PacketCable™
IMS Delta Specifications

3G security; Access security for IP-based services Specification
3GPP TS 33.203

PKT-SP-33.203-C01-140314

CLOSED

Notice

DISCLAIMER

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any affiliated company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	PKT-SP-33.203-C01-140314			
Document Title:	3G security; Access security for IP-based services Specification			
Revision History:	I01 - Released 04/06/06 I02 - Released 10/13/06 I03 - Released 09/25/07 I04 - Released 04/25/08 I05 - Released 05/28/09 C01 - Released 03/14/14			
Date:	March 14, 2014			
Status:	~~Work in Progress~~	~~Draft~~	~~Issued~~	**Closed**
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	**Public**

Key to Document Status Codes:

Work in Progress	An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks

Abstract

This CableLabs-modified 3GPP technical specification includes the cable-specific requirements necessary for implementing 3GPP technical specifications in PacketCable™ and the delivery of PacketCable services.

Because these are modified 3GPP documents, their document formatting has been retained except as follows. Changes to the original 3GPP requirements are shown in this document by color coding of text. Unchanged text appears normal, while new text appears in blue underline and deleted 3GPP text appears as ~~violet strikethrough hidden text~~. To view the deleted 3GPP text, the reader must have Word configured so the 'view hidden text' is turned on.

The intended audience for this document includes developers of equipment intended to be conformant to PacketCable specifications.

NOTE: Special permission has been granted by 3GPP Organizational Partners to reproduce their technical specification, 3GPP 33.203, in this document.

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP) and further modified by CableLabs.
The present document provides a mechanism giving reliable transfer of signalling messages within the 3GPP system.

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 updated and re-released by CableLabs. ~~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.

Since the scope also encompasses the use of these security features and mechanisms for secure access to IMS in the context of fixed broadband networks, Annex L specifies how the material in the main body and other normative Annexes of this document apply to the fixed broadband networks.

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.
- PacketCable defines several specifications which are based on 3GPP technical specifications. These PacketCable specifications are commonly referred to as PacketCable Delta specifications. For references within this specification which have a corresponding PacketCable Delta specification, the PacketCable Delta specification must be used. The list of PacketCable Delta specifications is:

  PKT-SP-23.008 PKT-SP-29.229
  PKT-SP-24.229 PKT-SP-33.203
  PKT-SP-29.228

  References which have corresponding delta specifications are highlighted with an * below.

[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 (2003): "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".

[26] ETSI ES 282 001: "TISPAN - Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture for NGN Release 1".

[27] IETF RFC 3947 (2005): "Negotiation of NAT-Traversal in the IKE".

[28] IETF RFC 3948 (2005): "UDP Encapsulation of IPsec ESP Packets".

[29] IETF RFC 3323 (2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[30] IETF RFC 3325 (2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network".

[31] 3GPP TS 23.167: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions"".

[32] draft-ietf-sip-outbound-16 (October 2008): "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[33] IETF RFC 3268 (2002): "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)".

[34] IETF RFC 2246 (1999): "The TLS Protocol Version 1.0".

[35] IETF RFC 3280 (2002) "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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.

Authentication vector: A quintet (as defined in TS 33.102 [1]) or an SD-AV.

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.

SIP Digest authentication vector (SD-AV): Temporary authentication data that enables the IMS network to engage in SIP Digest with a particular user. An SD-AV consists of five elements: a) protection space user hint realm, b) protection space domain, c) the authentication algorithm, d) the quality of protection value qop and e) the hash of IMPI, realm and password H(A1).

Editor's Note: The inclusion of the domain parameter in the SD-AV is ffs.

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
AV	Authentication Vector
CSCF	Call Session Control Function
HSS	Home Subscriber Server
IBCF	Interconnection Border Control Function
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
NAPT	Network Address and Port Translation
NAT	Network Address Translation

SA	Security Association
SEG	Security Gateway
SD-AV	SIP Digest Authentication Vector
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TLS	Transport Layer Security
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 UE 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.

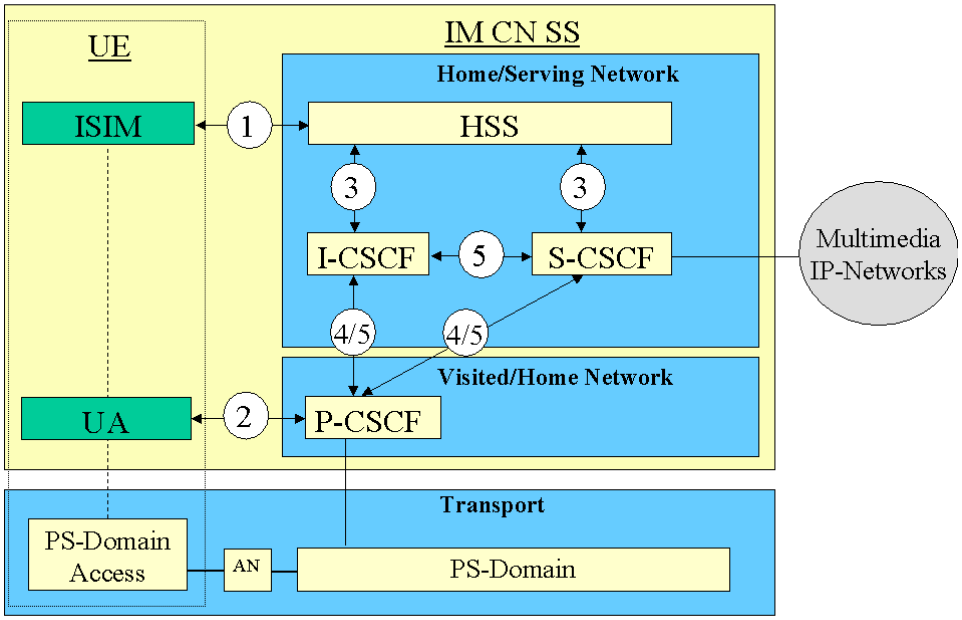

Figure 1: The IMS security architecture

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

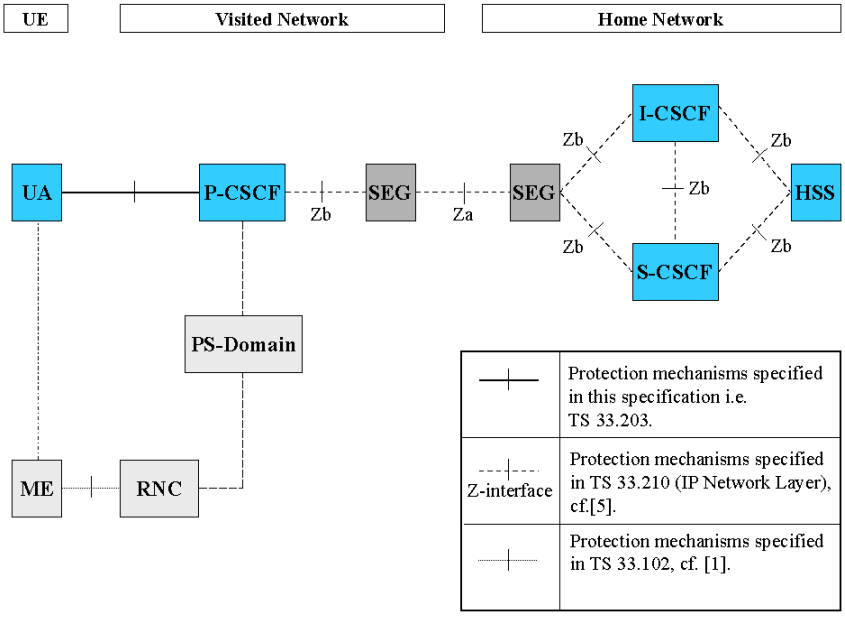

Figure 2: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the VN

P-CSCF in the Home Network

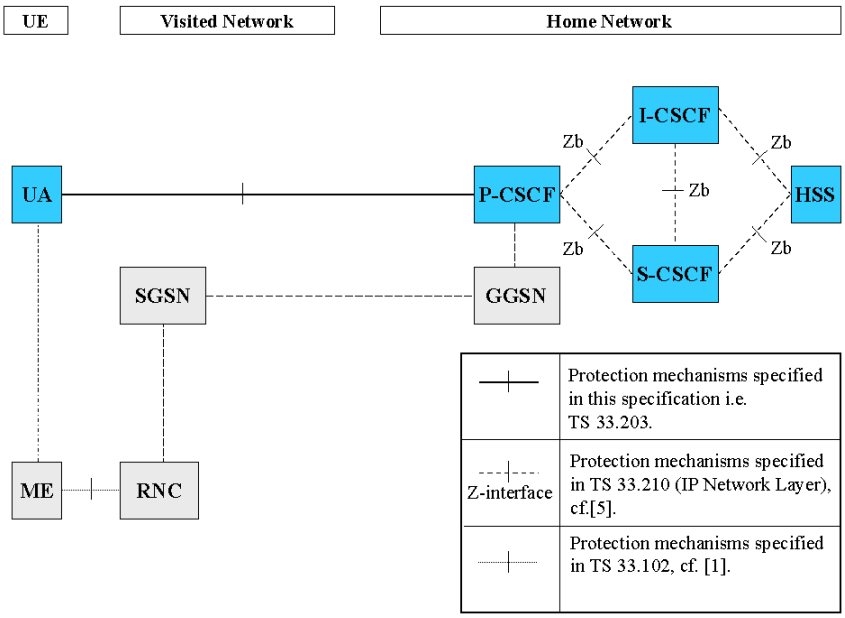

Figure 3: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the HN

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 UE 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. 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 ensure backward compatibility between CSCFs that do not support TLS and those CSCFs and other networks that do support it. These management and capability issues need then to be solved by manual configuration of the involved operators. If TLS is to be applied then the authentication framework in TS 33.310 [24] can be used.

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/IBCF shall have the capability to encrypt the addresses of all the entities of the operator network in SIP Via, Record-Route, Route and Path headers and then decrypt the addresses 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/IBCF s in the HN may encrypt and decrypt the addresses of all the entities of the operator network.

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 3323 [29] and IETF RFC 3325 [30].

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.

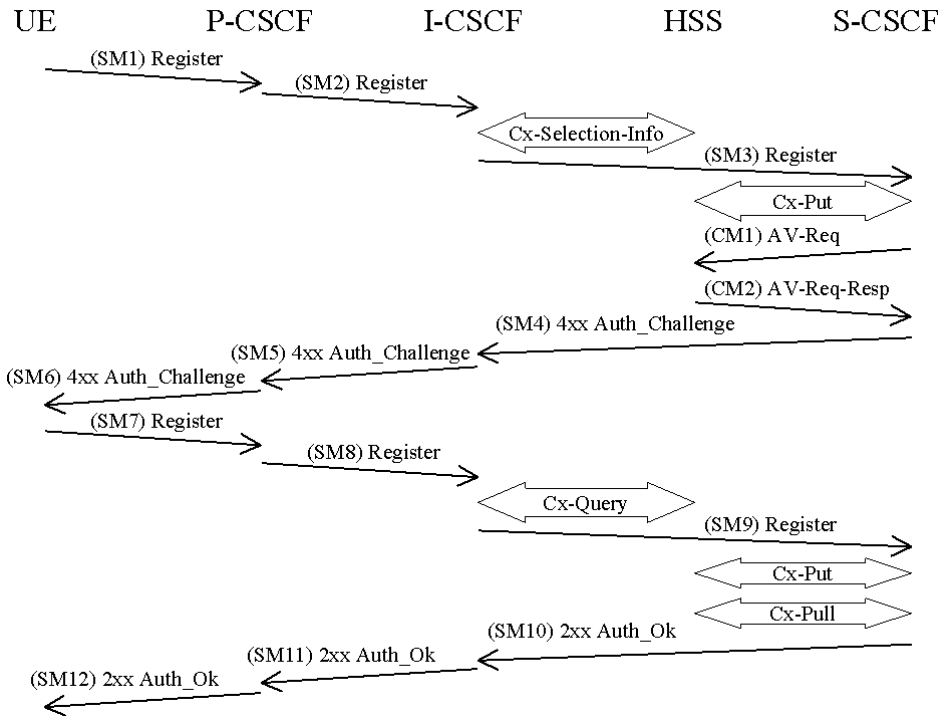

Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

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 UE 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.

If the user has been successfully authenticated, the S-CSCF sends a SM10 SIP 2xx Auth_OK message to the I-CSCF indicating that the registration was successful. In SM11 and SM12 the I-CSCF and the P-CSCF respectively forward the SIP 2xx Auth_OK towards the UE.

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, when registered, shall not be de-registered if it fails an authentication.

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.

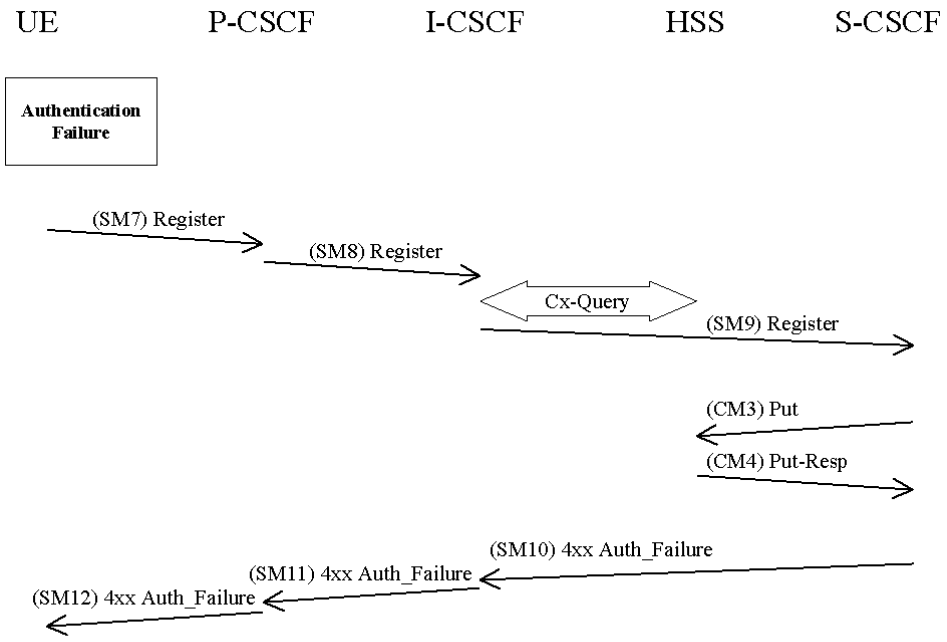

Figure 5

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 clear the S-CSCF name in the HSS, if the IMPU is currently *Not registered*. To clear the S-CSCF name the S-CSCF sends in CM3 a Cx-Put to the HSS. 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. The update to the HSS is performed in the same way as if receiving an SM9 indicating authentication failure (see message CM3 in clause 6.1.2.2).

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.

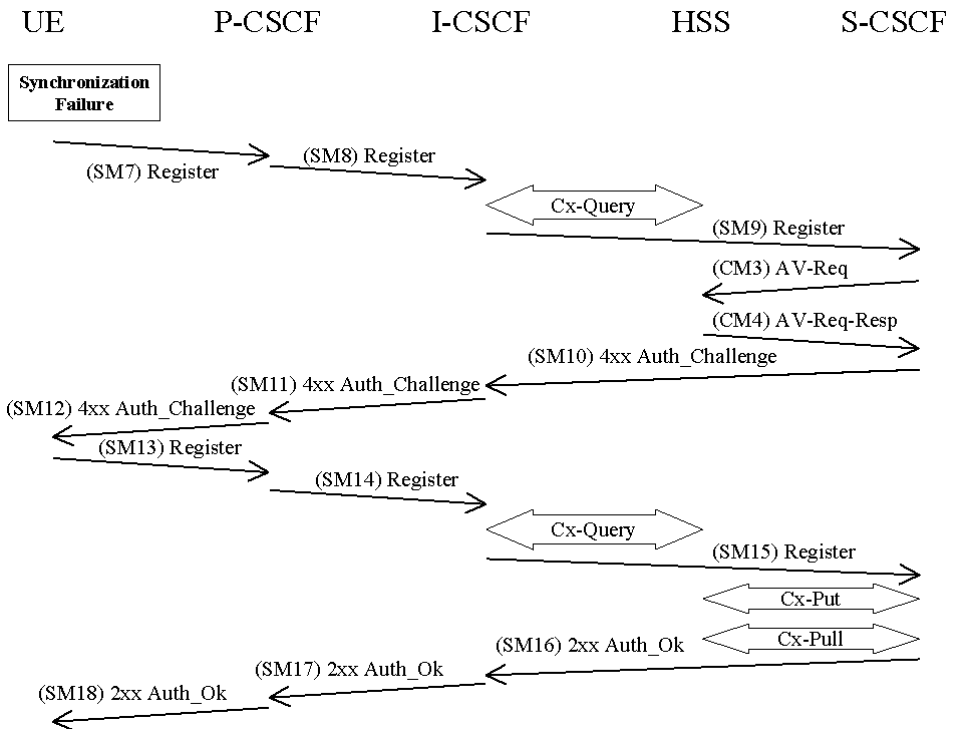

Figure 6

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.

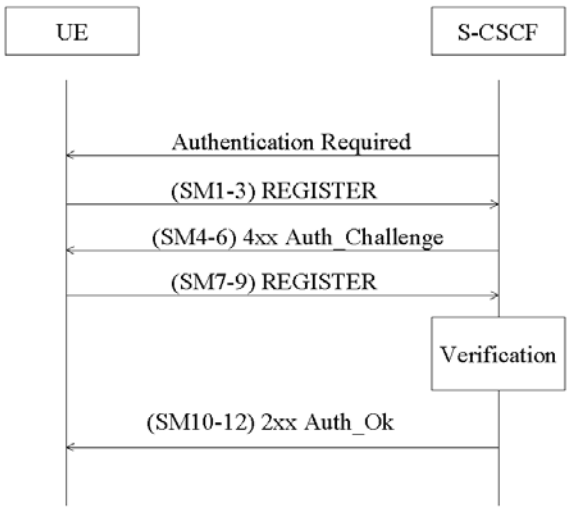

Figure 7

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/IBCFs 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/IBCF shall encrypt the hiding information elements when the I-CSCF/IBCF 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/IBCF receives a SIP Request or Response message from outside the hiding network's domain, the I-CSCF/IBCF shall decrypt those information elements that were encrypted by I-CSCF/IBCF 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~~ initiated 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~~ associations 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~~ associations 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, messages relating to emergency services in accordance with [31] and [8], and error messages related to unprotected 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;
   - messages relating to emergency services in accordance with [31] and [8];
   - error messages related to unprotected 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 or a re-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 ensure that the user associated with the SA, which was used to protect the incoming message from the UE, is identical to the user who is associated at SIP level with the message sent by the P-CSCF towards the network.

NOTE: Not all SIP messages necessarily contain public or private identities, e.g. subsequent messages in a dialogue. Other information, e.g. a dialogue identifier, may be used to associate the message with a user at SIP level.

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.

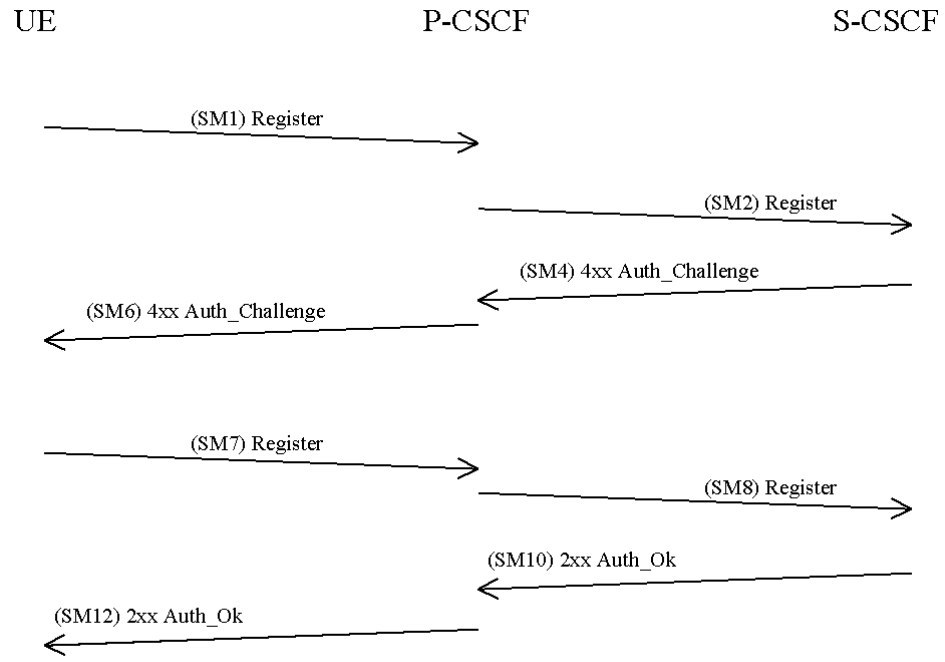

Figure 8

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.

The P-CSCF then selects the SPIs for the inbound SAs. 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. The P-CSCF selects the first algorithm combination on its own list which is also supported by the UE. If the UE did not include any confidentiality algorithm in SM1 then the P-CSCF shall either select the NULL encryption algorithm or abort the procedure, according to its policy on confidentiality.

NOTE: It should be noted that, if the P-CSCF policy requires confidentiality, then all UEs with no encryption support would be denied access to the IMS network. This would apply in particular to UEs, which support only a Release 5-version of this specification or only Early IMS according to [25].

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. The only exception from this is the case that the P-CSCF is configured to never apply confidentiality. In this case, it shall not include encryption algorithms to the *Security-setup*-line in SM6.

NOTE: The P-CSCF may be configured to never apply confidentiality, e.g. because it trusts the encryption provided by the underlying access network. If the P-CSCF is configured to apply confidentiality whenever the UE supports it then the P-CSCF always includes the encryption algorithms in SM6, which it supports, even if the UE did not include encryption algorithms in SM1. This is to thwart bidding down attacks.

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. If the P-CSCF did not include any confidentiality algorithm in SM6 then the UE shall select the NULL encryption algorithm.

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 and encryption algorithms list, *SPI_P* and *Port_P* received in SM7 is identical with the corresponding 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 check in the P-CSCF.

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

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

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.

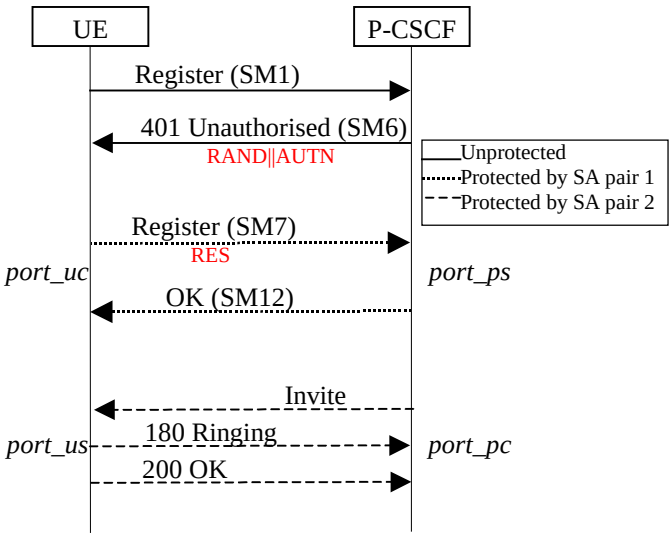

Figure 9

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], with the addition of the "aes-cbc" value for the "ealg" parameter and the "UDP-enc-tun" value for the "mode" parameter, is defined for negotiating security associations for semi-manually keyed IPsec or TLS 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" / "tls"
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"/ "UDP-enc-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.

Mech-parameters: Of the mech-parameters, only preference is relevant when the mechanism-name has the value "tls".

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 1: 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 2: 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~~misbehaviour 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.~~ i,e., 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. TLS certificate management as outlined in TS 33.310 [24] can be used ~~beween~~between two non-IMS CSCFs. 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 (Normative):
Application to fixed broadband access

L.1 Introduction

This Annex specifies how the material in the main body and other normative Annexes of this document apply to the TISPAN NGN [26].

NOTE 1: NGN specific abbreviations and terminology can be found in [26].

NOTE 2 : In the context of this Annex the term NGN-UE denotes the UE as defined in [26].

L.2 Application of clause 4

In 3GPP IMS, the ISIM is mandated to be present on UICC which is usually inserted within the MT component of the UE. In NGN-UEs, the ISIM shall be provided on the UICC, which shall be inserted within either:

1) The TE; or

2) The IMS Residential Gateway (IRG).

NOTE: For the exact definition of IRG will be published in ETSI TS 187 003: "TISPAN – NGN security: Security Architecture NGN Release 1".

Where the TE and IRG each contain an UICC with ISIM application, the ISIM should be used in following order of preference TE, IRG.

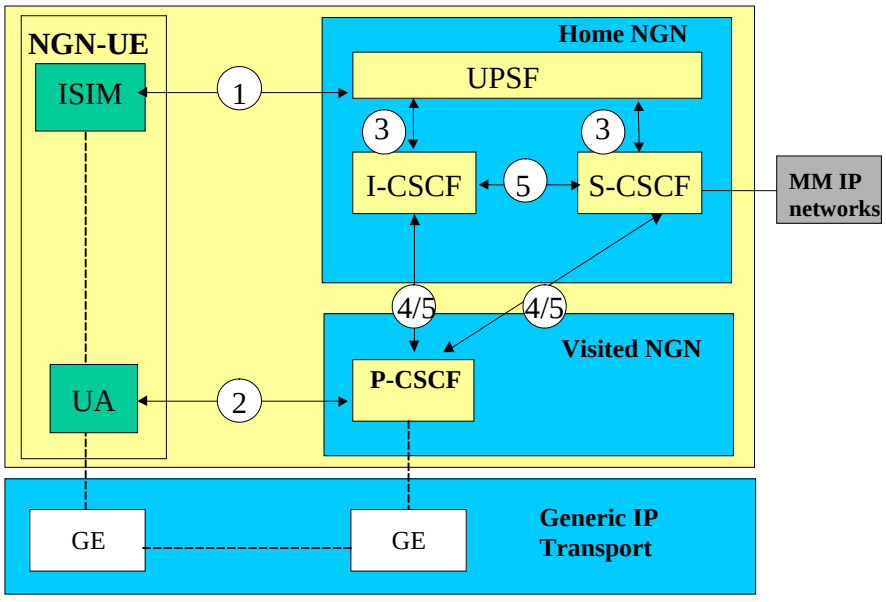

Figure L.1

Figure L.1 redraws figure 1 of the main body of this document replacing the 3GPP specific transport domain by Generic IP transport domain. The following observations support figure L.1.

1) The IMS is independent of the transport network.

2) Generic Entities (GE) equivalent to the 3GPP transport entities will be present in the Generic IP transport domain.

3) In the NGN architecture the AuC functionality is performed by the UPSF.

4) The Security Associations (SA) (referring to the corresponding arrows in Figure X.1) are retained:

   a) SA-1, SA-3, SA-4 and SA-5 are endorsed by this annex.

   b) SA-2 is endorsed by this Annex with the extension to ensure transport across NAT/Firewall boundaries.

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 (See figure X.2). The protection of all such interfaces and reference points (which may include other subsystems) apart from the Gm reference point are protected as specified in TS 33.210 [5].

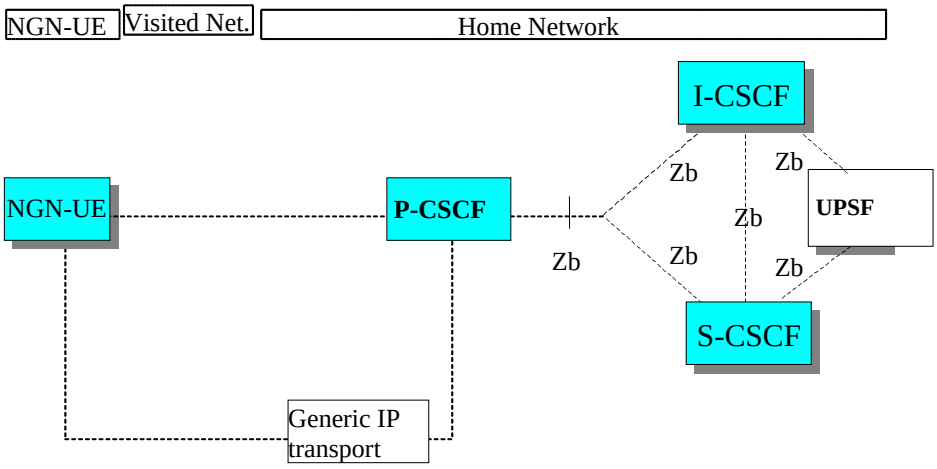

Figure L.2

Annex M (normative): Enhancements to the access security for IP based services to enable NAT traversal for signaling messages

Note: section M.x (x= 1, 2, …) in this annex corresponds to section x in the body of this specification.

M.1 Scope

It is assumed for the purposes of this annex that a NAT device may be located between the UE and the P-CSCF. Only NATs outside the borders of an IMS network are considered, i.e. NATs are assumed to be located at the subscriber's site or in the access network. If there are multiple NATs in either of these locations, it is assumed that their effect sums up in such a way that they can be treated as a single NAT so that the mechanisms described below are still valid.

In this annex enhancements to sections 4 through 8 of this specification are specified that allow a UE and a P-CSCF to detect whether they are located behind a NAT device, to inform each other about their NAT traversal capabilities, and, if there is a NAT present, to securely communicate. If there is no NAT device present, the procedures of sections 6, 7 and 8 apply. Examples of subscribers who are, in general, located behind a NAT device include subscribers accessing IMS via a DSL line.

Furthermore, this specification is restricted to the treatment of NAT traversal for signalling messages. Measures required for NAT traversal of media data are not considered in this specification. The general handling of NAT traversal for signalling messages is specified in TS 23.228 [3] and TS 24.229 [8]. Additional procedures for NAT traversal for protected signalling messages are specified in this specification.

It should be noted that many NAT routers in residential sites do also apply port translation, which is typically denoted as Network Address and Port Translation (NAPT). For reasons of simplicity the term NAT is used, no matter whether only address or address and port translation is actually applied.

NOTE: this annex is fully compliant with RFC 3948 [28], but only partially compliant with RFC 3947 [27] because 3GPP IMS security, as specified in this specification (main body and annexes), does not use IKE as the key management protocol for IPsec.

M.2 References

Additional references used in this section were incorporated directly into section 2.

M.3 Definitions, symbols and abbreviations

Additional definitions, symbols and abbreviations used in this section were incorporated directly into section 3.

M.4 Overview of the security architecture

The text in section 4 applies without changes.

M.5 Security features

The text in section 5 applies without changes.

M.6 Security mechanisms

M.6.1 Authentication and key agreement

The text in section 6.1 applies without changes.

M.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 either in transport mode if no NAT is present, or – if NAT traversal shall be supported – in UDP encapsulated tunnel mode.

The method to set up ESP security associations (SAs) during the SIP registration procedure is specified in clause M.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 M.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 M.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.

M.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 either in transport mode if no NAT is present or – if NAT traversal shall be supported – in UDP encapsulated tunnel mode.

The method to set up ESP security associations (SAs) during the SIP registration procedure is specified in clause M.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 M.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 M.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.

M.6.4 Hiding mechanisms

The text in section 6.4 applies without changes.

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

The text in section 6.5 applies without changes.

M.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 M.6.1. Subsequent signalling communications in this session will be integrity protected based on the keys derived during the authentication process.

M.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 M.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 M.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.

- **Mode**

  The IPSec SA mode of operation shall depend on whether the UE is located behind a NAT device or not. If the UE is located behind a NAT device UDP encapsulated tunnel mode according to [28] shall be used. Otherwise transport mode shall be used. The set-up of security associations (cf. clause M.7.2) allows the P-CSCF to detect whether the UE is located behind a NAT or not.

- **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 M.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 if no NAT is present:

Cf. section 7.1.

Selectors if a NAT is present:

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. If a NAT is present, it is assumed that the UE is configured locally with a (e.g. private) IP address. When the UE communicates with the P-CSCF via the NAT device, the NAT allocates a binding, mapping the local IP address to two pairs of SAs, as a publicly routable IP address (called public IP address in the sequel) and perhaps also mapping the source port used in clause 6.3, as follows: the UDP or TCP packet to another port number. In the following, the term UE_IP_address always denotes the public IP address of the UE.

NOTE: The IP addresses and ports used as selectors in IPsec tunnel mode are those of the inner IP header, in accordance with RFC2401 [14]. The inner IP addresses are always the public IP addresses. Please also note that the terminology used here may differ from that used in other scenarios, e.g. in VPN access to a corporate network, as in the latter scenario the inner IP address is not publicly routable in general.

- IP addresses:

  - 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~~ The source IP address bound to the outbound SA equals the destination IP address bound to the inbound SA;
    ~~the~~ 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 inner 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.

NOTE: This further implies that the source address in the inbound SA and the destination address in the outbound SA at the P-CSCF equals the public IP address of the UE.

  - outbound SA at the UE:
    The source IP address bound to the outbound SA equals the public IP address of the UE. The public IP address is learned by the UE from the received parameter in the Via header in the 401 Unauthorized response to the initial unprotected REGISTER Request (cf Section M.7.2).
    The destination IP address bound to the outbound SA equals the destination IP address in the header of the IP packet in which the initial SIP REGISTER was sent to the P-CSCF.

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

NOTE: For the handling of the outer IP header in UDP encapsulated tunnel mode, see section on "Data related to the use of UDP encapsulated tunnel mode" below.

- 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].

NOTE: The handling of the protected ports is the same, irrespective of whether transport or UDP encapsulated tunnel mode is used.

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]

NOTE: The handling of the protected ports is the same, irrespective of whether transport or UDP encapsulated tunnel mode is used.

3. The P-CSCF is allowed to receive only REGISTER messages, messages relating to emergency services in accordance with [31] and [8], and error messages related to unprotected 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;
   - messages relating to emergency services in accordance with [31] and [8];
   - error messages related to unprotected messages.

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

Data related to the use of UDP encapsulated tunnel mode

- Tunnel endpoint addresses and header construction for tunnel mode:

  In case UDP encapsulated tunnel mode is selected, an "outer" IP header is added to protected packets exchanged between UE and P-CSCF, following the rules of tunnel mode processing according to [14]. While the IP addresses of the inner IP header are as specified above in the section about "Selectors", the IP addresses of the outer IP header shall be selected as follows:

  - **P-CSCF**:
  For the outbound SA at the P-CSCF the source address shall be the IP address of the P-CSCF, the destination address shall be the public IP address of the UE. For the inbound SA only the destination address of the outer IP header is used to identify the SA at the P-CSCF, together with the SPI. This address is the IP address of the P-CSCF.

  - **UE**:
  For the outbound SA at the UE the source address shall be the local IP address of the UE, the destination address shall be the address of the P-CSCF as in the destination address of the IP header of the initial unprotected REGISTER message. For the inbound SA only the destination address of the outer IP header is used to identify the SA at the UE. This address is the local IP address of the UE.

  Other data of the outer IP header (apart from IP addresses) shall be constructed as specified in [14].

- **Ports used in the encapsulating UDP header:**

  In case UDP encapsulated tunnel mode is selected, an encapsulating UDP header is inserted after the outer IP header. With respect to the ports used in the UDP header, the following rules shall be applied in accordance with standard [28]:

  - UE:
  Each protected and UDP encapsulated packet shall use port 4500 as source and destination port in the encapsulating UDP header.

  - P-CSCF:
  When the UE sends an UDP encapsulated packet towards the P-CSCF with the ports as described in the previous paragraph, the NAT will change the source port to a port different from 4500. This port is called port_Uenc. When the P-CSCF receives the first protected and UDP encapsulated message from the UE it shall store port_Uenc (cf. Section 7.2). From then on, all protected UDP encapsulated messages from the P-CSCF to the UE shall use port 4500 as source port and port_Uenc as destination port in the encapsulating UDP header.

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, mode) 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 or a re-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". REQ20087 In addition, if the P-CSCF has detected that the UE is located behind a NAT (cf. Section A 7.2), the P-CSCF shall check upon receipt of an initial (unprotected) REGISTER message, or a REGISTER message protected with UDP encapsulated tunnel mode, that the pair (UE_IP_address, UE_protected_server_port) has not yet been associated with entries in the "SA_table". Here the UE_IP_address is the source IP address in the packet header, and the protected client and server ports are sent as part of the security mode set-up procedure (cf. clause A 7.2).

NOTE: In case of multiple UEs behind the same NAT, the same public IP address may be assigned by the NAT to two different UEs. Therefore, the P-CSCF shall not accept registration attempts from UEs with the same address and protected server port in order to ensure unambiguous addressing of SIP messages sent towards the UE, using the protected server port.

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 M.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 M.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 ensure that the user associated with the SA, which was used to protect the incoming message from the UE, is identical to the user who is associated at SIP level with the message sent by the P-CSCF towards the network.

NOTE: Not all SIP messages necessarily contain public or private identities, e.g. subsequent messages in a dialogue. Other information, e.g. a dialogue identifier, may be used to associate the message with a user at SIP level.

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_IP_address, UE_protected_port, P-CSCF_protected_port, SPI, lifetime, mode) 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". Furthermore, the UE should select port numbers (pseudo-)randomly from a sufficiently large set of numbers not yet allocated at the UE. When the UE receives an error message indicating a collision of a pair (IP address, port), according to rule 3 above, the UE may retry the registration with differently selected port numbers.

NOTE: The UE should select port numbers (pseudo-)randomly for two reasons:
1) to avoid collisions of pairs (IP address, port) at the P-CSCF, cf. rule 3 above.
2) to thwart a limited form of a Denial of Service attack. UMTS PS access link security also helps to thwart this attack.

NOTE: The (pseudo-)randomization of port numbers is meant for both initial registrations and re-registrations

7. For each incoming protected message the SIP application at the UE shall verify that the correct inbound SA according to clause M.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.

M.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.

For the purpose of the description of the message processing in case UDP encapsulated tunnel mode is used, a conceptual functional element called "UDP encapsulation function" is used. The UDP encapsulation function handles all tasks relevant to the UDP encapsulation processing, i.e. the addition and removal of UDP headers to packets. In that sense it does not perform any IPSec processing as such. From an implementation point of view, it is immaterial whether the UDP encapsulation function and the IPSec processing are combined or kept separate. On the network side, the UDP encapsulation function may reside on the P-CSCF or in a separate device.

Relation of this Annex with the NAT traversal functionality specified in TS 24.229 [8]:

If the UE is located behind a NAT, the unprotected REGISTER message and the corresponding unprotected response (messages SM1 and SM6) shall be handled according to Annex F of [8]. For SIP messages protected with UDP encapsulated tunnel mode, the P-CSCF shall rewrite only the SDP according to Annex F.3 of [8], and shall not perform the rewriting of the SIP headers specified in Annex F.2 of [8]. The P-CSCF recognises from the mode parameter in the SA table (cf. section 7.1) that UDP encapsulated tunnel mode is used.

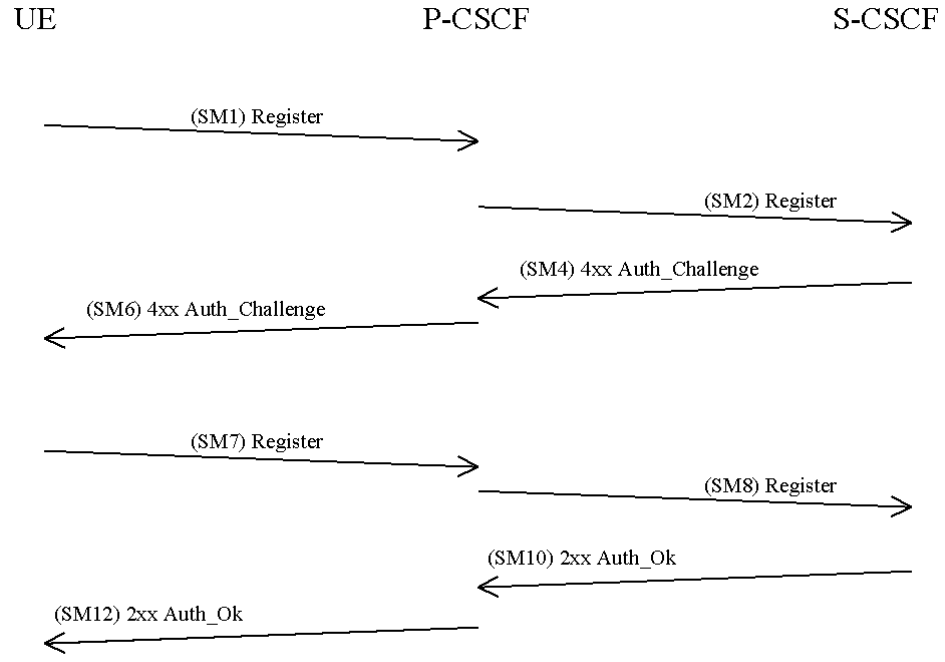

Figure M.8

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 M.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. It shall also contain the list of IPSec modes (i.e. transport and/or UDP encapsulated tunnel mode) supported by the UE.

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

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 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.

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.

If the source IP address of the IP packet header is different from the address contained in the top-most Via header, the P-CSCF concludes that the UE is located behind a NAT device parameter with the source IP address to the Via header and acts as described in Annex F of TS 24.229 [8]. In this case the P-CSCF concludes that the UE is located behind a NAT device. If the UE has not signalled support for UDP encapsulated tunnel mode in message SM1 the P-CSCF shall silently discard the message and stop performing any further steps.

Otherwise, if the source IP address of SM1 matches the UE address in the Via header, the P-CSCF concludes that the UE is not located behind a NAT. The P-CSCF then continues with the set-up of security associations as specified in section 7.2, otherwise it continues as specified in this annex.

NOTE: If the top-most Via header contains a domain name the P-CSCF shall perform the appropriate DNS procedures in order to retrieve the address information to be used for the comparison, as specified in Annex F of TS 24.229 [8].

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.

The P-CSCF then selects the SPIs for the inbound SAs. 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, cf. Annex H. 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. If the UE did not include any confidentiality algorithm in SM1 then the P-CSCF shall either select the NULL encryption algorithm or abort the procedure, according to its policy on confidentiality.

NOTE: It should be noted that, if the P-CSCF policy requires confidentiality, then all UEs with no encryption support would be denied access to the IMS network. This would apply in particular to UEs, which support only a Release 5-version of this specification or only Early IMS according to [25].

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

In case the P-CSCF has discovered before that the UE is located behind a NAT, it informs the UDP encapsulation function about the IPSec SA data relevant for the UDP encapsulation process. This data consists of the IP source and destination addresses of the outer IP headers and the SPIs used in all four SAs (cf. section M.6.3) established. At this point in time the UDP encapsulation function creates a table, the "UDP encapsulation table", with the following contents:

"UDP Encapsulation Table on the network side "				
	SA1	SA2	SA3	SA4
Src Addr	PCSCF	UE_pub	PCSCF	UE_pub
Dest Addr	UE_pub	PCSCF	UE_pub	PCSCF
Src Port	4500	***undef***	4500	***undef***
Dest Port	***undef***	4500	***undef***	4500
SPI	SPI_us	SPI_ps	SPI_uc	SPI_pc

The P-CSCF shall use port 4500 as the source port for UDP encapsulated packets towards the UE. The P-CSCF will also receive packets from the UE with and as the destination port 4500. This is the IPSec standard port for UDP ~~encpasulated~~encapsulated IPSec packets (see [28]). The source port for packets received by the P-CSCF from the UE and the destination port for packets sent by the P-CSCF towards the UE is not known yet and can only be learned in a later step (see below).

NOTE: A corresponding table on the UE side is not required as the ports used by the UE are not affected by the NAT.

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. The only exception from this is the case that the P-CSCF is configured to never apply confidentiality. In this case, it shall not include encryption algorithms to the *Security-setup*-line in SM6.

Furthermore, the P-CSCF indicates the IPSec mode of operation. In case the P-CSCF detected that the UE is behind a NAT, it indicates UDP encapsulated tunnel mode, otherwise transport mode is indicated.

NOTE: The P-CSCF may be configured to never apply confidentiality, e.g. because it trusts on the encryption provided by the underlying access network. In this case, the P-CSCF acts according to Release 5 specifications, and does not include encryption algorithms to the *Security-setup*-line in SM6. If the P-CSCF is configured to apply confidentiality whenever the UE supports it then the P-CSCF always includes the encryption algorithms in SM6, which it supports, even if the UE did not include encryption algorithms in SM1. This is to thwart bidding down attacks. 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 specifications, 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), IPSec mode)*

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 shall either configure UDP encapsulated tunnel mode or determine the IPsec mode according to the mode information contained in SM6. If no mode information is included in SM6, the UE shall first check whether it is located behind a NAT by checking for the presence of a "received"-parameter in the Via header of SM6. If the UE is not located behind a NAT, the UE assumes transport mode, otherwise it aborts the communication. If transport mode is used the UE continues with the set-up of security associations as specified in section 7.2, otherwise it continues as specified in this annex.

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)*

If UDP encapsulated tunnel mode is used, the UE shall use the following addresses and ports in the various headers of message SM7:

SIP header:
In the Via and Contact header the UE shall use its public IP address and protected server port. The UE learns its public IP address by inspecting the received parameter in the top-most Via header included in message SM6, in case such a parameter is present.

IP and UDP/TCP headers are used as specified in M.7.1.

If UDP encapsulated tunnel mode is applied, the UE shall start sending keep alive messages according to [28]. This ensures that the NAT binding is kept alive for the duration of the registration.

When SM 7 arrives at the P-CSCF it is at first processed by the UDP encapsulation function. The UDP encapsulation function can now learn port_Uenc, which the NAT has chosen for the UDP encapsulated packet. The UDP encapsulation function inserts this port in the UDP encapsulation table, so that the table is complete.

"UDP Encapsulation Table" on the network side				
	SA1	SA2	SA3	SA4
Src Addr	PCSCF	UE_pub	PCSCF	UE_pub
Dest Addr	UE_pub	PCSCF	UE_pub	PCSCF
Src Port	4500	***Port_Uenc***	4500	***Port_Uenc***
Dest Port	***Port_Uenc***	4500	***Port_Uenc***	4500
SPI	SPI_us	SPI_ps	SPI_uc	SPI_pc

The UDP encapsulation function removes the UDP header from the IP packet and hands it over to the IPSec processing.

After successful IPSec processing the SIP application in the P-CSCF shall check whether the integrity algorithms list, SPI_P and Port_P received in SM7 is identical with ~~the~~the corresponding 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 check in the P-CSCF.

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

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

After receiving SM12 not indicating an error, the UE can assume the successful completion of the security-mode setup.

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.

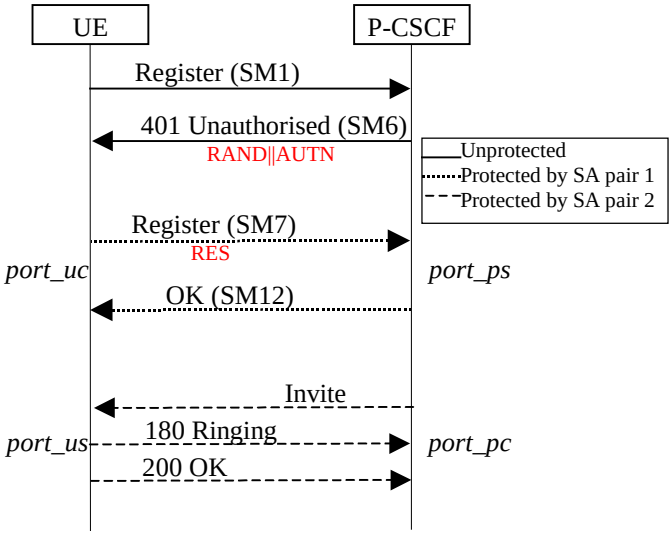

Figure 9

M.7.3 Error cases in the set-up of security associations

M.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.

M.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.

M.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.

M.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.

M.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.

The text in section 7.3.1 applies without changes.

M.7.3.2 Error cases related to the Security-Set-up

M.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.

M.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.

M.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).

M.7.3.2.4 Missing NAT traversal capabilities in the presence of a NAT

In case the P-CSCF detects the presence of a NAT, but the UE or the P-CSCF do not support NAT traversal as specified in this annex, the P-CSCF shall abort the procedure.

M.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.

M.7.4.1 Void

M.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. If SM1 was protected and UDP encapsulated tunnel mode is used in the old SAs, the new SAs shall also be configured in with UDP encapsulated tunnel mode. 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.

M.7.4.2 Void

M.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. If SM1 was protected and UDP encapsulated tunnel mode is used in the old SAs, the new SAs shall also be configured with UDP encapsulated tunnel mode. 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.

M.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.

The text in section 7.5 applies without changes.

M.8 ISIM

The text in section 8 applies without changes.

Annex N (normative): Enhancements to the access security to enable SIP Digest

N.1 SIP Digest

SIP Digest authentication and the requirements in this Annex shall not apply to access networks defined in 3GPP specifications. SIP Digest authentication and the requirements in Annex N shall be implemented by to the P-CSCF, S-CSCF, I-CSCF and HSS as specified below.

The provisions in Annex N is mandated for implementation on network components, but optional for implementation at the UE. The provisions in Annex N are optional for use. However, the use of one of the authentication mechanisms in this specification is mandated.

SIP Digest shall not be used in conjunction with IPsec.

NOTE 1: The use of SIP Digest in conjunction with IPsec, as specified in the main body and in Annex N of this specification, is technically impossible because SIP Digest does not generate session keys for use with IPsec security associations.

An additional scheme for authentication is SIP Digest as specified in RFC 3261 [6]. SIP Digest achieves mutual authentication between the UE and the HN, and is based on HTTP Digest as specified in RFC 2617 [12]. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI. The HSS and the UE share a preset secret (e.g., a password) associated with the IMPI. The generation of the authentication challenge shall be done in the same way as specified in RFC 2617 [12] and this document.

It is the policy of the HN that decides if an authentication shall take place for the registration of an additional IMPU that is not part of the already registered set of IMPUs associated with the same IMPI. If a UE supports SIP Digest as well as further authentication methods, the UE shall proceed as follows:

- If the access network is of a type defined in 3GPP specifications then the UE shall not select SIP Digest, in accordance with the requirement at the start of this clause.

NOTE 2: The rules listed in TR 33.978 [25] say how a UE can select between IMS AKA and Early IMS.

- If the access network is of a type not defined in 3GPP specifications then
  - if both the UE and network support IMS AKA according to the main body or Annex M of this specification, as determined by the use of sip-sec-agree [21], the authentication method shall be IMS AKA;
  - otherwise the authentication method shall be SIP Digest as specified in Annex N of this specification.

N.2 Authentication

N.2.1 Authentication Requirements

N.2.1.1 Authentication Requirements for Registrations

For the purposes of this subclause, the name "authentication" is used synonymously with "entity authentication".

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, i.e. the S-CSCF, cf. figure N.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. Every SIP REGISTER message shall contain the IMPI of the user.

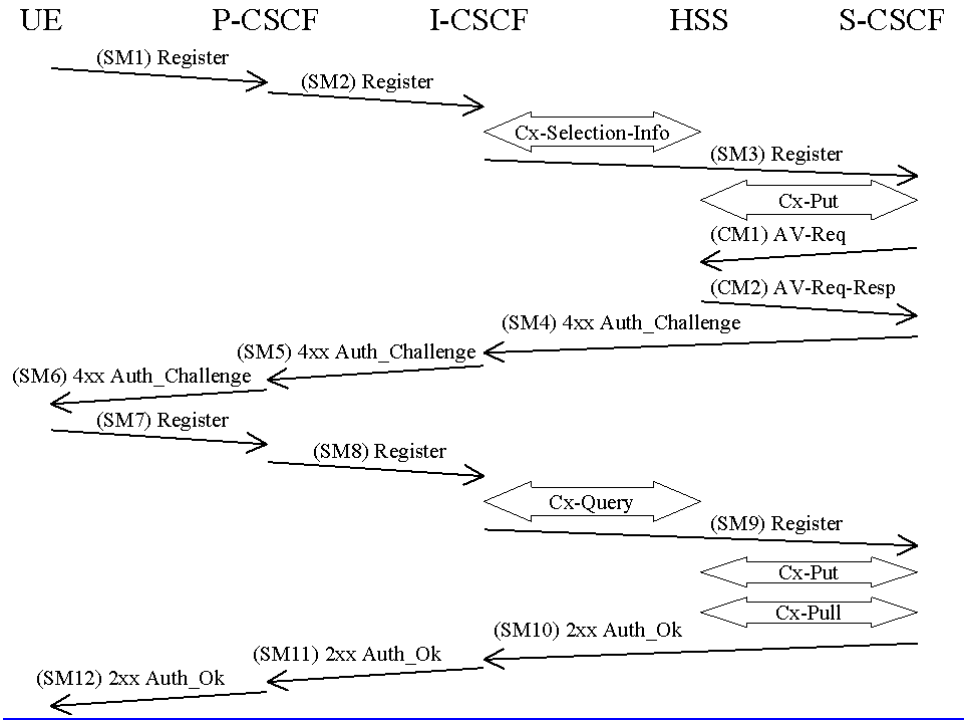

Figure N.1: The IMS Authentication using SIP Digest for an unregistered IM subscriber and successful mutual authentication

The detailed registration procedures are defined in TS 24.229 [8].

The NAT traversal procedures in draft-ietf-sip-outbound [32] and in TS 24.229 [8] clause K.4 shall apply.

NOTE 1: It is recognized that outbound can be useful for capabilities beyond NAT traversal (e.g. multiple registrations) however this annex does not consider such capabilities at this time.

The UE should include an indication of outbound support as defined in draft-ietf-sip-outbound [32] in all REGISTER requests. Per outbound, the P-CSCF shall be able to accept registration request with or without an indication of outbound support. However, the P-CSCF should only accept a register request without outbound support if it can determine that no NAT is present in the signaling path between the UE and the P-CSCF.

NOTE 2: It is left to stage 3 specifications how a P-CSCF can determine whether the conditions in the preceding paragraph are met. An operator may configure all UEs and P-CSCFs in his network not to use Outbound (provided there is no roaming). Cf. also the implications of the indication of outbound support for the P-CSCF procedures after receiving SM11.

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 UE 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.

The S-CSCF shall determine the type of authentication based on the rules in Annex P. If the IMS registration request is related to SIP Digest, then the procedures below apply.

Upon receiving the SIP REGISTER the S-CSCF shall use a SIP Digest Authentication Vector (SD-AV) for authenticating the user. If the S-CSCF has no valid SD-AV for the specific IMPI, then the S-CSCF shall send a request for SD-AV(s) to the HSS in CM1 where the number m of SD-AVs wanted is equal to 1.

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

Upon receipt of a request from the S-CSCF, the HSS sends one SD-AV to the S-CSCF using CM2. The SD-AV consists of the qop (quality of protection) value, the authentication algorithm, realm, and a hash, called H(A1), of the IMPI, realm, and password. Refer to RFC 2617 [12] for additional information on the values in the authentication vector for SIP Digest based authentication.

The qop value shall be set to "auth" since SIP Digest, as used in IMS, can only provide authentication, not message integrity.

CM2:
Cx-AV-Req-Resp(IMPI, realm, domain, algorithm, qop, H(A1))

The S-CSCF generates a random nonce, stores H(A1) and the nonce against the IMPI, and then sends a SIP 401 Auth_Challenge i.e., an authentication challenge towards the UE including the nonce in SM4. It also includes the qop and algorithm parameters. RFC 2617 [12] specifies how to populate the parameters of a 401 Auth_Challenge .

SM4:
401 Auth_Challenge(IMPI, realm, nonce, qop, algorithm, domain)

The I-CSCF forwards the SIP 4xx Auth_Challenge message towards the P-CSCF as SM5.

When the P-CSCF receives SM5 it shall forward the message to the UE.

SM6:
401 Auth_Challenge(IMPI, realm, nonce, qop, algorithm, domain)

Upon receiving the challenge, SM6, the UE generates a cnonce. It then uses the cnonce as well as parameters provided in the SM6 such as nonce and qop to calculate an authentication response according to RFC 2617 [12]. This response and other parameters are put into the Authorization header and sent back towards the network in SM7.

SM7:
REGISTER(IMPI, realm, nonce, response, cnonce, qop, nonce-count, algorithm, digest-uri)

NOTE 3: As specified in RFC 3261 [6], when the P-CSCF receives a SIP request from the UE, the P-CSCF checks the IP address in the "sent-by" parameter of the Via header field provided by the UE. If the "sent-by" parameter contains a domain name, or if it contains an IP address that differs from the packet source IP address, the P-CSCF adds a "received" parameter to that Via header field value. This parameter contains the source IP address from which the packet was received.

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 calculates the expected response using the previously stored H(A1) and stored nonce together with other parameters contained in SM9 (e.g., cnonce, nonce-count, qop, as specified in RFC 2617 [12]) and uses this to check against the response sent by the UE. 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.

NOTE 4: Depending on its local security policy, the S-CSCF may delete H(A1) immediately after checking the Digest response, but this may then lead to an increased exposure of H(A1) on the Cx-interface as H(A1) would then have to be fetched from the HSS more often.

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 of 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.

If the user has been successfully authenticated, the S-CSCF sends a SM10 SIP 2xx Auth OK message to the I-CSCF indicating that the registration was successful. The 2xx Auth OK message contains the Authentication-Info header with a response digest as specified in RFC 2617 [12]. The response digest allows the UE to authenticate the HN.

In SM11 the I-CSCF forwards the SIP 2xx Auth OK towards the P-CSCF.

The P-CSCF associates the UE's packet source IP address along with the "sent-by" parameter of the Via header, cf. RFC 3261 [6], of the REGISTER message with the IMPI and all the successfully registered IMPUs related to that IMPI. If draft-ietf-sip-outbound [32] is used then the P-CSCF shall also include the UE's packet source port of the REGISTER message as part of the association. The P-CSCF stores the associated parameters in an IP address check table. If draft-ietf-sip-outbound [32] is not used then the P-CSCF shall overwrite any existing entry in the IP address check table which has the same IP address, but a different IMPI. If draft-ietf-sip-outbound [32] is used then the P-CSCF shall overwrite any existing entry in the IP address check table which has the same (IP address, port) pair, but a different IMPI.

NOTE 5: If a P-CSCF associated the port with the IMPI even when draft-ietf-sip-outbound [32] was not used then the UE would be unnecessarily restricted in opening new connections during a registration.The restriction is unavoidable in the presence of NAT.

Upon receiving SM12, the UE shall calculate the expected response from the HN as described in RFC 2617 [12]. To authenticate the HN, the UE shall compare its expected response to the response provided by the HN. If the comparison fails the UE shall abort the communication.

N.2.1.2 Authentication Requirements for Non-registration Messages

For the purposes of this subsection, the name "authentication" is used synonymously with "message origin authentication".

The IP address check table (cf. subclause N.2.1.1) shall be used by the P-CSCF to identify the initiator of subsequent requests as follows: one of the public user identities associated with the packet IP address (and port if applicable) is selected and asserted to the S-CSCF according to the rules in TS 24.229 [8], subclause 5.2.6.3.

In addition, subsequent requests (e.g. INVITE) may be authenticated with SIP Digest, as described in the following:

NOTE 1: The assertion of IMPUs based on checks of IP address (and ports if applicable) provides a reasonable level of security only in environments where the risk from source IP address and port spoofing or from IP address re-assignment unnoticed by the SIP application is sufficiently low. If the environment does not fulfill this condition then it is recommended to use SIP Digest in conjunction with either TLS, as specified in Annex O of this specification, or with the SIP Digest proxy authentication mechanism as specified in this subclause. It is not part of this specification to determine which environments fulfill the conditions in this NOTE. This is left to specifications, possibly maintained by standardization bodies other than 3GPP, describing these environments.

When the S-CSCF receives a SIP request with a method other than the REGISTER method from the UE, the S-CSCF may perform authentication on the SIP request according to the operator's policy and according to the following procedures.

- If the request does not contain a Proxy-Authorization header or the Proxy-Authorization header does not contain a digest response the S-CSCF shall send a 407 (Proxy Authentication Required) response to challenge the UE. The 407 response shall contain digest challenge parameters in a Proxy-Authenticate header as defined by RFC 2617 [12]. Upon receiving the challenge the UE shall extract digest challenge parameters from the Proxy-Authenticate header field and calculate a digest response as indicated in RFC 2617[12]. The UE should store the received digest challenge. The UE then sends a new request to the network containing a Proxy-Authorization header in which the header fields are populated as described in RFC 2617 [12] using the calculated digest response. Upon receiving the new request which contains a digest response, the S-CSCF verifies the user's identity by validating the digest response information (e.g. the nonce-count) contained in the Proxy-Authorization header field against the expected information;

- If the check is successful then the request has been authenticated, and the S-CSCF sends a Proxy-Authentication-Info header along with the 2xx AUTH_OK towards the UE. The S-CSCF includes the response-auth parameter containing the S-CSCF's challenge response in the Proxy-Authentication-Info header which allows the UE to authenticate the S-CSCF;

  Editor's Note: The Proxy-Authentication-Info header is not currently defined in RFC 3261 [bb]. The progress of this issue in the IETF will need to be evaluated and a decision made on whether to include this feature in Release 8 of this specification.

- If the check fails, based on local policy the S-CSCF may choose to re-challenge the user by using the same procedure described in this subclause, or reject the request by sending a 403 response.

When the UE is to send a non-REGISTER SIP request it should first check whether it has a digest challenge stored which was previously received in a Proxy-Authorization header. If such a digest challenge is available in the UE the UE should use it together with the nonce-count mechanism as specified in RFC 2617 [12] to calculate a digest response, include the digest response in a Proxy-Authorization header and send this header together with the non-REGISTER SIP request.

NOTE 2: According to RFC 2617 [12], the S-CSCF may send a 407 (Proxy Authentication Required) as a response to any non-REGISTER request, indicating that the nonce is stale and the digest response shall be recomputed using the fresh challenge sent in the same 407 message.

When the S-CSCF has successfully used the SIP Digest proxy authentication mechanism it shall check the public user identities associated with the authenticated user against the public user identity asserted by the P-CSCF. In case of conflict, the result of SIP Digest proxy authentication shall take precedence, and the S-CSCF shall base further processing of the message on one of the public identities associated with the authenticated user.

NOTE 3: Such a conflict may occur when one of the conditions mentioned in NOTE x is not fulfilled.

Alternatively, TLS may be used by the P-CSCF to authenticate non-registration messages, cf. Annex O.

N.2.2 Authentication failures

N.2.2.1 User Authentication failure

If the S-CSCF detects the user authentication failure due to an incorrect response (received in SM9), the S-CSCF sends a failure notification to the UE. The S-CSCF shall set the registration-flag in the HSS to unregistered or Not registered if the IMPU is not currently registered. To set the flag the S-CSCF sends in CM3 a Cx-Put to the HSS as shown in Figure 5. If the IMPU is currently registered, the S-CSCF does not update the registration flag. 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

N.2.2.2 Network authentication failure

For network authentication failures, the flow is identical as for the successful registration in N.2.1 up to SM12. After receipt of the 2xx Auth_OK, the UE shall attempt to validate the response digest. If the response digest authentication fails, the UE shall consider registration as failed and may start a new registration.

N.2.2.3 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 N.2.1.

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 Not registered or 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.

N.2.3 SIP Digest synchronization failure

For SIP Digest based authentication, the UE can not detect synchronization failures when processing SM6 but the S-CSCF can check if the nonce value in SM9 is invalid with a valid digest for that nonce (indicating that the client knows the correct username/password) to determine that a synchronization failure has occurred.

Another possible synchronization failure may occur (e.g. during a replay attack) when the nonce-count value (sent by the UE) is different from the one expected by the network. In order to detect such a synchronization failure, the S-CSCF shall store the value of the nonce-count value sent by the specific UE (in the SM7) during the last successful authentication.

In both of these situations, the S-CSCF shall reject the request and send out the challenge (i.e., SM4) again using a new nonce. The stale parameter in the www-Authenticate header is set to TRUE (case-insensitive) in this message.

For SIP Digest, when the UE receives the challenge with the stale parameter in the www-Authenticate header set to TRUE, it shall retry the REGISTER request with a new response with Digest computed over the new nonce (i.e., starting from SM7 in Figure N.1).

N.2.4 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 SIP Digest procedure that will allow the S-CSCF to re-authenticate the user.

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

Annex O (normative): Enhancements to the access security to enable TLS

O.1 TLS

O.1.1 TLS Access Security

TLS access security and the requirements in this Annex shall not apply to access networks defined in 3GPP specifications. The requirements in Annex O shall be implemented in the P-CSCF, S-CSCF and HSS as defined specified below.

SIP Digest, as specified in Annex N, shall be used when TLS access security, as specified in Annex O, is used.

The provisions in Annex O are mandatory for implementation on network components, but optional for implementation at the UE. The provisions in Annex O are optional for use.

NOTE: If the risk of man-in-the-middle attacks in the access network between UE and P-CSCF cannot be ruled out then the operator should configure the UEs such that the UEs always use either TLS, according to Annex O, or IPsec, according to the main body or Annex M, or abort the communication. Otherwise, there is a risk of a man-in-the-middle bidding down the UE to "no signalling security" without the P-CSCF even noticing, even when both, the UE and P-CSCF support TLS and want to use it.

O.1.2 Confidentiality protection

Operators shall take care that the deployed confidentiality protection solution and roaming agreements fulfils the confidentiality requirements presented in the local privacy legislation.

When TLS is used to protect signalling information between the UE and the P-CSCF, the following confidentiality mechanisms are provided for TLS based access security:

1. Negotiation of TLS related confidentiality protection features shall take place at the TLS layer as specified in clause O.2.
2. The UE shall always offer TLS CipherSuites to the P-CSCF to be used for the session, as specified in RFC 2246 [34] and clause O.2.1.
3. The P-CSCF shall decide which TLS CipherSuites are used, as specified in RFC 2246 [34].

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

O.1.3 Integrity protection

When TLS is used to protect signalling information between the UE and the P-CSCF, the following integrity mechanisms are provided for TLS based access security:

1. Negotiation of TLS related integrity protection features shall take place at the TLS layer.
2. The UE shall always offer TLS CipherSuites for P-CSCF to be used for the session, as specified in RFC 2246 [34] and clause O.2.1.

3. The P-CSCF shall decide which TLS CipherSuites are used, as specified in RFC 2246 [34].

4. The UE and the P- CSCF shall both verify that the data is sent and received according to RFC 2246 [34]. This verification is also used to detect if the received data has been tampered with.

5. Replay attacks and reflection attacks shall be mitigated by using the mechanism provided by TLS.

6. UE and P-CSCF shall verify the identities of the TLS session endpoints according to clause O.2.1.

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

O.1.4 TLS integrity protection indicator

For REGISTER messages protected by TLS according to this Annex, the P-CSCF shall attach an appropriate indicator to the message when forwarding it to the S-CSCF. This indicator shall enable the S-CSCF to distinguish between protection by IPsec according to the main body or Annex M and protection by TLS according to this Annex. For more details on the use of this indicator cf. clause O.2.2. When a REGISTER message is not protected by TLS the P-CSCF shall not include any indication about integrity protection by TLS in the messages.

O.2 TLS Session set-up procedure

O.2.1 TLS Profile for TLS based access security

The UE and the P-CSCF shall support the TLS version as specified in RFC 2246 [34].

Editor's Note: TLS CipherSuites and X.509 certificate profiles are discussed in other technical specifications (e.g., 33.222, 33.234 and 33.310). Alignment of these and the text in this clause is ffs.

- Protection mechanisms:
  - The UE and P-CSCF shall support the CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA and TLS_RSA_WITH_AES_128_CBC_SHA. All other CipherSuites as defined in RFC 2246 [34] and RFC 3268 [33] are optional for implementation.
  - CipherSuites with NULL encryption may be used. The UE shall always include at least one CipherSuite that supports (non-NULL) encryption during the handshake phase.
  - CipherSuites with NULL integrity protection (or HASH) are not allowed.
  - The key exchange method shall not be anonymous. Hence CipherSuites with anonymous Diffie-Hellman key exchange (all CipherSuites with key exchange algorithm DH_anon or DH_anon_EXPORT) are not allowed.
  - RFC 2246 [34] supports the negotiation and use of compression methods. However, since these methods are not specified within RFC 2246 [34], compression shall not be used.
- Authentication of the P-CSCF
  - The P-CSCF shall be authenticated by the UE as specified in RFC 2246 [34] by presenting a valid server certificate. The P-CSCF certificate profile shall be based on TLS certificates as presented in clause O.5.1.
- Authentication of the UE

- The P-CSCF shall not request a certificate in a Server Hello Message from the UE. The HN shall authenticate the UE as specified in Annex N of this specification.

- Verification of the TLS session endpoints

  - In order for the UE to be able to trust the TLS session endpoint, the P-CSCF certificate shall be used during the authentication procedure.

  - In order for the P-CSCF to be able to trust that the UE, which was authenticated according to Annex N, is the TLS session endpoint, the P-CSCF shall use the mechanism for associating the TLS Session ID with registration parameters IP address, port, IMPI, IMPU(s), specified in clause O.2.2, and shall have assurance that man-in-the-middle attacks can be mitigated, e.g. by following the rules in the NOTE in clause O.1.1.

- TLS session parameters

  - The TLS Handshake Protocol negotiates a session, which is identified by a Session ID.

    - The lifetime of a Session ID is subject to local policies of the UE and the P-CSCF. A recommended lifetime is one hour (or at least more than the re-REGISTRATION time out). The maximum lifetime specified in RFC 2246 [34] is 24 hours. The procedure for TLS session re-negotiation in IMS is specified in clauses O.4.1 and O.4.2.

- Ports

  - The P-CSCF shall be prepared to accept TLS session requests on port 5061or on a port published by the operator.

- Forwarding requests

  - The procedures for forwarding requests by the edge proxy in draft-ietf-sip-outbound [32] shall apply to the P-CSCF when managing TLS connections.

NOTE 1: The use of draft-ietf-sip-outbound [32] in conjunction with TLS is needed so that terminating requests can re-use an existing TLS connection.

O.2.2 TLS session set-up during registration

The TLS session 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. Subsequent signalling communications in this session will be integrity protected based on the TLS session that was established during the authentication process.

The set-up of the TLS session between the UE and the P-CSCF is based on the TLS profile specified in clause O.2.1. The sip-sec-agree negotiation according to RFC 3329 [21] is performed during the registration procedure to negotiate the choice of the security mechanism. Annex H of this specification describes the parameters of RFC 3329 [21] for the set-up of TLS sessions.

The following describes how TLS session set-up is integrated with the initial registration procedure described in Annex N.1:

Up to and including message SM6 received by the UE, the procedures for the cases with and without TLS are identical, except for the following:

- In SM1 the UE includes sip-sec-agree negotiation headers according to RFC 3329 [21], which must include one header with value "tls" (cf. annex H), if TLS is to be used.

- In SM 6 the P-CSCF includes sip-sec-agree negotiation headers, which must include one header with value "tls" and the highest q-value of all security mechanisms common to UE and P-CSCF (cf. annex H), if TLS is to be used.

After receiving SM6, when TLS was selected by the P-CSCF the procedure continues as follows:

- the UE performs a TLS handshake with the P-CSCF, the UE shall not re-use an existing TLS connection for initial registrations;
- after successful establishment of a TLS connection, the UE sends SM7 over this TLS connection, including sip-sec-agree negotiation headers;
- the P-CSCF then sends SM8, together with a TLS integrity protection indicator indicating the logical value "authentication pending".
- the S-CSCF receives this message as SM9 and treats it according to Annex N. If the authentication of the UE is successful the S-CSCF shall associate the registration with the local state "tls-protected".
- when the P-CSCF receives message SM11 (200 OK) it shall associate the UE's IP address and port of the TLS connection with the TLS Session ID, the IMPI and all the successfully registered IMPUs related to that IMPI. From this point on, the P-CSCF shall not accept any SIP signalling messages outside the TLS connection other than REGISTER messages, messages relating to emergency services in accordance with [8] and [31], and error messages.
- after the UE has received SM12 it shall not accept any SIP signalling messages outside the TLS connection other than responses to REGISTER messages, messages relating to emergency services in accordance with [8] and [31], and error messages.

An S-CSCF shall accept a REGISTER message with a TLS integrity protection indicator indicating "authentication pending" only if it contains a verifiable Digest value computed over a valid challenge according to Annex N.

NOTE: The S-CSCF may have a local security policy to treat messages other than initial REGISTER messages, messages relating to emergency services, and error messages, differently depending on whether the registration is associated with the state "tls-protected".

O.3 Error cases in the set-up of TLS sessions

O.3.1 Error cases related to TLS

Errors related to SIP Digest failures are specified in Annex N. However, this clause additionally describes how these shall be treated, related to security setup.

O.3.1.1 User authentication failure

If the UE response does not match with the response calculated by the S-CSCF, the authentication of the user fails at the S-CSCF. The S-CSCF shall send a 4xx Auth_Failure message to the UE, via the P-CSCF. Afterwards, both the UE and the P-CSCF shall close the TLS connection and delete the associated TLS session if one was established.

O.3.1.2 Network authentication failure

If the UE is not able to successfully authenticate the network due to failed validation of the P-CSCF certificate, the UE shall send an alert message to the P-CSCF, which includes the failure information as specified in RFC 2246 [34].

O.3.1.3 Synchronisation failure

When the UE receives the challenge with the stale parameter in the www-Authenticate header set to TRUE, the UE shall retry the REGISTER request with a new encrypted response. The existing TLS session shall be used for the retry.

O.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 new registration procedure if it still requires any IM services.

O.3.2 Error cases related to the Security-Set-Up

The requirements in clauses 7.3.2.1 and 7.3.2.2 apply.

O.4 Management of TLS sessions

O.4.1 Management of TLS sessions at 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, including any TLS connection and session successfully created in a previous incomplete registration procedure.

The UE may initiate a TLS session renegotiation at any time. When the UE receives a HELLO request from the P-CSCF it should initiate a renegotiation. The UE shall send all TLS session renegotiation messages inside the existing TLS connection, according to RFC 2246 [34].

When the TLS connection is lost the UE shall initiate a registration procedure according to Annex N.

O.4.2 Management of TLS sessions at the P-CSCF

The lifetime of the TLS session negotiated between the UE and the P-CSCF is subject to local policies.

The P-CSCF may trigger a TLS session renegotiation at any time by sending a HELLO request message to the UE. The P-CSCF shall send this message and all TLS session renegotiation messages inside the existing TLS connection, according to RFC 2246 [34]. According to its local policy, the PCSCF may abort the communication if the UE does not initiate a TLS session renegotiation.

When the TLS session renegotiation is successfully completed, the P-CSCF shall replace the old Session ID with the new TLS Session ID associated with the UE's IP address and port of the TLS connection, the IMPI and all the successfully registered IMPUs related to that IMPI, cf. clause O.2.2.

The P-CSCF shall accept TLS handshake messages outside TLS connections associated with an existing registration only during a registration procedure according to Annex N.

O.4.3 Authenticated re-registration

If the UE has an already active TLS session, then it shall use this to protect the REGISTER message for re-registration.

When the P-CSCF receives a REGISTER message protected by a TLS session whose TLS Session ID is associated with an IMPI from a previously successful registration (cf. O.2.2), then the P-CSCF shall verify that the IMPI in the REGISTER matches the IMPI associated with the TLS Session ID. If the IMPIs match, then the P-CSCF shall

forward this REGISTER message together with a TLS integrity protection indicator indicating the logical value "authentication complete".

When the S-CSCF receives a REGISTER message with a TLS integrity protection indicator indicating the logical value "authentication complete" it may authenticate the user by means of SIP Digest, according to the local security policy of the S-CSCF.

If the UE considers the TLS session 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. In this case, the S-CSCF shall determine the applicable authentication scheme according to Annex P.

O.5 TLS Certificate Profile and Validation

O.5.1 TLS Certificate

X.509 digital certificates [35] shall be used for authentication in TLS. All X.509 certificates shall be signed by a trusted party. The certificates shall be profiled as follows:

Editor's Note: TLS CipherSuites and X.509 certificate profiles are discussed in other technical specifications (e.g., 33.222, 33.234 and 33.310). Alignment of these and the text in this clause is ffs.

TLS Server Certificates	
Subject Name Form	C=<Country> O=<Company> CN=<FQDN> Additional fields may be present in the subject name. FQDN is the server's fully qualified domain name (e.g., server.example.com). Only a single FQDN is allowed in the CN field.
Intended Usage	These certificates are used to authenticate TLS handshake exchanges (and encrypt when using RSA key exchange).
Validity Period	Set by operator policy
Modulus Length	1024, 1536, 2048
Extensions	KeyUsage[critical](digitalSignature, keyEncipherment) extendedKeyUsage (id-kp-serverAuth, id-kp-clientAuth) authorityKeyIdentifier (keyIdentifier=<subjectKeyIdentifier value from CA cert>)

O.5.2 Certificate validation

TLS certificates shall be verified as part of a certificate chain that chains up to a trusted Root certificate. The chain may contain intermediate Certification Authority (CA) certificates.

Usually the first certificate in the chain is not explicitly included in the certificate chain that is sent by the P-CSCF to the UE. In the cases where the first certificate is explicitly included, it shall already be known to the verifying party ahead of time and shall not contain any changes to the certificate, with the possible exception of the certificate serial

number, validity period and the value of the signature. If changes other than the certificate serial number, validity period and the value of the signature exist in the root certificate that was sent by the P-CSCF to the UE in comparison to the known root certificate, the UE shall conclude that the certificate verification has failed.

UEs shall build the certificate chain and validate the TLS certificate according to the "Certificate Path Validation" procedures described in [35]. In general, X.509 certificates support a liberal set of rules for determining if the issuer name of a certificate matches the subject name of another. The rules are such that two name fields may be declared to match even though a binary comparison of the two name fields does not indicate a match. [35] recommends that certificate authorities restrict the encoding of name fields so that an implementation can declare a match or mismatch using simple binary comparison. Accordingly, the DER-encoded tbsCertificate.issuer field of a certificate shall be an exact match to the DER-encoded tbsCertificate.subject field of its issuer certificate. An implementation may compare an issuer name to a subject name by performing a binary comparison of the DER-encoded tbsCertificate.issuer and tbsCertificate.subject fields.

O.5.3 Certificate Revocation

Certificate Revocation Lists (CRLs) may be checked as part of certificate path validation. The CRL profile and how a UE obtains a CRL is not defined.

Annex P (normative): Co-existence of authentication schemes IMS AKA, Early IMS and SIP Digest

The authentication schemes IMS AKA and SIP Digest are specified in the main body and Annex N of this specification respectively. Early IMS is specified in TR 33.978 [25].

The way the S-CSCF will determine the authentication scheme associated with a registration request is ffs.

Annex Q (informative): Usage of the authentication mechanisms for non-registration messages in Annexes N and O

Q.1 General

The name “authentication mechanism” is used here synonymously with “mechanism for message origin authentication”. The following three authentication mechanisms for non-registration messages, which can only be used in conjunction with SIP Digest authentication for registrations, are included in Annexes N and O:

- TLS:
  In this procedure, the P-CSCF associates source IP address and port of the TLS connection with the TLS Session ID, the IMPI and all the successfully registered IMPUs related to that IMPI. The P-CSCF uses this association later, when receiving non-registration messages, to assert identities to the S-CSCF based on the TLS connection over which the packet was received, cf. Annex O.2. For more information on the assertion of identities cf. below. TLS is optional according to Annex O.

- IP address check:
  In this procedure, the P-CSCF associates IP address and, if draft-ietf-sip-outbound [32] is used, also the source port of the packet in which the REGISTER message was received, with the identities of the user during a successful registration. The P-CSCF uses this association later, when receiving non-registration messages, to assert identities to the S-CSCF based on IP address and, if applicable, port of the received packet, cf. Annex N.2.1. The IP address check is mandatory according to Annex N.

- SIP Digest proxy-authentication:
  In this procedure, the S-CSCF authenticates a non-registration message by verifying the Digest response in the Proxy-Authorization header. If the non-registration message contains no Proxy-Authorization header, or if the nonce is stale, the S-CSCF may challenge the non-registration message by sending a 407 SIP message with a Proxy-authenticate header containing a nonce. This procedure is transparent for the P-CSCF. SIP Digest proxy-authentication is optional according to Annex N.

Q.2 Assertion of identities by the P-CSCF

Assertion of identities by the P-CSCF is currently described in TS 24.229 [8], clause 5.2.6.3. This clause is referenced in Annex N.2.1 of this specification. The underlying assumption of this clause is the use of IMS AKA with IPsec.

It is briefly recapped how identity assertion works for IMS AKA with IPsec as this helps to understand its use in Annex N: The P-CSCF stores the IP address and port together with the IMPI and the registered IMPUs in an "SA table" during a successful registration. The idea of identity assertion for non-registration message is that the P-CSCF securely knows from the source IP address and port, tied to the IPsec security association, which user sent the non-registration message. The P-CSCF therefore can assert to the S-CSCF that a certain IMPU is related to the sender of the non-registration message. The P-CSCF uses the P-Asserted-Identity header for this purpose. The S-CSCF has to rely on the P-CSCF for the verification of user identities as the security is provided by IPsec which terminates at the P-CSCF.

The relevant paragraphs from TS 24.229, clause 5.2.6.3, are:

> "When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.
>
> When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more than one default public user identity available, the P-CSCF shall randomly select one of them.
>
> NOTE 1: The contents of the From header do not form any part of this decision process."

It is clear that the S-CSCF needs to be certain about the user identities associated with a non-registration message, e.g. for charging purposes or for being able to convey the asserted identities to application servers (ASs). The concept of identity assertion may be applied to the three authentication mechanisms for non-registration messages, which may be used in conjunction with SIP Digest authentication for registrations, as follows:

- TLS:
  This case is very similar to the IPsec case as the P-CSCF knows the originator of a message from the TLS session (i.e. security association) with which the corresponding packet was protected. The procedures in TS 24.229, clause 5.2.6.3 apply without changes.

- IP address check:
  This case is also similar to the IPsec and TLS cases. The P-CSCF knows the originator of a message from the association of IP address and, if applicable, port with the user identities in the IP address check table which it established during registration. The procedures in TS 24.229, clause 5.2.6.3 apply in the P-CSCF without changes. A minor change of the local S-CSCF behaviour is required when the mechanism is used in conjunction with SIP Digest proxy-authentication, cf. next paragraph.

- SIP Digest proxy-authentication:
  This case is different from the previous cases in that proxy-authentication is transparent to the P-CSCF. The P-CSCF therefore cannot assert any identity to the S-CSCF. However, the S-CSCF has now secure knowledge of the user's private identity. The P-CSCF-related procedures in TS 24.229, clause 5.2.6.3 therefore can remain the same only when they are used in conjunction with the IP address check. In order to cover a potential error condition of a mismatch in the S-CSCF between the identity asserted by the P-CSCF by means of IP address check and the identity verified by the S-CSCF by means of Digest proxy-

authentication, the rule is added that the latter shall take precedence as Digest proxy-authentication is the stronger of the two mechanisms, cf. below.

Q.3 Strengths and boundary conditions for the use of authentication mechanisms for non-registration messages

- TLS:

  During the set-up phase SIP Digest with TLS is somewhat weaker than IMS AKA with IPsec because the client end of the TLS tunnel is authenticated by means of the password-based Digest mechanism, and not the UICC-based AKA mechanism, and because the session keys are cryptographically tied to authentication with IMS AKA, which is not the case for SIP Digest with TLS. But once the TLS tunnel has been set up securely, the strengths of TLS and IPsec are comparable, and no attacks, except attacks on the security of endpoint platforms, seem feasible. TLS requires TCP and does not work for UDP.

- SIP Digest proxy-authentication:

  This mechanism is weaker than TLS or IPsec because the message origin authentication relies on a message authentication code (the Digest response in the Proxy-Authorization header), which is not cryptographically tied to the body nor to the header of the SIP message. (Note that qop = auth-int, which would at least provide a cryptographic tie with the message body, cannot be used in the IMS context.) Therefore, certain man-in-the-middle attacks are theoretically conceivable where an attacker could "steal" a Digest response from one message and append it to another. These attacks may, however, be impractical in many deployment scenarios so that the SIP Digest proxy-authentication provides sufficient security in these scenarios. An attacker being only able to spoof source IP address and port would not be able to break SIP Digest proxy-authentication.

  There would be no technical problem in using SIP Digest proxy-authentication together with TLS, but the only security advantage would be increased home control, in case the P-CSCF is in a visited network.

- IP address check:

  This mechanism has two main benefits:

  - One benefit of the IP address check mechanism is for operators who would otherwise rely entirely on link layer security. If only link layer security was provided then an attacker, although correctly authenticated at the link layer, could spoof SIP addresses and impersonate another IMS user. The IP address check provides the missing link between lower layers and SIP layer to prevent this kind of attack. Reasons why operators may not want to use TLS or SIP Digest proxy-authentication may include clients not supporting these mechanisms, need for server certificates (in the TLS case) or performance.
  - Another benefit of the IP address check mechanism is that the existing mechanism for identity assertion in the P-CSCF can be used in the same way as for IMS AKA with IPsec, cf. above.

  However, the IP address check mechanism has to fulfill additional boundary conditions to work securely. If there is uncertainty about the boundary conditions of a given environment it is recommended to use TLS or SIP Digest proxy-authentication.

  - An attacker being able to spoof source IP address and port of another registered user can break this mechanism. Therefore, this mechanism can only be used in environments where IP address and port spoofing occurs neither in the public access network nor on the customer premises. In this sense, the IP address check mechanism is weaker than SIP Digest proxy-authentication.

- When the IP address check mechanism is not used in conjunction with draft-ietf-sip-outbound [32], then only the IP address is associated with the user's identities, cf. Annex N.2. In this case, it is additionally required to ensure that two different users cannot share the same IP address. An example of when this could happen would be when a UE not fully compliant to Annex N does not use draft-ietf-sip-outbound [32], although it sits behind a NAT, and the P-CSCF does not realise that there is a NAT. Hence the requirement in Annex N.2 that "the P-CSCF should only accept a register request without outbound support if it can determine that no NAT is present in the signaling path between the UE and the P-CSCF". Another example would be two users sharing the same machine with one IP address, and not using draft-ietf-sip-outbound [32]. It depends on the environment whether the additional requirement in this bullet can be fulfilled.
- It may happen that a UE loses connection without being able to deregister in the IMS, and the access network consequently re-assigns the IP address to another user, or a NAT re-assigns the port to another user. To cover such cases, Annex N states that the P-CSCF shall overwrite any existing entry in the IP address check table when a new registration with a different IMPI, but the same IP address (and port, if applicable) is successfully performed. In the absence of malicious attacks the IP address check mechanism then works correctly.
- An attacker may try to exploit IP address and port re-assignment as follows: he repeatedly attaches to the network hoping to be assigned the IP address or port of another user who dropped off without deregistering in IMS. If this indeed happens then any non-registration message sent by the attacker would be accepted by the IP address check mechanism in the P-CSCF as coming from the previous user. The attacker does not attempt to register in IMS as he would not be able to send a correct SIP Digest response. This possibility of attack seems difficult to exploit, but again, the likelihood for success depends on the environment.

Appendix I Acknowledgements

We wish to thank the vendor participants contributing directly to this document:

Steve Dotson and Bernard McKibben, CableLabs

Sean Schneyer - Ericsson

Guenther Horn - Nokia Siemens Networks

Nhut Nguyen - Samsung

Stuart Hoggan - CableLabs

Appendix II Change History

Base document for I01:
3GPP TS 33.203 V6.90 (2005-12) plus cable-specific changes.

Base document for I02:
3GPP TS 33.203 V6.90 (2005-12) plus cable-specific changes and the following engineering changes.

ECN	ECN Date	Summary
33.203-N-06.0332-5	9/11/06	Minor Technical and Editorial Clarifications

Base document for I03:
3GPP TS 33.203 V7.60 (2006-07) plus cable-specific changes and the following engineering changes.

ECN	ECN Date	Summary
33.203-N-07.0413-5	5/14/07	To add PacketCable 2.0 specific specifications to 3GPP Release 7 of TR 33.203 (R7 alignment). [This EC not incorporated, see below.]
33.203-N-07.0474-3	8/6/07	To add PacketCable 2.0 specific requirements to 3GPP Release 7 of TR 33.203 (R7 alignment). [This EC supersedes 33.203-N-07.0413-5.]

Base document for I04:
3GPP TS 33.203 V7.8 (2007-12) plus cable-specific changes and the following engineering changes.

ECN	ECN Date	Summary
33.203-N-07.0491-2	11/5/07	Removal of GBA references
33.203-N-08.0510-1	3/24/08	PKT 33.203 update for 3GPP R7 December 2007 base
33.203-N-08.0511-3	3/31/08	PKT 33.203 SIP Digest and TLS updates

Base document for I05:
3GPP TS 33.203 V7.8 (2007-12) plus cable-specific changes and the following engineering changes.

ECN	ECN Date	Summary
33.203-N-09.0561-1	4/27/2009	IETF draft alignment