3GPP TSG SA WG3 Security — S3#15
12-14 September, 2000
Washington D.C., USA

S3-000553

3G TR 33.cde V0.1~~0~~.0 (2000-09~~8~~)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group <Name>;
Access security for IP-based services
(Release 2000)

Keywords

Access security, IP Multimedia

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Copyright Notification

Contents

Foreword ... 4
Introduction ... 4
1 Scope ... 5
2 References ... 5
2.1 Normative references ... 5
2.2 Informative references ... 5
3 Definitions, symbols and abbreviations ... 6
3.1 Definitions ... 6
3.2 Symbols ... 6
3.3 Abbreviations ... 6
4 Requirements ... 7
5 Security architecture ... 8
6 Security features ... 10
7 Secure access ... 10
7.1 User identity confidentiality ... 10
7.2 Entity authentication ... 10
7.3 Confidentiality ... 11
7.4 Data integrity ... 12
7.5 Visibility and configurability ... 12
8 Security mechanisms ... 13
8.1 Authentication and key agreement ... 13
8.2 Access confidentiality ... 14
8.3 Access integrity ... 14
Annex <A> (normative): <Normative annex title> ... 15
Annex <X> (informative): Change history ... 16

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

IP-based services in UMTS Release 00 are services for which user data as well as signalling data are transmitted as IP packets in the UMTS user plane. An example for such a service is the provision of IP-based multimedia (IM) services in the IM domain of UMTS. It was decided by 3GPP to use the Session Initiation Protocol (SIP) [RFC 2543] as signalling protocol for the UMTS IM domain. The SIP messages will be carried in the user plane of the PS domain.

UMTS Release '99 security will be re-used in UMTS Release '00 to provide security at the bearer level. The confidentiality mechanism is the only mechanism which provides protection of the user plane, but its use is only optional. Only the signalling plane provides mandatory integrity. This means that the signalling for IP-based services does not enjoy the same level of protection as the signalling for other services which for carried in the signalling plane unless additional measures are specified.

The use of only bearer level security to protect the IP-based services may also prove problematic for two other reasons: one reason is that, according to the UMTS R’00 architecture principles, signalling for the IM-domain should be access network independent. Another reason is that bearer level security as specified in R’99 does not extend far enough into the core network. In R’99, only the radio access (up to the RNC) is protected. In the IM domain it may be required to extend protection of IM signalling data up to the proxy/serving CSCF (Call State Control Function) in the core network. For IM user data, which is not routed via the CSCF further protection, measures may be required.

1 Scope

The scope for this technical report is to define the requirements, functions and solutions for secure access to the IM CN subsystem for the 3G mobile telecommunication system. The TR focuses on new or modified functionality as compared to R99 and technical description of the features, functions and solutions of R00.

This TR will act as a basis for the detailed Stage 2 specification work. Note that this is not a specification i.e. everything in this document may be changed at any time.

This TR is based on the contributions presented and approved at the SA meetings, see [3]-[6].

According to the WI "Access security for IP-based services" the objectives and the corresponding time plan are:

- Objectives:

  "The objective with this WI is to solve the security aspects that are related to secure access for the new IP Multimedia services, IM services in R00. The IM services will include different applications like voice, video and data. The trustrelations and the security services between the end-user, the IM CN subsystem, the PS-domain and the CS-domain shall be defined. Also the mechanisms for registration/authentication of a roaming/non-roaming end-user making registration to the IM CN subsystem using SIP will be treated in this WI. This shall include the definition of the needed encryption and integrity mechanisms for protection of the control plane and the user plane. The evolution and/or reuse of the existing R99 architecture for authentication and key agreement shall be considered."

- Timeplan:
  - August 2000, SA3#14 Requirements capture
  - September 2000, SA3#15 Security feature specification
  - ….
  - June 2001 CRs approved at TSG level

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.

2.1 Normative references

[1] 3G TS 33.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture".

[2] 3G TR 23.821: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Architecture principles for Release 2000".

2.2 Informative references

[3] S3-000446 (Siemens): "Requirements on access security for IP-based services "

[4] S3-000447 (Siemens): “Overview of security mechanisms for access security for IP-based services”

[5] S3-000456 (Nokia): “UMTS AKA in SIP”

[6] S3-000458 (Nortel): “Security requirements for access to R’00 IM subsystem”

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and 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.

3.2 Symbols

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

3.3 Abbreviations

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

AAA	Authentication Authorisation Accounting
AKA	Authentication and key agreement
CS	Circuit Switched
CSCF	Call State Control Function
GGSN	Gateway GPRS Support Node
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IM	IP Multimedia
MAC	Message Authentication Code
ME	Mobile Equipment
MGCF	Media Gateway Control Function
MS	Mobile Station
MSC	Mobile Services Switching Centre
PS	Packet Switched
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
UE	User Equipment
UICC	UMTS IC Card
USIM	User Services Identity Module
VLR	Visitor Location Register

4 Requirements

In this section some important requirements that will or may affect the security solutions for R'00 are listed.

For access to IP-based services at least the same level of protection shall be provided as for access to services provided in the CS- and PS-domains.

The limits of processing power, storage capacity of a UICC and the bandwidth on the UICC-UE interface have to be taken into account in the selection of mechanisms. Note that these limits are not a priori fixed, but can be extended e.g. by the use of more expensive HW (e.g. use of smart card crypto co-processors).

The air interface has limitations on the bandwidth and is error prone. This may have effects on the delay and failure rate of security procedures.

Any security solution must be scalable to accommodate a very large user base (up to one billion).
Any security solution must support global roaming, i.e. a user must be able to get access to a serving system without previous contact between the user and the serving system.

In the past there has been a trust relationship between the voice client in the GSM terminal and the GSM network providing the service. In the more open Internet environment software clients can be developed extremely easily e.g. on home computers. This opens the possibility for rogue or badly written applications to threaten the integrity of the network. Therefore, it essential that firewalls and policing functions are installed in the network to protect against virus attacks and rogue software client. This would be inline with the internet model on which the IM CN subsystem is being built, and would not run the risk of what could happen if the trust relationships are broken.

Referring to [2] R'00 shall comply with the following requirements:

- In order to achieve access independence and to maintain a smooth interoperation with wireline terminals across the Internet, it is important to be conformant to IETF "Internet standards". Therefore, R00 shall, as far as possible, conform to IETF "Internet standards" for the cases where an IETF protocol has been selected, e.g. SIP.

- **Independence of access technology:** The GSM/UMTS reference architecture shall be designed to ensure that a common core network can be used with multiple wireless and wireline access technologies (e.g. xDSL, Cable, Wireless LAN, Digital Broadcast, all IMT2000 radio access technologies).

- **Support of Service Requirements:** The GSM/UMTS reference architecture shall include mechanisms for operators and third-parties to rapidly develop and provide services and for users to customise their service profile.

- **Support of regulatory requirements:** The GSM/UMTS reference architecture shall include features to support regulatory requirements such as legal intercept, number portability, other regional requirements. To all terminal types and communication type (CS and PS) as appropriate.

- The Cx reference point, see Figure 1, shall support the transfer of *CSCF-UE security parameters* from HSS to CSCF, unless SA3 defines a different method to support a secure association between UE and CSCF.

    - This allows the CSCF and the subscriber to communicate in a trusted and secure way (there is no à priori trust relationship between a subscriber and a CSCF)

    - The security parameters can be for example pre-calculated challenge-response pairs, or keys for an authentication algorithm, etc.

- The UE and HSS may need to exchange information that is transparent to CSCF, for example activation or modification of supplementary services. The CSCF may forward this information between UE and HSS, and the Cx reference point shall support tunnelling of this information between CSCF and HSS.

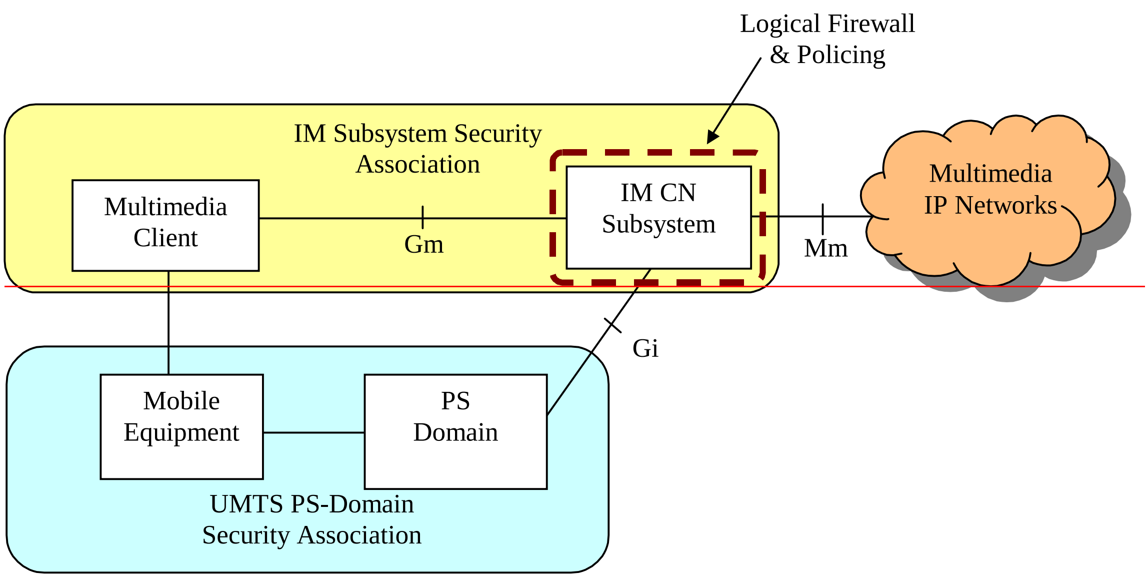
- HSS is responsible for holding the following user related information:

- User Identification, Numbering and addressing information.
- User Security information: Network access control information for authentication and authorization
- User Location information at inter-system level; HSS handles the user registration, and stores inter-system location information, etc.
- The User profile (services, service specific information…)
- Based on this information, the HSS is also responsible of supporting the CC/SM entities of the different control systems (CS Domain control, PS Domain control, IP Multimedia control…) offered by the operator.

[Editors note: At what interface shall legal interception take place? Maybe it can take place at the GGSN and the Gi reference point?]

5 Security architecture

In the PS domain, service is not provided until a security association is established between the mobile equipment and the network. IM CN subsystem is essentially an overlay to the PS-Domain and is not embedded in the SGSN or GGSN nodes consequently a second security association is required between the multimedia client and IM CN subsystem before access is granted to multimedia services. The IM CN Subsystem Security Architecture is shown in the following figure.



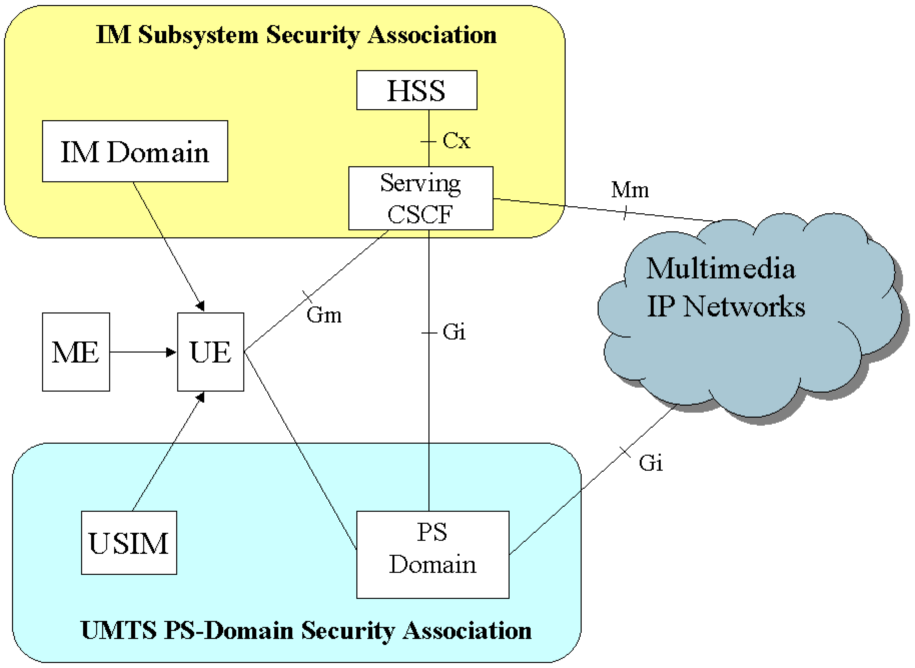


Figure 1IM CN Subsystem Security Architecture. Note that not all interfaces are covered in this figure for a more detailed overview cf. [2].

[Editor's note: the final approval of Figure 1 and related text is dependent on the R00 requirements~~. Amongst other things mobile equipment should be changed to user equipment.~~ At what interface legal interception shall take place has not yet been analysed. One option is to do it on the Gi interface at the GGSN. Furthermore it is a requirement in [2] that the Cx reference point shall support tunnelling information that is exchanged between UE and HSS and forwarded transparently by the serving CSCF. Shall this WI take care of security issues related to this tunnelling feature?]

A requirement of 3GPP is the consideration of access independence, which opens the possibility in future releases for a multimedia client to access the IM CN Subsystem via alternative access technologies e.g. xDSL, Cable Wireless. Therefore, it is essential that the IM CN Subsystem Security does not rely on the security provided by the PS-Domain and provides a smooth evolution path that would allow access via alternative access technologies. In addition, the IM CN subsystem security mechanism shall be consistent with security techniques employed in the Internet as this likely to be the termination point of the majority of traffic.

An independent IM CN Subsystem security mechanism provides additional protection against security breaches. For example, if the PS-Domain security is breached the IM CN Subsystem would continue to be protected by it's own security mechanism.

6 Security features

- Secure storage of long-term keys

Long-term secret keying material for the protection of access to IP-based services shall be stored in only two types of security entities in the system. On the user side on a tamper-resistant HW module ~~(the UICC)~~ and on the network side in ~~an Authentication Centre~~ an IP Multimedia authentication server which is part of the HSS.

- Secure storage and execution of cryptographic algorithms

All algorithms using long-term keys shall be executed on the same security entities on which the long-term keys are stored~~, i.e. the UICC and the Authentication Centre~~.

- Transfer of session keys, storage and execution

The session keys for integrity and confidentiality may be transferred from ~~the USIM~~ a secure storage to an insecure storage in the ~~UE~~ ME where the integrity and confidentiality algorithms may be performed.

7 Secure access

7.1 User identity confidentiality

A user to whom IM services ~~are~~ is delivered needs to have a permanent identity for the IM domain. ~~This identity or other data from which this identity may be derived or which may allow to trace the user or to derive his location (e.g. the IP address of the UE) shall not be disclosed.~~ This unique ID known by the multimedia domain part of e.g. the UICC and the HSS shall not be disclosed. The subscriber shall have a public address which relation with the unique ID is only known by the MM domain part of e.g. the UICC and HSS. Furthermore when applicable the relation between the IMSI and the unique ID used for IM domain registration shall be hidden.

The user identity may be protected by PS domain confidentiality where it is available. Core network interfaces not contained in the PS domain need to be considered separately.

Other data e.g. the IP address of the UE shall not reveal the location of the subscriber.

[Editors Note: The use of DNS names, NAI, SIP URL etc for application level registration is FFS in S2 referring to [2].]

7.2 Entity authentication

~~□Mutual authentication and key agreement between a (roaming) user and the IM CN subsystem~~

~~**Need for three-party AKA protocol:** When a (roaming) user registers in the IM domain it has to be assured that the serving IM CN subsystem corroborates the IM identity of the user. Furthermore the user also has to be assured that user is connected to a serving IM CN subsystem that is authorised by the user's HSS to provide IM services to him. Therefore an authentication mechanism is needed which involves three entities: UE, HSS of the user and the serving CSCF. In addition, in the course of the authentication process keys have to be agreed which can be used for the subsequent integrity and confidentiality protection of IM signalling/user data.~~

~~The suggested working assumption is to perform an AKA in the IM domain. This will assure that the requirement that the IM CN subsystem shall be access network independent is fulfilled.~~

R'00 architecture is based on the principle that the Home network designates the service control for a roaming subscriber. Since there is a requirement for access independence one option for authentication could be based on AKA mechanisms defined in R'99, see [1].

The entities that need to be authenticated mutually are the UE, the serving CSCF and the HSS. The serving CSCF will get subscriber data from the HSS that shall not be disclosed. Note that the serving CSCF for a roaming user may, depending on the policy of the home network operator, be located in the visited network.

[Editors Note: Do we need to authenticate the Proxy CSCF?]

The following features are provided:

1. Authentication mechanism agreement i.e. the user and the serving CSCF negotiates what authentication algorithm and authentication key they shall use

2. User authentication i.e. the serving CSCF verifies the identity of the user

3. Serving CSCF authentication i.e. the user verifies that the HSS of the home network has a trust relationship with the serving CSCF

The protocol applied on the Gm reference point is the IETF protocol SIP defined in RFC 2543. SIP uses either the basic authentication scheme or the digest access authentication scheme. Since there already exist a relationship between the UE, i.e. the user (USIM), and the HSS (HLR) it is advantageous to introduce the AKA mode in SIP. This mode shall be generic in its design such that it follows the principal ideas of IETF (i.e. it shall not be a unique mode only allocated for AKA).

A new domain designated for the multimedia access shall be defined e.g. in the UICC with the same authentication data as in the USIM but they will take separate values. Hence unique session keys (CK, IK etc) will be derived for the IP multimedia domain.

7.3 Confidentiality

~~□Confidentiality of IM signalling data between UE and CSCF~~

~~There are two alternatives to provide the required confidentiality~~

~~1.hop-by-hop or~~

~~2.end-to-end between the UE and the CSCF.~~

~~Similar considerations as in 5.1.4 apply.~~

~~The suggested **working assumption** is end-to-end protection between the UE and the CSCF.~~

~~□Confidentiality of IM user data~~

~~It clearly is a requirement that user data for services in the IM domain enjoy the same degree of protection as user data for services in the PS or CS domain. The situation differs from that for signalling data in that IM user data originating from the UE do not necessarily pass through any node (such as the CSCF for IM signalling data) specific to the IM domain. E.g. in the case of a UMTS IM user communicating with a SIP user in the Internet, the IM user data will pass from the GGSN straight into the Internet. Therefore, IM domain specific protection does not seem possible in the general case. What remains is, on the one hand, end-to-end protection between users and, on the other hand, protection provided in the PS user plane. End-to-end protection between users is out of scope for the work item "access security for IP-based services".~~

~~The suggested **working assumption** therefore is that no additional measures need to be provided.~~

All SIP signalling data will be carried in the user plane from a GPRS perspective. The SIP signalling data may be confidentiality protected end-to-end between the UE and serving CSCF (this is an option). The payload may get some protection on the underlying layers e.g. by IPSec.

The features that are provided end-to-end between the UE and the serving CSCF are cipher algorithm agreement, cipher key agreement and confidentiality of the signalling data (as an option).

[Editors Note: The main idea is that only SIP signalling data will get protection between the UE and the serving CSCF and that the user data, e.g. UE-UE, is (if necessary) protected by the application and should then not be included in this WI. The constraint for this is however that it does not exist any kind of dependency between them.]

7.4 Data integrity

~~There are two alternatives to provide the required integrity~~

~~1.hop-by-hop or~~

~~2.end-to-end between the UE and the CSCF~~

~~□Hop-by-hop protection would require integrity protection of the following hops in the user plane of the PS domain.:~~

~~□UE-RNC: This is not available in UMTS R'99, but may be available in R'00 as there is a corresponding work item. Note, however, that concerns have been raised that such protection may adversely affect Quality of Service for certain services.~~

~~□RNC-SGSN: This is not available in UMTS R'99, but may be available in R'00 as there is a corresponding work item.~~

~~□SGSN-GGSN: This is not available in UMTS R'99, but will may available in R'00 (GTP security).~~

~~In addition, the hop GGSN-CSCF has to be protected which is outside the PS domain.~~

~~Whether hop-by-hop protection is sufficient for the protection of the IM domain depends on the availability of the protection on the individual hops, the assumptions on the vulnerability of the intermediate nodes and the trust relationship between the IM domain and the PS domain. Note also that this alternative would not be compatible with the requirement that the IM-domain be access network independent.~~

~~The suggested **working assumption** therefore is end-to-end protection between the UE and the CSCF.~~

All SIP signalling data will be carried in the user plane from a GPRS perspective. The SIP signalling data shall be integrity protected end-to-end between the UE and serving CSCF. The payload may get some protection on the underlying layers e.g. by IPSec.

The features that are provided end-to-end between the UE and the serving CSCF are integrity algorithm agreement, MAC key agreement and integrity of the signalling data.

[Editors Note: The main idea is that only SIP signalling data will get protection between the UE and the serving CSCF and that the user data, e.g. UE-UE, is(if necessary) protected by the application and should then not be included in this WI. The constraint for this is however that it does not exist any kind of dependency between them.]

7.5 Visibility and configurability

[Editor's note:

Following features related to multimedia services shall be visible and/or configurable to the user:

- *Access encryption*
- *Level of security (access security and multimedia security)*
- *Accepting/rejecting non-ciphered multimedia sessions*
- *Accepting/rejecting the use of different security level*
- *Etc]*

8 Security mechanisms

8.1 Authentication and key agreement

The working assumption to perform a UMTS AKA through the SIP Protocol is:

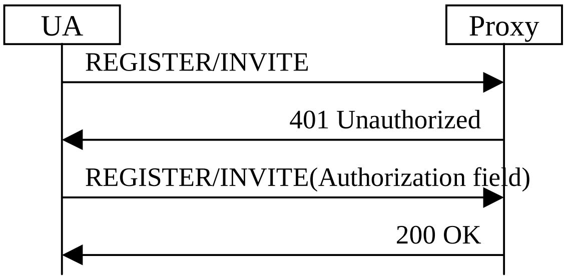
- Since three different authentication mechanisms (HTTP basic mode, HTTP digest mode, PGP) have already been defined for SIP, a new authentication mode, a UMTS AKA mode, with the necessary fields, could be defined.

Procedure

According to the security policies, when an UMTS AKA needs to be performed (e.g. at a call set up, or at registration), the User Agent - UA sends a REGISTER or INVITE request to the proxy; the SIP proxy then asks for an authentication with a 401 Unauthorised response. This 401 response includes the WWW-Authenticate response header field which contains the UMTS AKA authentication vectors i.e. the random challenge (RAND) and the authentication token (AUTN).

[Editors note: A multimedia domain shall be defined e.g. in the UICC such that it is possible to distinguish between the CS-domain, PS-domain and the multimedia domain.]

After a 401 response, the UA sends a new REGISTER or INVITE request which should contain the appropriate authentication information in the Authorisation header field: the authentication response (RES), the synchronisation failure parameter (AUTS) or an error code.



For a call set-up, the 407 Proxy Authentication Required Response can also be used to carry the UMTS AKA Parameters.

- **Working assumption:**

Definition of a new authentication mode

This solution introduces a new authentication mode. It tries to keep the headers as short as possible since the SIP messages are going through the air interface.

WWW-Authenticate response header

The WWW-Authenticate response header in the case of UMTS AKA mechanism must be able to carry the random challenge (RAND) and the authentication token (AUTN). The following simple format can be used:

WWW-Authenticate = " WWW-Authenticate" ":" "UMTS" RAND AUTN
RAND = "RAND" "=" RAND-value
AUTN = "AUTN" "=" AUTN-value

The hexadecimal format is proposed for the AUTN and RAND value.

Authorisation header

The Authorisation header in the case of UMTS AKA mechanism must be able to carry the user authentication response (RES) value or the authentication synchronisation parameter (AUTS) value. The following simple format can enough for this purpose:

Authorisation = "Authorisation" ":" "UMTS" RES | AUTS | AUTH-REJECT
RES = "RES" "=" RES-value
AUTS = "AUTS" "=" AUTS-value
AUTH-REJECT = " AUTH-REJECT" "=" error-code

The hexadecimal format is proposed for the RES and AUTS value. The possible value of the error-code is FFS.

Pros:

Specific to UMTS AKA

Necessary fields can be present (format, length)

Cons:

Difficult to have a new mode defined in IETF

8.2 Access confidentiality

[Editor’s note: This section shall deal with cipher algorithms, key length etc for the control plane and the user plane]

8.3 Access integrity

[Editor’s note: This section shall deal with integrity algorithms, key length etc for the control plane and the user plane]

Annexes are only to be used where appropriate:

Annex <A> (normative): <Normative annex title>

Annex <X> (informative): Change history

It is usual to include an annex (usually the final annex of the document) for specifications under TSG change control which details the change history of the specification using a table as follows:

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**