
3G TS 33.203 V0.34.0 (2001-0506)

Technical Specification

**3rd Generation Partnership Project;
Technical Specification Group SA3;
Access security for IP-based services
(Release 5)**



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organisational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organisational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organisational Partners' Publications Offices.

Keywords

Access security, IP Multimedia, [SIP](#)

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

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2000, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Foreword.....	5
Introduction.....	5
1 Scope.....	6
2 References.....	6
3 Definitions, symbols and abbreviations.....	7
3.1 Definitions.....	7
3.2 Symbols.....	7
3.3 Abbreviations.....	7
4 Overview of the security architecture.....	8
5 Security features.....	10
5.1 Secure access to IM CN SS.....	10
5.1.1 Authentication of the subscriber and the network.....	10
5.1.2 Confidentiality protection.....	11
5.1.3 Integrity protection.....	11
5.2 Visibility and configurability.....	12
6 Security mechanisms.....	12
6.1 Authentication and key agreement.....	12
6.1.1 Registration of an IM-subscriber.....	12
6.1.3 Authentication failures.....	15
6.1.3 Synchronization failure.....	15
6.2 Confidentiality mechanisms.....	15
6.3 Integrity mechanisms.....	15
7 Security mode set-up.....	16
Annex <A> (normative): <Normative annex title>.....	17
Annex <X> (informative): Change history.....	18
Foreword.....	4
Introduction.....	4
1 Scope.....	5
2 References.....	5
3 Definitions, symbols and abbreviations.....	5
3.1 Definitions.....	5
3.2 Symbols.....	6
3.3 Abbreviations.....	6
4 Overview of the security architecture.....	6
5 Security features.....	7
5.1 Secure access to IM CN SS.....	7
5.1.1 Authentication of the subscriber and the network.....	7
5.1.2 Confidentiality protection.....	8
5.1.3 Integrity protection.....	9
5.1.4 Visibility and configurability.....	9
6 Security mechanisms.....	9
6.1 Authentication and key agreement.....	9
6.2 Confidentiality mechanisms.....	10
6.3 Integrity mechanisms.....	11

7	Security mode set up	11
Annex <A> (normative): <Normative annex title>	12
Annex <X> (informative): Change history	13

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~~ signaling protocol for creating and terminating Multimedia sessions, cf. [6]. This specification only deals with how the SIP ~~signalling~~ signaling 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 33.210~~xx~~: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Network domain security; IP network layer 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"
- [649] IETF RFC 2543bis-032 (20010) "SIP: Session Initiation Protocol"
- [11] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication"[7]
IETF RFC 2284 (1998) "PPP Extensible Authentication Protocol (EAP)"
- [8] IETF Draft (2001) "draft-arkko-pppext-eap-aka-00.txt"
- [9] IETF Draft (2001) "draft-http-eap-basic-01.txt"
- [10] IETF RFC 2716 (1999) "PPP EAP TLS Authentication Protocol"
- [11] IETF Draft (2001) "draft-haverinen-pppext-eap-sim-01.txt"

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.

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

ISIM – IM Services Identity Module. In a security context, this module is responsible for performing subscriber and network authentication and key agreement in IM CN SS. The ISIM resides on the UICC.

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
<u>HN</u>	<u>Home Network</u>
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IM	IP Multimedia
<u>IMPI</u>	<u>IM Private Identity</u>
<u>IMPU</u>	<u>IM Public Identity</u>
<u>ISIM</u>	<u>IM Services Identity Module</u>
MAC	Message Authentication Code
ME	Mobile Equipment
<u>PPP</u>	<u>Point to Point Protocol</u>
PS	Packet Switched
<u>SEG</u>	<u>Security Gateway</u>
<u>SDP</u>	<u>Session Description Protocol</u>
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
<u>UA</u>	<u>User Agent</u>
<u>UAC</u>	<u>UA Client</u>
<u>UAS</u>	<u>UA Server</u>
UE	User Equipment

UICC UMTS IC Card

USIM User Services Identity Module

USIM - User Services Identity Module VN Visited Network

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, the 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. The ISIM is responsible for the handling of keys, SQN etc that are tailored to IM CN SS. The keys, SQN etc handled by the ISIM are all independent of the similar parameters that exist in the USIM.

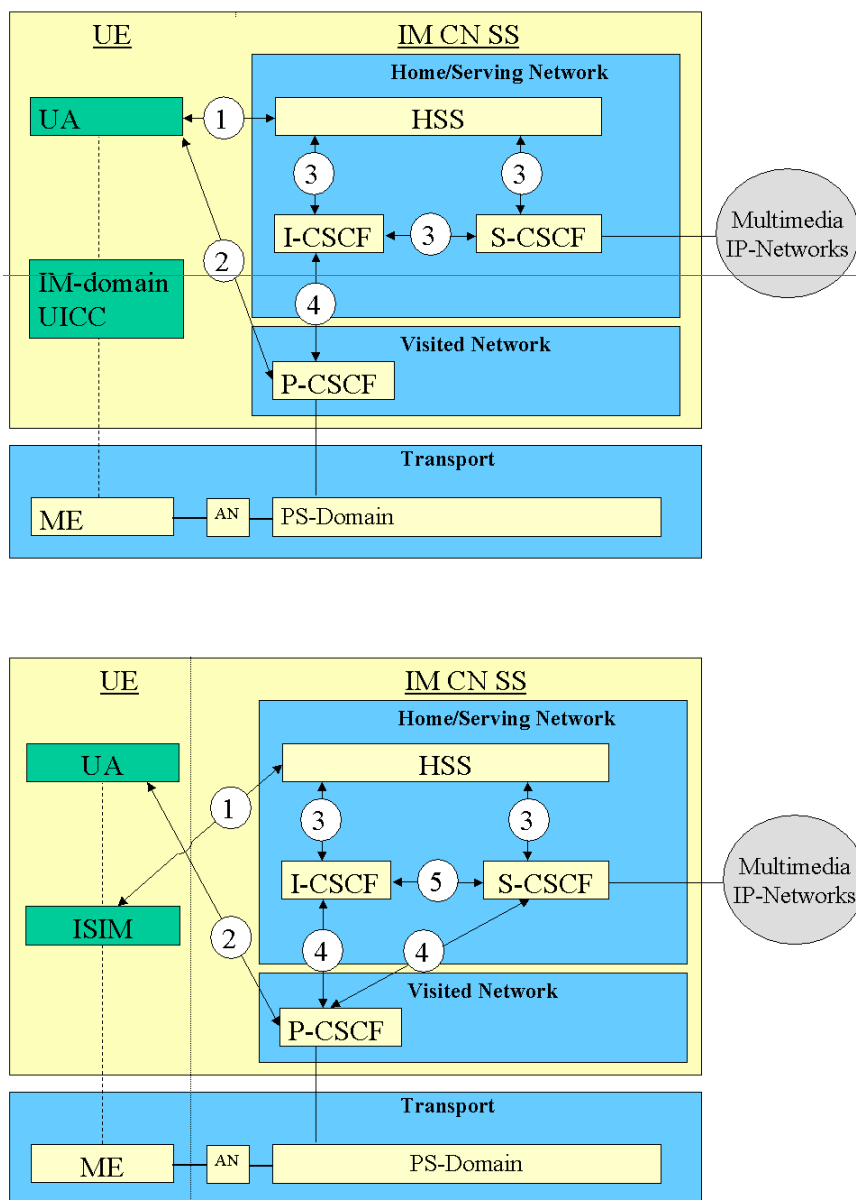


Figure 1. This is the security architecture for the IM CN Subsystem.

There are ~~four~~ five different security associations and different needs for security protection for IM CN SS and they are numbered 1,2, ~~3-3,~~ 4 and 5 in figure 1 where:

1. Provides mutual authentication. The HSS delegates the performance of subscriber authentication to the S-CSCF. However the HSS is responsible for generating keys and challenges. The long-term key in the ISIM and the HSS is associated with the IMPI. 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 for the Cx-interface. This part is not covered in this specification instead [5] specifies what security measures shall be defined in the internal network over the Cx-interface.
4. Provides security between different networks for SIP capable nodes. This part is not covered in this specification instead [5] specifies what security measures shall be defined for these type of interfaces.
5. Provides security within the network internally between SIP capable nodes. This part is not covered in this specification instead [5] specifies what security measures shall be defined for these types of interfaces.

Mutual authentication is required between the UE and the HNSS.

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.

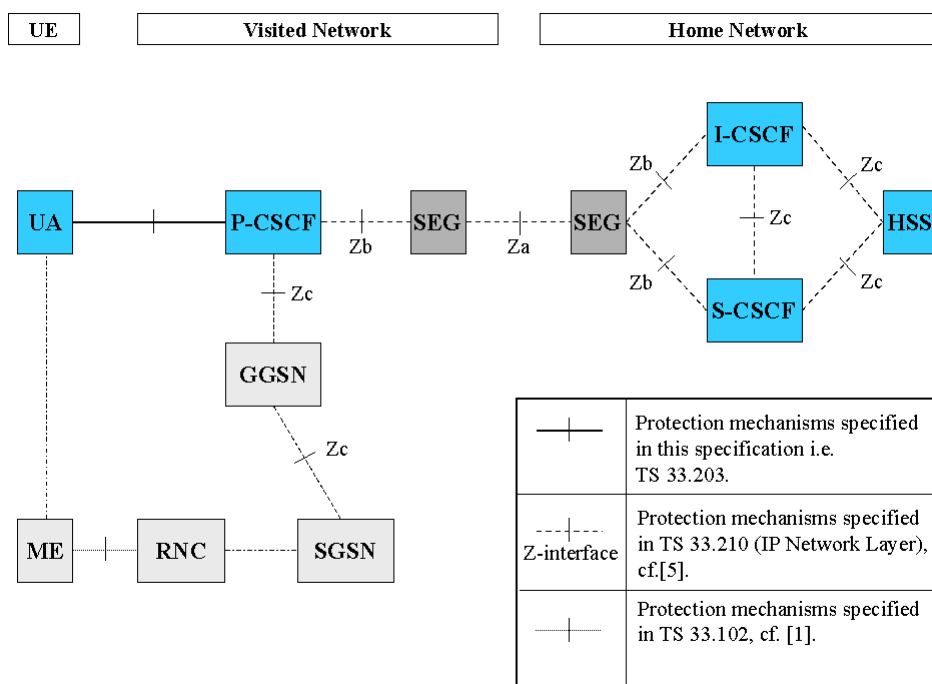


Figure 2. This figure gives an overview of the security architecture for IM CN SS and the relation with Network Domain security, cf. [5].

The confidentiality and integrity protection for SIP-signalling is provided in a hop-by-hop fashion, cf. Figure 2. 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].

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 (Authorization of IM-services).

All SIP-~~signalling~~signaling 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~~Authorization 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 MAC~~X~~, 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.

~~The SIP signalling is protected in a hop-by-hop fashion and integrity is provided between the UE and the P-CSCF with a MAC.~~The Home Network authenticates the subscriber at registrations or re-registrations only. In order to re-authenticate a subscriber the Home Network can force a re-registration by using e.g. a re-registration timer.

[Editors Note: The IMS AKA is an extension to the existing IETF SIP draft. It has been discussed whether session establishments shall be authenticated or not. It is a standard SIP feature to do this by using the fact that the S-CSCF is not only a registrar but also a proxy server and hence can send a 407 Proxy Authentication Required towards the UE and require authentication at every n:th INVITE. It is also open how to perform authentication at long calls without interrupting the call. The requirements are not clear and has to be defined.]

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 protection by the confidentiality protection defined in R'99 at the bearer level. In R'99 confidentiality protection is provided for ~~signalling~~signaling 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 for UMTS is optional to use.

For UMTS access confidentiality protection for SIP ~~signalling~~signaling ~~can~~will rely on the confidentiality mechanisms provided by UMTS and mechanisms provided by Network Domain Security, cf. [5].

[Editor's note: It is optional to implement confidentiality protection and it should be applied at the same level as the integrity protection.]

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~~signaling. 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.]

5.1.45.2 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, IK and CK, are derived and delivered to the different nodes.]

This scheme for authentication and key agreement in the IM CN SS is called IMS AKA. The IMS AKA achieves mutual authentication between the USIM and the HSS, cf. Figure 32. 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]. IMS AKA is based on EAP, cf. [7], and the AKA extension to EAP and HTTP, cf. [8] and [9] respectively.

EAP, PPP Authentication Extensible Protocol, is defined for PPP and is a general authentication protocol which supports several authentication schemes and it is straightforward to extend EAP with any new desired scheme. Examples of authentication schemes that EAP supports are Public based authentication through EAP TLS, cf. [10] and GSM Authentication through EAP SIM see [11]. EAP can not negotiate authentication scheme but that is in this specification contemplated as a security feature since then the protocol is secure against 'bidding-down' attacks. The HN shall choose the EAP AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g. keys generated by the AKA scheme are transported by SIP and embedded in EAP.

The generation of the authentication vector AV that 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 ISIM are specified in [1]. The AMF field can be used in the same way as in [1].

The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. [3]. The HSS and the IM-domain part share a long-term key associated with the IMPI.

6.1.1 Registration of an IM-subscriber

Before a user can get access to the IM services he needs to be registered and authenticated at application level. In order to get registered the UA sends a SIP REGISTER message towards the SIP registrar server i.e. the S-CSCF, cf. Figure 3, which will perform the authentication of the user.

[Editor's note: Currently there are more than one alternative available when to send key(s) which are under discussion. Therefore no keys have been included in the flow below. However during the authentication process the P-CSCF will need key(s). The IK and optionally the CK could be sent either in the 401 message or in the 200 message.]

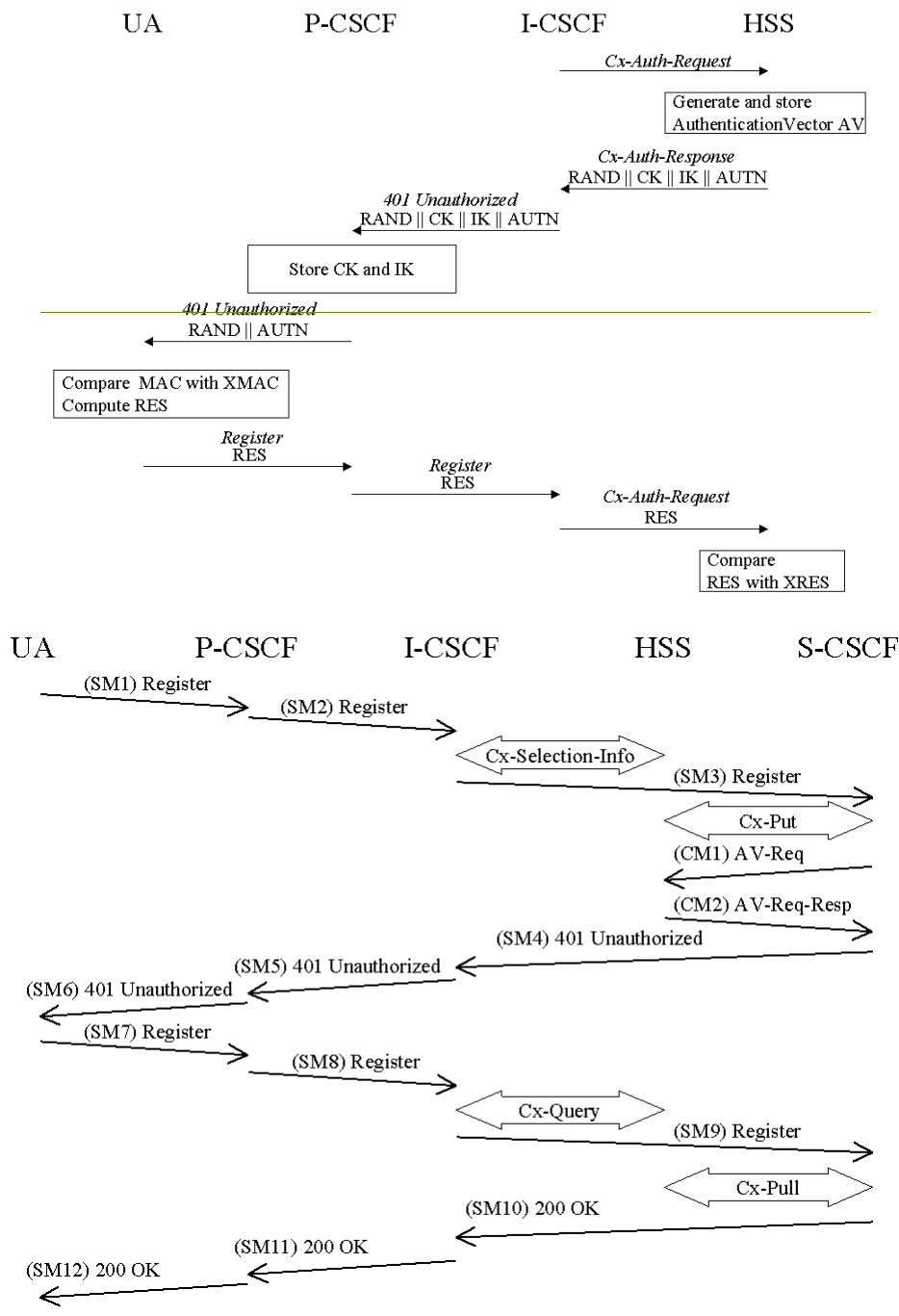


Figure 23: The IMS Authentication and Key Agreement. for an unregistered IM subscriber and successful mutual authentication with no synchronization error.

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

The flows in more detail

SMn stands for SIP Message n and CMm stands for Cx message m which has a relation to the authentication process:

SM1:
 REGISTER sip: ----
 Via: ----
 From: IMPI
 To: IMPU
 Call-ID: ----

Cseq: 1 REGISTER
Content-Length: 0

[Editor's note: This example covers the case when only one public identity is registered. It is still FFS how to treat the case when the subscriber registers several public identities.]

The P-CSCF and the I-CSCF forwards the SIP REGISTER towards the S-CSCF and adds a Via header with their addresses included, i.e. SM2 and SM3. Upon receiving the SIP REGISTER the S-CSCF will need one or several AVs in order to send a challenge to the user. The S-CSCF sends a request for the AV(s) to the HSS, CM1 together with the number n of AVs wanted where n is at least one but less than or equal to nmax.

CM1:

Cx-AV-Req(IMPI, IMPU, n)

The HSS creates the Avs for that user and sends it to the S-CSCF, CM2.

CM2:

Cx-AV-Req-Resp(IMPI, IMPU, n, RAND₁||AUTN₁||XRES₁||CK₁||IK₁,..., RAND_n||AUTN_n||XRES_n||CK_n||IK_n)

The S-CSCF sends a SIP 401 Unauthorized to the UA including the challenge RAND and the authentication token AUTN, SM4. 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].

SM4:

SIP/2.0 401 Unauthorized
Via: ----
From: IMPI
To: IMPU
Call-ID: ----
Cseq: 1 REGISTER
WWW-Authenticate: eap parameters: RAND||AUTN
Content-Length: 0

Upon receiving the challenge, SM6, the UA takes the AUTN which includes a MAC and the SQN. The UE calculates the XMAC and checks that XMAC=MAC and that the SQN is in the correct range as in [1]. If both these checks are successful the UE then calculates the response, RES, puts it in the Authorization header and sends it back to the registrar in SM7.

SM7:

REGISTER sip: ----
Via: ----
From: IMPI
To: IMPU
Call-ID: ----
Cseq: 1 REGISTER
Authorization: eap parameters: RES
Content-Length: 0

Upon receiving the response, RES, the S-CSCF retrieves the active XRES for that user and checks if XRES=RES. If the check is successful then the user has been authenticated and the IMPU is registered in the S-CSCF.

When a subscriber has been registered this registration will be valid for some period of time. Both the UA and the S-CSCF will keep track on a timer for this purpose but the expiration time in the UE is smaller than the one in the S-CSCF in order to make it possible for the UE to be registered and reachable without interruptions. This feature is FFS in [3]. The re-registration feature opens up a potential denial-of-service attack in the sense that an attacker could re-register a subscriber and respond with the wrong RES and the HN could then de-register the subscriber. This shall be avoided by letting the subscriber be registered with the old set of parameters until a re-registration is successfully authenticated.

[Editor's note: It is FFS if this way of protecting the user from DoS attack is feasible or not.]

The re-registration looks the same as the registration case except that CM1 and CM2 can be omitted as long as the S-CSCF has valid AV(s).

[Editor's note: Potential failure scenarios and potential extra requirements needed for the handling several AV(s) in the S-CSCF are left FFS.]

The HSS receives a *Cx-Auth-Request* that shall include the private user identity (the NAI), which the home operator assigns. 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].

6.1.3 Authentication failures

[Editor's note: This subsection shall deal with the requirements for network and user authentication failures.]

6.1.3 Synchronization failure

[Editor's note: This subsection shall deal with the requirements for the case when the SQNs in the ISIM and the HSS are not in synch.]

6.2 Confidentiality mechanisms

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

For access to IMS through UMTS no cipher algorithms are specified for IM CN SS other than those provided by UMTS R'99 i.e. [1] and Network Domain Security [5].

[Editor's note: No other accesses than UMTS are within the scope of R5. Since it is optional to implement the text above seems too stringent. Hence the editor believes that it would be good if also confidentiality mechanisms were defined.]

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.		
2001-05	SA3#17bis	33.203		0.3.0	Input from the SA3#17bis meeting in Madrid.		
2001-06 2001-05	SA3#18SA 3#17bis	33.20333. 203		0.4.00. 3.0	Input from the SA3#18 meeting in Phoenix. Input from the SA317#bis meeting in Madrid.		
Editor Krister Boman, Ericsson Email: krister.boman@emw.ericsson.se Telephone: +46 31 747 6045 (Office) +46 70 987 6045 (Mobile)							