3GPP TSG SA WG3 Security — S3#19 **S3-010355**

4 - 6 July, 2001

London, UK

Source: **Siemens AG**

Title: **Information flows for IMS authentication and key agreement**

Document for: **Discussion / Decision**

Agenda Item: **7.3, IP multimedia subsystem security**

Abstract

This contribution proposes information flows for an authenticated IMS registration and re-registration with the S-CSCF as termination point for authentication. The proposal includes flows for a successful authentication as well as in cases with failure conditions.

1 Introduction

~~□~~At S3#18 (Phoenix, USA, 21 - 24 May, 2001) 3G SA3 decided to confirm the decision of S2#18 that 3G S2 preferred the authentication to terminate in the S-CSCF.

This document provides the appropriate information flows, including those for successful authentication for registration and re-registration, but also those for cases with failure conditions.

For the different flows optimisation options are described. They are only mentioned here in order to show possibilities for optimisation. They are not meant to be included into [3G TS 33.203], as a corresponding decision is not the responsibility of SA 3.

~~2.1~~2 Authenticated registration – User not registered

Information flows have to be provided for an authenticated IMS registration in the case that authentication is successful, but also for all possible failure conditions, i.e. user authentication failure, network authentication failure and synchronisation failure.

2.1 Authenticated registration with successful authentication

Figure 1 provides the information flow for IMS registration of a previously unregistered user in case that authentication is successful.

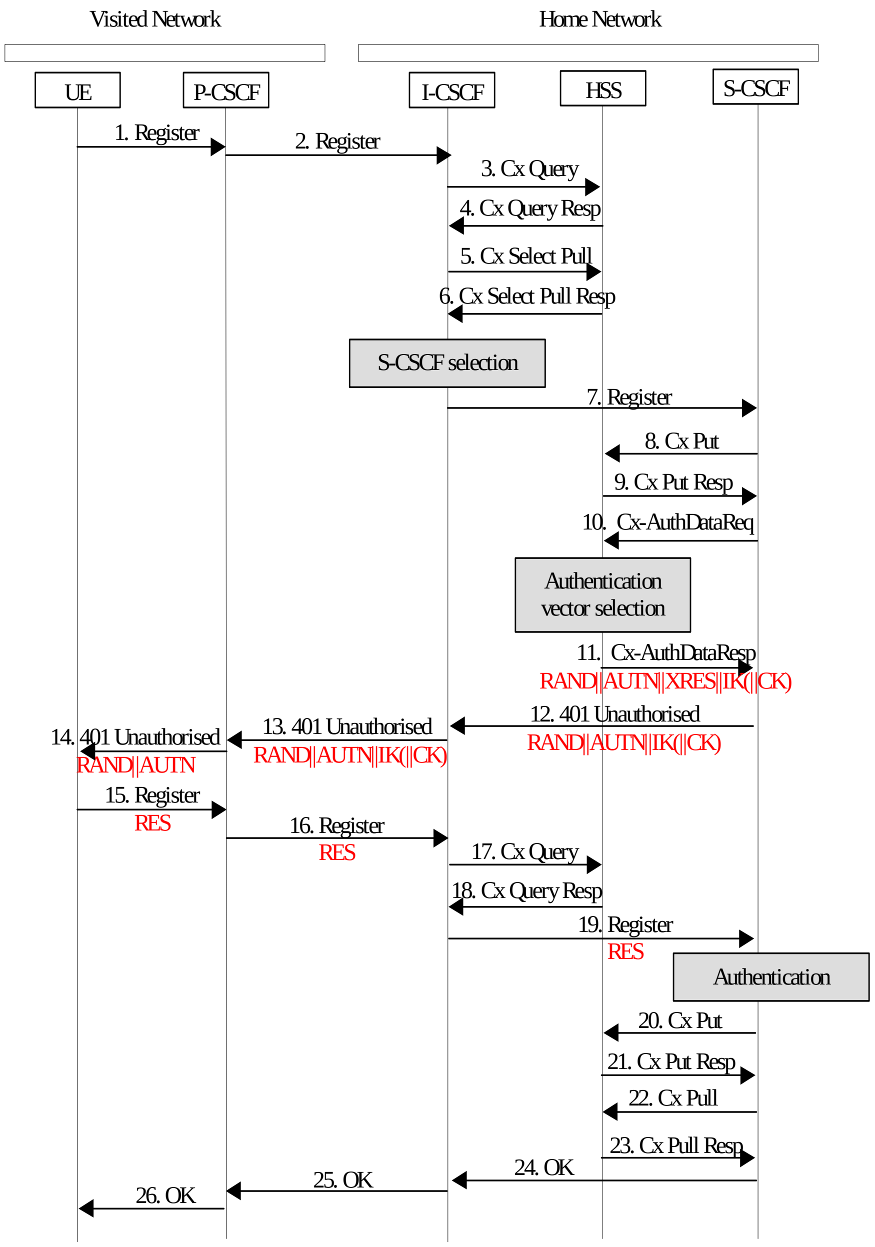

Figure 1: Authenticated registration, authentication successful

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.*

~~20.~~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.

~~21.~~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.

~~23.~~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*.

~~24.~~26. The P-CSCF shall store the serving network contact name, and shall send *200 OK* to the UE.

Optimisation of the information flow

In order to optimise the information flow it may be optionally allowed to omit messages 17 and 18, if the I-CSCF receives information from which the I-CSCF can derive the previously selected S-CSCF in a way other than through a request to the HSS. This may e.g. be facilitated by sending the appropriate information in the *401 Unauthorised* messages from the S-CSCF to the P-CSCF or to the UE. The S-

CSCF may send this information in message 12 by using a cookie mechanism or by using an extension in the SIP header or in the SIP message body. This information shall then be sent back to the I-CSCF within the subsequent *Register* messages.

Note, that in case that network hiding is applied, is shall not be possible outside the IMS home network to derive the S-CSCF address from the received information.

Further optimisation may be achieved by combining message 3 with message 5 and the appropriate responses (messages 4 and 6). Similarly messages 20 and 22 and the appropriate responses (messages 21 and 23) may also be combined.

These optimisation options are included here so as they are not forgotten. They are not meant to be included in TS 33.203 as it is not the responsibility of S3 to decide on them. But it is suggested to forward the information on optimisation options to S2, N1 and N4 in an LS together with a new version of TS 33.203 as soon as this new version of TS 33.203 includes the information flows presented in this contribution.

Handling of mobile terminated call in course of registration

After having received message 8 the HSS stores the S-CSCF name for that subscriber together with a flag which indicates that registration is still in progress, i.e. registration could still fail. If after message 8 and before message 20 the user receives a mobile terminated call, then the handling of this call has to be specified. In this case a mobile terminated call shall be handled as if the user were not registered.

In the situation above an I-CSCF receives the *Invite* message. This I-CSCF sends a *Cx-Location-Request* to the HSS. The HSS detects that the flag stored together with the S-CSCF address indicates that registration is not yet successfully completed. The HSS maps this information to the state "user not registered" and sends an appropriate indication in the *Cx-Location-Response* message to the I-CSCF. The I-CSCF proceeds as usual in the case of a mobile terminated call for an unregistered user.

2.2 Authenticated registration with user authentication failure

In this section the case of an authenticated registration is described where the authentication of the user is not successful. Up to message 19 inclusive Figure 2 is identical to Figure 1. Then the S-CSCF detects that the received value *RES* and the stored value *XRES* differ, i.e. a user authentication failure has occurred. Afterwards the information flow is continued as follows:

20. The S-CSCF shall send *Cx-Put* (subscriber identity, clear S-CSCF name) to the HSS. The HSS shall clear the S-CSCF name and the accompanying flag of that subscriber.
21. The HSS shall send *Cx-Put Resp* to the S-CSCF to acknowledge the sending of *Cx-Put*.
22. The S-CSCF shall send an *401 Unauthorised* message to the I-CSCF in order to indicate that the registration requested by the UE was rejected.
23. The I-CSCF shall forward the *401 Unauthorised* message to the P-CSCF. The I-CSCF shall release all registration information after sending *401 Unauthorised*.
24. The P-CSCF shall forward the *401 Unauthorised* message to the UE.

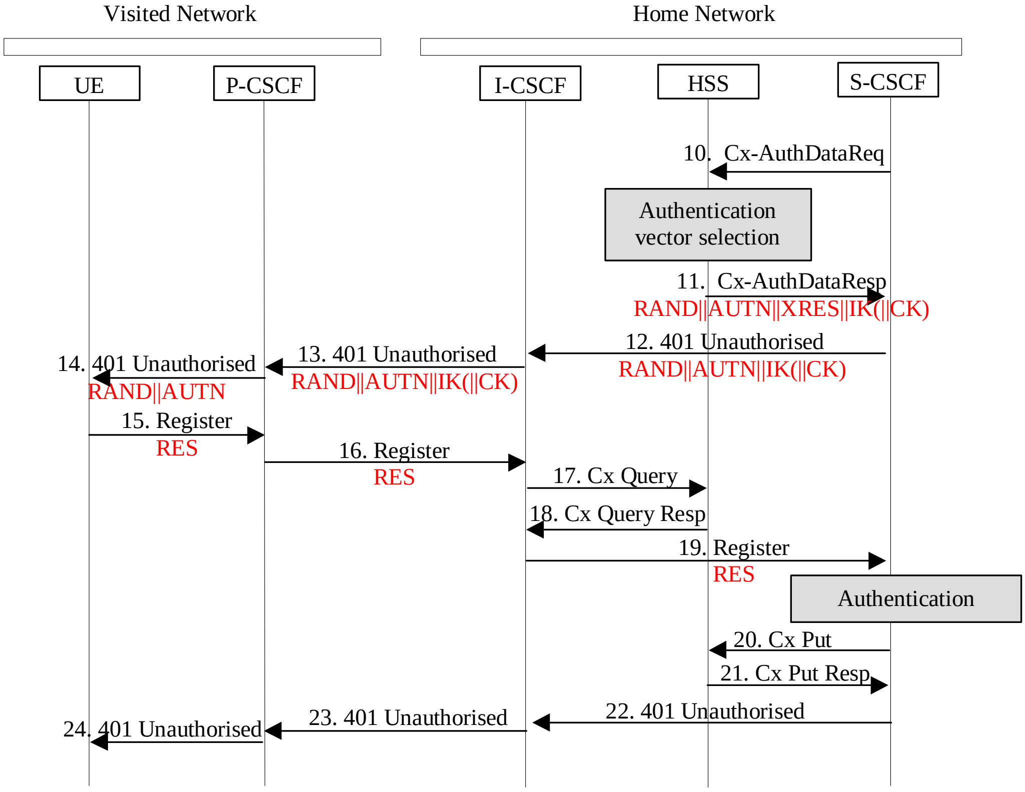

Figure 2: Authenticated registration, user authentication failure

Optimisation of the information flow

For messages 17 and 18 the same optional optimisation method as in section 2.1 above can be applied.

As in section 2.1 further optimisation may be achieved by combining message 3 with message 5 and the appropriate responses (messages 4 and 6).

2.3 Authenticated registration with network authentication failure

In this section the case of an authenticated registration is described where the authentication of the network is not successful.

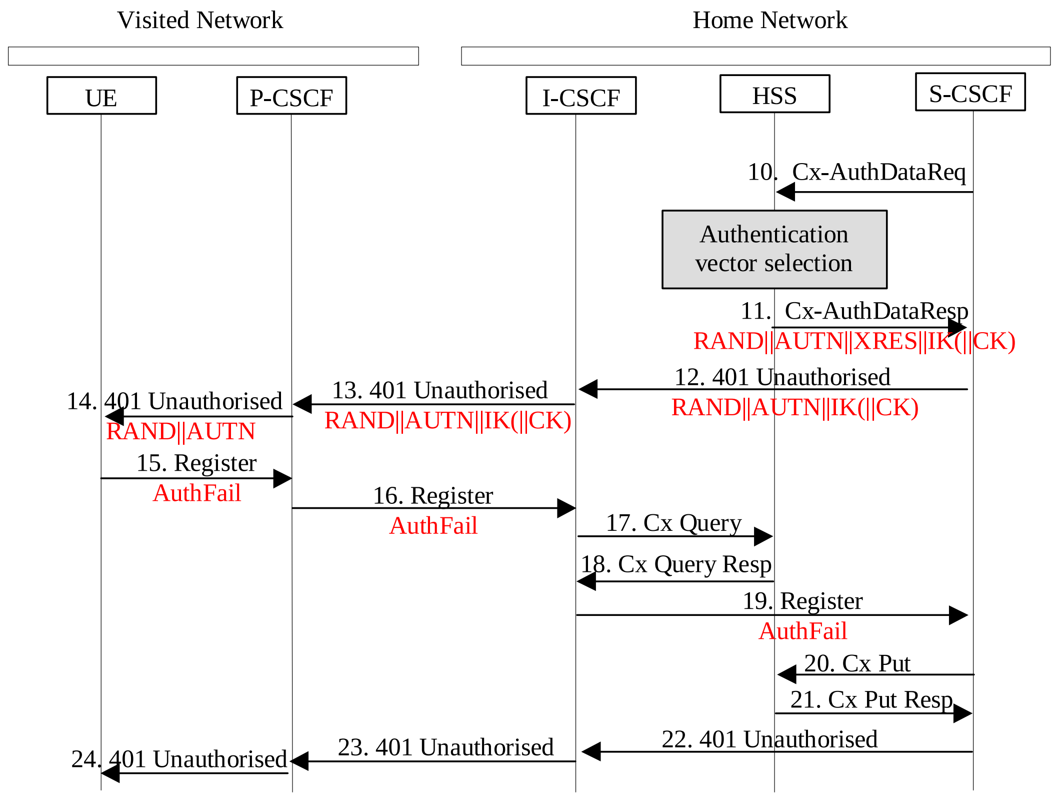

Figure 3: Authenticated registration, network authentication failure

Up to message 14 inclusive Figure 3 is identical to Figure 1. After the UE has detected that network authentication has failed the information flow is continued as follows:

15. The UE shall send a *Register* message to the P-CSCF indicating that authentication of the network failed by including the *AuthFail* indicator.
16. The P-CSCF shall forward the received message (including the parameter *AuthFail*) 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 *AuthFail*) to the S-CSCF.
20. After the S-CSCF detects from the *AuthFail* value in the received *Register* message that authentication of the network by the UE failed, it shall send *Cx-Put* (subscriber identity, clear S-CSCF name) to the HSS. The HSS shall clear the S-CSCF name and the accompanying flag for that subscriber.
21. The HSS shall send *Cx-Put Resp* to the S-CSCF to acknowledge the sending of Cx-Put.
22. The S-CSCF shall send an 401 Unauthorised message to the I-CSCF in order to indicate that the registration requested by the UE was rejected.
23. The I-CSCF shall forward the 401 Unauthorised message to the P-CSCF. The I-CSCF shall release all registration information after sending 401 Unauthorised.
24. The P-CSCF shall forward the 401 Unauthorised message to the UE.

Optimisation of the information flow

For messages 17 and 18 the same optional optimisation method as in section 2.1 above can be applied.

As in section 2.1 further optimisation may be achieved by combining message 3 with message 5 and the appropriate responses (messages 4 and 6).

2.4 Authenticated registration with synchronisation failure

In this section the case of an authenticated registration with synchronisation failure is described. After re-synchronisation, 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 Figure 4 only the case of a synchronisation failure with subsequent successful authentication is shown. The other cases can be derived by combination with the flows for the other failure conditions.

Messages 1 - 9 are the same as in section 2.1 above and are therefore not shown in the Figure 4 below.

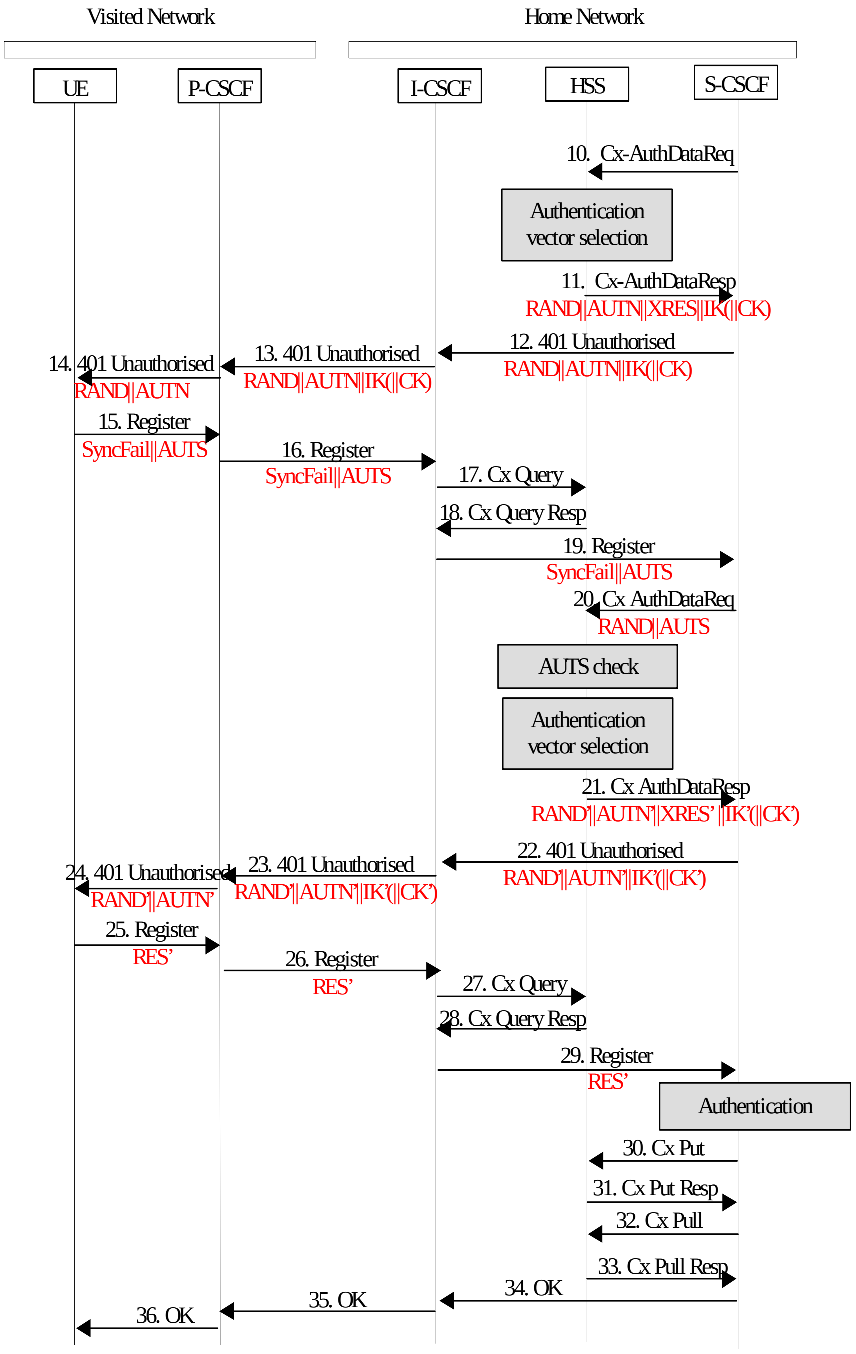

Figure 4: Authenticated registration with re-synchronisation

Optimisation of the information flow

For messages 17 and 18 but also messages 27 and 28 the same optional optimisation method as in section 2.1 above can be applied.

As in section 2.1 further optimisation may be achieved by combining message 3 with message 5 and the appropriate responses (messages 4 and 6). Similarly messages 30 and 32 and the appropriate responses (messages 31 and 33) may also be combined.

~~2.2~~3 Authenticated re-registration – User currently registered

Re-registration will usually be initiated by a UE some time before the validity of the last successful registration or re-registration expires. A general decision to be made is what the consequence of an unsuccessful re-registration is, i.e. a re-registration with network and/or user authentication failures. There are two possibilities:

- An authentication failure in course of a re-registration results in an immediate de-registration.
- The last registration or re-registration with successful authentication only expires when its lifetime expires.

This decision will influence the information flow for re-registration.

Below an information flow for an authenticated IMS re-registration with successful authentication is shown under the assumption that the last registration or re-registration with successful authentication only expires when its lifetime expires.

Note, that in the case of re-registration, failure conditions may occur in a way analogous to the ones described in section 2. We do not show the information flows for the failure conditions, as they can be easily derived from to the appropriate flows in section 2.

The re-registration information flow can be found in Figure 6. We do not give a full textual description of the re-registration information flow, as it is very similar to registration which is in detail described in section 2.1 above. We would only like to point out that if message 6 of Figure 5 (which is optional according to TS 23.228) is send at all, the S-CSCF sends its address (which is already available in the HSS) together with the accompanying flag, which indicates that this S-CSCF is also assigned for mobile terminated calls, i.e. the flag value is to be the same as that in message 20 of Figure 1 which, in that message, indicates a successfully authenticated initial registration.

Section 2.2 and 2.3 describe the failure cases “user authentication failure” and “network authentication failure”, respectively. The appropriate failure cases for re-registration are analogous with the exception that messages 20 and 21 *Cx-Put/Cx-Put-Resp* (cf. Figure 2 and Figure 3, respectively) are not required. This modification is a consequence of the assumption above that the UE remains registered until the expiration of the timer of the last successful (re-) registration. If this assumption is not valid then the messages *Cx-Put/Cx-Put-Resp* have to be additionally included.

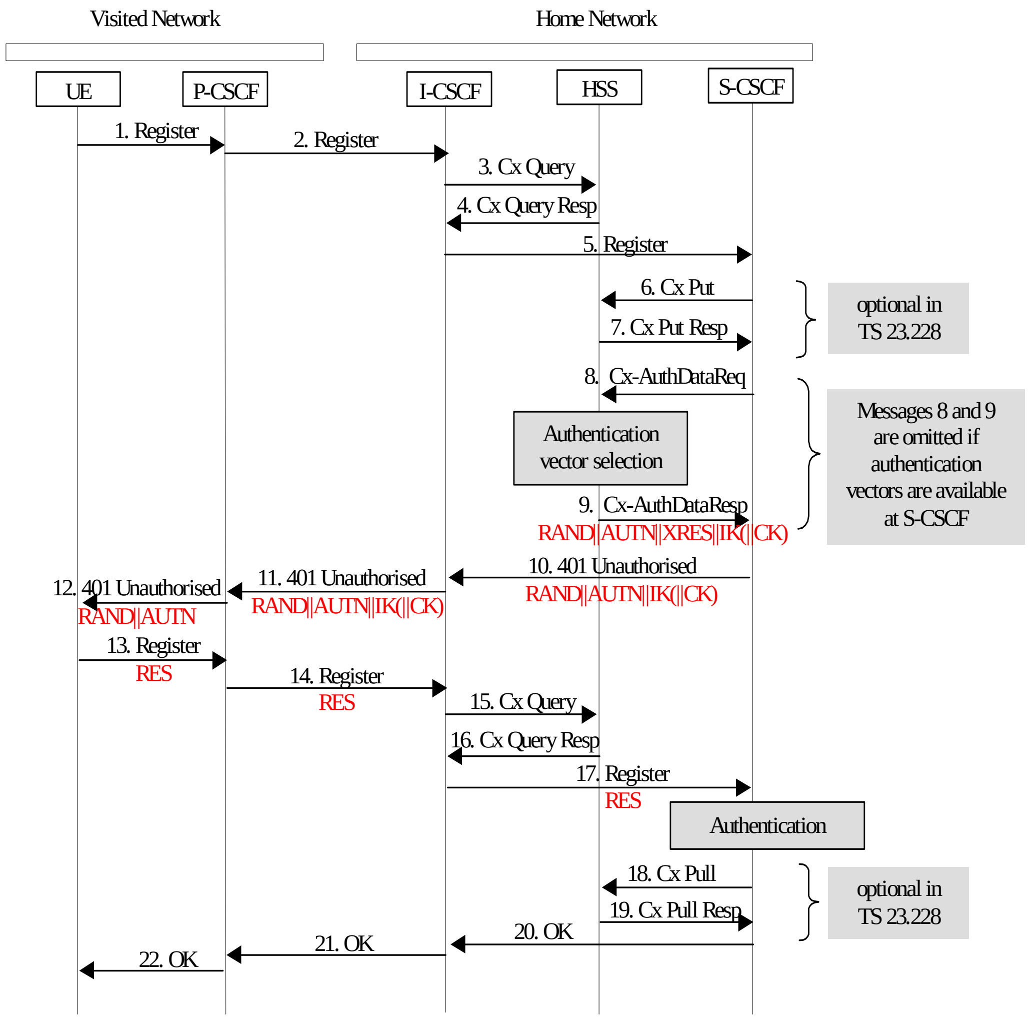

Figure 5: Authenticated re-registration

Optimisation of the information flow

According to [TS 23.228, section 5.2.2.4] in Figure 5 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.

For messages 15 and 16 the same optional optimisation method as in section 2.1 above can be applied.

If this optimisation method described in section 2.1 could be also applied to messages 3 and 4 in Figure 5 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.

~~5~~4Proposal

It is proposed that IMS authentication is carried out according to the information flows presented above and that the flows are incorporated in the technical standard 3G TS 33.203.

Furthermore, it is suggested to forward the information on optimisation options to S2, N1 and N4 in an LS together with a new version of TS 33.203 as soon as this new version of TS 33.203 includes the information flows presented in this contribution.

~~6~~5 References

[3G TS 23.228] 3GPP TSG SA WG2 Architecture, TS 23.228: *IP Multimedia (IM) Subsystem - Stage 2;* v. 5.0.0, March 2001.

[3G TS 33.203] 3GPP TSG SA WG3 Security, TS 33.203: *Access security for IP-based services;* v. 0.3.0, May 2001.