3GPP Systems and Services TSG, Security WG
London, 2-4 February, 1999

Tdoc s3-99005
Source: ETSI SMG10

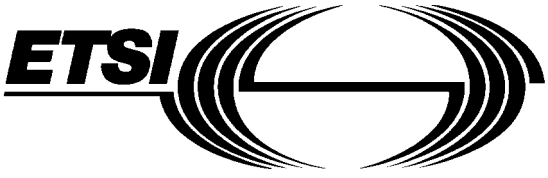
Draft UMTS 33.23 V 0.2.0 (1999-01)

Technical Specification

Special Mobile Group (SMG): Universal Mobile Telecommunications System (UMTS); Security Mechanisms and Architecture (UMTS 33.23, version 0.2.0)

UMTS

Universal Mobile
Telecommunications System



European Telecommunications Standards Institute

Reference
UMTS 33.23

Keywords
Universal Mobile Telecommunications System

ETSI Secretariat

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

X.400
c= fr; a=atlas; p=etsi; s=secretariat

Internet
secretariat@etsi.fr
http://www.etsi.fr

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present specification may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETR 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr or http://www.etsi.org/ipr).

Pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETR 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present specification.

Foreword

This specification has been produced by the Special Mobile Group (SMG) of the European Telecommunications Standards Institute (ETSI).

Introduction

To be drafted by the ETSI secretariat.

1. Scope

This document presents the security architecture and mechanisms (hereafter referred to as the “security architecture”) for UMTS Phase 1. The security architecture provides the security features defined in 33.22 “Security Features” [2], which in turn meet the identified security requirements specified in UMTS 33.21 “Security Requirements” [1].

The structure of this technical specification is as follows:

Clause 2 lists the references used in this specification.

Clause 3 lists the definitions and abbreviations used in this specification.

Clause 4 gives an overview of the security architecture for UMTS.

Clause 3 specifies functions which provide security features at the transport security layer. These include features relating to confidentiality and integrity of user related traffic and signalling in the UTRAN.

Clause 4 specified functions which provide security features at the network security layer. These include features relating to user location and identity confidentiality, authentication and key agreement.

Clause 5 specifies functions which provide support for security features at the application level. Application security does not provide standardised security features as such but instead provides support for the provision of non-standardised security features and services between the USIM and a VASP or HE.

Annex A (Informative) contains the status of UMTS 33.23.

Annex B (Informative) contains ...

Annex C (Informative) contains …

Annex D (Informative) contains …

Annex E (Informative) contains …

2. References

[1] UMTS 33.21: ”Universal Mobile Telecommunications System (UMTS): Security requirements”

[2] UMTS 33.22: ”Universal Mobile Telecommunications System (UMTS): Security features”

3. Definitions and abbreviations

3.1 Definitions

Access Control: The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.

Confidentiality: The property of information that it has not been disclosed to unauthorised parties.

Data integrity: The property of information that it has not been changed by unauthorised parties.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

3.2 Abbreviations

AN	Access Network
AuC	Authentication Centre
CK	Cipher Key
Ffs	For further study
GSM	Global System for Mobile Communications
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMEI	International Mobile Equipment Identity
IMUI	International Mobile User Identity
KSN	Key Sequence Number
MAC	Message Authentication Code
MExE	Mobile Execution Environment
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
PIN	Personal Identification Number
RNC	Radio Network Controller
SAT	SIM Application Toolkit
SIM	Subscriber Identity Module
SN	Serving Network
TMUI	Temporary Mobile User Identity
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
USIM	User Services Identity Module
VASP	Value-Added Service Provider
VLR	Visited Location Register

3.3 Glossary

AUTN	An authentication token to allow the user to authenticate the network and obtain assurance on the freshness of RAND
CK	A cipher key established between the user and the network
IK	An integrity key established between the user and the network
K	A long term authentication and key establishment key

Ka	An anonymity key used to protect the confidentiality of the sequence number against passive attacks
MAC	A message authentication code used as part of the authentication token AUTN
RAND	A random challenge to be sent to the user
RES	A value to be sent by the user in response to RAND
SEQ	A sequence number
Text	An optional text field
XAUTN	An expected authentication token to match AUTN
XMAC	An expected authentication code to match MAC
XRES	An expected value to match RES

4. Overview of security architecture

The security features provided by the security architecture are illustrated in Figure 4.1.

[This diagram needs to be refined as in the ISO layered model. Explanatory text needs to be added]

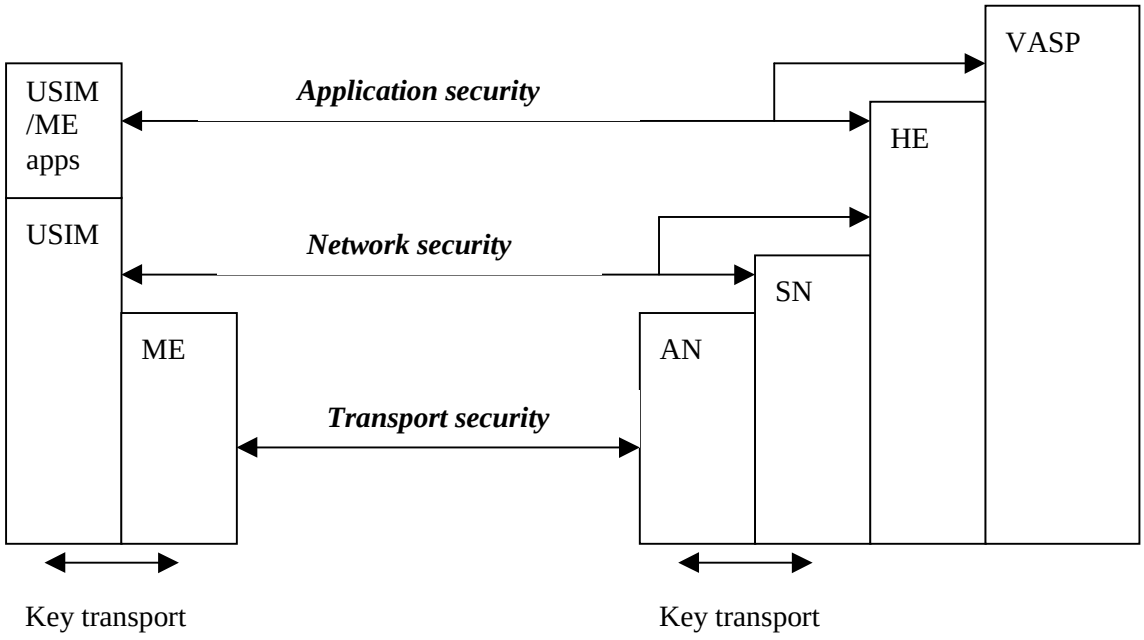


Figure 4.1 - UMTS security architecture

5. Transport security

[Transport security relies on the establishment of integrity and cipher keys between the MS and the network as part of network security features]

5.1 Integrity protection

5.1.1 Overview

Some signalling information elements are considered sensitive and must be integrity protected. An integrity function shall be applied on certain signalling information elements transmitted between the MS and the RNC. It is not an end-to-end integrity service.

5.1.2 The integrity protection method

The UMTS Integrity Algorithm (UIA) shall be implemented in the USIM and in the RNC.

The UIA shall be used with an Integrity Key (IK) to compute a message authentication code for a given message.

The following signalling elements sent by the MS to the RNC should be protected:

a) - The MS capabilities, including authentication mechanism, ciphering and integrity capabilities.

b) - The security mode accept/reject message.

c) - The called party number in a mobile originated call.

d) - Periodic message authentication messages.

The following signalling elements sent by the RNC to the MS should be protected:

e) - The security mode command, including whether ciphering is enabled or not and the ciphering and integrity algorithm to be used.

f) - Periodic message authentication messages.

[The point at which integrity protection is applied in the UTRAN architecture is for further study. At this stage we assume that integrity protection is applied at the RNC but may be applied at the MSC/VLR]

5.1.3 Integrity key setting

Mutual key setting is the procedure that allows the MS and the RNC to agree on the key IK used to compute message authentication codes using algorithm UIA.

Key setting is triggered by the authentication procedure. Key setting may be initiated by the network as often as the network operator wishes.

Key setting can occur as soon as the identity of the mobile subscriber (i.e. TMUI or IMUI) is known by the SN/VLR. The procedures for the management of IK are the authentication procedures described in subclause 6.2

The key IK is stored in the SN/VLR and transferred to the RNC when it is needed.

The key IK is stored in the USIM until it is updated at the next authentication.

5.1.4 Key sequence number

The key sequence number (KSN) is a number which is associated with the cipher and integrity keys derived during authentication. It is stored together with the cipher and integrity keys in the MS and in the network.

5.1.5 Integrity key lifetime

A mechanism is needed to ensure that a particular integrity key is not used for an unlimited period of time, to avoid attacks using compromised keys. Authentication which generates integrity keys is not mandatory at call setup, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. The USIM shall therefore contain a mechanism to limit the number of calls that can be made with a specific integrity key.

Operators shall decide on the value of this number of calls, and write this parameter on the USIM. The USIM shall have a counter that counts the number of times the integrity key is used and shall trigger the generation of a new integrity key if the counter reaches the maximum value set in the USIM[1]. This mechanism will ensure that an integrity key cannot be reused more times than the limit set by the operator.

5.1.6 UIA numbering

[The following table is for illustration only]

Information Element	*Length*	*Value*	*Remark*
UEA Number	4	0000_2	Standard UMTS Integrity Algorithm, UEA1
		0001_2	Standard UMTS Integrity Algorithm, UEA2
		0010_2	Standard UMTS Integrity Algorithm, UEA3
		0011_2 to 0111_2	Reserved for future expansion
		$1xxx_2$	Proprietary UMTS Algorithms

Table 5.1 - UIA numbering

5.1.7 UIA negotiation

Not more than [n] versions of the UIA algorithm will be defined.

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM classmark which version of the UIA algorithm the USIM supports.

[This message itself must be integrity protected itself which effectively means that there must be at least one UIA algorithm in common, otherwise the connection is released]

The network shall compare its integrity protection capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the UIA algorithm in common, then the connection shall be released.

2) If the MS and the network have at least one version of the UIA algorithm in common, then the network shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection.

3) If the MS and the network have no versions of the UIA algorithm in common and the network is willing to use an unprotected connection, then an unprotected connection shall be used.

5.1.8 Integrity protection procedures

[The integrity protection procedures are for further study]

---

[1] *Which message should be chosen as a parameter? Using this would register call attempts as well as calls...*

5.1.8.1 Handover

When a handover occurs, the IK is transmitted within the system infrastructure from the old RNC to the new one to enable the communication to proceed. The key IK remains unchanged at handover.

5.2 Confidentiality protection

5.2.1 Overview

Some signalling information elements are considered sensitive and must be confidentiality protected. To ensure identity confidentiality (see clause 6.1), the Temporary Mobile User Identity must be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it. The confidentiality of user information concerns the information transmitted on traffic channels

These needs for a protected mode of transmission are fulfilled by a confidentiality function which is applied on dedicated channels between the MS and the RNC. It is not an end-to-end confidentiality service.

5.2.2 The ciphering method

Algorithm UEA is implemented in both the MS and the RNC. On the RNC side the description below assumes that one algorithm UEA is implemented for each dedicated physical channel. The data flow on dedicated channels is ciphered by a bit per bit or stream cipher generated by an algorithm UEA.

The UEA shall produce one output as a sequence of keystream bits referred to as a Key Stream Segment (KSS). A KSS of length n shall be produced to encrypt a given segment of plaintext of length n. The bits of KSS are labelled KSS(0), …KSS(n-1), where KSS(0) is the first bit output from the generator. The bits in the KSS shall be used to encrypt or decrypt the data.

[The point at which confidentiality protection is applied in the UTRAN architecture is for further study. At this stage we assume that confidentiality protection is applied at the RNC]

5.2.3 Cipher key setting

Mutual key setting is the procedure that allows the MS and the RNC to agree on the key CK to use in the ciphering and deciphering algorithms UEA.

Key setting is triggered by the authentication procedure. Key setting may be initiated by the network as often as the network operator wishes.

Key setting must occur on a dedicated channel not yet encrypted and as soon as the identity of the mobile subscriber (i.e. TMUI or IMUI) is known by the SN/VLR. The procedures for the management of CK are the authentication procedures described in subclauses 6.2.

The key CK is stored in the SN/VLR and transferred to the RNC when it is needed.

The key CK is stored by the MS until it is updated at the next authentication.

5.2.4 Key sequence number

The key sequence number (KSN) is a number which is associated with the cipher and integrity keys derived during authentication. It is stored together with the cipher and integrity keys in the MS and in the network.

5.2.5 Cipher key lifetime

A mechanism is needed to ensure that a particular cipher key is not used for an unlimited period of time, to avoid attacks using compromised keys. Authentication which generates cipher keys is not mandatory at call setup, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. The USIM shall therefore contain a mechanism to limit the number of calls that can be made with a specific cipher key.

Operators shall decide on the value of this number of calls, and write this parameter on the USIM. The USIM shall have a counter that counts the number of times the cipher key is used and shall trigger the generation of a new cipher key if the counter reaches the maximum value set in the USIM[2]. This mechanism will ensure that an cipher key cannot be reused more times than the limit set by the operator.

5.2.6 UEA numbering

[The following table is for illustration only]

Information Element	Length	Value	Remark
UEA Number	4	0000_2	Standard UMTS Encryption Algorithm, UEA1
		0001_2	Standard UMTS Encryption Algorithm, UEA2
		0010_2	Standard UMTS Encryption Algorithm, UEA3
		0011_2 to 0111_2	Reserved for future expansion
		$1xxx_2$	Proprietary UMTS Algorithms

Table 5.2 – UEA numbering

5.2.7 UEA negotiation

Not more than [n] versions of the UEA algorithm will be defined.

When an MS wishes to establish a connection with the network, the MS shall indicate to the network which version of the UEA algorithm it supports.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the UEA algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.

2) If the MS and the network have at least one version of the UEA algorithm in common, then the network shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection.

3) If the MS and the network have no versions of the UEA algorithm in common and the network is willing to use an unciphered connection, then an unciphered connection shall be used.

5.2.8 Ciphering procedures

5.2.8.1 Starting of the ciphering and deciphering processes

The MS and the RNC must co-ordinate the instants at which the enciphering and deciphering processes start.

This procedure takes place under the control of the network some time after the completion of the authentication procedure (if any), or after the key CK has been made available at the RNC.

No information elements for which protection is needed must be sent before the ciphering and deciphering processes are operating.

---

[2] *Which message should be chosen as a parameter? Using this would register call attempts as well as calls...*

The transition from clear text mode to ciphered mode proceeds as follows: deciphering starts in the RNC, which sends in clear text to the MS a specific message, here called “Start cipher”. Both the enciphering and deciphering start on the MS side after the message “Start cipher” has been correctly received by the MS. Finally, enciphering on the RNC side starts as soon as a frame or a message from the MS has been correctly deciphered at the RNC.

[diagram to be added]

5.2.8.2 Synchronisation

The enciphering stream at one end and the deciphering stream at the other end must be synchronised, for the enciphering bit stream and the deciphering bit streams to coincide.

Synchronisation is guarantied by driving UEA by an explicit time variable, COUNT, derived from an appropriate frame number available at the MS and at the RNC.

The diagram below summarises the implementation indications listed above, with only one enciphering/deciphering procedure represented (the second one for deciphering/enciphering is symmetrical).

[diagram to be added]

5.2.8.3 Handover

When a handover occurs, the CK is transmitted within the system infrastructure from the old RNC to the new one to enable the communication to proceed, and the synchronisation procedure is resumed. The key CK remains unchanged at handover.

6. Network security

6.1 User identity and location confidentiality

[This mechanism is essentially the one used in GSM. Further study is required into whether separate procedures are required for circuit switched (MSC) and packet switched (SGSN) core networks.]

[Further study may be required into what this service feature is really providing and why it is needed? Is it undermined by a IMUI catcher? Will the existence of this feature encourage the development of an IMUI catcher?]

6.1.1 Overview

The purpose of this function is to avoid the possibility for an intruder to identify which user is using a given resource on the radio path by listening to the signalling exchanges on the radio path. This allows both a high level of confidentiality for user data and signalling and protection against the tracing of a user's location.

The provision of this function implies that the IMUI (International Mobile User Identity), or any information allowing a listener to derive the IMUI easily, should not normally be transmitted in clear text in any signalling message on the radio path.

Consequently, to obtain the required level of protection, it is necessary that:

- a protected identifying method is normally used instead of the IMUI on the radio path; and
- the IMUI is not normally used as addressing means on the radio path;
- when the signalling procedures permit it, signalling information elements that convey information about the mobile subscriber identity must be ciphered for transmission on the radio path.

The identifying method is specified in the following subclause. The ciphering of communication over the radio path is specified in clause 5.2.

6.1.2 Identifying method

The means used to identify a mobile user on the radio path consists of a TMUI (Temporary Mobile User Identity). This TMUI is a local number, having a meaning only in a given location area; the TMUI must be accompanied by the LAI (Location Area Identification) to avoid ambiguities. The maximum length and guidance for defining the format of a TMUI are specified in [same specification as other UMTS identities].

The SN manages suitable databases to keep the relation between TMUIs and IMUIs. When a TMUI is received with an LAI that does not correspond to the current VLR, the IMUI of the MS must be requested from the VLR in charge of the indicated location area if its address is known; otherwise the IMUI is requested from the MS.

A new TMUI must be allocated at least in each location updating procedure. The allocation of a new TMUI corresponds implicitly for the MS to the de-allocation of the previous one. In the SN, the cancellation of the record for an MS in a VLR implies the de-allocation of the corresponding TMUI.

To cope with some malfunctioning, e.g. arising from a software failure, the fixed part of the network can require the identification of the MS in clear. This procedure is a breach in the provision of the service, and should be used only when necessary.

When a new TMUI is allocated to an MS, it is transmitted to the MS in a ciphered mode. This ciphered mode is defined in clause 5.2.

The USIM must store its current TMUI in a non volatile memory, together with the LAI, so that these data are not lost when the MS is switched off.

6.1.3 General procedure for location updating in the same MSC area

The general procedure is described. Procedures which deviate from the general case are described in Annex B.

The general procedure is part of the location updating procedure which takes place when the original location area and the new location area depend on the same MSC. The part of this procedure relative to TMUI management is reduced to a TMUI re-allocation (from TMUIo with “o” for “old” to TMUIn with “n” for “new”).

The MS sends TMUIo as an identifying field at the beginning of the location updating procedure.

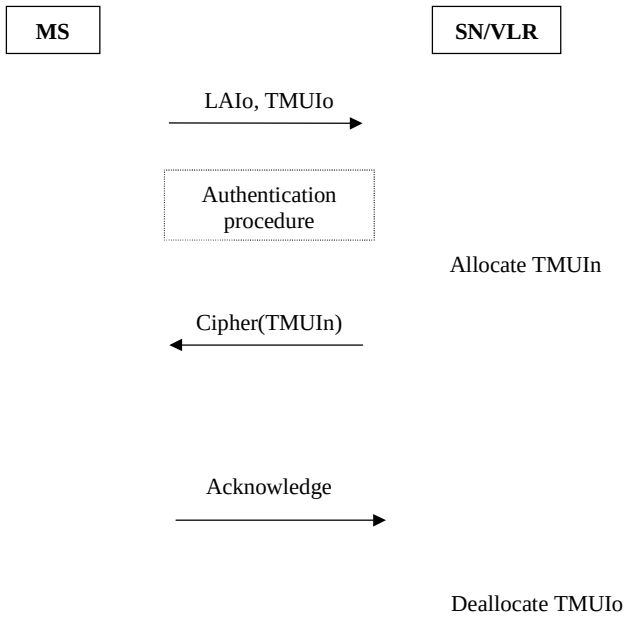


Figure 6.1 - Location updating in the same MSC area

Signalling Functionalities:

Management of means for new ciphering:

The MS and SN/VLR agree on means for ciphering signalling information elements, in particular to transmit TMUIn.

6.2 Authentication and key establishment (SEQ protocol)

[This is essentially the GSM protocol combined with a sequence number-based one-pass protocol for network authentication derived from the ISO standard ISO/IEC 9798-4. An alternative mechanism is included in Annex D]

6.2.1 Overview

The authentication and key establishment method described is of symmetric secret key type. In this method one secret, the authentication and key establishment key, K, shall be shared by each of the authenticating parties, and there should be strictly two parties with knowledge of the secret. Authentication shall be achieved by the parties proving to each other knowledge of the shared secret.

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 two-pass challenge-response protocol identical to the GSM user authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication derived from the ISO standard ISO/IEC 9798-4 (section 5.1.1).

The authenticating parties shall be the Authentication Centre of the Home Environment (HE/AuC) and the user, defined by the IMUI and represented by the USIM. Authentication and key establishment consists of two procedures: First, authentication information is distributed to the Visiting Location Register in the Serving Network (SN/VLR) by the HE/AuC. Second, an authentication exchange is run between the user and the SN/VLR based on that authentication information. These procedures are discussed in more detail in the following subclauses.

The SN/VLR is assumed to be trusted by the Home Environment to handle this authentication information securely. It is also assumed that the intra-system interfaces linking the SN/VLR to the HE/AuC, and linking SN/VLRs, are adequately secure. Mechanisms to secure these links are described in clause 6.4. It is further assumed that the user trusts the HE.

The authentication key K is allocated together with the IMUI, when the USIM is issued. K is stored on the network side in the HE/AuC. An HE may contain one or more AuCs.

In order to control the use of sequence numbers, counters SEQ-US and SEQ-HE need to be maintained by the USIM and by the HE/AuC respectively. In the general case, there is one counter SEQ-HE for each user. The use of these counters is explained below.

Figure 4.1 provides an overview of the authentication and key establishment method. Detailed definitions can be found in the subsections 6.2.2 and 6.2.3 below. Figure 4.1 shows that, after receiving an authentication information request, the HE/AuC generates an ordered array of n authentication vectors. Each authentication vector consists of five components (and hence may be called a UMTS “quintuplet” in analogy to GSM “triplets”): A random number RAND, an expected response XRES, a cipher key CK, an integrity IK and an authentication token AUTN. This array of n authentication vectors is then sent from HE/AuC to SN/VLR. It is good for n authentication exchanges between the SN/VLR and the USIM. In an authentication exchange the SN/VLR first selects the next (the i-th) authentication vector from the array and sends the parameters RAND(i) and AUTN(i) to the user. The USIM checks whether AUTN(i) can be accepted and, if so, produces a response RES(i) which is sent back to the SN/VLR. The USIM also computes CK(i) and IK(i). The SN/VLR compares the received RES(i) with XRES(i). If they match SN/VLR considers the authentication exchange to be successfully completed. The established keys CK(i) and IK(i) will then be transferred by the USIM and the SN/VLR to the entities which perform ciphering and integrity functions (cf. section 5).

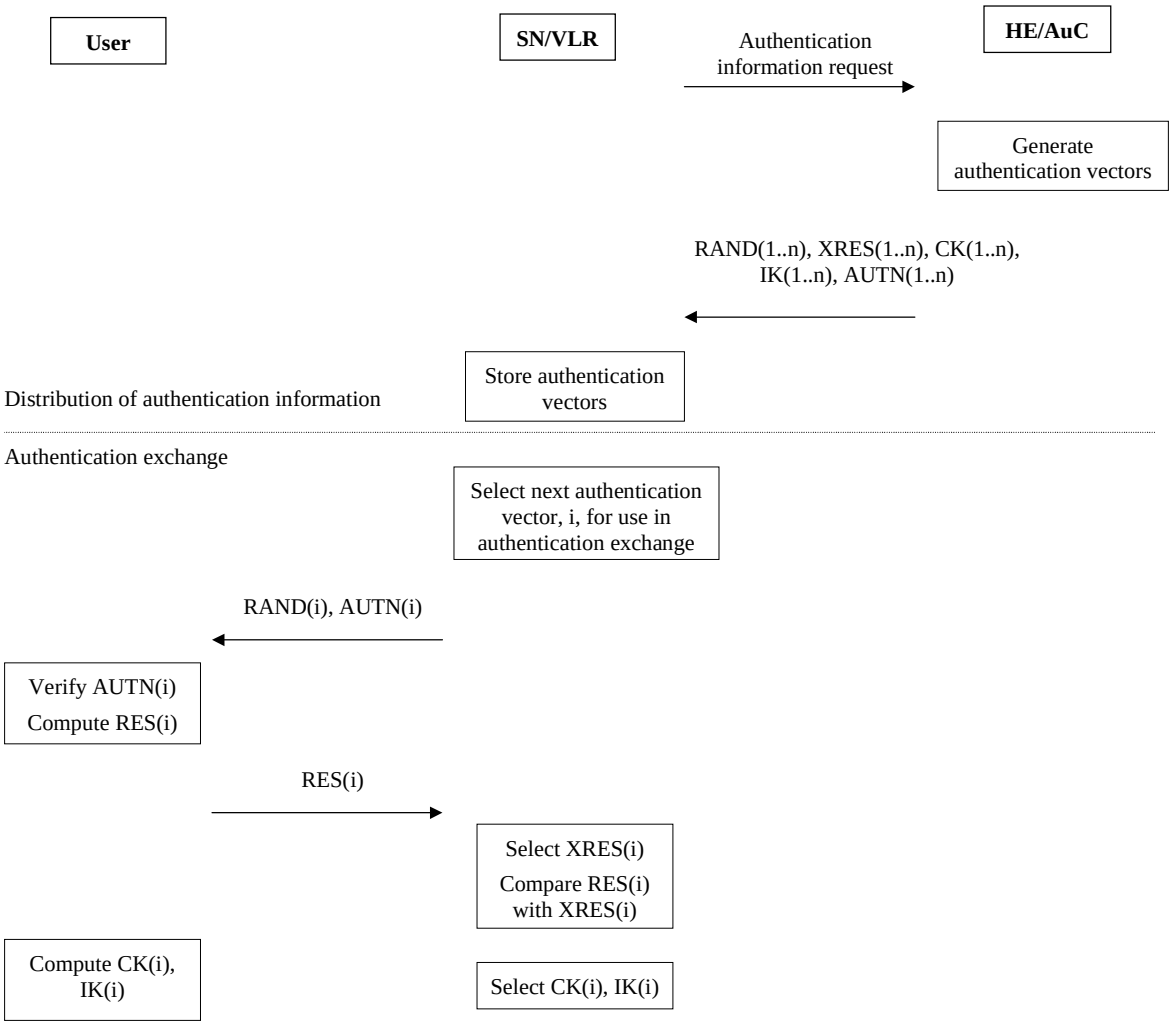


Figure 6.2 Overview of authentication and key establishment method

The presented protocol is valid under the general assumptions stated. Under certain additional assumptions simplifications of the above protocol are possible. These will be discussed in the notes in subsection 6.2.3 further below.

6.2.2 General procedure for distributing authentication vectors (“quintuplets”) to the SN/VLR

The general procedure is described. Procedures which deviate from the general case are described in Annex C.

When needed for each user, the SN/VLR sends a request for authentication information to the HE/AuC corresponding to the user. The HE/AuC generates n random challenges RAND(1..n) and n consecutive sequence numbers SEQ(1..n) from the appropriate HE/AuC counter, starting with SEQ(1) = SEQ-HE+1. The counter SEQ-HE is then reset to SEQ(n). An optional text field Text(i) to be integrity protected and sent to the user may also be generated. These parameters are used to generate an ordered array of authentication parameters as follows:

AUTN(i) = $SEQ(i) \oplus Ka(i) \parallel Text(i) \parallel f1_K (PAR1 \parallel SEQ(i) \parallel RAND(i) \parallel Text(i))$

where f1 is a MAC function.

$XRES(i) = f2_K (PAR2 \parallel RAND(i))$ where f2 is a (possibly truncated) MAC function.

$CK(i) = f3_K (PAR3 \parallel RAND(i))$ where f3 is a key generating function.

$IK(i) = f4_K (PAR4 \parallel RAND(i))$ where f4 is a key generating function.

$Ka(i) = f5_K (PAR5 \parallel RAND(i))$ where f5 is a key generating function.

Here, Ka(i) is an “anonymity” key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only.

The need for f5 to use a long-term key different from K is ffs.

The requirements on f3, f4 and f5 are ffs. It is also ffs in how far the functions f1, ..., f5 need to differ and how they may be suitably combined.

PAR1, ..., PAR5 are different fixed initial values which may be used when similar or identical functions are used for f1, ..., f5. The need for the inclusion of PAR1, ... PAR5 is ffs. When omitted they may be thought of as being integrated in the definition of the functions f1, ..., f5 respectively.

These authentication parameters are used to construct an ordered array of authentication vectors for the user consisting of RAND(i), XRES(i), CK(i), IK(i) and AUTN(i). This array is used by the SN/VLR in an authentication exchange with a user.

.

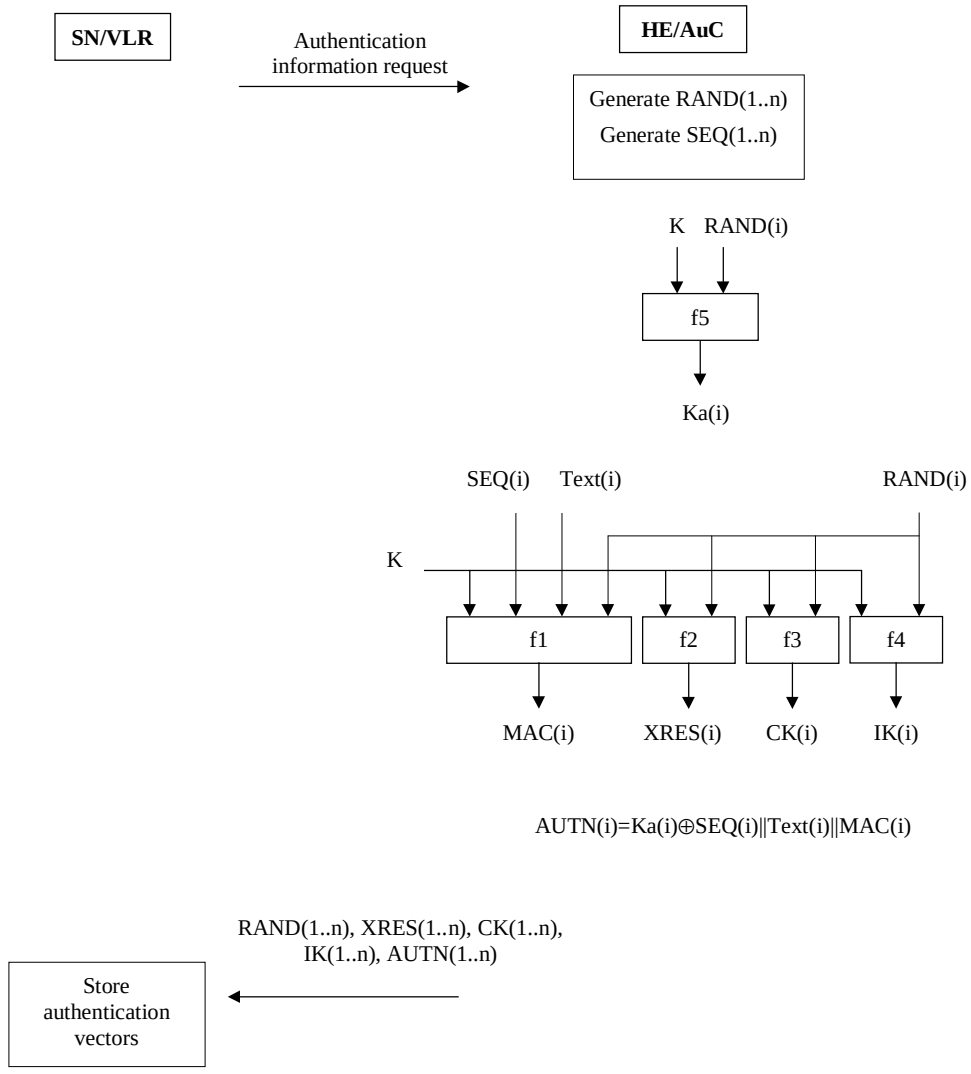


Figure 6.3 - Procedure for distributing authentication vectors from the HE/AuC to the SN/VLR

6.2.3 The authentication exchange

When the SN/VLR performs an authentication, it uses an ordered array of authentication vectors, corresponding to the user.

To authenticate a user, the SN/VLR selects the next vector i from the ordered array of authentication vectors corresponding to the user. The SN/VLR sends to the user the random challenge RAND(i) and an authentication token for network authentication AUTN(i) from the selected authentication vector.

When the user receives RAND(i) and AUTN(i) it first verifies AUTN(i) as follows:

The USIM first computes Ka(i) from RAND(i) and K using the function f5. It then computes SEQ(i) from SEQ(i)⊕Ka(i) and Ka(i). Next the USIM computes XMAC(i) = $f1_K$ (PAR1 || SEQ(i) || RAND(i) || Text(i)) from the available parameters and compares it with the received value. If there is a match and if SEQ(i) is greater than the current value of the counter SEQ-US, the counter SEQ-US is set to SEQ(i). Otherwise, the authentication procedure is aborted indicating the cause of failure to the SN.

The user then computes RES(i), CK(i) and IK(i) from PAR2 (PAR3, PAR4 respectively), RAND(i) and K using the function f2 (f3, f4 respectively). If this is more efficient, RES(i), CK(i) and IK(i) could also be computed earlier at any time after receiving RAND(i).

The user sends the response RES(i) to the SN/VLR. The SN/VLR verifies RES(i) by checking it against the expected response XRES(i) from the selected authentication vector. If XRES1(i) equals RES1(i) then the authentication of the user has passed. The SN/VLR also selects the appropriate derived cipher key CK(i) and derived integrity key IK(i) from the selected authentication vector.

The authentication exchange is described in Figure 6.4.

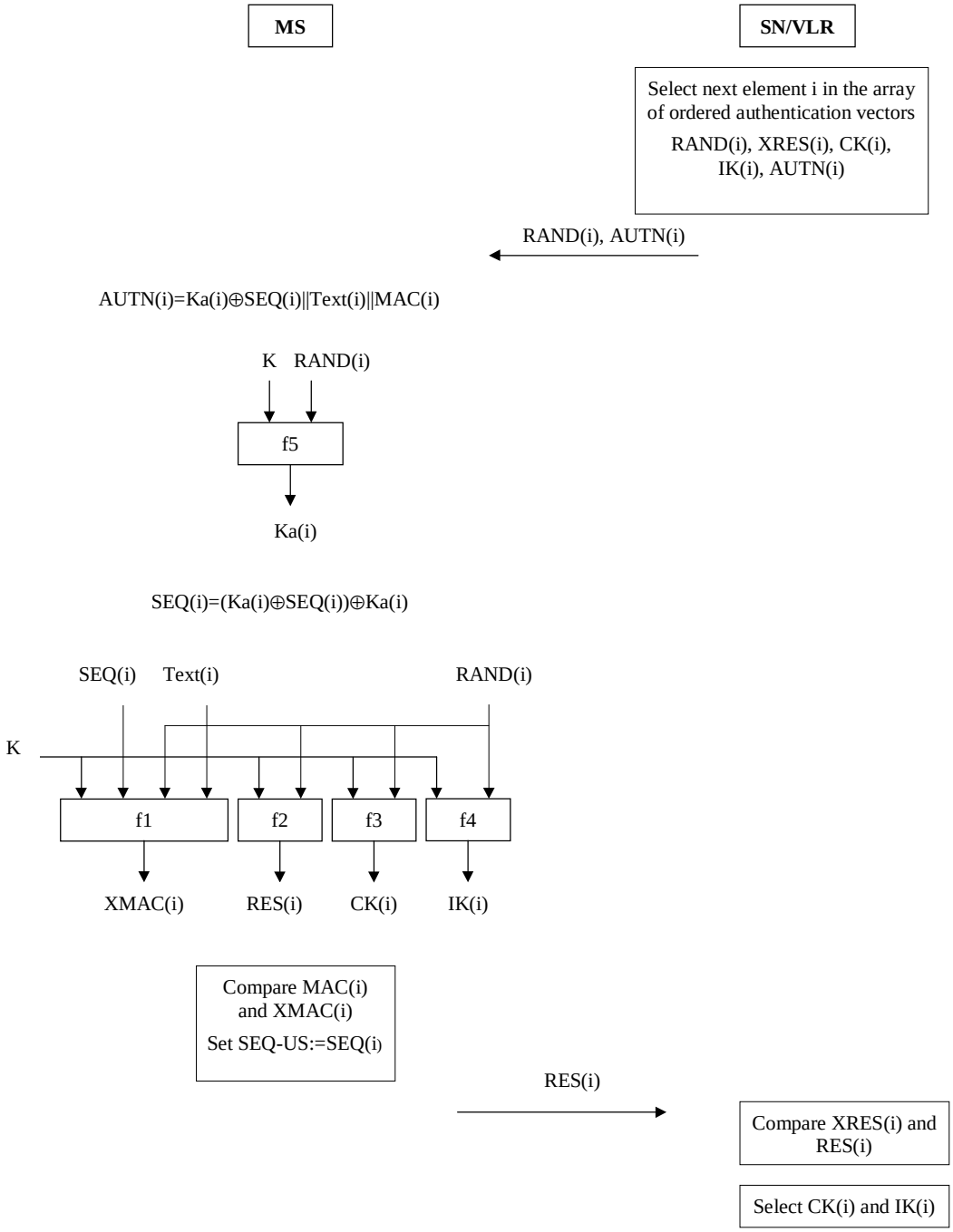


Figure 6.4 - Overview of authentication exchange

Notes:

1) It is ffs whether the HE/AuC has to maintain separate counters SEQ-HE for each user, or whether the generation of sequence numbers as part of the generation of authentication vectors can be based on a global counter. This global counter may in turn be based on a clock with an appropriate granularity giving e.g. Universal Time Co-ordinates (UTC). It should be remembered in this context that sequence numbers have to be unique only on a per user basis, not across all users. This is important to determine the required granularity of the clock.

2) If sequence numbers are derived from a global counter the information which can be derived from a sequence number on the identity of a user may be considered not a serious threat to the anonymity of the user. (If authentication vectors are generated in arrays using consecutive sequence numbers chaining of authentication attempts pertaining to the same user may still be possible.) If the residual threat to the user's anonymity is deemed negligible then the use of the anonymity key Ka to conceal the sequence number is no longer needed.

3) If Ka was no longer needed in order to conceal the sequence number then it could be considered to replace RAND with SEQ. It was decided, however, to keep RAND for maximum compatibility with GSM.

6.2.4 Conditions on the use of authentication vectors and recovery from failures

6.2.4.1 Conditions on the use of authentication information

Using the procedure described in the previous subsections, an array of authentication vectors will have to be used in the specific order in which they were generated, otherwise the user will reject the authentication attempt. The SN/VLR shall use a quadruplet only once and, hence, shall send out the message RAND(i) || AUTN(i) only once no matter whether the authentication attempt was successful or not. A consequence is that authentication vectors cannot be reused. (Note: Re-use of authentication vectors is an insecure practice anyway.)

The procedure described in the previous subsections can be generalised, however, to take advantage of the fact that it has to be only guaranteed that a sequence number is used only once, not necessarily that they are used in ascending order. The procedure can be generalised in such a way that not only the greatest sequence number used (the value of SEQ-US), but the m greatest sequence numbers used are explicitly stored on the USIM. (Here, m is a small number.) Introducing this generalised procedure would affect only the USIM. Then unused authentication vectors would be retained by a VLR for a certain period after the user has left the VLR area. If the new VLR does not fetch the authentication vectors from the old VLR, but requests fresh authentication vectors from the HE/AuC the unused authentication vectors in the old VLR could then be used later nevertheless in case the user returns to the old VLR. In case the user frequently switches between VLRs (possibly belonging to different networks) which do not forward authentication information to one another this generalised procedure may improve the efficiency of the use of authentication vectors. The need for such a generalised procedure is ffs.

6.2.4.2 Unavailability of link between SN/VLR and HE/AuC

SN/VLRs 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 explicit authentication exchange using a new authentication vector. This is true because the use of integrity keys is mandatory. It requires in addition that sequence numbers are used with the integrity protected messages in an appropriate fashion. Details are elaborated in the section on integrity protection for signalling messages.

6.2.4.3 Re-synchronisation procedures

In normal operations, as described in the preceding subsections, it should not happen that SEQ(i)<=SEQ-US. (But it could happen in normal operations when the generalised procedure described in the preceding paragraph is used.) If there is a failure and the sequence number is not accepted by the user, re-synchronisation of the sequence number is needed.

At least two possible cases of synchronisation failure may be distinguished:

1. If the user indicates to the SN/VLR that he could verify the message AUTN(i) sent by the SN/VLR, but that SEQ(i)<=SEQ-US - i.e. that there was a replay of RAND(i) || AUTN(i) - then the SN/VLR may determine that there is a synchronisation failure.

2. The value of the counter SEQ-HE is lost due to a database failure in the HE/AuC.

It is ffs whether further cases of synchronisation failure need to be distinguished.

Options for re-synchronisation procedures are described in the following:

1. If the SN/VLR determines there is a synchronisation failure it may simply request new authentication vectors from the HE/AuC.

2. To protect against failures in the HE/AuC, the USIM may store the last RAND(i) || AUTN(i) received, together with SEQ-US = SEQ(i). For re-synchronisation the user may send the stored RAND(i) || AUTN(i) to the HE/AuC. The HE/AuC then verifies AUTN(i). The HE/AuC updates SEQ-HE only when the value of SEQ(i) received is greater than SEQ-HE. In this case, the HE/AuC sets SEQ-HE to SEQ(i).

3. If sequence numbers derived from a global, time-based counter (cf. notes above) are used then for re-synchronisation the counter SEQ-HE will simply be re-synchronised with the global time.

It is ffs whether further options for re-synchronisation procedures need to be specified.

6.2.4.4 Length of sequence numbers

Sequence numbers shall be sufficiently long so that they cannot wrap around during the lifetime of the system.

Consequently, in normal operations neither SEQ-US nor SEQ-HE can wrap around during the lifetime of a USIM. It is ffs whether additional measures against wrap around are required.

6.3 Secure connection establishment

[Further study is required into whether similar procedures are required for packet services]

This procedure shall be followed when an MS initiates a connection establishment, by sending a Setup Indication message (e.g. LOCATION UPDATING REQUEST, CM SERVICE REQUEST, PAGING RESPONSE, CM RE-ESTABLISHMENT REQUEST in GSM).

In order to establish a secure connection without conducting an authentication exchange, key sequence numbers are introduced. The sequence numbers are managed by the network in such a way that a number is sent to the MS during authentication and allocated to the integrity and cipher keys which are derived during that authentication. The MS/USIM stores this number with the integrity and cipher keys, and indicates to the network in the Setup Indication message which sequence number the stored keys have.

If the Setup Indication message indicates that the MS/USIM has a cipher key and integrity key which the SN/VLR also possesses, then it may proceed to establish a secure connection without conducting an authentication exchange. Otherwise it may initiate authentication using the procedures described in subclause 6.2.

The keys and algorithms to be used in establishing a secure connection are then indicated to the MS in the Security Mode Command. This message itself is integrity protected in accordance with the Security Mode indicated in the command using the mechanisms described in subclause 5.1 for integrity protecting signalling information elements.

The MS then checks the integrity of the Security Mode Command. If the check fails then the connection establishment is abandoned. If the check is valid then the MS switches to the indicated Security Mode using the indicated keys and algorithms.

If the Security Mode indicates that subsequent signalling messages and user traffic should be ciphered then the methods described in subclause 5.1 shall be used.

If the Security Mode indicates that subsequent signalling messages and user traffic should be integrity protected then the methods described in sub-clause 5.2 shall be used.

[The full description of Security Modes and the Security Mode Command is for further study]

6.4 Signalling security

The authentication and key agreement scheme assumes that authentication information passed between network nodes in appropriate signalling information elements is adequately protected. This subclause describes mechanisms for establishing secure signalling links between network nodes, in particular between SN/VLRs and HE/AuCs. Such procedures may be incorporated into the roaming agreement establishment process.

[These mechanisms are for further study. Mechanisms are required to allow all SN-HE pairs to establish a secure signalling connection. These mechanisms could be part of the roaming agreement establishment process between operators. In addition to the usual signalling link establishment and testing, the SN-HE pair could agree on algorithms and keys for protecting signalling links.]

7. Application security

[for further study – to include MExE and SAT security]

8. Annex A (Informative): Status of UMTS 33.23

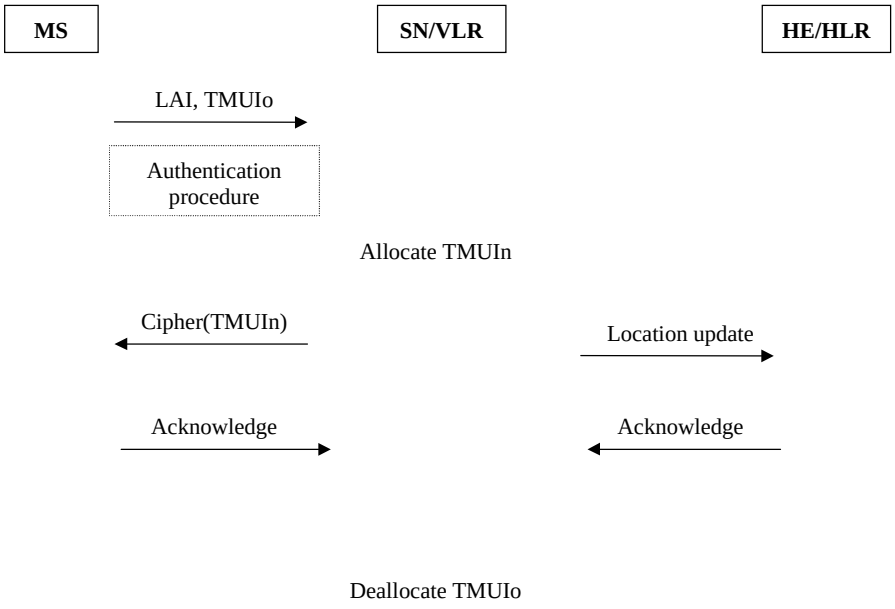
Status of Technical Specification UMTS 33.23 "Security mechanisms and architecture"		
Version	**Date**	**Comments**
v 0.0.1	16 December 1998	Initial version produced at SMG10 WPC #7/98 (Herentals).
v 0.0.2	30 December 1998	Changes based on comments received.
v 0.0.3	15 January 1999	Changes based on comments received.
v 0.2.0	January 1999	Further changes based on decisions made at SMG10 WPC #1/99 (Newbury).
Text and figures: WinWord 7.0 **Stylesheet**: etsiw_70.dot **Rapporteur**:		

9. Annex B (Normative): Procedures for identification and location confidentiality

This subclause presents the procedures, or elements of procedures, pertaining to the management of TMUIs which deviate from the general case.

9.1 Location updating in a new MSCs area, within the same VLR area

This procedure is part of the location updating procedure which takes place when the original location area and the new location area depend on different MSCs, but on the same VLR.



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 9.1 - Location updating in a new MSCs area, within the same VLR area

Signalling functionalities:

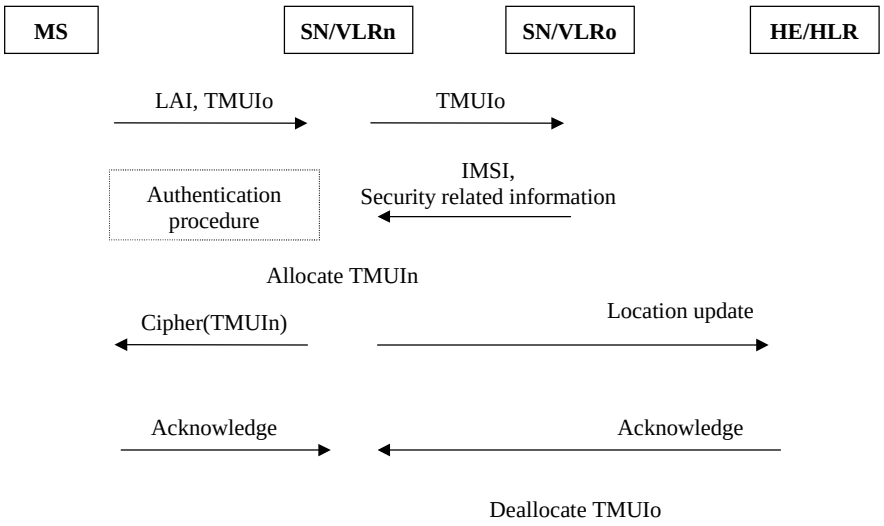
Location Updating

The SN/VLR indicates that the location of the MS must be updated.

9.2 Location updating in a new VLR; old VLR reachable

This procedure is part of the normal location updating procedure, using TMUI and LAI, when the original location area and the new location area depend on different VLRs.

The MS is still registered in VLRo (“o” for old or original) and requests registration in VLRn (“n” for new). LAI and TMUIo are sent by MS as identifying fields during the location updating procedure.



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 9.2 - Location updating in a new VLR; old VLR reachable

Signalling functionalities:

Security Related information

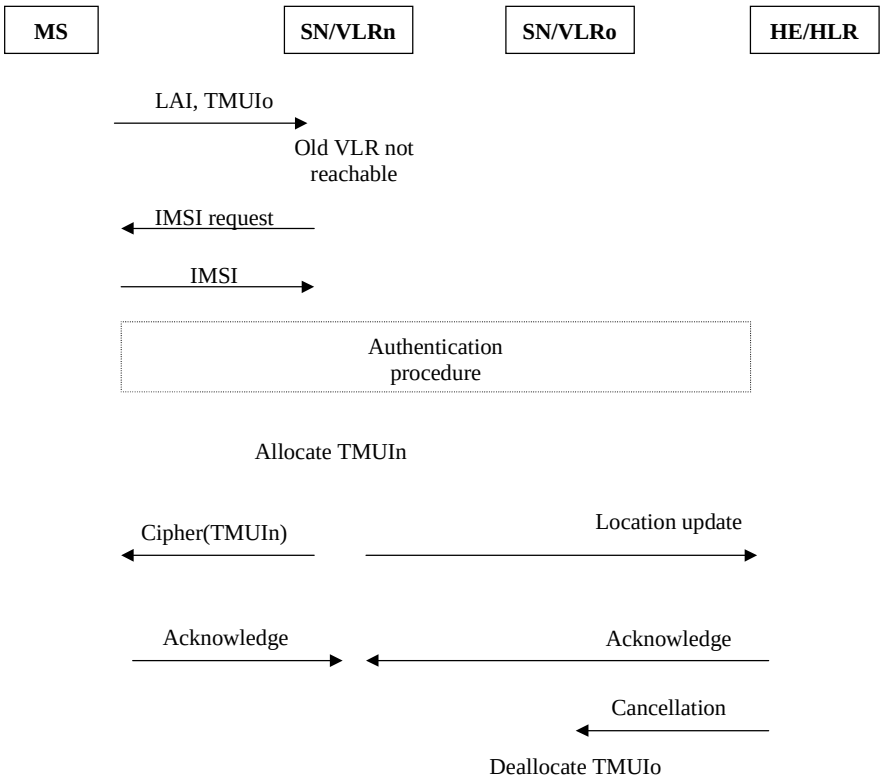
The SN/VLRn needs some information for authentication and ciphering; this information is obtained from SN/VLRo.

Cancellation:

The HLR indicates to VLRo that the MS is now under control of another VLR. The “old” TMUI is free for allocation.

9.3 Location Updating in a new VLR; old VLR not reachable

This variant of the procedure in subclause 9.2 arises when the VLR receiving the LAI and TMUIo cannot identify the VLRo. In that case the relation between TMUIo and IMUI is lost, and the identification of the MS in clear is necessary.



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 9.3 - Location Updating in a new VLR; old VLR not reachable

9.4 Reallocation of a new TMUI

This function can be initiated by the network whenever a radio connection exists. The procedure can be included in other procedures, e.g. through the means of optional parameters. The execution of this function is left to the network operator.

When a new TMUI is allocated to an MS the network must prevent the old TMUI from being allocated again until the MS has acknowledged the allocation of the new TMUI.

[Need to define what happens when an IMUI record in the VLR is deleted by O&M action]

If an IMUI record is deleted in the VLR by O&M action, the network must prevent any TMUI associated with the deleted IMUI record from being allocated again until a new TMUI is successfully allocated to that IMUI.

The case where allocation of a new TMUI is unsuccessful is described in subclause 9.7.

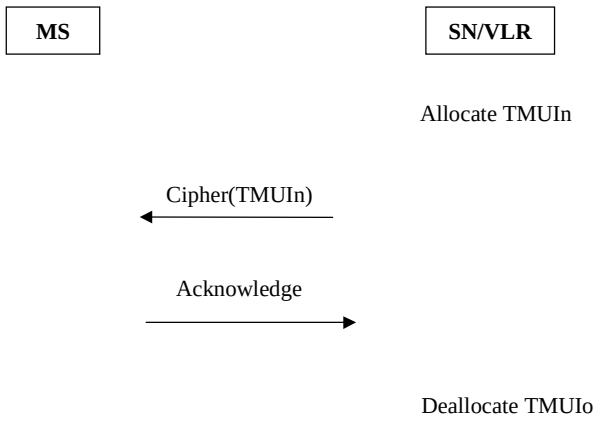
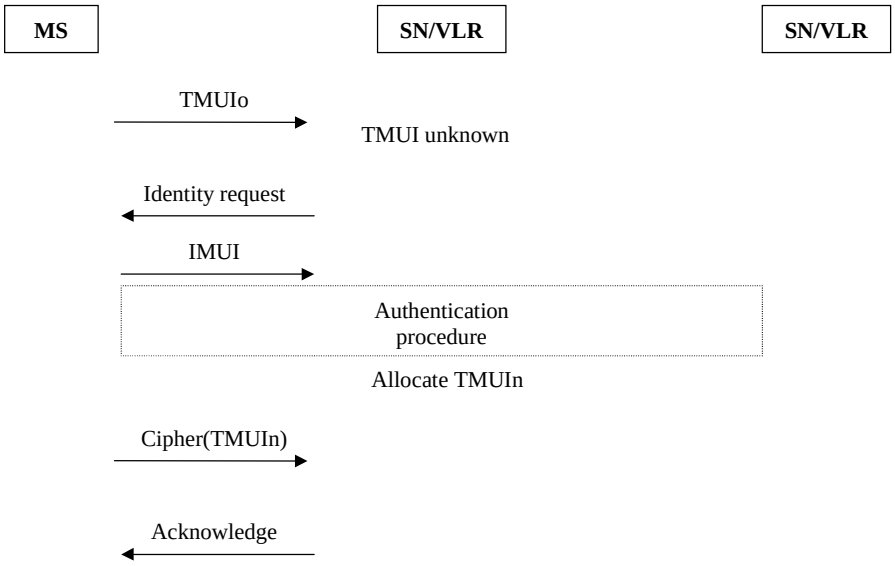


Figure 9.4 - Reallocation of a new TMUI

9.5 Local TMUI unknown

This procedure is a variant of the procedure described in subclauses 2.3.1 and 2.3.2, and happens when a data loss has occurred in a VLR and when a MS uses an unknown TMUI, e.g. for a communication request or for a location updating request in a location area managed by the same VLR.

This procedure is schematised in figure 2.6.

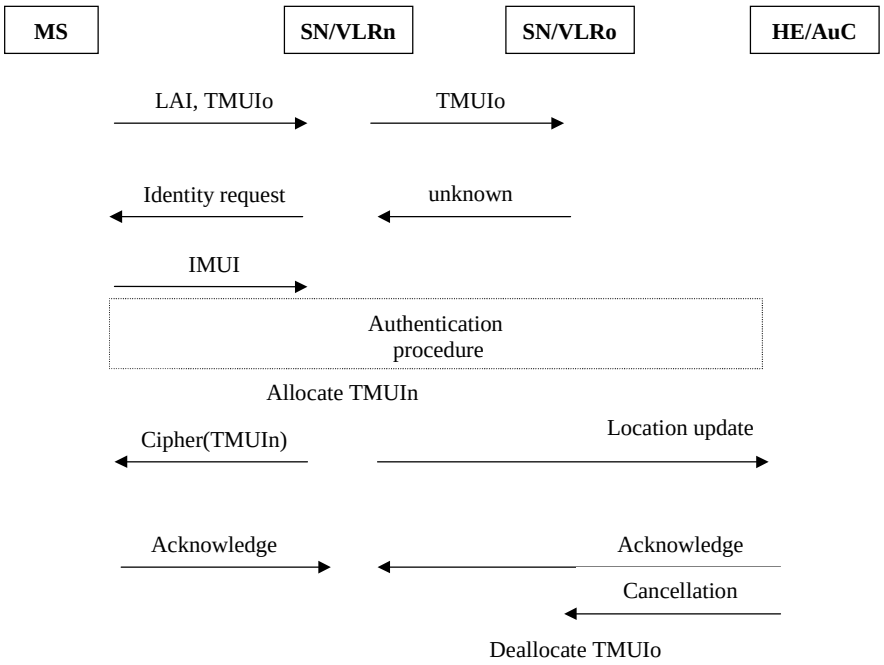


NOTE: Any message in which TMUIo is used as an identifying means in a location area managed by the same VLR.

Figure 9.5 - Location updating in the same MSC area; local TMUI unknown

9.6 Location updating in a new VLR in case of a loss of information

This variant of the procedure described in 9.2 arises when the VLR in charge of the MS has suffered a loss of data. In that case the relation between TMUIo and IMUI is lost, and the identification of the MS in clear is necessary.



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 9.6 - Location updating in a new VLR in case of a loss of information

9.7 Unsuccessful TMUI allocation

If the MS does not acknowledge the allocation of a new TMUI, the network shall maintain the association between the old TMUI and the IMUI and between the new TMUI and the IMUI.

For an MS-originated transaction, the network shall allow the MS to identify itself by either the old TMUI or the new TMUI [does this open up a possible attack?]. This will allow the network to determine the TMUI stored in the MS; the association between the other TMUI and the IMUI shall then be deleted, to allow the unused TMUI to be allocated to another MS.

For a network-originated transaction, the network shall identify the MS by its IMUI. When radio contact has been established, the network shall instruct the MS to delete any stored TMUI. When the MS has acknowledged this instruction, the network shall delete the association between the IMUI of the MS and any TMUI; this will allow the released TMUIs to be allocated to another MS.

In either of the cases above, the network may initiate the normal TMUI reallocation procedure.

Repeated failure of TMUI reallocation (passing a limit set by the operator) may be reported for O&M action.

10. Annex C (Normative): Procedures for distributing authentication vectors (SEQ protocol)

10.1 Authentication vectors obtained from old SN/VLR

[Further study is required into whether this procedure is required. There may be dangers. Network element impersonation attacks should be considered]

During location updating in a new VLR (VLRn), the procedure to obtain authentication information may differ from that described in the general case. In the case when identification is done using a TMUI based identity confidentiality mechanism, authentication information shall be obtained from the old VLR (VLRo) when possible.

The MS identifies itself to the new VLR using a TMUIo previously allocated by the old VLR and the corresponding Location Area Identification (LAI). The new VLR uses this information to find out the address of the old VLR and sends it TMUIo together with an authentication information request.

The old VLR responds with the IMUI corresponding to TMUIo together with the array of unused authentication vectors for that IMUI.

[There may also be a need to request authentication vectors from an old SN/VLR when TMUIs are not used. In this case the MS would have to identify itself using LAIo/IMUI rather than LAIo/TMUIo. Note however that this mechanism does not seem to be provided in GSM.]

11. Annex D (Informative): Alternative authentication and key agreement scheme

11.1 Authentication and key agreement (TETRA REV protocol)

11.1.1 Glossary

CK	A cipher key established between the user and the network
CK1	A cipher key component established between the user and the network (network contribution)
CK2	A cipher key component established between the user and the network (user contribution)
IK	An integrity key established between the user and the network
IK1	An integrity key component established between the user and the network (network contribution)
IK2	An integrity key component established between the user and the network (user contribution)
K	A long term authentication key
RAND1	A random challenge sent to the user
RAND2	A random challenge sent to the network
RES1	A value sent by the user in response to RAND1
RSh	A random seed component from the home environment used to compute temporary authentication keys
RSu	A random seed component from the user used to compute temporary authentication keys
XRES1	An expected value received from the user in response to RAND1

11.1.2 Overview

The authentication and key agreement method described is a symmetric secret key type. In this method one secret, the authentication key, K, shall be shared by each of the authenticating parties, and there should be strictly two parties with knowledge of K. Authentication shall be achieved by the parties proving to each other knowledge of the shared secret.

The authenticating parties shall be the Authentication Centre of the Home Environment (HE/AuC) and the user defined by the IMUI, and represented by the USIM. The authentication exchange proves knowledge of temporary authentication keys KT1 and KT2, given to the Visiting Location Register in the Serving Network (SN/VLR) by the HE/AuC. The SN/VLR is assumed to be trusted by the Home Environment to handle this authentication information securely. It is also assumed that the intra-system interfaces linking the SN/VLR to the HE/AuC are adequately secure. Mechanisms to secure these links are described in clause 6.4.

The authentication key K is allocated together with the IMUI, when the USIM is issued. K is stored on the network side in the HE/AuC. An HE may contain one or more AuC. The temporary authentication key KT is derived from the long term authentication key K. The temporary authentication key is shared with the Serving Network, while the long term authentication key K is never exposed outside of the HE/AuC.

The mutual authentication protocol is composed of a two pass challenge response protocol for user authentication combined with a one pass challenge and subsequent use of a derived integrity key for implicit network authentication.

The authentication and key agreement method consists of a procedure for new registrations and a procedure for current registrations. These procedures are discussed in the following subsections. The overall scheme is summarised in Figure 11.1.

[Because the user contributes to the generation of the temporary authentication keys, it seems more sensible to describe this scheme in terms of new and current registrations. This is preferred to the GSM 03.20 approach which involves separating out the distribution of authentication information from the HE/AuC to the SN/VLR from the authentication exchange between the SN/VLR and the user.]

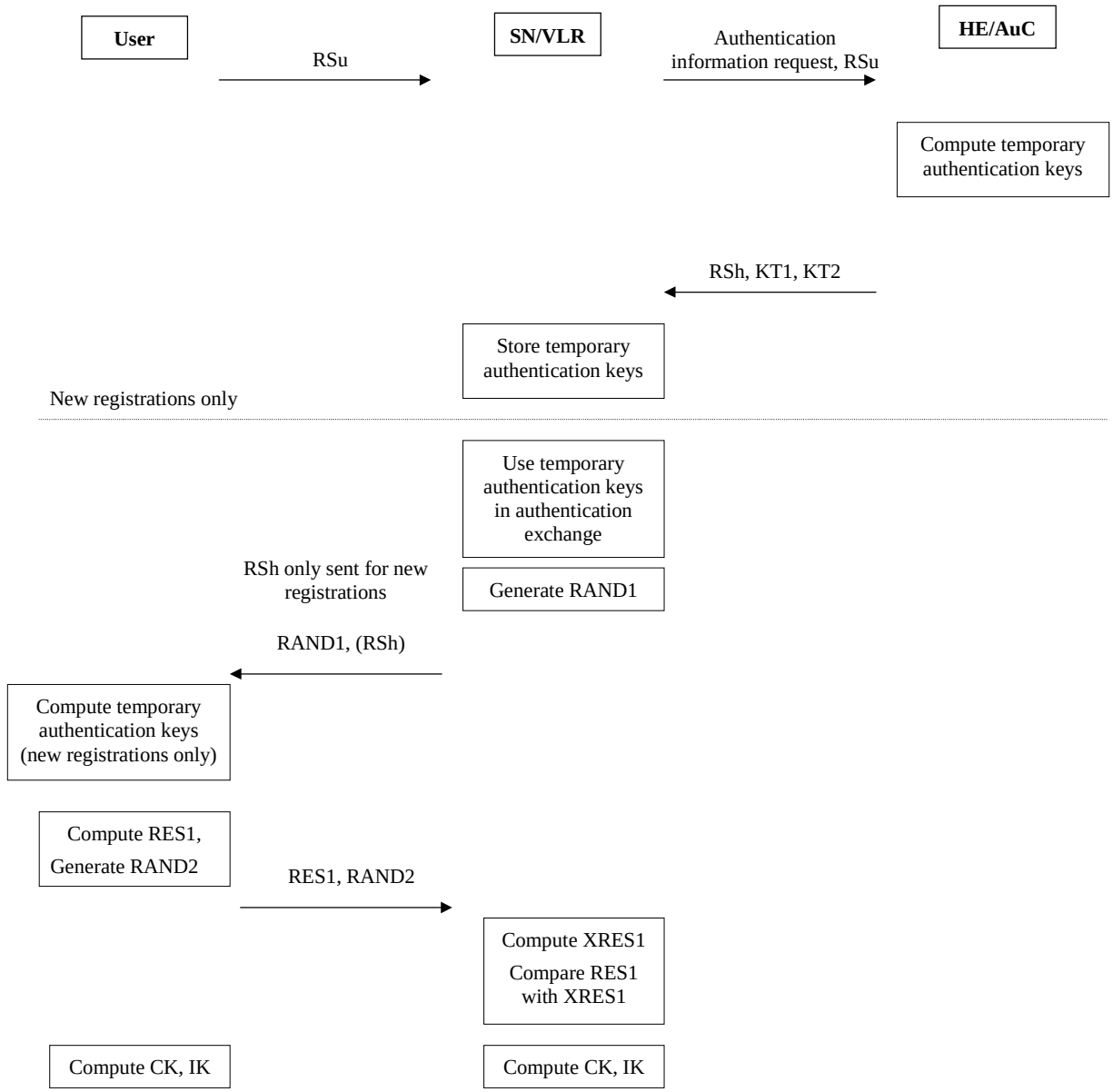


Figure 11.1 – Overview of authentication procedure

11.1.3 General authentication procedure - New registrations

The general case for new registrations is described where temporary authentication keys are distributed to the SN/VLR and used in the authentication exchange with the user. Other cases are described in the Annex.

To initiate a new registration the user generates a random seed component RSu and sends it to the SN/VLR. The SN/VLR then forwards this to the HE/AuC as part of an authentication information request. The HE/AuC generates a random seed component, RSh. RSu and RSh are then used together with the authentication key K to compute the temporary authentication keys. The temporary authentication keys consist of KT1 for user authentication, which is generated using UA11, and KT2 for network authentication, which is generated using UA21. The temporary authentication keys and the corresponding random seed component RSh are then passed to the requesting SN/VLR.

The SN/VLR uses the temporary authentication keys in the authentication exchange with the user. In the first message a random challenge RAND1 and the random seed from the HE/AuC RSh are sent to the user. The user first uses RSh and RSu to generate the temporary authentication keys KT1 and KT2 using the authentication key K and the algorithms UA11 and UA12, respectively.

The user then uses the random challenge RAND1 to compute a response RES1 using the temporary authentication key KT1 and the algorithm UA12 and sends this back to the SN/VLR, together with a random challenge, RAND2. The user

also uses RAND1 to compute a derived cipher key CK1 and a derived integrity key IK1 using the temporary authentication key KT1 and the algorithms UA13 and UA14 respectively. Similarly, the user uses RAND2 to compute a derived cipher key CK2 and a derived integrity key IK2 using the temporary authentication key KT2 and the algorithms UA23 and UA24 respectively.

The SN/VLR verifies the response from the user by using RAND1 to compute XRES1 using KT1 and the algorithm UA12. If XRES1 equals RES1 then the authentication of the user has passed. The SN/VLR also uses RAND1 to compute a derived cipher key CK1 and a derived integrity key IK1 using the temporary authentication key KT1 and the algorithms UA13 and UA14 respectively. Similarly, the SN/VLR uses the random challenge RAND2 to compute a derived cipher key CK2 and a derived integrity key IK2 using KT2 and the algorithms UA23 and UA24 respectively.

After the authentication exchange both the user and the SN/VLR can compute the cipher key CK from its two components CK1 and CK2 using algorithm UB1, and the integrity key IK from its two components IK1 and IK2 using algorithm UB2.

(The user implicitly authenticates the network through use of the integrity key, IK, which is derived from IK1 and IK2.)

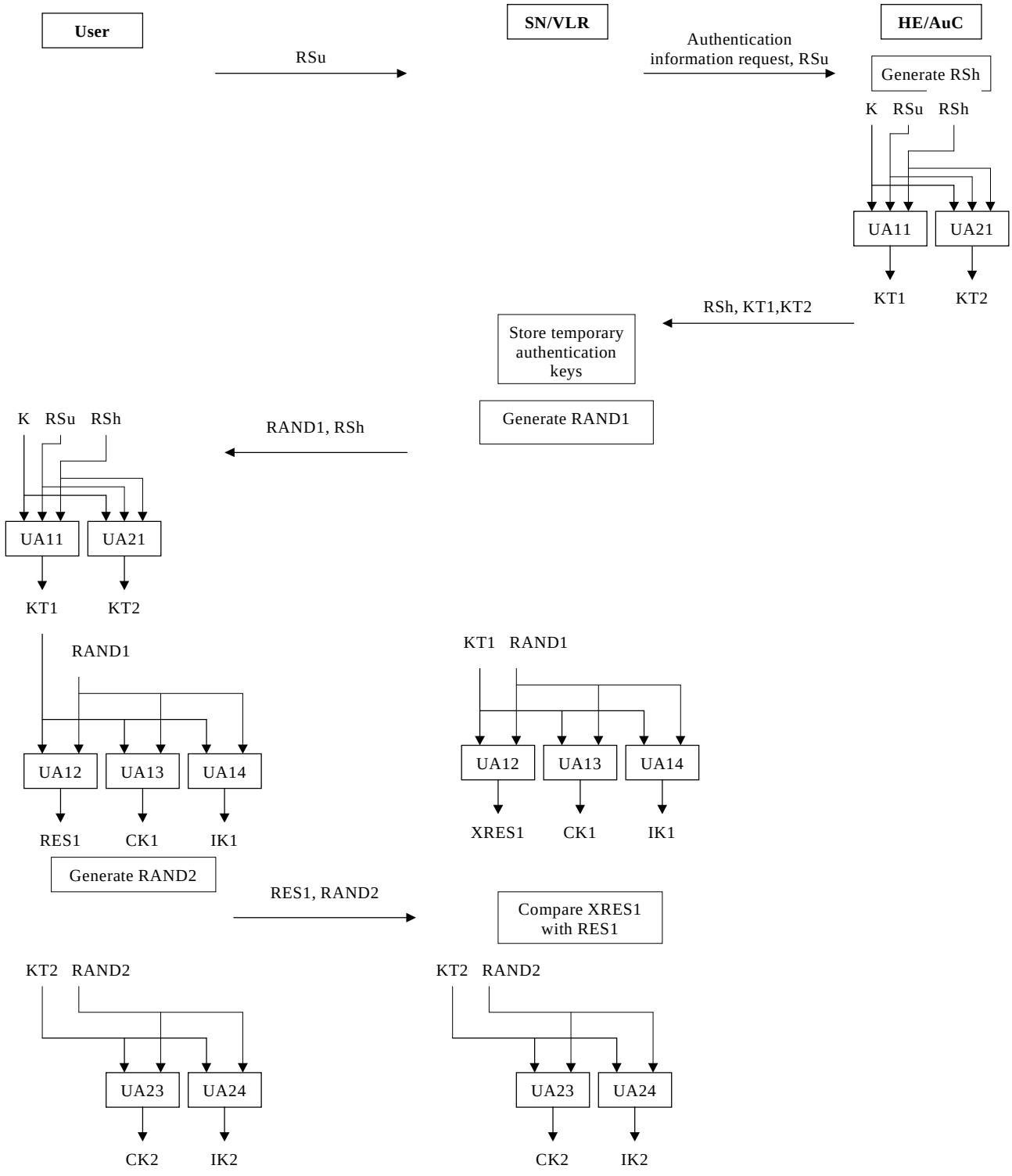


Figure 11.2 General procedure for new registrations

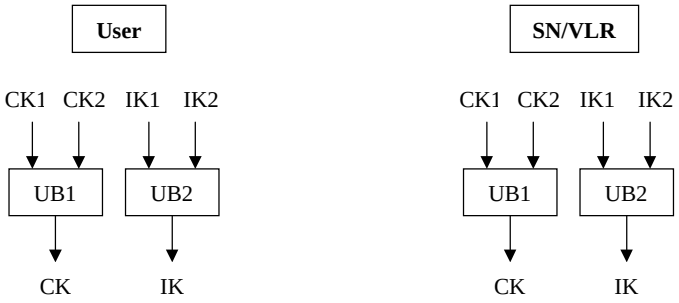


Figure 11.3 - Procedure for cipher and integrity key construction

11.1.4 Current registrations

The general case for current registrations is described where temporary authentication keys have been distributed to the SN/VLR in advance (perhaps as part of a new registration). Other cases are described in the Annex.

When the SN/VLR performs an authentication, it uses the temporary authentication keys corresponding to the user. In the first message a random challenge RAND1 is sent to the user. The user uses the random challenge RAND1 to compute a response RES1 using the temporary authentication key KT1 and the algorithm UA12 and sends this back to the SN/VLR, together with a random challenge, RAND2. The user also uses RAND1 to compute a derived cipher key CK1 and a derived integrity key IK1 using the temporary authentication key KT1 and the algorithms UA13 and UA14 respectively. Similarly, the user uses RAND2 to compute a derived cipher key CK2 and a derived integrity key IK2 using the temporary authentication key KT2 and the algorithms UA23 and UA24 respectively.

The SN/VLR verifies the response from the user by using RAND1 to compute XRES1 using KT1 and the algorithm UA12. If XRES1 equals RES1 then the authentication of the user has passed. The SN/VLR also uses RAND1 to compute a derived cipher key CK1 and a derived integrity key IK1 using the temporary authentication key KT1 and the algorithms UA13 and UA14 respectively. Similarly, the SN/VLR uses the random challenge RAND2 to compute a derived cipher key CK2 and a derived integrity key IK2 using KT2 and the algorithms UA23 and UA24 respectively.

After the authentication exchange both the user and the SN/VLR can compute the cipher key CK from its two components CK1 and CK2 using algorithm UB1, and the integrity key IK from its two components IK1 and IK2 using algorithm UB2.

(The user implicitly authenticates the network through use of the integrity key, IK, which is derived from IK1 and IK2.)

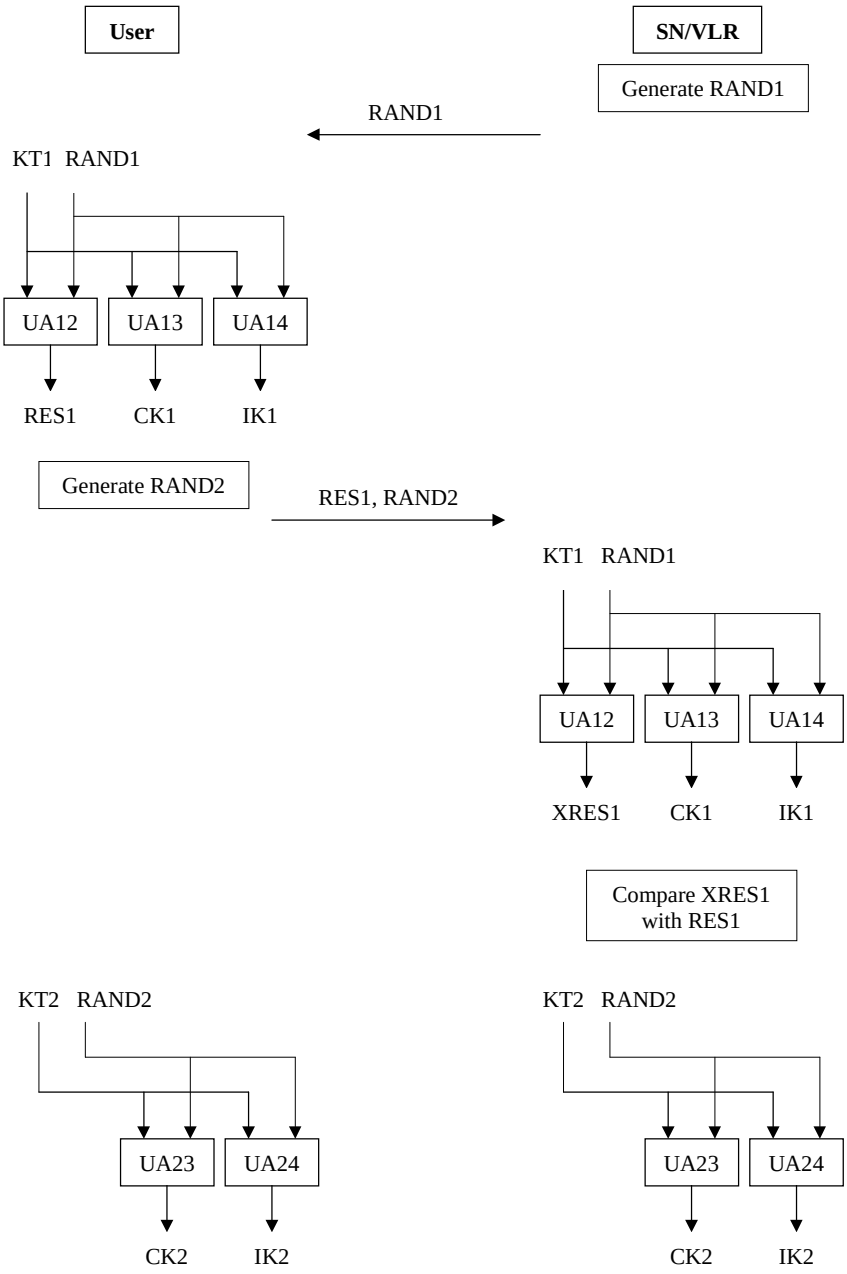


Figure 11.4 General procedure for current registrations

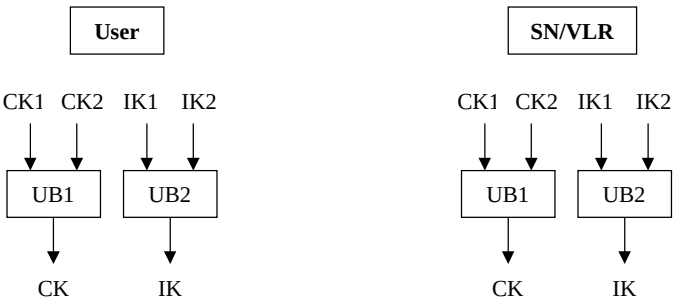


Figure 11.5 - Procedure for cipher and integrity key construction

11.1.5 Temporary authentication key lifetime

A mechanism is needed to ensure that a particular set of temporary authentication keys is not used for an unlimited period of time, to avoid attacks using compromised keys. Authentication which generates fresh temporary authentication keys is not mandatory at call setup, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. The USIM shall therefore contain a mechanism to limit the number of calls that can be made with a specific set of temporary authentication keys.

Operators shall decide on the value of this number of calls, and write this parameter on the USIM. The USIM shall have a counter that counts the number of times the temporary authentication key is used and shall trigger a new registration that will generate new temporary authentication keys if the counter reaches the maximum value set in the USIM[3]. This mechanism will ensure that a set of temporary authentication keys cannot be reused more times than the limit set by the operator.

11.1.6 Other procedures for obtaining temporary authentication keys

The section describes authentication procedures which deviate from the general cases.

11.1.6.1 Temporary authentication keys obtained from old SN/VLR

[Further study is required into whether this procedure is required. There may be dangers. Network element impersonation attacks should be considered]

During location updating in a new VLR (VLRn), the procedure to obtain authentication information may differ from that described in the general case. In the case when identification is done using a TMUI based identity confidentiality mechanism, authentication information shall be obtained from the old VLR (VLRo) when possible.

The MS identifies itself to the new VLR using a TMUIo previously allocated by the old VLR and the corresponding Location Area Identification (LAI). The new VLR uses this information to find out the address of the old VLR and sends it TMUIo together with an authentication information request.

The old VLR responds with the IMUI corresponding to TMUIo together with the temporary authentication keys for that IMUI.

[There may also be a need to request temporary authentication keys from an old SN/VLR when TMUIs are not used. In this case the MS would have to identify itself using LAIo/IMUI rather than LAIo/TMUIo. Note however that this mechanism does not seem to be provided in GSM.]

---

[3] *Which message should be chosen as a parameter? Using this would register call attempts as well as calls...*

12. Annex E (Informative): Reasons behind decision on authentication and key agreement mechanism

This section presents the reasons why SMG10 WPC recommended the sequence number proposal (SEQ) for the UMTS AKA over the revised TETRA proposal (TETRA REV).

SEQ and TETRA REV were evaluated against a number of criteria. Those criteria where the two mechanisms were **not** equal are given below in Table 12.1.

Category	Criteria	TETRA REV	SEQ	Better mechanism
Standards	Compatibility with GSM security architecture	No	Yes	SEQ
Standards	Need for standard AKA algorithm	Yes	No	SEQ
Standards	Compatibility with current IS-41 security architecture	Yes	No	TETRA REV
Signalling	Frequency of SN-HE signalling	At registration in new SN or at expiry of temporary authentication key	For each new batch of quintuplets	TETRA REV
Signalling	No of passes – new registration	3	2	SEQ
Signalling	No of passes – current registration	2	2	Equal
Resilience	Resilience to breakdown of links between SN and HE	SN can continue for duration of temporary authentication key	Quintuplets can only be used once[4].	TETRA REV
Processing	Processing load as number of calls to an algorithm, for new registration/for current registration	USIM: 2/1 SN: 1/1 HE: 1/0	USIM: 2/2 SN: 0/0 HE: 2n/0 (where n is the number of quarters generated per batch)	TETRA REV SEQ TETRA REV
Processing	Pre-computation of authentication information at HE possible?	No	Yes	SEQ[5]
Processing	SN/VLR has to act as authentication centre?	Yes	No	SEQ

Table 12.1 - Criteria for assessing authentication and key agreement mechanisms

[4] Though with use of the cipher and integrity keys from one quintuplet over many calls, a batch of quintuplets can be used securely over a significant number of calls.

[5] However, networks may not want to pre-compute authentication information, but to generate the information as required, and so reduce storage requirements.

The group felt that there was not sufficient time or expertise to weight the criteria and assign scores to the two mechanisms for each criteria. A qualitative approach was therefore followed. As this approach was not precise, the group decided not to reject the lesser of the two mechanisms, but to detail this mechanism in an informative appendix to 33.23, so that it could be reviewed and assessed by groups other than SMG10 WPC. The qualitative decision process is detailed below.

The criteria were divided into five categories: Standards, Signalling, Security, Resilience and Processing.

Standards. As it is a stated aim of UMTS that it is an evolution from GSM, compatibility with GSM security architecture was judged to be more important than compatibility with IS-41 security architecture. SEQ was therefore judged to be ahead of TETRA REV in the Standards category.

Signalling. The temporary authentication key for TETRA REV can be used autonomously by the SN for longer than a batch of SEQ quartets. There is therefore less need for SN-HE signalling with TETRA REV than with SEQ. SEQ and TETRA REV are roughly equal with the regard to the number of passes involved in each run of the AKA mechanism and the number of calls to algorithms in each pass. TETRA REV was therefore judged to be superior in the Signalling category.

Security. The temporary authentication key in TETRA REV, precisely because it can be used without contacting the SN, represents a greater security risk than the quartets of SEQ. Therefore, SEQ is the better mechanism in the Security category.

Processing. SEQ was judged to be the better mechanism in the Processing category. SEQ, like GSM, does not require any cryptographic functionality in the VLR. TETRA REV however, delegates a certain amount of the work done by the AuC in GSM, to the VLR. SEQ allows the possibility of the pre-computation of quartets in the HE, whereas in TETRA REV, security information must be generated in real time, as a challenge from the user is required at the time of the request for security information.

Resilience. TETRA REV was judged to be the better mechanism in the Resilience category. TETRA REV can withstand breaks in the SN to HE link over an extended period more securely than SEQ. TETRA REV does not require measures to retain sequence number synchronisation between the HE and USIM unlike SEQ.

Based on this comparison, but mainly because of the significance attached to the fact that SEQ is compatible with the GSM security architecture and TETRA REV is not, SEQ was described in the main body of the report, and TETRA in an informative annex.