3GPP TSG SA WG3 Security — S3#18 **S3-010209**

21 - 24 May, 2001

Phoenix, USA

3GPP TSG-SA WG2 #18 ***Tdoc S2-011528***
14-18 May, 2001
Puerto Rico

Title: **LS on the termination of authentication in the IMS**

Source: **3GPP TSG SA2**

To: **3GPP TSG SA3**

Cc: **3GPP TSG CN1**

Work Item: **IMS-CCR**

Contact Person:
Name: Balazs Bertenyi, Nokia
E-mail Address: balazs.bertenyi@nokia.com

At SA3#17 meeting in Göteborg SA3 has decided that authentication of an IM-subscriber shall take place in the Home Network. It was left for further study if the HSS or the S-CSCF should perform the authentication. The issue was addressed in the last SA3 ad hoc meeting on SIP in Madrid, but no compelling security arguments were found to bias the solution towards either the HSS or S-CSCF terminating user authentication.

SA2 would like to kindly inform SA3 that it has discussed the two alternatives during SA2#18, and has agreed in principle that subscriber authentication shall be performed in the S-CSCF.

Information flows for subscriber's registration and re-registration with authentication terminating in the S-CSCF are presented below for information only, and the details of which have not been examined within the S2 discussions. S2 does not plan to include authentication flows within the S2 specifications.

Authenticated registration

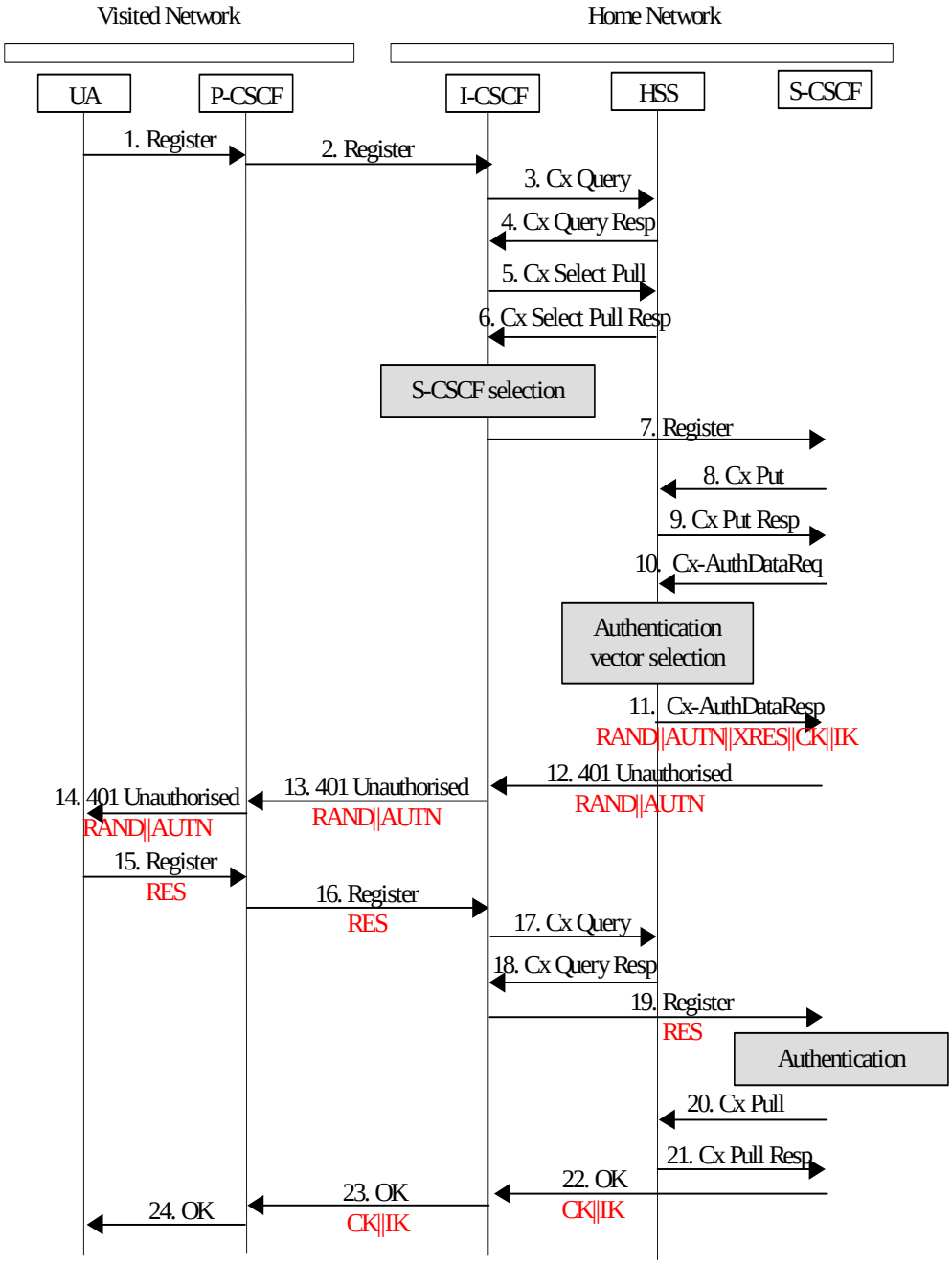


Figure 2.1: Authenticated registration

Description of the Information flow:

Up to message 9 the information flow does not differ from the one without security given in [3G TS 23.228], section 5.3.

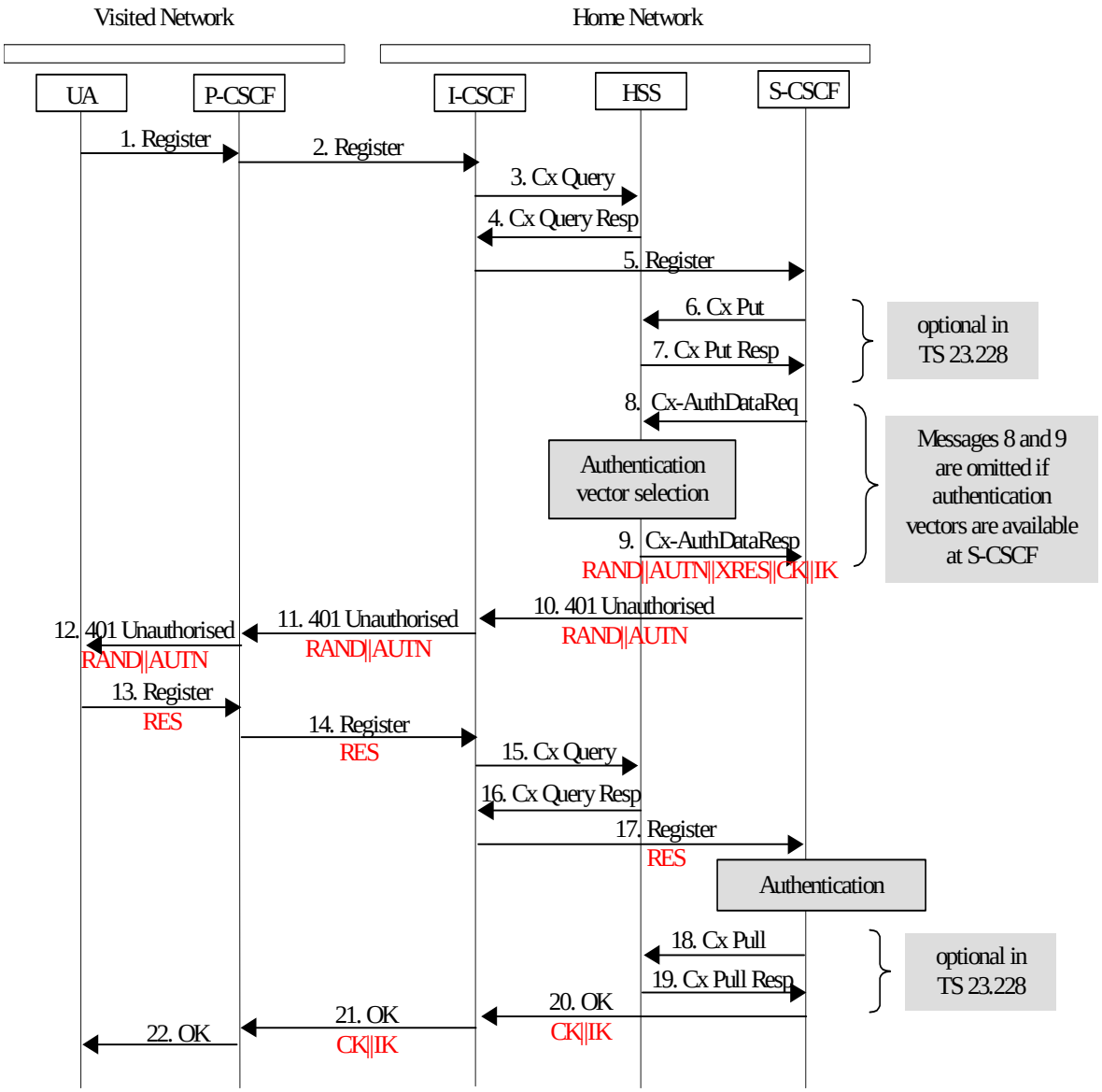
8. The S-CSCF sends a *Cx-Put* to the HSS.
9. The HSS stores the association between subscriber identity and S-CSCF address and sends back a *Cx-Put Resp*.
10. The S-CSCF sends a request for authentication data *Cx-AuthDataReq* to the HSS.
    The HSS selects an authentication vector with user specific authentication data *RAND||AUTN||XRES||CK||IK*.
    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.)
11. In an *Cx-AuthDataResp* message the HSS sends the authentication vector *RAND||AUTN||XRES||CK||IK* 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.

12. The S-CSCF sends 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 contains the parameters *RAND* and *AUTN* which are needed for authentication purposes in the UA.
13. The I-CSCF forwards the received message (including the parameters *RAND* and *AUTN*) to the P-CSCF.
14. The P-CSCF forwards the received message (including the parameters *RAND* and *AUTN*) to the UA.
15. The UA checks *AUTN*, computes the authentication response *RES* and sends *RES* in a Register message to the P-CSCF.
16. The P-CSCF forwards 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 forwards 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. S-CSCF sends a *Cx-Pull* to the HSS.
21. The HSS sends a *Cx-Pull Resp* to the S-CSCF.
22. The S-CSCF indicates to the I-CSCF that authentication was successfully completed by sending an *OK* message, which includes the session keys *IK* for integrity protection and *CK* for confidentiality protection of SIP signalling.
23. The I-CSCF forwards the received message (including the keys *IK and CK*) to the P-CSCF.
24. The P-CSCF sends an *OK* to the UA (which does not include the keys *IK and CK*).

Authenticated re-registration

Below an information flow for IMS re-registration is shown where the S-CSCF terminates IMS authentication. We do not give a description of the re-registration feature, as it is very similar to registration which is in detail described in the section above.
According to [TS 23.228, section 5.2.2.4] in figure 2.2 below messages 6 and 7, but also messages 18 and 19 are optional for re-registration. They can be omitted if "as an optimisation, the S-CSCF can detect that this is a re-registration" [quote from TS 23.228].
If authentication vectors are available at the S-CSCF (i.e. if a batch of authentication vectors was sent with a previous registration) then messages 8 and 9 of the re-registration procedure can also be omitted. It would therefore be possible that the HSS has only to be contacted by the I-CSCF.
If this optimisation could be also applied then in the case that authentication vectors are already available at the S-CSCF, the HSS would not be part of the information flow at all. Note that re-registration is likely to be used much more frequently than the registration feature.


Visited Network
Home Network
UA
P-CSCF
I-CSCF
HSS
S-CSCF
1. Register
2. Register
3. Cx Query
4. Cx Query Resp
5. Register
6. Cx Put
7. Cx Put Resp
optional in TS 23.228
8. Cx-AuthDataReq
Authentication vector selection
9. Cx-AuthDataResp
RAND||AUTN||XRES||CK||IK
Messages 8 and 9 are omitted if authentication vectors are available at S-CSCF
10. 401 Unauthorised
RAND||AUTN
11. 401 Unauthorised
RAND||AUTN
12. 401 Unauthorised
RAND||AUTN
13. Register
RES
14. Register
RES
15. Cx Query
16. Cx Query Resp
17. Register
RES
Authentication
18. Cx Pull
19. Cx Pull Resp
optional in TS 23.228
20. OK
CK||IK
21. OK
CK||IK
22. OK