3GPP TSG SA WG3 Security — S3#19 **S3-010382**

4 - 6 July, 2001

Newbury, UK

Source: **TSG-SA WG3**

To: **SA2, CN1, CN4**
Cc:

Title: **Flows related to Authenticated Registrations and Re-Registrations**

Contact: Krister Boman, Ericsson
Email: krister.boman@emw.ericsson.se

SA3 is currently developing the signaling flows for authenticating an IMS subscriber in the S-CSCF.
In the Annex to this LS a flow, which is based on a contribution to this meeting (S3-010355), is given as an example. Although an example the flow contains the essentials valid for this liaison statement. The example assumes that the user has not yet been registered and that the authentication is successful. The example was discussed at S3#19 in the presence of CN1 delegates. During the discussion the following question arose:

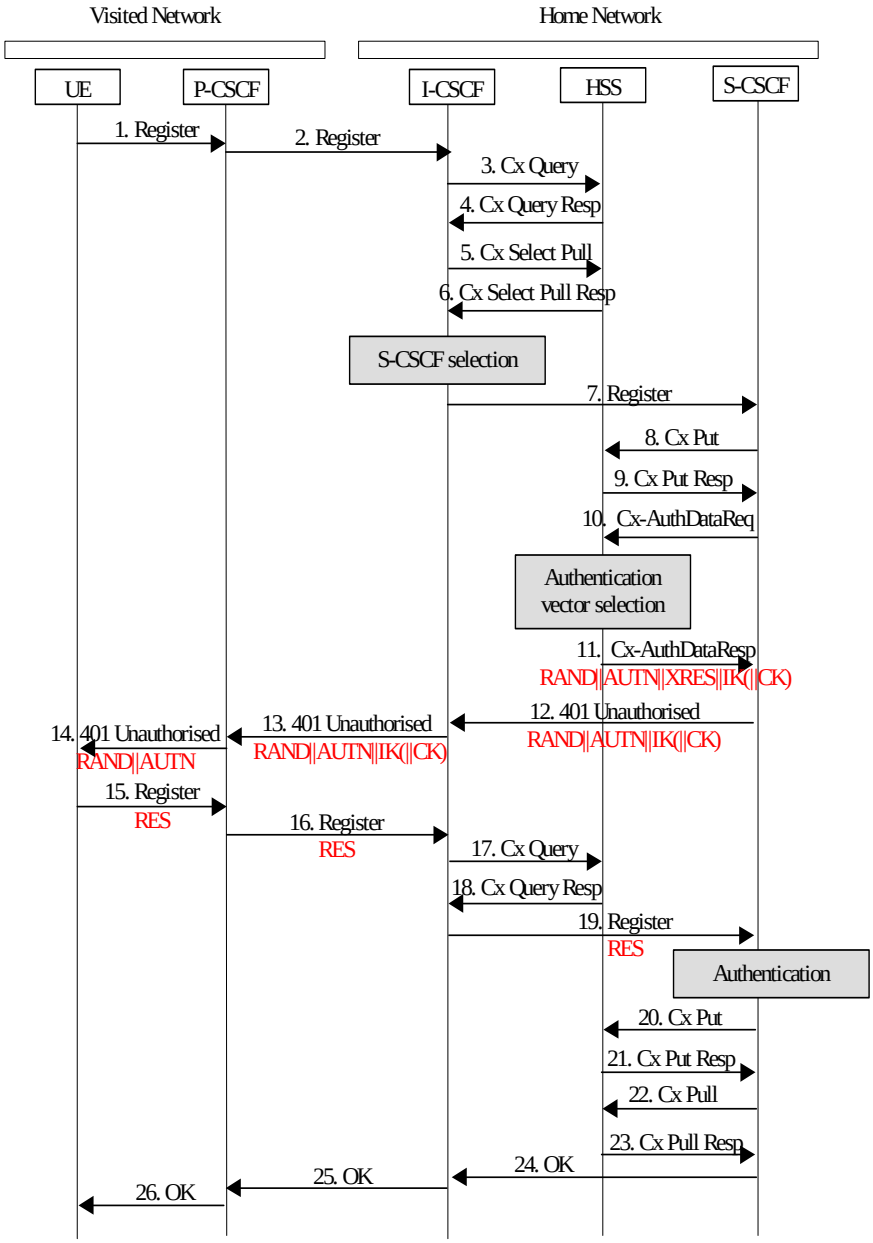
When the user is sending his/her first REGISTER message an S-CSCF will be selected by the I-CSCF. In Step 8 the S-CSCF will send a Cx-Put to the HSS. Here it is now assumed by SA3 that the HSS will store the name of the S-CSCF for future use, *S1* say. At Step 10 the S-CSCF will request authentication vector(s) from the HSS which contain the authentication challenge(s). Note that, as an optimization, more than one authentication vector may be sent to the S-CSCF.

The S-CSCF forwards one authentication challenge towards the user, who then sends an authentication response back at Step 15. At Step 17 the I-CSCF sends a Cx-Query to the HSS which should respond with the address of the already chosen S-CSCF i.e. *S1*. It is fundamental for the current solution that SA3 is working on that the I-CSCF at Step 18 can get access to *S1* without performing a new selection process where potentially a new S-CSCF might be chosen.

Furthermore since at Step 10 the S-CSCF i.e. *S1* may require more than one authentication vector it is important that when a user re-registers that the S-CSCF is not changed i.e. the user is re-registered in *S1.* Otherwise it does note make sense to send more than one authentication vector to *S1*. Moreover, it appears that it may then happen that the user is registered at two S-CSCFs at the same time, possibly with the same public identity. Also, it is the understanding of SA3 that re-registrations can be performed during ongoing SIP sessions. In case a change of S-CSCF was possible in a re-registration SA3 would appreciate an explanation of how the ongoing SIP session would be handled.

S3 would be pleased if SA2, CN1 and CN4 could confirm that the working assumptions described above are compliant with the requirements and the models currently agreed on in SA2, CN1 and CN4 and corresponding specifications.

1 Annex



Description of the Information flow:

Up to message 7 the information flow does not differ from the one without security given in [3G TS 23.228, section 5.2.2.3].

8. The S-CSCF shall send *Cx-Put* (subscriber identity, S-CSCF name) to the HSS, which includes a flag which indicates to the HSS that registration is in progress. The HSS stores the S-CSCF name for that subscriber together with this flag. (The flag is needed for the handling of mobile terminated calls while registration is still in progress, see below.)
9. The HSS shall send *Cx-Put Resp* to the I-CSCF to acknowledge the sending of *Cx-Put.*
10. The S-CSCF shall send a request for authentication data *Cx-AuthDataReq* to the HSS.
    The HSS selects an authentication vector with user specific authentication data *RAND||AUTN||XRES||IK(||CK).*
    Note, that it is a working assumption within S3 that confidentiality protection is optional for implementation in UMTS. However, we included *CK* in the information flow for reasons of access network independence. (Other access networks may require encryption at the SIP level.) *CK* is included in brackets in order to indicate that it is only optional.
11. In an *Cx-AuthDataResp* message the HSS shall send the authentication vector *RAND||AUTN||XRES||IK(||CK)* to the S-CSCF.

Note, that it is also possible to send a batch of pre-computed authentication vectors to the S-CSCF, if desired. This could facilitate that in re-registrations authentication steps 10 and 11 of the information flow could be omitted.

It is up to the IMS provider if he makes use of this option and how many authentication vectors he sends in one batch. There is no need to standardise a policy for the handling of authentication vectors in the S-CSCF which are still unused. This is up to the IMS provider.

12. The S-CSCF shall send an *401 Unauthorised* message to the I-CSCF in order to indicate that the registration requested by the UA needs to be authenticated. This message shall contain the concatenation of *RAND*, *AUTN* , *IK* and optionally *CK*.
13. The I-CSCF shall forward the received message (including the concatenation of *RAND*, *AUTN*, *IK* and if included in the previously received message also *CK*) to the P-CSCF.
14. The P-CSCF shall send an *401 Unauthorised* message which contains the concatenation of *RAND* and *AUTN* to the UE.
15. The UE shall check *AUTN*, compute the authentication response *RES* and send *RES* in a *Register* message to the P-CSCF.
16. The P-CSCF shall forward the received message (including the parameter *RES*) to the I-CSCF.
17. The I-CSCF sends a *Cx-Query* to the HSS.
18. The HSS sends a *Cx-QueryResp* to the I-CSCF with the address of the S-CSCF.
19. The I-CSCF shall forward the received *Register* message (including the parameter *RES*) to the S-CSCF.
    The S-CSCF authenticates the user by checking if the received value *RES* and the stored value *XRES* are equal. If yes, then the UA is successfully authenticated.
20. The S-CSCF shall send *Cx-Put* (subscriber identity, S-CSCF name) to the HSS, which includes a flag that indicates to the HSS that registration was successful. The HSS stores the S-CSCF name for the subscriber together with this flag.
21. The HSS shall send *Cx-Put Resp* to the I-CSCF to acknowledge the sending of *Cx-Put.*
22. The S-CSCF shall send the *Cx-Pull* message (subscriber identity) to the HSS in order to be able to download the relevant information from the subscriber profile to the S-CSCF. The S-CSCF shall store the P-CSCFs name, as supplied by the visited network. This represents the name that the home network forwards the subsequent terminating session signalling to for the UE.
23. The HSS shall return the *Cx-Pull Resp* message (user information) to the S-CSCF. The user information passed from the HSS to the S-CSCF shall include one or more names/addresses [and] information which can be used to access the platform(s) used for service control while the user is registered at this S-CSCF. The S-CSCF shall store the information for the indicated user.
24. The S-CSCF shall determine whether the home contact name is the S-CSCF name or an I-CSCF name. If an I-CSCF is chosen as the home contact name, it may be distinct from the I-CSCF that appears in this registration flow. The home contact name will be used by the P-CSCF to forward signalling to the home network. The S-CSCF shall return the *200 OK* message (serving network contact name, S-CSCF name) to the I-CSCF.
25. The I-CSCF shall send *200 OK* (serving network contact name) to the P-CSCF. The I-CSCF shall release all registration information after sending *200 OK*.
26. The P-CSCF shall store the serving network contact name, and shall send *200 OK* to the UE.