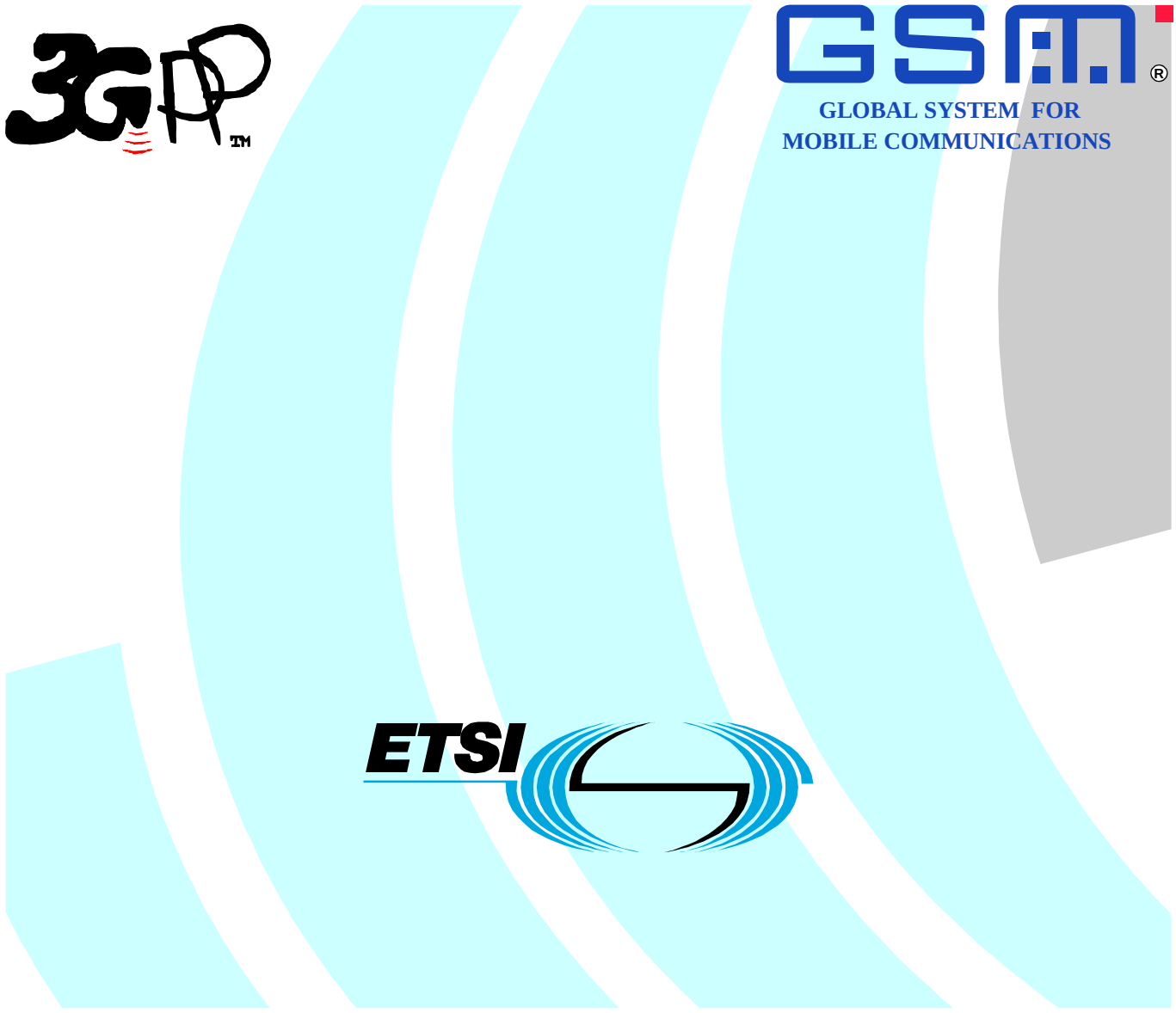
ETSI TS 133 203 V6.6.0 (2005-03)

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 6.6.0 Release 6)



Reference
RTS/TSGS-0333203v660

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

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 http://webapp.etsi.org/key/queryform.asp .

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 signalling protocol for creating and terminating Multimedia sessions, cf. RFC 3261 [6]. This specification only deals with how the SIP signalling 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] IETF RFC 3310 (2002): "HTTP Digest Authentication Using AKA". April, 2002.

[18] IETF RFC 3041 (2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[19] IETF RFC 2402 (1998): "IP Authentication Header".

[20] IETF RFC 2451 (1998): "The ESP CBC-Mode Cipher Algorithms ".

[21] IETF RFC 3329 (2002): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[22] IETF RFC 3602 (2003): " The AES-CBC Cipher Algorithm and Its Use with IPsec".

[23] IETF RFC 3263 (2002): "Session Initiation Protocol (SIP): Locating SIP Servers".

[24] 3GPP TS 33.310: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Domain Security (NDS); Authentication Framework (AF)".

[25] 3GPP TR 33.978: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Aspects Of Early IMS".

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, TS 21.905 [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 clause 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 clause 8.

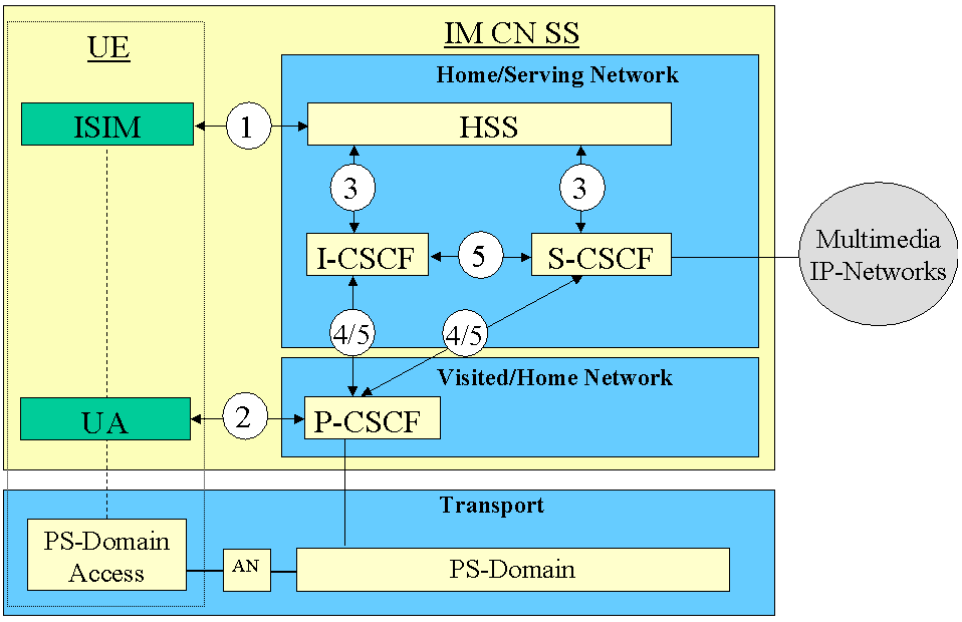


Figure 1: The IMS security architecture

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. TS 23.002 [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. TS 23.002 [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. TS 23.060 [10].

P-CSCF in the Visited Network

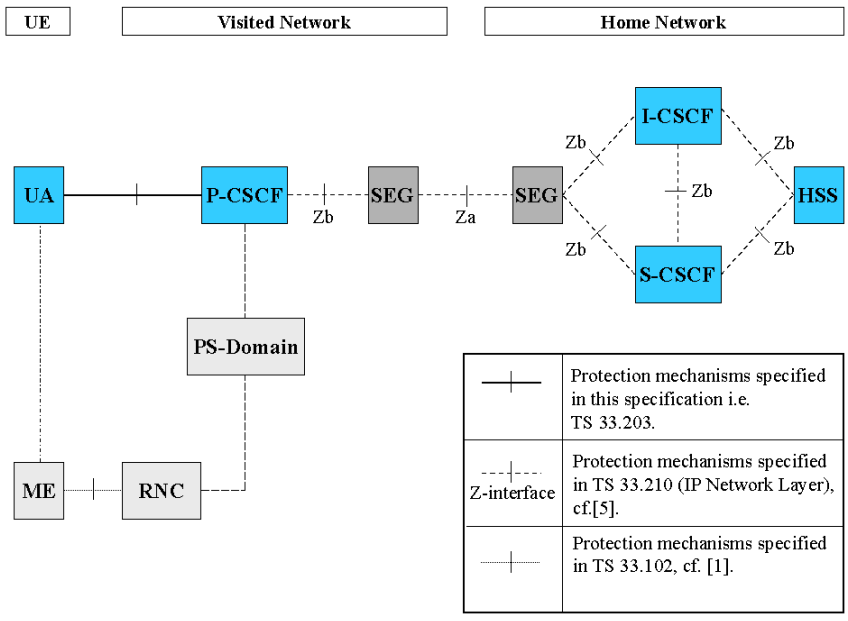


Figure 2: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the VN

P-CSCF in the Home Network

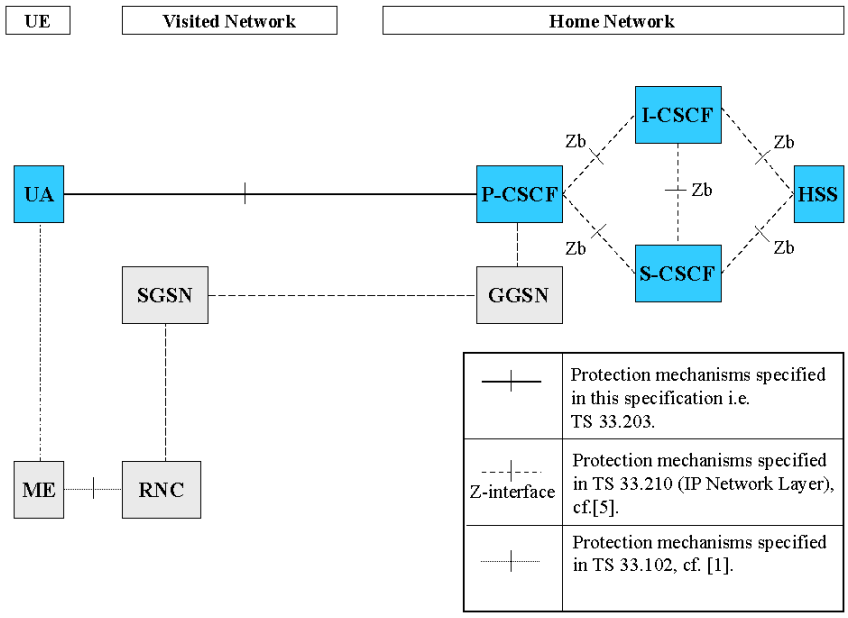


Figure 3: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the HN

The confidentiality and integrity protection for SIP-signalling 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].

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 clause 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. TS 23.228 [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-signalling 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.

NOTE: Although the method of calculating the parameters in UTMS AKA and IMS AKA are identical, the parameters are transported in slightly different ways. In UMTS, the UE"s response RES is sent in the clear, while in IMS RES is not sent in the clear but combined with other parameters to form an authentication response and the authentication response is sent to the network (as described in RFC 3310 [17]).

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

Possibility for IMS specific confidentiality protection shall be provided to SIP signalling messages between the UE and the P-CSCF. Mobile Operators shall take care that the deployed confidentiality protection solution and roaming agreements fulfils the confidentiality requirements presented in the local privacy legislation. The following mechanisms are provided at SIP layer:

1. The UE shall always offer encryption algorithms for P-CSCF to be used for the session, as specified in clause 7.
2. The P-CSCF shall decide whether the IMS specific encryption mechanism is used. If used, the UE and the P-CSCF shall agree on security associations, which include the encryption key that shall be used for the confidentiality protection. The mechanism is based on IMS AKA and specified in clause 6.1.

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in TS 33.210 [5].

5.1.4 Integrity protection

Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signalling, as specified in clause 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 clause 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 TS 33.210 [5].

NOTE 1: TLS is mandatorily supported by SIP proxies according to RFC 3261 [6], and operators may use it to provide confidentiality and integrity inside their networks instead of or on top of IPsec, as the intra-domain Za interface is optional, and TLS may also be used between IMS networks on top of IPsec. It should be pointed out, that the 3GPP specifications do not provide support for TLS certificate management in a fashion similar to TS 33.310 (NDS/AF) [24] nor do they ensure backward compatibility with Release 5 CSCFs nor interoperability with other networks which do not use TLS, in case TLS is used by Release 6 CSCFs. These management and capability issues need then to be solved by manual configuration of the involved operators.

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.

5.3 SIP Privacy handling in IMS Networks

Privacy may in many instances be equivalent with confidentiality i.e. to hide the information (using encryption and encryption keys) from all entities except those who are authorized to understand the information. The SIP Privacy Extensions for IMS Networks do not provide such confidentiality. The purpose of the mechanism is rather to give an IMS subscriber the possibility to withhold certain identity information of the subscriber as specified in IETF RFC 3602 [22] and IETF RFC 3263 [23].

NOTE 1: It is useful that the privacy mechanism for IMS networks does not create states in the CSCFs other than the normal SIP states.

5.4 SIP Privacy handling when interworking with non-IMS Networks

When a Rel-6 IMS is interworking with a non-IMS network, the CSCF in the IMS network shall decide the trust relation with the other end. The other end is trusted when the security mechanism for the interworking (see clause 6.5) is applied as well as the availability of an inter-working agreement. If the interworking non-IMS network is not trusted, the privacy information shall be removed from the traffic towards to this non-IMS network. When receiving SIP signalling, the CSCF shall also verify if any privacy information is already contained. If the interworking non-IMS network is not trusted, the information shall be removed by the CSCF, and retained otherwise.

Because absence of the security mechanism for the interworking (see clause 6.5) indicates an untrusted non-IMS network, separate CSCFs are usually needed to interface with IMS and non-IMS networks. The CSCF interfacing with IMS networks implicitly trusts all IMS networks reachable via the SEG that establishes security according to TS 33.210 [5]. A Rel-5 CSCF always assumes this trust relationship and network configuration. For a Rel-6 CSCF, this implicit trust setting shall be a configuration option, that an operator can set according to his network and interface configuration.

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. TS 23.228 [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 TS 33.102 [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 TS 33.102 [1]. The AMF field can be used in the same way as in TS 33.102 [1].

Furthermore two pairs of (unilateral) security associations (SAs) are 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 two pairs of SAs shall be active between the UE and the P-CSCF. These two pairs of SAs shall be updated when a new successful authentication of the subscriber has occurred, cf. clause 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. TS 23.228 [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.

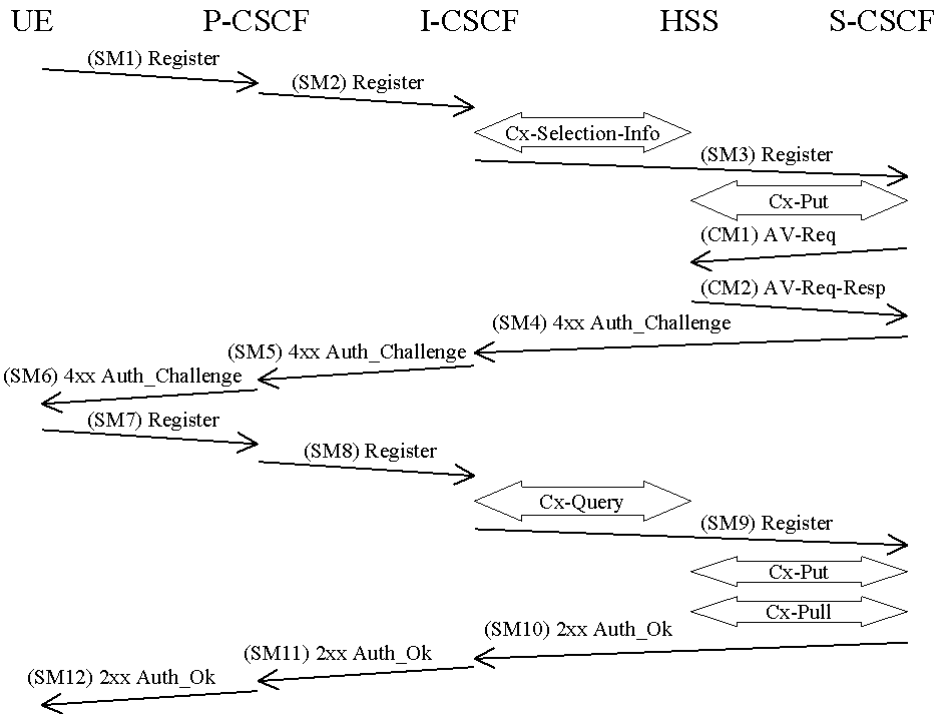


Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

The detailed requirements and complete registration flows are defined in TS 24.229 [8] and TS 24.228 [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 m of AVs wanted where m is at least one.

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

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. RFC 3310 [17] specifies how to populate the parameters of an authentication challenge. The S-CSCF also stores the RAND sent to the UE for use in case of a synchronization failure.

The verification of the SQN by the USIM and ISIM will cause the UE to reject an attempt by the S-CSCF to re-use a AV. Therefore no AV shall be sent more than once.

NOTE: This does not preclude the use of the normal SIP transaction layer re-transmission procedures.

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 TS 33.102 [1]. If both these checks are successful the UE uses RES and some other parameters to calculate an authentication response. This

response is put into the Authorization header and sent back to the registrar in SM7.RFC 3310 [17] specifies how to populate the 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, Authentication response)

The P-CSCF forwards the authentication response 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 authentication response 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 authentication response sent by the UE as described in RFC 3310 [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). (see clause 4.3.3.4 in TS 23.228 [3]). 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 an incorrect authentication response 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 clause 6.3.7 of TS 33.102 [1].

6.1.2 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 response (received in SM9). However, if the response is incorrect, then the IK used to protect SM7 will normally be incorrect as well, which will normally cause the integrity check at the P-CSCF to fail before the response can be verified at S-CSCF. In this case SM7 is discarded by the IPsec layer at the P-CSCF.

If the integrity check passes but the response is incorrect, the message flows are identical up to and including SM9 as a successful authentication. Once the S-CSCF detects the user authentication failure it should proceed in the same way as having received SM9 in a network authentication failure (see clause 6.1.2.2).

6.1.2.2 Network authentication failure

In this clause 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.

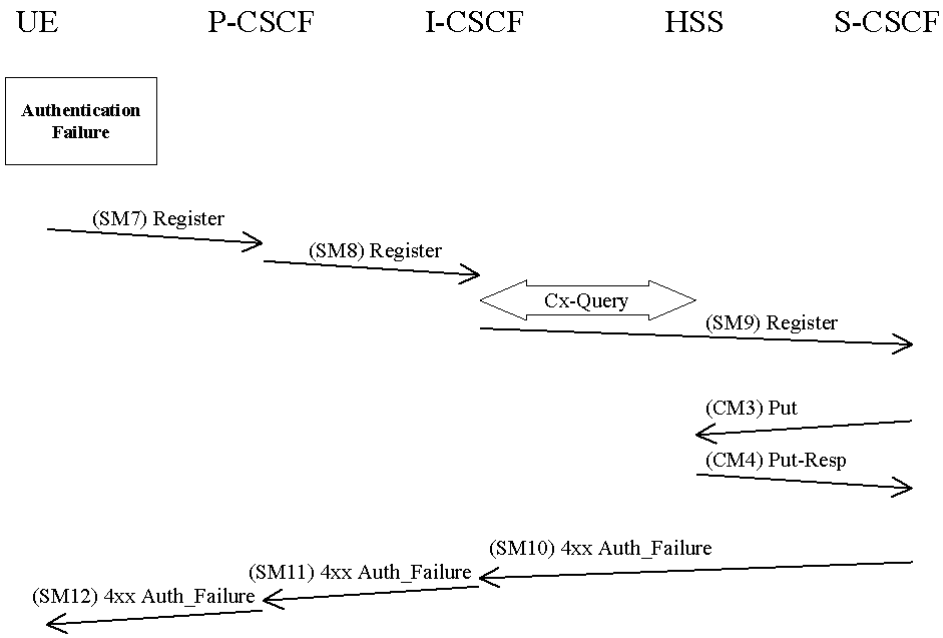


Figure 5

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 shall set the registration-flag in the HSS to *unregistered*, if the IMPU is not currently registered. To set the flag the S-CSCF sends in CM3 a Cx-Put to the HSS. If the IMPU is currently registered, the S-CSCF does not update the registration flag.

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

The HSS responds to CM3 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

6.1.2.3 Incomplete authentication

When the S-CSCF receives a new REGISTER request and challenges this request, it considers any previous authentication to have failed. It shall delete any information relating to the previous authentication, although the S-CSCF may send a response if the previous challenge is answered. A challenge to the new request proceeds as described in clause 6.1.1.

If the S-CSCF does not receive a response to an authentication challenge 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

In this clause 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.

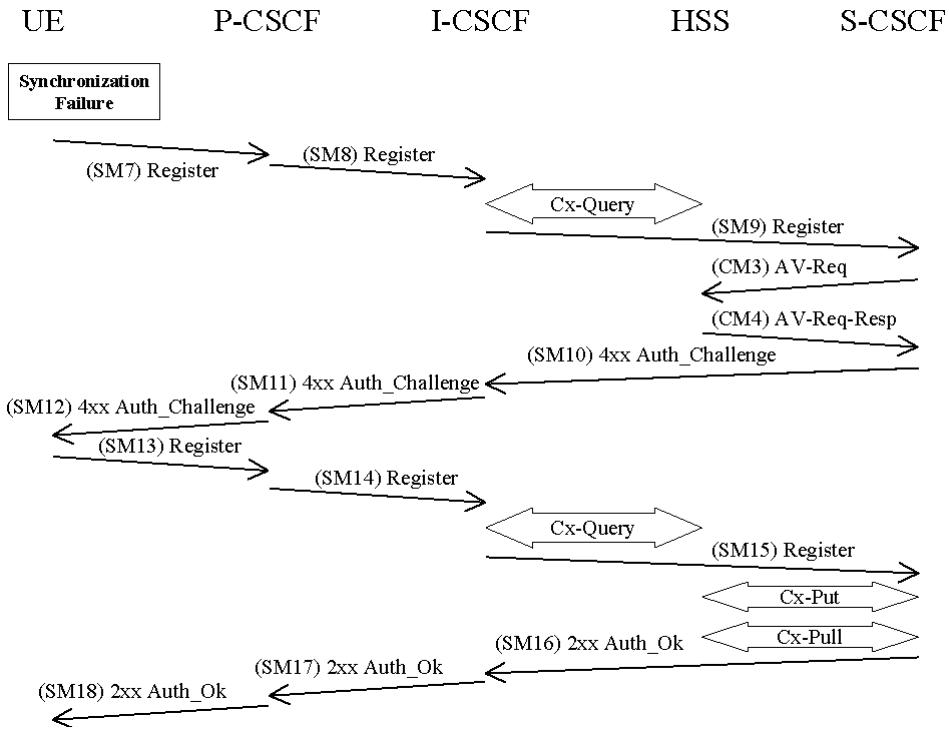


Figure 6

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. RFC 3310 [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 RAND stored by the S-CSCF and the required number of Avs, m.

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

The HSS checks the AUTS as in clause 6.3.5 of TS 33.102 [1]. After potentially updating the SQN, the HSS 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)

When the S-CSCF receives the new batch of authentication vectors from the HSS it deletes the old ones for that user in the S-CSCF.

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.

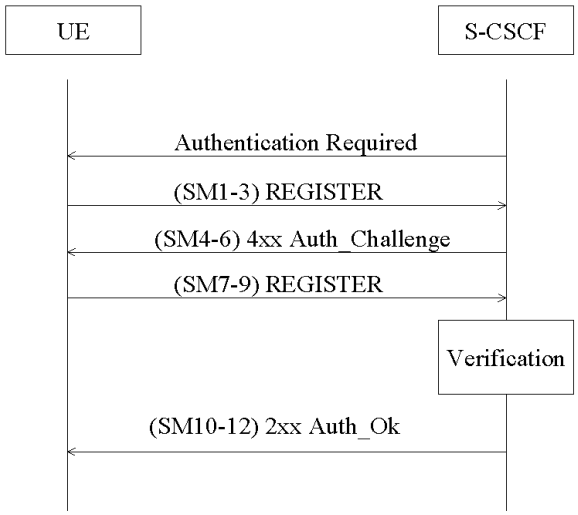


Figure 7

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 an SA created during this authentication procedure; or
- the P-CSCF receives a REGISTER not containing an authentication response and the message is protected with an 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

If the local policy in P-CSCF requires the use of IMS specific confidentiality protection mechanism between UE and P-CSCF, IPsec ESP as specified in RFC 2406 [13] shall provide confidentiality 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 RFC 2401 [14] shall also be considered. ESP confidentiality 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 an authenticated registration procedure, two pairs of unidirectional SAs between the UE and the P-CSCF all shared by TCP and UDP, shall be established in the P-CSCF and later in the UE. One SA pair is for traffic between a client port at the UE and a server port at the P-CSCF and the other SA is for traffic between a client port at the P-CSCF and a server port at the UE. For a detailed description of the establishment of these security associations see clause 7.

The encryption key CK_{ESP} is the same for the two pairs of simultaneously established SAs. The encryption key CK_{ESP} is obtained from the key CK_{IM} established as a result of the AKA procedure, specified in clause 6.1, using a suitable key expansion function.

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

6.3 Integrity mechanisms

IPsec ESP as specified in reference RFC 2406 [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 RFC 2401 [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 an authenticated registration procedure, two pairs of unidirectional SAs between the UE and the P-CSCF, all shared by TCP and UDP, shall be established in the P-CSCF and later in the UE. One SA pair is for traffic between a client port at the UE and a server port at the P-CSCF and the other SA is for traffic between a client port at the P-CSCF and a server port at the UE. For a detailed description of the establishment of these security associations see clause 7.

The integrity key IK_{ESP} is the same for the two pairs of 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.

6.5 CSCF interoperating with proxy located in a non-IMS network

SIP signalling protected by TLS specified in RFC 3261 [6] may be used for protecting the SIP interoperation between an IMS CSCF with a proxy/CSCF located in a foreign network. The CSCF may request the TLS connection with a foreign Proxy by publishing sips: URI in DNS server, that can be resolved via NAPTR/SRV mechanism specified in RFC 3263 [23]. When sending/receiving the certificate during the TLS handshaking phase, the CSCF shall verify the name on the certificate against the list of the interworking partners.

The TLS session could be inititiated from either network. A TLS connection is capable of carrying multiple SIP dialogs.

Applying this method is to prevent attacks on SIP level, but it does not prohibit other security methods to be applied so as to strengthen the security for IP based networks. This part is specified in Annex A of TS 33.210 [5].

NOTE 1: NOTE 1 in clause 5.1.4 on the use of TLS also applies here.

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 signalling 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 signalling 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 and confidentiality, in accordance with the provisions in clauses 5.1.3 and 6.2.

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

- **Encryption algorithm**

  The encryption algorithm is either DES-EDE3-CBC as specified in RFC 2451 [20] or AES-CBC as specified in RFC 3602 [22] with 128 bit key.

  Both encryption algorithms shall be supported by both, the UE and the P-CSCF.

- **Integrity algorithm**

NOTE: What is called "authentication algorithm" in RFC 2406 [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].

  Both integrity algorithms shall be supported by both, the UE and the P-CSCF as mandated by RFC 2406 [13]. In the unlikely event that one of the integrity algorithms is compromised during the lifetime of this specification, this algorithm shall no longer be supported.

NOTE: 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 UE shall select the SPIs uniquely, and different from any SPIs that might be used in any existing SAs (i.e. inbound and outbound SAs). The SPIs selected by the P-CSCF shall be different than the SPIs sent by the UE, cf. clause 7.2. In an authenticated registration, the UE and the P-CSCF each select

two SPIs, not yet associated with existing inbound SAs, for the new inbound security associations at the UE and the P-CSCF respectively.

NOTE: 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: 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.
- Key length: the length of the encryption key depends on the encryption algorithm. The entropy of the key shall at least be 128 bits.

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 protocols that share the SA, and source and destination ports.

- IP addresses are bound to two pairs 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: 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 selector shall allow UDP and TCP.
- Ports:

1. The P-CSCF associates two ports, called *port_ps* and *port_pc*, with each pair of security assocations established in an authenticated registration. The ports *port_ps* and *port_pc* are different from the standard SIP ports 5060 and 5061. No unprotected messages shall be sent from or received on the ports *port_ps* and *port_pc*. From a security point of view, unprotected messages may be received on any port which is different from the ports *port_ps* and *port_pc*. The number of the ports *port_ps* and *port_pc* are communicated to the UE during the security mode set-up procedure, cf. clause 7.2. These ports are used with both, UDP and TCP. The use of these ports may differ for TCP and UDP, as follows:

   UDP case: the P-CSCF receives requests and responses protected with ESP from any UE on the port *port_ps* (the"protected server port"). The P-CSCF sends requests and responses protected with ESP to a UE on the port *port_pc* (the "protected client port").

   TCP case: the P CSCF, if it does not have a TCP connection towards the UE yet, shall set up a TCP connection from its *port_pc* to the port *port_us* of the UE before sending a request to it..

NOTE: Both the UE and the P-CSCF may set up a TCP connection from their client port to the other end's server port on demand. An already existing TCP connection may be reused by both the P-CSCF or the UE; but it is not mandatory.

NOTE: The protected server port *port_ps* stays fixed for a UE until all IMPUs from this UE are de-registered. It may be fixed for a particular P-CSCF over all UEs, but there is no need to fix the same protected server port for different P-CSCFs.

NOTE: The distinction between the UDP and the TCP case reflects the different behaviour of SIP over UDP and TCP, as specified in section 18 of RFC 3261 [6].

2. The UE associates two ports, called *port_us* and *port_uc*, with each pair of security assocations established in an authenticated registration. The ports *port_us* and *port_uc* are different from the standard SIP ports 5060 and 5061. No unprotected messages shall be sent from or received on the ports *port_us* and *port_uc*. From a security point of view, unprotected messages may be received on any port which is different from the ports *port_us* and *port_uc*. The number of the ports *port_us* and *port_uc* are communicated to the P-CSCF during the security mode set-up procedure, cf. clause 7.2. These ports are used with both, UDP and TCP. The use of these ports may differ for TCP and UDP, as follows:

   UDP case: the UE receives requests and responses protected with ESP on the port *port_us* (the"protected server port"). The UE sends requests and responses protected with ESP on the port *port_uc* (the "protected client port").

   TCP case: the UE, if it does not have a TCP connection towards the P-CSCF yet, shall set up a TCP connection to the port *port_ps* of the P-CSCF before sending a request to it.

NOTE: Both the UE and the P-CSCF may set up a TCP connection from their client port to the other end's server port on demand. An already existing TCP connection may be reused by both the P-CSCF or the UE, but it is not mandatory.

NOTE: The protected server port *port_us* stays fixed for a UE until all IMPUs from this UE are de-registered.

NOTE: The distinction between the UDP and the TCP case reflects the different behaviour of SIP over UDP and TCP, as specified in section 18 of RFC 3261 [6]

3. The P-CSCF is allowed to receive only REGISTER messages and error messages on unprotected ports. All other messages not arriving on a protected port shall be either discarded or rejected by the P-CSCF.

4. 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 rejected or silently discarded by the UE.

The following rules apply:

1. For each unidirectional 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, P-CSCF_protected_port, SPI, IMPI, IMPU1, ... , IMPUn, lifetime) in an "SA_table". The pair (UE_protected_port, P-CSCF_protected_port) equals either (*port_uc*, *port_ps*) or (*port_us*, *port_pc*).

NOTE: 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 headers coincide with the UE"s IP address inserted in the Via header of the protected REGISTER message. If the Via 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 the pair (UE_IP_address, UE_protected_client_port), where the UE_IP_address is the source IP address in the packet header and the protected client 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 six SAs per direction 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: According to clause 7.4 on SA handling, at most six SAs per direction may 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, P-CSCF_protected_port) 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 unidirectional SA which has been established and has not expired, the SIP application at the UE stores at least the following data: (UE_protected_port, P-CSCF_protected_port, SPI, lifetime) in an "SA_table". The pair (UE_protected_port, P-CSCF_protected_port) equals either (*port_uc*, *port_ps*) or (*port_us*, *port_pc*).

NOTE: 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 a new pair of SAs (cf. clause 6.3) the SIP application at the UE shall ensure that the selected numbers for the protected ports do not correspond to an entry in the "SA_table".

NOTE: 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, P-CSCF_protected_port) in the "SA table".

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

7.2 Set-up of security associations (successful case)

The set-up of security associations is based on RFC 3329 [21]. Annex H of this specification shows how to use RFC 3329 [21] for the set-up of security associations.

In this clause 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.

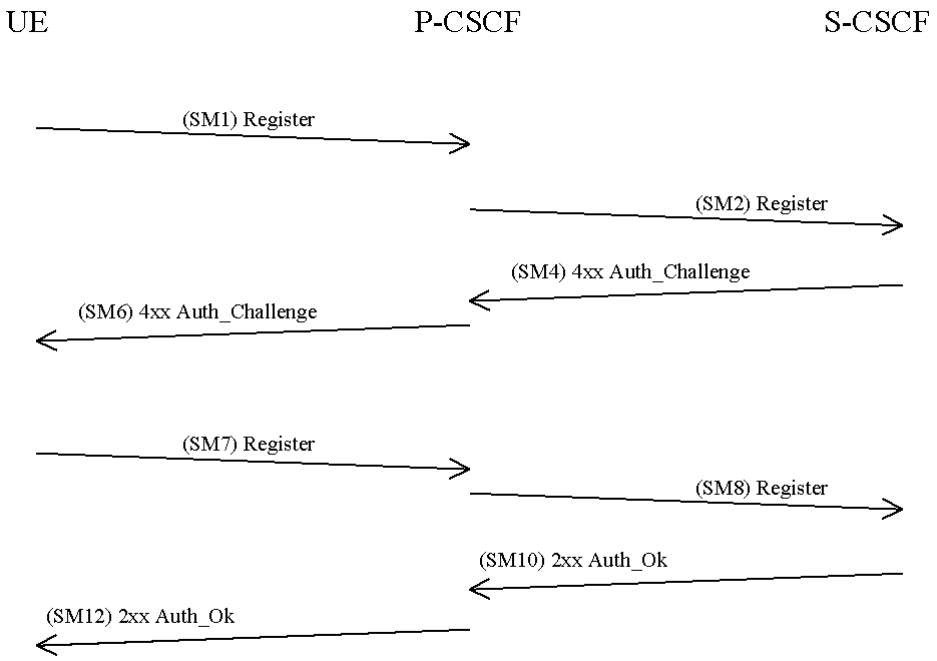


Figure 8

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 Security Parameter Index values and the protected ports selected by the UE. It also contains a list of identifiers for the integrity and encryption algorithms, which the UE supports.

SM1:
REGISTER(Security-setup = *SPI_U, Port_U, UE integrity and encryption algorithms list)*

SPI_U is the symbolic name of a pair of SPI values (cf. clause 7.1) (spi_uc, spi_us) that the UE selects. *spi_uc* is the SPI of the inbound SA at UE"s the protected client port, and *spi_us* is the SPI of the inbound SA at the UE"s protected server port. The syntax of spi_uc and spi_us are defined in Annex H.

Port_U is the symbolic name of a pair of port numbers (*port_uc, port_us*) as defined in clause 7.1. The syntax of port_uc and port_us is defined in Annex H.

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 keys IK_{IM} and CK_{IM} received from the S-CSCF to the temporarily stored parameters.

A Release 6 P-CSCF shall propose SA alternatives for Release 5 and Release 6 UE"s since the UE may or may not support confidentiality protection. The P-CSCF selects the SPI for the inbound SA. The P-CSCF then selects the SPIs for the inbound SAs. The same SPI number shall be used for Release 5 and Release 6 options. The P-CSCF shall define the SPIs such that they are unique and different from any SPIs as received in the *Security-setup-line* from the UE.

NOTE: This rule is needed since the UE and the P-CSCF use the same key for inbound and outbound traffic.

In order to determine the integrity and encryption algorithm the P-CSCF proceeds as follows: the P-CSCF has a list of integrity and encryption algorithms it supports, ordered by priority. Release 6 algorithms shall have higher priority than Release 5 algorithms.The P-CSCF selects the first algorithm combination on its own list which is also supported by the UE.

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

The *Security-setup*-line in SM6 contains the SPIs and the ports assigned by the P-CSCF. It also contains a list of identifiers for the integrity and encryption algorithms, which the P-CSCF supports.

NOTE: P-CSCF may be configured to trust on the encryption provided by the underlying access network. In this case, the P-CSCF acts according to Release 5 specificatons, and does not include encryption algorithms to the *Security-setup*-line in SM6.

SM6:
4xx Auth_Challenge(Security-setup = *SPI_P, Port_P*, *P-CSCF integrity and encryption algorithms list)*

SPI_P is the symbolic name of the pair of SPI values (cf. clause 7.1) (*spi_pc, spi_ps*) that the P-CSCF selects. *spi_pc* is the SPI of the inbound SA at the P-CSCF"s protected client port, and *spi_ps* is the SPI of the inbound SA at the P-CSCF"s protected server port. The syntax of spi*_pc* and *spi_ps* is defined in Annex H.

Port_P is the symbolic name of the port numbers (*port_pc*, *port_ps*) as defined in clause 7.1. The syntax of Port_P is defined in Annex H.

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

NOTE: Release 5 UE will not support any encryption algorithms, and will choose the first Release 5 integrity algorithm on the list received from the P-CSCF in SM6.

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

The UE shall integrity and confidentiality protect SM7 and all following SIP messages. Furthermore the integrity and encryption algorithms list, *SPI_P,* and *Port_P* received in SM6, and *SPI_U, Port_U sent in SM1* shall be included:

SM7:
REGISTER(Security-setup = *SPI_U, Port_U, SPI_P, Port_P*, *P-CSCF integrity and encryption algorithms list)*

After receiving SM7 from the UE, the P-CSCF shall check whether the integrity algorithms list, *SPI_P* and *Port_P* received in SM7 is identical with thecorresponding parameters sent in SM6. It further checks whether *SPI_U* and *Port_U* received in SM7 are identical with those received in SM1. If these checks are not successful 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 as indicated in clause 6.1.5. The P-CSCF shall add this information to all subsequent REGISTER messages received from the UE that have successfully passed the integrity and confidentiality check in the P-CSCF.

SM8:
REGISTER(Integrity-Protection = *Successful, Confidentiality-Protection = Seccessful,* 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.

An example of how to make use of two pairs of unidirectional SAs is illustrated in the figure below with a set of example message exchanges protected by the respective IPsec SAs where the INVITE and following messages are assumed to be carried over TCP.

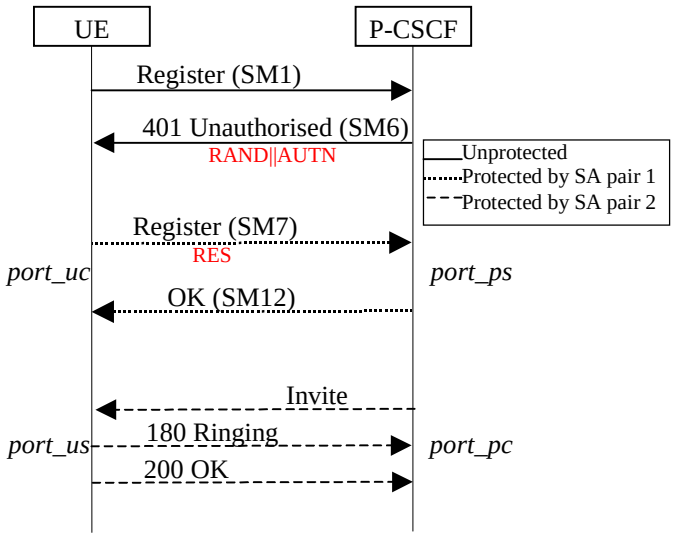


Figure 9

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 clause 6.1. However, this clause 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 shall 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 shall 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.

When the P-CSCF receives a challenge from the S-CSCF and creates the corresponding SAs during a registration procedure, it shall delete any information relating to any previous registration procedure (including the SAs created during the previous registration procedure).

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

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. The P-CSCF shall respond to SM1 indicating a failure, by sending an error response to the UE.

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 abandon 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 and encryption algorithms list received in SM7 is identical with the authentication and encryption 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

Every registration that includes a user authentication attempt produces new security associations. If the authentication is successful, then these new security associations shall replace the previous ones. This clause describes how the UE and P-CSCF handle this replacement and which SAs to apply to which message.

When security associations are changed in an authenticated re-registration then the protected server ports at the UE (*port_us*) and the P-CSCF (*port_ps*) shall remain unchanged, while the protected client ports at the UE (*port_uc*) and the P-CSCF (*port_pc*) shall change. For the definition of these ports see clause 7.1.

If the UE has an already active pair of security associations, then it shall use this to protect the REGISTER message. If the S-CSCF is notified by the P-CSCF that the REGISTER message from the UE was integrity-protected it may decide not to authenticate the user by means of the AKA protocol. However, the UE may send unprotected REGISTER messages at any time. In this case, the S-CSCF shall authenticate the user by means of the AKA protocol. In particular, if the UE considers the SAs no longer active at the P-CSCF, e.g., after receiving no response to several protected messages, then the UE should send an unprotected REGISTER message.

Security associations may be unidirectional or bi-directional. This clause assumes that security associations are unidirectional, as this is the general case. For IP layer SAs, the lifetime mentioned in the following clauses is the lifetime held at the application layer. Furthermore deleting an SA means deleting the SA from both the application and IPsec layer. The message numbers, e.g. SM1, used in the following clauses relate to the message flow given in clause 6.1.1.

7.4.1 Void

7.4.1a Management of security associations in the UE

The UE shall be involved in only one registration procedure at a time, i.e. the UE shall remove any data relating to any previous incomplete registrations or authentications, including any SAs created by an incomplete authentication.

The UE may start a registration procedure with two existing pairs of SAs. These will be referred to as the old SAs. The authentication produces two pairs of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication flow. In the same way, certain messages in the authentication shall be protected with a particular SA. If the UE receives a message protected with the incorrect SA, it shall discard the message.

A successful authentication proceeds in the following steps:

- The UE sends the SM1 message to register with the IMS. If SM1 was protected, it shall be protected with the old outbound SA.

- The UE receives an authentication challenge in a message (SM6) from the P-CSCF. This message shall be protected with the old inbound SA if SM1 was protected and unprotected otherwise.

- If this message SM6 can be successfully processed by the UE, the UE creates the new SAs, which are derived according to clause 7.1. The lifetime of the new SAs shall be set to allow enough time to complete the registration procedure. The UE then sends its response (SM7) to the P-CSCF, which shall be protected with the new outbound SA. Meanwhile, if SM1 was protected, the UE shall use the old SAs for messages other than those in the authentication, until a successful message of new authentication is received (SM12); if SM1 was unprotected, the UE is not allowed to use IMS service until it receives an authentication successful message (SM12).

- The UE receives an authentication successful message (SM12) from the P-CSCF. It shall be protected with the new inbound SA.

- After the successful processing of this message by the UE, the registration is complete. The UE sets the lifetime of the new SAs such that it either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the message, depending which gives the SAs the longer life. For further SIP messages sent from UE, the new outbound SAs are used, with the following exception: when a SIP message is part of a pending SIP transaction it may still be sent over the old SA. A SIP transaction is called pending if it was started using an old SA. When a further SIP message protected with a new inbound SA is successfully received from the P-CSCF, then the old SAs shall be deleted as soon as either all pending SIP transactions have been completed, or have timed out. The old SAs shall be always deleted when the lifetime is expired. This completes the SA handling procedure for the UE.

A failure in the authentication can occur for several reasons. If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SA. If SM1 was protected, the old SAs shall be used to protect the failure messages. In both cases, after processing the failure message, the UE shall delete the new SAs.

The UE shall monitor the expiry time of registrations without an authentication and if necessary increase the lifetime of the SAs created by the last successful authentication such that it will expire shortly after the registration timer in the message.

NOTE: In particular this means that the lifetime of a SA is never decreased.

The UE shall delete any SA whose lifetime is exceeded. The UE shall delete all SAs it holds once all the IMPUs are de-registered.

7.4.2 Void

7.4.2a Management of security associations in the P-CSCF

When the S-CSCF initiates an authentication by sending a challenge to the UE, the P-CSCF may already contain existing SAs from previously completed authentications. It may also contain two existing pairs of SAs from an incomplete authentication. These will be referred to as the old and registration SAs respectively. The authentication produces two pairs of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication flow. Similarly certain messages in the authentication shall be protected with a particular SA. If the P-CSCF receives a message protected with the incorrect SA, it shall discard the message.

The P-CSCF associates the IMPI given in the registration procedure and all the successfully registered IMPUs related to that IMPI to an SA.

A successful authentication proceeds in the following steps:

- The P-CSCF receives the SM1 message. If SM1 is protected, it shall be protected with the old inbound SA.

- The P-CSCF forwards the message containing the challenge (SM6) to the UE. This shall be protected with the old outbound SA, if SM1 was protected and unprotected otherwise.

- The P-CSCF then creates the new SAs, which are derived according to clause 7.1. The expiry time of the new SAs shall be set to allow enough time to complete the registration procedure. The registration SAs shall be deleted if they exist.

- The P-CSCF receives the message carrying the response (SM7) from the UE. It shall be protected using the new inbound SA. If SM1 was protected, the old SAs are used to protect messages other than those in the authentication.

- The P-CSCF forwards the successful registration message (SM12) to the UE. It shall be protected using the new outbound SA. This completes the registration procedure for the P-CSCF. The P-CSCF sets the expiry time of the new SAs such that they either equals the latest lifetime of the old SAs or it will expire shortly after the registration timer in the message, depending which gives the SAs the longer life.

- After SM12 is sent, the P-CSCF handles the UE related SAs according to following rules:

    - If there are old SAs, but SM1 belonging to the same registration procedure was received unprotected, the P-CSCF considers error cases happened, and assumes UE does not have those old SAs for use. In this case the P-CSCF shall remove the old SAs.

    - If SM1 belonging to the same registration procedure was protected with an old valid SA, the P-CSCF keeps this inbound SA and the corresponding three SAs created during the same registration with the UE active, and continues to use them. Any other old SAs are deleted. When the old SAs have only a short time left before expiring or a further SIP message protected with a new inbound SA is successfully received from the UE, the P-CSCF starts to use the new SAs for outbound messages with the following exception: when a SIP message is part of a pending SIP transaction it may still be sent over the old SA. A SIP transaction is called pending if it was started using an old SA. The old SAs are then deleted as soon as all pending SIP transactions have been completed, or have timed out. The old SAs are always deleted when the old SAs lifetime are expired. When the old SAs expire without a further SIP message protected by the new SAs, the new SAs are taken into use for outbound messages. This completes the SA handling procedure for the P-CSCF.

A failure in the authentication can occur for several reasons. If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SAs. If SM1 was protected, the old SAs shall be used to protect the failure messages. In both cases, after processing the failure message, the P-CSCF shall delete the new SAs.

The P-CSCF shall monitor the expiry time of registrations without an authentication and if necessary increase the lifetime of SAs created by the last successful authentication such that it will expire shortly after the registration timer in the message.

The P-CSCF shall delete any SA whose lifetime is exceeded. The P-CSCF shall delete all SAs it holds that are associated with a particular IMPI once all the associated IMPUs are de-registered.

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 delete the existing SA's and initiate an unprotected registration procedure using the new IP address as the source IP address in the packets carrying the REGISTER messages.

8 ISIM

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 USIM application on a UICC.

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

If there is an ISIM and a USIM application on a UICC, then the ISIM application shall always be used for IMS authentication.

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 clause 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 signalling 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 TS 33.102 [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 "Security Mechanism Agreement for SIP Sessions" [21] for security mode set-up

The BNF syntax of RFC 3329 [21] is defined for negotiating security associations for semi-manually keyed IPsec in the following way:

security-client	= "Security-Client" HCOLON sec-mechanism *(COMMA sec-mechanism)
security-server	= "Security-Server" HCOLON sec-mechanism *(COMMA sec-mechanism)
security-verify	= "Security-Verify" HCOLON sec-mechanism *(COMMA sec-mechanism)
sec-mechanism	= mechanism-name *(SEMI mech-parameters)
mechanism-name	= "ipsec- 3gpp"
mech-parameters	= (preference / algorithm / protocol / mode / encrypt-algorithm / spi-c / spi-s / port-c / port-s)
preference	= "q" EQUAL qvalue
qvalue	= ("0" ["." 0*3DIGIT]) / ("1" ["." 0*3("0")])
algorithm	= "alg" EQUAL ("hmac-md5-96" / "hmac-sha-1-96")
protocol	= "prot" EQUAL ("ah" / "esp")
mode	= "mod" EQUAL ("trans" / "tun")
encrypt-algorithm	= "ealg" EQUAL ("des-ede3-cbc" /"aes-cbc" / "null")
spi-c	= "spi-c" EQUAL spivalue
spi-s	= "spi-s" EQUAL spivalue
spivalue	= 10DIGIT; 0 to 4294967295
port-c	= "port-c" EQUAL port
port-s	= "port-s" EQUAL port
port	= 1*DIGIT

The parameters described by the BNF above have the following semantics:

Mechanism-name: For manually keyed IPsec, this field includes the value "ipsec- 3gpp". "ipsec- 3gpp" mechanism extends the general negotiation procedure of RFC 3329 [21] in the following way:

1 The server shall store the Security-Client header received in the request before sending the response with the Security-Server header.

2 The client shall include the Security-Client header in the first protected request. In other words, the first protected request shall include both Security-Verify and Security-Client header fields.

3 The server shall check that the content of Security-Client headers received in previous steps (1 and 2) are the same.

Preference: As defined in RFC 3329 [21].

Algorithm: Defines the authentication algorithm. May have a value "hmac-md5-96" for algorithm defined in RFC 2403 [15], or "hmac-sha-1-96" for algorithm defined in RFC 2404 [16]. The algorithm parameter is mandatory.

Protocol: Defines the IPsec protocol. May have a value "ah" for RFC 2402 [19] and "esp" for RFC 2406 [13]. If no Protocol parameter is present, the value will be "esp".

NOTE: According to clause 6 only "esp" is allowed for use in IMS.

Mode: Defines the mode in which the IPsec protocol is used. May have a value "trans" for transport mode, and value "tun" for tunneling mode. If no Mode parameter is present, the value will be "trans".

NOTE: According to clause 6.3 ESP integrity shall be applied in transport mode i.e. only "trans" is allowed for use in IMS.

Encrypt-algorithm: If present, defines the encryption algorithm. May have a value "des-ede3-cbc" for algorithm defined in RFC 2451 [20] or "aes-cbc" for the algorithm defined in IETF RFC 3602 [22] or "null" if encryption is not used. If no Encrypt-algorithm parameter is present, the algorithm will be "null".

Spi-c: Defines the SPI number of the inbound SA at the protected client port.

Spi-s: Defines the SPI number of the inbound SA at the protected server port.

Port-c: Defines the protected client port.

Port-s: Defines the protected server port.

It is assumed that the underlying IPsec implementation supports selectors that allow all transport protocols supported by SIP to be protected with a single SA.

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

Integrity Keys:

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 32 zero bits to the end of IK_{IM} to create a 160-bit string.

Encryption Keys:

Divide CK_{IM} into two blocks of 64 bits each:

$$CK_{IM} = CK_{IM1} || CK_{IM2}$$

Where CK_IM1 are the 64 most significant bits and CK_IM2 are the 64 least significant bits.

The key for DES-EDE3-CBC is then defined to be:

$$CK_{ESP} = CK_{IM1} || CK_{IM2} || CK_{IM1},$$

after adjusting parity bits to comply with RFC 2451 [20].

If selected encryption algorithm is AES-CBC as specified in RFC 3602 [22] with 128 bit key then $CK_{ESP} = CK_{IM}$

Annex J (informative): Recommendations to protect the IMS from UEs bypassing the P-CSCF

After the UE does a successful SIP REGISTER with the P-CSCF, malicious UE could try to send SIP messages directly to the S-CSCF. This could imply that the UE would be able to bypass the integrity protection provided by IPSec ESP between the UE and the P-CSCF.

NOTE: The TS 24.229 [8] defines a trust domain that consists of the P-CSCF, the I-CSCF, the S-CSCF, the BGCF, the MGCF, the MRFC and all the AS:s that are not provided by 3rd party service providers. There are nodes in the edge of the trust domain that are allowed to provide with an asserted identity header. The nodes in the trust domain will trust SIP messages with asserted identity headers. The asserted identity information is useful as long as the interfaces in an operator"s network can be trusted.

If a UE manages to bypass the P-CSCF it presents at least the following problems:

1) The P-CSCF is not able to generate any charging information.

2) Malicious UE could masquerade as some other user (e.g. it could potentially send INVITE or BYE messages).

The following recommendations for preventing attacks based on such misbehavior are given:

- Access to S-CSCF entities shall be restricted to the core network entities that are required for IMS operation, only. It shall be ensured that no UE is able to directly send IP packets to IMS-entities other than the required ones, ie. assigned P-CSCF, or HTTP servers.

- Impersonation of IMS core network entities at IP level (IP spoofing), especially impersonation of P-CSCFs by UEs shall be prevented.

- It is desirable to have a general protection mechanism against UEs spoofing (source) IP addresses in any access network providing access to IMS services.

If the traffic is between two non-IMS CSCFs, it is recommended to use TLS mechanisms as specified in RFC 3261 [6]. This will mitigate the problems caused by misbehaviour of the UE. If neither intra-CSCF traffic nor CSCF-SEG traffic can be trusted and if this traffic is not protected by the NDS/IP, TS 33.210 [5] mechanisms, then physical protection measures or IP traffic filtering should be applied. This is anyhow not in the scope of 3GPP specification.

Annex K (informative): Security aspects of early IMS

An interim security solution for early IMS implementations, that are not fully compliant with the IMS security architecture specified in the present document, is given in TR 33.978 [25].

Annex L (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
2002-09	SP-17	SP-020583	012		F	SA handling when the UE changes IP address	5.2.0	5.3.0
2002-09	SP-17	SP-020583	013		F	Removal of some editor notes in TS 33.203	5.2.0	5.3.0
2002-09	SP-17	SP-020583	014		F	Correction to S-CSCF behaviour on Network Authentication Failure	5.2.0	5.3.0
2002-09	SP-17	SP-020583	015		F	Correcting the network behaviour in response to an incorrect AUT-S	5.2.0	5.3.0
2002-09	SP-17	SP-020583	016		F	Mitigating reflection attacks in IMS	5.2.0	5.3.0
2002-09	SP-17	SP-020583	017		F	Protect port number to be assigned by UE in re-registration	5.2.0	5.3.0
2002-09	SP-17	SP-020583	018		F	One SA for both TCP and UDP sockets	5.2.0	5.3.0
2002-09	SP-17	SP-020583	019		F	Correction of authentication vector distribution procedure	5.2.0	5.3.0
2002-09	SP-17	SP-020583	020		F	The definition of the key to be used for HMAC-SHA1-96 within ESP	5.2.0	5.3.0
2002-09	SP-17	SP-020583	021		F	Draft-ietf-sip-sec-agree syntax for manually keyed IPsec	5.2.0	5.3.0
2002-09	SP-17	SP-020583	022		F	Update of User Authentication Failure	5.2.0	5.3.0
2002-09	SP-17	SP-020583	023		F	Update of SA handling procedures	5.2.0	5.3.0
2002-12	SP-18	SP-020710	024		F	Correction of IP address acquisition in P-CSCF	5.3.0	5.4.0
2002-12	SP-18	SP-020711	025		F	Sending error response when P-CSCF receives unacceptable proposal	5.3.0	5.4.0
2002-12	SP-18	SP-020712	026		F	The use of SAs in user authentication failures	5.3.0	5.4.0
2002-12	SP-18	SP-020713	027		F	Clean up one Editor"s note in 33.203	5.3.0	5.4.0
2002-12	SP-18	SP-020714	028		F	Re-use and re-transmission of RAND and AUTN	5.3.0	5.4.0
2002-12	SP-18	SP-020715	029		F	Update of SIP Security Agreement Syntax in Appendix H	5.3.0	5.4.0
2002-12	SP-18	SP-020716	030		F	Registration and SA lifetimes	5.3.0	5.4.0
2002-12	SP-18	SP-020717	031		F	Open issues in SA handling	5.3.0	5.4.0
2002-12	SP-18	SP-020760	033		F	TCP and UDP share the same SA	5.3.0	5.4.0
2002-12	SP-18	SP-020761	034		F	Indication in the UE that the SA is no longer active in P-CSCF	5.3.0	5.4.0
2003-03	SP-19	SP-030100	035		F	Clarification of the use of ISIM and USIM for IMS access	5.4.0	5.5.0
2003-03	SP-19	SP-030101	036		F	Malicious UE bypassing the P-CSCF	5.4.0	5.5.0
2003-03	SP-19	SP-030102	037		F	Ensuring the deletion of unwanted SAs	5.4.0	5.5.0
2003-03	SP-19	SP-030103	038		F	Add protected port into Via header	5.4.0	5.5.0
2003-03	SP-19	SP-030111	039		F	Correction of the Port 2 definition for SA establishment	5.4.0	5.5.0

2003-06	SP-20	SP-030222	040		F	Annex H: Alignment of Authentication algorithm handling with RFC3329	5.5.0	5.6.0
2003-06	SP-20	SP-030223	041		F	Clarification on USIM-based access to IMS	5.5.0	5.6.0
2003-09	SP-21	SP-030484	043		F	Modification of the security association lifetime management	5.6.0	5.7.0
2003-09	SP-21	SP-030485	044		F	Annex H in 33.203	5.6.0	5.7.0
2003-09	SP-21	SP-030486	045		F	Security association handling, behaviour of SIP over TCP and re-authentication	5.6.0	5.7.0
2003-09	SP-21	SP-030483	042		B	Introducing Cipher key Expansion for IMS	5.6.0	6.0.0
2003-09	SP-21	SP-030487	046		B	Introducing Confidentiality Protection for IMS	5.6.0	6.0.0
2003-12	SP-22	SP-030596	048	1	A	Correcting the text on sending an authentication response	6.0.0	6.1.0
2003-12	SP-22	SP-030597	050	-	A	SA procedures	6.0.0	6.1.0
2003-12	SP-22	SP-030598	052	-	A	SA parameters and management	6.0.0	6.1.0
2003-12	SP-22	SP-030599	054	-	A	Reject or discard of messages	6.0.0	6.1.0
2003-12	SP-22	SP-030600	056	-	A	Correcting the SA handling procedures	6.0.0	6.1.0
2003-12	SP-22	SP-030601	057	-	F	Terminology alignment	6.0.0	6.1.0
2003-12	SP-22	SP-030603	059	-	D	Removing anti-replay requirement from Confidentiality clause	6.0.0	6.1.0
2003-12	SP-22	SP-030604	061	-	A	Ensuring the correct RAND is used in synchronization failures	6.0.0	6.1.0
2003-12	SP-22	SP-030605	063	-	A	Network behaviour when a new REGISTER is challenged during an on going authentication	6.0.0	6.1.0
2004-03	SP-23	SP-040153	064	-	B	Addition of AES transform	6.1.0	6.2.0
2004-03	SP-23	SP-040154	065	-	B	Deploying TLS (sips:) for interoperation between IMS and non-IMS network	6.1.0	6.2.0
2004-06	SP-24	SP-040372	066	-	F	Correction on IMS confidentiality protection	6.2.0	6.3.0
2004-06	SP-24	SP-040373	067	-	F	SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network	6.2.0	6.3.0
2004-09	SP-25	SP-040618	069	-	A	Deletion of old authentication vectors in S-CSCF after re-synchronization	6.3.0	6.4.0
2004-09	SP-25	SP-040618	071	-	F	SIP Privacy mechanism when IMS interworking with non-IMS (foreign) network	6.3.0	6.4.0
2004-09	SP-25	SP-040618	072	-	F	IMS Service Profile is independent from Implicit Registration Set	6.3.0	6.4.0
2004-12	SP-26	SP-040854	075	1	D	Editorial corrections	6.4.0	6.5.0
2005-03	SP-27	SP-050137	077	3	F	Addition of reference to early IMS security TR	6.5.0	6.6.0

History

Document history		
V6.5.0	December 2004	Publication
V6.6.0	March 2005	Publication