Technical Specification Group Services and System Aspects
Meeting #17, Biarritz, France, 9-12 September 2002

TSGS#17(02)0508

Source: **SA WG3**

Title: **11 CRs to 33.203 (Rel-5)**

Document for: **Approval**

Agenda Item: **7.3.3**

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-020508	33.203	012		Rel-5	SA handling when the UE changes IP address	F	5.2.0	IMS-ASEC	S3-020380
SP-020508	33.203	013		Rel-5	Removal of some editor notes in TS33.203	F	5.2.0	IMS-ASEC	S3-020383
SP-020508	33.203	014		Rel-5	Correction to S-CSCF behaviour on Network Authentication Failure	F	5.2.0	IMS-ASEC	S3-020407
SP-020508	33.203	015		Rel-5	Correcting the network behaviour in response to an incorrect AUT-S	F	5.2.0	IMS-ASEC	S3-020409
SP-020508	33.203	016		Rel-5	Mitigating reflection attacks in IMS	F	5.2.0	IMS-ASEC	S3-020411
SP-020508	33.203	017		Rel-5	Protect port number to be assigned by UE in re-registration	F	5.2.0	IMS-ASEC	S3-020412
SP-020508	33.203	018		Rel-5	One SA for both TCP and UDP sockets	F	5.2.0	IMS-ASEC	S3-020416
SP-020508	33.203	019		Rel-5	Correction of authentication vector distribution procedure	F	5.2.0	IMS-ASEC	S3-020419
SP-020508	33.203	020		Rel-5	The definition of the key to be used for HMAC-SHA1-96 within ESP	F	5.2.0	IMS-ASEC	S3-020435
SP-020508	33.203	021		Rel-5	Draft-ietf-sip-sec-agree syntax for manually keyed Ipsec	F	5.2.0	IMS-ASEC	S3-020436
SP-020508	33.203	022		Rel-5	Update of User Authentication Failure	F	5.2.0	IMS-ASEC	S3-020442

3GPP TSG-SA3 Meeting #24 ***S3-020380***
Helsinki, Finland, 9-12 July 2002

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.203** **CR** **012** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM [ ] ME/UE [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	SA handling when the UE changes IP address
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	2002-07-04
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	If the UE changes it's IP address for privacy reasons, then the UE shall initiate an unprotected Register message in order to establish new SA's between the UE and P-CSCF. The UE is no longer allowed to use any existing SA's.
Summary of change:	⌘	This CR proposes to clarify the UE behaviour in chapter 7.5, to state that the UE shall delete the existing SA's, before sending of the unprotected (SM1) Register message to the P-CSCF.
Consequences if not approved:	⌘	It's not clear in the UE implementation how the UE shall treat the existing SA's when the IP address is changed.

Clauses affected:	⌘	7.5
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

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

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

3GPP TSG-SA3 Meeting #24
Helsinki, Finland, 9-12 July 2002

S3-020383

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.203** **CR** **013** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Removal of some editor notes in TS33.203
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	2002-07-01
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change: ⌘ TS33.203 version 5.2.0 still contains a number of editor notes. It is proposed that the following editor notes are removed, with the following reasoning:

Chapter 4 contains an editor note regarding the UE Functionality split. As SA plenary #16 has concluded that no UE Functionality Split will take place in REL-5, we can remove this editor note.

Chapter 6.1.2 contains an editor note stating that chapter 6.1.2 shall handle requirements for network and user authentication failures. As this subsection already covers these requirements this editor note can be removed.

Chapter 6.1.2.2 contains an editor note which states that it is FFS whether the same header i.e. 4xx Auth_Failure shall be used for both UE and network authentication failure. The Editors Note can be removed, since what SIP header shall be used for UE and Network failures is not an issue for 33.203 to solve since it is specified in TS 24.229.

Chapter 6.1.3 contains an editor note stating that this subsection shall deal with requirements for the case when the SQNs in the ISIM and the HSS are not in synch. As this subsection already covers these requirements this editor note can be removed.

Chapter 8 contains an editor note stating that this section is based on the current working assumption in SA1 and SA2. As the ISIM concept and the re-use of R99/REL-4 USIM's for IMS has been agreed at the SA plenary, this chapter is no longer based on working assumptions and therefore this editor note can be removed.

Summary of change: ⌘ TS33.203 version 5.2.0 still contains a number of editor note's. This CR proposes to remove the majority of these note's based on the reasoning above.

Consequences if not approved: ⌘ A number of Editors Note will remain in TS33.203, which may lead the reader to incorrectly believe certain issues are still unresolved or based on outdated assumptions.

Clauses affected: ⌘ 4, 6.1.2, 6.1.2.2, 6.1.3, 8

Other specs affected: ⌘
☐ Other core specifications ⌘
☐ Test specifications
☐ O&M Specifications

Other comments: ⌘

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.

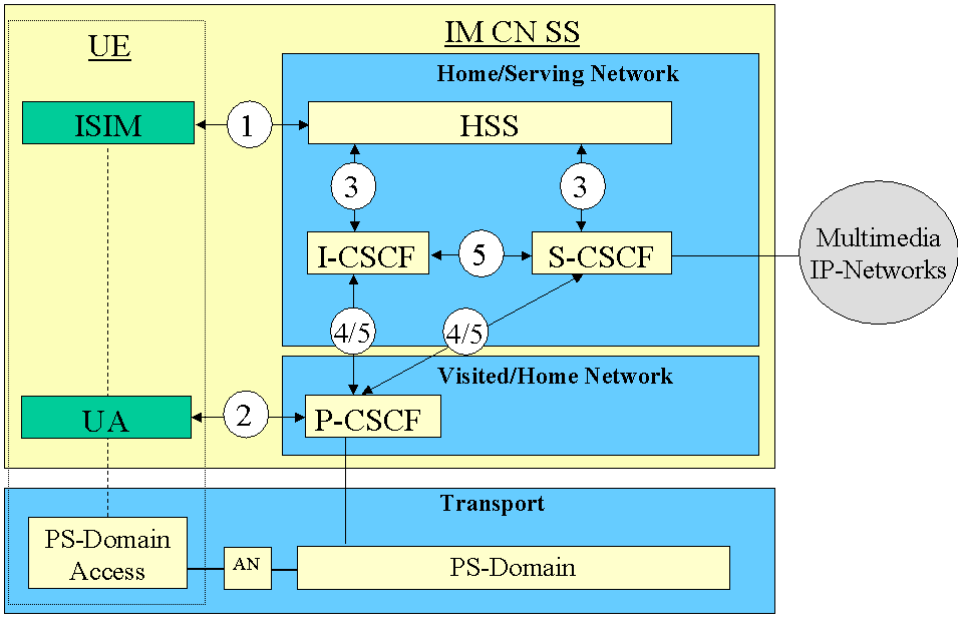


Figure 1: The IMS security architecture

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

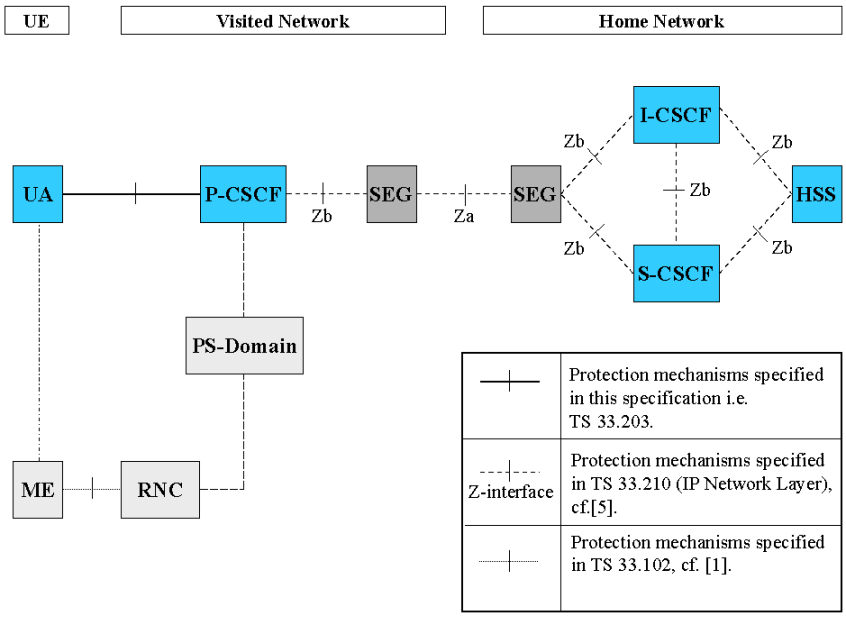


Figure 2: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the VN

P-CSCF in the Home Network

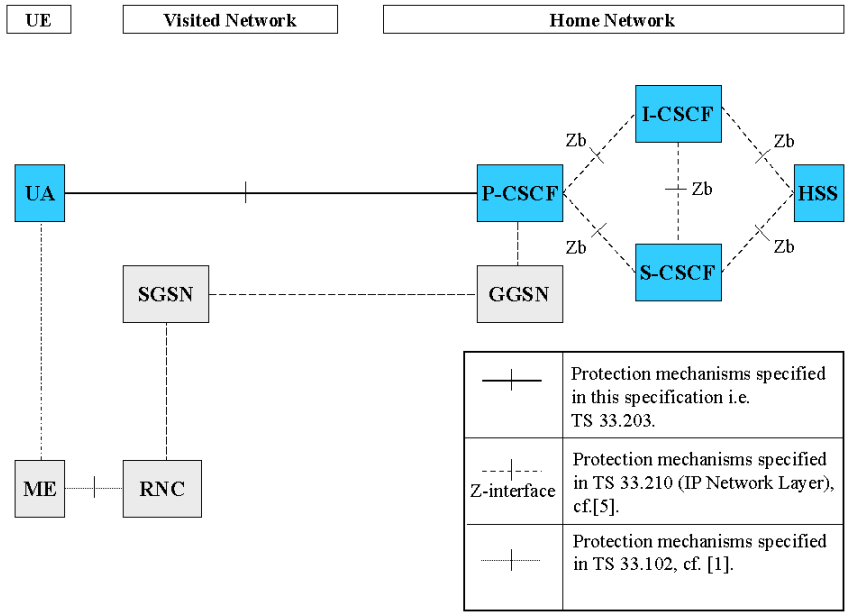


Figure 3: This figure gives an overview of the security architecture for IMS and the relation with Network Domain security, cf. TS 33.210 [5], when the P-CSCF resides in the HN

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).]~~

********** NEXT CHANGE **********

6.1.2 Authentication failures

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

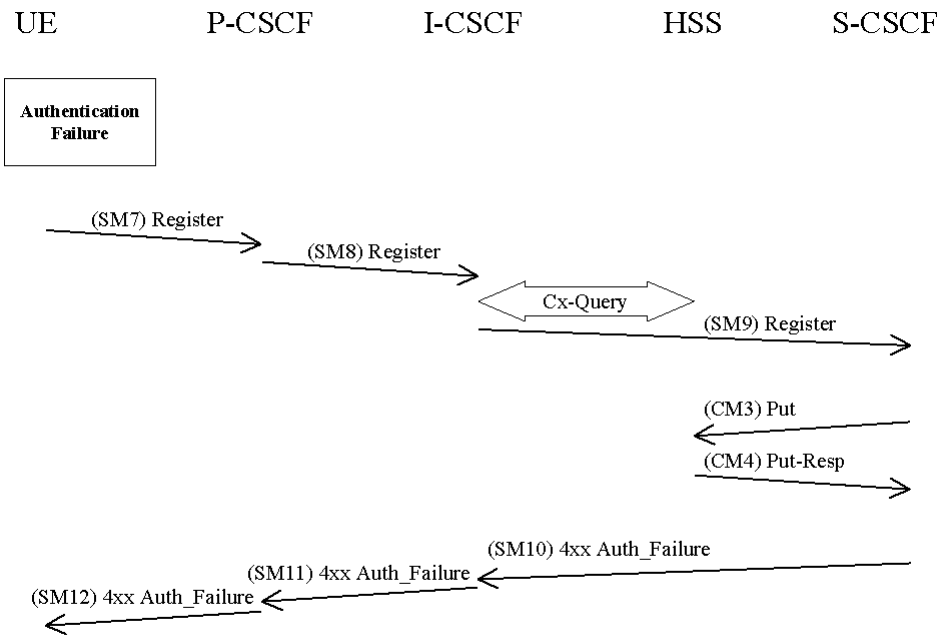
6.1.2.1 User authentication failure

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.

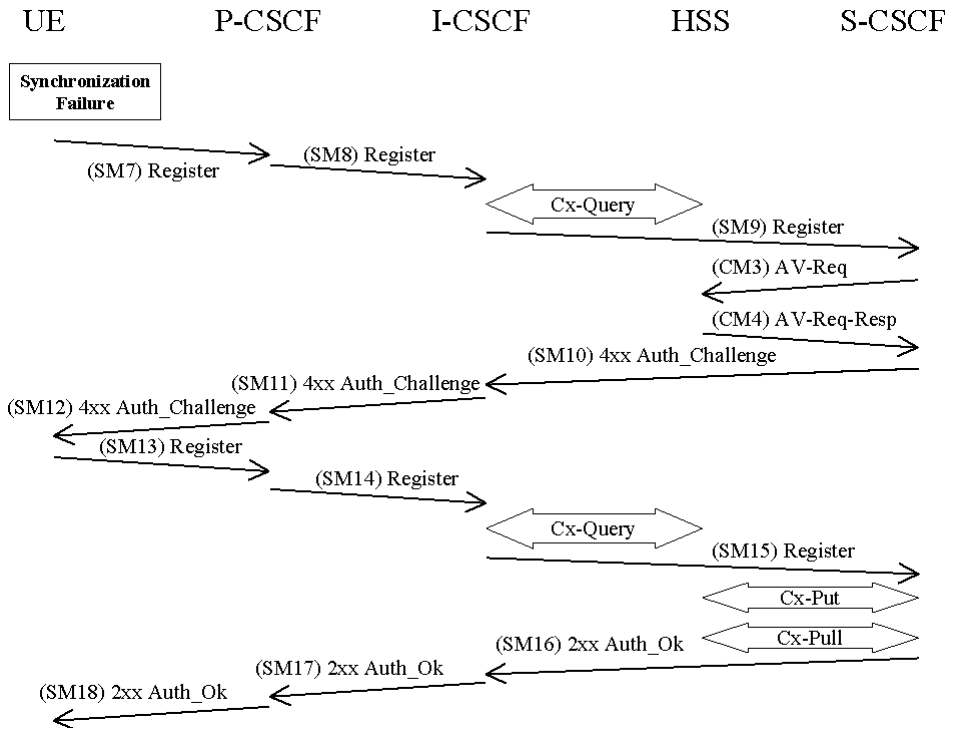
~~[Editor's note: It is FFS if same header i.e. 4xx Auth_Failure shall be used for both UE and network authentication failure.]~~

********** NEXT CHANGE **********

6.1.3 Synchronization failure

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

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



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

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

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

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

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

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

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

********** NEXT CHANGE **********

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.

3GPP TSG SA WG3 Security — S3#24 S3-020407

9 - 12 July 2002, Helsinki, Finland

CR-Form-v5

CHANGE REQUEST

⌘ **TS 33.203** **CR** **014** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Correction to S-CSCF behaviour on Network Authentication Failure
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	11/7/02
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

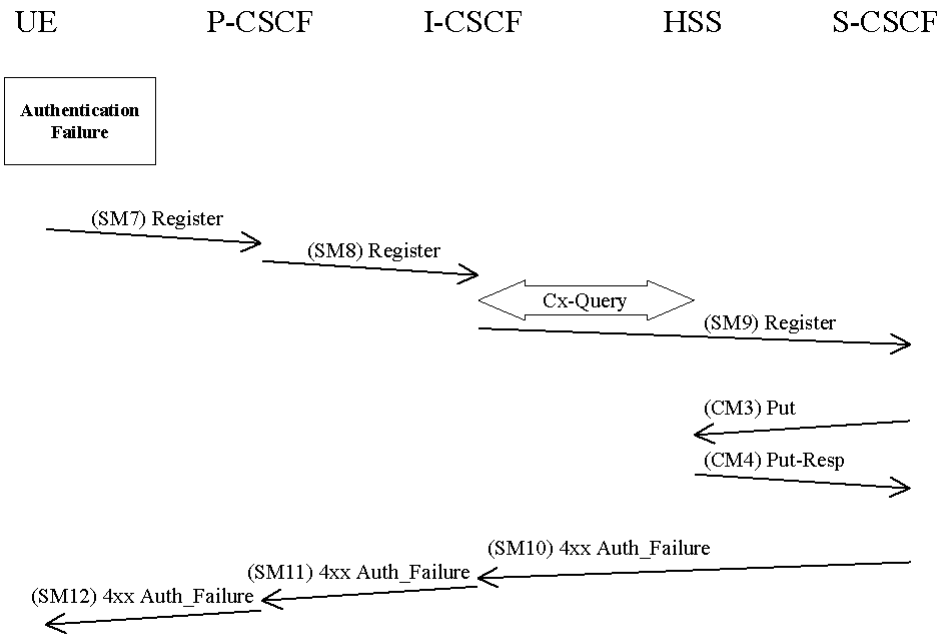
2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	Currently the S-CSCF de-registers the user on network authentication failure. This is not the desired behaviour as it allows an attacker to de-register a subscriber.
Summary of change:	⌘	The S-CSCF does not de-register the IMPU on network authentication failure if the IMPU is already registered.
Consequences if not approved:	⌘	An attacker could force an IMPU to be de-registered.

Clauses affected:	⌘	6.1.2.2
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

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 shall set the registration-flag in the HSS to *unregistered*, if the IMPU is not currently registered. To set the flag the S-CSCF sends in CM3 a Cx-Put to the HSS. ~~in CM3 and receives a Cx-Put-Resp in CM4.~~ If the IMPU is currently registered, the S-CSCF does not update the registration flag.

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

~~The 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 to CM3 with a Cx-Put-Resp in CM4.

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

SM10:
SIP/2.0 4xx Auth_Failure

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.]

3GPP TSG SA WG3 Security — S3#24 S3-020409

9 – 12 July 2002, Helsinki, Finland

CR-Form-v5

CHANGE REQUEST

⌘ **33.203** **CR** **015** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Correcting the network behaviour in response to an incorrect AUT-S		
Source:	⌘	SA WG3		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	11/7/02
Category:	⌘	**F**	***Release:*** ⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

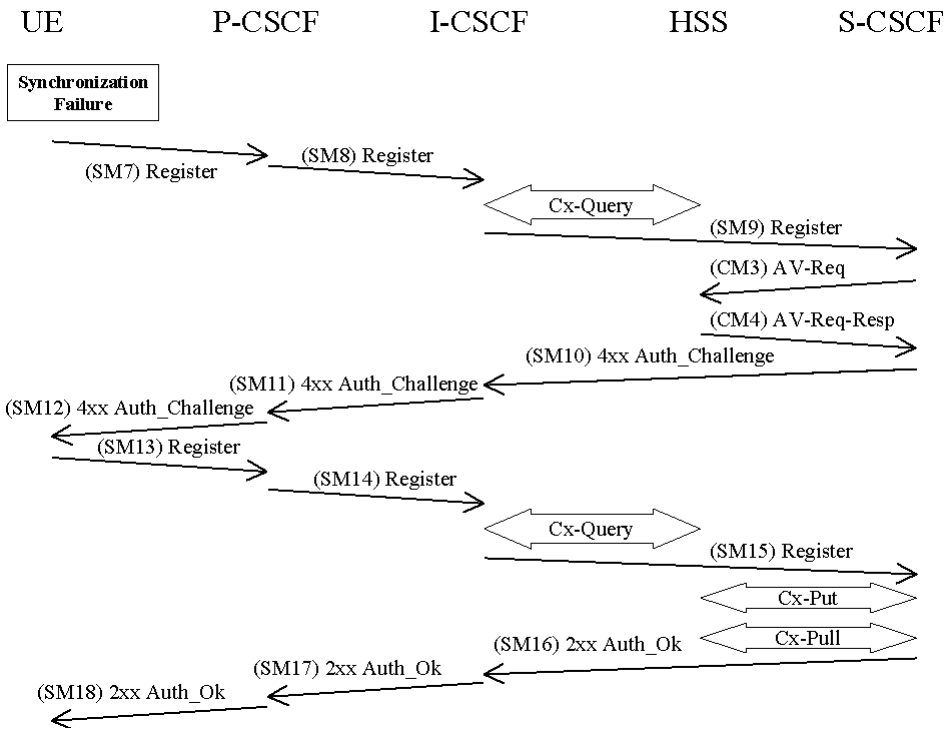
Reason for change:	⌘	Currently the text states the behaviour should follow the behaviour in TS 33.102. It also makes returning AVs conditional on a successful checking of AUTS. This is out of line with TS 33.102 which returns AVs regardless of whether AUTS was successful or not. The change is to align the behaviour of the specification with TS 33.102
Summary of change:	⌘	To make the HSS always return AVs whether the AUTS check is successful or not.
Consequences if not approved:	⌘	Inconsistency in the specification that could lead to incompatible implementations.

Clauses affected:	⌘	6.1.3		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

6.1.3 Synchronization failure

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

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



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

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

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

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

The HSS checks the AUTS as in section 6.3.5 in [1]. ~~If the check is successful and~~ After 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.

3GPP TSG-SA3 Meeting #24 **S3-020411**
Helsinki, Finland, Date

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.203** **CR** **016** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Mitigating reflection attacks in IMS
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	2002-07-05
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	The IPsec SPI is currently specified in TS33.203 to include a 'direction bit' in order to allow the use of one integrity key for both directions. However, this solution puts non-necessary restriction on implementations of IPsec. In particular, compatibility of the use of IPSEC including IKE would be restricted. One example is that the P-CSCF will handle SPIs differently in IMS towards the UE being compliant with the direction bit requirement in TS33.203 and towards other network nodes being compliant with NDS/IP i.e. TS 33.210. The same functionality with better compatibility to the IPSec use with IKE can be achieved by adding a rule to P-CSCF to check that the SPI values are not the same when the SIP Security Agreement is done.
Summary of change:	⌘	Two changes have been done: 1) The 'direction bit' from IPsec SPI has been removed. 2) A rule for P-CSCF to check that the SPI values are not the same when the same key is used for both directions has been added.
Consequences if not approved:	⌘	It is required to implement different behaviour in the P-CSCF for IPSec towards UE compared with IPSec towards other network elements. Also the UE may be impacted in a similar fashion. The SPI will no longer have only local significance which is breaking the definition of the SPI in RFC 2401.

Clauses affected:	⌘	7.1 and 7.2		
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	TS24.229
Other comments:	⌘			

7.1 Security association parameters

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

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

- **Integrity algorithm**

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

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

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

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

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

- **SPI (Security Parameter Index)**

The SPI is allocated locally for inbound SAs. The triple (SPI, destination IP address, security protocol) uniquely identifies an SA at the IP layer. The UE shall select the SPIs uniquely, and different from any SPIs that might be used in any existing SAs (i.e. inbound and outbound SAs). The SPIs selected by the P-CSCF shall be different than the SPIs sent by the UE, cf. section 7.2.~~The most significant bit of any SPI allocated by the P-CSCF shall be "0" and the most significant bit of any SPI allocated by the UE shall be "1".~~

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

The following SA parameters are not negotiated:

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

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

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

Selectors:

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

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

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

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

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

- The transport protocol is either TCP or UDP.

- Ports:

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

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

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

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

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

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

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

   - responses to unprotected REGISTER messages;

   - error messages.

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

The following rules apply:

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

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

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

3. The SIP application at the P-CSCF shall check upon receipt of an initial REGISTER message that, for each transport protocol, the triple (UE_IP_address, UE_protected_port, transport protocol), where the UE_IP_address is the source IP address in the packet header and the protected port is sent as part of the security mode set-up

procedure (cf. clause 7.2), has not yet been associated with entries in the "SA_table". Furthermore, the P-CSCF shall check that, for any one IMPI, no more than three SAs per direction and per transport protocol are stored at any one time. If these checks are unsuccessful the registration is aborted and a suitable error message is sent to the UE.

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

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

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

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

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

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

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

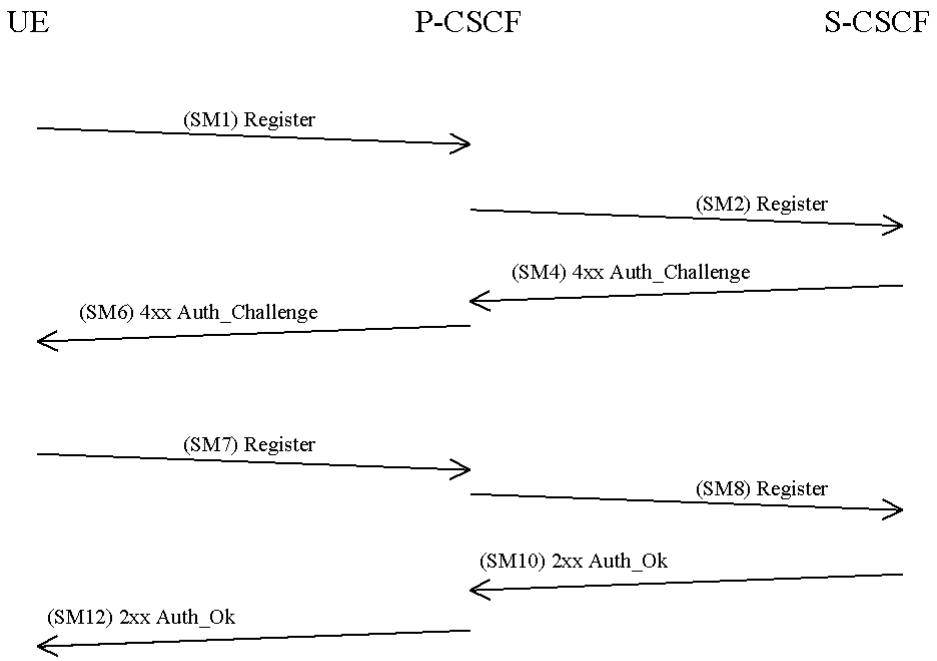
NOTE 12: If the integrity check of a received packet fails then IPsec will automatically discard the packet.

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

7.2 Set-up of security associations (successful case)

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

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



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

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

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

Upon receipt of SM1, the P-CSCF temporarily stores the parameters received in the *Security-setup-line* together with the UE's IP address from the source IP address of the IP packet header, the IMPI and IMPU. Upon receipt of SM4, the P-CSCF adds the key IK_{IM} received from the S-CSCF to the temporarily stored parameters. The P-CSCF then selects the SPIs for the inbound SAs for TCP and UDP. The P-CSCF shall define the SPIs such that they are unique and different from any SPIs as received in the *Security-setup-line* from the UE. Note that this rule is needed since the UE and the P-CSCF use the same key for inbound and outbound traffic.

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

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

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

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

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

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

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

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

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

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

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

3GPP TSG SA WG3 Security — S3#23 **S3-020412**
9 - 12 July 2002
Helsinki, Finland

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **017** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Protect port number to be assigned by UE in re-registration
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	04/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	The current specification only specifies the SA negotiation procedure when UE is challenged and new SA is to be established. It should further specify UE's behavior in re-registration procedure if UE is not be challenged and therefore no new SA is to be established.
Summary of change:	⌘	To clarify UE's behavior during re-registraiton that new port number must be assigned by UE and communicated to the P-CSCF, preparing a new SA is to be established.
Consequences if not approved:	⌘	Implementation may assume no port number need to be assigned if no new SA is to be established.

Clauses affected:	⌘	7.1

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 24.228, 24.229
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

7.1 Security association parameters

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

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

- **Integrity algorithm**

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

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

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

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

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

- **SPI (Security Parameter Index)**

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

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

The following SA parameters are not negotiated:

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

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

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

Selectors:

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

- IP addresses are bound to a pair of SAs, as in clause 6.3, as follows:
  - inbound SA at the P-CSCF:
    The source and destination IP addresses associated with the SA are identical to those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

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

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

- The transport protocol is either TCP or UDP.

- Ports:

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

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

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

3. For each security association, the UE assigns a port to send or receive protected messages to and from the P-CSCF ("protected port"). No unprotected messages shall be sent to or received on this port. The UE may use different protected port numbers for TCP and UDP. The numbers of these ports are communicated to the P-CSCF during the security mode set-up procedure, cf. clause 7.2. When the UE sends a re-REGISTER request, it shall always pick up a new port number and send it to the network. If the UE is not challenged by the network, the port number shall be obsolete. Annex H of this specification gives detail how the port number is populated in SIP message. From a security point of view, the UE may send or receive unprotected messages to or from the P-CSCF on any ports which are not protected ports.

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

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

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

   - responses to unprotected REGISTER messages;

   - error messages.

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

The following rules apply:

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

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

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

3. The SIP application at the P-CSCF shall check upon receipt of an initial REGISTER message that, for each transport protocol, the triple (UE_IP_address, UE_protected_port, transport protocol), where the UE_IP_address is the source IP address in the packet header and the protected port is sent as part of the security mode set-up procedure (cf. clause 7.2), has not yet been associated with entries in the "SA_table". Furthermore, the P-CSCF

shall check that, for any one IMPI, no more than three SAs per direction and per transport protocol are stored at any one time. If these checks are unsuccessful the registration is aborted and a suitable error message is sent to the UE.

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

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

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

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

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

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

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

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

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

3GPP TSG SA WG3 Security — S3#23 **S3-020416**
9 - 12 July 2002
Helsinki, Finland

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **018** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	One SA for both TCP and UDP sockets
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	11/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The current specification requires two SAs to be established for UDP and TCP each in either direction. This design permits a SPI number modification attack investigated in Tdoc S3-020384. The design also introduces confliction with SIP behaviour defined in RFC3261.
Summary of change:	⌘	The new text specifies that two sockets share always the same SA for the same direction.
Consequences if not approved:	⌘	• The SPI number modification attack may be allowed, • It can not achieve SIP requirement, • It makes the SA management too complicated, • The resource is half wasted in both UE and P-CSCF.

Clauses affected:	⌘	7.1, 7.2

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		TS 24.228, 24.229
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

7.1 Security association parameters

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

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

- **Integrity algorithm**

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

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

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

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

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

- **SPI (Security Parameter Index)**

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

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

The following SA parameters are not negotiated:

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

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

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

Selectors:

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

- IP addresses are bound to a pair of SAs, as in clause 6.3, as follows:
  - inbound SA at the P-CSCF:
    The source and destination IP addresses associated with the SA are identical to those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

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

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

- The transport protocol is either TCP or UDP.

- Ports:

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

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

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

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

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

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

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

   - responses to unprotected REGISTER messages;

   - error messages.

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

The following rules apply:

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

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

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

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

are stored at any one time. If these checks are unsuccessful the registration is aborted and a suitable error message is sent to the UE.

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

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

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

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

6. When establishing ~~two~~ a new pair~~s~~ of SAs (cf. clause 6.3) the SIP application at the UE shall ensure that~~, for each transport protocol,~~ the selected number for the protected port, as well as SPI number, doe~~s~~ not correspond to an entry in the "SA_table".

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

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

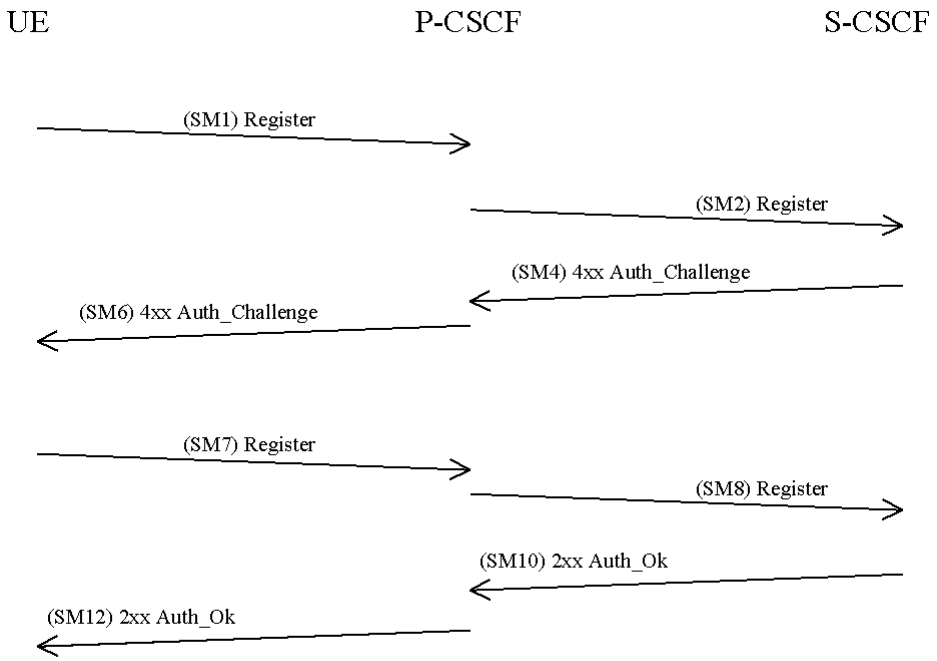
NOTE 12: If the integrity check of a received packet fails then IPsec will automatically discard the packet.

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

7.2 Set-up of security associations (successful case)

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

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



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

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

SM1:
REGISTER(Security-setup = *SPI_U_~~TCP, SPI_U_UDP~~, Port_U_~~TCP, Port_U_UDP~~, UE integrity algorithms list)*

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

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

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

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

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

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

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

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

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

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

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

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

3GPP TSG-SA WG3 Security Meeting #24
Helsinki, Finland, 9-12 July 2002

Tdoc ⌘S3-020419

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **019** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Correction of authentication vector distribution procedure.
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	05/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The requirement that the number of IMS authentication vectors supplied by the HSS is exactly the same as the number requested by the S-CSCF is too restrictive.
Summary of change:	⌘	The authentication vector distribution procedure is changed so that the number of IMS authentication vectors supplied by the HSS need not be exactly the same as the number requested by the S-CSCF.
Consequences if not approved:	⌘	The HSS is unable to supply fewer authentication vectors than the number requested by the S-CSCF.

Clauses affected:	⌘	6.1.1, 6.1.3

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

6.1.1 Authentication of an IM-subscriber

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

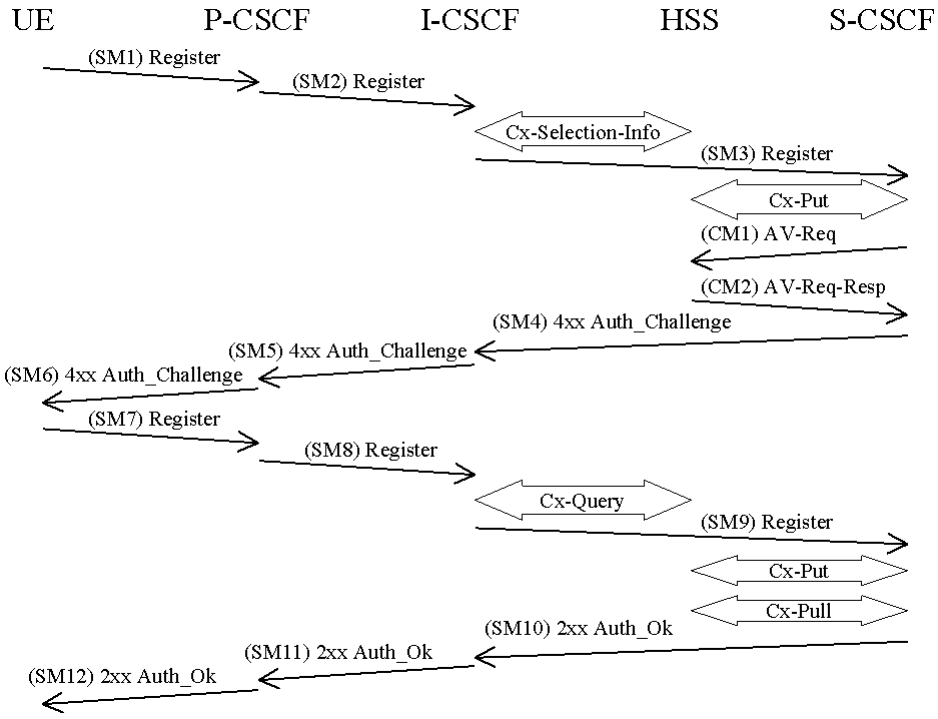


Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

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

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

SM1:
REGISTER(IMPI, IMPU)

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

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

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

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

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

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

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

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

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

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

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

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

Upon receiving the challenge, SM6, the UE takes the AUTN, which includes a MAC and the SQN. The UE calculates the XMAC and checks that XMAC=MAC and that the SQN is in the correct range as in [1]. If both these checks are successful the UE calculates the response, RES, puts it into the Authorization header and sends it back to the registrar in SM7. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of the response. It should be noted that the UE at this stage also computes the session keys CK and IK.

SM7:
REGISTER(IMPI, RES)

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

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

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

When an IMPU has been registered this registration will be valid for some period of time. Both the UE and the S-CSCF will keep track on a timer for this purpose but the expiration time in the UE is smaller than the one in the S-CSCF in order to make it possible for the UE to be registered and reachable without interruptions. A successful registration of a previously registered IMPU (including implicitly registered IMPUs) means the expiry time of the registration is refreshed.

It should be noted that the UE initiated re-registration opens up a potential denial-of-service attack. That is, an attacker could try to register an already registered IMPU and respond with the wrong RES and in order to make the HN de-

register the IMPU. For this reason a subscriber should not be de-registered if it fails an authentication. It shall be defined by the policy of the operator when successfully registered IMPU(s) are to be de-registered.

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

6.1.2 Authentication failures

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

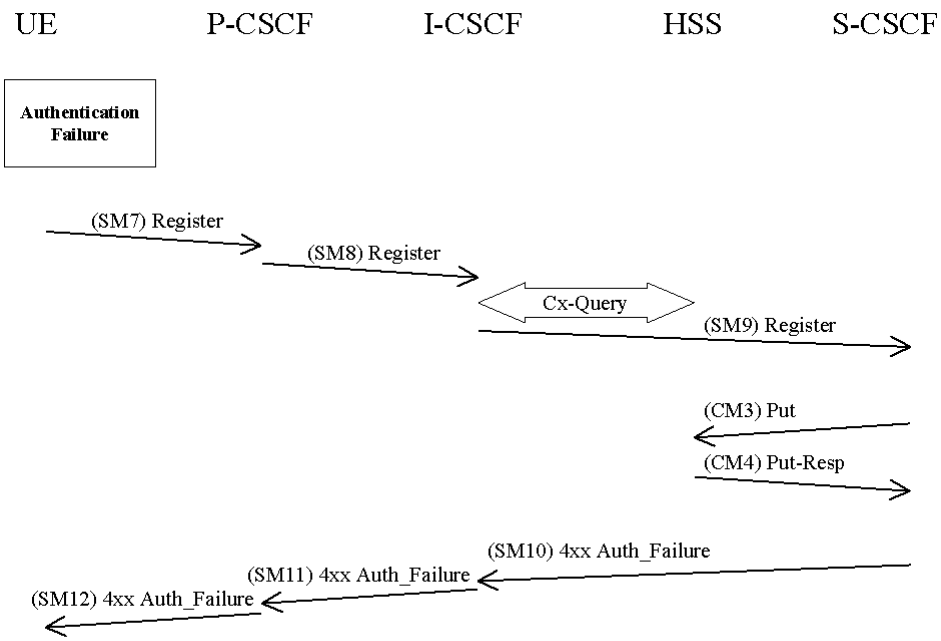
6.1.2.1 User authentication failure

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

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

6.1.2.2 Network authentication failure

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



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

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

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

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

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

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

SM10:
SIP/2.0 4xx Auth_Failure

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

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

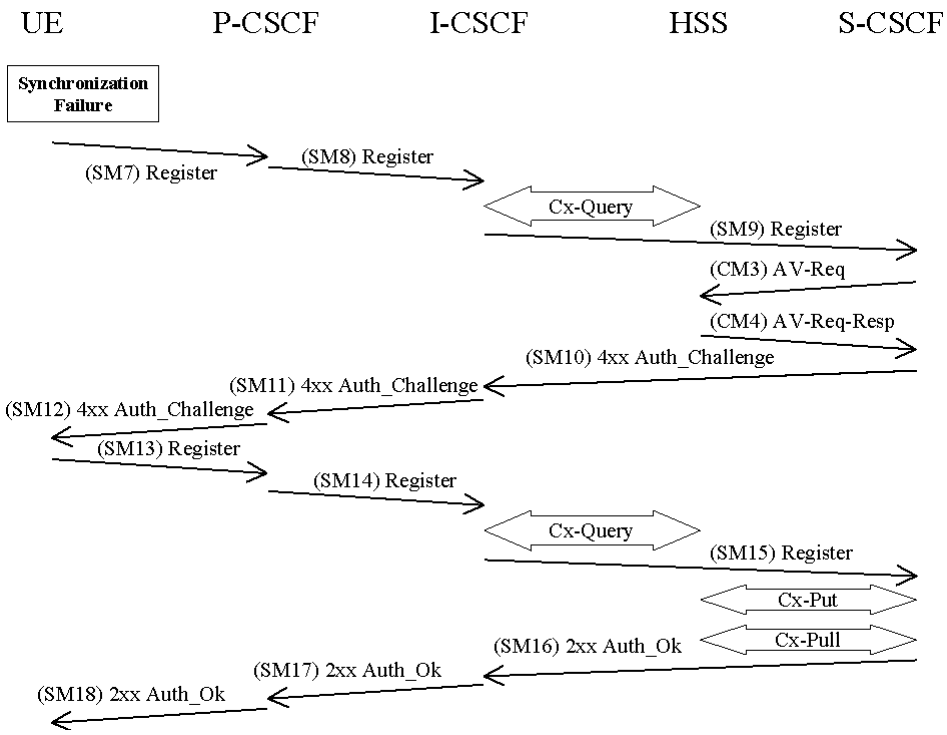
6.1.2.3 Incomplete authentication

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

6.1.3 Synchronization failure

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

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



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

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

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

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

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.

3GPP TSG-SA3 Meeting #24
Helsinki, Finland, 9-12 July 2002

S3-020435

CR-Form-v5

CHANGE REQUEST

⌘ **33.203** **CR** **020** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	The definition of the key to be used for HMAC-SHA1-96 within ESP
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	July 10 2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	Create conformity with IETF RFC 2104
Summary of change:	⌘	Specifies how to expand IK from 128 bits to 160 bits
Consequences if not approved:	⌘	TS 33.203 will not follow the principles as specified in IETF RFC 2104

Clauses affected:	⌘	Annex I
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

********** FIRST CHANGED SECTION **********

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

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

If the selected authentication algorithm is HMAC-SHA-1-96 then IK_{ESP} is obtained from IK_{IM} by appending ~~the 32 most significant bits~~32 zero bits ~~of IK_{IM}~~ to the end of IK_{IM} to create a 160-bit string.

3GPP TSG-SA3 Meeting #24 ***S3-020436***
Helsinki, Finland, Date

CR-Form-v5.1

CHANGE REQUEST

⌘ **33.203** **CR** **021** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Draft-ietf-sip-sec-agree syntax for manually keyed IPsec
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	2002-07-04
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	[draft-ietf-sip-sec-agree] does not have detail on how it will be used with manually keyed IPsec. For this missing information, 33.203 has an empty annex (H) to be included later. This CR proposes text for annex H.
Summary of change:	⌘	This document defines the syntax for [draft-ietf-sip-sec-agree] so that the mechanism can be used to negotiate IPsec security associations. The syntax is defined in annex H. Some additions and editorial changes to the references are also included.
Consequences if not approved:	⌘	Security mode setup procedure will not work before the exact syntax of the [draft-ietf-sip-sec-agree] for manually keyed IPsec is defined.

Clauses affected:	⌘	2, Annex H
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[20] IETF RFC 2405 (1998) "The ESP DES-CBC Cipher Algorithm With Explicit IV".

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

~~[To be added]~~

The BNF syntax of [draft-ietf-sip-sec-agree] is defined for negotiating security associations for manually keyed IPsec in the following way:

security-client = "Security-Client" HCOLON sec-mechanism *(COMMA sec-mechanism)

security-server = "Security-Server" HCOLON sec-mechanism *(COMMA sec-mechanism)

security-verify = "Security-Verify" HCOLON sec-mechanism *(COMMA sec-mechanism)

sec-mechanism = mechanism-name *(SEMI mech-parameters)

mechanism-name = "ipsec-man"

mech-parameters = (preference / algorithm / protocol / mode / encrypt-algorithm / spi / port1 / port2 / transport)

preference = "q" EQUAL qvalue

qvalue = ("0" ["." 0*3DIGIT]) / ("1" ["." 0*3("0")])

algorithm = "alg" EQUAL ("hmac-md5-96" / "hmac-sha-1-96" / "null")

protocol = "prot" EQUAL ("ah" / "esp")

mode = "mod" EQUAL ("trans" / "tun")

encrypt-algorithm = "ealg" EQUAL ("des-cbc" / "null")

spi = "spi" EQUAL spivalue

spivalue = 10DIGIT; 0 to 4294967295

port1 = "port1" EQUAL port

port2 = "port2" EQUAL port

port = 1*DIGIT

transport = "transport" EQUAL ("TCP" / "UDP")

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

Mechanism-name: For manually keyed IPsec, this field includes the value “ipsec-man”.

Preference: As defined in [draft-ietf-sip-sec-agree].

Algorithm: If present, defines the authentication algorithm. May have a value “hmac-md5-96” for algorithm defined in [15], “hmac-sha-1-96” for algorithm defined in [16] or “null” if authentication is not used. If no Algorithm parameter is present, the algorithm will be “null”.

Note: According to clause 7.1 the “null” algorithm is not allowed for use in IMS.

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

Note: According to clause 6 only “esp” is allowed for use in IMS.

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

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

Encrypt-algorithm: If present, defines the encryption algorithm. May have a value “des-cbc” for algorithm defined in [20] or “null” if encryption is not used. If no Encrypt-algorithm parameter is present, the algorithm will be “null”.

Note: According to clause 6.2 no encryption is provided in IMS i.e. only Encrypt-algorithm “null” is allowed for use in IMS.

Spi: Defines the SPI number used for inbound messages.

Note: The SPI number will be used for outbound messages for the entity which did not generate the “spi” parameter

Port1: Defines the port number for inbound messages

Port2: Defines the port number for outbound messages. If no Port2 parameter is present port1 is also used for outbound messages.

Note: According to clause 7.1, Port2 parameter is not used in IMS.

Transport: If present, defines the transport layer protocol. May have a value “TCP” for TCP, or value “UDP” for UDP. If not present, any transport protocol can be used (cf. transport = “wildcard” as in [14]).

3GPP TSG SA WG3 Security — S3#24 S3-020442

9 - 12 July 2002, Helsinki, Finland

CR-Form-v5

CHANGE REQUEST

⌘ 33.203 CR 022 ⌘ rev - ⌘ Current version: 5.2.0 ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Update of User Authentication Failure
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	12/7/02
Category:	⌘	F
Release:	⌘	Rel-5

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	The text is updated to account for using Digest AKA, as RES is no longer directly checked. It also describes what to do if the integrity protection passes and the response fails.
Summary of change:	⌘	The text is changed to make it the authentication response that is checked as opposed to the RES. It also describes what happens in the unlikely circumstances that the integrity check passes but the response fails.
Consequences if not approved:	⌘	The text will not reflect the use of Digest AKA to carry the authentication response. No behaviour will be described in the unlikely event that the integrity check passes but the authentication response fails. Both issues could lead to incorrect implementations.

Clauses affected:	⌘	6.1.2, 6.1.2.1
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

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

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

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