3GPP TSG-SA3 Meeting #28 **Tdoc ⌘S3-030229**

Berlin, Germany, 6-9 May 2003

CR-Form-v7

CHANGE REQUEST

⌘	**33.203**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	**5.5.0** ⌘

*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:	⌘	UA behavior in Network authentication failures		
Source:	⌘	Nokia		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	28/04/2003
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 RFC 3310 does not contain the indication of authentication failure. This is because SIP convention does not send response to another response. The change allows the UE to handle this case the same way as any incomplete authentications specified in further chapter, thus the state machines in both terminal and the network side are simplified.
Summary of change:	⌘	A new behavior of UA is proposed in Network authentication failure scenario. UE passively ignores the false challenge due to the failure of the MAC checking.
Consequences if not approved:	⌘	The current specificaton is not workable with SIP message.

Clauses affected:	⌘	6.1.2, 7.3.1.2				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	24.229
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

6.1.2 Authentication failures

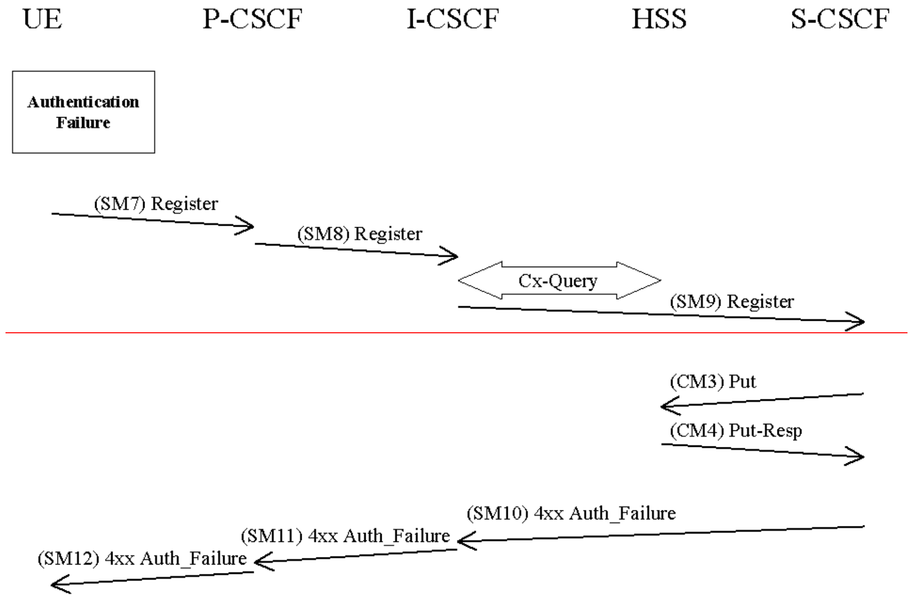
6.1.2.1 User authentication failure

In this case the authentication of the user should fail at the S-CSCF due an incorrect response (received in SM9). However, if the response is incorrect, then the IK used to protect SM7 will normally be incorrect as well, which will normally cause the integrity check at the P-CSCF to fail before the response can be verified at S-CSCF. In this case SM7 is discarded by the IPsec layer at the P-CSCF.

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)~~.

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 section 6.1.1 up to SM6. However, the UE shall abort the registration attempt when identifying a wrong MAC value in the AUTN~~A~~N. The UE may start a completely new registration procedure as specified in section 6.1.1, if it still requires any IM services.



~~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. 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 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~~

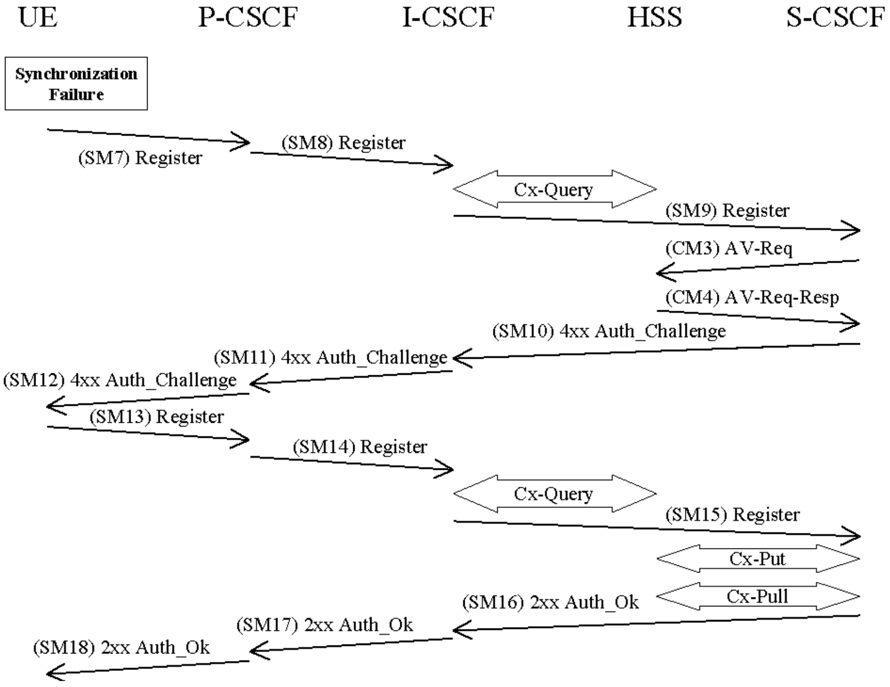
~~Upon receiving SM10 the I-CSCF shall clear any registration information related to the IMPI.~~

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. Similar as the scenario described in section 6.1.2.2, the UE may start a completely new registration procedure as specified in section 6.1.1.

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 required number of Avs, m.

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

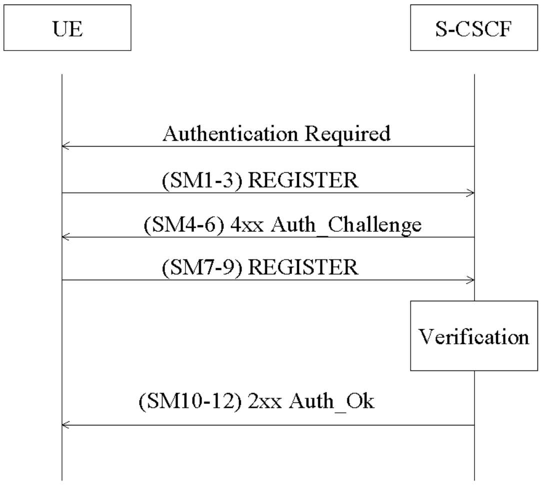
The HSS checks the AUTS as in section 6.3.5 in [1]. After potentially updating the SQN, the HSS sends new AVs to the S-CSCF in CM4.

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.

6.1.4 Network Initiated authentications

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



Both the UE and the P-CSCF shall shorten the lifetime of the old SA pair generated from the last successful authentication, so as to guarantee that the new SA pair shall be used.
The UE shall initiate the re-registration on the reception of the Authentication Required indication. In the event that the UE does not initiate the re-registration procedure after the request from the S-CSCF, the S-CSCF may decide to de-register the subscriber or re-issue an Authentication-Required.

6.1.5 Integrity protection indicator

In order to decide whether a REGISTER request from the UE needs to be authenticated, the S-CSCF needs to know about the integrity protection applied to the message. The P-CSCF attaches an indication to the REGISTER request to inform the S-CSCF that the message was integrity protected if:

- the P-CSCF receives a REGISTER containing an authentication response and the message is protected with the SA created during this authentication procedure; or

- the P-CSCF receives a REGISTER not containing an authentication response and the message is protected with the SA created by latest successful authentication (from the P-CSCF perspective).

For all other REGISTER requests the P-CSCF attaches an indication that the REGISTER request was not integrity protected or ensures that there is no indication about integrity protection in the message.

******* THE NEXT CHANGE******

7.3 Error cases in the set-up of security associations

7.3.1 Error cases related to IMS AKA

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

7.3.1.1 User authentication failure

In this case, SM7 fails integrity check by IPsec at the P-CSCF if the IK_{IM} derived from RAND at UE is wrong. The SIP application at the P-CSCF never receives SM7. It shall delete the temporarily stored SA parameters associated with this registration after a time-out.
In case IK_{IM} was derived correctly, but the response was wrong the authentication of the user fails at the S-CSCF due to an incorrect response. The S-CSCF will send a 4xx Auth_Failure message to the UE, via the P-CSCF, which may pass through an already established SA. Afterwards, both, the UE and the P-CSCF delete the new SAs.

7.3.1.2 Network authentication failure

If the UE is not able to successfully authenticate the network, the UE shall passively abort the attempt ~~send a REGISTER message which may pass through an already established SA, indicating a network authentication failure, to the P-CSCF~~. The P-CSCF deletes the new SAs when request is time out ~~after receiving this message.~~. The UE may start another registration procedure if it still requires any IM services.

7.3.1.3 Synchronisation failure

In this situation, the UE observes that the AUTN sent by the network in SM6 contains an out-of-range sequence number. The UE shall send a REGISTER message to the P-CSCF, which may pass through an already established SA, indicating the synchronization failure. The P-CSCF deletes the new Sas after receiving this message.

7.3.1.4 Incomplete authentication

If the UE responds to an authentication challenge from a S-CSCF, but does not receive a reply before the request times out, the UE shall start a registration procedure if it still requires any IM services. The first message in this registration should be protected with an SA created by a previous successful authentication if one exists.
If the P-CSCF deletes a registration SA due to its lifetime being exceeded, the P-CSCF should delete any information relating to that registration procedure.

7.3.2 Error cases related to the Security-Set-up

7.3.2.1 Proposal unacceptable to P-CSCF

In this case the P-CSCF cannot accept the proposal set sent by the UE in the Security-Set-up command of SM1. The P-CSCF shall respond to SM1 indicating a failure, by sending an error response to the UE.

7.3.2.2 Proposal unacceptable to UE

If the P-CSCF sends in the security-setup line of SM6 a proposal that is not acceptable for the UE, the UE shall terminate the registration procedure.

7.3.2.3 Failed consistency check of Security-Set-up lines at the P-CSCF

The P-CSCF shall check whether authentication algorithms list received in SM7 is identical with the authentication algorithms list sent in SM6. If this is not the case the registration procedure is aborted. (Cf. clause 7.2).