3G TS 33.203 V0.~~6~~7.0 (2001-~~09~~11)

Technical Specification

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

3GPP

3GPP

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.

~~Introduction~~

~~This clause is optional. If it exists, it is always the third unnumbered clause.~~

1 Scope

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

The IM CN SSIMS 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, how the subscriber is authenticated and how the subscriber authenticates the IM CN SSIMS network.

2 References

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

[1]   3G TS 33.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture".

[2]   3G TS 22.228: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Service Requirements for the IP Multimedia Core Network".

[3]   3G TS 23.228: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; IP Multimedia (IM) Subsystem".

[4]   3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Security Threats and Requirements ".

[5]   3G TS 33.210: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Network domain security; IP network layer security".

[6]   IETF RFC 2543bis-043 (2001) "SIP: Session Initiation Protocol"

[7]   IETF RFC 2284 (1998) "PPP Extensible Authentication Protocol (EAP)"

[8]   IETF Draft (2001) "draft-arkko-pppext-eap-aka-010.txt"

[9]   IETF Draft (2001) "draft-torvinen-http-eap-basic-011.txt"

[10]   IETF RFC 2716 (1999) "PPP EAP TLS Authentication Protocol"

[11]   IETF Draft (2001) "draft-haverinen-pppext-eap-sim-01.txt"

[12]   3G TS 21.905: "3rd Generation Partnership Project (3GPP): Technical Specification Group (TSG) SA; Vocabulary for 3GPP specifications

[13]   3G TS 24.229: "3rd Generation Partnership Project (3GPP): Technical Specification Group (TSG) Core Network; IP Multimedia Call Control Protocol based on SIP and SDP"

3   Definitions, symbols and abbreviations

3.1   Definitions

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

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

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

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

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

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

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

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

~~3.2~~   ~~Symbols~~

~~For the purposes of the present document, the following symbols apply:~~

3.3   Abbreviations

For the purposes of the present document, the following abbreviations apply, [12] contains additional applicable abbreviations:

AAA	Authentication Authorisation Accounting
AKA	Authentication and key agreement
CSCF	Call Session ~~State~~ Control Function
~~GGSN~~	~~Gateway GPRS Support Node~~
~~HN~~	~~Home Network~~
HSS	Home Subscriber Server~~r~~
~~HTTP~~	~~Hypertext Transfer Protocol~~
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 Equipmen~~t~~t
~~PPP~~	~~Poin to Point Protocol~~
~~PS~~	~~Packet Switched~~
SA	Security Association
SEG	Security Gateway
SDP	Session Description Protocol
~~SGSN~~	~~Serving GPRS Support Node~~
SIP	Session Initiation Protocol
UA	User Agent
~~UAC~~	~~UA Client~~

~~UAS~~ ~~UA Server~~
~~UE~~ ~~User Equipment~~
~~UICC~~ ~~UMTS IC Card~~
~~USIM~~ ~~User Services Identity Module~~
~~VN~~ ~~Visited Network~~

4 Overview of the security architecture

[Editor's note This section shall have a figure of the overall architecture for the IM CN SS and explaining text on the trust relations, possible threats and a brief overview of the provided security features.]

In the PS domain, the service is not provided until a security association is established between the mobile equipment and the network. ~~IM CN subsystem~~IMS is essentially an overlay to the PS-Domain and has a low dependency of the PS-domain.~~is not embedded in the SGSN or GGSN nodes C~~consequently a ~~second~~ separate security association is required between the multimedia client and the IMS~~IM CN subsystem~~ before access is granted to multimedia services. The ~~IM CN Subsystem~~IMS Security Architecture is shown in the following figure. The ISIM is responsible for the handling of keys, SQN etc that are tailored to ~~IM CN SS~~IMS. The ~~keys i.e. CK and IK, SQN etc~~security parameters handled by the ISIM are ~~all~~ independent of the similar security parameters that exist in the USIM.

Although ISIM and USIM are logically independent, all the following cases are possible for implementation:

- ISIM and USIM are implemented as a single application inside one UICC
- ISIM and USIM are implemented as two distinct applications inside one UICC
- ISIM and USIM are implemented inside two distinct UICCs.
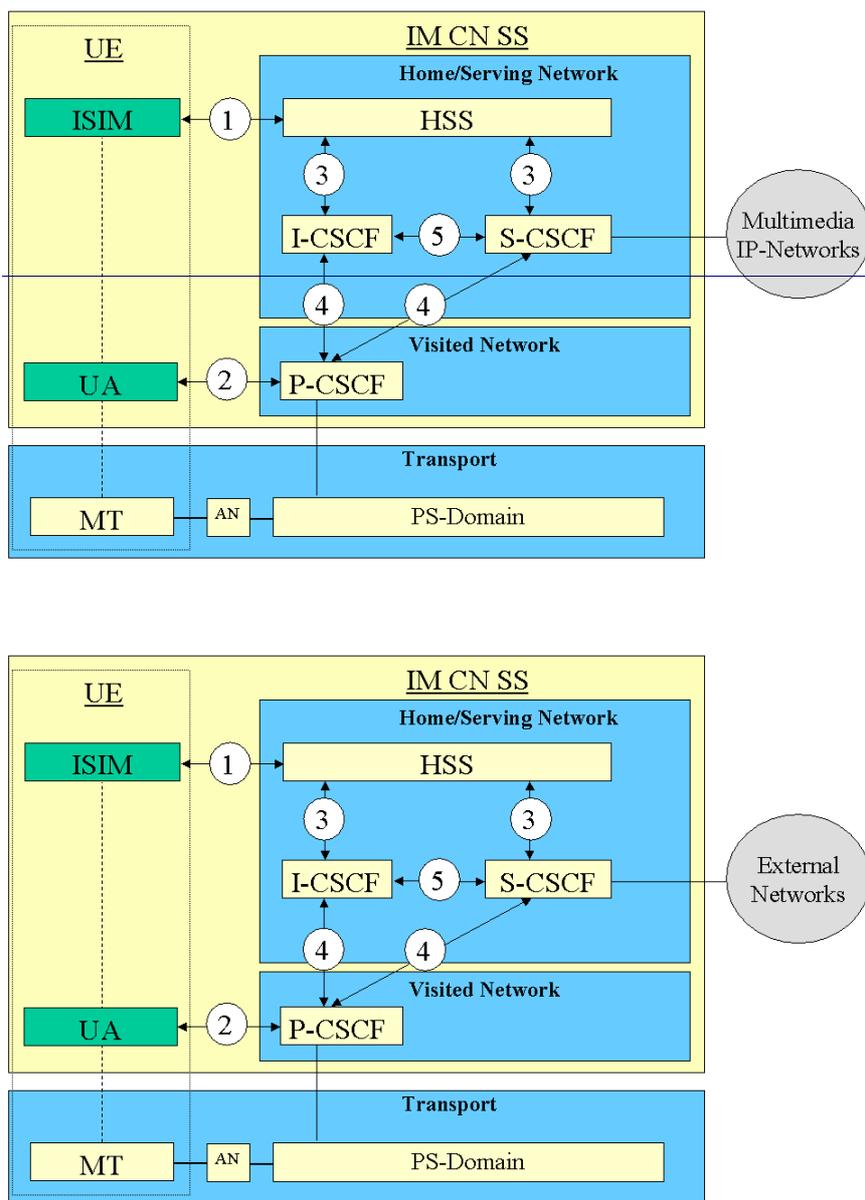
Figure 1. The ~~This is the security~~IMS security architecture ~~for the IM CN Subsystem.~~

There are five different security associations and different needs for security protection for ~~IM CN SS~~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 several IMS identities i.e. the IMPI and at least one IMPU. The HN authenticates the IMPI.

2. Provides a secure link and a security association between the UE and a P-CSCF.

3. Provides security within the network domain internally for the Cx-interface. ~~This part is not covered in this specification instead [5] specifies what security measures shall be defined in the internal network over the Cx-interface.~~This security association is covered by TS 33.210 [5].

4. Provides security between different networks for SIP capable nodes. This security association is covered by TS 33.210 [5]~~This part is not covered in this specification instead [5] specifies what security measures shall be defined for these type of interfaces.~~

5.   Provides security within the network internally between SIP capable nodes. This security association is covered by TS 33.210 [5]. ~~This part is not covered in this specification instead [5] specifies what security measures shall be defined for these types of interfaces.~~

[Editors Note: Security measures for application servers (OSA and SIP AS) and IM SSF is FFS but it seems that this is covered by NDS]

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 ~~IM CN Subsystem~~IMS security mechanism provides additional protection against security breaches. For example, if the PS-Domain security is breached the ~~IM CN Subsystem~~ IMS would continue to be protected by it's own security mechanism.
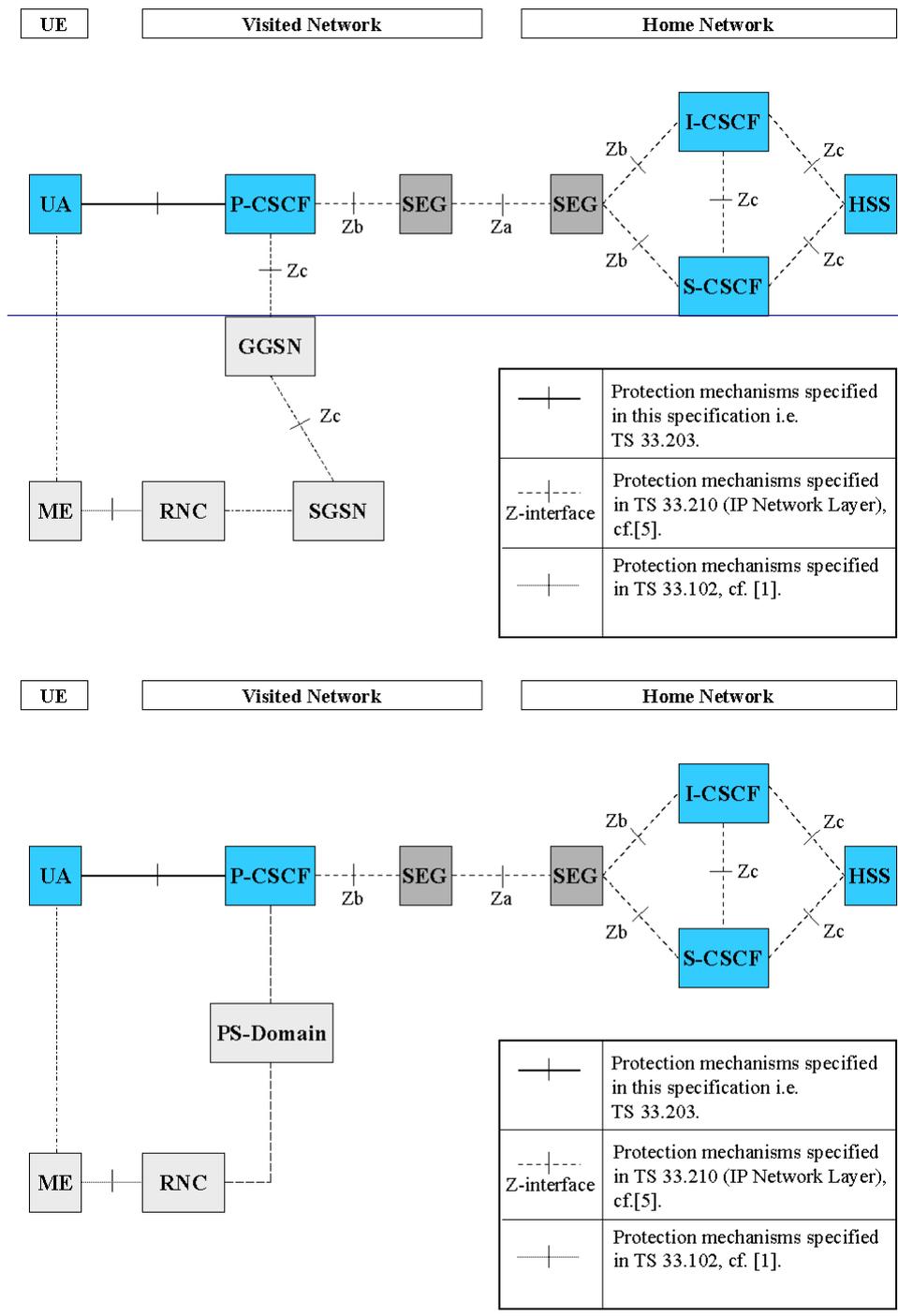
Figure 2. This figure gives an overview of the security architecture for ~~IM CN SS~~IMS and the relation with Network Domain security, cf. [5].

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

5 Security features

[Editor's note: This section shall explain the provided security features in detail]

5.1 Secure access to ~~IM CN SS~~IMS

5.1.1 Authentication of the subscriber and the network

[Editor's note: This section shall deal with subscriber identity and authentication of the subscriber and Home Network/Serving Network]

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

All SIP-signaling will take place over the PS-domain in the user plane i.e. IM-services are essentially an overlay to the PS-domain. Hence the Visited Network will have control of all the subscribers in the PS-domain i.e. Visited Control (Authorization of bearer resources) since the Visited Network provides with a transport service and QoS.

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

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

The AKA-protocol is a secure protocol developed for UMTS and it will be reused for IM-services and then called IMS AKA.

The Home Network authenticates the subscriber ~~at~~ via registrations or re-registrations only. ~~In order to re-authenticate a subscriber the Home Network can force a re-registration by using e.g. a re-registration timer.~~

5.1.2 Re-Authentication of the subscriber

The S-CSCF shall be able to initiate an authenticated re-registration of a user at any time, independent of previous registrations, see figure below.
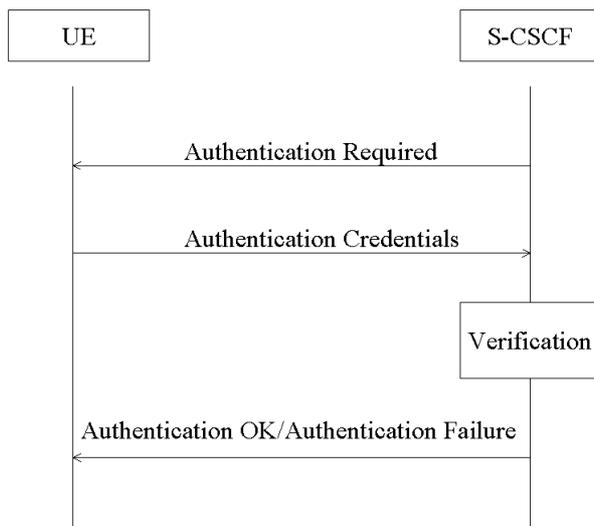
[Editors Note: It is FFS whether the P-CSCF should also be able to initiate re-registrations].

[Editors Note: Solutions for the initiation of network initiated authenticated re-registration shall be elaborated by CN1. The stage 2 information flows shall be included in this TS 33.203.] [Editors Note: Authentication shall according to the current requirements only take place at (Re-)Registrations.]

~~5.1.2~~5.1.3   Confidentiality protection

Confidentiality protection shall optionally be used between the UE and the P-CSCF. If it is provided, then it shall be as specified in section 6.2. The UE and P-CSCF shall negotiate what confidentiality algorithm shall be used for the session and shall agree on a confidentiality key CK_{IM}. IP-based services cannot rely on confidentiality being provided in the access network.

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in [5].~~IP-based services will get protection by the confidentiality protection defined in R'99 at the bearer level. In R'99 confidentiality protection is provided for signaling data and user data between the UE and the serving RNC. The serving RNC retrieves the cipher key CK from the SN. The ciphering protection for UMTS is optional to use.~~

~~For UMTS access confidentiality protection for SIP signaling can either rely on the confidentiality mechanisms provided by UMTS and mechanisms provided by Network Domain Security, cf. [5] or as specified in section 6.2.~~

[Editor's note: At this stage both Annex B and Annex C provides with potential measures for confidentiality protection. One of these solutions will be the normative solution. Note that for R5 confidentiality measures are optional.]

~~5.1.3~~5.1.4   Integrity protection

Integrity protection shall be used end-to-end 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 what integrity algorithm that shall be used for the session, specified in chapter 7.

2. The UE and the P-CSCF shall agree on an integrity key, IK 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 make verify that the data received originates from a node, which has the agreed session key, IK. This ~~check~~ verification is also used ~~to~~for ~~detecting~~ detect if the data has been tampered with ~~by a man-in-the-middle~~.

[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.]

5.2 Visibility and configurability

[Editor's note: This section shall contain what the subscriber shall be able to configure and what is visible for the subscriber regarding the actual protection the subscriber is provided with.]

The user shall be informed which level of protection that is in use.

5.3 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.

[Editor's note: The hiding requirements for the P-CSCFs are FFS]

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

[Editor's note: This section shall describe the security mechanisms that are provided inter domain, intra domain and to the UE.]

6.1 Authentication and key agreement

[Editor's note: This section shall describe in detail how the authentication is performed and how the keys, IK and CK, are derived and delivered to the different nodes.]

The scheme for authentication and key agreement in the ~~IM CN SS~~IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. Figure 3. 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.

For the IMS the ISIM and the HSS keeps track of the counters SQN_{ISIM} and SQN_{HSS}. The handling of the SQN can be as in [1]. 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 and embedded in EAP, cf. [7]-[9].

[Editors Note: Shall the HN choose EAP AKA for 3GPP-access or is it to be an option for the HN to choose either EAP AKA or perhaps any other mechanism e.g. HTTP digest depending on policy?]

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. For each user it is the HSS that keeps track of the counter SQN_{HSS}. The requirements on

the SQN handling both in the Home Network i.e. the HSS and the ISIM are specified in [1]. The AMF field can be used in the same way as in [1].

Furthermore a security association is established between the UE and the P-CSCF. The subscriber may have several IMPUs associated with one IMPI and 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 authenticated re-registration 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.The ISIM and the HSS keeps track of the counters SQN_{ISIM} and SQN_{HSS} for the IM-domain. The handling of the SQN can be as in [1]. IMS AKA is based on EAP, cf. [7], and the AKA extension to EAP and HTTP, cf. [8] and [9] respectively.

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

[Editors Note: Shall the HN choose EAP AKA for 3GPP-access or is it to be an option for the HN to choose either EAP AKA or perhaps any other mechanism e.g. HTTP digest depending on policy?]

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. For each user it is the HSS that keeps track of the counter SQN_{HSS}. The requirements on the SQN handling both in the Home Network i.e. the HSS and the ISIM are specified in [1]. The AMF field can be used in the same way as in [1].

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

6.1.1   Registration of an IM-subscriber

Before a user can get access to the IM services at least on IMPUhe needs to be registered and the IMPI authenticated in the IM CN SSIMS 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 3, which will perform the authentication of the user.
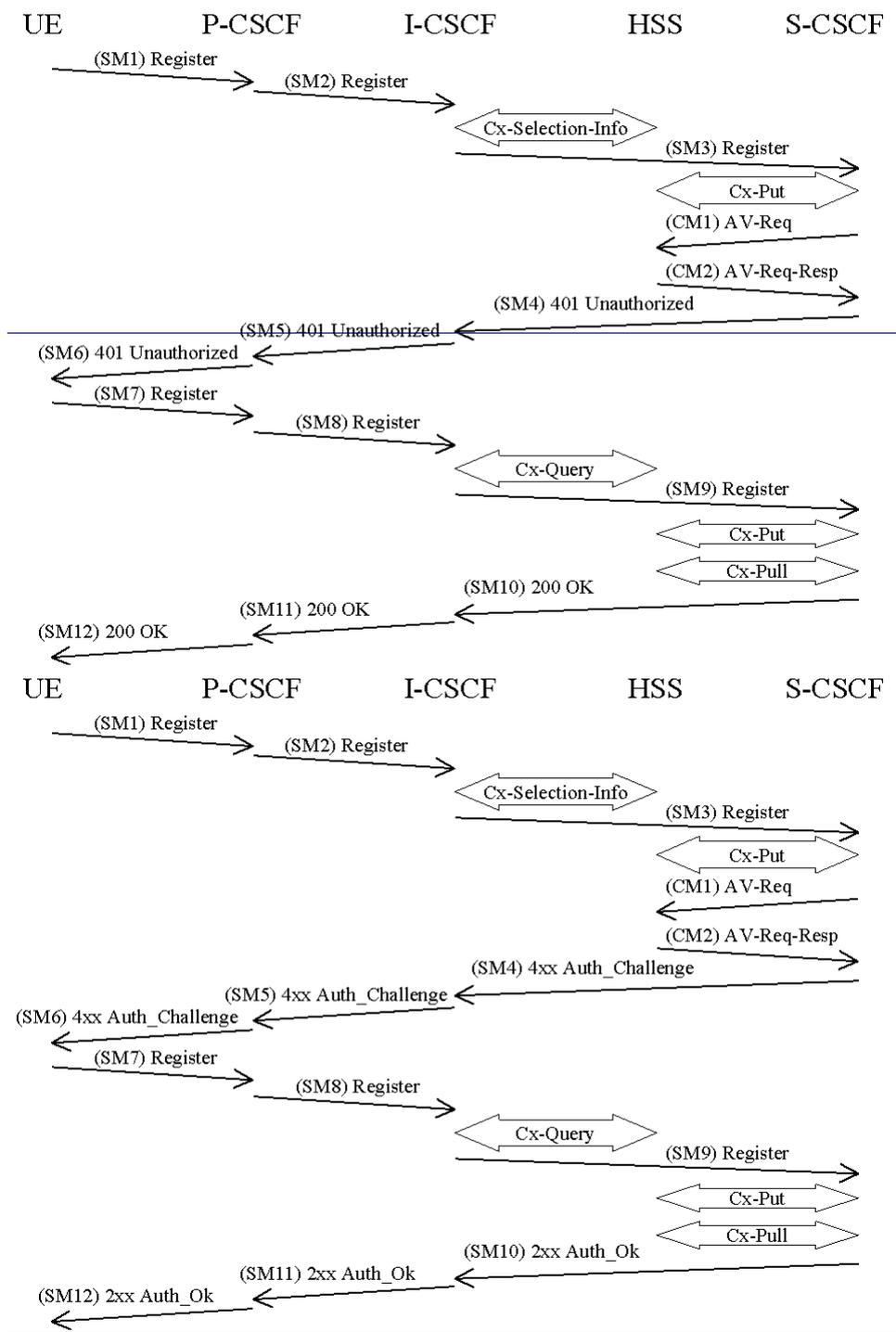
Figure 3: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error.

The flows in more detail (for clarification: TS 24.229, cf. [13], specifies the details)

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

SM1:

REGISTER sip: ----

Authorization-EAP(IMPI)

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

The P-CSCF and the I-CSCF forwards the SIP REGISTER towards the S-CSCF and adds a Via header with their addresses included, i.e. SM2 and SM3.

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 *registration pending* at the Cx-Put procedure after SM3 has been received by the S-CSCF

Upon receiving the SIP REGISTER the S-CSCF will need one AV which includes the challenge. As an option the S-CSCF can require more than one AVs. If the S-CSCF has no valid AV then the S-CSCF shall send a request for the 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.

CM1:

Cx-AV-Req(IMPI, IMPU, 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, IMPU,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~~401 Unauthorized~~ i.e. an authentication challenge to the UE including the challenge RAND, the authentication token AUTN in SM4 and the integrity key IK and optionally the cipher key CK.

SM4:

SIP/2.0 4xx Auth_Challenge~~401 Unauthorized~~
~~Via: ----~~
~~From: IMPI~~
~~To: IMPU~~
~~Call-ID: ----~~
~~Cseq: 1 REGISTER~~
WWW-Authenticate~~:~~ ~~eap~~EAP(~~ *paramaters:*~~*IMPI, RAND, ‖AUTN)*
Key parameters(~~:~~*IK, (‖CK))*

~~Content-Length: 0~~

[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:

SIP/2.0 4xx Auth_Challenge~~SIP/2.0 401 Unauthorized~~
~~Via: ----~~

~~From: IMPI~~
~~To: IMPU~~
~~Call-ID: ----~~
~~Cseq: 1 REGISTER~~

WWW-Authenticate~~-:~~ EAP~~eap~~*(paramaters:*__IMPI,__ RAND__,__ ~~||~~AUTN*)*

~~Content-Length: 0~~

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.

SM7:

REGISTER sip: ---- ~~SIP/2.0 401 Unauthorized~~
~~Via: ----~~
~~From: IMPI~~
~~To: IMPU~~
~~Call-ID: ----~~
~~Cseq: 1 REGISTER~~

Authorization~~-:~~ ~~eap~~EAP ~~*parameters:*~~ *(IMPI, RES)*

~~Content-Length: 0~~

The P-CSCF forwards the RES in SM8 to the I-~~CSCF which~~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.

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. This feature is FFS in [3]. The re-registration feature opens up a potential denial-of-service attack in the sense that an attacker could re-register a subscriber and respond with the wrong RES and the HN could then de-register the subscriber. This shall be avoided by letting the subscriber be registered with the old set of parameters until a re-registration is successfully authenticated.

[Editor's note: It is FFS if this way of protecting the user from DoS attack is feasible or not. The current assumption by SA3 is that DoS attacks are difficult to standardize against e.g. error messages shall not be integrity protected.]

The re-registration looks the same as the registration case except that CM1 and CM2 can be omitted as long as the S-CSCF has valid AV(s). At a re-registration the registration flag has already the value *registered*. Whether the registration flag shall be changed to *register pending* is based on the policy of the operator. There are two cases:

- The IMS subscriber is de-registered after unsuccessful registration. In this case the registration flag shall be set to *unregistered* and an error message shall be sent to from the S-CSCF to the HSS.

- The IMS subscriber remains registered after unsuccessful re-registration. In this case the registration flag is kept in the HSS to the value *registered* even if the authentication was unsuccessful.

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

[Editor's note: The current assumption has been that all IMPUs will be registered in the same S-CSCF. This however is not the general scenario adopted by SA2. It is left FFS how the current solutions need to be adapted to the general scope as shown in the figure:

```
                                              ┌──────────────┐
                                              │   Public     │───────┐
                                              │ User Identity│       │   ┌──────────┐
                                              └──────────────┘       ├───│ Service  │
┌──────────────┐   ┌──────────────┐          ┌──────────────┐       │   │ Profile  │
│     IMS      │───│   Private    │──────────│   Public     │───────┘   └──────────┘
│ Subscription │   │ User Identity│          │ User Identity│
└──────────────┘   └──────────────┘──────────┐
                                              │   Public     │   ┌──────────┐
                                              │ User Identity│───│ Service  │
                                              └──────────────┘   │ Profile  │
                                                                 └──────────┘
```
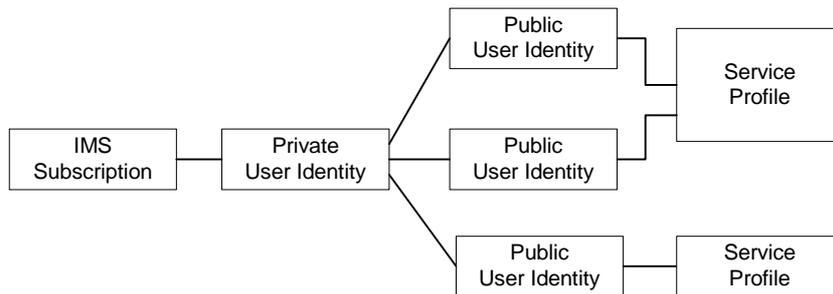
According to the SA1 requirement this is the scenario that should be supported by the IMS in Release 5. All public user identities that are associated with the same profile should have the same set of services. Public user identities that are associated with a different profile could have a different set of services.]

[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.]

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

When the check of the RES in the S-CSCF fails the user can not be authenticated and hence registration fails. The flow is identical as for the successful registration in 6.1.1 up to SM9.
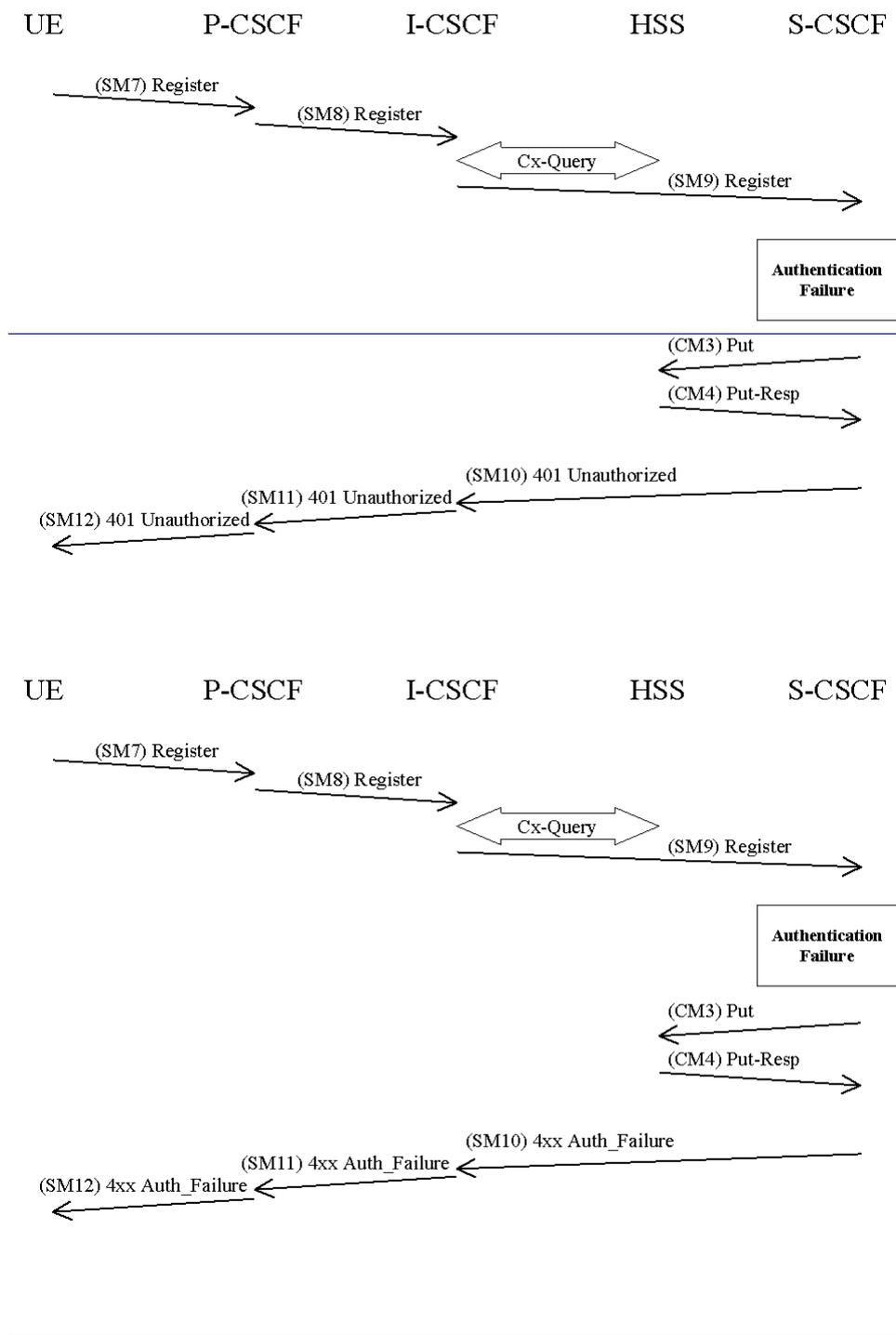
CM3:

Cx-AV-~~Req~~Put(IMPI, IMPU, 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 for that particular IMPU. The HSS responds with a Cx-Put-Resp in CM4. In SM10 the S-CSCF sends a ~~401 4xx unauthorized~~ Auth_Failure towards the UE indicating that the authentication failed, no security parameters shall be included in this message.

SM10:

SIP/2.0 ~~401 Unauthorized~~4xx Auth_Failure
~~Via: ----~~
~~From: IMPI~~
~~To: IMPU~~
~~Call-ID: ----~~
~~Cseq: 1 REGISTER~~
~~Content-Length: 0~~

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

[Editors Note: It is FFS if the IMPI shall be included in SM10.]

6.1.~~3~~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.

UE   P-CSCF   I-CSCF   HSS   S-CSCF

Authentication
Failure

(SM7) Register

(SM8) Register

Cx-Query

(SM9) Register

(CM3) Put

(CM4) Put-Resp

(SM10) 401 Unauthorized

(SM11) 401 Unauthorized

(SM12) 401 Unauthorized

UE   P-CSCF   I-CSCF   HSS   S-CSCF

Authentication
Failure

(SM7) Register

(SM8) Register

Cx-Query

(SM9) Register

(CM3) Put

(CM4) Put-Resp

(SM10) 4xx Auth_Failure

(SM11) 4xx Auth_Failure

(SM12) 4xx Auth_Failure

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 sip: -----
Via: ----
From: IMPI
To: IMPU
Call-ID: ----
Cseq: 1 REGISTER

Failure(: *AuthenticationFailure, IMPI)*

~~Content-Length: 0~~

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. The S-CSCF sends a ~~401 Unauthorized~~4xx Auth_Failure towards the UE. The messages CM3, CM4 and SM10-SM12 shall be the same as in 6.1.2.1.

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

6.1.4 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.
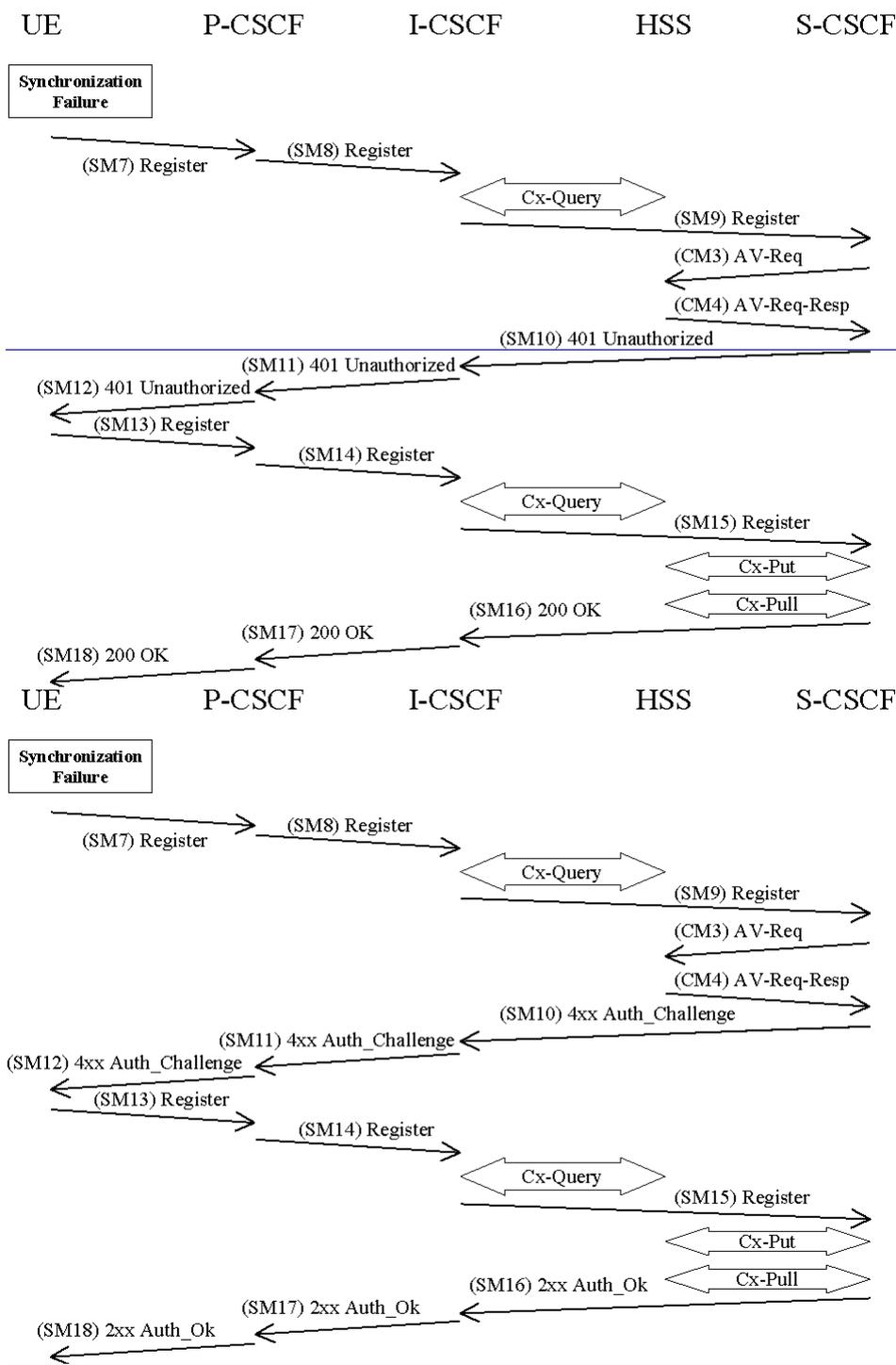
The flow equals the flow in 6.1.3.1 up to SM6. When the UE receives SM6 it detects that the SQN is out of range and sends a synchronization failure back to the S-CSCF in SM7.

SM7:

REGISTER sip: ----
~~Via: ----~~
~~From: IMPI~~
~~To: IMPU~~
~~Call-ID: ----~~
~~Cseq: 1 REGISTER~~

Failure(~~: Synch~~*ronization Failure*~~, |~~*AUTS, IMPI)*

~~Content-Length: 0~~

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, IMPU, 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, IMPU,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.

6.2 Confidentiality mechanisms

[Editor's note: This section shall deal with cipher algorithms used between the UE and the P-CSCF]

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

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

[Editor's note: At this stage both Annex B and Annex C provides with potential measures for confidentiality protection. One of these solutions will be the normative solution. Note that for R5 confidentiality measures are optional.]

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 address of the S-CSCF. An IV of 128-bit is needed at the encryption and decryption phase and it shall be appended to the encrypted information. The information shall also be MAC protected with a block cipher in CBC-MAC mode.

When the I-CSCF decrypts the information it shall verify the integrity.

[Editor's note: The above text is very brief and the mechanisms have to be described in more detail.]

7 Security association set-up procedure

The security ~~mode~~ association set-up ~~setup~~ procedure is necessary in order to decide what security services that apply and when ~~and how~~ the security services start. In the ~~IM CN SS~~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:

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

- Authentication (integrity) algorithm, and optionally encryption algorithm

- ~~Life type: the life type is always seconds~~

- SA ~~duration~~lifetime

- SA_ID that is used to uniquely identify the SA at the receiving side.~~: the SA duration has a fixed length of 2^{32} -1.~~

- Key length: the length of encryption and authentication (integrity) keys is 128 bits.

~~[Editors Note:~~ Parameters specifically related to certain protection methods are kept in~~IPSec~~ the annexes describing the protection methods.

[Editors Note: The support of different mechanisms is FFS.]~~are kept in Annex D and should be moved into this section if that solution is finally chosen.]~~

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.

UE   P-CSCF   S-CSCF

(SM1) Register

(SM2) Register

(SM3) 401 Unauthorized

(SM4) 401 Unauthorized

(SM5) Register

(SM6) Register

(SM7) 200 OK

(SM8) 200 OK

UE   P-CSCF   S-CSCF

(SM1) Register

(SM2) Register

(SM3) 4xx Auth_Challenge

(SM4) 4xx Auth_Challenge

(SM5) Register

(SM6) Register

(SM7) 2xx Auth_Ok

(SM8) 2xx Auth_Ok
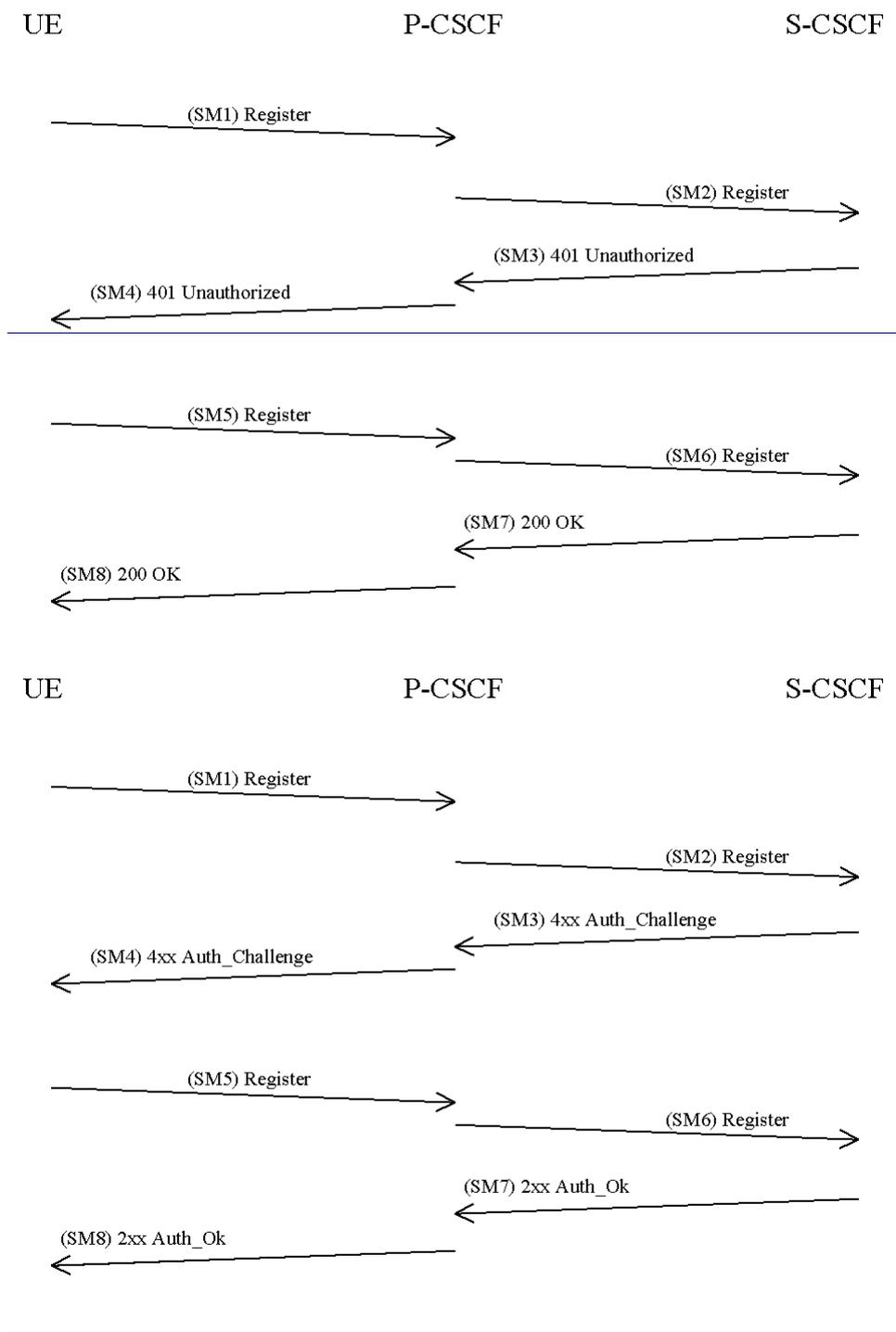
The UE sends a Register message towards the S-CSCF ~~for authentication purposes~~ to register the location of the UE and to set-up the security mode. This has been described in 6.1. In order to ~~setup the security services~~ start security mode setup the UE shall include a *Security-setup:* line in this message, including the protection method, the proposed set of integrity ~~security~~ 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. ~~In this case a list of n integrity algorithms and a list of m confidentiality algorithms are proposed.~~ The SA_ID_U ~~SPI_U~~ shall be chosen in such a way that it uniquely identif~~identifyy~~ the (unidirectional) inbound SA at the UE side, within the UE.

Elements in [...] are optional.

SM1:

> REGISTER sip: ----
> ~~Via: ----~~
> ~~From: IMPI~~
> ~~To: IMPU~~
> ~~Call-ID: ----~~
> ~~Cseq: 1 REGISTER~~
> ~~...~~
>
> Security-setup(~~:~~ *integrity mechanism,* ~~esp |~~*[confidentiality mechanism],* *integrity algorithms list,* ~~|~~*[confidentiality algorithms list* ~~],~~*|* ~~SPI_U~~*SA_ID_U, [info])*
> Authorization-EAP*(IMPI)*
> ~~Content-Length: 0~~

[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]

The P-CSCF shall choose <u>exactly</u> one of the proposed <u>mechanisms respectively and exactly one of the proposed</u> algorithms <u>respectively</u> based on the ~~policy that applies and send~~<u>policies that applies and send</u> the selected <u>mechanisms and</u> algorithm<u>s</u> to the UE in SM4.

The ~~SPI_P~~<u>SA_ID_P</u> 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: The unprotected port specifies the port where the P-CSCF is willing to accept unprotected error messages sent by the UE.]

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

> SM4:
>
> SIP/2.0 ~~401~~ <u>4xx</u> ~~Unauthorized~~ <u>Auth_Challenge</u>
> ~~Via: ----~~
> ~~From: IMPI~~
> ~~To: IMPU~~
> ~~Call-ID: ----~~
> ~~Cseq: 1 REGISTER~~
> ~~...~~
>
> Security-setup*(integrity mechanism, [confidentiality mechanism], integrity algorithms list, [confidentiality algorithms list], SA_ID_P, [info])*
> Authorization-EAP*(IMPI)*~~Security-setup: esp | *integrity algorithm | [confidentiality algorithm] | SPI_P | unprotected_port*~~

> ~~Content-Length: 0~~

[Editors Note: The parameters esp and SPI_P are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_P should probably defined for the SIP-level protection solution. The unprotected port is only valid for the IPSec solution and shall be removed if Sip-level protection is chosen. The unprotected port for IPSec specifes what port shall be used for error messages sent from the UE.]

The UE shall in SM5 start the integrity protection – and optionally the confidentiality protection ~~–~~ of the whole SIP-message by setting up security associations according to <u>mechanisms and</u> the parameters negotiated in SM1 and SM4, and applying the corresponding protection to the SIP-message. Furthermore the Security-setup<u>:</u> line sent in SM1 shall be included:

SM5:

REGISTER sip: ----
~~Via: ----~~
~~From: IMPI~~
~~To: IMPU~~
~~Call-ID: ----~~
~~Cseq: 1 REGISTER~~
Security-setup(*integrity mechanism, [confidentiality mechanism], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info]*)

Authorization-EAP*(IMPI)*~~Security-setup: *esp | integrity algorithms list | [confidentiality algorithms list]| SPI_U*~~

...

~~Content-Length: 0~~

~~[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]~~

After receiving SM5 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 finally sends SM8 to the UE. SM8 does not contain information specific to security mode setup (i.e. a Security-setup line), but with sending SM8 not indicating an error the P-CSCF confirms that security mode setup has been successful. After receiving SM8 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 SM8 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   User authentication failure

In this case the authentication of the user fails in the network due an incorrect RES. The S-CSCF will send a 4xx Auth_Failure~~401 Unauthorized~~ message SM7, which will pass through the already established SA to the UE as SM8.

Note, that this failure will already occur in SM5, when the UE does not use the correct integrity key IK. In this situation, the P-CSCF will receive protected packets that cannot be verified ~~and therefore will be discarded.~~

~~In order to handle this situation, 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..~~

It may seem from the above discussion that there is no requirement to check the RES at the S-CSCF since a false RES sent by a UE will never reach the S-CSCF. However, it is still necessary to check RES at the S-CSCF since this

prevents a P-CSCF from registering a UE without performing user authentication. It therefore reduces S-CSCF trust in the P-CSCF.

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 SM5 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 SM5, indicating a network authentication failure, to the P-CSCF, without protection. SM5 should not contain the security-setup line of the first message.

~~[Editors Note: For IPSec failure messages due to a network authentication failure shall be sent on a different port, the unprotected port. This text shall be moved into the main body if IPSec is finally chosen.]~~

7.3.1.3 Synchronisation failure

In this situation, the UE observes that the AUTN sent by the network in SM4 contains an out-of-range sequence number. The UE shall sends a new register message SM5 to the P-CSCF in the clear, indicating the synchronization failure. SM5 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.

[Editors Note: ~~For IPSec failure messages due to synchronization failures shall be sent on a different port.~~ This text shall be moved into the main body if IPSec is finally chosen.]

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. SM4 shall respond to SM1 with indicating a failure, by sending a ~~403~~ 4xx ~~Forbidden error message~~Unacceptable_Proposal.

The P-CSCF therefore shall modify the message SM2 such that the S-CSCF sends a 4xx Unacceptable_Proposal~~403 Forbidden error~~ message back to the UE in SM3/4 and the registration process is finished.

> SM2:
>
> REGISTER sip: ----
> ~~Via: ----~~
> ~~From: IMPI~~
> ~~To: IMPU~~
> ~~Call-ID: ----~~
> ~~Cseq: 1 REGISTER~~
> Security-setup*(integrity mechanism, [confidentiality mechanism], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info])*
> Authorization-EAP*(IMPI)*Security-setup: ~~*esp | integrity algorithms list | [confidentiality algorithms list]| SPI_U*~~
> Failure(~~:~~*NoCommonIntegrityAlgorithm*)
> ~~Content-Length: 0~~

[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]

[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 SM4 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 SM5 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 SM5 do not match. The P-CSCF shall respond to the UE by sending a 4xx Unacceptable_Proposal 403 Forbidden error message in SM8. The P-CSCF therefore shall modify the message SM6 such that the S-CSCF sends a 4xx Unacceptable_Proposal403 Forbidden error message back to the UE in SM7/8 and the registration process is finished.

SM6:

REGISTER sip: ----
Via: ----
From: IMPI
To: IMPU
Call-ID: ----
Cseq: 1 REGISTER

Security-setup(*integrity mechanism, [confidentiality mechanism], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info]*)

Authorization-EAP*(IMPI)*Security-setup: | integrity algorithms list | [confidentiality algorithms list]| esp | integrity algorithms list | [confidentiality algorithms list]| SPI_U

Failure(:*NoCommonIntegrityAlgorithm*)
Content-Length: 0

[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]

[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.

[Editors Note: It is FFS if these SAs shall protect the first two messages of the authenticated re-registration, i.e. SM1 and SM4.]

Before SM5 is sent by the UE, both peers shall replace the existing SA by the new SA negotiated during these first two messages.

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

[Editors Note: The following part of the description is independent of the particular mechanism for integrity and confidentiality protection.]

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 SM3 from the S-CSCF and then sends SM4 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 SM4 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends SM5 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. SM5 is protected with the new SA11.

4) The P-CSCF waits for the response SM7 from the S-CSCF and then sends SM8 to the UE, using the new SA 12.

5) After the reception of SM8 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.

Aspects specific to the use of IPsec/ESP:

~~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 first REGISTER message SM1 in the list of parameters to be negotiated in a security association set-up.~~

[Editor's note: If it is desired to use identical messages for new registrations and re-registrations then a new port can also be included in the first message for new registrations although it is not strictly needed there.]

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 SM8, and SM8 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

<u>User authentication failure</u>

The S-CSCF will send a ~~401~~ 4xx <u>~~Unauthorized~~ Auth_Failure</u> message SM7, which will pass through the already established SA to the UE as SM8. Afterwards, both, the UE and the P-CSCF delete the new SAs.

<u>Network authentication failure</u>

If the UE is not able to successfully authenticate the network, it does not establish a new SA. The UE sends a REGISTER message SM5 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.

<u>Synchronisation failure</u>

If the UE notices a synchronisation failure it does not establish a new SA. The UE sends a message SM5, 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

<u>Unacceptable proposal set</u>

The message SM4 shall respond to the first REGISTER message SM1 with a <u>4xx Unacceptable_Proposal</u>~~403 Forbidden~~, 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 <u>4xx Unacceptable_Proposal</u>~~403 Forbidden error~~ message back to the UE in SM3/4 and the registration process is finished.

> <u>SM2:</u>
>
> ——REGISTER sip: ----
> ~~—— Via: ----~~
> ~~—— From: IMPI~~
> ~~—— To: IMPU~~
> ~~—— Call-ID: ----~~
> ~~—— Cseq: 1 REGISTER~~
>
> > <u>Security-setup</u>(*integrity mechanism, [confidentiality mechanism], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info])*
> >
> > <u>Authorization-EAP</u>*(IMPI)* ~~Security-setup: | integrity algorithms list | [confidentiality algorithms list]| esp | integrity algorithms list | [confidentiality algorithms list]| —— SPI_U~~
> >
> > ——Failure(~~:~~*NoCommonIntegrityAlgorithm*)
>
> ~~Content-Length: 0~~

[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.]

~~[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]~~

<u>Failed consistency check of Security-Set-up lines</u>

This is the case if the Security-Setup line in SM5 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 SM5 do not match. In this case the P-CSCF shall respond to the UE by sending a <u>4xx Unacceptable_Proposal</u>~~403 Forbidden error~~ message in SM8 using the already established SA. Both sides delete the new SAs.

The P-CSCF therefore shall modify the message SM6 such that the S-CSCF sends the 4xx Unacceptable_Proposal~~403 Forbidden error~~ message back to the UE in SM7/8 and the registration process is finished.

SM6:

———REGISTER sip: ----

~~———Via: ----~~

~~———From: IMPI~~

~~———To: IMPU~~

~~———Call-ID: ----~~

~~———Cseq: 1 REGISTER~~

Security-setup(*integrity mechanism, [confidentiality mechanism], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info])*

Authorization-EAP*(IMPI)* ~~Security-setup: *| integrity algorithms list | [confidentiality algorithms list]| esp | integrity algorithms list | [confidentiality algorithms list]| SPI_U*~~

———Failure(~~:~~ *NoCommonIntegrityAlgorithm*)

~~Content-Length: 0~~

[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.]

[Editors Note: The parameters esp and SPI_U are related to the IPSec protection mechanism and should be removed from this TS if SIP-level integrity protection is chosen. A similar parameter as the SIP_U should probably defined for the SIP-level protection solution]

Annexes are only to be used where appropriate:

Annex <A> (normative): <Normative annex title>

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

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

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

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

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 ~~use~~ 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 outbound from the P-CSCF is CK_{MOD}.~~

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.~~[Note: CK_{MOD} is a suitable modification of CK. An example of a suitable modification is a rotation of the key bits by n bits, where n remains to be determined.]~~

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 ~~use~~ 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. The integrity key for the SA outbound from the P-CSCF is IK_{MOD}.~~

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.[Note: IK~~MOD~~ is a suitable modification of IK. An example of a suitable modification is a rotation of the key bits by n bits, where n remains to be determined.]

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]

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

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

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.

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.

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 "int". Digest supports integrity protection of the entire SIP message when the "qop-options" directive within the Digest challenge is set to the value "extended-int". (Use of either of these values of "qop-options" assumes that a context of client authentication has been previously established.)

To provide for protection of the entire SIP message, the P-CSCF shall issue a Digest challenge to the UE specifying the value "extended-int" for the "qop-options" directive.
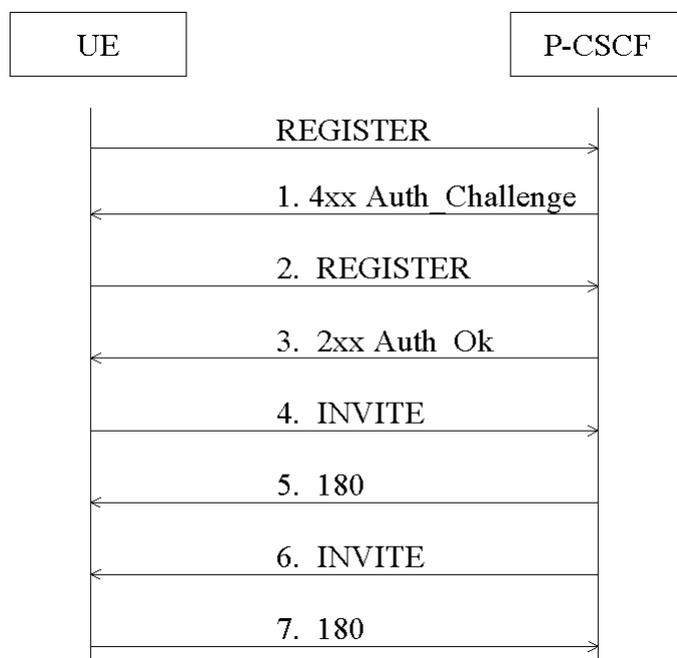
The message 'digest', or message authentication code, is conveyed in the "response" directive of the Digest response. The rules for computing "response" are as described in [1] with the following consideration: if the UE receives a Digest challenge with the "qop-options" directive set to either "int" or "extended-int", and the associated authentication challenge was an IMS AKA challenge, then the UE substitutes IK for the "password" component of A1 when computing "response=" in the Digest response. The UE sets the "username" component of A1 to a fixed value (e.g., "ims-user"). When sending messages to the UE that are to be integrity protected, the P-CSCF applies the same rules when computing "response". In this manner, the whole SIP message is always protected.

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 that is incremented by either endpoint when sending a message that is to be protected, facilitate anti-replay protection.

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

Per RFC 2617, the Digest challenge-related directives are carried in either the WWW-Authenticate or Proxy-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.

Per RFC 2617, the Digest response-related directives are carried in either the Authorization or Proxy-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 UE and the P-CSCF add the Authentication-Info header to all SIP responses. **Finally, the P-CSCF adds an Integrity header field to all SIP requests sent toward the UE.**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 (6-7).

```
        ┌──────────────┐                      ┌──────────────┐
        │      UE      │                      │    P-CSCF    │
        └──────────────┘                      └──────────────┘
               │                                     │
               │              REGISTER               │
               │────────────────────────────────────>│
               │         1. 4xx Auth_Challenge        │
               │<────────────────────────────────────│
               │           2. REGISTER               │
               │────────────────────────────────────>│
               │           3. 2xx Auth_Ok            │
               │<────────────────────────────────────│
               │             4. INVITE               │
               │────────────────────────────────────>│
               │              5. 180                 │
               │<────────────────────────────────────│
               │             6. INVITE               │
               │<────────────────────────────────────│
               │              7. 180                 │
               │────────────────────────────────────>│
               │                                     │
```

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: EAP <RAND AUTN>

Proxy-Authenticate: Digest realm=3GPP-IMS nonce=<random-number> algorithm=MD5 qop=extended-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: EAP <RES>

Proxy-Authorization: Digest username=ims-user, realm=3GPP-IMS, nonce=<echo-random-number>, uri=<SIP-URI>, response=<message-digest>, cnonce=<value>, nc=1, qop=extended-int

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

SIP/2.0 2xx Auth_Ok

Authentication-Info: qop=extended-int, rspauth=<message-digest>, nc=2

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=ims-user, realm=3GPP-IMS, nonce=<echo-random-number>, uri=<SIP-URI>, response=<message-digest>, cnonce=<value>, nc=3, qop=extended-int

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

SIP/2.0 180 Ringing

Authentication-Info: qop=extended-int, rspauth=<message-digest>, nc=4

6. **An incoming INVITE must also be integrity protected – the P-CSCF adds the Integrity header, which has the same syntax as Proxy-Authorization:**

INVITE sip: … SIP/2.0

Integrity: Digest username=ims-user, realm=3GPP-IMS, nonce=<echo-random-number>, uri=<SIP-URI>, response=<message-digest>, cnonce=<value>, nc=5, qop=extended-int

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

SIP/2.0 180 Ringing

Authentication-Info: qop=extended-int, rspauth=<message-digest>, nc=6

[Editors Note: Further details will be provided on how replay protection is accomplished.]

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

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

D.1   ~~7.1~~ 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 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. The only parameter that shall be negotiated, is a 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.

[Note: It is ffs whether case 3 can actually occur.]

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 SM4. 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 SM4. 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 SM5 to be dropped at the P-CSCF IP(sec) layer due to a failed integrity check within ESP processing.

As SM5 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):
Open issues in SA3 tailored to CN1

This annex contains issues that need discussion and resolution related to the work performed by SA3 and CN1. When the technical content is stable and the TS33.203 is going for approval to SA this Annex will be removed.

The issues in the issue column are ~~questions~~ issues defined by CN1 or SA3~~and sent to SA3~~ for clarification. In the Status/Answer column the status ~~in SA3 or the answer to the question~~ is given.

Issue ID	Issue description	Source	Date	Answer from SA3	Status
S3#19-1	Security work for the ISC interface	S3-010404	SA3#19/July	Work just started.	Open
S3#19-2	Security needed for OSA API interface between HN and 3rd party providers	S3-010404	SA3#19/July	Work just started.	Open
S3#19-3	Can a call be terminated towards an IMPU that has not been registered?	S3-010404	SA3#19/July	Current understanding of SA3 is no. However this requirement should be stated by SA2 not SA3.	Closed/SA3#20/October
S3#19-4	Is it necessary to transport the KSI or similar in SIP-register messages.	S3-010404	SA3#19/July	This is FFS.	Open
S3#19-5	What SIP messages shall be authenticated?	S3-010404	SA3#19/July	(Re-)Registrations.	Closed/SA3#20/October
S3#19-6	Network hiding performed by the I-CSCF.	S3-010404	SA3#19/July	Work started. See also S3#19-9	Open
S3#19-7	Questions related to session transfer.	S3-010404	SA3#19/July	SA3 has sent an LS to GSM association, S3-010383. Work has started.	Open
S3#19-8	Discrepancy in time plans between CN1 and SA3	S3-010404	SA3#19/July	TS33.203 shall be ready March 2002.	Closed/SA3#20/October
S3#19-9	What is the due date for the WI on hiding?	S3-010339	SA3#19/July	Included in TS33.203 section 6.4. The TS stage 2 will be ready March 2002.	Closed/SA3#20/October
S3#19-10	Should the system be able to authenticate e.g. INVITEs and not be bound to the Registration procedure?	S3-010339	SA3#19/July	Authentication shall only take place at (re-)registrations	Closed/SA3#20/October
S3#19-11	At what layer does encryption take place?	S3-010339	SA3#19/July	Encryption is optional to implement. If used it shall be at the same layer as integrity protection. It is still open if SIP-level or IP-level.	Closed/SA3#20/October
S3#19-12	Hiding the callers IP-address: anonymity	S3-010339	SA3#19/July	For further study	Open
S3#21-1	According to CN1 requirement to generalize the flows e.g. 401(vs 407 discussion) and 403 have been changed to 4xx. SA3 wants to take part of the decision on which response shall be chosen.	S3-010410	SA3#20/October	For further study	Open
S3#21-2	How is IK and optionally CK transported?	S3-010xxx	SA3#21/October	For further study	Open

Annex X (informative):
Change history

It is usual to include an annex (usually the final annex of the document) for specifications under TSG change control which details the change history of the specification using a table as follows:

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2000-10	SA3#15bis	33.2xx		0.1.0	Initial version of the specification		
2000-11	SA3#16			0.1.1	Input from AdHoc meeting		
2001-03	SA3#17	33.203		0.2.0	Input from the SA3#17 meeting in Göteborg		
2001-04		33.203		0.2.1	Termination of confidentiality in the P-CSCF moved to an editors note. Kept the R'99 mechanism in the main document. Where to terminate is FFS.		
2001-05	SA3#17bis	33.203		0.3.0	Input from the SA3#17bis meeting in Madrid.		
2001-06	SA3#18	33.203		0.4.0	Input from the SA3#18 meeting in Phoenix.		
2001-08	SA3#19	33.203		0.5.0	Input from the SA3#19 meeting in Newbury.		
2001-09	SA3#19bis	33.203		0.6.0	Input from the SA3#19bis meeting in Nice		
2001-11	SA3#20	33.203		0.7.0	Input from the SA3#20 meeting in Sydney		
Editor Krister Boman, Ericsson							
Email: krister.boman@emw.ericsson.se							
Telephone: +46 31 747 6045 (Office)							
+46 70 987 6045 (Mobile)							