN. A *GPRS detach* procedure disassociates the mobile station. The GPRS attach procedure is usually done when the mobile station is powered on.

3 Security Services in a GPRS Network

The network security of a GPRS network is based on GSM network security [ETS99e]. The main difference between the systems is the existence of the GPRS backbone, and the existence of packet data. This causes some changes to the way that radio interface encryption is done in GPRS.

GSM encipherment is done at the radio burst level, after channel coding and just before the burst is formatted and modulated on the air interface. This is the lowest possible layer and constrains the use of encryption between the mobile terminal and the base station.

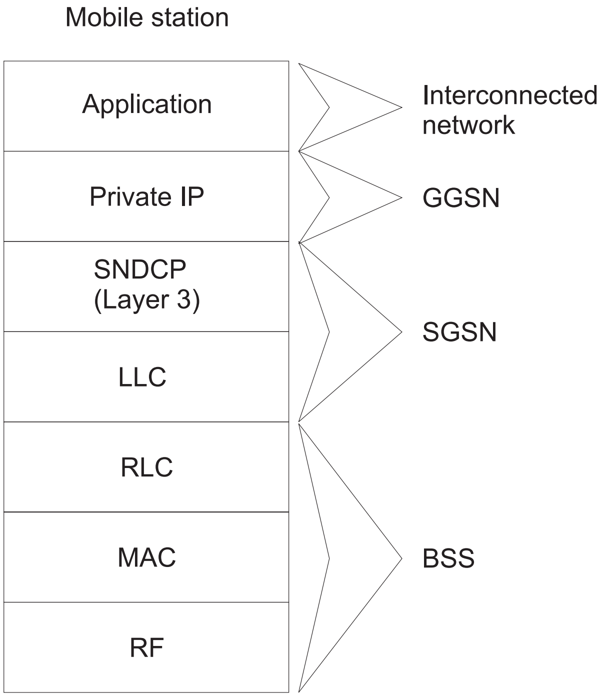

Figure 2: GPRS stack at the mobile station and layer peers

This is possible as in circuit switched connection, the time slot is always reserved for only one mobile terminal. In GPRS, the same radio resource is divided between several mobile stations. Existing GSM base stations cannot cope with the key management problems that this leads to, and therefore encryption is done on LLC level instead. LLC ends in SGSN instead of the BTS (figure 2), so

GPRS encryption traverses the whole base station subsystem, and no changes are required to existing BTSes.

In GSM, all data traffic was circuit-switched, meaning that the data flow was a continuous stream of bits. This lends itself well for a stream cipher, which is initialised in the start of stream.

The problem related to packet data is analogous to that of IPSec. In IPSec, encryption is applied at IP packet level. Packets may arrive out-of-order or get lost, but the recipient must still be able to decrypt all received packets successfully. Therefore, the encipherment of data cannot depend on the previous packets.

There is no rearrangement of packets at the SGSN or the mobile terminal at LLC level. Therefore, it has to be possible to decrypt all packets in the order they have been received. When using a stream cipher, whose output state is determined by the number of input bytes, or a block cipher, whose output also depends on the previous input (in other modes than ECB), loss of data results in a desynch between the sender and the receiver, as the encryption block sizes are not constant.

3.1 Authentication and Key Setup in GPRS

As mentioned earlier, the SIM card contains the subscriber data and is responsible for authentication at the mobile station side. The SIM card contains the A3 and A8 algorithms and a subscriber-specific key K_i. A3 and A8 are hash algorithms, meaning that an input x to the algorithm always causes an output $y = H(x)$, but one cannot (or should not be able to) reverse-engineer x from the output y. K_i is also stored in the authentication centre (AuC), a part of home location register (HLR). HLR handles the user's subscriber data.

Ciphering is usually started during the GPRS attach procedure. SGSN contacts the authentication centre to receive so-called *authentication triplets* (see figure 3). A triplet contains a RAND, which is a random value, an SRES, which is an A3 hash of K_i for the user in question and the RAND, and the K_c (the encryption key). SGSN sends the RAND, the CKSN (ciphering key sequence number[1]) and the algorithm identifier to the mobile station, which then has all the required information to start ciphering. RAND and CKSN end up on the SIM card. SIM calculates an SRES based on the RAND and K_i (using the A3 algorithm) and sends the SRES back to SGSN. The SGSN compares the SRES received from the AuC and from the mobile station and if they are equal, the mobile station has been authenticated. The mobile station is also able to calculate K_c based on RAND and K_i, using algorithm A8. Bidirectional ciphering is now possible, as both the mobile station and SGSN know the encryption key K_c and the algorithm to be used. Ciphering is used from this point onward.

[1] ETSI GSM 03.20 [ETS99e] calls the K_c and CKSN by the names GPRS-K_c and GPRS-CKSN to distinguish them from their GSM counterparts.

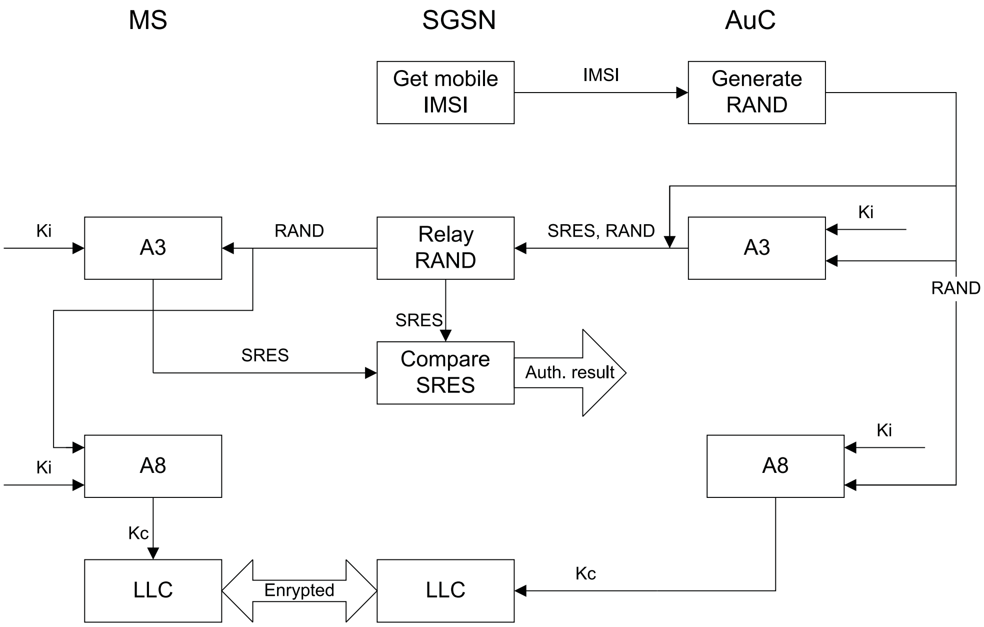

Figure 3: GPRS authentication and key establishment (simplified)

In a device which uses both GPRS packet data and GSM circuit switched connections, a different K_c is used for each connection. In addition, keys can be changed whenever the network chooses to do so.

3.2 Encryption on the LLC layer

As mentioned before, the LLC (Logical Link Control) layer [ETS99d] is the lowest protocol layer that is common to the mobile station and the SGSN. As the ciphering has been negotiated between the MS and SGSN, it takes place on the LLC layer.

When ciphering is to be started, a higher layer (layer 3) entity tells the LLC layer the K_c and the ciphering algorithm to be used. It is also possible to indicate that no ciphering will be used. As the algorithm selection is done by the network, this is a network option. The algorithm to be used is selected from the set of algorithms supported by the mobile station. The MS advertises its algorithm set to the network during the authentication.

The LLC layer then initialises the encryption algorithm using the K_c, a direction bit, and a special input parameter. The direction bit specifies whether the current keystream will be used for upstream or downstream communication (from and to the mobile station, respectively) as both directions use a different keystream[2]. The input parameter is used as an additional input so that each

[2] This differs from the GSM, which uses the same keystream for both directions.

LLC frame is ciphered with a different segment of the keystream. This parameter is calculated from the LLC frame number, a frame counter, and a value supplied by the SGSN called the IOV (input offset value) [ETS99d]. The IOV is negotiated during the LLC layer and layer 3 parameter negotiation.

There are two types of LLC frames that are ciphered: I and UI frames. I frames are used for confirmed information transfer, that is, the received frames are acknowledged. UI frames are used for unconfirmed information transfer and there is no sequence number checking. Lost UI frames are not indicated to the upper layer (that is, layer 3). The encipherment differs between these frame types. Both use their own IOV, called I-IOV and UI-IOV, respectively. As UI frames do not have the sequence number check, UI-IOV defaults to a fixed value of zero, although it can be negotiated during LLC parameter negotiation.

The encipherment covers the information and frame check sequence (FCS) fields. LLC frames also contain address and control fields, which are outside of the encrypted portion.

For UI frames, the upper layer can decide whether to send the frame encrypted or not. Also, indication of received UI frames to the upper layer contains a flag that shows whether the frame was encrypted. UI frames contain an 'E' bit, which is used to indicate the presence of encryption to the LLC peer.

4 Overview of the UMTS Network

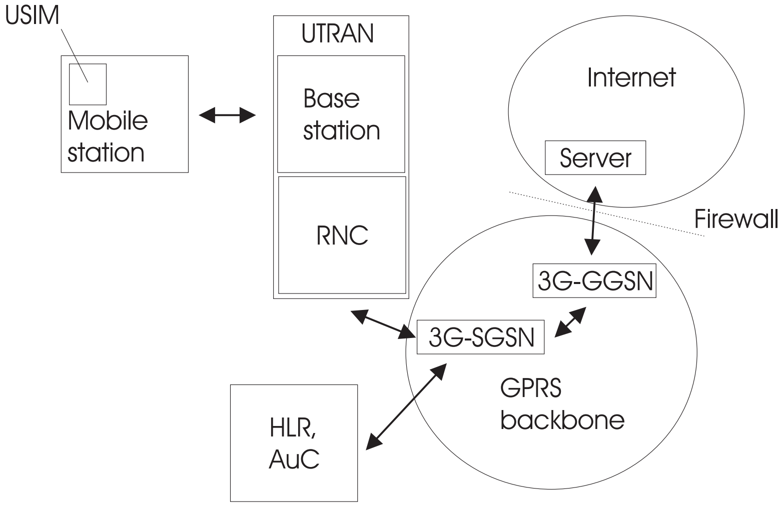

Figure 4: WCDMA UMTS network elements (release 99; packet data)

Figure 4 shows the network elements of the UMTS network. Only the packet data side is shown (corresponding to the GPRS network, see figure 1).

The first noticeable similarity is the core network, which contains the *3G serving node* (3G-SGSN) and *3G gateway node* (3G-GGSN), which are similar to those of GPRS. The SIM card is called USIM. The base station now logically belongs to a larger entity called UTRAN (*UMTS terrestial radio access network*), which corresponds to the GSM base station subsystem. The network elements in UTRAN are Node B and radio network controllers (RNCs). Depending on the channel, the RLC protocol peer is either Node B or serving or controlling RNC. UTMS radio interface protocol architecture is specified in [3GP99].

5 Security Services in a UMTS Network

According to [Wal00], even if 3G network security builds on the GSM principles, it has been designed against certain problems which have been present in existing GSM networks. Such issues are the small effective key length of existing GSM ciphers, the insecurity of the widely used COMP128 authentication algorithm, and the lack of network authentication. The latter has even lead to the existence of fraudulent base stations.

In UMTS, security services are categorised to five different classes, of which we will concentrate on only one: the network access security, which is the counterpart of air interface security in GSM and GPRS. Actually, in a hybrid GSM/UMTS case, the network access security services have been defined to use GSM network security when either one of the peers is not capable of UMTS access authentication and ciphering.

5.1 Authentication and Key Setup in UMTS

The negotiation of ciphering keys in UMTS bears many similarities to the GPRS case. Packet and circuit switched connections have separate cipher streams; upstream and downstream have their own streams as well. Keys are generated from a random value, supplied by the authentication centre. Despite of the similarities, there are some deviations, which we discuss below [3GP00b].

As shown in figure 5, the authentication centre (AuC) in the home environment (HE) generates a sequence number, SQN, and a random value, RAND. AuC then generates an *authentication vector* (AV), which corresponds to the GSM authentication triplet. AV consists of the following:

- The random value RAND
- XRES, which is analogous to SRES in the GSM case, and calculated from the RAND and a shared secret K with algorithm f2
- The *encryption key* CK, which is analogous to C_k in GPRS, generated from K and RAND with algorithm f3

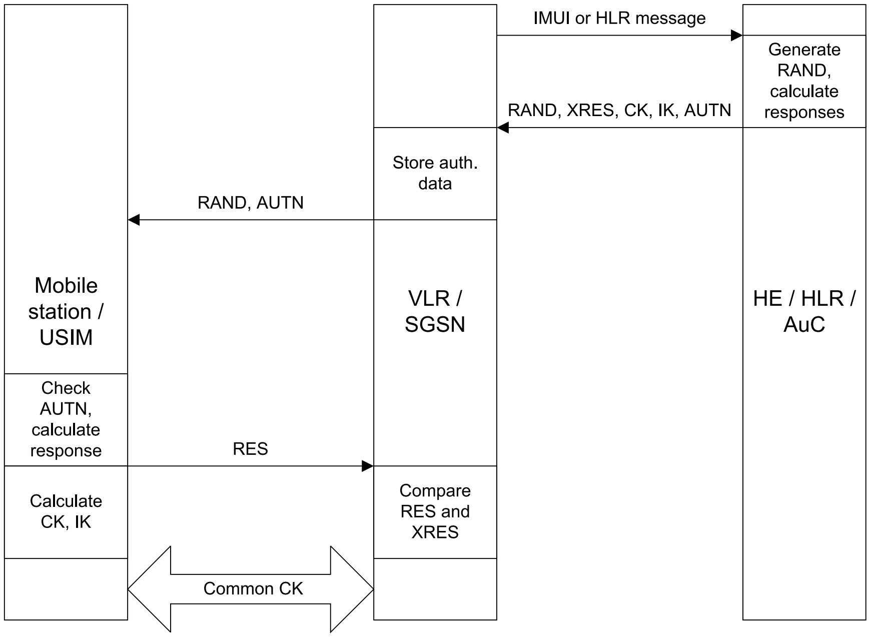

Figure 5: UMTS authentication and key establishment

- An *integrity key* IK, also generated from K and RAND with algorithm f4
- An *anonymity key* AK, again generated from K and RAND with algorithm f5
- An *authentication token* AUTN that contains a *sequence number* SQN (shrouded with AK, if the sequence number would divulge information about the subscriber's identity), an *authentication management field* AMF, and a *message authentication code* MAC-A[3]. AMF can be used for disaster recovery purposes, such as phasing out a compromised algorithm, or for controlling the amount of data that can be encrypted with a given CK. MAC-A is used to check the authenticity of the AUTN message.

RAND and AUTN are sent to the mobile station, calculates the MAC (using SQN, RAND, AMF and K), and if the AUTN is successfully authenticated and if SQN is in an accepted range, ciphering and integrity keys are calculated and taken into use. The mobile station also calculates the response RES, as in GPRS, and sends it back to the network in order to authenticate itself. All of the calculations on the mobile side take place in the USIM. The shared secret K is also stored on the USIM.

The ciphering algorithm to be used is determined when the network receives an *MS/USIM classmark* from the mobile station. The classmark lists the supported

[3] Also referred to as MAC in 3GPP specifications. MAC-A is a more specific acronym for the MAC in AUTN. Do not confuse the MAC layer with MAC-A.

encryption and integrity algorithms. Network selects the algorithm to be used from these, or may opt for no encryption if both MS and the network agree. However, integrity checking algorithm must always be successfully negotiated.

To ease the load on AuC, encryption keys and integrity keys can be reused. A *key set identifier* (KSI) is given to the negotiated CK and IK, and the network can refer to the already-negotiated keys by sending this KSI to the mobile station in subsequent connection set-ups.

5.2 Encryption on the MAC and RLC Layers

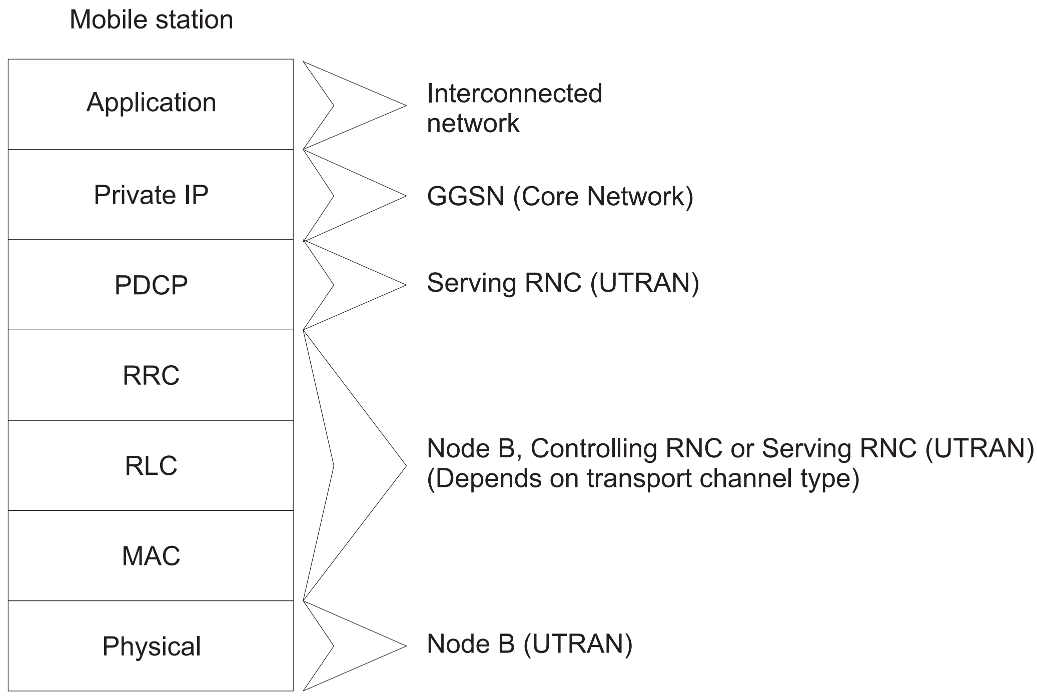

Figure 6: UMTS stack at the mobile station and layer peers

UMTS ciphering is done either on the MAC layer or the RLC layer (see figure 6) [3GP99], depending on the RLC mode of operation. For transparent RLC mode, meaning that RLC passes all data from its upper layer directly to the MAC layer without applying any of the RLC headers, the encryption is done on the MAC layer. Otherwise it will be done on the RLC layer. RLC is roughly analogous to the LLC layer in GPRS, with the distinction that LLC ends in SGSN and RLC ends in UTRAN.

This means that the air interface encryption will take place between mobile station and the UTRAN (Node B or an RNC). This differs from the GPRS case, where the air interface encryption is extended to the SGSN. However, there is a provision in UMTS to extend the encryption, which we will discuss later.

Whether ciphering is available depends on the logical channel in which the data is sent [3GP00a]. Dedicated control channel and dedicated traffic channel are covered [3GP99].

When either MAC or RLC is asked to start ciphering, the upper layer provides *ciphering elements* to the layer. These elements consist of the ciphering key, ciphering sequence number, which is used with the bearer number and direction as an input to the ciphering algorithm, and a time at which the new configuration will be taken into use.

The UMTS encryption algorithm is denoted by f8.

6 Encryption Algorithms in GPRS

6.1 GPRS Algorithm Requirements

ETSI has published the GPRS ciphering algorithm requirements [ETS98b]. The requirements state that:

- The encryption key length is 64 bits, and created in the GPRS authentication and key management procedure, as we discussed earlier.
- The key may be either unique or it can be shared for multicast communications.
- The algorithm is a keystream generator (a stream cipher), whose output is exclusive-ored with the plaintext to create the ciphertext (see figure 7).
- The keystream generator takes the key K_c, a direction bit Z (upstream/downstream) and an LLC frame specific input parameter $X[n]$ as the input. The input parameter is a counter which is initialized to a random value at the start of an LLC connection (for I frames) or a constant (for UI frames). The size of the input parameter is 32 bits.
- The strength of the algorithm should 'provide at least comparable protection as the baseline security provided by the GSM encryption algorithms' (sic), and should be continuously usable for a period of at least 10 years.
- The algorithm will not be encumbered by export restrictions. Many governments restrict the export (and sometimes use) of encryption as it is considered to be a dual-use product, meaning that it has military as well as civilian uses. In general, GSM phones have had a special treatment, as the calls can be eavesdropped on and monitored on the network side anyway. UMTS even clearly specifies a LIG, legal interception gateway.

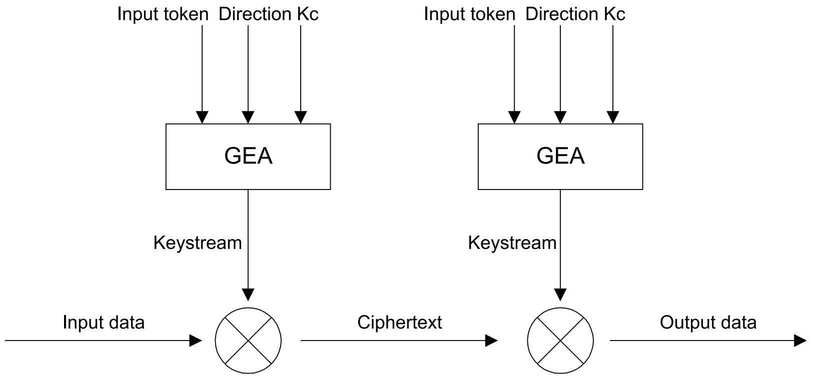

Figure 7: Using a stream cipher, such as GEA

- The algorithm details will be kept confidential.

Figure 7 shows how the GPRS encryption works on a general level (algorithm details being confidential).

6.2 GEA

ETSI has a working group called SAGE (Security Algorithms Group of Experts), which was appointed the task of creating the GPRS encryption algorithm (GEA). Based on the requirements from ETSI's SMG10 working group [ETS98b]. SAGE, in turn, founded another working group which they called Special Task Force 123 (STF123), which did the algorithm design [ETS98a]. This algorithm is referred to as GEA, GPRS encryption algorithm, or GPRS-A5.

A private evaluation report was written, which is only accessable to SAGE members. The public version [ETS98a] quotes that the algorithm design and evaluation took a total of 355 person-days, it passes a set of statistical tests for pseudorandom bit generators (which this keystream generator essentially is), and a 75 MHz Pentium achieved a data rate of 110 to 143 kilobytes per second when using this algorithm. SAGE concluded that it offers 'an adequate level of security' within its operational context.

The GEA specification and its test vectors remain confidential and can only be released under a confidentiality agreement to competent designers and manufacturers of GPRS equipment and testing systems, and to GPRS network operators. Distribution is controlled by the ETSI secretariat ('algorithm custodian') in France.

6.3 GEA2

After GEA had been specified, the encryption export control regulations changed due to the Wassenaar Arrangement. This allowed a stronger encryption algorithm to be used, and SAGE specified an algorithm called GEA2. The requirements for GEA2 were the same as for GEA, but further information is confidential [ETS99c] and no analysis of the algorithm has been published as a public ETSI Technical Report.

For more information on the ETSI way of algorithm specification, see [ETS99b].

7 Encryption Algorithms in UMTS

7.1 UMTS Algorithm Requirements

As with GPRS, there is a set of requirements that has been placed on UMTS encryption algorithms [ETS99a].

- The algorithm should be resilient against attacks for 20 years.
- The algorithms should be exportable under the Wassenaar Arrangement.
- The algorithm should be suitable for both software and hardware implementation, less than 10000 gates in hardware.
- The algorithm must enable a transmission speed of about 2 Mbit/s in both directions. (The hardware on which this figure is expected is not defined.)
- The algorithm should be a synchronous stream cipher.
- *The algorithms will be open for public evaluation.*

7.2 UMTS Encryption Algorithm f8 and Integrity Algorithm f9

UMTS defines two mandatory encryption algorithms: UEA0 is a null cipher (no confidentiality algorithm) whereas UEA1 is a cipher called Kasumi [Wal00]. Other algorithms are also possible, but implementing these algorithms is mandatory. Kasumi is a derivative of a block cipher called Misty [Mat97], another Japanese algorithm.

For integrity, UIA1 is Kasumi. There is no null integrity option. Kasumi (and its test data) are defined in 3GPP 35 series documents, which were at first publicly and directly downloadable from the Internet. Unfortunately, at the time of writing, they are not publicly available. However, they should be available again in the summer of 2000 [Wal00].

As for the origin of the algorithms, the ETSI web site states that Mitsubishi Electric Corporation holds patents on the algorithm(s) in question. According to the current understanding, the ME and SIM card should not be encumbered by export legislation. Network elements, however, are bound by the normal Wassenaar export controls.

8 Encryption Elsewhere

8.1 GPRS

The radio interface is not the only place in a GPRS or a UMTS network that uses ciphering. Encryption is also used in other locations in which it is mainly used to protect the operator's network.

The GPRS backbone is by definition a closed network. Even if it uses the Internet Protocol, it is not a part of the Internet. All traffic to and from the Internet passes in a tunnel (using a protocol called GTP, GPRS tunneling protocol) from GGSN to SGSN (where it leaves the GPRS backbone). Each operator operates its own GPRS backbone, and communication between them has to be done using a virtual private network (VPN). VPNs are implemented using an encrypted tunnel.

Another location in the GPRS network where encrypted tunnels are used is between a corporate intranet and the GGSN. A corporate customer may wish a direct connection from the GPRS network to its intranet, without forcing the data to pass thorugh the Internet. GGSN is then connected to the intranet using a VPN (which usually uses the Internet as the carrier).

On a higher protocol layer, the mobile station may wish to use encryption as well. Not all applications consider the GPRS encryption as adequate, perhaps because it only covers the radio interface, and perhaps because the security of the algorithm has not been publicly proven. In this case, the mobile station can use for example IPSec to protect its IP traffic, or SSL, TLS or SSH to protect a TCP pipe between applications. As 'application-level' (from the network perspective) security protocols take care of all of the security problems on the lower layers, they also solve the problems inherent with the Internet, after the data has left the GPRS core network.

As a side note, IPSec cannot be used when IP version 4 is in use, as network address translation on the Internet-GPRS border breaks all IPSec authentication modes. Network address translation is more or less a must when IPv4 is in use, as its address space is limited.

8.2 UMTS

All of the discussion about GPRS core network security also applies to UMTS, as it inherits the core network from GPRS. In addition to these security services, UMTS has a provision for network-wide encryption as well as the air interface. In theory, it should be possible to create an encrypted connection through the whole UMTS core network. In principle, this may not be possible, as the legal interception gateway (LIG) requires access to the data in any case.

The network-wide encryption also may encounter problems when transcoding is used. Voice calls may need to be transcoded when they cross network borders, meaning that the voice data may have to go through a codec change, a bitrate change or some other transformation. It is not possible to apply such transformations on an encrypted signal, which implies that the signal has to be decrypted before transcoding.

Network-wide encryption is discussed in more depth in [3GP00b]. ETSI SAGE also defines an algorithm for encryption between network elements. The block encryption algorithm is called Beano. However, only the new 3G-related messages between network elements are ciphered [Wal00]. As is usual with SAGE algorithms, there is no publicly available specification for Beano, although it is listed in a listing of ETSI standard encryption algorithms [ETS].

References

[3GP99] 3G TS 25.301 V3.3.0: 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio Interface Protocol Architecture, December 1999. 3GPP.

[3GP00a] 3G TS 25.322 V3.1.2: 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RLC Protocol Specification, January 2000. 3GPP.

[3GP00b] 3G TS 33.102 V3.3.1: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture, January 2000. 3GPP.

[ETS] ETSI. ETSI Security Algorithms. http://www.etsi.org/dvbandca/ALGO/listtest.htm (valid 24th May 2000).

[ETS98a] ETSI TR 101 375 V1.1.1: Security Algorithms Group of Experts (SAGE); Report on the Specification, Evaluation and Usage of the GSM GPRS Encryption Algorithm (GEA), September 1998. ETSI.

[ETS98b] ETSI TS 101 106 V6.0.1: Digital Cellular Telecommunications System (Phase 2+); General Packet Radio Service (GPRS); GPRS Ciphering Algorithm Requirements, July 1998. ETSI.

[ETS99a] 3G TS 33.105: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements, December 1999. 3GPP.

[ETS99b] Draft ETSI EG 200 234 V1.2.1: Telecommunications Security; A Guide to Specifying Requirements for Cryptographic Algorithms, October 1999. ETSI.

[ETS99c] ETSI TR 101 740 V1.1.1: Security Algorithms Group of Experts (SAGE); Rules of the Management of the Standard GSM GPRS Encryption Algorithm 2 (GEA2), August 1999. ETSI.

[ETS99d] ETSI TS 100 351 V7.1.1: Digital Cellular Telecommunications System (Phase 2+); General Packet Radio Service (GPRS); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) Layer Specification, November 1999. ETSI.

[ETS99e] ETSI TS 100 929 V7.2.0: Digital Cellular Telecommunications System (Phase 2+); Security Related Network Functions, November 1999. ETSI.

[Häm96] Jari Hämäläinen. *Design of GSM High Speed Data Services.* PhD thesis, Tampere University of Technology, Finland, October 1996.

[Mat97] Mitsuru Matsui. New block encryption algorithm MISTY. In Eli Biham, editor, *Fast Software Encryption: 4th International Workshop*, volume 1267 of *Lecture Notes in Computer Science*, pages 54–68, Haifa, Israel, 20–22 January 1997. Springer-Verlag.

[Wal00] Michael Walker. On the Security of 3GPP Networks, May 2000. Presentation in Eurocrypt 2000.