

CR-Form-v7

## CHANGE REQUEST

# **33.203** CR **CRNum** # 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

<b>Title:</b>	# Correction of authentication vector distribution procedure.		
<b>Source:</b>	# Vodafone		
<b>Work item code:</b>	#	<b>Date:</b>	# 05/07/2002
<b>Category:</b>	# <b>F</b>	<b>Release:</b>	# Rel-5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	<b>F</b> (correction)	<b>2</b> (GSM Phase 2)	
	<b>A</b> (corresponds to a correction in an earlier release)	<b>R96</b> (Release 1996)	
	<b>B</b> (addition of feature),	<b>R97</b> (Release 1997)	
	<b>C</b> (functional modification of feature)	<b>R98</b> (Release 1998)	
	<b>D</b> (editorial modification)	<b>R99</b> (Release 1999)	
	Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<b>Rel-4</b> (Release 4)
			<b>Rel-5</b> (Release 5)
			<b>Rel-6</b> (Release 6)

<b>Reason for change:</b>	# 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.
<b>Summary of change:</b>	# 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.
<b>Consequences if not approved:</b>	# The HSS is unable to supply fewer authentication vectors than the number requested by the S-CSCF.

<b>Clauses affected:</b>	# 6.1.1, 6.1.3										
<b>Other specs affected:</b>	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="width: 20px; text-align: center;">#</td> <td style="width: 20px; text-align: center;">#</td> </tr> <tr> <td style="width: 20px; text-align: center;">#</td> <td style="width: 20px; text-align: center;">#</td> </tr> <tr> <td style="width: 20px; text-align: center;">#</td> <td style="width: 20px; text-align: center;">#</td> </tr> </table>	Y	N	#	#	#	#	#	#	Other core specifications	#
Y	N										
#	#										
#	#										
#	#										
		Test specifications	#								
		O&M Specifications	#								
<b>Other comments:</b>	#										

**How to create CRs using this form:**

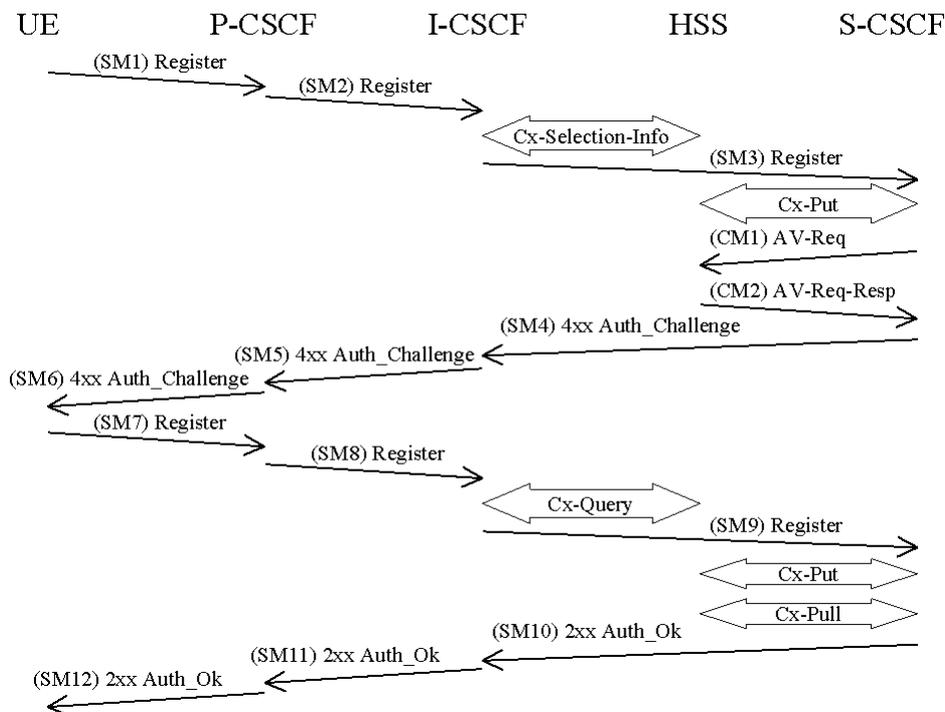
Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked # contain pop-up help information about the field that they are closest to.

- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/>. For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

### 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 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.]

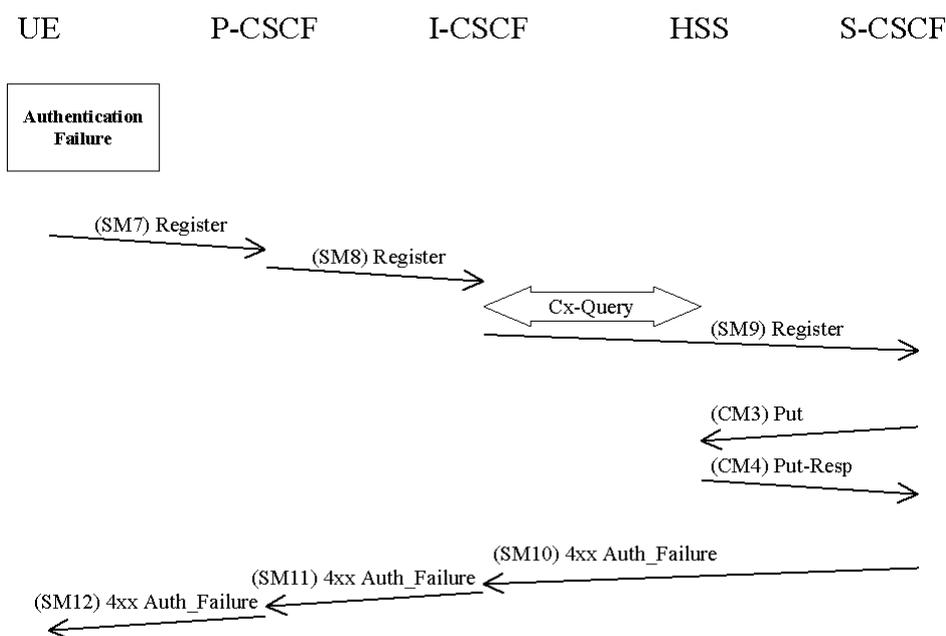
### 6.1.2.1 User authentication failure

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*, IMPU)

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.]

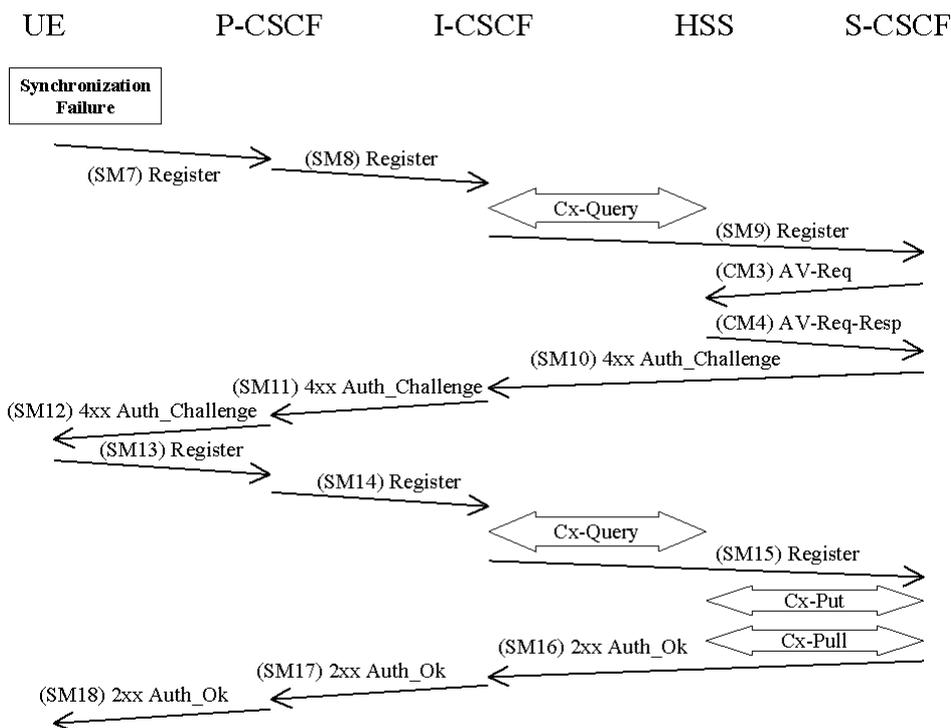
### 6.1.2.3 Incomplete authentication

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,  $n$ .

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<sub>1</sub>||AUTN<sub>1</sub>||XRES<sub>1</sub>||CK<sub>1</sub>||IK<sub>1</sub>,...,RAND<sub>n</sub>||AUTN<sub>n</sub>||XRES<sub>n</sub>||CK<sub>n</sub>||IK<sub>n</sub>)

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.