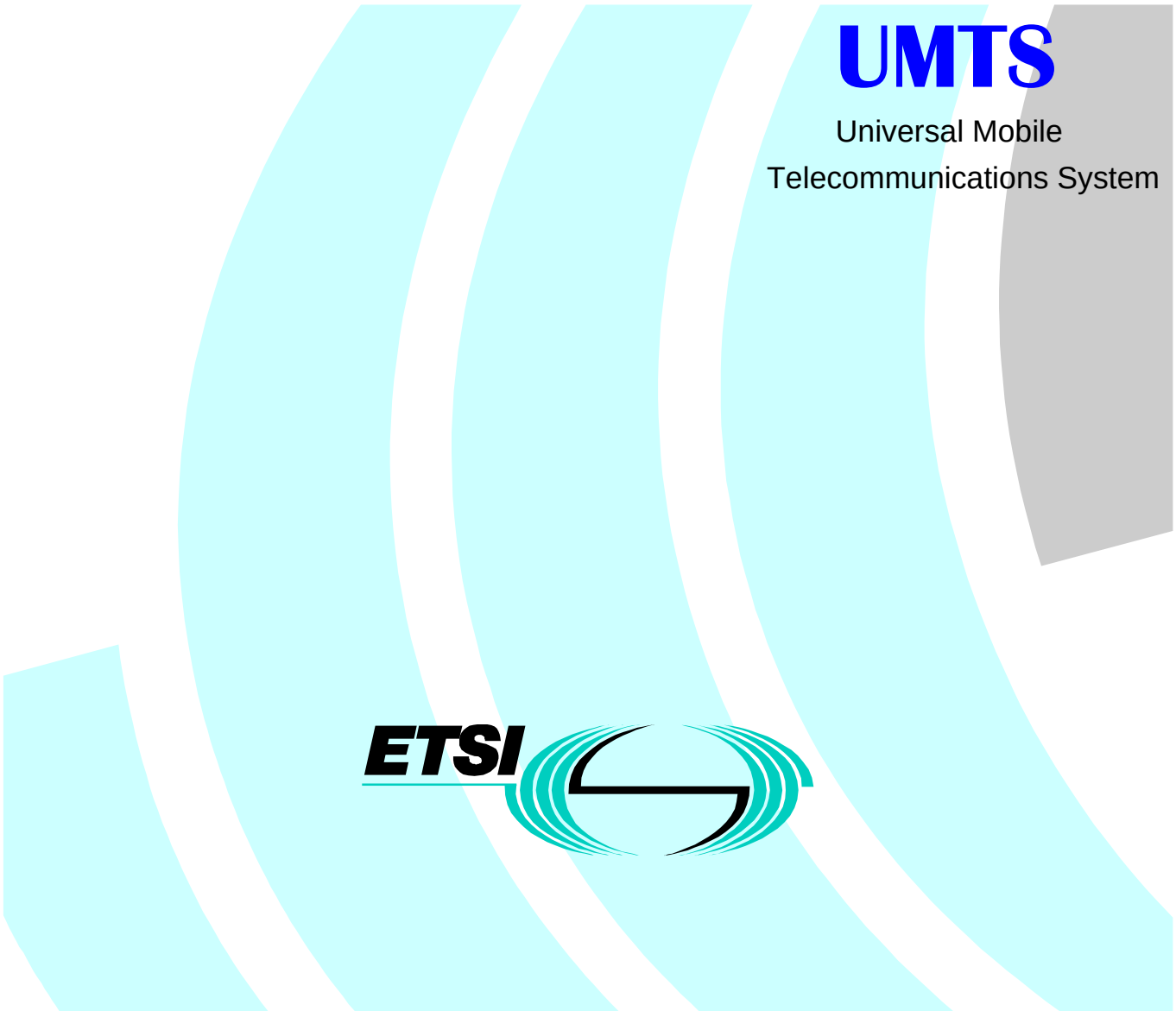
3GPP Systems and Services TSG, Security WG
London, 2-4 February, 1999

Tdoc s3-99004
Source: ETSI SMG10

UMTS 33.22 V1.0.0 (1999-02)

European Standard (Telecommunications series)

Universal Mobile Telecommunications System (UMTS); Security Features (UMTS 33.22 version 1.0.0)



Reference
SMG-103322 (xxxx.PDF)

Keywords
Universal Mobile Telecommunications System

ETSI

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

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 SR 000 314: *"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.org/ipr).

Pursuant to the ETSI 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 SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Special Mobile Group (SMG), and is now submitted to the ETSI standard One-step Approval Procedure.

The present document contains the list of security features for UMTS Phase 1.

The contents of the present document is subject to continuing work within SMG and may change following formal SMG approval. Should SMG modify the contents of the present document it will be re-released with an identifying change of release date and an increase in version number as follows:

Version 3.x.y

where:

3 indicates version approved by SMG for UMTS Phase 1

x the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

y the third digit is incremented when editorial only changes have been incorporated in the specification.

1 Scope

This technical specification contains the list of security features for UMTS Phase 1.

The range of security features defined in this specification embraces those features required to meet the requirements listed in UMTS 33.21 "Security Requirements". The security mechanisms that implement the identified security features are specified in UMTS 33.23 "Security Mechanisms".

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 lists the general requirements on UMTS Phase 1 security features;

clause 5 defines all security features for UMTS Phase 1 in a uniform format;

annex A (informative) deals with the requirements that the network security features impose on the data protection of data elements stored in databases in network entities and transmitted over network links;

annex B (informative) deals with security features that run between wireline links between provider domains. They are outside the scope of this specification;

annex C (informative) contains an alternative set of security mechanisms for the security features related with authentication and key establishment;

annex D (informative) contains the history of this specification.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] UMTS 33.21: "Universal Mobile Telecommunications System (UMTS): Security Requirements".

[2] UMTS 33.23: "Universal Mobile Telecommunications System (UMTS): Security Mechanisms".

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

AuC	Authentication Centre
DCK	Derived Cipher Key
DIK	Derived Integrity Key
HE	Home Environment
HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMUI	International Mobile User Identity
MAC	Message Authentication Code
MS	Mobile Station
MSC	Mobile-services Switching Centre
PAK	Permanent Authentication Key
PDCK	Partial Derived Cipher Key
PDIK	Partial Derived Integrity Key
PIN	Personal Identification Number
RNC	Radio Network Controller
TAK	Temporary Authentication Key
SN	Serving Network
TMUI	Temporary Mobile User Identity
TNAK	Temporary Network Authentication Key
TUAK	Temporary User Authentication Key
UE	User Equipment
UICC	UMTS Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
USIM	User Services Identity Module
VLR	Visitor Location Register

4 Requirements on security features

This clause provides a list of requirements on UMTS security features.

Those provided for the benefit of UMTS human users should be user friendly, require a minimum of user interaction and, as far as possible, be transparent to the users.

If the activation of a security feature provided for the benefit of a customer is controlled by another party, e.g. a network operator, then the customer should be made aware of a failure to activate the feature.

Those provided for the benefit of UMTS users should work without any reduction in security when a user roams.

They must not affect the confidentiality of third parties.

They should not unduly increase time delays for UMTS procedures.

They are compatible with the correct operation of UMTS procedures.

They are such that differences in security functionality for terrestrial and satellite components of UMTS can be minimised.

They have a minimal impact on the use of radio resources.

They are compatible with the use of sequential radio paths.

5 Security features

5.1 Entity authentication

5.1.1 Authentication mechanism agreement

Security Services: Authentication mechanism agreement allows the Serving Network (SN) and the Mobile Station (MS) to agree on the authentication mechanism they will subsequently use.

Assumptions: One or more authentication mechanisms are standardised. The User Services Identity Module (USIM) and the SN database store their respective authentication capabilities in a standardised format.

Invocation: The MS shall invoke the feature at first registration or after a request from the SN, for instance after a database malfunction in the SN.

Involved entities: USIM, MSC/VLR.

Mechanism: The MS sends the SN the authentication capabilities of the USIM, as a part of the "MS capabilities". Based on the authentication capabilities of the USIM and of the SN, the SN then decides which authentication mechanism to use. After establishment of a Derived Integrity Key (DIK), the MS sends a Message Authentication Code (MAC) computed on the "MS capabilities". The SN then verifies the data integrity and origin of the received "MS capabilities".

Requisites: The feature relies on data integrity of data stored in the USIM (authentication mechanism capabilities), and data integrity and origin authentication of signalling elements (MS capabilities).

5.1.2 User-to-network authentication

Security Services: User-to-network authentication allows the SN to corroborate the International Mobile User Identity (IMUI) of the MS.

Assumptions: The MS and the HE share a Permanent Authentication Key (PAK).

Invocation: The SN shall invoke user-to-network authentication at first registration and may or shall invoke the feature at location update and service requests, according to the agreement with the user's Home Environment (HE).

Involved entities: USIM (derivation of Temporary User Authentication Key (TUAK), computation of user response), MSC/VLR (storage of challenge-expected response pair, verification of the user responses), HLR/AuC (derivation of TUAK, generation of challenges, computation of expected responses).

Mechanism: The HE generates a challenge-expected response pair from the user's PAK and forwards it to the MS. The SN sends the challenge to the MS. The MS computes the response and sends it to the SN. The SN compares the response received from the MS with the expected response received from the HE.

Requisites: The feature relies on the confidentiality and data integrity of data stored in the USIM (PAK), MSC/VLR (challenge-expected response pairs) and HLR (PAK, pre-computed challenge-expected response pairs) and confidentiality and data integrity and origin authentication of signalling elements transmitted between MSC/VLR and HLR/AuC (challenge-expected response pairs).

5.1.3 Network-to-user authentication

Security Services: Network-to-user authentication allows the MS to verify that the SN is authorised to provide the user services on behalf of the user's HE.

Assumptions: The MS and the HE share a PAK.

Invocation: The SN shall invoke network-to-user authentication at first registration and may or shall invoke the feature at location updates and at service requests, according to the agreement with the user's HE.

Involved entities: USIM (verification of the data integrity of the network authentication token, verification of the freshness of the sequence number), MSC/VLR (storage of network authentication tokens), HLR/AuC (generation of fresh sequence numbers, computation of MACs).

Mechanism: The HE generates a network authentication token that contains a fresh sequence number with a MAC appended and sends the token to the SN. The SN forwards the token to the MS. The MS verifies the data integrity of the network authentication token and the freshness of the sequence number. Network-to-user authentication is then implicitly achieved when the SN proves knowledge of the DIK. This occurs at the first mandatory integrity protected signalling message.

Requisites: This feature relies on the confidentiality and data integrity of data stored in the USIM (PAK), VLR (network authentication tokens) and HLR (PAK, pre-computed network authentication tokens) and data integrity and origin authentication of signalling elements transmitted between HLR/AuC and MSC/VLR (network authentication token).

5.1.4 User equipment-to-network identification

Security Services: User equipment-to-network identification allows the SN to corroborate the International Mobile Equipment Identity (IMEI).

Assumptions: The User Equipment (UE) stores an IMEI.

Involved entities: UE (storage of IMEI), MSC/VLR.

Invocation: The SN may invoke user equipment-to-network identification via a UE identification request. Typically, the request is sent on a encrypted signalling channel, in order not to compromise the user identity confidentiality.

Mechanism: User equipment-to-network identification will be implemented by a simple request-response mechanism. The response contains the IMEI.

Requisites: The feature relies on data integrity of data stored in the UE (IMEI).

5.1.5 User-to-USIM authentication

Security Services: User-to-USIM authentication restricts the use of a USIM to authorised (human) users.

Assumptions: The USIM stores user authentication data.

Involved entities: USIM (storage of user authentication data), UE, user.

Invocation: The USIM may invoke the feature at power-on of the MS, when a user tries to access UMTS services, or when he tries to access data stored on the USIM. The user can enable and disable the feature completely or for certain events only, e.g. service access.

Mechanism: Access is granted after successful verification of the authentication response that the user provides to the USIM via the UE. Several mechanisms can be used, according to the capabilities of the UE, such as a Personal Identification Number (PIN) or voice, eye or fingerprint recognition. For all mechanisms the data that allows the verification of the user authentication response is stored in the USIM.

Requisites: The feature relies on the confidentiality and data integrity of data stored in the USIM (user authentication data).

5.1.6 USIM-to-UE authentication

Security Services: USIM-to-UE authentication restricts the use of UE to authorised USIMs.

Assumptions: FFS.

Involved entities: USIM, UE.

Invocation: The UE may invoke the feature at power-on of the UE and when a new USIM is inserted. The user can enable and disable the feature.

Mechanism: Access is granted after successful verification of the authentication response that the USIM provides the UE via the UE- UMTS Integrated Circuit Card (UICC) interface. Several mechanisms can be used, according to the capabilities of the USIM and the UE. The mechanism is FFS.

Requisites: The feature relies on the confidentiality and data integrity of data stored in the USIM and in the UE.

5.2 Confidentiality of transmitted data

5.2.1 Ciphering algorithm agreement

Security Services: Ciphering algorithm agreement allows the SN and the MS to agree on the ciphering algorithm they will use.

Assumptions: One or more ciphering algorithms are standardised. The MS and the SN database store their respective ciphering capabilities in a standardised format.

Involved entities: UE (stores the MS ciphering capabilities), MSC/VLR (stores the SN ciphering capabilities, decides on the cipher mode) and the USIM (computes the MAC).

Invocation: At first registrations, the MS shall start the full negotiation by sending the MS capabilities to the SN. At subsequent registrations, call set-ups and location updates, the MS may be requested by the SN to retransmit its MS capabilities. At current registrations, call set-up and location update, the SN shall send security mode command such that the SN can control ciphering on a per-call basis.

Mechanism: The MS sends its ciphering capabilities as they are stored on the UE, and the ciphering preferences, as they are stored in the USIM, as a part of the MS capabilities, to the SN. The SN then decides to cipher or not. If it decides to cipher it decides on a ciphering algorithm. It then sends the chosen cipher mode as part of the security mode command to the MS. The MS verifies the data integrity and origin of the received security mode command and checks whether the cipher mode:

- is available in the UE;
- is acceptable according to the user's service profile;
- conforms to the user's preferences according to its service profile and information sent by the HE to the MS, as part of the authentication tokens, on the ciphering capabilities of the SN.

After establishment of a DIK, the MS computes a MAC on the MS capabilities and sends it to the SN. The SN verifies the data integrity and origin of the previously received MS capabilities message.

Requisites: The feature relies on the data integrity of data stored in the UE (ciphering capabilities) and data integrity and origin authentication of signalling elements transmitted between MS and SN (MS capabilities, cipher mode command).

5.2.2 Establishment of a derived cipher key

Security Services: Establishment of a derived cipher key provide the MS and the SN with a secret Derived Cipher Key (DCK) to prevent eavesdropping on user and signalling data transmitted between MS and SN, which freshness guarantees towards the MS and the SN.

Assumptions: This feature is integrated with user-to-network authentication and network-to-user authentication.

Involved entities: USIM (derivation of DCK), UE (storage of DCK), Radio Network Controller (RNC) (storage of DCK), VLR (storage of DCK), HLR (derivation of DCK).

Invocation: The establishment of a new derived DCK is integrated in the mechanism for user- network authentication and key establishment.

Mechanism: The HE generates a fresh challenge and computes the DCK from the challenge and the user's PAK. The HE then computes an authentication token that consists of a fresh sequence number, and a MAC on the sequence number and the challenge. The user trusts the HE to generate a fresh challenge with a fresh sequence number. The HE

sends the challenge, the authentication token and the DCK to the SN. The SN forwards the challenge and the authentication token to the MS. The MS verifies the data integrity and origin of the challenge and the sequence number and the freshness of the sequence number and therefore also the freshness of the challenge. The MS then computes the fresh DCK from the fresh challenge.

Requisites: The feature relies on the data integrity of data stored in the UE (DCK), RNC (DCK), VLR (DCK) and confidentiality of signalling data transmitted between HLR and VLR (DCK).

5.2.3 Confidentiality of user data

Security Services: Confidentiality of user data prevents eavesdropping on user data sent on the radio access links.

Assumptions: MS and SN have established a DCK using the security feature "Establishment of a derived cipher key".

Involved entities: UE (encryption/decryption, storage DCK), RNC (encryption/decryption, storage DCK).

Invocation: Confidentiality of user data may be invoked by the SN with the mandatory security mode command that shall be sent at the establishment of each user data channel.

Mechanism: Confidentiality of user data will be implemented by a stream cipher that uses the DCK. As soon as the security mode command is sent out, the SN starts encryption. The MS initiates encryption and decryption as soon as it receives the security mode command and sends the security mode confirm message to the SN. The SN initiates encryption as soon as it receives the security mode confirm message.

Requisites: The feature relies on the confidentiality and data integrity of data stored in the UE (DCK) and RNC (DCK).

5.2.4 Confidentiality of signalling data

Security Services: Confidentiality of signalling data prevents eavesdropping on signalling data (including user-related data) sent on the radio access links.

Assumptions: MS and SN have established a DCK using the security feature "Establishment of a derived cipher key".

Involved entities: UE (encryption/decryption, storage DCK), RNC (encryption/decryption, storage DCK).

Invocation: The feature may be invoked by the SN with the mandatory security mode command that shall be sent at the establishment of each signalling channel.

Mechanism: Confidentiality of signalling data will be implemented by a stream cipher that uses a DCK. As soon as the security mode command is sent out, the SN starts encryption. The MS initiates encryption and decryption as soon as it receives the security mode command and sends the security mode confirm message to the SN. The SN initiates encryption as soon as it receives the security mode confirm message.

Requisites: The feature relies on the confidentiality and data integrity of data stored in the UE (DCK) and RNC (DCK).

5.2.5 Confidentiality of user identity

Security Services: Confidentiality of user identity ensures that the user identity is not revealed to eavesdroppers when the user accesses services.

Assumptions: MS and SN have executed the authentication and key establishment mechanism and established a DCK.

Involved entities: USIM (storage of the permanent and Temporary Mobile User Identity (TMUI)), VLR (storage of the permanent and TMUI).

Invocation: The SN may update the TMUI at registration, location update, or service attempts.

Mechanism: The SN updates or assigns a TMUI to a MS, using an encrypted signalling channel. On successive identification or paging requests the MS is identified by the TMUI.

Requisites: The feature relies on the confidentiality and data integrity of data stored in the USIM (IMUI, TMUI) and the VLR (IMUI, TMUI) and the confidentiality of signalling data transmitted between SN and MS (TMUI).

5.2.6 Indication of ciphering

Security Services: Indication of ciphering informs the user whether the confidentiality of his user data is ensured.

Assumptions: The UE implements at least one ciphering algorithm.

Involved entities: UE.

Invocation: The feature shall be invoked by the UE after receipt and subsequent verification of the data integrity and origin by the USIM of the "security mode command."

Mechanism: No standardisation of a security mechanism is required beyond that required for the verification of the data integrity of signalling messages.

Requisites: The feature relies on the data integrity of data stored in the UE (the program code that implements the Indication of ciphering).

5.3 Data integrity and origin authentication of transmitted data

5.3.1 Integrity algorithm agreement

Security Services: Integrity algorithm agreement allows the SN and the MS to agree on the integrity algorithm they will use.

Assumptions: One or more integrity algorithms are standardised. The USIM and the MSC/VLR store their respective integrity capabilities in a standardised format.

Involved entities: MSC/VLR (stores the SN integrity capabilities, decides on an integrity mode) and the USIM (verifies the integrity mode is acceptable).

Invocation: At first registrations, the MS shall start the full negotiation by sending the MS capabilities to the SN. At subsequent registrations, call set-ups and location updates, the MS may be requested by the SN to retransmit its MS capabilities. At current registrations, call set-up and location update, the SN shall send security mode command such that the SN can control the security mode on a per-call basis.

Mechanism: The MS sends its integrity capabilities and preferences as they are stored on the USIM, as a part of the MS capabilities, to the SN. Upon receipt of the MS capabilities, the SN decides on an integrity algorithm to use. It then sends the chosen integrity mode as part of the security mode command to the MS. The MS verifies the data integrity and origin of the received security mode command and checks whether the proposed integrity mode

- is available in the USIM;
- is acceptable according to the user’s service profile;
- is conform to the user’s preferences according to its service profile and information sent by the HE to the MS, as part of the authentication tokens, on the integrity capabilities of the SN.

After establishment of a DIK, the MS computes a MAC on the MS capabilities and sends it to the SN. The SN verifies the data integrity and origin of the previously received MS capabilities message.

Requisites: The feature relies on the data integrity of data stored in the UE (integrity capabilities) and data integrity and origin authentication of signalling elements transmitted between MS and SN (MS capabilities, cipher mode command).

5.3.2 Establishment of a derived integrity key

Security Services: Establishment of a derived integrity key provide the MS and the SN with a secret DIK to ensure the data integrity and origin authentication of signalling data transmitted between MS and SN, with freshness guarantees to the user.

Assumptions: This feature is integrated with user-to-network authentication and network-to-user authentication.

Involved entities: USIM (derivation of DIK), VLR (storage of DIK), HLR (derivation of DIK).

Invocation: The establishment of a new derived integrity key is integrated in the mechanism for user-to-network and network-to-user authentication and key establishment.

Mechanism: The HE generates a fresh challenge and computes the DIK from the challenge and the user's PAK. The HE then computes an authentication token that consists of a fresh sequence number, and a MAC on the sequence number and the challenge. The user trusts the HE to generate a fresh challenge with a fresh sequence number. The HE sends the challenge, the authentication token and the DIK to the SN. The SN forwards the challenge and the authentication token to the MS. The MS verifies the data integrity and origin of the challenge and the sequence number and the freshness of the sequence number and therefor also the freshness of the challenge. The MS then computes the fresh DIK from the fresh challenge.

Mechanism: The MS and the HE compute the DIK from the challenge generated by the HE. The HE sends the DIK to the SN.

Requisites: The feature relies on the data integrity of data stored in the USIM (DIK), VLR (DIK) and the confidentiality of signalling data transmitted between HLR and VLR (DIK).

5.3.3 Data integrity and origin authentication of signalling elements

Security Services: Data integrity and origin authentication of signalling elements provides the SN and the MS the ability to verify the data integrity and origin of certain signalling elements exchanged over the radio access link.

Assumptions: MS and SN have established a DIK using the security feature "Establishment of a derived integrity key".

Involved entities: USIM (computation of the MAC, storage DIK), MSC/VLR (computation of the MAC, storage DIK).

Invocation: The feature shall be applied on the following signalling elements sent by the MS to the SN:

- The MS capabilities, including authentication mechanism, ciphering and integrity capabilities.
- The security mode accept/reject message.
- The called party number in a mobile originated call.
- Periodic message authentication messages.

The feature shall be applied on the following signalling elements sent by the SN to the MS:

- The security mode command, including whether ciphering is enabled or not and the ciphering and integrity algorithm to be used.
- Periodic message authentication messages.

Mechanism: Data integrity and origin authentication will be implemented by a MAC appended to a message and computed from that message using a DIK that is established previously between the SN and the MS. The computation of the MAC will occur in the USIM in the MS, and in the MSC/VLR in the SN.

Requisites: The feature relies on the data integrity of data stored in the USIM (DIK) and the MSC/VLR (DIK).

NOTE: The allocation of the integrity functionality to the USIM and the MSC/VLR is provisional and open for further study.

Annex A (informative): Requisites for the security features

A.1 Confidentiality and data integrity of stored data

The security features in clause 5 and some of the security requirements in UMTS 33.21: "Universal Mobile Telecommunications System (UMTS): Security Requirements" require confidentiality and/or data integrity of data stored in network elements. The data elements that require protection are listed for each network element:

USIM: authentication mechanism capabilities, PAK, TUAK, Temporary Network Authentication Key (TNAK), user authentication data, a secret value for authentication towards the UE, the Partial Derived Cipher Key (PDCK), the Partial Derived Integrity Key (PDIK), IMUI, TMUI, user-related data;

UE: Ciphering capabilities, DCK, DIK, IMEI, secret value for USIM-to-UE authentication, user-related data;

RNC: DCK, DIK;

MSC/VLR: Authentication capabilities, ciphering capabilities, TUAK, TNAK, DCK, DIK, PDCK, PDIK, TMUI, IMUI, challenge-response pairs, network authentication tokens, user-related data;

HLR/AuC should be exercised on: PAK, TUAK, TNAK, DCK, DIK, PDCK, PDIK, challenge-response pairs, network authentication tokens, user-related data.

A.2 Security features related to communication between providers

The security features in clause 5 and some of the security requirements in UMTS 33.21: "Universal Mobile Telecommunications System (UMTS): Security Requirements" require confidentiality and/or data integrity of data transmitted between HE and SN in the wireline network. These security features are outside the scope of this specification.

The data elements that require protection are: temporary authentication keys, (partial) derived cipher keys, (partial) derived integrity keys, challenge-expected response pairs and user-related data.

Annex B (informative): Network security features

B.1 Access control to stored data in a provider database

Security services: Access control to stored data in a provider database ensures the data integrity and/or confidentiality of data stored in a SN or HE database.

Assumptions: Access is granted after successful authentication of the accessing entity or application towards the provider database and verification that the authenticated entity or application has the appropriate access rights for that data element and for the attempted action.

Involved entities: Provider database, accessing entity or application

Invocation: The feature is invoked by the provider database when an entity or an application attempts to access data stored in the SN or HE, or when data is downloaded to the SN or HE.

Mechanism: FFS.

Requisites: FFS.

B.2 Entity authentication between providers

Security services: Entity authentication between providers allows providers to corroborate each other's identity.

Assumptions: A single mechanism shall be standardised.

Involved entities: Provider entities

Invocation: The feature is invoked by the provider when an entity or an application attempts to access data stored in the provider database, or when data is downloaded to the provider database. It may also be invoked in the even of the automatic establishment of roaming agreements.

Mechanism: FFS.

Requisites: FFS.

B.3 Data integrity and origin authentication of signalling and control data

Security services: Data integrity and origin authentication of signalling data ensures the data integrity and origin authentication of data exchanged between provider domains.

Assumptions: A single mechanism shall be standardised.

Involved entities: Provider entities

Invocation: The feature may or shall be invoked on the transfer of signalling and control traffic between network domains.

Mechanism: FFS.

Requisites: FFS.

B.4 Confidentiality of signalling and control data

Security services: Confidentiality of signalling and control data prevents eavesdropping of signalling and control data when transmitted between provider domains.

Assumptions: A single mechanism shall be standardised.

Involved entities: Provider entities

Invocation: The feature may or shall be invoked on the transfer of user-related signalling and control traffic between network domains.

Mechanism: FFS.

Requisites: FFS.

Annex C (informative): Alternative mechanisms for authentication and key establishment

C.1 User-to-network authentication

Security Services: User-to-network authentication allows the SN to corroborate the IMUI of the MS.

Assumptions: For new registrations the MS and the HE share a secret PAK. For current registrations, in addition, the MS and the SN share a Temporary Authentication Key (TAK).

Invocation: The SN shall invoke the user-to-network authentication mechanism for new registration at first registration of a MS in a SN and may invoke the mechanism for new or current registration on location update or service requests, according to the agreement with the user's HE.

Involved entities: Current registrations: USIM (computation of user response, generation of user nonce), MSC/VLR (generation of network challenge, computation of expected user response, verification of user response). In addition, for new registrations: USIM (generation of user nonce, derivation of TUAK), HLR/AuC (generation of network nonce, derivation of TUAK).

Mechanism 1: Establishment of the temporary user authentication key. The MS sends the HE a user nonce. HE generates a network nonce. MS and HE compute the TUAK from both nonces and the PAK. The HE sends the TUAK and the network nonce to the SN, which forwards the network nonce to the user upon the first user-to-network authentication.

Mechanism 2: User-to-network authentication. The SN generates a challenge and computes the expected response from the TUAK and sends the challenge to the MS. The MS computes the response and sends it to the SN. The SN compares the received response with the expected response.

Requisites: The feature relies on the confidentiality and data integrity of data stored in the USIM (PAK, TUAK), MSC/VLR (TUAK) and HLR/AuC (PAK) and confidentiality and data integrity and origin authentication of signalling elements transmitted between MSC/VLR and HLR/AuC (TUAK).

C.2 Network-to-user authentication

Security Services: Network-to-user authentication allows the MS to verify that the SN is authorised to provide the user services on behalf of the user's HE.

Assumptions: The MS and the HE share a PAK.

Invocation: The SN shall invoke network-to-user authentication at first registration, location update and may or shall invoke the feature at service requests, according to the agreement with the user's HE.

Involved entities: USIM (derivation of TNAK, generation of challenge, derivation of expected response, verification of network response), MSC/VLR (computation of network responses), HLR/AuC (derivation of TNAK).

Mechanism 1: Establishment of a TNAK. The MS sends the HE a user nonce. HE and MS compute a TNAK from the user nonce and the PAK. The HE sends the TNAK to the SN.

Mechanism 2: Network-to-user authentication. The MS generates a challenge and computes the expected response from the TNAK and sends the challenge to the SN. The SN computes the response and sends it to the MS. The MS compares the received response with the expected response.

Requisites: This feature relies on the confidentiality and data integrity of data stored in the USIM (PAK, TNAK), VLR (TNAK) and HLR (PAK) and confidentiality and data integrity and origin authentication of signalling data transmitted between HLR and VLR (TNAK).

C.3 Establishment of a derived cipher key

Security Services: Establishment of a derived cipher key provide the MS and the SN with a secret cipher key to prevent eavesdropping on user and signalling data, with freshness guarantees towards the MS and the SN.

Assumptions: This feature is integrated with user-to-network authentication and network-to-user authentication.

Involved entities: USIM and MSC/VLR (derivation of the DCK), UE and RNC (subsequent use and storage of the DCK).

Invocation: The establishment of a new DCK is integrated in the mechanism for user-to-network and network-to-user authentication and key establishment.

Mechanism: The SN and the MS compute the DCK from the user challenge, the network challenge, the TNAK and the TUAK.

Note: Is there still a need for two temporary keys, as the protocol has been changed and network-to-user authentication has been removed?

Requisites: The feature relies on the data integrity of data stored in the USIM (TUAK, TNAK), UE (DCK), RNC (DCK), MSC (TNAK, TUAK).

C.4 Establishment of a derived integrity key

Security Services: Establishment of a DIK provide the MS and the SN with a secret derived integrity key to ensure data integrity and origin authentication on signalling data sent over the radio access link.

Assumptions: This feature is integrated with user-to-network authentication and network-to-user authentication.

Involved entities: USIM and MSC/VLR (derivation and storage of the DIK).

Invocation: The establishment of a DIK is integrated in the mechanism for user-to-network and network-to-user authentication and key establishment.

Mechanism: The SN and the MS compute the DIK from the user challenge, the network challenge, the TNAK and the TUAK.

Requisites: The feature relies on the data integrity of data stored in the USIM and VLR (TNAK, TUAK).

Annex D (informative): Status of UMTS 33.22

Status of Technical Specification UMTS 33.22 "Security features"		
Version	**Date**	**Comments**
0.1.0	April 1998	First version based on material in UMTS 33.20.
0.2.0	September 1998	Addition of security feature descriptions (by Stefan Pütz)
0.2.3	October 1998	Move of the security feature descriptions to the appendix and addition of security features (by Stefan Pütz).
0.2.4	November 1998	Revision in view of the discussion and comments at the SMG10-WPC meeting in Borehamwood.
0.2.5	November 1998	Revision in view of the comments received during the SMG10-WPC meeting in Paris, including the creation of an appendix on network security and the transfer of all network security features to that appendix; the removal of the feature "Control of user access to UE," and minor editorial changes.
0.3.0	January 1999	Revision in view of the comments received during the SMG10-WPC meeting and addition of detail on the mechanisms that are proposed.
0.3.1	January 1999	Revision in view of the comments received during SMG10-WPC meeting in Newbury, i.e., removal of all but one version of the authentication and key establishment mechanisms from the main body of the specification, and creation of an informative appendix with an alternative proposal. Introduction of a feature "integrity algorithm agreement," and the reduction of the possible mechanisms to two options
0.3.2	January 1999	Revision in view of minor comments from SMG10-WPC members.
1.0.0	February 1999	specification to SMG#28 for information
Text and figures: WinWord 6.0 **Stylesheet**: etsiw_70.dot **Rapporteur**: Bart Vinck (Siemens Atea)		