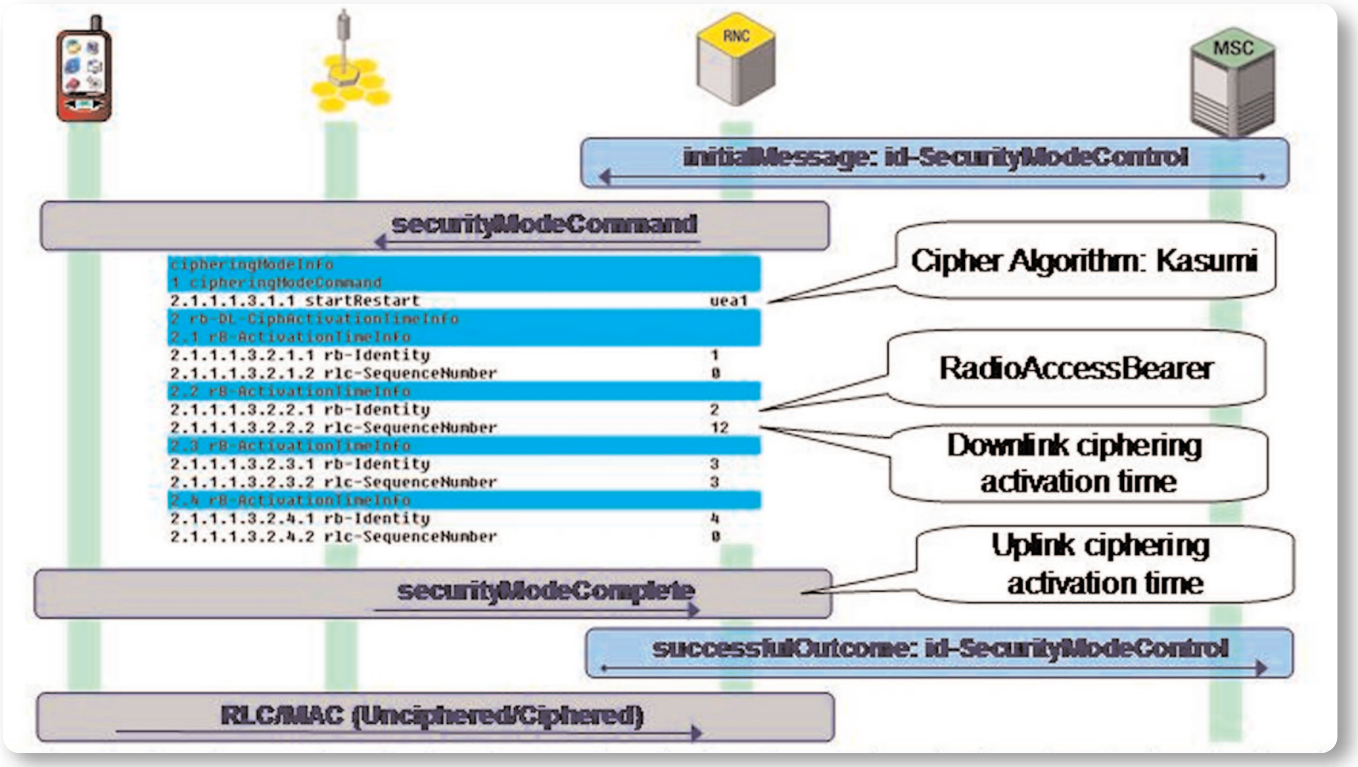


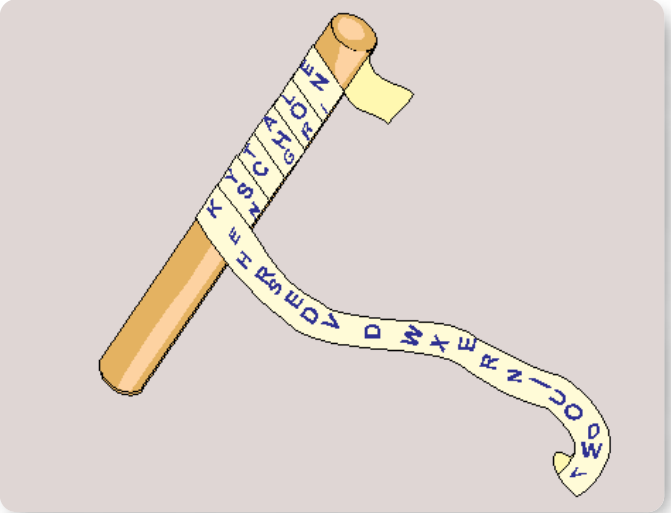
UMTS Security Features

Although Ciphering and Cryptanalysis became a hot topic accelerated by the current geo-politic environment, information security is not a new issue. Caesar was ciphering secret information simply by replacing every character with another one that was in the alphabet three places behind it. The word “cryptology” would be ciphered as “fubswrorjb”. Code books were widely used in the 12th century. Certain key words of a text were replaced by other pre-defined words with completely different meaning.

In a digital mobile network the subscriber is exposed to five basic attacks and needs to be protected against them. Eavesdropping (theft of voice and data information); Unauthorized Identification; Unauthorized Usage of Services; and Offending the Data Integrity (data falsification by an intruder).

This paper describes the principles of GSM Protection and the evolution to UMTS security. Details of the UMTS security architecture and used algorithms will be discussed.

Content



▶ **Figure 1.** *Ciphering in ancient Greece.*

▶ **Figure 2.** *Enigma and Bomb as examples for decryption and encryption.*

Historic Development

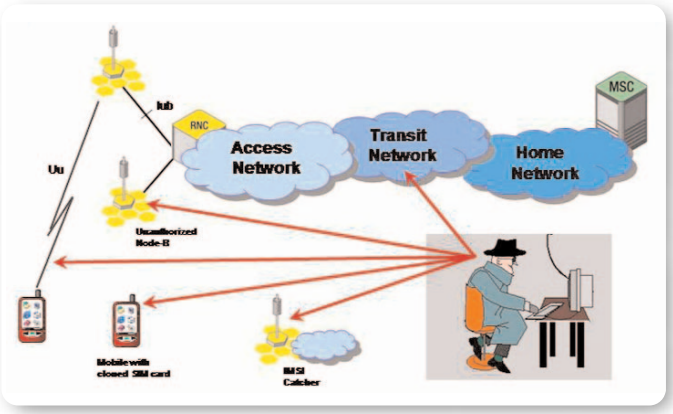
Although Ciphering and Cryptanalysis became a hot topic accelerated by the current geo-politic environment, information security is not a new issue.

400 years B.C. the ancient Greeks used so called “skytals” for encryption. A skytal is a wooden stick of fixed diameter with a long paper strip wound around the stick. The sender wrote a message on the paper in longitudinal direction. The unwound paper strip gave no meaningful information to the courier or other unauthorized person. Only a receiver who owns a stick with the same diameter was able to decipher the message (see Figure 1).

Caesar was ciphering secret information simply by replacing every character with another one that was in the alphabet three places behind it. The word “cryptology” would be ciphered as “fubswrorjb”. Code books were widely used in the 12th century. Certain key words of a text were replaced by other pre-defined words with completely different meaning. A receiver who owns an identical code book is able to derive the original message.

Kasiski’s and William F. Friedman’s fundamental research about statistical methods in the 19th century are the foundation of modern methods for ciphering and cryptanalysis.

The Second World War gave another boost for ciphering technologies. The Enigma was an example of advanced ciphering machines used by the German



▶ **Figure 3.** *Potential attack points of intruders.*

military. Great Britain, under Alan Turing with his “bomb”, was able to crack Enigma (Figure 2).

Another milestone was Claude E. Shannon’s article “Communication Theory of Secret Systems” published in 1949. It gives the information-theoretic basis for cryptology and proves Vernam’s “One-Time-Pad” as a secure crypto-system.

In the last century several ciphering technologies has been developed, which can be divided in symmetric and asymmetric methods. Symmetric methods are less secure because the same key is used for ciphering and deciphering. Examples are the Data Encryption Standard (DES) developed by IBM and the International Data Encrypted Algorithm (IDEA) proposed by Lai and Massey.

```
000001--  Actual Timing Advance                          1
L3 Information
00001011  IE Name                                       L3 Information
00000000  Spare                                         0
00010010  LLSDU Length                                  18
**B18***  DTAP LLSDU                                    06 15 2a 2a 01 25 06 a7 97 63 85...
E-GSM 04.08 (DTAP) 5.3.0) (DTAP)  MEASREP (= Measurement report)
Measurement report
----0110  Protocol Discriminator                        radio resources management msg
0000----  Skip Indicator                                0
-0010101  Message Type                                  21
0-------  Extension bit                                 0
Measurement Results
0-------  BA-USED                                       0
-0------  DTX-USED                                      not used
--101010  RXLEV-FULL-SERVING-CELL                       -69 dBm to -68 dBm
0-------  Spare                                         0
-0------  Measurement results valid                     Valid
--101010  RXLEV-SUB-SERVING-CELL                        -69 dBm to -68 dBm
0-------  Spare                                         0
-000----  RXQUAL-FULL-SERVING-CELL                      BER less than 0.2%
----000-  RXQUAL-SUB-SERVING-CELL                       BER less than 0.2%
***b3***  NO-NCELL-M                                    4 NCELL measurement result
--100101  RXLEV-NCELL 1                                -74 dBm to -73 dBm
00000---  BCCH-FREQ-NCELL 1                             0
-----110  BSIC-NCC-NCELL 1                              6
101-----  BSIC-BCC-NCELL 1                              5
```

▶ **Figure 4.** *Measurement result message.*

Asymmetric technologies use one encryption key (public key) and another decryption key (private key). It is not possible to calculate the decryption key only by knowing the encryption key. The most common asymmetric ciphering method is RSA, developed by **R**ivest, **S**hamir and **A**dleman in 1978. The method is based on the principle of big prime numbers: It is relatively easy to detect two prime numbers x and y with 1000 and more digits. However, even today it is not possible to calculate the factors of the product "x * y" in reasonable time. Mitsubishi developed an algorithm for ciphering and integrity protection used in UMTS networks. The 3GPP standard is open for other ciphering methods, but today Kasumi is the first and only ciphering algorithm used in UMTS.

Security Threats and Protection in Mobile Networks

In a digital mobile network the subscriber is exposed five basic attacks as described below:

– Eavesdropping (theft of voice and data information)

– Unauthorized Identification

– Unauthorized usage of services

– Offending the data integrity (data falsification by an intruder)

– Observation

  – Detection of the current location

  – Observation of communication relations (Who is communicating with whom?)

  – Generation of behaviour profiles

As an example for unlawful observation, Figure 4 shows a part of a Measurement Report Message captured on the GSM Abis Interface. An active mobile permanently measures the power level and the bit error rate of its serving cell and up to six neighbour cells. This information is transmitted from the mobile over the base transceiver station (BTS) to the base station controller (BSC). In addition, the BTS sends the Timing Advance Information to the mobile. The Timing Advance is a value in the range from 0 to 63. The Timing Advance is an indicator of the distance between BTS and mobile. Assuming that the maximum cell size in GSM is 30 km, the Timing Advance value allows to estimate the distance with 500 m precision. In urban places however, the cell size is much smaller. Combining that information, a potential intruder can relatively exactly determine the location of the mobile subscriber.

GSM was originally designed as a circuit-switched voice network. In contradiction to the voice data, controlling information are never ciphered in GSM. In addition, the ciphering is limited to the air interface. Needless to say, that Short Messages are transferred over the signaling network and therefore are never ciphered.

GPRS as extension to GSM already offers significant security improvements. User *and* controlling information are ciphered not only over air interface but also over the Gb-Interface between BSC and SGSN. Commonly used in commercial networks are GEA1 and GEA2, recently under development is GEA3. The most secure mobile network is the UMTS network.

UMTS actively combats prior mentioned threats offering the following security procedures:

– Ciphering of control information and user data

– Authentication of the user towards the network

– Authentication of the network towards the user

– Integrity protection

– Anonymity

The UMTS security procedures are described in the following chapters. Security mechanism over transport networks (Tunneling, IPsec) are not part of this article.

Principles of GSM Security and the Evolution to UMTS Security

As UMTS can be seen as an evolution of the 2G (GSM) communication mobile systems, the security features for UMTS are based on the GSM security features and are enhanced. When UMTS was defined from the Third Generation Partnership Project, better known as 3GPP, there was the basic requirement to adopt the proven and robust security features from GSM and to be as compatible with the 2G security architecture as possible. UMTS should correct the problems with GSM by addressing its real and perceived security weaknesses and to added new security features to secure the new services offered by 3G.

The limitations and weaknesses of the GSM security architecture stem by large from designing limitations rather than on defects in the security mechanisms themselves. GSM has the following specific weaknesses that are corrected within UMTS.

– Active attacks using a false basestation

  – Used as “IMSI” catcher – cloning risk

  – Used to intercept mobile originated calls - Encryption is controlled by the network, so user is unaware if it is not activated

– Cipher keys and authentication data are transmitted in clear between and within networks

  – Signaling system vulnerable to interception and impersonation

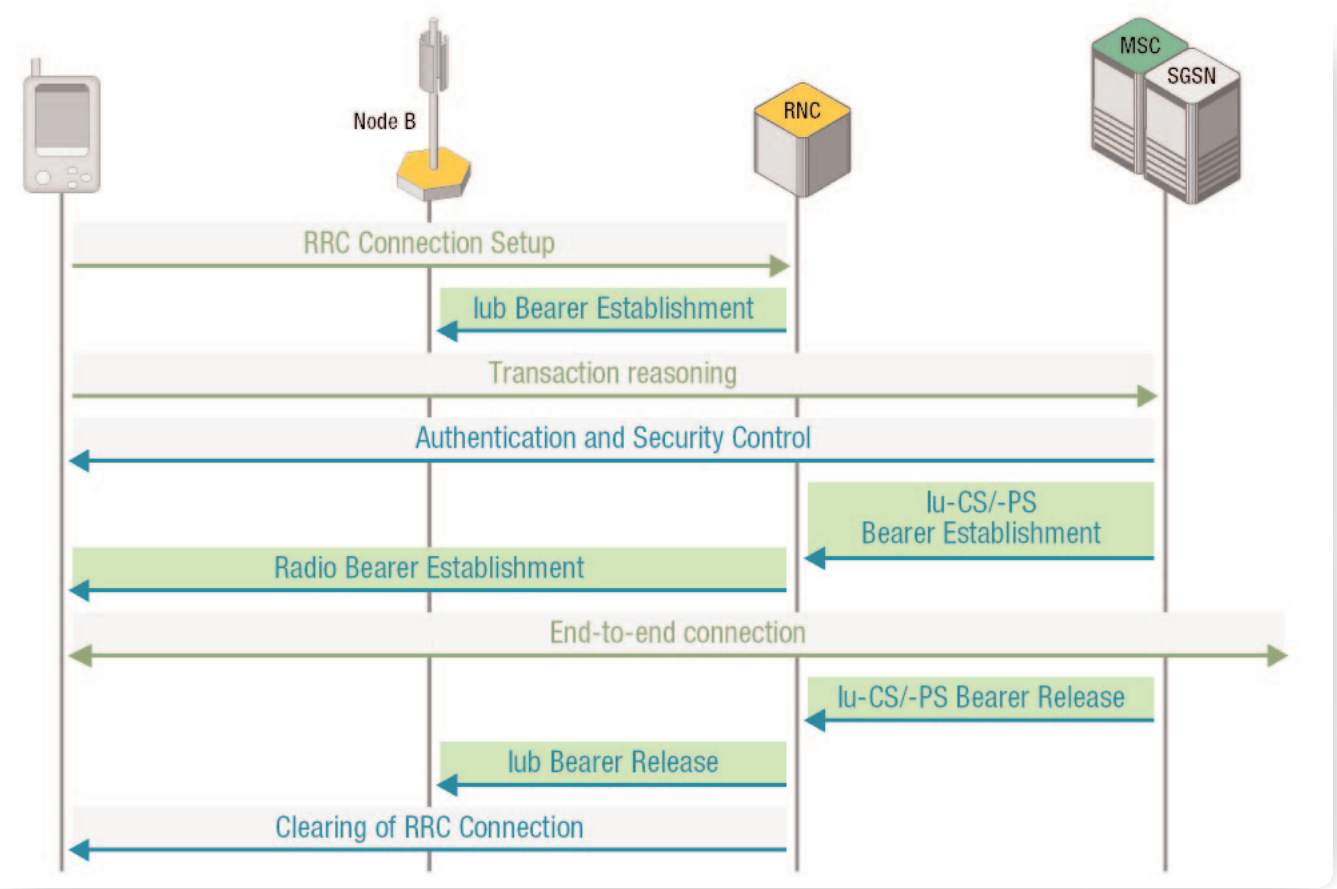
– Encryption of the user and signaling data does not carry far enough through the network to prevent being sent over microwave links (BTS to BSC) – Encryption terminated too soon

– Possibility of channel hijack in networks that does not offer confidentiality

– Data integrity is not provided, except traditional non-cryptographic link-layer checksums

– IMEI (International Mobile Equipment identifier - unique) is an unsecured identity and should be treated as such – as the Terminal is an unsecured environment, trust in the terminal identity is misplaced

– Fraud and lawful interception was not considered in the design phase of 2G



▶ **Figure 5.** *Network Transitions.*

– There is no HE (Home Environment) knowledge or control of how an SN (Serving Network) uses authentication parameters for HE subscribers roaming in that SN

– Systems do not have the flexibility to upgrade and improve security functionality over time

– Confidence in strength of algorithms

  – Failure to choose best authentication algorithm

  – Improvements in cryptanalysis of A5/1

    – Key length too short

    – Lack of openness in design and publication

Furthermore, there are challenges that security services will have to cope within 3G systems that will probably be

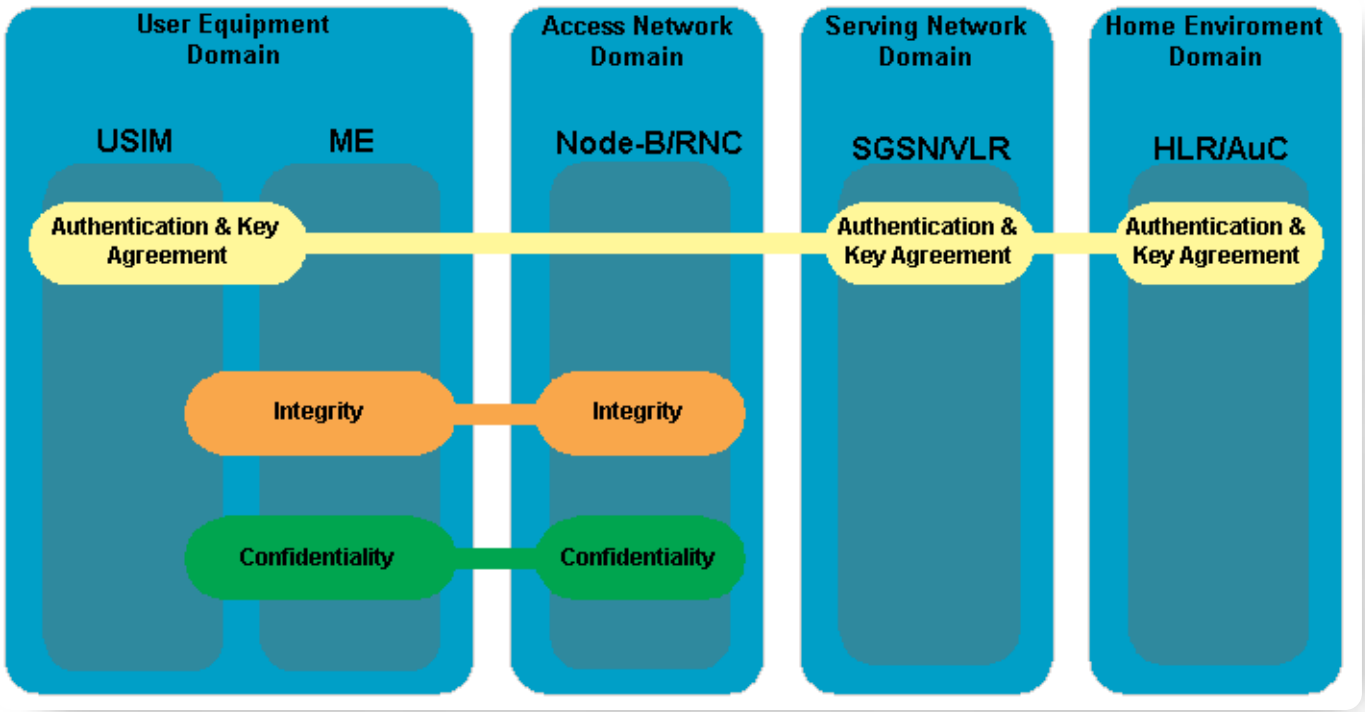
– Totally new services

– There will be new and different providers of services

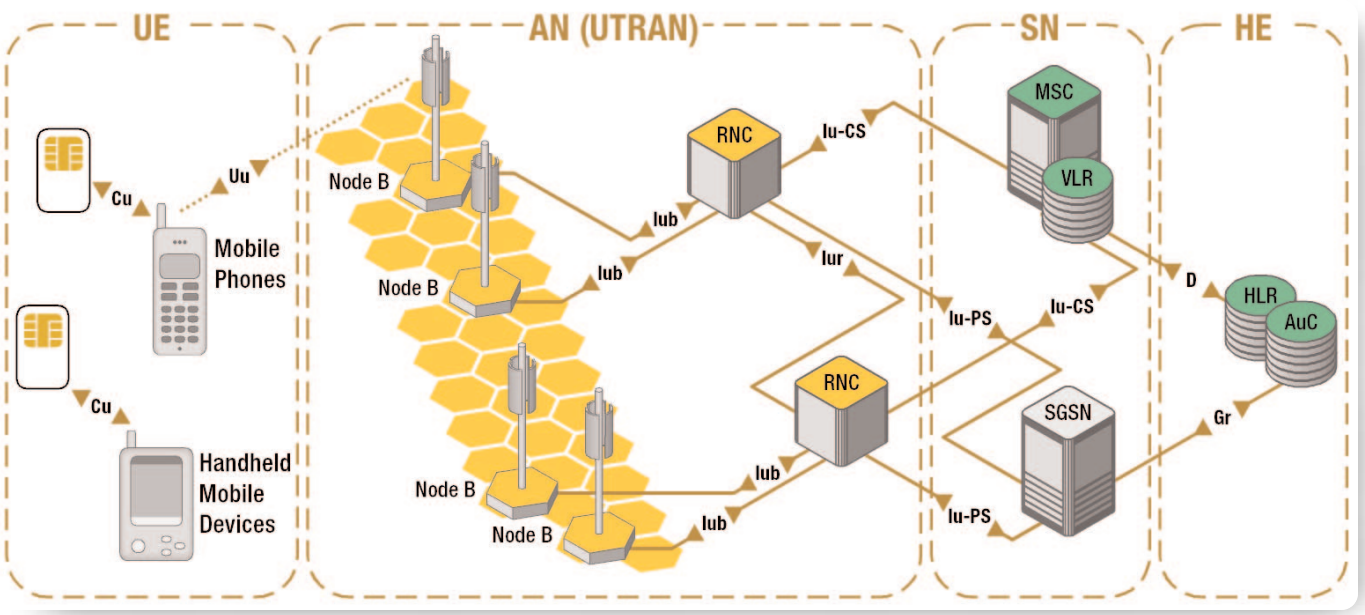
– Mobile systems will be positioned as preferable to fixed line systems for users

– Users will typically have more control over their service profile

Data services will be more important than voice services



▶ **Figure 6.** *UMTS Security Architecture.*



▶ **Figure 7.** *UMTS Interface and Domain Architecture Overview.*

– The Terminal will be used as a platform for e-commerce and other sensitive applications

The following features of GSM security are reused for UMTS:

– User Authentication and radio interface encryption

– Subscriber identity confidentiality on the radio interface

– SIM as a removable, hardware security module, in UMTS called USIM

  – Terminal independent

  – Management of all customer parameter

– Operation without user assistance

– Minimized trust of the SN by the HE

UMTS Security Architecture

Based on Figure 5, showing the order of all transactions of a connection, the next chapters will cover the Authentication and Security Control part and explain the overall security functions for the connection.

The 3G security architecture is a set of security features and enhancements that are fully described in the 3GPP 33.102 and is based on the three security principles:

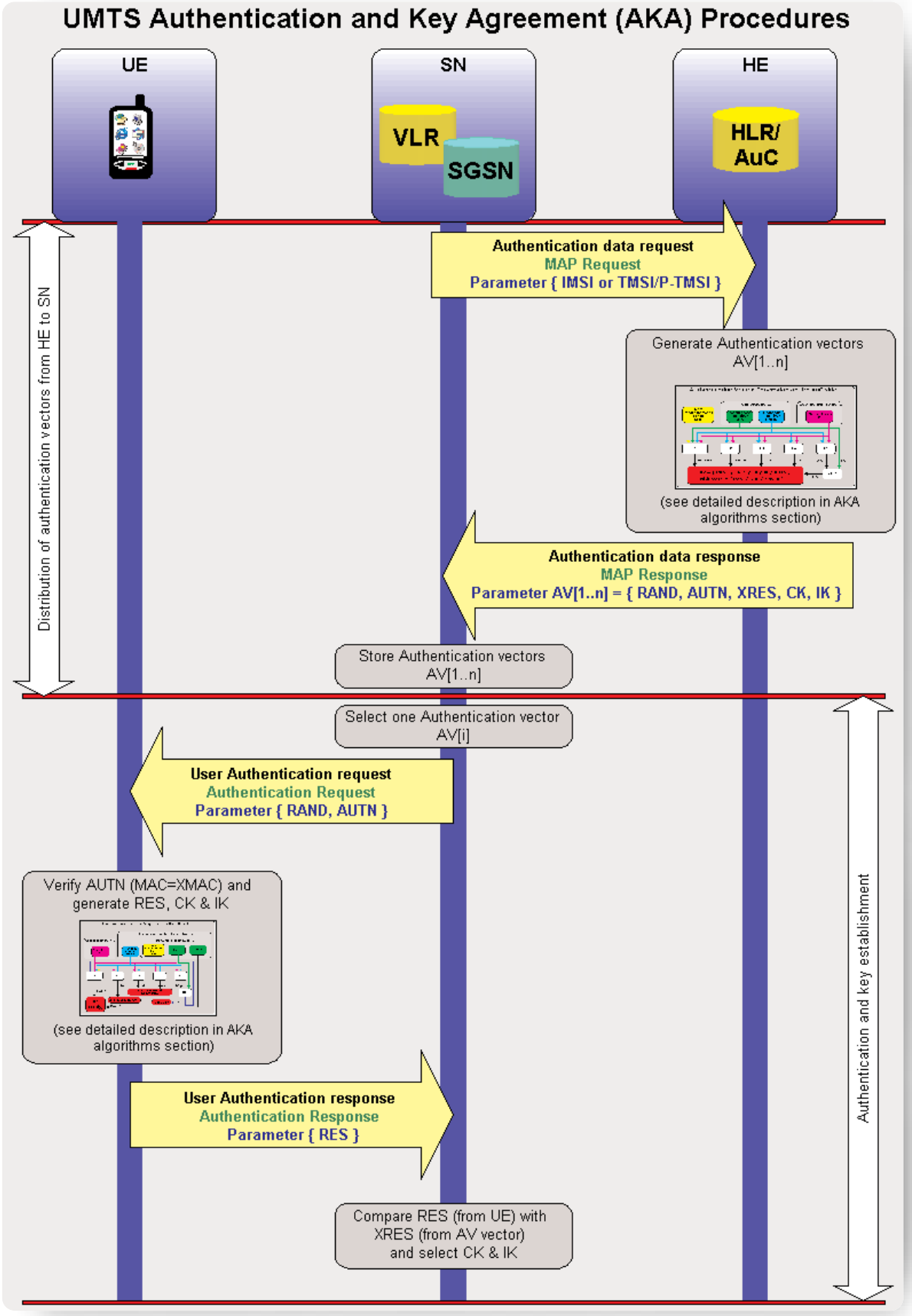
– **Authentication** and Key Agreement (AKA)

  Authentication is provided to assure the claimed identity between the user and the network, divided in into two parts

  – Authentication of the user towards the network

  – Authentication of the network towards the user (new in UMTS)

  This is done in so called “one-pass authentication” reducing messages sent back and forth. After these procedures the user will be sure that he is connected to his served/trusted network and the network is sure that the claimed identity of the user is true. Authentication is needed for the other security mechanisms like confidentiality and integrity.



▶ **Figure 8.** *AKA procedure – sequence diagram.*

From	2. MSG	3. Prot	3. MSG	Procedure Code	Last Prot	Last MSG
G62 -..	SD	RL	RL		SCCP	CC
Gr G62	MSU	SCCP	UDT		MAP	BEG
Gr G62	MSU	SCCP	UDT		MAP	END

Frame View

BITMASK	ID Name	Comment or Value
01010110	Length	86
3.1.2.2.1	Quintuplet List	
10100001	Tag	(CONT C [1])
01010100	Length	84
3.1.2.2.1.1	Authentication Quintuplet	
00110000	Tag	(UNIV C Sequence (of))
01010010	Length	82
3.1.2.2.1.1.1	Rand	
00000100	Tag	(UNIV P OctetString)
00010000	Length	16
B16*	Authentication Random No	02 05 96 bd 18 7a 9a d7 20 07 cd 7f be 01 60 d9
3.1.2.2.1.1.2	XRES	
00000100	Tag	(UNIV P OctetString)
00001000	Length	8
B8	XRES	cc f5 58 34 bb 2c b0 75
3.1.2.2.1.1.3	CK	
00000100	Tag	(UNIV P OctetString)
00010000	Length	16
B16*	CK	57 58 f4 11 f4 47 15 11 f1 19 42 d3 54 85 66 15
3.1.2.2.1.1.4	IK	
00000100	Tag	(UNIV P OctetString)
00010000	Length	16
B16*	IK	f9 26 d5 9e c9 33 95 aa 51 c9 d0 68 75 12 e5 d0
3.1.2.2.1.1.5	AUTN	
00000100	Tag	(UNIV P OctetString)
00010000	Length	16
B16*	AUTN	52 e5 03 bf 78 83 00 00 6f a9 2e dc 4b cd 67 4e

▶ **Figure 9.** *Example for AC (Authentication Vector) sending from HE to SN in Authentication data response.*

communication and are not equivalent to transport level integrity.

– **Confidentiality**

Confidentiality is used to keep information secured from unwanted parties. This is achieved by ciphering of the user/signaling data between the subscriber and the network and by referring to the subscriber by temporary identities (TMSI/P-TMSI) instead of using the global identity, IMSI. Ciphering is carried out between the Users terminal (USIM) and the RNC. User confidentiality is between the subscriber and the VLR/SGSN. If the network does not provide user data confidentiality, the subscriber is informed and has the opportunity to refuse connections.

Parts that are confidential are:

– Subscriber identity
– Subscriber's current location
– User Data (Voice and data)
– Signaling data

Authentication and Key Agreement (AKA)

UMTS security starts with the Authentication and Key Agreement (AKA), the most important feature in the UMTS system. All other services depend on them since no higher level services can be used without authentication of the user.

Mutual Authentication

– Identifying the user to the network

– Identifying the network to the user

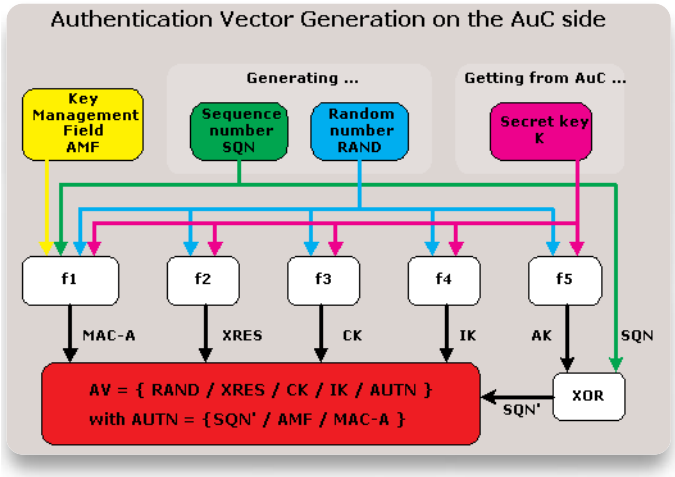
Key agreement

– Generating the cipher key

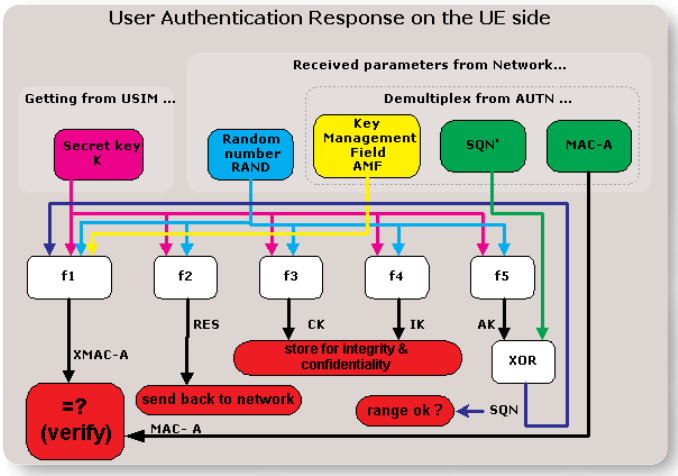
– Generating the Integrity key

After Authentication and Key Agreement

– Integrity protection of messages



▶ **Figure 10.** *Authentication Vector generation on the AuC side (HE).*



▶ **Figure 11.** *User Authentication Response on the User side.*

– Confidentiality protection of signaling data

– Confidentiality protection of user data

The mechanism of mutual authentication is achieved by the user and the network showing knowledge of a secret key (K) which is shared between and available only to the USIM and the AuC in the user's HE. The method was chosen in such a way as to achieve maximum compatibility with the current GSM security architecture and facilitate migration from GSM to UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication

The authenticating parties are the AuC of the user's HE (HLR/AuC) and the USIM in the user's mobile station. The mechanism consists of the distribution of authentication data from the HLR/AuC to the VLR/SGSN and a procedure to authenticate and establish new cipher and integrity keys between the VLR/SGSN and the MS.

AKA Procedure

Once the HE/AuC has received a request from the VLR/SGSN, it sends an ordered array of *n* authentication vectors to the VLR/SGSN. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is only valid for one authentication and key agreement between the VLR/SGSN and the USIM and are ordered based on sequence number. The VLR/SGSN initiates an authentication and key agreement by selecting the next authentication vector from the ordered array and sending the parameters RAND and AUTN to the user. If the AUTN is accepted by the USIM, it produces a response RES that is sent back to the VLR/SGSN. Authentication vectors in a particular node are used on a first-in/first-out basis. The USIM also computes CK and IK. The VLR/SGSN compares the received RES with XRES. If they match the VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be transferred by the USIM and the VLR/SGSN to the entities that perform ciphering and integrity functions. VLR/SGSNs can offer secure service even when HE/AuC links are unavailable by allowing them to use previously derived cipher and integrity keys for a user so that a secure connection can still be set up without the need for an authentication and key agreement. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signalling messages.

Function	Description	Input Parameter	Output Parameter
f0	The random challenge generating function	RAND	RAND
f1	The network authentication function	AMF, K, RAND	MAC-A (AuC side) /XMAC-A (UE side)
f2	The user authentication function	K, RAND	RES (UE side) /XRES (AuC side)
f3	The cipher key derivation function	K, RAND	CK
f4	The integrity key derivation function	K, RAND	IK
f5	The anonymity key derivation function	K, RAND	AK
f8	The confidentiality key stream generating function	Count-C, Bearer, Direction, Length, CK	<Keystream block>
f9	The integrity stamp generating function	IK, FRESH, Direction, Count-I, Message	MAC-I (UE side) /XMAC-I (RNC side)

Parameter	Definition	Bit size
K	Pre-shared secret **k**ey stored in the USIM and AuC	128
RAND	The **rand**om challenge to be sent to the USIM	128
SQN	**Seq**uence **n**umber	48
AK	**A**nonymity **K**ey	48
AMF	**A**uthentication **M**anagement **F**ield	16
MAC	**M**essage **A**uthentication **C**ode	64
MAC-A / XMAC-A	MAC used for authentication and key agreement	64
MAC-I / XMAC-I	Message authentication code for data integrity	64
CK	**C**ipher **k**ey for confidentiality	128
IK	**I**ntegrity **k**ey for integrity checking	128
RES	**Res**ponse	32-128
X-RES	The e**x**pected **res**ult from the USIM	32-128
AUTN	**Aut**hentication token that authenticates the AuC towards the USIM (AMF, MAC-A, SQN')	128 (16+64+48)
COUNT-I	The integrity sequence number	32
FRESH	The network-side random value	32
DIRECTION	Either 0 (UE->RNC=uplink) or 1 (RNC->UE=downlink)	1
Message	The message themselves	variant

AKA is performed when the following events happen:

– Registration of a user in a Serving Network
– After a service request
– Location Update Request
– Attach Request
– Detach request
– Connection re-establishment request

Registration of a subscriber in a serving network typically occurs when the user goes to another country. The coverage area of an operator is nationwide, and roaming between national operators will therefore be limited. The first time the subscriber then connects to the serving network, he gets registered in the Serving Network.

Service Request is the possibility for higher-level protocols/applications to ask for AKA to be performed. E.g. performing AKA to increase security before an online banking transaction.

The terminal updates the HLR regularly with its position in Location Update Requests.

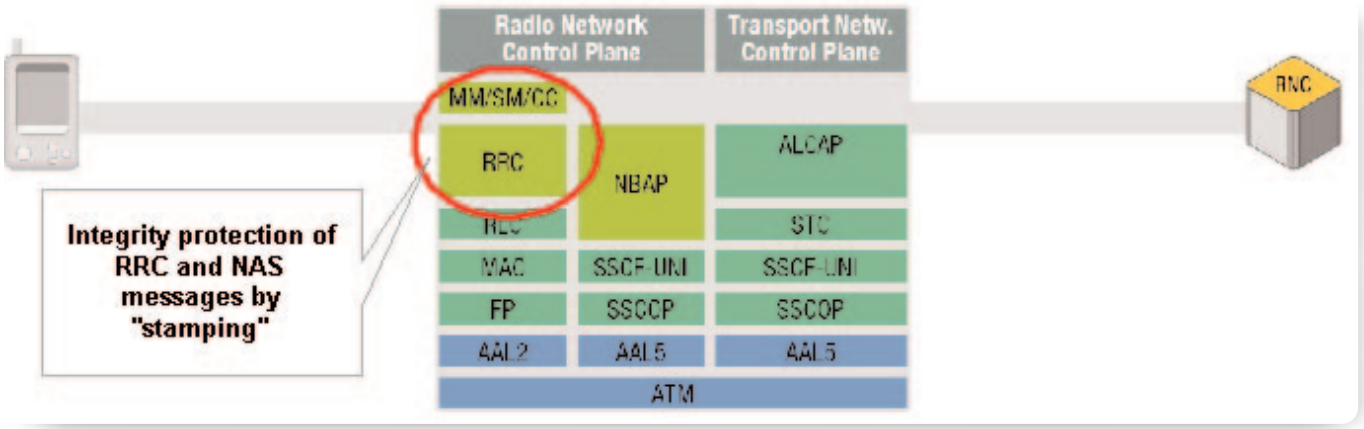
Attach request and detach request are procedures to connect and disconnect the subscriber to the network.

Connection re-establishment request is performed when the maximum number of local authentications has been conducted.

A weakness of the AKA is, that the HLR/AuC does not check if the information sent from the VLR/SGSN (Authentication information) is correct or not.

Algorithms used for AKA

The security features of UMTS are fulfilled with a set of cryptographic functions and algorithms. A total of 10 functions are needed to perform all the necessary features, f0-f5, f8 and f9.



▶ **Figure 12.** *Iub Control plane.*

f0 is the random challenge generating functions, the next seven are key generating functions, so they are all operator specific. The keys used for authentication are only generated in USIM and the AuC, the two domains that the same operator is always in charge of.

Function f8 and f9 are used in USIM and RNC, and since these two domains may be of different operators, they cannot be operator specific. The functions use the pre-shared secret key (K) indirectly. This is to keep from distributing K in the network, and keep it safe in the USIM and AuC.

The functions f1-f5 are called key generating functions and are used in the initial Authentication and Key agreement procedure. The life time of the Key is dependent on how long the keys have been used. The maximum limits for use of same keys are defended by the operator, and whenever the USIM finds the keys being used for as long as allowed, it will trigger the VLR/SGSN to use a new AV.

The functions f1-f5 shall be designed so that they can be implemented with a 8-bit microprocessor running at 3.25MHz with 8kbyte ROM and 300byte RAM and produce AK, XMAC-A, RES, CK and IK in less than 500ms execution time.

When generating a new AV the AuC reads the stored value of the sequence number, SQN and then generates a new SQN' and a random challenge RAND. Together with the stored AV and Key Management Field (AMF) and the pre-shared secret key (K), these four input parameters are ready to be used. The functions f1..f5 uses these inputs and generates the values for the message authentication code, MAC-A, the expected result, XRES, the Cipher Key (CK), the Integrity Key (IK) and the Anonymity Key (AK). With the SQN xor'ed AK, AMF and MAC, the Authentication Token, AUTN is made. The Authentication vector (AV) is sent to the SGSN/VLR and stored there, while the parameter pair AUTN and RAND are then transmitted from the SGSN/VLR to the User. The cipher key (Ck) and integrity key (Ik) are used, after a successful authentication, for confidentiality (ciphering) and integrity.

Only one of the four parameters that the AuC has is stored in the USIM, the pre-shared secret key (K). The rest of the parameters it has to receive from the network (RAND and AUTN).

The secret key K is then used with the received AMF, SQN' and RAND to generate the Expected Message Authentication Code (XMAC-A). This is then compared with the MAC-A. If the X-MAC and MAC matches, the USIM have authenticated that the message is originated in its Home Environment and thereby connected to a Serving Network that is trusted by the HE.

With a successful network authentication, the USIM verifies if the sequence number received is in within the correct range. With a sequence number within the correct range, the USIM continues to generate the RES, which is sent back to the network to verify a successful user authentication.

KASUMI/Misty

The KASUMI algorithm is the core algorithm used in functions f8 (Confidentiality) and f9 (Integrity). KASUMI is based on the block cipher "Misty" proposed by Mitsuru Matsui (Mitsubishi), first published in 1996. Misty translated from English to Japanese means KASUMI.

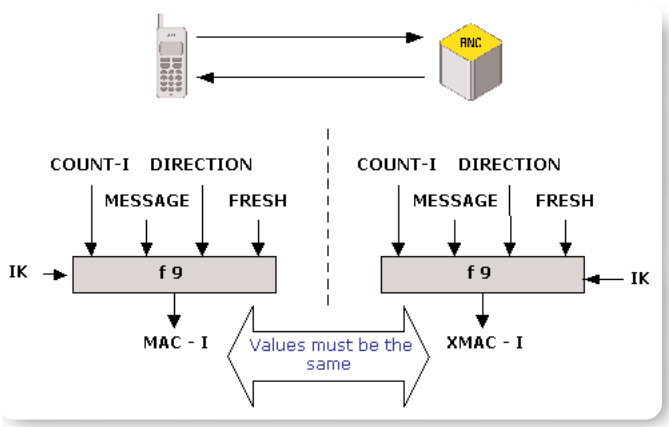
Misty was designed to fulfill the following design criteria:

– **High security:**
  – Provable security against differential and linear cryptanalysis
– **Multi platform:**
  – High speed in both software and hardware implementations
    – Pentium III (800MHz) (Assembly Language Program)
      – Encryption speed 230Mbps
    – ASIC H/W (Mitsubishi 0.35 micron CMOS Design Library)
      – Encryption speed 800Mbps
      – Gate size 50Kgates
– **Compact:**
  – Low gate count and low power consumption in hardware
    – ASIC (Mitsubishi 0.35 micron CMOS Design Library)
      – Gate size 7.6Kgates
      – Encryption speed 72Mbps
  – A requirement for W-CDMA encryption algorithm: "gate size must be smaller than 10Kgates"

KASUMI is a variant of MISTY1 designed for W-CDMA systems and has been adopted as a mandatory algorithm for data confidentiality and data integrity in W-CDMA by 3GPP in 1999. Here are some examples of improvement:

– Simpler key schedule
– Additional functions to complicate cryptanalysis without affection provable security aspects
– Changes to improve statistical properties
– Minor changes to speed up
– Stream ciphering f8 uses KASUMI in a form of output feedback, but with:
  – BLKCNT added to prevent cycling
  – Initial extra encryption added to protect against chosen plaintext attack and collision
– Integrity f9 uses KASUMI to form CBC MAC with Non-standard addition of 2nd feedforward

Mitsubishi Electric Corporation holds the rights on essential patents on the Algorithms. Therefore the Beneficiary must get a separate royalty free IPR License Agreement from Mitsubishi Electronic Corporation Japan.

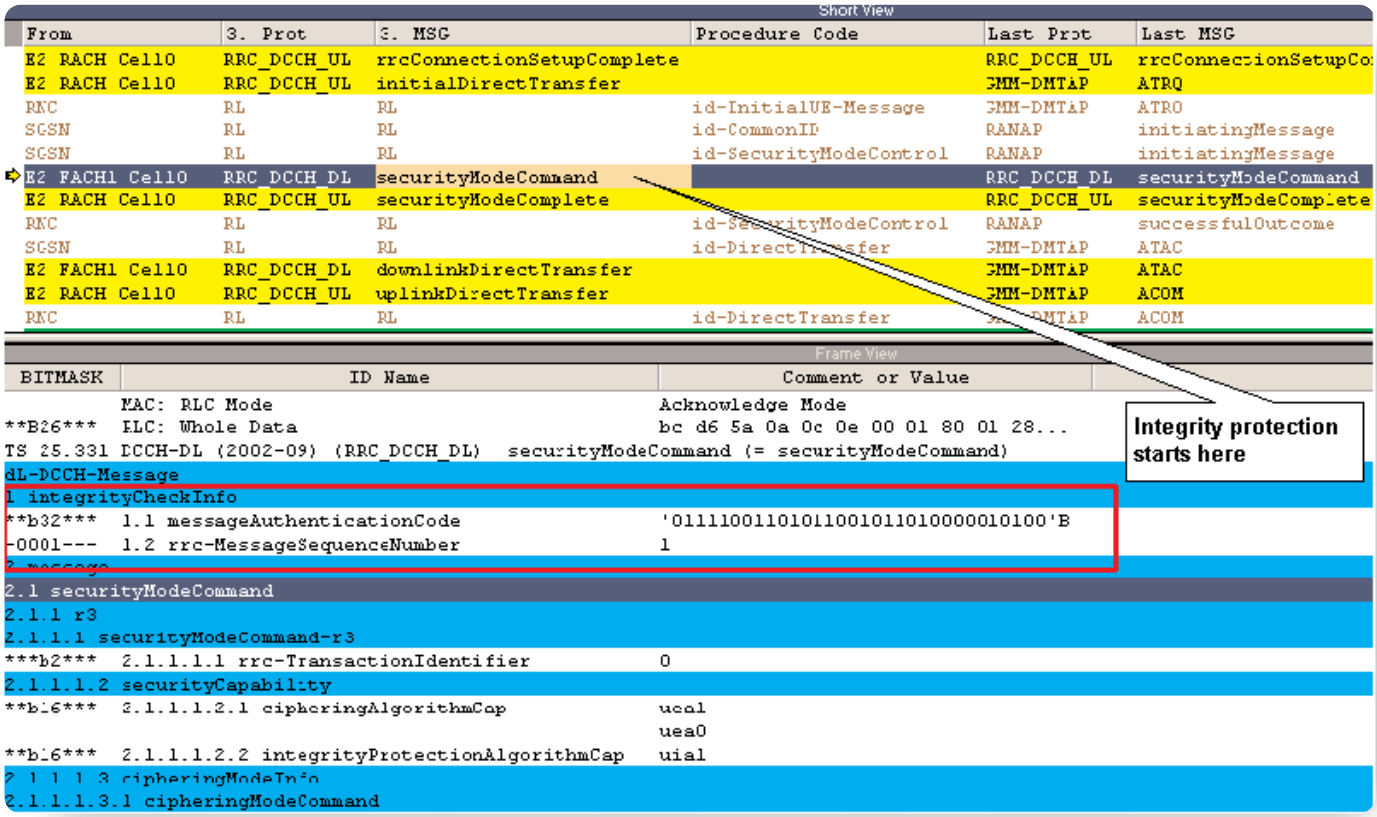


▶ **Figure 13.** *Integrity check procedure.*

Basically KASUMI is a block cipher that produces a 64-bit output from a 64-bit input under the control of a 128-bit key. A detailed description can be found in the 3GPP Specification TS 35.202. MISTY1 and KASUMI have been widely studied since its publication, but no serious flaws have been found.

Integrity - Air Interface Integrity Mechanism

Most control signalling information elements that are sent between the User Equipment (UE) and the network are considered sensitive and must be integrity protected. Integrity protection shall apply at the RRC layer. On messages transmitted between the UE and the RNC, a message integrity function (f9) shall be applied on the signalling information. User data are on the other hand not integrity protected and it's up to higher-level protocols to add this if needed. Integrity protection is required, not optional, in UMTS for signalling messages.



▶ **Figure 14.** *Example of "stamped" message for Integrity check.*

After the RRC connection has been established and the security mode set-up procedure has been performed, all dedicated control signalling messages between UE and the network shall be integrity-protected.

Threats Against Integrity

Manipulation of messages is the one generic threat against integrity. This includes deliberate or accidental modification, insertion, replaying or deletion by an intruder.

Both user data and signaling/control data are venerable to manipulation. And the attacks may be conducted on the radio interface, in the fixed network or on the terminal and the USIM/UICC.

The threats against integrity can be summarized to:

– Manipulation of transmitted data: Intruders may manipulate data transmitted over all reachable interfaces.

– Manipulation of stored data: Intruders may manipulate data that are stored on system entities, in the terminal or stored by the USIM. These data includes the IMEI stored on the terminal, and data and applications downloaded to the terminal or USIM. Only the risks associated with the threats to data stored on the terminal or USIM are regarded to be significant, and only the risk for manipulation of the IMEI is regarded as being of major importance.

– Manipulation by masquerading: Intruders may masquerade as a communication participant and thereby manipulate data on any interface. It is also possible to manipulate the USIM behavior by masquerading as the originator of malicious applications or data downloaded to the terminal or USIM.

On the radio interface this is considered to be a major threat, whereas manipulation of the terminal or USIM behavior by masquerading as the originator of applications and/or data is considered to be of medium significance. Masquerading could be done both to fake a legal user and to fake a serving network.

Distribution of Keys

The integrity protection in UMTS is implemented between the RNC and the UE. Therefore IK must be distributed from the AuC to the RNC. The IK is part of an authentication vector which is sent to the SN (VLR/SGSN) from the AuC following an authentication

data request. To facilitate subsequent authentications, up to 5 authentication vectors are sent for each request. The IK is sent from the VLR/SGSN to the RNC as part of a RANAP message called security mode command.

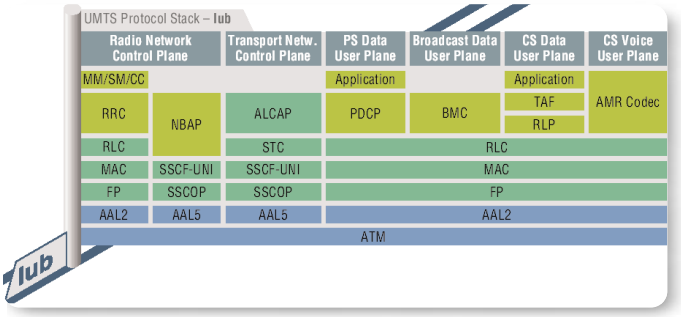
Integrity Function f9

The function f9 is used in a similar way as the Authentication token (AUTN). It adds a 'stamp' to messages to ensure that the message is generated at the claimed identity, either the USIM or the Serving Network, on behalf of the HE. It also makes sure that the message has not been tampered with.

The input parameters to the algorithm are the Integrity Key (IK), the integrity sequence number (COUNT I), a random value generated by the network side (FRESH), the direction bit DIRECTION and the signalling data MESSAGE. Based on these input parameters the user computes message authentication code for data integrity MAC-I using the integrity algorithm f9. The MAC-I is then appended to the message when sent over the radio access link. The receiver computes XMAC-I on the message received in the same way as the sender computed MAC-I on the message sent and verifies the data integrity of the message by comparing it to the received MAC-I.

Protection against replay is important and guaranteed with:

– The value of COUNT-I is incremented for each message, while the generation of a new FRESH value and initialization of COUNT-I take place at connection set-up.



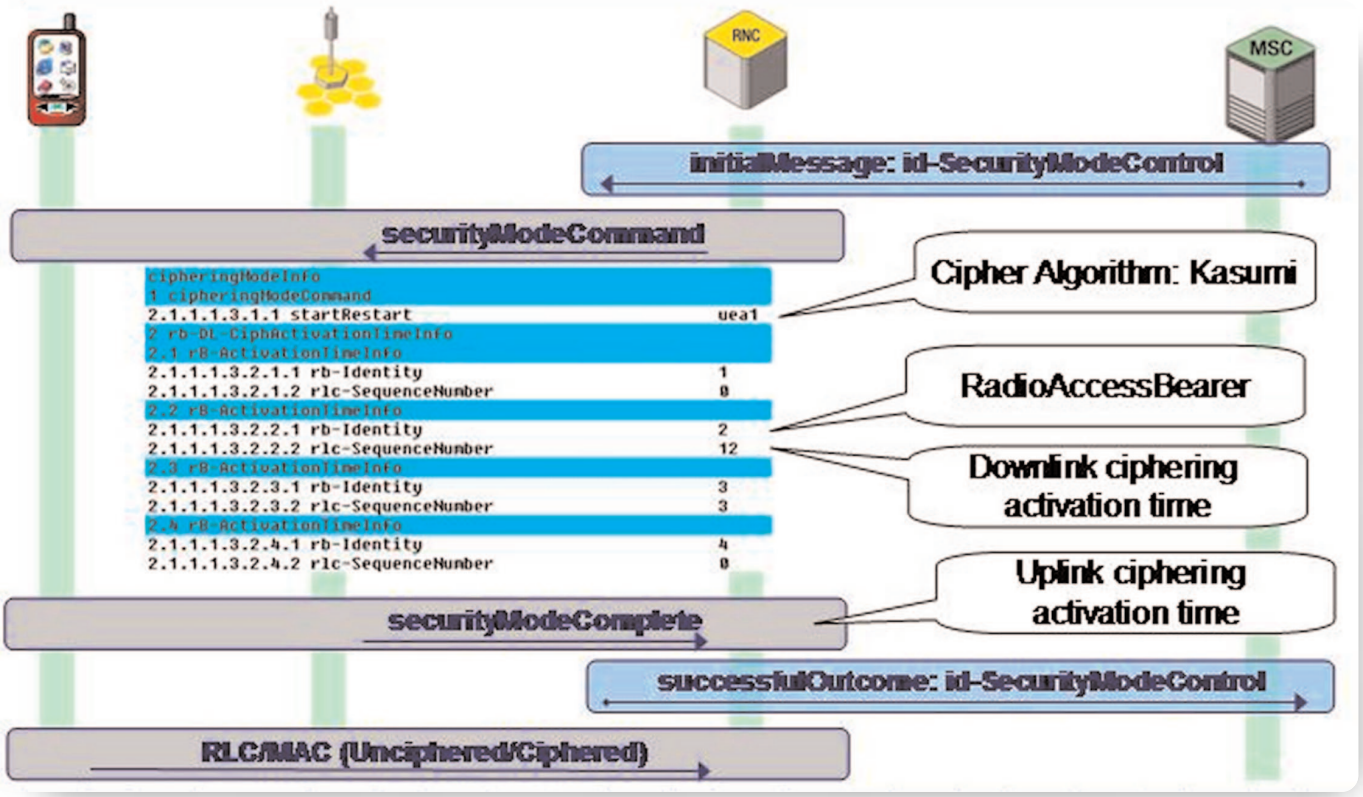
▶ **Figure 15.** *Iub Protocol stack.*

– The COUNT-I value is initialized in the UE and therefore primarily protects the user side from replay attacks. Likewise the FRESH value primarily provides replay protection for the network side.

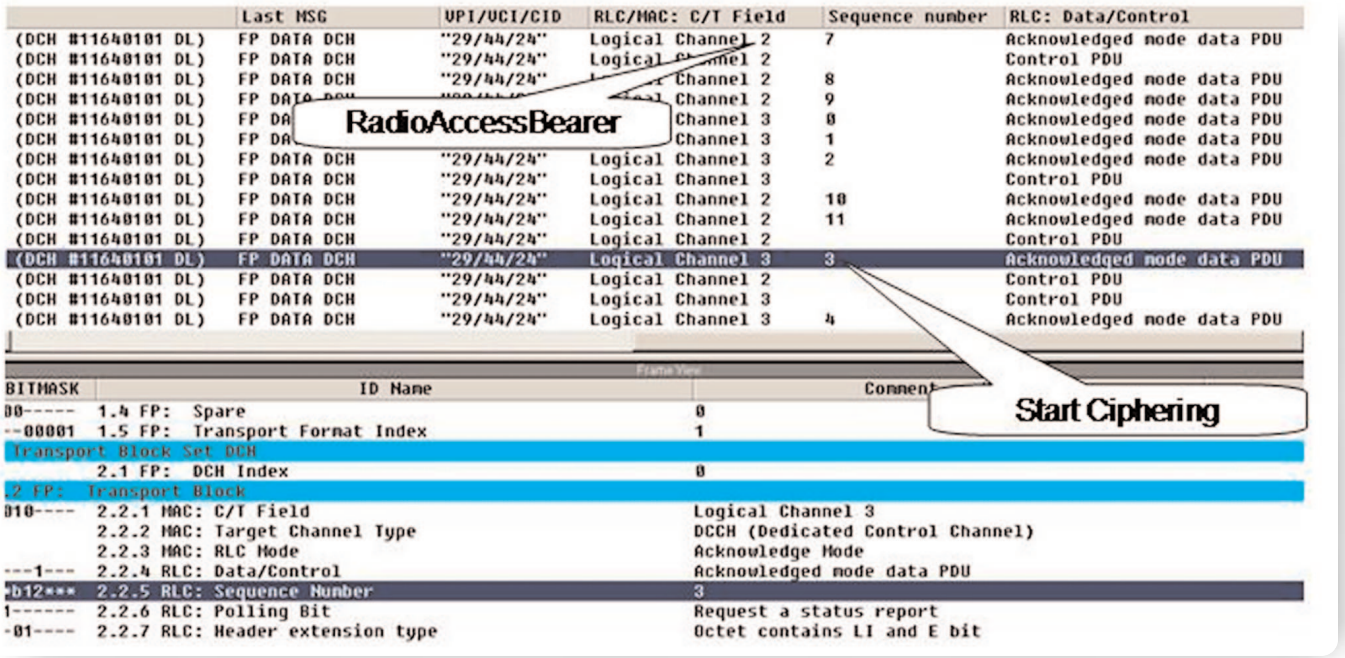
Integrity Initiation - Security Mode Setup Procedure

The VLR/SGSN initiates integrity protection (and encryption) by sending the RANAP message security mode control to the SRNC. This message contains a list of allowed integrity algorithms and the IK to be used. Since the UE can have two ciphering and integrity key sets (for the PS and CS domains, respectively), the network includes a Core Network type indicator in the security mode command message.

The security mode command to UE starts the downlink integrity protection, i.e. all subsequent downlink messages sent to the UE are integrity protected. The security mode complete from UE starts the uplink integrity protection, i.e. all subsequent messages sent from the UE are integrity protected. The network must have the "UE security capability" information before the integrity protection can start, i.e. the "UE security capability" must be sent to the network in an UMTS security – integrity protection unprotected message. Returning the "UE security capability" to the UE in a protected message later will allow UE to verify that it was the correct "UE security capability" that reached the network.



▶ **Figure 16.** *Ciphering activation procedure.*



▶ **Figure 17.** *RLC: Ciphering Activation Time.*

Some messages do not include integrity protection, these messages are:

– HANDOVER TO UTRAN COMPLETE

– PAGING TYPE 1

– PUSCH CAPACITY REQUEST

– PHYSICAL SHARED CHANNEL ALLOCATION

– RRC CONNECTION REQUEST

– RRC CONNECTION SETUP

– RRC CONNECTION SETUP COMPLETE

– RRC CONNECTION REJECT

– RRC CONNECTION RELEASE (CCCH only)

– SYSTEM INFORMATION (BROADCAST INFORMATION)

– SYSTEM INFORMATION CHANGE INDICATION

– TRANSPORT FORMAT COMBINATION CONTROL (TM DCCH only)

Key lifetime

To avoid attacks using compromised keys, a mechanism is needed to ensure that a particular integrity key set is not used for an unlimited period of time. Each time an RRC connection is released, the values STARTcs and STARTps of the bearers that were protected in that RRC connection are stored in the USIM. When the next RRC connection is established these values are read from the USIM.

The operator shall decide on a maximum value for STARTCS and STARTPS. This value is stored in the USIM. When the maximum value has been reached, the cipher key and integrity key stored on USIM shall be deleted, and the ME shall trigger the generation of a new access link key set (a cipher key and integrity key) at the next RRC connection request message.

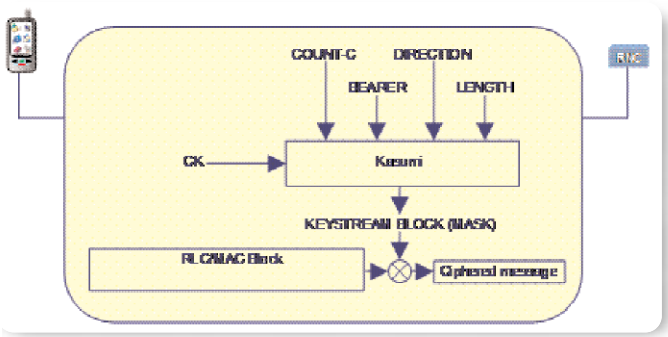
Weaknesses

The main weaknesses in UMTS integrity protection mechanisms are:

– Integrity keys used between UE and RNC generated in VLR/SGSN are transmitted unencrypted to the RNC (and sometimes between RNCs)

– Integrity of user data is not offered

– For a short time during signalling procedures, signalling data are unprotected and hence exposed to tampering.



▶ **Figure 18.** *RLC/MAC Encryption.*

Confidentiality - Encryption (Ciphering) on Uu and Iub

Threats Against Confidentiality

There are several different threats against confidentiality-protected data in UMTS. The most important threats are:

– **Eavesdropping** on user traffic, signalling or control data on the radio interface.

– **Passive traffic analysis**: Intruders may observe the time, rate, length, sources or destinations of messages on the radio interface to obtain access to information.

– **Confidentiality of authentication data in the UICC/USIM**: Intruders may obtain access to authentication data stored by the service provider in the UICC/USIM.

The radio interface is the easiest interface to eavesdrop, and should therefore always be encrypted. If there is a penetration of the cryptographic mechanism, the confidential data would be accessible on any interface between the UE and the RNC. Passive traffic analysis is considered as a major threat. Initiating a call and observing the response, active traffic analysis,

is not considered as a major threat. Disclosure of important authentication data in the USIM, as i.e., the long-term secret K, is considered a major threat. The risk of eavesdropping on the links between RNCs and the UICC-terminal interface is not considered a major threat, since these links are less accessible for intruders than the radio access link.

Eavesdropping of signalling or control data, however, may be used to access security management data or other information, which may be useful in conducting active attacks on the system.

Ciphering Procedure

Ciphering in UMTS is performed between UE and RNC over Air and Iub-Interface. The Figure 15 shows the protocol stack of the Iub-Interface for R99.

The Iub protocol stack contains a Radio Network Control Plane, a Transport Network Control Plane and a User Plane for AMR coded voice, IP packages, video streaming, etc. The Radio Network Control Plane is spitted into two parts, the non-access stratum (NAS) and the Node-B application part (NBAP). The non-access stratum contains mobility management (MM), session management (SM) and call control management (CC) for communication between UE and core network.

Before UE and RNC are able to exchange NAS messages and user data, one or more transport channel is required. All information related to the establishment, modification and release of transport channels are exchanged between RNC and Node-B over NBAP and ALCAP. Transport channels are based on AAL2 connections (Figure 15). The concept of those transport channels is very important for the understanding of ciphering and integrity protection.

Task of the transport channel is an optimal propagation of signaling information and user data over the air interface. In order to do so, a transport channel is composed of several Radio Access Bearers (RAB). The characteristic of every Radio Access Bearer is defined during establishment by the NBAP layer. This is done by a list of attributes, so called Transport Format Set (TFS). The Transport Format Set describes the way of data transmission using different parameters, like block size, transmission time interval (TTI), and channel coding type.

The UTRAN selects for the communication between mobile and network these Radio Access Bearers, which use the radio resources in the most efficient way. Every RAB has its own identifier and every transport block has its own sequence number. This technique allows from one side a fast switch-over between Radio Bearers and from the other one a parallel communication over several Radio Access Bearers. This technique requires a bearer-independent ciphering mechanism.

Ciphering will be activated with the messages flow shown in Figure 16. Ciphering is always related to a certain transport channel. Therefore ciphering will be activated independently for Control and User Plane and independently for packet-switched and circuit-switched plane. In other words, if a mobile subscriber has two independent sessions (voice calls and IP packet transfer) activated, UE and RNC need to exchange the ciphering activation procedure two times. Important to note that NAS messages exchanged prior ciphering activation (typically the Authentication procedure) are not ciphered.

Message securityModeCommand establishes the Activation Time for the Radio Access Bearers in downlink direction and the message securityModeComplete determines the Activation Time in uplink direction. Ciphering for a certain RAB starts for that RLC block where Sequence Number is equal to Activation Time (Figure 17).

The ciphering depth depends on the RLC mode. The RLC protocol contains Control PDU's (never ciphered) and Data PDU's. For Data PDU's, the RLC protocol works in three different modes:

– UM Unacknowledged Mode

– AM Acknowledged Mode

– TM Transparent Mode

UM and AM messages (e.g., Data) are secured against bit errors with a check sequence, while TM information (e.g., AMR voice) aren't. Therefore RLC UM and RLC AM are ciphered beginning with RLC layer and above, while ciphering for RLC TM already starts with the MAC layer.

The KASUMI algorithm itself needs the following parameters (Figure 18):

– Cipher Sequence Number COUNT

– Direction (uplink or downlink)

– Radio Access Bearer Identifier

– Block Length

– Ciphering Key CK

CK is never sent over the Uu and Iub-Interface. The RNC receives this value from MSC or SGSN and the USIM calculates CK as described before.

COUNT is initially derived from the START value of the rrcConnectionSetupComplete message. The START value is not constant during a ciphering session. It can be modified by different procedures, like Cell Reselection or Channel Type Switching. The following messages can trigger an update of the COUNT value:

– rrcConnectionSetupComplete

– physicalChannelReconfigurationComplete

– transportChannelReconfigurationComplete

– radioBearerSetupComplete

– radioBearerReconfigurationComplete

– radioBearerReleaseComplete

– utranMobilityInformationComplete

– initialDirectTransfer

If the message securityModeFailure is received the ciphering information shall be removed from USIM and RNC.

Contact Tektronix:

ASEAN / Australasia / Pakistan (65) 6356 3900
Austria +43 2236 8092 262
Belgium +32 (2) 715 89 70
Brazil & South America 55 (11) 3741-8360
Canada 1 (800) 661-5625
Central Europe & Greece +43 2236 8092 301
Denmark +45 44 850 700
Finland +358 (9) 4783 400
France & North Africa +33 (0) 1 69 86 80 34
Germany +49 (221) 94 77 400
Hong Kong (852) 2585-6688
India (91) 80-22275577
Italy +39 (02) 25086 1
Japan 81 (3) 6714-3010
Mexico, Central America & Caribbean 52 (55) 56666-333
The Netherlands +31 (0) 23 569 5555
Norway +47 22 07 07 00
People's Republic of China 86 (10) 6235 1230
Poland +48 (0) 22 521 53 40
Republic of Korea 82 (2) 528-5299
Russia, CIS & The Baltics +358 (9) 4783 400
South Africa +27 11 254 8360
Spain +34 (91) 372 6055
Sweden +46 8 477 6503/4
Taiwan 886 (2) 2722-9622
United Kingdom & Eire +44 (0) 1344 392400
USA 1 (800) 426-2200
USA (Export Sales) 1 (503) 627-1916
For other areas contact Tektronix, Inc. at: 1 (503) 627-7111
Updated 01 March 2004

For Further Information
Tektronix maintains a comprehensive, constantly expanding collection of application notes, technical briefs and other resources to help engineers working on the cutting edge of technology. Please visit **www.tektronix.com**

05/04 FLG/WWW 2FW-17826-0

Tektronix
Enabling Innovation