3G TS 33.203 V0.2.10 (2001-043)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group SA3; Access security for IP-based services (Release 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

This clause is optional. If it exists, it is always the third unnumbered clause.

1 Scope

The scope for this technical specification is to specify the security features and mechanisms for secure access to the IM CN subsystem for the 3G mobile telecommunication system.

The IM CN SS in UMTS will support IP Multimedia applications such as video, audio and multimedia conferences. 3GPP has chosen SIP, Session Initiation Protocol as the signalling protocol for creating and terminating Multimedia sessions. This specification only deals with how the SIP signalling is protected, how the subscriber is authenticated and how the subscriber authenticate the IM CN SS network.

2 References

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

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

[2] 3G TS 22.228: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Service Requirements for the IP Multimedia Core Network".

[3] 3G TS 23.228: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; IP Multimedia (IM) Subsystem".

[4] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Security Threats and Requirements ".

[5] 3G TS 33.200: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Network domain security".

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

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

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

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

[10] IETF RFC 2543bis-02 (2000) “SIP: Session Initiation Protocol”

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

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
CSCF	Call State Control Function
GGSN	Gateway GPRS Support Node
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IM	IP Multimedia
MAC	Message Authentication Code
ME	Mobile Equipment
PS	Packet Switched
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
UE	User Equipment
UICC	UMTS IC Card
USIM	User Services Identity Module

4 Overview of the security architecture

[Editor's note This section shall have a figure of the overall architecture for the IM CN SS and explaining text on the trust relations, possible threats and a brief overview of the provided security features.]

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.

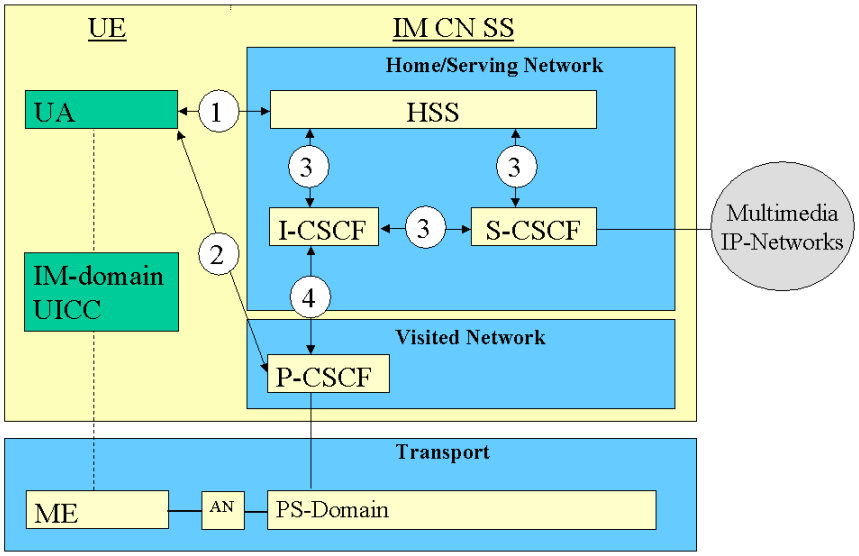

Figure 1. This is the security architecture for the IM CN Subsystem.

There are four different security associations and different need for security protection for IM CN SS and they are numbered 1,2, 3 and 4 in figure 1 where:

1. Provides mutual authentication. It is FFS whether the HSS or the S-CSCF is the termination point for authentication.

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

3. Provides security within the network domain internally

4. Provides security between different networks

Mutual authentication is required between the UE and the HSS.

The mechanisms specified in this technical specification are independent of the mechanisms defined for the CS- and PS-domain.

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.

The confidentiality and integrity protection for SIP-signalling is provided in a hop-by-hop fashion. The first hop i.e. between the UE and the P-CSCF is specified in this technical specification. The other hops, inter-domain and intra-domain are specified in [3]

5 Security features

[Editor's note: This section shall explain the provided security features in detail]

5.1 Secure access to IM CN SS

5.1.1 Authentication of the subscriber and the network

[Editor's note: This section shall deal with subscriber identity and authentication of the subscriber and Home Network/Serving Network]

An IM-subscriber will have its subscriber profile located in the HSS in the Home Network. The exact details of the subscriber profile are FFS but it will contain information on the subscriber that may not be revealed to an external partner, cf. [3]. At registration an S-CSCF is assigned to the subscriber by the I-CSCF. The subscriber profile will be downloaded to the S-CSCF over the Cx-reference point from the HSS (Cx-Pull). When a subscriber requests an IM-service the S-CSCF will check, by matching the request with the subscriber profile, if the subscriber is allowed to continue with the request or not i.e. Home Control (Authorisation of IM-services).

All SIP-signalling will take place over the PS-domain in the user plane i.e. IM-services are essentially an overlay to the PS-domain. Hence the Visited Network will have control of all the subscribers in the PS-domain i.e. Visited Control (Authorisation of bearer resources) since the Visited Network provides with a transport service and QoS.

For IM-services a new security association is required between the mobile and the IM CN SS before access is granted to IM-services. The Home Network or a 3rd party even (which does not have to be an UMTS operator) provides the user with the IM-services.

The mechanism for mutual authentication in UMTS is called UMTS AKA. It is a challenge response protocol and the AuC in the Home Stratum derives the challenge. A Quintet containing the challenge is sent from the Home Stratum to the Serving Network. The Quintet contains the expected response XRES and also a message authentication code MAC. The Serving Network compares the response from the UE with the XRES and if they match the UE has been authenticated. The UE calculates an expected MAX, XMAC, and compares this with the received MAC and if they match the UE has authenticated the Serving Network.

The AKA-protocol is a secure protocol developed for UMTS and it will be reused for IM-services and then called IMS AKA.

[Editors Note: The IMS AKA is an extension to the existing IETF SIP-draft.]

5.1.2 Confidentiality protection

[Editor's note: This section shall deal with what confidentiality protection that is provided between different nodes both inter domain, intra domain and the UE]

IP-based services will get ~~some~~ protection by the confidentiality protection defined in R'99 at the bearer level. In R'99 confidentiality protection is provided for signalling data and user data between the UE and the serving RNC. The serving RNC retrieves the cipher key CK from the SN. The ciphering protection is optional to use.

[Editor's note: It is FFS if it is enough to rely on the UE-RNC encryption, as stated above, and the Intranet solution provided by the visited network.

Confidentiality protection may be used between the UE and the P-CSCF for protecting SIP-signalling.

The following mechanisms could then be used:

1. *The UE and the P-CSCF shall negotiate what ciphering algorithm shall be used for the session, as specified in chapter 7.*
2. *The UE and the P-CSCF shall agree on a cipher key, CK_{IM} that shall be used for encryption/decryption of the SIP-signalling data. The cipher key is derived by the mechanisms defined in IMS AKA specified in chapter 6.1.*

3. Confidentiality protection between the UE and the P-CSCF of SIP-signalling.]

~~Confidentiality protection may be used between the UE and the P-CSCF for protecting SIP-signalling.~~

~~The following mechanisms shall be used:~~

~~1.The UE and the P-CSCF shall negotiate what ciphering algorithm shall be used for the session, as specified in chapter 7.~~

~~2.The UE and the P-CSCF shall agree on a cipher key, CK_{IM} that shall be used for encryption/decryption of the SIP-signalling data. The cipher key is derived by the mechanisms defined in IMS AKA specified in chapter 6.1.~~

3. ~~Confidentiality protection between the UE and the P-CSCF of SIP-signalling.~~

~~*[Editor's note: It is FFS if confidentiality protection is needed. It is FFS at what layer the SIP signalling shall be protected. It can be placed from the IP-Level up to the SIP-level.]*~~

5.1.3 Integrity protection

[Editor's note: This section shall deal with what integrity protection that is provided between different nodes both inter domain, intra domain and the UE]

Integrity protection shall be used between the UE and the P-CSCF for protecting the SIP signalling. The following mechanisms are provided.

1. The UE and the P-CSCF shall negotiate what integrity algorithm that shall be used for the session, specified in chapter 7.
2. The UE and the P-CSCF shall agree on an integrity key, IK_{IM} that shall be used when calculating a MAC. The mechanism is based on IMS AKA and specified in chapter 6.1.
3. The UE and the P-CSCF shall both make a MAC check to verify that the data received originates from a node which has the agreed session key, IK_{IM}. This check is also used for detecting if the data has been tampered with by a man-in-the-middle.

[Editor's note: It is FFS at what layer the SIP signalling shall be protected. It can be placed from the IP-Level up to the SIP-level.]

5.1.4 Visibility and configurability

[Editor's note: This section shall contain what the subscriber shall be able to configure and what is visible for the subscriber regarding the actual protection the subscriber is provided with.]

The user shall be informed which level of protection that is in use.

6 Security mechanisms

[Editor's note: This section shall describe the security mechanisms that are provided inter domain, intra domain and to the UE.]

6.1 Authentication and key agreement

[Editor's note: This section shall describe in detail how the authentication is performed and how the keys are derived and delivered to the different nodes.]

This scheme for the IM CN SS is called IMS AKA. The IMS AKA achieves mutual authentication between the USIM and the HSS, cf. Figure 2. Furthermore a security association is established between the UE and the P-CSCF. The USIM and the HSS keeps track of the counters SQN_{UE} and SQN_{HSS} for the IM-domain. The handling of the SQN can be as in [1].

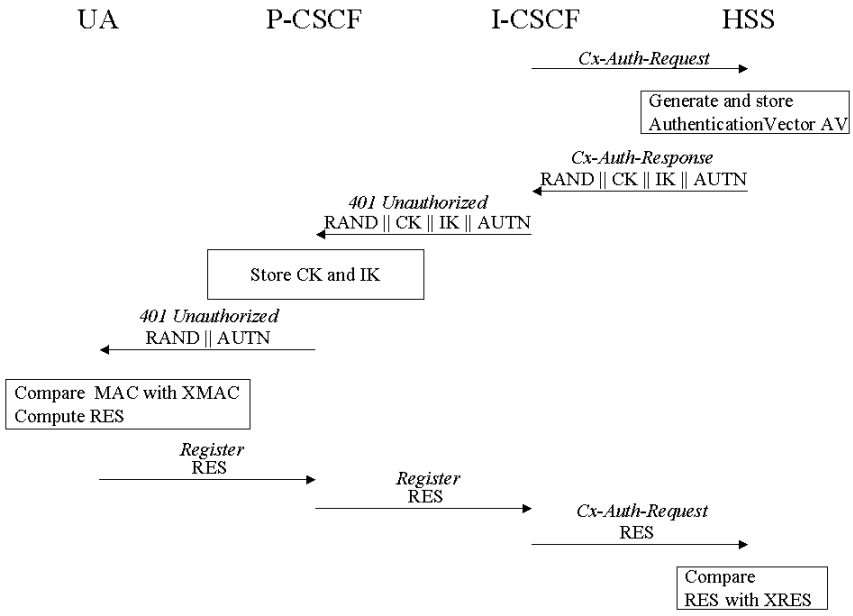

Figure 2: The IMS Authentication and Key Agreement.

[Editor's note It is FFS where to perform the authentication. Another open alternative is to perform the authentication in the S-CSCF.]

The generation of the authentication vector AV which includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. For each user it is the HSS that keeps track of the counter SQN_{HSS}. The requirements on the SQN handling both in the Home Network i.e. the HSS and the USIM are specified in [1]. The AMF field can be used in the same way as in [1].

The HSS receives a *Cx-Auth-Request* that shall include the private user identity (the NAI), which the home operator assign. Upon receiving the *Cx-Auth-Request* the HSS generates an AV and sends the I-CSCF a *Cx-Auth-Response* that shall include a RAND, CK, IK and AUTN. The I-CSCF sends a SIP-message *401 Unauthorized*, which shall include RAND, CK, IK and AUTN. The P-CSCF stores the CK and IK, which shall be used in the subsequent protection of the SIP-signalling between the UE and the P-CSCF.

The P-CSCF forwards the SIP-message *401 Unauthorized*, which shall include RAND and AUTN. The USIM calculates an XMAC and compares it with the received MAC. If they are the same the USIM has authenticated the HSS. Otherwise the UE shall send a *Register-user-auth-reject* to the P-CSCF. The SQN freshness is checked by the USIM if it is not in the correct range a *Register-synch-failure* is sent to the P-CSCF. The synchronisation failure message shall include the parameter AUTS as specified in [1].

If the SQN is in the correct range and if the MAC and the XMAC are equal then the UE shall send the response to the P-CSCF i.e. *Register* with the RES included. The P-CSCF shall forward this SIP message to the I-CSCF. The I-CSCF shall send a *Cx-Auth-Request* to the HSS including the RES. Upon receipt of the RES the HSS compares the RES with the XRES and if they are equal the subscriber is authenticated.

[Editor's note: It is FFS if re-use and re-transmission of RAND and AUTN is allowed. If allowed the mechanisms have to be defined.]

[Editor's note: The exact mechanisms for re-synchronisation are FFS.]

The lengths of the IMS AKA parameters are specified in chapter 6.3.7 in [1].

6.2 Confidentiality mechanisms

[Editor's note: This section shall deal with cipher algorithms]

[Editor's note: the following mechanisms are FFS:

Confidentiality protection method

etc]

6.3 Integrity mechanisms

[Editor's note: This section shall deal with integrity algorithms]

[Editor's note: the following mechanisms are FFS:

data integrity protection method

etc]

7 Security mode set-up

[Editor's note: the following mechanisms are FFS:

Key settings

Mechanisms for ciphering and integrity mode negotiation

Key lifetime

Key identification

When to start encryption and integrity protection]

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**
2000-10	SA3#15bis	33.2xx		0.1.0	Initial version of the specification		
2000-11	SA3#16			0.1.1	Input from AdHoc meeting		
2001-03	SA3#17	33.203		0.2.0	Input from the SA3#17 meeting in Göteborg		
2001-04		33.203		0.2.1	Termination of confidentiality in the P-CSCF moved to an editors note. Kept the R'99 mechanism in the main document. Where to terminate is FFS.		
Editor Krister Boman, Ericsson Email: krister.boman@emw.ericsson.se Telephone: +46 31 747 6045/ +46 70 604 0564							