3G TR 33.8xx V0.~~2~~3.0 (2000-~~10~~11)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group ~~<Name>;~~SA3
Access security for IP-based services
(Release ~~20000~~5)

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

Contents

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) [15] 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".

2.2Informative 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”

[7] S3-000561 (Siemens) “Proposed changes and discussion of open issues for draft 3G TR "Access security for IP-based services”

[8] S3-000588 (Nokia) “Authentication and key agreement in IM CN subsystem”

[9] S3-000625 (Ericsson) “Protection between the UE and the serving CSCF”

[10] IETF RFC 2246 (1999) “The TLS Protocol Version 1.0”

[11] IETF RFC 2402 (1998) “IP Authentication Header”

[12] IETF RFC 2406 (1998) “IP Encapsulating Security Payload (ESP)”

[13] IETF RFC 2409 (1998) “The Internet Key Exchange (IKE)”

[14] IETF RFC 2440 (1998) “Open PGP Message Format”

[15] IETF RFC 2543bis-01 (2000) “SIP: Session Initiation Protocol”

[16] IETF RFC 2617 (1999) “HTTP Authentication: Basic and Digest Access Authentication”

[17] S3z000010 (Ericsson) “Authentication and protection mechanisms for IM CN SS”

[18] 3G TR 23.228: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; IP Multimedia (IM) Subsystem-Stage 2"

[19] S3z000022 (Siemens) “IMS authentication and integrity/confidentiality protection”

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.

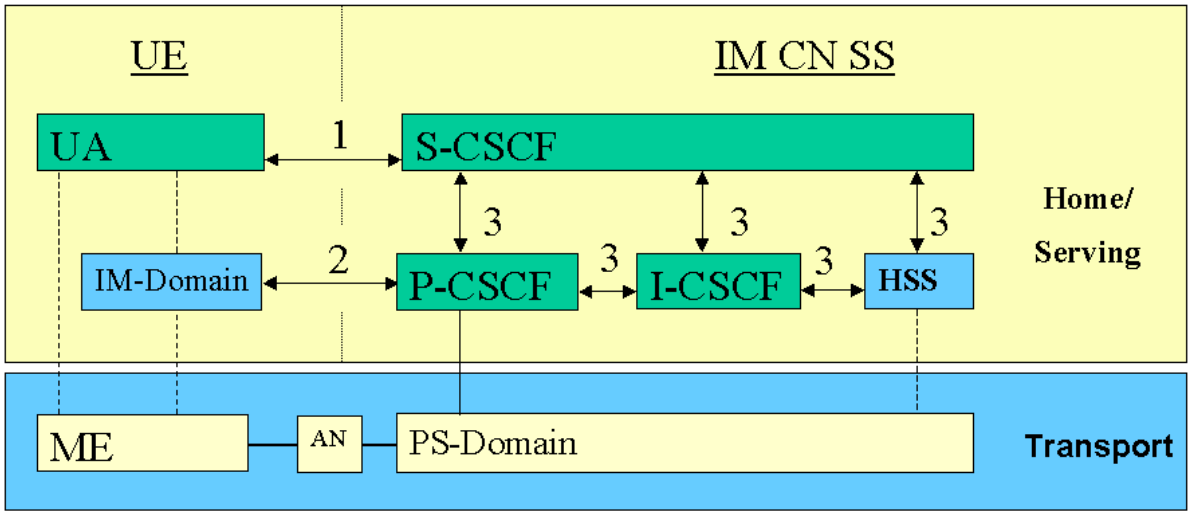


Figure 1IM CN Subsystem Security Architecture. Note that not all interfaces are covered in this figure for a more detailed overview cf. [2].

[Editor's note: the final approval of Figure 1 and related text is dependent on the R00 requirements 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?]

There are three different security associations and different need for security protection for IM CN SS and they are numbered 1,2 and 3 in figure 1 where:

1. Provides secure access to IM services

2. Provides a secure link and a security association between the UE and a P-CSCF

3. Provides security in the network domain; intra domain security and/or inter domain security

Mutual authentication is required between the IM-Domain and the HSS.

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 should be as far as possible 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 and on the network side in 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.

– Transfer of session keys, storage and execution

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

7 Secure access

[Editors Note: Several changes have to be made in this chapter. The changes are dependent on the final decisions in S3 on how the security architecture shall look like cf. the open issues in chapter 9.]

7.1 User identity confidentiality

A user to whom IM services is delivered needs to have a permanent identity for the IM domain. 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

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? There are two alternatives where authentication should take place cf. chapter 9.]

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 [15]. 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

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 a ~~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~~a 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

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: There are two alternatives for in which node the integrity protection shall terminate cf. chapter 9.]

[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:

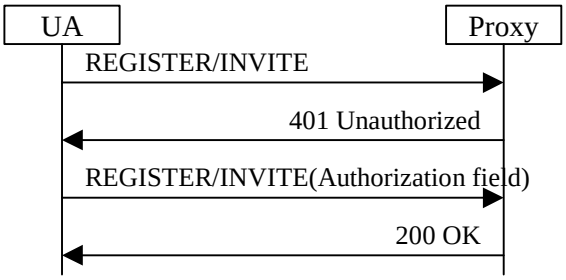
– Since three different authentication mechanisms (HTTP basic mode, HTTP digest mode, PGP) have already been defined for SIP, a new authentication mode, a UMTS AKA mode, with the necessary fields, could be defined.

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.

[Editors note: the session keys for access confidentiality and integrity have to be derived on UA and on proxy side.]

– **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~~]

9 Open Issues

9.1 Open issues in section 8.1

The section contains the description how the UMTS AKA can be performed through the SIP protocol by introducing a new authentication mode for SIP. For the further development of the proposal some issues to be considered are raised below. Section 8.1 only describes the exchange of the crypto-messages for the UMTS AKA.

9.1.1 User identity

~~□~~It ~~additionally~~ has to be clarified by which identity a user is authenticated. It is proposed to authenticate a user by his unique user identity in the IM domain (the structure of this identity is still under discussion in SA2). It then has to be clarified if this identity has to be bound to the (temporary) IP address of the terminal on the bearer level, given by the PDP context. (This would not imply that IM domain security depended on PS domain security.)

[Editors note: Since there is a requirement for access independence it is FFS if the user identity used for authentication shall not be based on IMSI.]

9.1.2 Separation of the exchange of AKA parameters

It is proposed to keep the description of the exchange of the AKA parameters between the MS and the CSCF separate from the description how the parameters are obtained by the CSCF from the HSS as different protocols may be used in both cases. In section 8.1 the protocol used to exchange the crypto-parameters is SIP. Between CSCF and HSS of the user the protocol to be used is not yet specified by SA2, it may be SIP as well, but also other protocols, e.g. AAA protocols may be used.

9.1.3 Authentication

It has to be determined at which entity the authentication is carried out. It seems to be reasonable to carry out the AKA at the same CSCF that received the user profile data from the HSS. If this will be the serving CSCF, and whether the serving CSCF will be located in the home or in the visited network is still under discussion within SA2.

At the moment there are two different proposals; 1) authentication in the HN and 2) authentication in the VN.

9.1.3.1 Authentication in the HN

In [17] it is proposed to perform the authentication in the HN more specifically in the HSS/AAA. The main reason for this is that in 23.228 cf. [18] it is a requirement that the HN has the control of determining if the HN or the VN shall be the SN. Hence it is assumed in [17] that it is natural that the HN also can control the authentication (and have knowledge of the outcome of the authentication) of its IM-subscribers, cf. [17] for a more detailed description on the actual mechanisms.

9.1.3.1 Authentication in the VN

In [19] it is proposed to perform the authentication in the VN (in the P-CSCF). Then the concepts from the UMTS can be reused i.e. the AuC calculates quintets and sends it to a node in the VN which performs the authentication, cf. [19] for a more detailed description on the actual mechanisms.

[Editors note: It is FFS to decide where to authenticate the subscriber i.e. if it shall be in the VN or in the HN and in which node]

9.2 Open issues in section 8.2 and in section 8.3

9.2.1 Encryption and integrity termination

It has to be determined at which entity encryption / integrity protection of SIP messages has to be performed, using the session keys agreed in the previous run of the AKA. It seems to be reasonable that this is the CSCF (most likely the serving CSCF) that also carries out the AKA, but it may also be possible that there are reasons that a different CSCF is used. (This may e.g. be the case if the serving CSCF is located in the home environment of the user and a CSCF in the visited network acts as a SIP proxy.)

At the moment there are two different proposals; 1) termination of encryption in the P-CSCF and termination of integrity in S-CSCF and 2) termination of encryption and integrity in the P-CSCF. The two different philosophies are briefly described here.

9.2.1.1 Termination of encryption in the P-CSCF and termination of integrity in S-CSCF

In [17] it is proposed that confidentiality protection shall be hop-by-hop as specified in the SIP standard [15]. The main reason for this is that it is the only way to protect the whole SIP message. If the protection takes place on the SIP level then cf. [15] several parts of the SIP message has to be sent in clear and there exist several attacks for this case. Another reason is lawful interception. Hence termination of encryption will by definition be in the P-CSCF.

Furthermore it is proposed in [17] that integrity protection shall terminate in the S-CSCF. The main reason for this is home control. If the HN decides that the SN will be in the HN then if integrity protection terminates in the VN (i.e. the P-CSCF) a bogus P-CSCF may do changes in the SIP message and the HN can not detect this.

9.2.1.2 Termination of encryption and integrity in the P-CSCF

In [19] it is proposed that encryption and integrity shall terminate in the P-CSCF. The main reason for this is the reuse of VLR/SGSN and AuC concept and it is viewed as being simpler (key management, signalling, VN can control the keys i.e. integrity and confidentiality keys etc) to give protection in only on node instead of two as in 9.2.1.1. Furthermore it is assumed that the HN shall rely on the VN for IM-services and that a bogus P-CSCF is not an issue. It is also assumed (and it is necessary) that IPSec protects the communication path between the VN and the HN.

9.2.2 Encryption and integrity mechanisms

It has to be specified which mechanisms are to be used to carry out encryption / integrity protection of SIP messages.

In [4] the security mechanisms specified by the IETF for SIP are discussed and evaluated. It is concluded that IPSec meets the security as well as the system requirements of [3] (if an appropriate AKA protocol would be specified). The other security mechanisms proposed so far for SIP which are also discussed in [4] do not meet these requirements.

In [17] it is proposed that WTLS is used for confidentiality protection (as an option) between the UE and the P-CSCF based upon a shared secret. WTLS shall then use the abbreviated handshake for fast set-up of session keys. The main reasons for the use of WTLS is that it fulfils the requirements in [4] and it is optimised for a wireless channel.

[Editors Note: It is FFS if WTLS is a good candidate (signalling load has to be analysed etc) or if it should be applied on the SIP-level.]

It is also proposed in [17] that the mechanism used for integrity protection shall be conformant with [15] however a new mode has to be defined since it is concluded in [4] that PGP shall not be used.

In both [17] and [19] it is proposed to use IPSec for inter domain security.

It is therefore proposed as a working assumption to use IPSec to provide confidentiality and integrity of SIP messages between UE and CSCF. The following issues need to be addressed in order to show the viability of this working assumption:

- **Establishment of security associations (SAs):** In the course of the SIP registration procedure, authentication and key agreement has to be carried out. If IPSec were used for the protection of SIP messages besides the keys themselves also other parameters for the IPSec SA (security association) would have to be established. All these parameters have to be made available to the UE in the course of the AKA procedure.

- **Replay protection for IPSec:** If an automated key management is used for IPSec then IPSec also provides replay protection. If this is not the case then a replay protection has to be additionally specified.

- **Security session concept**: It is desirable that the security association for IPSec established in the course of the registration procedure is used to protect subsequent calls until the user de-registers himself at the CSCF (or the security association expires). We denote the life-time of a security association by " security session".) This would avoid that for each call the AKA protocol would have to be run between UE and CSCF.

- **Change of IP addresses:** Under certain circumstances a new run of the AKA may be required, however: The IP addresses of the communicating endpoints are at least part of the selectors for an SA. This implies, that if for a roaming user the IP address of the UE or of the serving CSCF changes during a session a new SA has to be established. This could occur if the user roams into the area of another GGSN during a security session and subsequently gets a new PDP context with a new temporary IP address or if the serving CSCF changes.

- **Multiple users on a terminal**: If there is only one user on a UMTS terminal, then the IP-addresses of the UE and the CSCF, respectively, are sufficient to identify the appropriate SA established in the AKA procedure.

If, however, there are two or more users (which should be charged based on their different IM identities) using the same UE (e.g. a mobile laptop) for overlapping security sessions then the IP-addresses of CSCF and UE are not sufficient as selectors for the SAs. As the IM identities are not available at IP level, additionally the port numbers of the SIP applications on the UE are needed to distinguish between users, whereas on the server side the IP address of the CSCF is still sufficient. As port numbers used by SIP clients may change in each SIP request, the support for multiple users on a terminal would raise the new requirement for UMTS IM-capable terminals that SIP is implemented in a way that an instance of a SIP client relating to one user on the UE always uses the same port number during a session.

It has to be clarified whether multiple users on an IM-terminal are a requirement, and if so, whether SIP implementations can satisfy the above requirement.

9.3 Issues on security mechanisms for access security for IP-based services

There are two different approaches for the provision of security in the IM domain: it can be based on security mechanisms specifically defined for 3GPP or on security mechanisms mentioned in SIP [15].

A general decision to be made is, if security mechanisms for the IM domain should be based on public key cryptography or on symmetric key cryptography. This requires a careful analysis which has to consider the restrictions imposed by a UMTS environment as well as the implications of having to provide a global public key infrastructure. Some of the mechanisms defined by the IETF use public key cryptography. Those defined so far by 3GPP for UMTS do not.

9.3.1 Security mechanisms specifically defined for 3GPP:

One possibility could be to re-use the 3GPP AKA (authentication and key agreement) of the bearer level (as specified in [TS 33.102]) for authentication and key agreement in the IM domain. For integrity and confidentiality protection 3GPP specific mechanisms may be re-used as well.

9.3.2 Security mechanisms specified by the IETF for SIP:

For the protection of SIP several alternatives are mentioned in [15]. The mechanisms are taken from other RFCs. [15] only describes in which way these mechanisms are applied to SIP. Below the alternatives mentioned in the SIP standard are listed together with some of their characteristics. A first analysis is given whether the mechanisms meet the requirements assembled in our related contribution [3]:

- HTTP security mechanism "Basic Authentication" [16]
  - Provides authentication of a client to a server based on passwords, where the password is transmitted in the clear.
  - Authentication by a simple password transmitted without protection, does not fulfill any of the security requirements given in [3].
- HTTP security mechanism "Digest Authentication" [16]
  - Provides authentication of a client to a server based on passwords. The password is not transmitted in the clear, instead a digest (hash value) of the password and other parameters including a challenge parameter (issued by the server) to protect from replay attacks, is sent.
  - Authentication of a server to a client is not possible at the moment, but appropriate mechanisms are under discussion in the IETF SIP working group, cf. [15].
  - As mentioned in [15] chapter 13.2 Digest Authentication does not offer message integrity.

Digest Authentication was designed as a replacement for Basic Authentication. [16] itself discusses several weaknesses of this mechanism (sections 3.1.4; 4, but see also [SIP2000]). It is therefore questionable whether it meets the system requirements in [3].

- Pretty good privacy (PGP) [14] provides
  - Mutual authentication between client and server based on public key cryptography
  - Message integrity based on digital signatures
  - Message confidentiality, where data encryption is based on symmetric key cryptography and session key transport is protected by public key encryption.

The provided mechanisms offer a sufficient level of security and fulfill the security requirements given in [3], except the three-party AKA protocol. But PGP makes extensive use of public key mechanisms for authentication and key agreement. In particular, the use of digital signatures for message integrity seems inefficient.

- Transport layer security (TLS) [10]
  - Mandates public key cryptography for authentication and key management
  - The record layer provides message integrity as well as confidentiality based on symmetric key cryptography, but TLS is monolithic, i.e. key management is not separable from the record layer.
  - TLS is only defined for TCP, not for UDP, and some servers used in SIP must support UDP

Although a strong security protocol, TLS is not suitable for providing access security for IP-based services, since it only supports TCP at the transport layer which is not sufficient. TLS also relies on public key mechanisms. TLS does not allow to separate key management from the record layer which provides integrity and confidentiality for the transmitted data.

- IPSec [11], [12] provides
  - Mutual authentication between the communicating entities based on symmetric key cryptography
  - Message integrity based on symmetric key cryptography
  - Confidentiality protection of messages based on symmetric key cryptography
  - A protection mechanism against replay attacks, when used with automated keying (e.g. IKE)
  - Optional key management (IKE [RFC2409]) based on public key schemes

IPsec meets the security requirements of [3], except for the three-party AKA protocol. The IPsec base protocols AH and ESP do not use public key mechanisms and seem to meet all system requirements.

Note that, according to a decision in 3GPP, IPv6 addresses shall be used in the IM domain. Note that if IPv6 was implemented with full functionality then all nodes involved in the IM domain would have to support IPSec AH and ESP.

IETF has not defined AKA for roaming SIP users: For authentication and key management IKE [13] is an alternative to be considered. But note that neither IKE nor any of the alternatives listed above defined by the IETF for SIP specifies a three party authentication and key management for roaming users which is needed in UMTS. An appropriate mechanism would additionally have to be specified.

9.3.2.1 Protection using either TLS or IPSec

In the SIP specification three options for protection of the SIP messages are given:

1. Hop-by-hop encryption to protect “who is calling whom” (e.g. using IPSec or TLS). This protects the users from being tracked by eavesdroppers
2. Hop-by-hop encryption of the VIA field to hide the route The route may give useful information for an attacker
3. End-to-end (e.g. using mechanisms defined in PGP). The SIP message body can be encrypted and also some certain sensitive headers as well. However some parts of the SIP-message must be in clear such as the TO and VIA field to make it possible for the proxies to route the message correctly.

It is important to note that the SIP proxies will do changes in the SIP message.

Then e.g. in a call set up scenario between UE-to-UE SIP provides either hop-by-hop protection between proxies or/and end-to-end protection between the two UEs. This is valid both for confidentiality protection and integrity protection. Hence the serving CSCF must have a trustrelation with the proxy CSCF.

9.3.3 Pros and cons of various methods

- RFC 2617 methods, cf. [16]:

+ quite simple methods

- do not seem to meet requirements

- PGP, see [14]:

+ meets other requirements except it is not a 3-party protocol

- PKI mandated

- TLS, see [10]:

+ meets other requirements except it is not 3-party protocol

+ widely deployed in Internet

- does not work with UDP

- PKI mandated

- IPSEC/IKE, cf. e.g. [11]-[13]:

+ meets other requirements except it is not a 3-party protocol

+ IM CN is based on IPv6 hence all nodes support IPSEC

- not clear how to be used as a 3-party protocol

- UMTS AKA, see [1]:

+ meets all requirements

+ already implemented in UMTS environment in both USIM and AuC. It may even be possible to use R99 USIMs without any updates.

+ protocol between CSCF and AuC can be chosen freely (e.g. DIAMETER)

- not clear how to be used with other access networks than UTRAN or GERAN

- A completely new mechanism from scratch:

+ can be tailored for the purpose

- big specification and implementation effort needed

9.3.4 Analysis

The two basic criteria used to evaluate various approaches are:

1. How well the requirements are met by the solution?

2. How feasible the solution is ?

We discuss first (1) with respect to each mechanism and then we study (2) respectively.

As the requirements for authentication and key agreement method are not yet frozen it is not possible to give a final judgement regarding criterion 1. However, based on the understanding we have about the requirements (see Tdoc S3-000513) the following can be summarized:

RFC 2617 methods fall short of the requirements. Also, there seems to be no natural way to enhance these mechanisms in such way that the requirements would be met.

More advanced Internet mechanisms, i.e. PGP, SSL/TLS, IPSEC/IKE fall short in one requirement: they are not 3-party protocols. Instead, they are designed to fulfil the requirement of entity authentication between two parties. Otherwise, these mechanisms seem to meet the requirements.

Our judgement can now be based on the following two aspects:

How important is the requirement of being a 3-party protocol ?

Is it possible to enhance the mechanism to cover the case of a 3-party protocol ?

The architecture of the IM CN subsystem is stable enough to be able to conclude that a 2-party protocol is not sufficient for authentication. Therefore, the judgement must be based on the latter issue: potential extensions. At first sight, there seems to be no easy way to do these extensions but, on the other hand, it is surely not impossible.

UMTS AKA meets all requirements identified.

The same is, of course, true for any potential new mechanism.

As regards feasibility issues it is difficult to give final answers.

Clearly, RFC 2617 methods are simple enough to be feasible to implement in IM CN environment.

For more advanced Internet mechanisms, the extension to 3-party case probably restrict their feasibility considerably. Both PGP and SSL/TLS require PKI support which decreases their feasibility. The wide deployment of SSL/TLS in the Internet communications is a big advantage from the feasibility point of view. The same will most probably be true for IPSEC/IKE in the future. For all these methods, the feasibility on the UE side has to be studied carefully.

The UMTS AKA solution seems feasible as it has direct support from the legacy solutions in both USIMs and AuCs. The open questions are the extendability to cover other access technologies (other than UTRAN/GERAN) and interoperation with the chosen confidentiality and integrity protection mechanisms.

A completely new mechanism approach can hardly be seen feasible.

9.3.5 Proposal

Based on the analysis in 9.3.4 it is proposed that use of UMTS AKA also in IM CN subsystem is kept as a working assumption and further specification work is based on this assumption.

In addition, the approaches based on use of either SSL/TLS or IPSEC/IKE are seen as fall-back solutions if it turns out that the open questions with UMTS AKA cannot be solved. However, it must be noted that these fall-back solutions contain also open questions and further development requires substantial amount of effort.

9.4 Firewalls

The figure 1 (of version 0.0.0 of this TR) shows the security architecture for the IM CN subsystem and indicates that the IM CN subsystem provides “Logical firewall policy” functionality. In the section there is no accompanying text supporting the need for this. It is proposed to further examine if this functionality is really needed, for the following reason:

Firewalls are needed to protect the overall IP-based part of the core network from attacks, and are not specifically needed to protect the IM CN subsystem. It does not seem to be likely that the IM CN subsystem has its own firewall systems irrespective of the firewall systems installed to protect the overall IP core network. In the accompanying text to the figure in [6] it is stated that the firewall functionality has to be provided from the IM CN subsystem to protect it from rogue software clients. The protection of the network from rogue clients is however provided by access security mechanisms, i.e. by authentication and by integrity protection of the messages from the client. Thereby threatening IP packets received over the air interface could be discarded without having a firewall in the communication path.

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