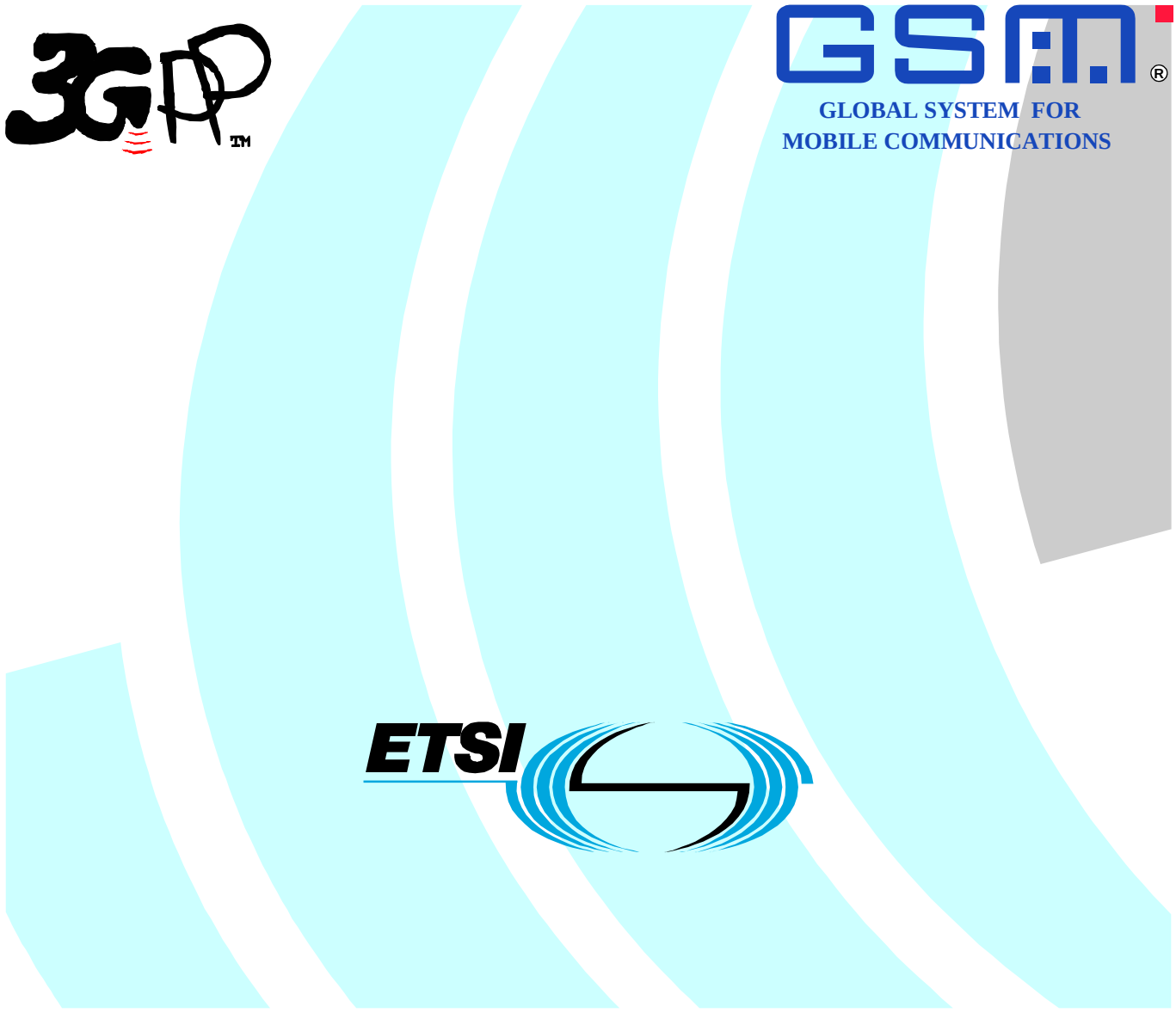
ETSI TS 133 203 V5.2.0 (2002-06)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
3G security;
Access security for IP-based services
(3GPP TS 33.203 version 5.2.0 Release 5)



Reference
RTS/TSGS-0333203v520

Keywords
GSM, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

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.

1 Scope

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

The IMS in UMTS will support IP Multimedia applications such as video, audio and multimedia conferences. 3GPP has chosen SIP, Session Initiation Protocol, as the signaling protocol for creating and terminating Multimedia sessions, cf. [6]. This specification only deals with how the SIP signaling is protected between the subscriber and the IMS, how the subscriber is authenticated and how the subscriber authenticates the IMS.

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[2] 3GPP TS 22.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for the IP Multimedia Core Network".

[3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem".

[4] 3GPP TS 21.133: "3rd Generation Partnership Project; T Technical Specification Group Services and System Aspects; Security Threats and Requirements ".

[5] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[6] IETF RFC 3261 "SIP: Session Initiation Protocol".

[7] 3GPP TS 21.905: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Vocabulary for 3GPP specifications".

[8] 3GPP TS 24.229: "3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".

[9] 3GPP TS 23.002: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, Network Architecture".

[10] 3GPP TS 23.060: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, General Packet Radio Service (GPRS); Service Description".

[11] 3GPP TS 24.228: "3rd Generation Partnership Project: Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".

[12] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication".

[13] IETF RFC 2406 (1998) "IP Encapsulating Security Payload (ESP)".

[14] IETF RFC 2401 (1998) "Security Architecture for the Internet Protocol".

[15] IETF RFC 2403 (1998) "The Use of HMAC-MD5-96 within ESP and AH".

[16] IETF RFC 2404 (1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[17] Draft-ietf-sip-digest-aka-01: "HTTP Digest Authentication Using AKA". April, 2002.

[18] IETF RFC 3041 "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

Authenticated (re-) registration: A registration i.e. a SIP register is sent towards the Home Network which will trigger a authentication of the IMS subscriber i.e. a challenge is generated and sent to the UE.

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.

ISIM – IM Subscriber Identity Module: For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on a UICC. The ISIM may be a distinct application on the UICC.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply, [7] contains additional applicable abbreviations:

AAA	Authentication Authorisation Accounting
AKA	Authentication and key agreement
CSCF	Call Session Control Function
HSS	Home Subscriber Server
IM	IP Multimedia
IMPI	IM Private Identity
IMPU	IM Public Identity
IMS	IP Multimedia Core Network Subsystem
ISIM	IM Services Identity Module
MAC	Message Authentication Code
ME	Mobile Equipment
SA	Security Association
SEG	Security Gateway
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UA	User Agent

4 Overview of the security architecture

In the PS domain, the service is not provided until a security association is established between the mobile equipment and the network. IMS is essentially an overlay to the PS-Domain and has a low dependency of the PS-domain.

Consequently a separate security association is required between the multimedia client and the IMS before access is granted to multimedia services. The IMS Security Architecture is shown in the following figure.

IMS authentication keys and functions at the user side shall be stored on a UICC. It shall be possible for the IMS authentication keys and functions to be logically independent to the keys and functions used for PS domain authentication. However, this does not preclude common authentication keys and functions from being used for IMS and PS domain authentication according to the guidelines given in section 8.

For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on a UICC. Further information on the ISIM is given in section 8.

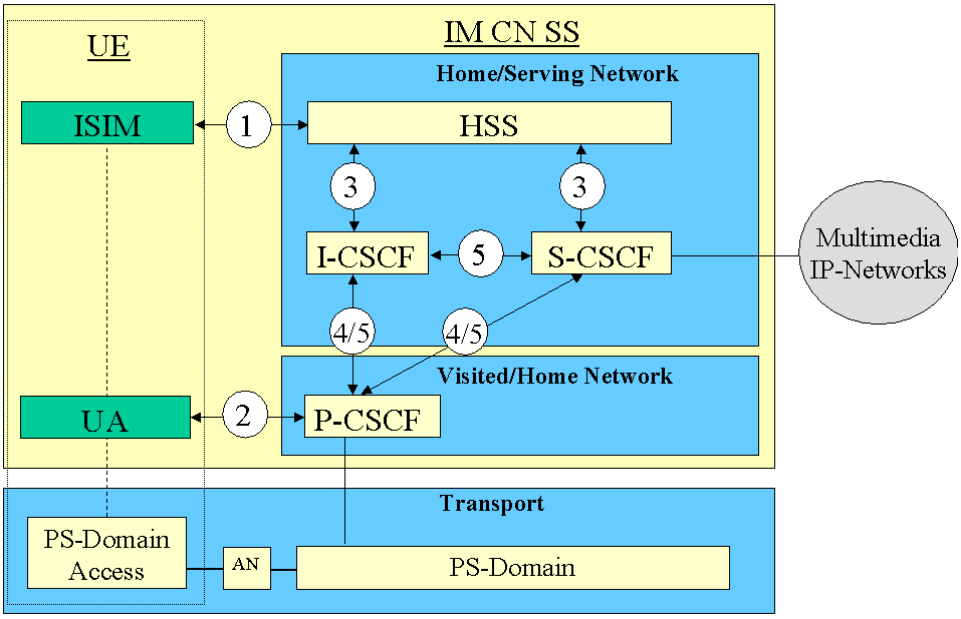


Figure 1: The IMS security architecture

There are five different security associations and different needs for security protection for IMS and they are numbered 1,2, 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. The subscriber will have one (network internal) user private identity (IMPI) and at least one external user public identity (IMPU).

2. Provides a secure link and a security association between the UE and a P-CSCF for protection of the Gm reference point. Data origin authentication is provided i.e. the corroboration that the source of data received is as claimed. For the definition of the Gm reference point cf. TS23.002 [9].

3. Provides security within the network domain internally for the Cx-interface. This security association is covered by TS 33.210 [5]. For the definition of the Cx-interface cf. TS23.002 [9].

4. Provides security between different networks for SIP capable nodes. This security association is covered by TS 33.210 [5]. This security association is only applicable when the P-CSCF resides in the VN and if the P-CSCF resides in the HN then bullet point number five below applies, cf. also Figure 2 and Figure 3.

5. Provides security within the network internally between SIP capable nodes. This security association is covered by TS 33.210 [5]. Note that this security association also applies when the P-CSCF resides in the HN.

There exist other interfaces and reference points in IMS, which have not been addressed above. Those interfaces and reference points reside within the IMS, either within the same security domain or between different security domains. The protection of all such interfaces and reference points apart from the Gm reference point are protected as specified in TS 33.210 [5].

Mutual authentication is required between the UE and the HN.

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

An independent IMS security mechanism provides additional protection against security breaches. For example, if the PS-Domain security is breached the IMS would continue to be protected by it's own security mechanism. As indicated in Figure 1 the P-CSCF may be located either in the Visited or the Home Network. The P-CSCF shall be co-located within the same network as the GGSN, which may reside in the VPLMN or HPLMN according to the APN and GGSN selection criteria, cf. TS23060 [10].

P-CSCF in the Visited Network

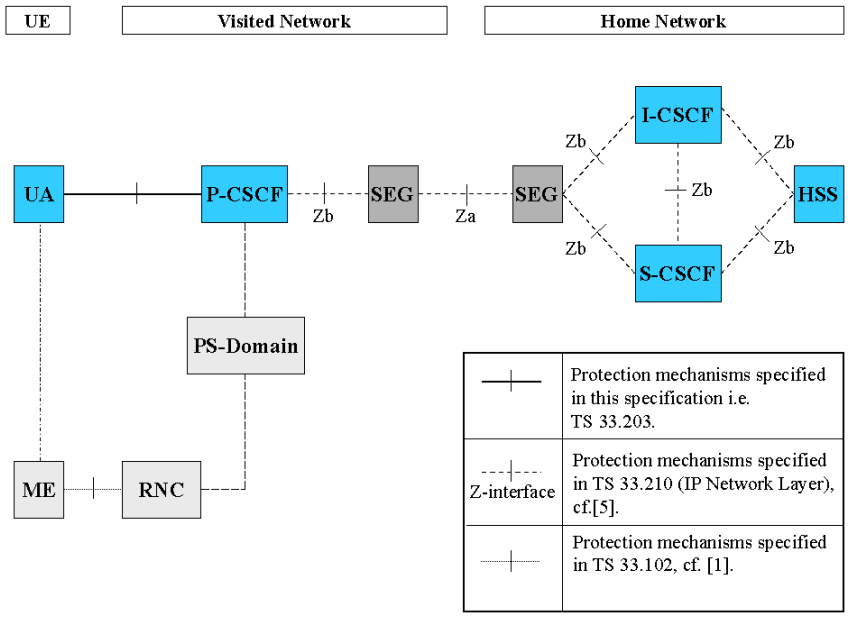


Figure 2: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the VN

P-CSCF in the Home Network

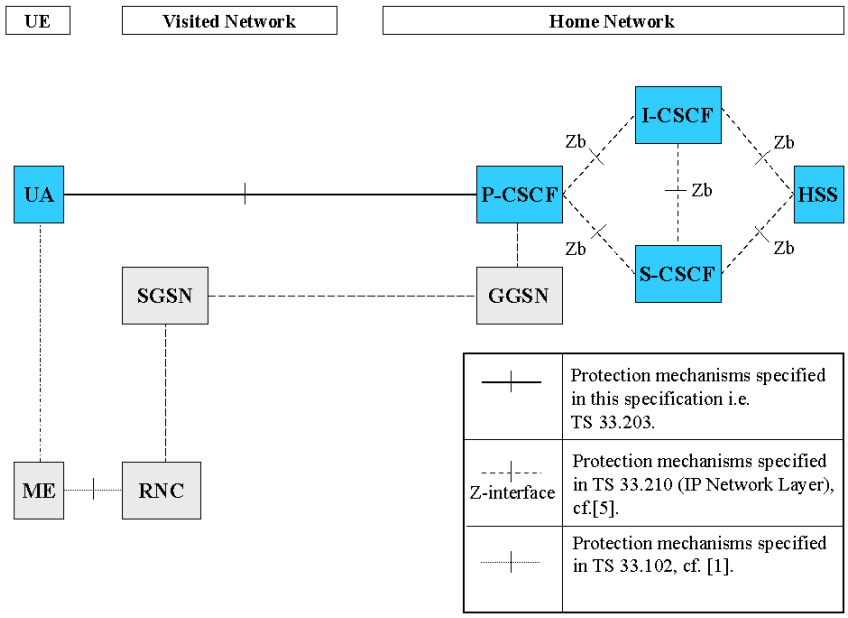


Figure 3: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the HN

The confidentiality and integrity protection for SIP-signaling is provided in a hop-by-hop fashion, cf. Figure 2 and Figure 3. 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 TS 33.210 [5].

[Editors Note: The UE Functional split security architecture is FFS e.g. if a section "security for the local interface between the TE and the MT in UE functional split scenarios" would be added to this specification. In this section, it would be pointed out what security features are required on this local interface. Security mechanisms would not be specified, as they would depend on the particular nature of this interface. The new section would also not attempt to assess security mechanisms available for technologies, which may be used to realise this interface (e.g. Bluetooth, Wireless LAN).]

5 Security features

5.1 Secure access to IMS

5.1.1 Authentication of the subscriber and the network

Authentication between the subscriber and the network shall be performed as specified in section 6.1.

An IM-subscriber will have its subscriber profile located in the HSS in the Home Network. The subscriber profile 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 access to the IP Multimedia Core Network Subsystem this 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-signaling will take place over the PS-domain in the user plane i.e. IP Multimedia Core Network Subsystem is 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 (Authorization of bearer resources) since the Visited Network provides the subscriber with a transport service and its associated QoS.

For IM-services a new security association is required between the mobile and the IMS before access is granted to 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, 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 the same concept/principles will be reused for the IP Multimedia Core Network Subsystem, where it is called IMS AKA.

The Home Network authenticates the subscriber at anytime via the registration or re-registration procedures.

5.1.2 Re-Authentication of the subscriber

Initial registration shall always be authenticated. It is the policy of the operator that decides when to trigger a re-authentication by the S-CSCF. Hence a re-registration might not need to be authenticated.

A SIP REGISTER message, which has not been integrity protected at the first hop, shall be considered as initial registration.

The S-CSCF shall also be able to initiate an authenticated re-registration of a user at any time, independent of previous registrations.

5.1.3 Confidentiality protection

Confidentiality protection shall not be applied to SIP signalling messages between the UE and the P-CSCF.It is recommended to offer encryption for SIP signalling at link layer i.e. between the UE and the RNC using the existing mechanisms as defined in [1].

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [5].

5.1.4 Integrity protection

Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signaling, as specified in section 6.3. The following mechanisms are provided.

1. The UE and the P-CSCF shall negotiate the integrity algorithm that shall be used for the session, as specified in chapter 7.
2. The UE and the P-CSCF shall agree on security associations, which include the integrity keys, that shall be used for the integrity protection. The mechanism is based on IMS AKA and specified in clause 6.1.
3. The UE and the P-CSCF shall both verify that the data received originates from a node, which has the agreed integrity key. This verification is also used to detect if the data has been tampered with.
4. Replay attacks and reflection attacks shall be mitigated.

Integrity protection between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [5].

5.2 Network topology hiding

The operational details of an operator's network are sensitive business information that operators are reluctant to share with their competitors. While there may be situations (partnerships or other business relations) where the sharing of such information is appropriate, the possibility should exist for an operator to determine whether or not the internals of its network need to be hidden.

It shall be possible to hide the network topology from other operators, which includes the hiding of the number of S-CSCFs, the capabilities of the S-CSCFs and the capability of the network.

The I-CSCF shall have the capability to encrypt the address of an S-CSCF in SIP Via, Record-Route, Route and Path headers and then decrypt the address when handling the response to a request. The P-CSCF may receive routing information that is encrypted but the P-CSCF will not have the key to decrypt this information.

The mechanism shall support the scenario that different I-CSCFs in the HN may encrypt and decrypt the address of the S-CSCFs.

6 Security mechanisms

6.1 Authentication and key agreement

The scheme for authentication and key agreement in the IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. Figure 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 ISIM share a long-term key associated with the IMPI.

The HN shall choose the IMS AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g. keys generated by the IMS AKA scheme are transported by SIP.

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]. The ISIM and the HSS keep track of counters SQN_{ISIM} and SQN_{HSS} respectively. The requirements on the handling of the counters and mechanisms for sequence number management are specified in [1]. The AMF field can be used in the same way as in [1].

Furthermore a security association is established between the UE and the P-CSCF. The subscriber may have several IMPUs associated with one IMPI. These may belong to the same or different service profiles. Only one SA shall be active between the UE and the P-CSCF. This single SA shall be updated when a new successful authentication of the subscriber has occurred, cf. section 7.4.

It is the policy of the HN that decides if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles. Regarding the definition of service profiles cf. [3].

6.1.1 Authentication of an IM-subscriber

Before a user can get access to the IM services at least one IMPU needs to be registered and the IMPI authenticated in the IMS at application level. In order to get registered the UE sends a SIP REGISTER message towards the SIP registrar server i.e. the S-CSCF, cf. Figure 1, which will perform the authentication of the user. The message flows are the same regardless of whether the user has an IMPU already registered or not.

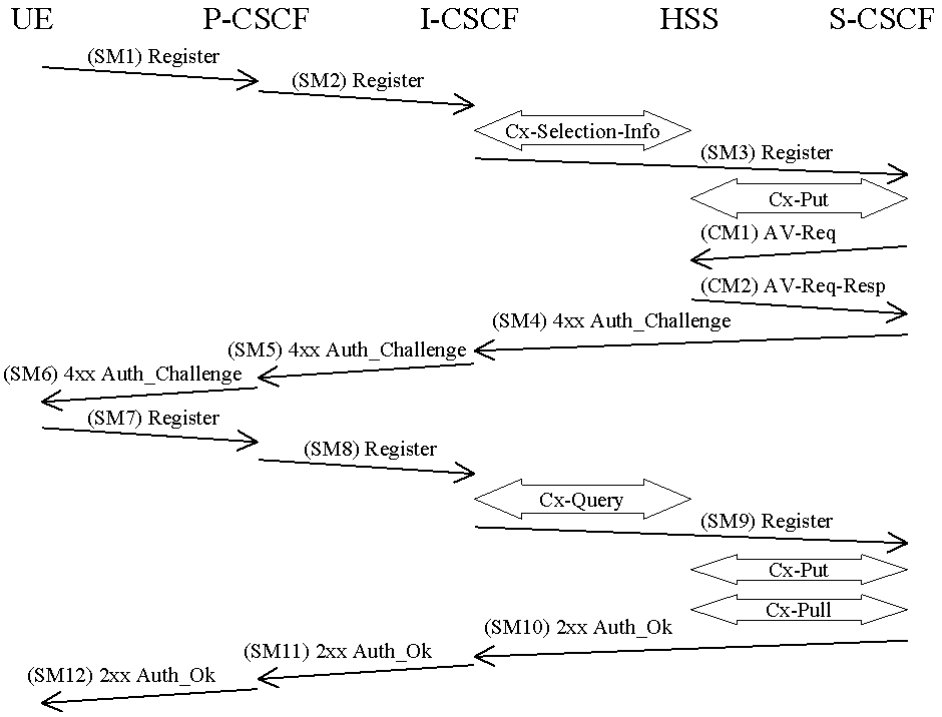


Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

The detailed requirements and complete registration flows are defined in [8] and [11].

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

SM1:
REGISTER(IMPI, IMPU)

In SM2 and SM3 the P-CSCF and the I-CSCF respectively forwards the SIP REGISTER towards the S-CSCF.

After receiving SM3, if the IMPU is not currently registered at the S-CSCF, the S-CSCF needs to set the registration flag at the HSS to initial registration pending. This is done in order to handle mobile terminated calls while the initial registration is in progress and not successfully completed. The registration flag is stored in the HSS together with the S-CSCF name and user identity, and is used to indicate whether a particular IMPU of the user is unregistered or registered at a particular S-CSCF or if the initial registration at a particular S-CSCF is pending. The registration flag is set by the S-CSCF sending a Cx-Put to the HSS. If the IMPU is currently registered, the S-CSCF shall leave the registration flag set to *registered*. At this stage the HSS has performed a check that the IMPI and the IMPU belong to the same user.

Upon receiving the SIP REGISTER the S-CSCF CSCF shall use an Authentication Vector (AV) for authenticating and agreeing a key with the user. If the S-CSCF has no valid AV then the S-CSCF shall send a request for AV(s) to the HSS in CM1 together with the number n of AVs wanted where n is at least one.

CM1:
Cx-AV-Req(IMPI, n)

Upon receipt of a request from the S-CSCF, the HSS sends an ordered array of *n* authentication vectors to the S-CSCF using CM2. The authentication vectors are ordered based on sequence number. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the S-CSCF and the IMS user.

CM2:
Cx-AV-Req-Resp(IMPI, RAND1||AUTN1||XRES1||CK1||IK1,….,RANDn||AUTNn||XRESn||CKn||IKn)

When the S-CSCF needs to send an authentication challenge to the user, it selects the next authentication vector from the ordered array, i.e. authentication vectors in a particular S-CSCF are used on a first-in / first-out basis.

The S-CSCF sends a SIP 4xx Auth_Challenge i.e. an authentication challenge towards the UE including the challenge RAND, the authentication token AUTN in SM4. It also includes the integrity key IK and the cipher key CK for the P-CSCF. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of authenticate challenge.

[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.]

SM4:
4xx Auth_Challenge(IMPI, RAND, AUTN, IK, CK)

When the P-CSCF receives SM5 it shall store the key(s) and remove that information and forward the rest of the message to the UE i.e.

SM6:
4xx Auth_Challenge(IMPI, RAND, AUTN)

Upon receiving the challenge, SM6, the UE 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 calculates the response, RES, puts it into the Authorization header and sends it back to the registrar in SM7. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of the response. It should be noted that the UE at this stage also computes the session keys CK and IK.

SM7:
REGISTER(IMPI, RES)

The P-CSCF forwards the RES in SM8 to the I-CSCF, which queries the HSS to find the address of the S-CSCF. In SM9 the I-CSCF forwards the RES to the S-CSCF.

Upon receiving SM9 containing the response, the S-CSCF retrieves the active XRES for that user and uses this to check the response sent by the UE as described in Draft-ietf-sip-digest-aka-01 [17]. If the check is successful then the user has been authenticated and the IMPU is registered in the S-CSCF. If the IMPU was not currently registered, the S-CSCF shall send a Cx-Put to update the registration-flag to *registered*. If the IMPU was currently registered the registration-flag is not altered.

It shall be possible to implicitly register IMPU(s). The implicitly registered IMPU(s) all belong to the same Service Profile. All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S-CSCF and subsequently to the P-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

When an IMPU has been registered this registration will be valid for some period of time. Both the UE 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. A successful registration of a previously registered IMPU (including implicitly registered IMPUs) means the expiry time of the registration is refreshed.

It should be noted that the UE initiated re-registration opens up a potential denial-of-service attack. That is, an attacker could try to register an already registered IMPU and respond with the wrong RES and in order to make the HN de-register the IMPU. For this reason a subscriber should not be de-registered if it fails an authentication. It shall be defined by the policy of the operator when successfully registered IMPU(s) are to be de-registered.

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

6.1.2 Authentication failures

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

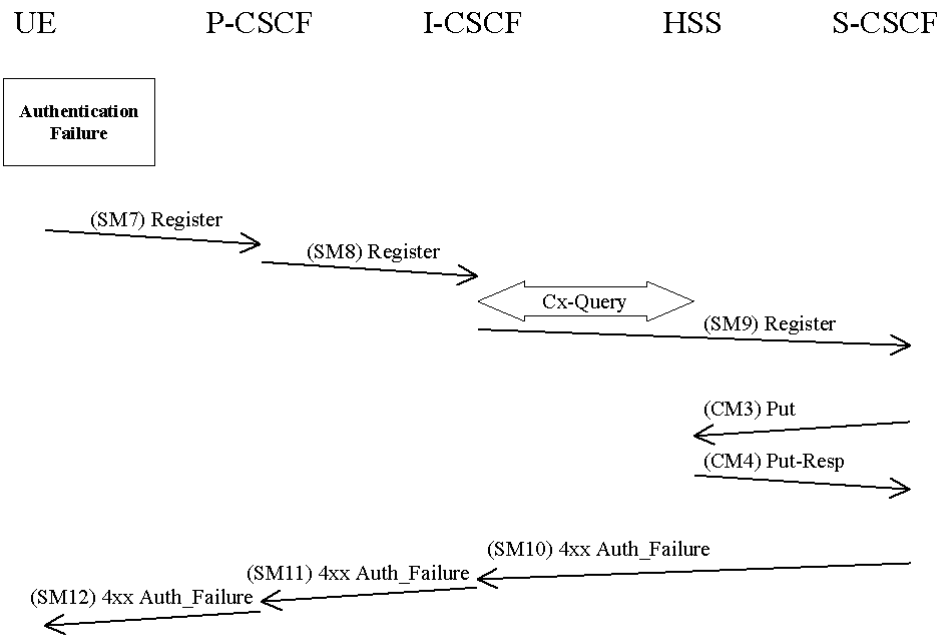
6.1.2.1 User authentication failure

In this case the authentication of the user should fail at the S-CSCF due an incorrect RES (received in SM9). However, in this case when RES is incorrect, the IK used to protect SM7 will be incorrect as well and integrity check at P-CSCF will fail before RES can be verified at S-CSCF.

P-CSCF in this case shall discard SM7 and the registration and authentication procedures shall be then aborted.

6.1.2.2 Network authentication failure

In this section the case when the authentication of the network is not successful is specified. When the check of the MAC in the UE fails the network can not be authenticated and hence registration fails. The flow is identical as for the successful registration in 6.1.1 up to SM6.



The UE shall send a Register message towards the HN including an indication of the cause of failure in SM7. The P-CSCF and the I-CSCF forward this message to the S-CSCF.

SM7:
REGISTER(Failure = *AuthenticationFailure*, IMPI)

Upon receiving SM9, which includes the cause of authentication failure, the S-CSCF sends a Cx-Put in CM3 and receives a Cx-Put-Resp in CM4.

CM3:
Cx-AV-Put(IMPI, Clear S-CSCF name)

The S-CSCF sends a Cx-Put (CM3) to the HSS, which indicates that authentication failed and that, the S-CSCF should be cleared. The HSS responds with a Cx-Put-Resp in CM4.

In SM10 the S-CSCF sends a 4xx Auth_Failure towards the UE indicating that authentication has failed, no security parameters shall be included in this message.

SM10:
SIP/2.0 4xx Auth_Failure

Upon receiving SM10 the I-CSCF shall clear any registration information related to the IMPI.

[Editor's note: It is FFS if same header i.e. 4xx Auth_Failure shall be used for both UE and network authentication failure.]

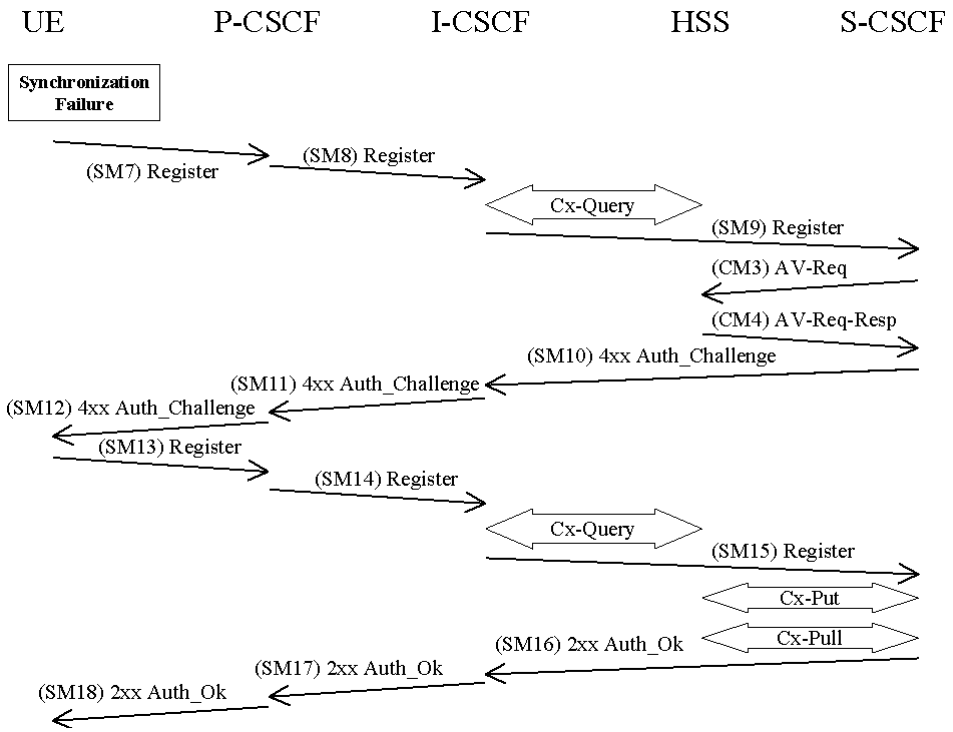
6.1.2.3 Incomplete authentication

If the S-CSCF does not receive a response to an authentication within an acceptable time, it considers the authentication to have failed. If the IMPU was not already registered, the S-CSCF shall send a Cx-Put to the HSS to set the registration-flag for that IMPU to unregistered (see message CM3 in clause 6.1.2.2). If the IMPU was already registered, the S-CSCF does not change the registration-flag.

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.]

In this section the case of an authenticated registration with synchronization failure is described. After re-synchronization, authentication may be successfully completed, but it may also happen that in subsequent attempts other failure conditions (i.e. user authentication failure, network authentication failure) occur. In below only the case of synchronization failure with subsequent successful authentication is shown. The other cases can be derived by combination with the flows for the other failure conditions.



The flow equals the flow in 6.1.1 up to SM6. When the UE receives SM6 it detects that the SQN is out of range and sends a synchronization failure back to the S-CSCF in SM7. Draft-ietf-sip-digest-aka-01 [17] describes the fields to populate corresponding parameters of synchronization failure.

SM7:
REGISTER(Failure = *Synchronization Failure,* AUTS, IMPI*)*

Upon receiving the *Synchronization Failure* and the AUTS the S-CSCF sends an Av-Req to the HSS in CM3 including the required number of Avs, n.

CM3:
Cx-AV-Req(IMPI, RAND,AUTS, n)

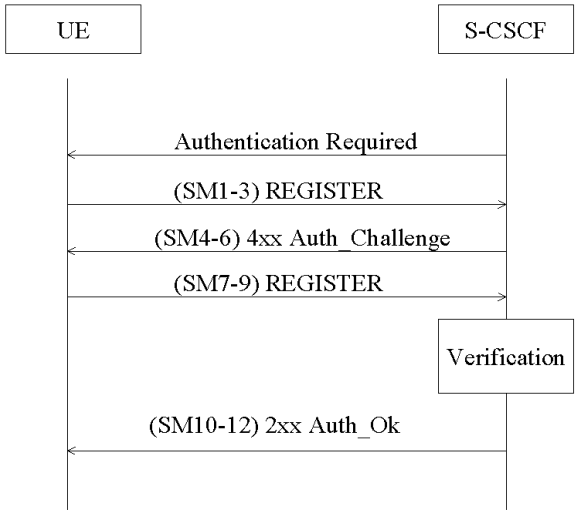
The HSS checks the AUTS as in section 6.3.5 in [1]. If the check is successful and potentially after updating the SQN the HSS creates and sends new AVs to the S-CSCF in CM4.

CM4:
Cx-AV-Req-Resp(IMPI, n,$RAND_1$||$AUTN_1$||$XRES_1$||CK_1||IK_1,….,$RAND_n$||$AUTN_n$||$XRES_n$||CK_n||IK_n)

The rest of the messages i.e. SM10-SM18 including the Cx messages are exactly the same as SM4-SM12 and the corresponding Cx messages in 6.1.1.

6.1.4 Network Initiated authentications

In order to authenticate an already registered user, the S-CSCF shall send a request to the UE to initiate a re-registration procedure. When received at the S-CSCF, the re-registration shall trigger a new IMS AKA procedure that will allow the S-CSCF to re-authenticate the user.



The UE shall initiate the re-registration on the reception of the Authentication Required indication. In the event that the UE does not initiate the re-registration procedure after the request from the S-CSCF, the S-CSCF may decide to de-register the subscriber or re-issue an Authentication-Required.

6.1.5 Integrity protection indicator

In order to decide whether a REGISTER request from the UE needs to be authenticated, the S-CSCF needs to know about the integrity protection applied to the message. The P-CSCF attaches an indication to the REGISTER request to inform the S-CSCF that the message was integrity protected if:

- the P-CSCF receives a REGISTER containing an authentication response and the message is protected with the SA created during this authentication procedure; or

- the P-CSCF receives a REGISTER not containing an authentication response and the message is protected with the SA created by latest successful authentication (from the P-CSCF perspective).

For all other REGISTER requests the P-CSCF attaches an indication that the REGISTER request was not integrity protected or ensures that there is no indication about integrity protection in the message.

6.2 Confidentiality mechanisms

No confidentiality mechanism is provided in this specification, cf. clause 5.1.3.

6.3 Integrity mechanisms

IPsec ESP as specified in reference [13] shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. IPSec ESP general concepts on Security Policy management, Security Associations and IP traffic processing as described in reference [14] shall also be considered. ESP integrity shall be applied in transport mode between UE and P-CSCF.

The method to set up ESP security associations (SAs) during the SIP registration procedure is specified in clause 7. As a result of the registration procedure, two pairs of unidirectional SAs between the UE and the P-CSCF, one pair for TCP and one pair for UDP, shall be simultaneously established. Each pair consists of an SA for traffic from the UE to the P-CSCF (inbound SA at the P-CSCF) and an SA for traffic from the P-CSCF to the UE (outbound SA at the P-CSCF).

The integrity key IK_{ESP} is the same for the four simultaneously established SAs. The integrity key IK_{ESP} is obtained from the key IK_{IM} established as a result of the AKA procedure, specified in clause 6.1, using a suitable key expansion function. This key expansion function depends on the ESP integrity algorithm and is specified in Annex I of this specification.

The integrity key expansion on the user side is done in the UE. The integrity key expansion on the network side is done in the P-CSCF.

The anti-replay service shall be enabled in the UE and the P-CSCF on all established SAs.

6.4 Hiding mechanisms

The Hiding Mechanism is optional for implementation. All I-CSCFs in the HN shall share the same encryption and decryption key Kv. If the mechanism is used and the operator policy states that the topology shall be hidden the I-CSCF shall encrypt the hiding information elements when the I-CSCF forwards SIP Request or Response messages outside the hiding network's domain. The hiding information elements are entries in SIP headers, such as Via, Record-Route, Route and Path, which contain addresses of SIP proxies in hiding network. When I-CSCF receives a SIP Request or Response message from outside the hiding network's domain, the I-CSCF shall decrypt those information elements that were encrypted by I-CSCF in this hiding network domain.

The purpose of encryption in network hiding is to protect the identities of the SIP proxies and the topology of the hiding network. Therefore, an encryption algorithm in confidentiality mode shall be used. The network hiding mechanism will not address the issues of authentication and integrity protection of SIP headers. The AES in CBC mode with 128-bit block and 128-bit key shall be used as the encryption algorithm for network hiding. In the CBC mode under a given key, if a fixed IV is used to encrypt two same plaintexts, then the ciphertext blocks will also be equal. This is undesirable for network hiding. Therefore, random IV shall be used for each encryption. The same IV is required to decrypt the information. The IV shall be included in the same SIP header that includes the encrypted information.

[Editor's note: The following open issues are still to be resolved:

- use of a key identifier for the support of multiple encryption secret keys
- possible use of a MAC to protect integrity of the resulting cipher text
- impact on compressibility of incoming SIP messages
- key management and distribution amongst I-CSCFs
- implications on development of SIP are to be considered

]

7 Security association set-up procedure

The security association set-up procedure is necessary in order to decide what security services to apply and when the security services start. In the IMS authentication of users is performed during registration as specified in clause 6.1. Subsequent signaling communications in this session will be integrity protected based on the keys derived during the authentication process.

7.1 Security association parameters

For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys that are provided by IMS AKA, and a set of parameters specific to a protection method. The security mode setup (cf. clause 7.2) is used to negotiate the SA parameters required for IPsec ESP with authentication, but without confidentiality.

The SA parameters that shall be negotiated between UE and P-CSCF in the security mode set-up procedure, are:

- **Integrity algorithm**

NOTE 1: What is called "authentication algorithm" in [13] is called "integrity algorithm" in this specification in order to be in line with the terminology used in other 3GPP specifications and, in particular, to avoid confusion with the authentication algorithms used in the AKA protocol.

The integrity algorithm is either HMAC-MD5-96 [15] or HMAC-SHA-1-96 [16].

NOTE 2: This, in particular, excludes the use of the NULL integrity algorithm.

Both integrity algorithms shall be supported by both, the UE and the P-CSCF as mandated by [13]. In the unlikely event that one of the integrity algorithm is compromised during the lifetime of this specification, this algorithm shall no longer be supported.

NOTE 3: If only one of the two integrity algorithms is compromised then it suffices for the IMS to remain secure that the algorithm is no longer supported by any P-CSCF. The security mode set-up procedure (cf. clause 7.2) will then ensure that the other integrity algorithm is selected.

- **SPI (Security Parameter Index)**

The SPI is allocated locally for inbound SAs. The triple (SPI, destination IP address, security protocol) uniquely identifies an SA at the IP layer. The most significant bit of any SPI allocated by the P-CSCF shall be "0" and the most significant bit of any SPI allocated by the UE shall be "1".

NOTE 4: This allocation of SPIs ensures that protected messages in the uplink always differ from protected messages in the downlink in, at least, the SPI field. This thwarts reflection attacks. When several applications use IPsec on the same physical interface the SIP application should be allocated a separate range of SPIs.

The following SA parameters are not negotiated:

- Life type: the life type is always seconds;
- SA duration: the SA duration has a fixed length of 2^{32}-1;

NOTE 5: The SA duration is a network layer concept. From a practical point of view, the value chosen for "SA duration" does not impose any limit on the lifetime of an SA at the network layer. The SA lifetime is controlled by the SIP application as specified in clause 7.4.

- Mode: transport mode;
- Key length: the length of the integrity key IK_{ESP} depends on the integrity algorithm. It is 128 bits for HMAC-MD5-96 and 160 bits for HMAC-SHA-1-96.

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. source and destination IP addresses, transport protocol, and source and destination ports.

- IP addresses are bound to a pair of SAs, as in clause 6.3, as follows:

  - inbound SA at the P-CSCF:
    The source and destination IP addresses associated with the SA are identical to those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

  - outbound SA at the P-CSCF:
    the source IP address bound to the outbound SA equals the destination IP address bound to the inbound SA; the destination IP address bound to the outbound SA equals the source IP address bound to the inbound SA.

NOTE 6: This implies that the source and destination IP addresses in the header of the IP packet in which the protected SIP REGISTER message was received by the P-CSCF need to be the same as those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

- The transport protocol is either TCP or UDP.

- Ports:

1. The P-CSCF receives messages protected with ESP from any UE on one fixed port (the"protected port") different from the standard SIP port 5060. The number of the protected port is communicated to the UE during the security mode set-up procedure, cf. clause 7.2. No unprotected messages shall be sent to or received on this port. From a security point of view, the P-CSCF may receive unprotected messages from any UE on any port which is different from the protected port.

NOTE 7: The protected port is fixed for a particular P-CSCF, but may be different for different P-CSCFs.

2. For protected or unprotected outbound messages from the P-CSCF (inbound for the UE) any port number may be used at the P-CSCF from a security point of view.

3. For each security association, the UE assigns a port to send or receive protected messages to and from the P-CSCF ("protected port"). No unprotected messages shall be sent to or received on this port. The UE may use different protected port numbers for TCP and UDP. The numbers of these ports are communicated to the P-CSCF during the security mode set-up procedure, cf. clause 7.2. From a security point of view, the UE may send or receive unprotected messages to or from the P-CSCF on any ports which are not protected ports.

Editor's note: The condition that the UE sends and receives protected messages on the same port is not necessary from a security point of view. These ports could be made different, at the expense of one more parameter to be negotiated in the security mode set-up procedure, but they have to be fixed in the registration procedure.

4. The P-CSCF is allowed to receive only REGISTER messages on unprotected ports. All other messages not arriving on the protected port shall be discarded by the P-CSCF.

5. The UE is allowed to receive only the following messages on an unprotected port:

   - responses to unprotected REGISTER messages;

   - error messages.

   All other messages not arriving on a protected port shall be discarded by the UE.

The following rules apply:

1. For each SA which has been established and has not expired, the SIP application at the P-CSCF stores at least the following data: (UE_IP_address, UE_protected_port, transport protocol, SPI, IMPI, IMPU1, ... , IMPUn, lifetime) in an "SA_table".

NOTE 8: The SPI is only required when initiating and deleting SAs in the P-CSCF. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

2. The SIP application at the P-CSCF shall check upon receipt of a protected REGISTER message that the source IP address in the packet header coincides with the UE's IP address given in the contact header of the protected REGISTER message. If the contact header does not explicitly contain the UE's IP address, but rather a symbolic name then the P-CSCF shall first resolve the symbolic name by suitable means to obtain an IP address.

3. The SIP application at the P-CSCF shall check upon receipt of an initial REGISTER message that, for each transport protocol, the triple (UE_IP_address, UE_protected_port, transport protocol), where the UE_IP_address is the source IP address in the packet header and the protected port is sent as part of the security mode set-up procedure (cf. clause 7.2), has not yet been associated with entries in the "SA_table". Furthermore, the P-CSCF shall check that, for any one IMPI, no more than three SAs per direction and per transport protocol are stored at any one time. If these checks are unsuccessful the registration is aborted and a suitable error message is sent to the UE.

NOTE 9: According to clause 7.4 on SA handling, at most three SAs per direction and per transport protocol need to exist at a P-CSCF for one user at any one time.

4. For each incoming protected message the SIP application at the P-CSCF shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the triple (UE_IP_address, UE_protected_port, transport protocol) in the "SA_table". The SIP application at the P-CSCF shall further check that the IMPU associated with the SA in the "SA_table" and the IMPU in the received SIP message coincide. If this is not the case the message shall be discarded.

5. For each SA which has been established and has not expired, the SIP application at the UE stores at least the following data: (UE_protected_port, transport protocol, SPI, lifetime) in an "SA_table".

NOTE 10: The SPI is only required to initiate and delete SAs in the UE. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

6. When establishing two new pairs of SAs (cf. clause 6.3) the SIP application at the UE shall ensure that, for each transport protocol, the selected number for the protected port does not correspond to an entry in the "SA_table".

NOTE 11: Regarding the selection of the number of the protected port at the UE it is generally recommended that the UE randomly selects the number of the protected port from a sufficiently large set of numbers not yet allocated at the UE. This is to thwart a limited form of a Denial of Service attack. UMTS PS access link security also helps to thwart this attack.

7. For each incoming protected message the SIP application at the UE shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the pair (UE_protected_port, transport protocol) in the "SA table".

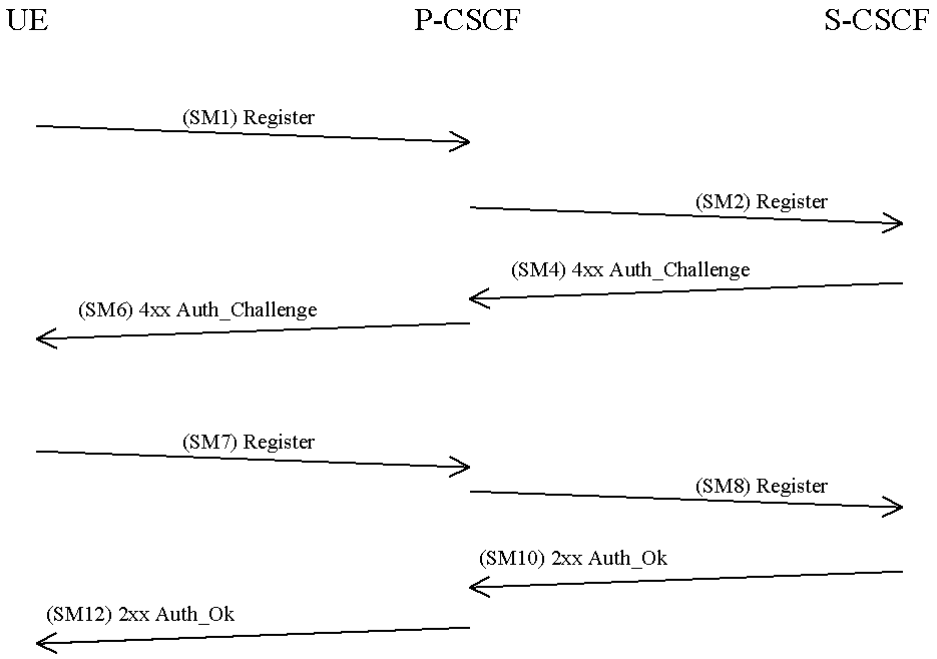
NOTE 12: If the integrity check of a received packet fails then IPsec will automatically discard the packet.

8. The lifetime of an SA at the application layer between the UE and the P-CSCF shall equal the registration period.

7.2 Set-up of security associations (successful case)

The set-up of security associations is based on [draft-IETF-sip-sec-agree]. Annex H of this specification shows how to use [draft-IETF-sip-sec-agree] for the set-up of security associations.

In this section the normal case is specified i.e. when no failures occurs. Note that for simplicity some of the nodes and messages have been omitted. Hence there are gaps in the numbering of messages, as the I-CSCF is omitted.



The UE sends a Register message towards the S-CSCF to register the location of the UE and to set-up the security mode, cf. clause 6.1. In order to start the security mode set-up procedure, the UE shall include a *Security-setup*-line in this message.

The *Security-setup-line* in SM1 contains the SPIs and the numbers of the protected ports assigned by the UE for the SAs for TCP and UDP. It also contains a list of identifiers for the integrity algorithms which the UE supports.

SM1:
REGISTER(Security-setup = *SPI_U_TCP, SPI_U_UDP, Port_U_TCP, Port_U_UDP, UE integrity algorithms list)*

Upon receipt of SM1, the P-CSCF temporarily stores the parameters received in the *Security-setup-line* together with the UE's IP address from the source IP address of the IP packet header, the IMPI and IMPU. Upon receipt of SM4, the P-CSCF adds the key IK_{IM} received from the S-CSCF to the temporarily stored parameters. The P-CSCF then selects the SPIs for the inbound SAs for TCP and UDP.

In order to determine the integrity algorithm the P-CSCF proceeds as follows: the P-CSCF has a list of integrity algorithms it supports, ordered by priority. The P-CSCF selects the first integrity algorithm on its own list which is also supported by the UE.

The P-CSCF then establishes the two pairs of SAs in the local security association database.

The *Security-setup*-line in SM6 contains the SPIs assigned by the P-CSCF for the SAs for TCP and UDP and the fixed number of the protected port at the P-CSCF. It also contains a list of identifiers for the integrity algorithms which the P-CSCF supports.

SM6:
4xx Auth_Challenge(Security-setup = *SPI_P_TCP, SPI_P_UDP, Port_P*, *P-CSCF integrity algorithms list)*

Upon receipt of SM6, the UE determines the integrity algorithm as follows: the UE selects the first integrity algorithm on the list received from the P-CSCF in SM 6 which is also supported by the UE.

The UE then proceeds to establish the two pairs of SAs in the local SAD.

The UE shall integrity-protect SM7 and all following SIP messages. Furthermore the integrity algorithms list received in SM6 shall be included:

SM7:
REGISTER(Security-setup = *P-CSCF integrity algorithms list)*

After receiving SM7 from the UE, the P-CSCF shall check whether the integrity algorithms list received in SM7 is identical with the integrity algorithms list sent in SM6. If this is not the case the registration procedure is aborted. The P-CSCF shall include in SM8 information to the S-CSCF that the received message from the UE was integrity protected. The P-CSCF shall add this information to all subsequent REGISTER messages received from the UE that have successfully passed the integrity check in the P-CSCF.

SM8:
REGISTER(Integrity-Protection = *Successful,* IMPI*)*

The P-CSCF finally sends SM12 to the UE. SM12 does not contain information specific to security mode setup (i.e. a Security-setup line), but with sending SM12 not indicating an error the P-CSCF confirms that security mode setup has been successful. After receiving SM12 not indicating an error, the UE can assume the successful completion of the security-mode setup.

7.3 Error cases in the set-up of security associations

7.3.1 Error cases related to IMS AKA

Errors related to IMS AKA failures are specified in section 6.1. However, this section additionally describes how these shall be treated, related to security setup.

7.3.1.1 User authentication failure

In this case, SM7 fails integrity check by IPsec at the P-CSCF if the IK_{IM} derived from RAND at UE is wrong. The SIP application at the P-CSCF never receives SM7. It shall delete the temporarily stored SA parameters associated with this registration after a time-out.

In case IK_{IM} was derived correctly, but the response was wrong the authentication of the user fails at the S-CSCF due to an incorrect response. The S-CSCF will send a 4xx Auth_Failure message to the UE, via the P-CSCF, which may pass through an already established SA. Afterwards, both, the UE and the P-CSCF delete the new SAs.

7.3.1.2 Network authentication failure

If the UE is not able to successfully authenticate the network, the UE shall send a REGISTER message which may pass through an already established SA, indicating a network authentication failure, to the P-CSCF. The P-CSCF deletes the new SAs after receiving this message.

7.3.1.3 Synchronisation failure

In this situation, the UE observes that the AUTN sent by the network in SM6 contains an out-of-range sequence number. The UE shall send a REGISTER message to the P-CSCF, which may pass through an already established SA, indicating the synchronization failure. The P-CSCF deletes the new SAs after receiving this message.

7.3.1.4 Incomplete authentication

If the UE responds to an authentication challenge from a S-CSCF, but does not receive a reply before the request times out, the UE shall start a registration procedure if it still requires any IM services. The first message in this registration should be protected with an SA created by a previous successful authentication if one exists.

If the P-CSCF deletes a registration SA due to its lifetime being exceeded, the P-CSCF should delete any information relating to that registration procedure.

7.3.2 Error cases related to the Security-Set-up

7.3.2.1 Proposal unacceptable to P-CSCF

In this case the P-CSCF cannot accept the proposal set sent by the UE in the Security-Set-up command of SM1. SM6 shall respond to SM1 with indicating a failure, by sending a 4xx Unacceptable_Proposal.

The P-CSCF therefore shall modify the message SM2 such that the S-CSCF sends a 4xx Unacceptable_Proposal message back to the UE in SM4 and 6 and the registration process is finished.

7.3.2.2 Proposal unacceptable to UE

If the P-CSCF sends in the security-setup line of SM6 a proposal that is not acceptable for the UE, the UE shall terminate the registration procedure.

7.3.2.3 Failed consistency check of Security-Set-up lines at the P-CSCF

The P-CSCF shall check whether authentication algorithms list received in SM7 is identical with the authentication algorithms list sent in SM6. If this is not the case the registration procedure is aborted. (Cf. clause 7.2).

7.4 Authenticated re-registration

If the registration is a re-registration, a pair of security associations between UE and P-CSCF is already active. The authenticated re-registration shall initially utilize the existing SA. This is the normal case. However, in the event the UE originates the (SM1) Register message using no protection, the P-CSCF shall still accept it and forward the request to the S-CSCF, indicating that the register message was not integrity protected. This shall trigger the S-CSCF to challenge the subscriber with the execution of a new IMS-AKA authentication procedure as described in clause 6.1.1.

[Editors Note: The exact mechanism for changing SAs is currently under investigation.]

Before SM7 is sent by the UE, both peers shall replace the existing SA by the new SA negotiated during these first two messages.

[Editors Note: The exact mechanism when to change SA1 to SA2 under certain error conditions is FFS.]

7.4.1 Handling of security associations in authenticated re-registrations (successful case)

Before re-registration begins the following SAs exist:

- SA1 from UE to P-CSCF;
- SA2 from P-CSCF to UE.

The re-registration then is as follows:

1) The UE sends SM1 to re-register with the IMS, using the existing SA1 to the P-CSCF. As in the case of a new registration, a list of parameters to be negotiated in a security association set-up is included.

[Editors Note: It is FFS if the SA1 shall be used for SM1 or not]

2) The P-CSCF waits for the response SM4 from the S-CSCF and then sends SM6 to the UE, using SA2. As in the case of a new registration, the parameters selected for the new security associations are included. The P-CSCF then creates two new security associations, in parallel to the existing ones, in its database:

   - SA11 from UE to P-CSCF;

   - SA12 from P-CSCF to UE.

3) If SM6 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends SM7 to the P-CSCF. As in the case of a new registration, the authentication response and the list of parameters repeated from message 1 are included. SM7 is protected with the new SA11.

4) The P-CSCF waits for the response SM10 from the S-CSCF and then sends SM12 to the UE, using the new SA 12.

5) After the reception of SM12 by the UE, the re-registration is complete.

The UE now uses the new SAs for all subsequent messages. The old (outbound) SA1 is deleted. The old (inbound) SA2 must be kept until a further SIP message protected with the new inbound SA12 is successfully received from the P-CSCF.

The P-CSCF keeps all four SAs with the UE active until a further SIP message protected with the new inbound SA11 is successfully received from the UE. In the meantime, the P-CSCF continues to use the old SA2 for outbound traffic to the UE.

7.4.2 Error cases related to authenticated re-registration

Whenever an expected message is not received after a time-out the receiving entity considers the registration to have failed. The receiving entity then deletes any new security associations it may have established and continues to use the old ones if they have not yet expired.

If the registration protocol goes well up to the last message SM12, and SM12 is sent by the P-CSCF, but not received by the UE , then the UE has only the olds SAs available (after the time-out), but the P-CSCF cannot know this. Therefore, the P-CSCF continues to use the old SA2 for outbound traffic to the UE, but keeps both, old and new SAs. The new SAs are deleted when a message is received from the UE which is protected with the old SA, or if a REGISTER message is received on the port where the P-CSCF accepts specific unprotected messages.

7.5 Rules for security association handling when the UE changes IP address

When a UE changes its IP address, e.g. by using the method described in RFC 3041 [18], then the UE shall initiate an unprotected registration procedure using the new IP address as the source IP address in the packets carrying the REGISTER messages.

8 ISIM

[Editors note: This section is based on the current working assumption in SA1 and SA2.]

For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on a UICC. The following implementation options are permitted:

- Use of a distinct ISIM application on a UICC which does not share security functions with the USIM;

- Use of a distinct ISIM application on a UICC which does share security functions with the USIM;

- Use of a R99/Rel-4 USIM application on a UICC.

NOTE: For later releases other implementations of ISIM are foreseen to be permitted.

There shall only be one ISIM for each IMPI. The IMS subscriber shall not be able to modify or enter the IMPI. The IMS subscriber shall not be able to modify or enter the Home Domain Name.

8.1 Requirements on the ISIM application

This section identifies requirements on the ISIM application to support IMS access security. It does not identify any data or functions that may be required on the ISIM application for non-security purposes.

The ISIM shall include:

- The IMPI;
- At least one IMPU;
- Home Network Domain Name;
- Support for sequence number checking in the context of the IMS Domain;
- The same framework for algorithms as specified for the USIM applies for the ISIM;
- An authentication Key.

The ISIM shall deliver the CK to the UE although it is not required that SIP signaling is confidentiality protected.

At UE power off the existing SAs in the MT shall be deleted. The session keys and related information in the SA shall never be stored on the ISIM.

8.2 Sharing security functions and data with the USIM

When an ISIM is used for IMS access, only the following options for sharing security functions and data are permitted:

- No security functions or data are shared;
- Only the sequence number checking mechanism is shared;
- Only the algorithm is shared;
- Only the algorithm and sequence number checking mechanism are shared;
- The authentication key, authentication functions and the sequence number checking mechanism are shared.

When a USIM is used for IMS access, only the following option is applicable:

- The authentication key, authentication functions and the sequence number checking mechanism are shared.

NOTE: If the authentication keys and functions are shared, the cipher/integrity key sets generated during authentication are used with different cipher/integrity algorithms in CS/PS domain and IMS. Note that the same cipher/integrity key set is never used for both CS/PS domain and IMS because the authentication and key agreement protocol is run independently between CS/PS domain and IMS. Therefore there is no danger that the compromise of the cipher/integrity algorithm in one domain would lead to vulnerabilities in the other domain.

If the mechanism and data for checking sequence numbers are shared then it shall be required for the authentication failure rate due to synchronization failures to be kept sufficiently low. In particular, the mechanism shall be required to support interleaving authentication in three domains (CS, PS and IMS). Example methods to achieve this are described in Annex G.

Annex A:
Void

Annex B:
Void

Annex C:
Void

Annex D:
Void

Annex E:
Void

Annex F:
Void

Annex G (informative): Management of sequence numbers

The example sequence number management schemes in [1] Informative Annex C can be used to ensure that the authentication failure rate due to synchronization failures to kept sufficiently low when the same sequence number mechanism and data is used for authentication in the PS/CS domains and in the IMS. This can be done by enhancing the method for the allocation of index values in the AuC so that authentication vectors distributed to different service domains shall always have different index values (i.e. separate ranges of index values are reserved for PS, CS and IMS operation). The AuC is required to obtain information about which type of service node has requested the authentication vectors. Reallocation of array elements to the IMS domain can be done in the AuC with no changes required to already deployed USIMs.

As the possibility for out of order use of authentication vectors within the IMS service domain may be quite low, the number of PS or CS array elements that need to be reallocated to the IMS domain could be quite small. This means that the ability to support out of order authentication vectors within the PS and CS domains would not be significantly affected.

Sequence number management is operator specific and for some proprietary schemes over the air updating of the UICC may be needed.

Annex H (normative): The use of [draft-IETF-sip-sec-agree] for security mode set-up

[To be added].

Annex I (normative): Key expansion functions for IPsec ESP

If the selected authentication algorithm is HMAC-MD5-96 then $IK_{ESP} = IK_{IM}$.

If the selected authentication algorithm is HMAC-SHA-1-96 then IK_{ESP} is obtained from IK_{IM} by appending the 32 most significant bits of IK_{IM} to IK_{IM}.

Annex J (informative): Change history

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New
2002-03	SP-15	SP-020116	-			Approved at TSG SA #15 and placed under change control	2.0.0	5.0.0
2002-03	SP-15	SP-020174	001		F	Correction of references to obsolete SIP RFC 2543bis IETF internet draft	5.0.0	5.1.0
2002-03	SP-15	SP-020175	002		F	Removal of reference to non Operator IMS provision	5.0.0	5.1.0
2002-06	SP-16	SP-020346	003		F	ISIM related parameters	5.1.0	5.2.0
2002-06	SP-16	SP-020347	004		F	Reference of HTTP Digest AKA in TS 33.203	5.1.0	5.2.0
2002-06	SP-16	SP-020348	005		D	Clean-up of section 6.1.1	5.1.0	5.2.0
2002-06	SP-16	SP-020349	006		F	Integrity protection indicator	5.1.0	5.2.0
2002-06	SP-16	SP-020350	007		F	UE and P-CSCF Behaviour on an Incomplete Authentication	5.1.0	5.2.0
2002-06	SP-16	SP-020351	008		C	Requested Changes for SIP integrity	5.1.0	5.2.0
2002-06	SP-16	SP-020352	009		F	Clean-up of 7.3	5.1.0	5.2.0
2002-06	SP-16	SP-020386	010	1	C	Security association handling in IMS when the UE changes IP address	5.1.0	5.2.0
2002-06	SP-16	SP-020354	011		D	Remove Annexes that describes Extended HTTP Digest solution	5.1.0	5.2.0

History

Document history		
V5.1.0	March 2002	Publication
V5.2.0	June 2002	Publication