



---

# 1 Scope

This specification defines the security architecture, i.e., the security features and the security mechanisms, for the third generation mobile telecommunication system.

A security feature is a service capability that meets one or several security requirements. The complete set of security features address the security requirements as they are defined in "3G Security: Threats and Requirements" (21.133 [1]). A security mechanism is an element that is used to realise a security feature. All security features and security ~~requirements~~ mechanisms taken together form the security architecture.

An example of a security feature is user data confidentiality. A security mechanism that may be used to implement that feature is a stream cipher using a derived cipher key.

This specification defines 3G security procedures performed within 3G capable networks (R99+), i.e. intra-UMTS and UMTS-GSM. As an example, UMTS authentication is applicable to UMTS radio access as well as GSM radio access provided that the serving network node and the subscriber-MS are UMTS capable. Interoperability with non-UMTS capable networks (R98-) is also covered.

---

## 3 Definitions, symbols and abbreviations

### 3.1 Definitions

For the purposes of the present document, the following definitions apply:

**Confidentiality:** The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

**Data integrity:** The property that data has not been altered in an unauthorised manner.

**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.

**USIM – User Services Identity Module.** In a security context, this module is responsible for performing UMTS subscriber and network authentication and key agreement. It should also be capable of performing GSM authentication and key agreement to enable the subscriber to roam easily into a GSM Radio Access Network.

**SIM – GSM Subscriber Identity Module.** In a security context, this module is responsible for performing GSM subscriber authentication and key agreement. This module is **not** capable of handling UMTS authentication nor storing UMTS style keys.

**UMTS Entity authentication and key agreement:** Entity authentication according to this specification.

**GSM Entity authentication and key agreement:** Entity authentication according to TS ETSI GSM 03.20

**User access module:** either a USIM or a SIM

**Mobile station, user:** the combination of user equipment and a user access module.

**UMTS subscriber:** a mobile station that consists of user equipment with a USIM inserted.

**GSM subscriber:** a mobile station that consists of user equipment with a SIM inserted.

**UMTS security context:** a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI.

**GSM security context:** a state that is established between a user and a serving network domain usually as a result of

the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

**Quintet, UMTS authentication vector:** temporary authentication data that enables an MSC/VLR or SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

**Triplet, GSM authentication vector:** temporary authentication data that enables an MSC/VLR or SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

**Authentication vector:** either a quintet or a triplet.

**Temporary authentication data:** either UMTS or GSM security context data or UMTS or GSM authentication vectors.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f1*	Message authentication function used to compute MACS
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK
K	Long-term secret key shared between the USIM and the AuC

## 3.3 Abbreviations

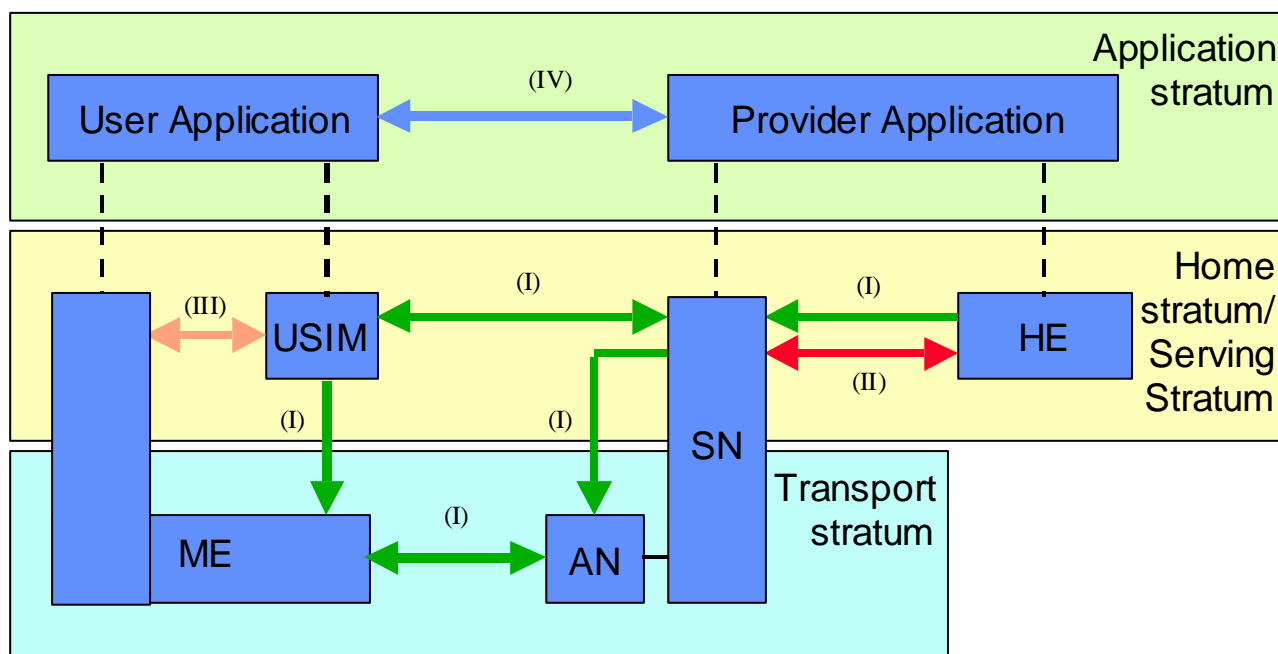
For the purposes of the present document, the following abbreviations apply:

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
MACS	The message authentication code included in AUTS, computed using f1*
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
SQN	Sequence number

$SQN_{HE}$	Sequence number counter maintained in the HLR/AuC
$SQN_{MS}$	Sequence number counter maintained in the USIM
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TMSI	Temporary Mobile Subscriber Identity
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	User Services Identity Module
VLR	Visitor Location Register
XRES	Expected Response

## 4 Overview of the security architecture

Figure 1 gives an overview of the complete 3G security architecture.



**Figure 1: Overview of the security architecture**

Five security feature groups are defined. Each of these feature groups meets certain threats and, accomplishes certain security objectives:

- **Network access security (I):** the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
- **User domain security (III):** the set of security features that secure access to mobile stations
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security features is in operation or not and whether the use and provision of services should depend on the security feature.

Figure 2 gives an overview of the ME registration and connection principles within UMTS with a CS service domain

and a PS service domain. As in GSM/GPRS, user (temporary) identification, authentication and key agreement will take place independently in each service domain. User plane traffic will be ciphered using the cipher key agreed for the corresponding service domain while control plane data will be ciphered and integrity protected using the cipher and integrity keys from either one of the service domains. In clause 6 the detailed procedures are defined and when not otherwise stated they are used in both service domains.

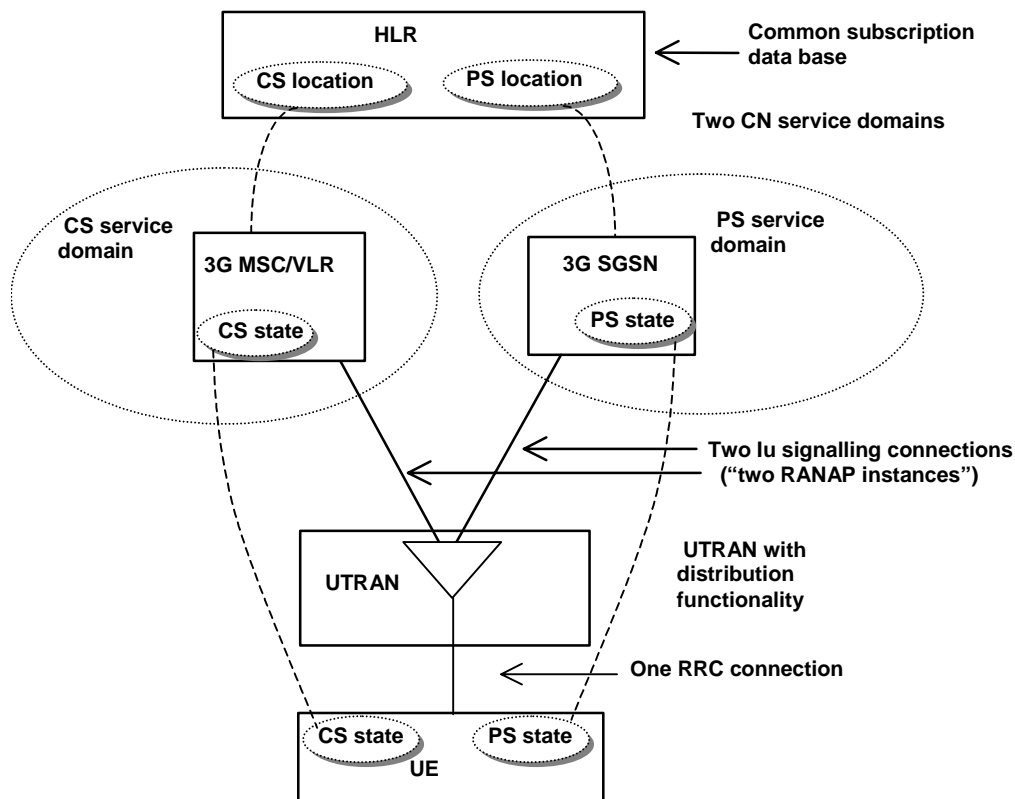


Figure 2: Overview of the ME registration and connection principles within UMTS for the separate CN architecture case when the CN consists of both a CS service domain with evolved MSC/VLR, 3G\_MSC/VLR, as the main serving node and an PS service domain with evolved SGSN/GGSN, 3G\_SGSN and 3G GGSN, as the main serving nodes (Extract from TS 23.121 – Figure 4-8)

## 5 Security features

### 5.1 Network access security

#### 5.1.1 User identity confidentiality

The following security features related to user identity confidentiality are provided:

- **user identity confidentiality:** the property that the permanent user identity (IMUI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;
- **user location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;
- **user untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

To achieve these objectives, the user is normally identified by a temporary identity by which he is known by the visited serving network, or by an encrypted permanent identity. To avoid user traceability, which may lead to the compromise

of user identity confidentiality, the user should not be identified for a long period by means of the same temporary or encrypted identity. To achieve these security features, in addition it is required that any signalling or user data that might reveal the user's identity is ciphered on the radio access link.

Clause 6.1 describes a mechanism that allows a user to be identified on the radio path by means of a temporary identity by which he is known in the visited serving network. This mechanism should normally be used to identify a user on the radio path in location update requests, service requests, detach requests, connection re-establishment requests, etc..

## 5.1.2 Entity authentication

The following security features related to entity authentication are provided:

- **authentication mechanism agreement:** the property that the user and the serving network can securely negotiate the mechanism for authentication and key agreement that they shall use subsequently;
- **user authentication:** the property that the serving network corroborates the user identity of the user;
- **network authentication:** the property that the user corroborates that he is connected to a serving network that is authorised by the user's HE to provide him services; this includes the guarantee that this authorisation is recent.

To achieve these objectives, it is assumed that entity authentication should occur at each connection set-up between the user and the network. Two mechanisms have been included: an authentication mechanism using an authentication vector delivered by the user's HE to the serving network, and a local authentication mechanism using the integrity key established between the user and serving network during the previous execution of the authentication and key establishment procedure.

Clause 6.3 describes an authentication and key establishment mechanism that achieves the security features listed above and in addition establishes a secret cipher key (see 5.1.3) and integrity key (see 5.1.4) between the user and the serving network. This mechanism should be invoked by the serving network after a first registration of a user in a serving network and after a service request, location update request, attach request, detach request or connection re-establishment request, when the maximum number of local authentications using the derived integrity key have been conducted.

Clause 6.5 describes the local authentication mechanism. The local authentication mechanism achieves the security features user authentication and network authentication and uses an integrity key established between user and serving network during the previous execution of the authentication and key establishment procedure. This mechanism should be invoked by the serving network after a service request, location update request, attach request, detach request or connection re-establishment request, provided that the maximum number of local authentications using the same derived integrity key has not been reached yet.

## 5.1.3 Confidentiality

The following security features are provided with respect to confidentiality of data on the network access link:

- **cipher algorithm agreement:** the property that the MS and the SN can securely negotiate the algorithm that they shall use subsequently;
- **cipher key agreement:** the property that the MS and the SN agree on a cipher key that they may use subsequently;
- **confidentiality of user data:** the property that user data cannot be overheard on the radio access interface;
- **confidentiality of signalling data:** the property that signalling data cannot be overheard on the radio access interface;

Cipher key agreement is realised in the course of the execution of the mechanism for authentication and key agreement (see 6.3). Cipher algorithm agreement is realised by means of a mechanism for security mode negotiation between the user and the network (see 6.6.9). This mechanism also enables the selected ciphering algorithm and the agreed cipher key to be applied in the way described in 6.6.

## 5.1.4 Data integrity

The following security features are provided with respect to integrity of data on the network access link:

- **integrity algorithm agreement:** the property that the MS and the SN can securely negotiate the integrity algorithm that they shall use subsequently;
- **integrity key agreement:** the property that the MS and the SN agree on an integrity key that they may use subsequently;
- **data integrity and origin authentication of signalling data:** the property that the receiving entity (MS or SN) is able to verify that signalling data has not been modified in an unauthorised way since it was sent by the sending entity (SN or MS) and that the data origin of the signalling data received is indeed the one claimed;

Integrity key agreement is realised in the course of the execution of the mechanism for authentication and key agreement (see 6.3). Integrity algorithm agreement is realised by means of a mechanism for security mode negotiation between the user and the network (see 6.6.9). This mechanism also enables the selected integrity algorithm and the agreed integrity key to be applied in the way described in 6.4.

## 5.1.5 Mobile equipment identification

**NOTE:**—In certain cases, SN may request the MS to send it the mobile equipment identity of the terminal. The mobile equipment identity shall only be sent after authentication of SN with exception of emergency calls. The IMEI should be securely stored in the terminal. However, the presentation of this identity to the network is not a security feature and the transmission of the IMEI is not protected. Although it is not a security feature, it should not be deleted from UMTS however, as it is useful for other purposes.

## 5.2 Network domain security

### 5.2.1 Void

### 5.2.2 Void

### 5.2.3 Void

### 5.2.4 Fraud information gathering system

**NOTE:** Some feature will be provided which will allow fraud information to be exchanged between 3GMS providers according to time constraints that yet have to be defined.

## 5.3 User domain security

### 5.3.1 User-to-USIM authentication

This feature provides the property that access to the USIM is restricted until the USIM has authenticated the user. Thereby, it is ensured that access to the USIM can be restricted to an authorised user or to a number of authorised users. To accomplish this feature, user and USIM must share a secret (e.g. a PIN) that is stored securely in the USIM. The user gets access to the USIM only if he/she proves knowledge of the secret.

This security feature is implemented by means of the mechanism described in [21].

### 5.3.2 USIM-Terminal Link

This feature ensures that access to a terminal or other user equipment can be restricted to an authorised USIM. To this end, the USIM and the terminal must share a secret that is stored securely in the USIM and the terminal. If a USIM fails to prove its knowledge of the secret, it will be denied access to the terminal.

This security feature is implemented by means of the mechanism described in [15].

## 5.4 Application security

### 5.4.1 Secure messaging between the USIM and the network

It is expected that 3GMS will provide the capability for operators or third party providers to create applications which are resident on the USIM (similar to SIM Application Toolkit in GSM). There exists a need to secure messages which are transferred over the 3GMS network to applications on the USIM, with the level of security chosen by the network operator or the application provider.

The following security features are provided with respect to protecting messages transferred to applications on the USIM over the 3GMS network:

- **Entity authentication of applications:** the property that two applications are able to corroborate each other's identity.
- **Data origin authentication of application data:** the property that the receiving application is able to verify the claimed data origin of the application data received;
- **Data integrity of application data:** the property that the receiving application is able to verify that application data has not been modified since it was sent by the sending application;
- **Replay detection of application data:** the property that an application is able to detect that the application data that it receives is replayed;
- **Sequence integrity of application data:** the property that an application is able to detect that the application data that it receives is received in sequence;
- **Proof of receipt:** the property that the sending application can proof that the receiving application has received the application data sent.
- **Confidentiality of application data:** the property that application data is not disclosed to unauthorised parties.

NOTE: It is assumed that these security features will be based on GSM SIM Application Toolkit security features. Further work is required to identify what enhancements need to be made to SIM Application Toolkit security. Possible areas of enhancement may include: key management support, enhancement of security mechanisms/features, increased flexibility in algorithm choice and security parameter size. A joint 3GPP TSG-SA 'Security'/3GPP TSG-T 'USIM' working group may be required to progress this issue.

### 5.4.2 Void

### 5.4.3 ~~Access to user profile data~~Void

{{fs}}

### 5.4.4 ~~IP security~~Void

{{fs}}



## 5.5 Security visibility and configurability

### 5.5.1 Visibility

Although in general the security features should be transparent to the user, for certain events and according to the user's concern, greater user visibility of the operation of security features should be provided. This yields to a number of features that inform the user of security-related events, such as:

- indication of access network encryption: the property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up;
- indication of the level of security: the property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with lower security level (3G → 2G).

### 5.5.2 Configurability

Configurability is the property that that the user and the user's HE can configure whether the use or the provision of a service should depend on whether a security feature is in operation. A service can only be used if all security features, which are relevant to that service and which are required by the configurations of the user or of the user's HE, are in operation. The following configurability features are suggested:

- Enabling/disabling user-USIM authentication: the user and/or user's HE should be able to control the operation of user-USIM authentication, e.g., for some events, services or use.
- Accepting/~~Rejecting~~ ~~rejecting~~ incoming non-ciphered calls: the user and/or user's HE should be able to control whether the user accepts or rejects incoming non-ciphered calls;
- Setting up or not setting-up non-ciphered calls: the user and/or user's HE should be able to control whether the user sets up connections when ciphering is not enabled by the network;
- Accepting/rejecting the use of certain ciphering algorithms: the user and/or user's HE should be able to control which ciphering algorithms are acceptable for use.

## 6.5.2 Layer of integrity protection

The UIA shall be implemented in the ME and in the RNC.

Integrity protection shall be ~~applied~~ ~~y~~ at the RRC layer.

## 6.8.4 Intersystem handover for CS Services – from UTRAN to GSM BSS

If ciphering has been started when an intersystem handover occurs from UTRAN to GSM BSS, the necessary information (e.g. Kc, supported/allowed GSM ciphering algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old RNC to the new GSM BSS, and to continue the communication in ciphered mode. The RNC requests the MS to send the MS Classmark, which includes information on the GSM ciphering algorithm capabilities of the MS. The intersystem handover will imply a change of ciphering algorithm from a UEA to a GSM A5. The GSM BSS includes the selected GSM ciphering mode in the handover command message sent to the MS via the RNC.

The integrity protection of signalling messages is stopped at handover to GSM BSS.

The highest hyperframe number value reached for all signalling and user data bearers during the RRC connection shall be stored in the ME/USIM at handover to GSM BSS.