3GPP TSG SA WG3 Security — S3#22 **S3-020167**

25 - 28 February 2002

Bristol, UK

Title: The use of USIMs and ISIMs for IMS
Source: SA3
To: SA2
Copy: SA1, T3, CN1, T2

Contact Person:
Name: Peter Howard
Tel. Number: +44 1635 676206
E-mail Address: peter.howard@vodafone.com

Attached: TS 33.203 v2.0.0

SA3 have handled the following incoming LSs on the use of USIMs and ISIMs for IMS:

- S2-013599 (=S3-0200018)
- T3-020139 (=S3-0200042)
- S1-020577 (=S3-0200059)
- S1-020579 (=S3-0200060)
- S2-020912 (=S3-0200127)

Based on these LSs, SA3 have updated the relevant parts of the IMS security specification TS 33.203 which will be presented to SA#15 for approval. Section 8 is devoted to the security functions which are required to be implemented on the UICC. In particular, it is specified how a R99/Rel-4 USIM may be used to provide the IMS security functions.

TS 33.203 does not contain any guidelines on how the relevant IMS identities should be derived when a USIM is used for IMS access. This is believed to be an issue for other WGs. However, SA3 have reviewed the CR on TS 23.228 on deriving IMS identities (S2-020912) and would like to make the following comments:

1. SA3 have reviewed the security implications of deriving the IMPI and Home Domain Name from the IMSI when a USIM is used for IMS access. SA3 did not identify any security problems with this approach, even if the derivation function is reversible. Furthermore, SA3 would like to indicate that a reversible function would allow the HSS to use the IMSI as the basis for indexing the correct record in the AuC without having to maintain a large look-up table.

2. SA3 have also reviewed the security implications of deriving the public identity (IMPU) from the IMSI when a R99/Rel-4 USIM is used for IMS access. SA2 are asked to clarify whether the derived IMPU would be listed in public directories or whether it would otherwise be made available outside the operator's domain (e.g. by included it in an INVITE message). If this is the case, then clearly the use of a reversible derivation function would increase the exposure of the customer's IMSI outside the operator's domain. Although the security of the system does not rely on the secrecy of the IMSI, SA3 consider it undesirable to make the IMSI publicly available in this way (i.e. listed in a public directory or included in the derived IMPU of an INVITE message). SA3 also note that SIP mechanisms are in place to enable additional implicitly registered public identities to be used (e.g. in an INVITE message) and these could be listed in a public directory.

Actions:

- SA2 should consider the above comments on the implications of deriving IMS identities from the IMSI when a USIM is used for IMS access. In particular, SA2 are asked to clarify whether the derived public identity (IMPU) or derived IMPI would have a chance to be made public.

- The involved groups should use the IMS security specifications in TS 33.203 to guide their specification work.

Technical Specification Group Services and System Aspects
Meeting #15, Cheju Island, Korea, 11-14 March 2002

TSGS#15(02)0116

3GPP TS 33.203 V2.0.0 (2002-03)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services (Release 5)

Keywords
Access security, IP Multimedia, SIP

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

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

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

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

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

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

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

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

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

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

[6] IETF RFC 2543bis-08 (2002) "SIP: Session Initiation Protocol".

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

[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".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

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

3.3 Abbreviations

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

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

4 Overview of the security architecture

In the PS domain, the service is not provided until a security association is established between the mobile equipment and the network. IMS is essentially an overlay to the PS-Domain and has a low dependency of the PS-domain. Consequently a separate security association is required between the multimedia client and the IMS before access is granted to multimedia services. The IMS Security Architecture is shown in the following figure.

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

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

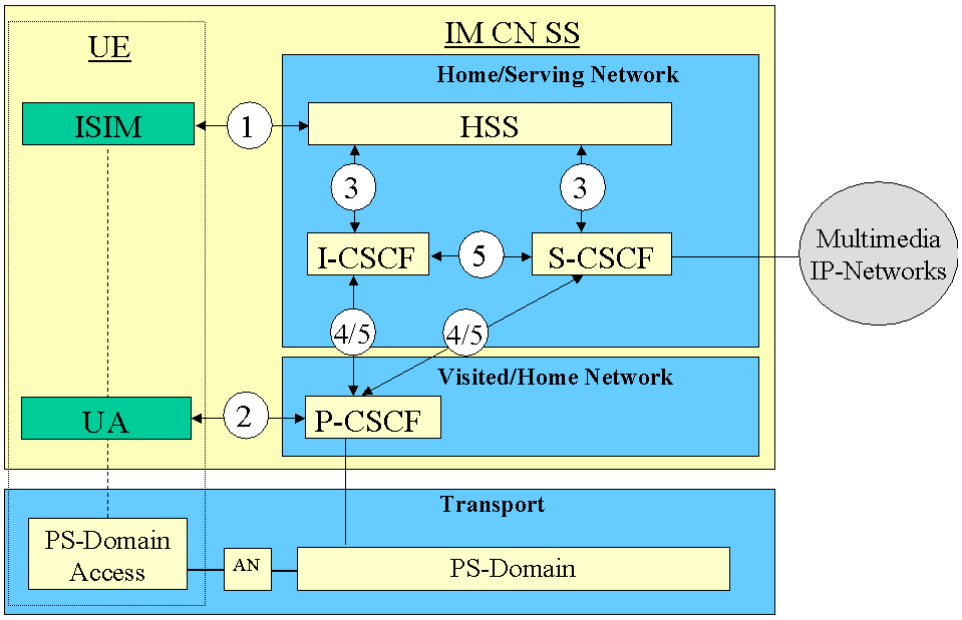


Figure 1: The IMS security architecture

There are five different security associations and different needs for security protection for IMS and they are numbered 1,2, 3, 4 and 5 in figure 1 where:

1. Provides mutual authentication. The HSS delegates the performance of subscriber authentication to the S-CSCF. However the HSS is responsible for generating keys and challenges. The long-term key in the ISIM and the HSS is associated with the IMPI. The subscriber will have one (network internal) user private identity (IMPI) and at least one external user public identity (IMPU).

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

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

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

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

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

Mutual authentication is required between the UE and the HN.

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

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

P-CSCF in the Visited Network

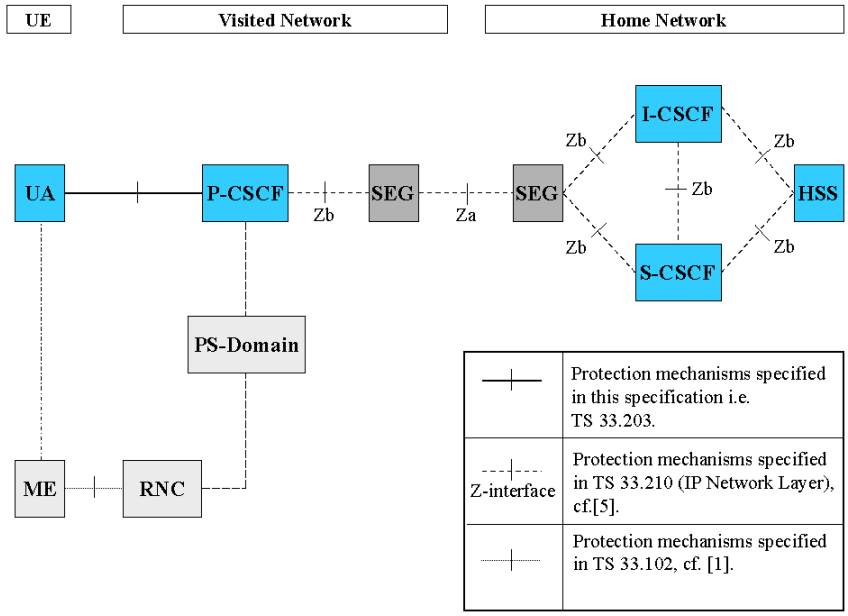


Figure 2: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the VN

P-CSCF in the Home Network

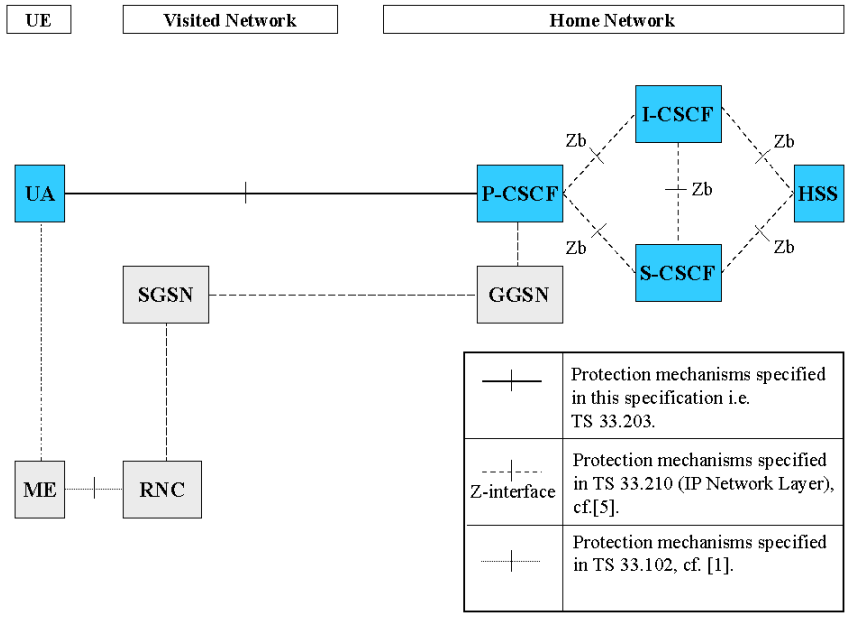


Figure 3: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the HN

The confidentiality and integrity protection for SIP-signaling is provided in a hop-by-hop fashion, cf. Figure 2 and Figure 3. The first hop i.e. between the UE and the P-CSCF is specified in this technical specification. The other hops, inter-domain and intra-domain are specified in TS 33.210 [5].

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

5 Security features

5.1 Secure access to IMS

5.1.1 Authentication of the subscriber and the network

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

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

All SIP-signaling will take place over the PS-domain in the user plane i.e. IP Multimedia Core Network Subsystem is essentially an overlay to the PS-domain. Hence the Visited Network will have control of all the subscribers in the PS-domain i.e. Visited Control (Authorization of bearer resources) since the Visited Network provides the subscriber with a transport service and its associated QoS.

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

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

The AKA-protocol is a secure protocol developed for UMTS and the same concept/principles will be reused for the IP Multimedia Core Network Subsystem, where it is called IMS AKA.

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

5.1.2 Re-Authentication of the subscriber

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

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

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

5.1.3 Confidentiality protection

Confidentiality mechanism need not be required for the first hop between the UE and the P-CSCF. It is recommended to offer encryption for SIP signalling at link layer i.e. between the UE and the RNC using the existing mechanisms as defined in [1].

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

5.1.4 Integrity protection

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

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

[Editor's note: At this stage both Annex B and Annex C provides with potential measures for integrity protection. One of these solutions will be the normative solution.]

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

5.2 Network topology hiding

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

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

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

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

6 Security mechanisms

6.1 Authentication and key agreement

The scheme for authentication and key agreement in the IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. Figure 1. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. [3]. The HSS and the ISIM share a long-term key associated with the IMPI.

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

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. The ISIM and the HSS keep track of counters SQN_{ISIM} and SQN_{HSS} respectively. The requirements on the handling of the counters and mechanisms for sequence number management are specified in [1]. The AMF field can be used in the same way as in [1].

Furthermore a security association is established between the UE and the P-CSCF. The subscriber may have several IMPUs associated with one IMPI. These may belong to the same or different service profiles. Only one SA shall be active between the UE and the P-CSCF. This single SA shall be updated when a new successful authentication of the subscriber has occurred, cf. section 7.3.3.

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

6.1.1 Authentication of an IM-subscriber

Before a user can get access to the IM services at least one IMPU needs to be registered and the IMPI authenticated in the IMS at application level. In order to get registered the UE sends a SIP REGISTER message towards the SIP registrar server i.e. the S-CSCF, cf. Figure 1, which will perform the authentication of the user.

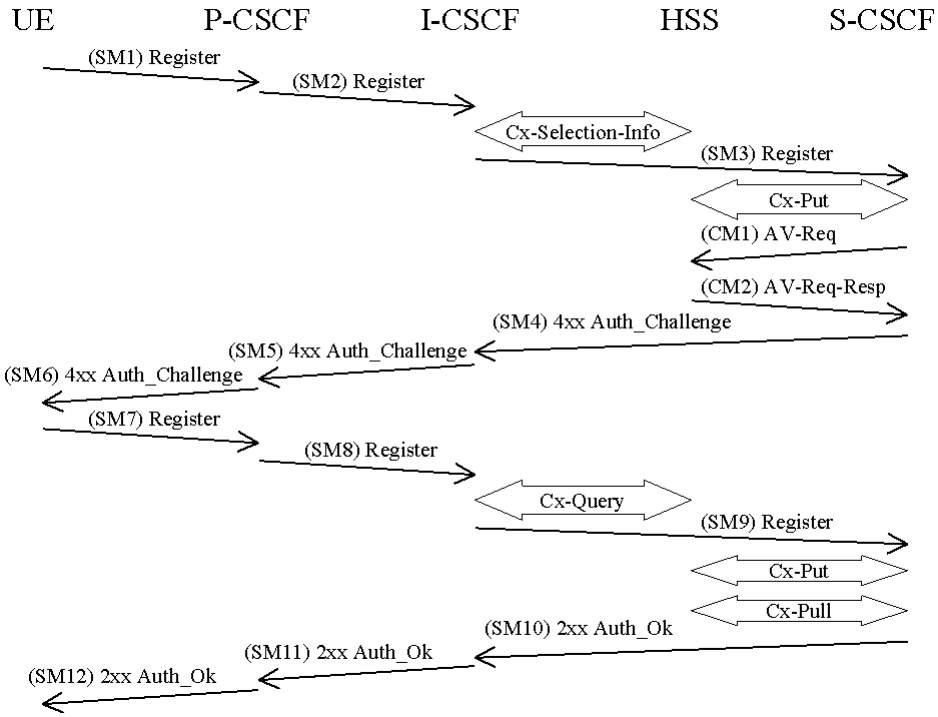


Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

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

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

SM1:
REGISTER(IMPI, IMPU)

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

In order to handle mobile terminated calls while the initial registration is in progress and not successfully completed the S-CSCF shall send a registration flag to the HSS. The registration flag shall be stored in the HSS together with the S-CSCF name. The aim of the registration flag is 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 HSS receives the information about this state (together with the S-CSCF name and the user identity) from the S-CSCF with which (re-) registration of the user is carried out only when a Cx-Put message is sent from the S-CSCF to the HSS. The registration flag shall be set to *initial registration pending* at the Cx-Put procedure after SM3 has been received by the S-CSCF.

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

[Editor's note: The maximum value of n i.e. nmax only if required by CN4.]

Upon receipt of a request from the S-CSCF, the HSS sends an ordered array of *n* authentication vectors to the S-CSCF. 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.

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

At this stage the HSS has performed a check that the IMPI and the IMPU belong to the same user.

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

If the HSS has no pre-computed AVs the HSS creates the needed AVs on demand for that user and sends it to the S-CSCF in CM2.

CM2:
Cx-AV-Req-Resp(IMPI, n,$RAND_1$||$AUTN_1$||$XRES_1$||CK_1||IK_1,….,$RAND_n$||$AUTN_n$||$XRES_n$||CK_n||IK_n)

The 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 and the integrity key IK and optionally the cipher key CK.

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

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

[Editor's note: The use of KSI i.e. Key Set Identifier for IMS is FFS.]

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

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

Upon receiving the challenge, SM6, the UE takes the AUTN, which includes a MAC and the SQN. The UE calculates the XMAC and checks that XMAC=MAC and that the SQN is in the correct range as in [1]. If both these checks are successful the UE calculates the response, RES, puts it into the Authorization header and sends it back to the registrar in SM7. It should be noted that the UE at this stage also computes the session keys CK and IK.

SM7:
REGISTER(IMPI, RES)

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

Upon receiving the response, RES, the S-CSCF retrieves the active XRES for that user and checks if XRES=RES. If the check is successful then the user has been authenticated and the IMPU is registered in the S-CSCF. To ensure that the S-CSCF is able to take the decision whether a subsequent registration shall trigger a new authentication and to be able to check that all INVITE messages will be sent to/from an authorized subscriber it shall be possible to implicitly register IMPU(s). The implicitly registered IMPU(s) all belong to the same Service Profile. All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

At this stage the S-CSCF shall send in the Cx-Put after receiving SM9 an update of the registration-flag. If the authentication of the subscriber is successful the registration flag shall take the value *registered*. When the authentication is unsuccessful the registration flag shall be set to *unregistered*.

When a subscriber 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. The UE initiated re-registration opens up a potential denial-of-service attack in the sense that an attacker could re-register a subscriber in an unprotected message and respond with the wrong RES and the HN could then de-register the subscriber. It shall be defined by the policy of the operator when successfully registered IMPU(s) are to be de-registered.

The authenticated re-registration looks the same as the initial registration except that CM1 and CM2 can be omitted as long as the S-CSCF has valid AV(s). The P-CSCF shall forward the unprotected REGISTER to S-CSCF with an indication that the existing SA is not applied. As a consequence, the S-CSCF shall trigger a new authentication procedure. At a re-registration the registration flag has already the value *registered.* The policy of the home provider states whether the flag shall be changed at a re-registration based on two scenarios.

- If the re-registration is successful, the registration status keeps registered and timer for next registration is refreshed in the S-CSCF.
- The IMS subscriber remains registered after unsuccessful re-registration until timer set for next re-registration is expired. Before that the registration flag is kept in the HSS to the value *registered* even if the authentication was unsuccessful. The S-CSCF shall not remove the data about subscriber's registration and the P-CSCF shall keep the existing SA.

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

6.1.2 Authentication failures

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

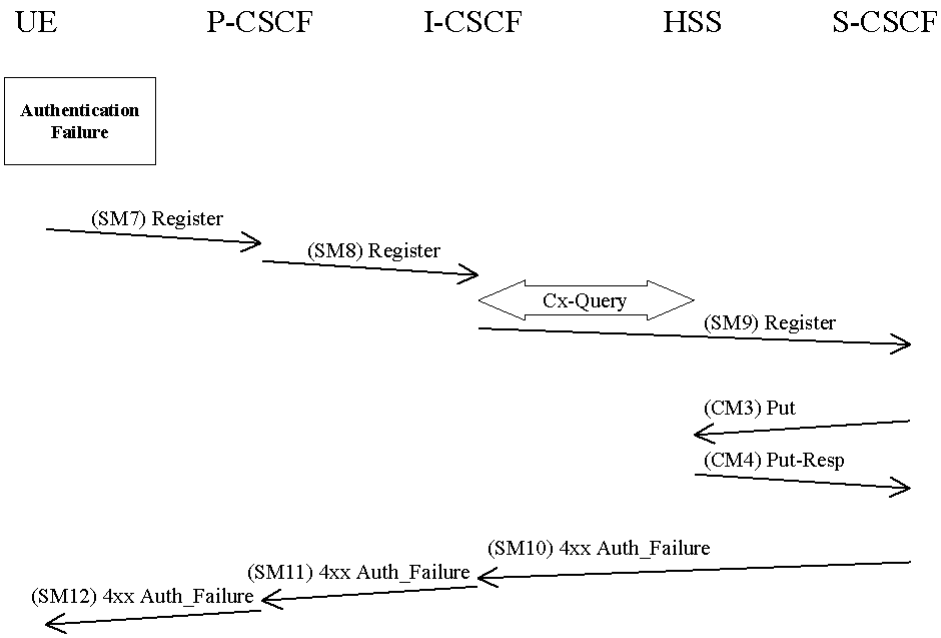
6.1.2.1 User authentication failure

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

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

6.1.2.2 Network authentication failure

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



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

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

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

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

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

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

SM10:
SIP/2.0 4xx Auth_Failure

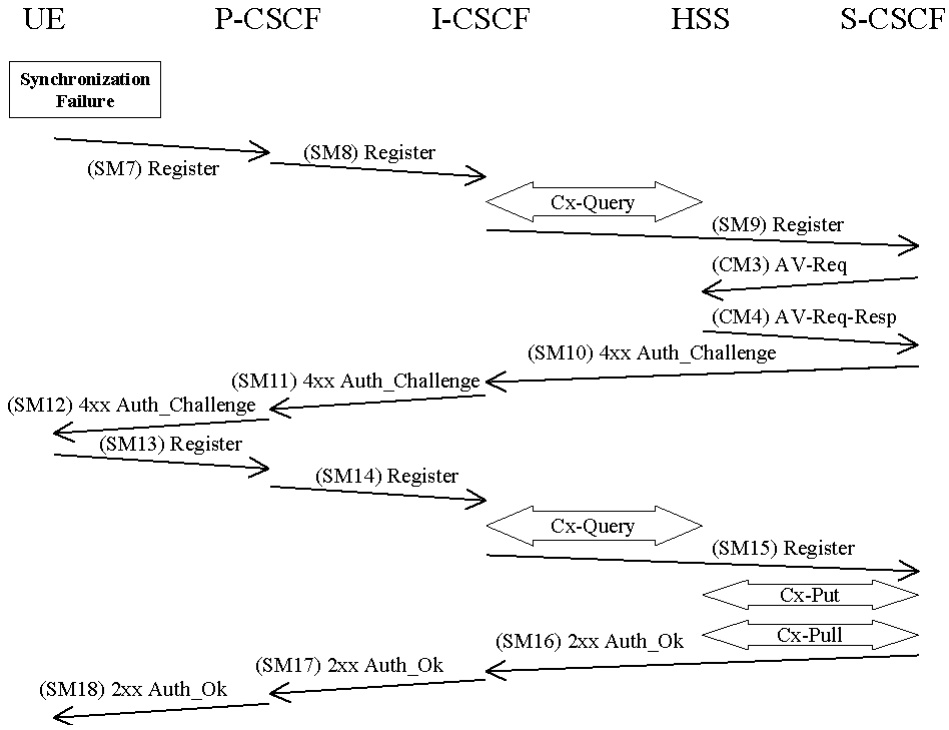
Upon receiving SM10 the I-CSCF shall clear any registration information related to the IMPI.

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

6.1.3 Synchronization failure

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

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



The flow equals the flow in 6.1.1 up to SM6. When the UE receives SM6 it detects that the SQN is out of range and sends a synchronization failure back to the S-CSCF in SM7.

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

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

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

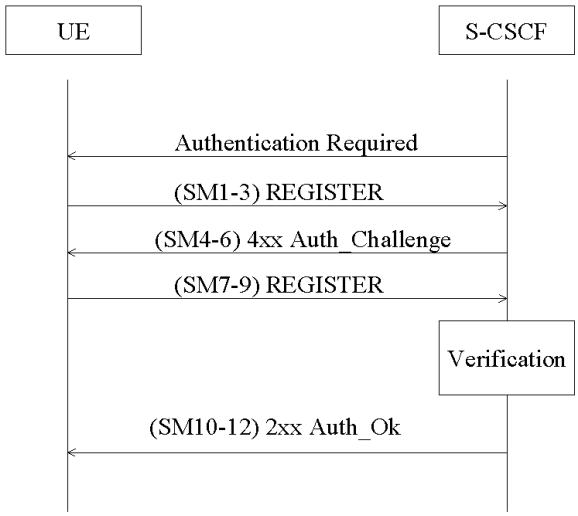
The HSS checks the AUTS as in section 6.3.5 in [1]. If the check is successful and potentially after updating the SQN the HSS creates and sends new AVs to the S-CSCF in CM4.

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

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

6.1.4 Network Initiated authentications

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



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

6.2 Confidentiality mechanisms

No confidentiality mechanism is provided in this version of the specification, cf. 5.1.3.

6.3 Integrity mechanisms

[Editor's note: At this stage both Annex B and Annex C provides with potential measures for integrity protection. One of these solutions will be the normative solution.]

6.4 Hiding mechanisms

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

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

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

- use of a key identifier for the support of multiple encryption secret keys

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

]

7 Security association set-up procedure

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

7.1 Security association parameters

For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys provided by IMS AKA, on certain protection methods (e.g. an integrity protection method) and a set of parameters specific to a protection method, e.g. the cryptographic algorithm to be used. The parameters negotiated are typically part of the security association to be used for a protection method.

The security mode setup shall support the negotiation of different protection mechanisms. It shall be able to negotiate or exchange the SA parameters required for these different protection mechanisms. Although the supported protection mechanisms could be quite different, there is a common set of parameters that have to be negotiated for each of them. This set of parameters includes:

- Authentication (integrity) algorithm, and optionally encryption algorithm;
- SA_ID that is used to uniquely identify the SA at the receiving side;
- Key length: the length of encryption and authentication (integrity) keys is 128 bits.

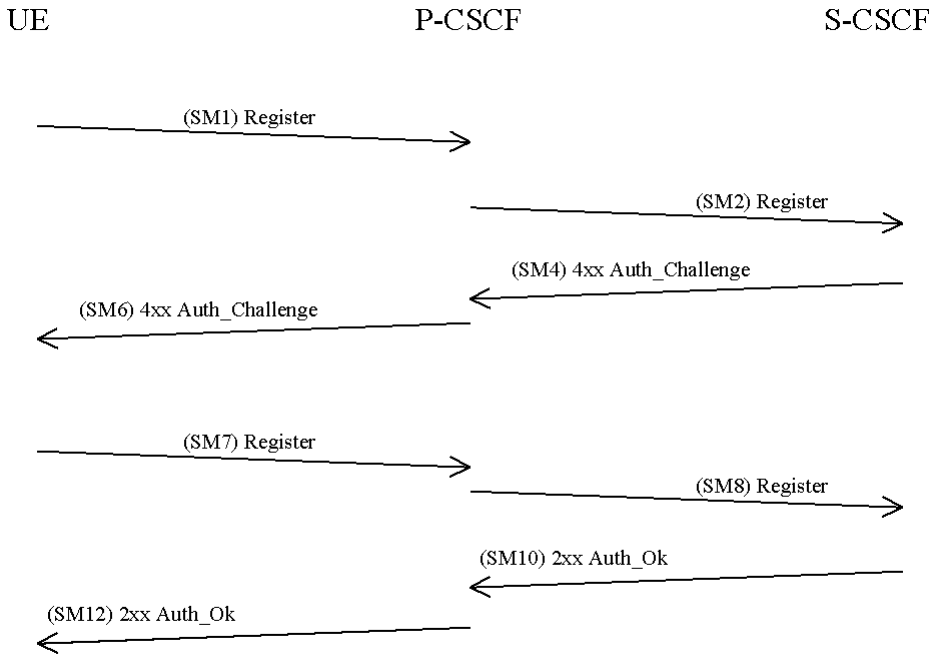
Parameters specifically related to certain protection methods are kept in the annexes describing the protection methods.

The SA between the UE and the P-CSCF will have a limited lifetime. The lifetime timer shall be the same as the registration timer, which is defined per contact address. When the UE registers the registration timer will be negotiated between the UE, the P-CSCF and the S-CSCF. The S-CSCF will be able to accept, decrease or increase the proposed expiration time from the UE and the final value is sent in the response to the UE. The expiry time in the UE will be shorter than the expiry time in the S-CSCF, such that the UE is able to re-register. For each new successful authentication the SA shall be updated. The S-CSCF shall align the expiration of subsequent registrations with any existing registration timer. The SA is deleted if the registration timers expires in the P-CSCF or in the S-CSCF.

[Editors Note: The support of different mechanisms is FFS.]

7.2 Set-up of security associations (successful case)

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



The UE sends a Register message towards the S-CSCF to register the location of the UE and to set-up the security mode. This has been described in 6.1. In order to start security mode setup the UE shall include a *Security-setup:* line in this message, including the protection method, the proposed set of integrity algorithms, the proposed set of confidentiality algorithms (optional), the SA_ID and an optional *info* field. The *info* field is reserved for method specific use, so any method supported by the security mode set-up must specify whether and how to use the *info* field. The SA_ID_U shall be chosen so that it uniquely identifies the (unidirectional) inbound SA at the UE side.

Elements in [...] are optional.

> SM1:
> REGISTER(Security-setup = *integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info]),* IMPI, IMPU*)*

The P-CSCF shall choose exactly one of the proposed mechanisms respectively and exactly one of the proposed algorithms respectively based on the policies that applies and send the selected mechanisms and algorithms to the UE in SM6.

The SA_ID_P shall be chosen in such a way that it uniquely identifies the (unidirectional) inbound SA at the P-CSCF side, within the P-CSCF.

[Editors Note: It is FFS if the HN shall take part in the negotiation of algorithms.]

> SM6:
> 4xx Auth_Challenge(Security-setup = *integrity mechanism, [confidentiality mechanism], integrity algorithm, [confidentiality algorithm], SA_ID_P, [info],* IMPI*)*

The UE shall in SM7 start the integrity protection – and optionally the confidentiality protection – of the whole SIP-message by setting up security associations according to mechanisms and the parameters negotiated in SM1 and SM6, and applying the corresponding protection to the SIP-message. Furthermore the Security-setup: line sent in SM1 shall be included:

SM7:
REGISTER(Security-setup = *integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info],* IMPI)

After receiving SM7 from the UE, the P-CSCF shall compare the Security-Setup line of this message with the Security-Setup line received in SM1. The P-CSCF shall in SM8 include information to the S-CSCF that the received message from the UE was integrity protected. The P-CSCF shall add this information to all subsequent 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.

[Editors Note: It is FFS if the HN shall take part in the negotiation process.]

7.3 Error cases in the set-up of security associations

Whenever an expected message is not received after a time-out the receiving entity considers the registration to have failed.

[Editor's note: Clarify, how SIP registration handles the inconsistent state that is created by a lost SM12 message]

7.3.1 Error cases related to IMS AKA

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

[Editors Note: It is FFS if this is appropriate taking DoS attacks into account.]

7.3.1.1 Integrity check failure in the P-CSCF

In this case, SM7 containing a potentially wrong RES fails integrity check at P-CSCF (IK derived from RAND at UE is wrong as well). The authentication of the user fails in the network due an incorrect RES. The P-CSCF shall discard SM7 and the registration and the authentication procedures shall be aborted (see also clause 6.1.2.1).

7.3.1.2 Network authentication failure

If the UE is not able to successfully authenticate the network, the UE is not able to create the key IK and therefore the SA with the P-CSCF, such that it is not possible to send SM7 in a protected way. Since the P-CSCF already expects SIP messages from the UE to be protected, and is not already aware of any errors, the P-CSCF shall accept such REGISTER messages indicating network authentication failure in the clear.

So the UE sends a new register message SM7, indicating a network authentication failure, to the P-CSCF, without protection. SM7 should not contain the security-setup line of the first 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 sends a new register message SM7 to the P-CSCF in the clear, indicating the synchronization failure. SM7 should not contain the Security-Setup line of the first message, and the P-CSCF shall keep the security-setup state created after receiving SM1 from the UE.

7.3.2 Error cases related to the Security-Set-up

7.3.2.1 Unacceptable proposal set

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

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

SM2:
REGISTER(Security-setup = *integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info],* Failure = *NoCommonIntegrityAlgorithm,* IMPI, IMPU)

[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]

7.3.2.2 Unacceptable algorithm choice

If the P-CSCF sends in the security-setup line of SM6 an algorithm that is not acceptable for the UE (i.e. has not been proposed), the UE shall not continue to create a security association with the P-CSCF and shall terminate the registration procedure.

7.3.2.3 Failed consistency check of Security-Set-up lines

This is the case if the Security-Setup line in SM7 from the UE to the P-CSCF cannot be verified, so the Security-Setup line of the unprotected SM1 and the Security-Setup line of the protected SM7 do not match. The P-CSCF shall respond to the UE by sending a 4xx Unacceptable_Proposal message in SM12. The P-CSCF therefore shall modify the message SM8 such that the S-CSCF sends a 4xx Unacceptable_Proposal message back to the UE in SM10 and SM12 and the registration process is finished.

SM8:
REGISTER(Security-setup = *integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info],* Failure = *NoCommonIntegrityAlgorithm,* IMPI)

[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]

7.3.3 Authenticated re-registration

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

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

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

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

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

Before re-registration begins the following SAs exist:

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

The re-registration then is as follows:

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

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

2) The P-CSCF waits for the response SM4 from the S-CSCF and then sends SM6 to the UE, using SA2. As in the case of a new registration, the parameters selected for the new security associations are included. The P-CSCF then creates two new security associations, in parallel to the existing ones, in its database:
   - SA11 from UE to P-CSCF;
   - SA12 from P-CSCF to UE.
3) If SM6 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends SM7 to the P-CSCF. As in the case of a new registration, the authentication response and the list of parameters repeated from message 1 are included. SM7 is protected with the new SA11.
4) The P-CSCF waits for the response SM10 from the S-CSCF and then sends SM12 to the UE, using the new SA 12.
5) After the reception of SM12 by the UE, the re-registration is complete.

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

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

7.3.3.2 Error cases related to authenticated re-registration

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

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

7.3.3.3 Error cases related to IMS AKA

User authentication failure

The S-CSCF will send a 4xx Auth_Failure message SM10, which will pass through the already established SA to the UE as SM12. Afterwards, both, the UE and the P-CSCF delete the new SAs.

Network authentication failure

If the UE is not able to successfully authenticate the network, it does not establish a new SA. The UE sends a REGISTER message SM7 indicating a network authentication failure to the P-CSCF, using the already established SA. The P-CSCF deletes the new SAs after receiving this message.

Synchronisation failure

If the UE notices a synchronisation failure it does not establish a new SA. The UE sends a message SM7, indicating the synchronisation failure, to the P-CSCF, using the already established SA. The P-CSCF deletes the new SA after receiving this message.

7.3.3.4 Error cases related to the Security-Setup

Unacceptable proposal set

The message SM6 shall respond to the first REGISTER message SM1 with a 4xx Unacceptable_Proposal, using the already established SA. Neither side establishes a new SA.

The P-CSCF therefore shall modify the message SM2 such that the S-CSCF sends the 4xx Unacceptable_Proposal message back to the UE in SM4and SM6 and the registration process is finished.

SM2:
REGISTER(Security-setup = *integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info],* Failure = *NoCommonIntegrityAlgorithm,* IMPI)

[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]

Failed consistency check of Security-Set-up lines

This is the case if the Security-Setup line in SM7 from the UE to the P-CSCF cannot be verified, so the Security-Setup line of the unprotected SM1 and the Security-Setup line of the protected SM7 do not match. In this case the P-CSCF shall respond to the UE by sending a 4xx Unacceptable_Proposal message in SM12 using the already established SA. Both sides delete the new SAs.

The P-CSCF therefore shall modify the message SM8 such that the S-CSCF sends the 4xx Unacceptable_Proposal message back to the UE in SM10 and SM12 and the registration process is finished.

SM8:
REGISTER(Security-setup = *integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info],* Failure = *NoCommonIntegrityAlgorithm),* IMPI)

[Editors Note: It is FFS how the exact mechanism shall be for the Unacceptable proposal set case. The editor believes that the S-CSCF is the registrar and hence the P-CSCF should only be able to modify the headers and not send back responses. The failure response should be sent by the S-CSCF. This however has not been agreed.]

8 ISIM

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

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

- Use of a distinct ISIM application on a UICC which does not share security functions with the USIM;
- Use of a distinct ISIM application on a UICC which does share security functions with the USIM;
- Use of a R99/Rel-4 USIM application on a UICC.

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

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

8.1 Requirements on the ISIM application

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

The ISIM shall include:

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

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

[Editors Note: It is FFS if a KSI, data equivalent to the START parameter, AMF related data, storage for CK and IK is needed or not.]

[Editors Note: It is FFS if an IMS subscriber shall be de-registered at power off]

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 (informative): Mechanisms for IPSec based solution

[Editors Note: If the IPSec solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

B.1 [6.2] Confidentiality mechanisms

IPsec ESP may optionally be implemented for providing confidentiality of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. If ESP confidentiality is used, it shall be applied in transport mode between UE and P-CSCF. If ESP confidentiality is provided, it is always provided in addition to ESP integrity protection.

The SAs that are required for ESP shall be derived from the 128-bit integrity key CK_{IM} generated through IMS AKA, as specified in chapter 6.1.

If confidentiality is required, for each direction, there is one ESP SA for both confidentiality and integrity that shall be used between the UE and the P-CSCF. The encryption transform is identical for the two SAs in either direction. The encryption key for the SA inbound from the P-CSCF is CK.

The encryption key for the SA inbound from the P-CSCF is CK_{IM_in}. The encryption key for the SA outbound from the P-CSCF is $CK_{IM\_out.}$

The encryption keys are derived as $CK_{IM\_in} = h1(CK_{IM})$ and $CK_{IM\_out} = h2(CK_{IM})$ using suitable key derivation functions h1 and h2.

The encryption key derivation on the user side is done in the ISIM. The encryption key derivation on the network side is done in the P-CSCF.

The method to set up ESP security associations during the SIP registration procedure is specified in chapter 7.

B.2 [6.3] Integrity mechanisms

IPsec ESP shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the IP level. ESP integrity shall be applied in transport mode between UE and P-CSCF.

The SAs that are required for ESP shall be derived from the 128-bit integrity key IK generated through IMS AKA, as specified in chapter 6.1. The transform used for the ESP SA shall be negotiated as specified in chapter 7. ESP shall use two unidirectional SAs between the UE and the P-CSCF, one in each direction. The integrity algorithm is identical for both SAs.

The integrity key for the SA inbound from the P-CSCF is IK_{IM_in}. The integrity key for the SA outbound from the P-CSCF is $IK_{IM\_out.}$

The integrity keys are derived as $IK_{IM\_in} = h1(IK_{IM})$ and $IK_{IM\_out} = h2(IK_{IM})$ using suitable key derivation functions h1 and h2. (They may be the same as those in section 6.2.)

The integrity key derivation on the user side is done in the ISIM. The integrity key derivation on the network side is done in the P-CSCF.

The method to set up ESP security associations during the SIP registration procedure is specified in chapter 7.

Annex C (informative): Mechanisms for SIP-level solution

[Editors Note: If the SIP-level solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

C.1 [6.2] Confidentiality mechanisms

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

C.2 [6.3] Integrity mechanisms

[Editors note: There seems to be an unexpected shortcoming in the way SIP provides integrity protection on messages between UE and Proxies. In current SIP, HTTP Digest can be used to partially integrity protect the messages originated by an UE. However, SIP fails to provide integrity for Proxy to UE communication, i.e. for terminating INVITEs, for example. Proxies are not able to add Authorization headers on these messages, thus leaving the messages unprotected.

For the reason above, the headers and field names used in this section may not be final. However, the found inconsistency will probably make it easier for 3GPP to discuss about new SIP level integrity protection schemes with IETF.]

HTTP Digest shall provide integrity protection of SIP signalling between the UE and the P-CSCF, protecting all SIP signalling messages at the SIP level.

C.2.1 [6.3.1] Security Association Setup

The SA that is required for Digest integrity protection shall use the 128-bit integrity key IK generated through IMS AKA, as specified in section 6.1. The integrity algorithm and key are identical for integrity protection applied to messages travelling in either direction. Negotiation of the integrity algorithm to use occurs in the following way: The UE communicates the set of integrity algorithms that it supports to the P-CSCF through the Security-setup header field of the REGISTER message, as described in section 7.2. The P-CSCF selects an algorithm to use from the set of algorithm capabilities common to both the UE and the P-CSCF. The P-CSCF indicates the algorithm to use in the "algorithm" directive of the Digest challenge that is subsequently issued to the UE.

C.2.2 [6.3.2] Scope of Integrity Protection

Digest supports integrity protection of the SIP message body (not the headers) when the "qop-options" directive within the Digest challenge is set to the value "auth-int".

Digest supports integrity protection of the SIP message body plus a named list of headers when the "qop-options" directive is set to the value "auth-hdr-int".

Digest supports integrity protection of the entire SIP message when the "qop-options" directive within the Digest challenge is set to the value "auth-extd-int".

To provide for protection of the entire SIP message, the P-CSCF shall issue a Digest challenge to the UE specifying the value "auth-extd-int" for the "qop-options" directive.

C.2.3 [6.3.3] Computation of Integrity Protection Credential

The message 'digest', or message authentication code, is conveyed in the "response" directive of the Digest response. The rules for computing "response" are as described in [1] with the following consideration: if the UE receives a Digest

challenge with “realm” directive including a 3GPP specific key word (e.g. “ik.”), then the UE substitutes IK for the “password” component of A1 when computing “response=” in the Digest response. The UE saves the content of the whole realm directive from the Proxy-Authentication header to be used as a key identifier for subsequent messages. At this stage UE can not be sure whether the proxy identified in the realm really knows the IK, however the Proxy-Authentication-Info header will be used for final verification.

The UE sets the “username” component of A1 to some user identifier, e.g. the IMPI. When sending messages to the UE that are to be integrity protected, the P-CSCF applies the same rules when computing “response”. Within these terminating messages, the rules for the content of ‘realm’ and ‘username’ parameters are opposite than for originating messages: the “realm” directive will include the same user identifier as above, e.g. the IMPI, and the “username” the identifier of the P-CSCF (including the 3GPP specific key word, e.g. “ik.”). In this manner, the whole SIP message is always protected.

Note that terminating messages arriving to the P-CSCF from the home network will probably not include IMPI. For these messages, P-CSCF must use some other identifier (e.g. Request-URI) to find the IMPI and the IK needed for the integrity protection.

C.2.4 [6.3.4] Anti-Replay Protection

The Digest framework specifies that a server-initiated nonce is to be used by the client as a random number input to the production of the message digest. This nonce, along with a counter (‘nonce-count’) that is incremented by the client when sending each SIP request that is to be protected, facilitate anti-replay protection. The anti-replay protection feature of the integrity protection mechanism is as described in [12] with the following considerations. Per [12], the role of the server is to issue the nonce and to detect replays (through validation of ‘nonce-count’), and the client must increment ‘nonce-count’ when computing the digest for each new SIP request that is to be integrity protected. In the one-hop environment that exists for the UE and the P-CSCF in the IMS, both the UE and the P-CSCF may fill either the client or server role in particular operational situations. When the UE sends an INVITE or other request towards the P-CSCF, the UE is the client and the P-CSCF is the server. When the P-CSCF sends (or re-submits) an INVITE towards the UE, the P-CSCF acts as the client and the UE acts as the server. The implications of supporting the Digest client-server model, then, are that both the UE and the P-CSCF must: 1) be able to issue Digest challenges, which includes issuing nonces; and 2) maintain its own counter for the ‘nonce-count’ directive for use when operating in the client role.

New nonce values are communicated by the server to the client in two ways: 1) through the ‘nonce’ directive that is an obligatory part of the Digest challenge; and 2) through the ‘nextnonce’ directive that is an obligatory part of the Digest authentication of SIP responses (e.g., Authentication-Info header). Nonce values themselves are selected entirely by the server implementation – counter-based, clock- or other random number-based, and hybrid implementations are all possible. It is also a matter of server implementation how frequently new nonces are to be issued. To minimize the number of “stale” authentication attempts (generation of credentials by the client using an older nonce), the server should maintain a list of reasonable size of previously issued nonce values.

Expected behaviour of the UE and P-CSCF in relation to anti-replay protection is illustrated in the example information flow that follows in this section.

C.2.5 [6.3.5] Mitigation of ‘Reflection Attacks’

When either the UE or P-CSCF receives a SIP request (i.e. is acting as Digest server), it expects the sending entity (acting as client) to use in the computation of the message digest a nonce that it (the server) has previously issued. If an unrecognized nonce appears in the Digest response, the receiving entity will deem the message to have failed the integrity check. In this way the Digest framework mitigates “reflection attacks” (attacks in which a Man-in-the-Middle reflects a genuine message from an entity back to its sender). It is possible that in the course of generating random nonces the UE and P-CSCF, while operating in the server role, happen to issue identical nonces for use; by making the nonces of sufficient length, the chance of such an occurrence is minimized.

C.2.6 [6.3.6] Digest Operation and Syntax in SIP

In the 3GPP IMS, then, normal operation of the Digest challenge-response mechanism for integrity protection is as follows:

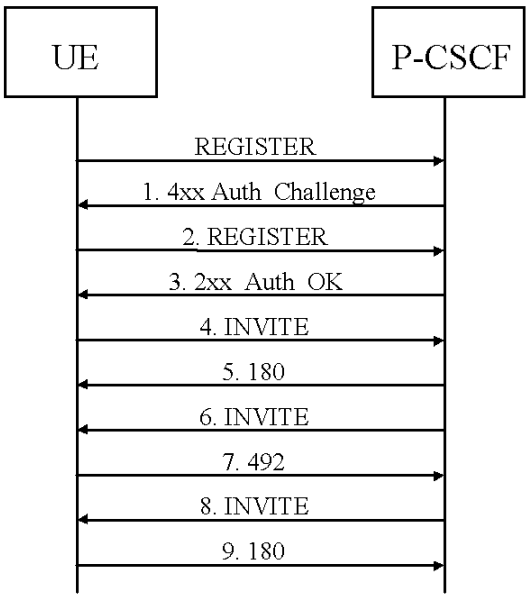
The Digest challenge-related directives are carried in the WWW-Authenticate, Proxy-Authenticate or UAS-Authenticate header fields. The P-CSCF adds a Proxy-Authenticate header field to the 4xx Auth_Challenge that is sent

by the S-CSCF (SIP registrar) toward the UE; the Proxy-Authenticate contains the Digest challenge that has been constructed by the P-CSCF.

The Digest response-related directives are carried in the Authorization, Proxy-Authorization or UAS-Authorization header fields, depending upon which header field carried the corresponding Digest challenge. These directives contain the credentials for the message integrity check. In the IMS context, the UE responds to the initial Digest challenge by adding a Proxy-Authorization header field to the REGISTER toward the S-CSCF (registrar). The UE pre-emptively adds a Proxy-Authorization header field to all subsequent UE-initiated SIP requests. The P-CSCF adds the Proxy-Authentication-Info header to all SIP responses. **The P-CSCF adds an UAS-Authorization header field to all SIP requests sent toward the UE. Finally, the UE adds the UAS-Authentication-Info header to all SIP responses.**

C.2.7 [6.3.7] Example Information Flow

The simplified message flow shown below illustrates the relevant header fields and contents for the SIP-level integrity protection mechanism. Please note that the message flow contains three cases: a registration (1-3), and two SIP sessions: one UE initiated (4-5) and one UE terminated (6-9).



1. **4xx response – this carries both the IMS AKA challenge (from the registrar) and the Digest challenge for integrity protection (from the P-CSCF):**

   SIP/2.0 4xx Auth_Challenge

   WWW-Authenticate: <RAND AUTN>

   Proxy-Authenticate: Digest realm=ik.p-cscf@operator2.com nonce=<P-nonce1> algorithm=MD5 qop=auth-extd-int

2. **Integrity protection is turned on with the next REGISTER – the integrity credentials are placed in the Digest response:**

   REGISTER sip: ... SIP/2.0

   Authorization: <RES>

   Proxy-Authorization: Digest username=IMPI, realm= ik.p-cscf@operator2.com, nonce=<P-nonce1>, uri=<SIP-URI>, response=<message-digest>, cnonce=<value>, nc=1, qop=auth-extd-int

3. **The 2xx response is also integrity protected – the P-CSCF adds the Proxy-Authentication-Info header to carry the message digest:**

   SIP/2.0 2xx Auth_Ok

Proxy-Authentication-Info: Digest realm=ik.p-cscf@operator2.com, nextnonce=<P-nonce2>, qop=auth-extd-int, rspauth=<message-digest>, nc=1, cnonce=<value>

4. **A subsequent INVITE request must also be integrity protected – the UE pre-emptively adds the Proxy-Authorization header:**

   INVITE sip: … SIP/2.0

   Proxy-Authorization: Digest username=IMPI, realm= ik.p-cscf@operator2.com, nonce=<P-nonce2>, uri=<SIP-URI>, response=<message-digest>, cnonce=<value>, nc=1, qop=auth-extd-int

NOTE: The client (UE) may re-use the previously issued nonce (i.e. set "nonce" to <P-nonce1> and "nc" to 2), but the Digest specification recommends against this. If the 2xx message containing 'nextnonce' were lost and not received by the UE, the UE would then use <P-nonce1> in the computation of the credential.

1. **The 180 is integrity protected in the same fashion was the 2xx response (message #3):**

   SIP/2.0 180 Ringing

   Proxy-Authentication-Info: Digest realm=ik.p-cscf@operator2.com, nextnonce=<P-nonce3>, qop=auth-extd-int, rspauth=<message-digest>, nc=1, cnonce=<value>

2. **An incoming INVITE must also be integrity protected – the first terminating SIP request, however, must be sent without the integrity credential (this permits the UE to issue a Digest challenge containing its own server-provided nonce).**

3. **The UE issues a 492 response containing a Digest challenge:**

   SIP/2.0 492 Proxies Unauthorized

   UAS-Authenticate: Digest realm=IMPI, nonce=<UE-nonce1>, algorithm=MD5, qop=auth-extd-int, target=ik.p-cscf@operator2.com

4. **The P-CSCF adds the UAS-Authorization header, which has similar syntax to Proxy-Authorization:**

   INVITE sip: … SIP/2.0

   UAS-Authorization: Digest username=ik.p-cscf@operator2.com, realm=IMPI, nonce=<UE-nonce1>, uri=<SIP-URI>, response=<message-digest>, cnonce=<value>, nc=1, qop=auth-extd-int, responder= ik.p-cscf@operator2.com

5. **The UE protects the 180 response by adding UAS-Authentication-Info:**

   SIP/2.0 180 Ringing

   UAS-Authentication-Info: Digest realm=ik.p-cscf@operator2.com, nextnonce=<UE-nonce2>, qop=auth-extd-int, rspauth=<message-digest>, nc=1, cnonce=<value>

[Editors Note: A description of the security mode setup headers shall be included in this Annex. Furthermore the message flows need to be enhanced.]

[Editors Note: It is FFS how to optimize the profiling of HTTP Digest such that the extra roundtrip can be avoided for the first terminating INVITE. It is also FFS the exact profiling of the nonces]

[Editors note: There might be a need for IMS specific rules on how the error situations are handled with HTTP Digest. HTTP Digest includes a mechanism for a server/proxy to communicate some information about the status of the username, password or nonce to the client. If a server/proxy adds a 'stale=true' parameter in an authentication challenge, the client will try using the same password (i.e. integrity key) with the delivered new nonce value. If the 'stale=false' or anything else, or if it is missing, the client must ask for a new password from the end-user. In IMS, stale values can be used to deal with different error situations related to the key update. For example, P-CSCF could ask the client to perform re-registration if it sent a "stale=false" parameter. The potential error situations are for further study.]

[Editors note: it is not so nice to test or try which SA is correct if the P-CSCF has two under certain situations. A better approach might be to add a counter in e.g. realm that not only indicates that IK should be used but also which IK. This could be e.g. a 2 bit field or similar. This is FFS]

Annex D (informative): Set-up procedures for IPSec based solution

[Editors Note: If the IPSec solution is finally chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.]

This section is based on section 7 and provides additional specification for the support of IPsec ESP.

D.1 Security association parameters

The SA parameters, identifiers and attributes that shall be negotiated between UE and P-CSCF, are

- ESP transform identifier
- Authentication (integrity) algorithm
- SPI

Further parameters:

- Life type: the life type is always seconds
- SA duration: the SA duration has a fixed length of 2^{32}-1.
- Key length: the length of encryption and authentication (integrity) keys is 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. IP addresses and ports. Both sides have to use the same policy here, but since the required selectors will be known from the SIP messages, there is no need to negotiate them. However, it is critical to keep the source IP address and source port number, the selector pair unique in P-CSCF. The P-CSCF must reject any REGISTER message sent from a valid SA's selector pair corresponding to a different IMPI than the one that is bound to this selector pair. The only parameter that shall be negotiated, is a fixed port for specific unprotected SIP messages at the P-CSCF:

1. For the inbound SA at the P-CSCF (outbound for the UE) the P-CSCF shall use a fixed port. This may be port 5060 as the standard SIP port, or any other fixed port where the server accepts SIP messages from the UE. In addition, another port for specific unprotected SIP messages from the UE to the server is fixed.
   For the outbound SA at the P-CSCF (inbound for the UE) ANY port number shall be allowed at the P-CSCF.
2. On the UE side, the SIP UAs shall use the same port for both sending and receiving SIP signalling to the P-CSCF.
3. If there are multiple SIP UAs belonging to different ISIMs in one UE they shall use different SAs and bind them to different ports on the UE side.
4. The UE may send only the following messages to the fixed port for unprotected messages:
   - initial REGISTER message;
   - REGISTER message with network authentication failure indication;
   - REGISTER message with synchronization failure indication.

   All other messages incoming on this port must be discarded by the SIP application on the P-CSCF.

[Editors' note: It is ffs whether case 3 can actually occur.]

For each incoming message the SIP application must verify that the correct inbound SA associated with the public ID (IMPU) given in the SIP message has been used. This shall be done by verifying that the correct source IP address and source port bound to the public ID (IMPU) of the SIP message have been used for sending the message.

D.2 Security mode setup for IPsec ESP

This section describes how the security mode setup described in chapter 7 shall be used for negotiating ESP as protection mechanism and setting up the parameters required by ESP.

D.2.1 General procedures specific to the ESP protection mechanism

The integrity and encryption mechanisms both have the value "esp". The fields SA_ID_U and SA_ID_P carry the SPI values to be exchanged, to identify the ESP SAs.

The P-CSCF shall use an unprotected port to be able to receive specific unprotected messages. This unprotected port has to be communicated to the UE, by using the *info* field of message SM6. This unprotected port is required, when an IPsec SA is already in place at the P-CSCF, but the UE due to any reason is not able to use this SA. In this case, the UE shall send error messages or a new REGISTER message in the clear to the P-CSCF port received in the *info* field within SM6. Otherwise at the P-CSCF side, ESP would simply drop all IP packets from the UE that fail the integrity check.

The error messages that shall be sent in the clear from the UE to the P-CSCF are these for network authentication failures (sections 7.3.1.2) and synchronization failures (section 7.3.1.3).

D.2.2 Handling of user authentication failure

(This extends the content of chapter 7.3.1.1 and 7.3.3.3 for IPsec ESP)

In the case of a user authentication failure, the user will usually not be able to use a security association with the correct key material. Therefore, when using ESP for integrity protection and encryption, this will cause SM7 to be dropped at the P-CSCF IP(sec) layer due to a failed integrity check within ESP processing.

As SM7 will not reach the P-CSCF IMS application, the P-CSCF shall implement a timer for the authentication process. When a message is received that passes the integrity-check and successfully completes the authentication, it is immediately processed. However, if during the registration timer the P-CSCF receives packets that cannot be verified, it discards them. At the end of the registration timer, it reports an authentication failure back to the home network.

D.2.3 Authenticated re-registration procedures specific to the ESP protection mechanism

The new security associations SA11 and SA12 shall be bound to a new port on the UE side. This new port shall be communicated by the UE in the *info* field of the first REGISTER message SM1.

Annex E (informative): Set-up procedures for SIP level based solution

[Editors Note: If the SIP level solution is chosen the chapters below shall be moved into the main body of this TS in the corresponding sections.] This chapter is based on chapter 7 and provides additional specification for the support of SIP level integrity protection].

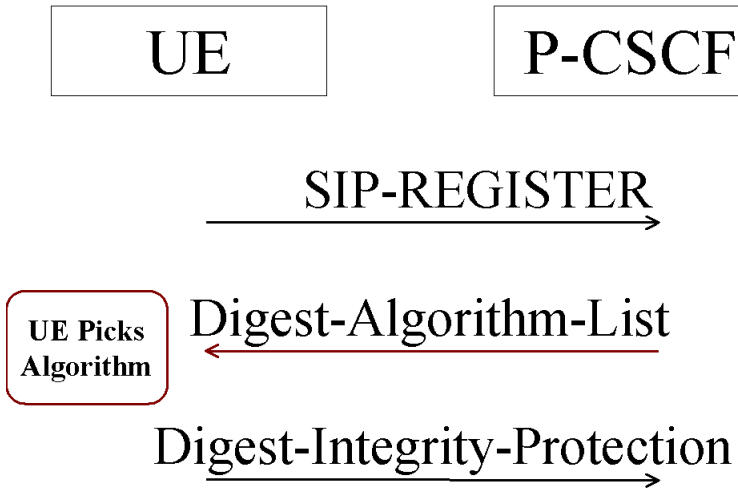
For each incoming message the SIP application must verify that the correct inbound SA associated with the public ID (IMPU) given in the SIP message has been used.

Annex F (informative): Bidding down protection

This annex contains the Bidding Down Protection mechanism which is an extension to HTTP Digest i.e. [12]. The purpose with this Annex is to keep track on the development of the Bidding Down Protection and to have it as a fallback solution if Security Mode Setup is not available in time from IETF.

[Editors note: This text is FFS but it has to be further developed describing the mechanism in more detail. It is also FFS how to ensure that the UE picks the strongest algorithm and what algorithms should be mandatory.]

The extended HTTP Digest can negotiate what integrity algorithm to use. The general scheme is described in the figure below.



This security mode set-up looks different to the current requirements defined in clause 7 where the P-CSCF chooses the algorithm. A proposed mechanism for bidding down protection is to utilise a nonce, which will have a meaning for the client. The nonce-value in this case is not longer only a random number it will include the integrity algorithm and quality of protection along with the traditional nonce value. The nonce in this case could look like:

Nonce = base64 encoding (auth-algorithms, auth-extd-int, time-stamp || Hash(time-stamp, Request URI, private-key))

The server (in the IMS profile the server will be the P-CSCF) issues a list of supported mechanisms like e.g. MD5 and SHA-1. The client (in the IMS profile the client is the UE) picks the strongest algorithm it supports i.e. SHA-1 and protects the following messages with this algorithm. A man in the middle could not degrade the proposed list since the client shall repeat the nonce value which in this case includes the proposed list of algorithms as suggested above. The server or the P-CSCF can check that the list is correct but it does not have to store the suggested list.

Annex G (informative): Management of sequence numbers

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

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

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

Annex H (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2001-12	SP_14	SP-010624	-		Presented to TSG SA #14 for Information		1.0.0
2002-03	SP_15	SP-020116	-		Presented to TSG SA #15 for Approval	1.4.0	2.0.0