3GPP TSG-SA-WG3 Meeting #31
18th – 21st November 2003, Munich, Germay

Tdoc ⌘S3-030713

CR-Form-v7

CHANGE REQUEST

⌘	TS 33.203	CR	CRNum	⌘rev	-	⌘	Current version:	6.0.0	⌘

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 [X]

Title:	⌘	Ensuring the correct RAND is used in synchronization failures
Source:	⌘	**3**, Nokia, Vodafone, Ericsson
Work item code:	⌘	IMS-ASEC
Date:	⌘	10/11/2003
Category:	⌘	A
Release:	⌘	Rel-6

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:	⌘	It is essential that the S-CSCF stores the RAND sent to the UE and passes this RAND back to the HSS in case of a synchronization failure. If the RAND passed back by the UE (in the Digest AKA nonce field) is used by the S-CSCF, it allows an attacker to store a RAND and AUTS combination and replay them at a later date. This stored pair of RAND and AUTS will be acccepted by the HSS as a valid indication of a synchronization error. In some scenarios the sequence number for that subcriber may be altered. This may result in a synchronization failure the next time the real UE tries to authenticate to the network. The S-CSCF storing RAND and using this in case of synchronization failure avoids the possibility of replay of synchronization failures. Note: this is not a problem for UMTS as RAND is not returned by the UE in this case.
Summary of change:	⌘	It is clarified that the RAND sent to the UE is stored by the S-CSCF and subsequently sent to the HSS when there is a synchronization failure.
Consequences if not approved:	⌘	If the RAND returned by the UE is sent to HSS, it allows a replay of synchronization failures.

Clauses affected:	⌘			6.1.1, 6.1.3		
		Y	**N**			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 24.229, TS 29.228
			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.

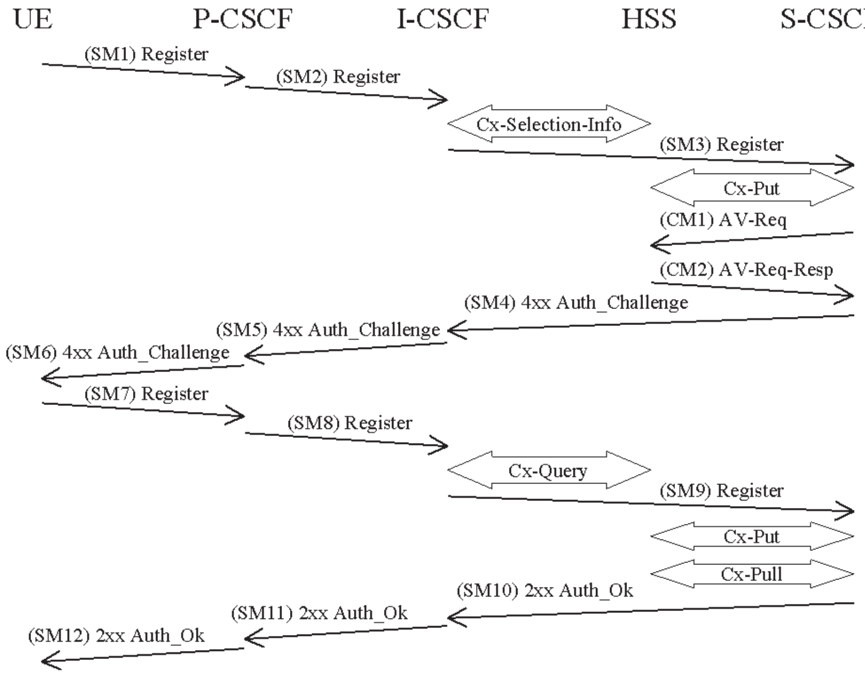


Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

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 m of AVs wanted where m is at least one.

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

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

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

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

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

The verification of the SQN by the USIM and ISIM will cause the UE to reject an attempt by the S-CSCF to re-use a AV. Therefore no AV shall be sent more than once.

NOTE: This does not preclude the use of the normal SIP transaction layer re-transmission procedures.

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

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

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

Upon receiving the challenge, SM6, the UE takes the AUTN, which includes a MAC and the SQN. The UE calculates the XMAC and checks that XMAC=MAC and that the SQN is in the correct range as in [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).

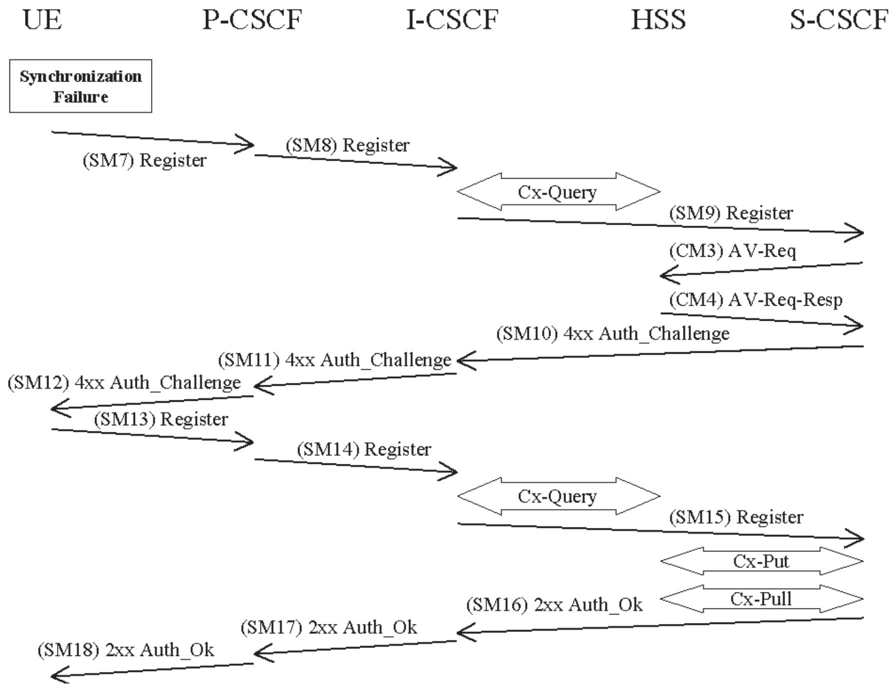
When an IMPU has been registered this registration will be valid for some period of time. Both the UE and the S-CSCF will keep track on a timer for this purpose but the expiration time in the UE is smaller than the one in the S-CSCF in order to make it possible for the UE to be registered and reachable 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].

6.1.3 Synchronization failure

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 RAND stored by the S-CSCF and the required number of Avs, m.

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

The HSS checks the AUTS as in section 6.3.5 in [1]. After potentially updating the SQN, the HSS sends new AVs to the S-CSCF in CM4.

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

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.