3GPP TSG WG3 S3#17bis
Madrid, Spain
25th April – 26th April, 2001

Tdoc S3z010025

Agenda Item: TBD

Source: Ericsson

Title: Termination of authentication

Document for: Discussion and decision

1 Scope and objectives

The scope for this document is to discuss the question on where authentication of an IM-subscriber shall take place; either at the HSS or at the S-CSCF.

After analysis of both options, this document proposes that

1 The authentication of the IM-subscriber shall take place in the HSS.

2 Background

In S3 it was decided at the SA3#17 meeting in Göteborg that authentication of an IM-subscriber shall take place in the Home Network. It was left for FFS if the HSS or the S-CSCF should perform the authentication.

Before the UE is registered it gets an IP-address, which logically belongs to the IM CN SS IP-domain, by using an appropriate PDP-context. Then the UE needs to know the address of a P-CSCF which is the first contact point in the IM CN SS. Depending on the UE capabilities either a DHCP or PDP Context Activation is used to transfer the P-CSCF IP address.

The requirements stated below are all taken from TS 23.228 v500 and the chapter where the requirement is stated is also given in brackets.

At registration:

1. The P-CSCF discovers, based on the home domain name, the entry point to the Home Network i.e. the I-CSCF.

2. The I-CSCF queries the HSS in order to find out if the subscriber is registered or authorised to register. Note that if the HN contains more than one HSS the I-CSCF has to interact with an SLF in order to find the address of an appropriate HSS. The HSS then authorises the registration and sends back a response to the I-CSCF. At this stage or earlier, according to 23.228, the user has been authenticated {Req. 1 (5.2.2.3)}.

3. The I-CSCF shall select an S-CSCF for the subscriber by using the Cx-Select-pull message and the information received from the HSS.

4. The I-CSCF forwards the Register message to the chosen S-CSCF and the registration procedure continues cf. TS 23.228.

After e.g. a registration transaction the I-CSCF shall not store any state information {Req. 2 (5.2.2.5)}. The HSS shall, after receiving a Cx-Put store the S-CSCF name/address {Req. 3 (5.2.2.3)}. The P-CSCF shall store the network entry point {Req. 4 (5.2.2.5)} but the P-CSCF shall not take into account previous registrations when routing SIP-registration messages {Req. 5 (5.1.4)}.

3 Analysis of the alternatives

There are at the moment two alternatives to analyse. Perform the authentication either in 1) the HSS or 2) the S-CSCF.

3.1 HSS/S-CSCF at registration

3.1.1 Authentication in the HSS

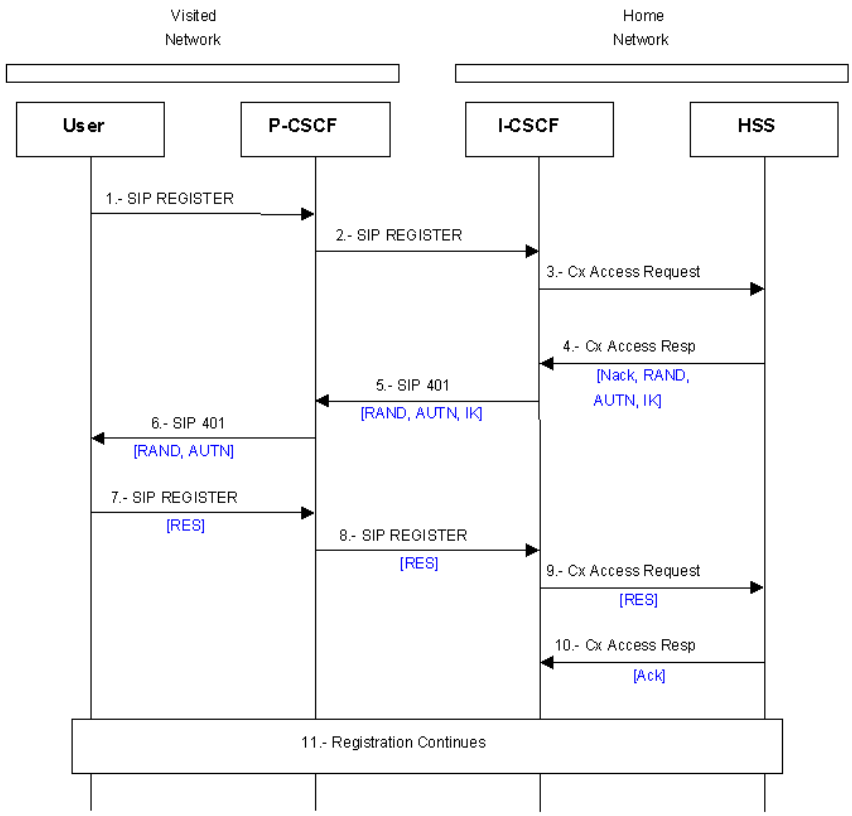

Figure 1.- Successful Registration (HSS control).

For a detailed content description of the signalling flow, cf. Annex A.

This signalling flow is compliant with {Req. 2} and {Req. 5}. When sending the SIP-401 message at Step 5 the I-CSCF will release all registration information. At Step 8 the P-CSCF might select a different I-CSCF {Req. 5} to route the new SIP REGISTER message (now including authentication information) than the one selected in step 2. In the signalling flow above the I-CSCF will behave in the same way in Step 8 as in Step 2 i.e. forward a Cx-Access-Request to an appropriate HSS. Note that the I-CSCF will employ a name-address resolution mechanism to determine the address of the HSS. This is excluded in the flow above.

This solution is also compliant with {Req. 1} since the Cx-Query is sent at Step 11 where the registration continues. In the example shown above the user is authorised to register and the HSS therefore creates the RAND, AUTN and IK and forwards the message to the I-CSCF.

The HSS has to keep information about the user and the XRES to be able to compare that with the incoming RES. This can be viewed as an extension of {Req. 3} since an entry in the HSS has to exist for correlation of user identity and corresponding S-CSCF. This extension does not add any extra complexity for the HSS.

In the Siemens contribution presented to this meeting [S3z010003], it is stated that the HSS has to wait for responses after sending out the requests. The proposed solution from Ericsson is that the HSS receives a Cx-

Access-Request and the HSS generates a 'Quintet' or part of it and stores the XRES together with a timestamp. The HSS should not then keep a process alive waiting for the response and a new Cx-Access-Request. The dialogue should always be closed when the HSS sends the Cx-Access-Resp to the I-CSCF. The HSS should when and if it receives a response check if it is still valid i.e. within the allowed timeframe. So there are no open dialogues and the HSS is not waiting for any responses it will only act upon requests. Hence there is no penalty in real time performance but some penalty on the amount of memory needed in the HSS.

3.1.2 Authentication in the S-CSCF

This is proposed by Siemens and the signalling flow is taken from their proposal, see [S3z010003].

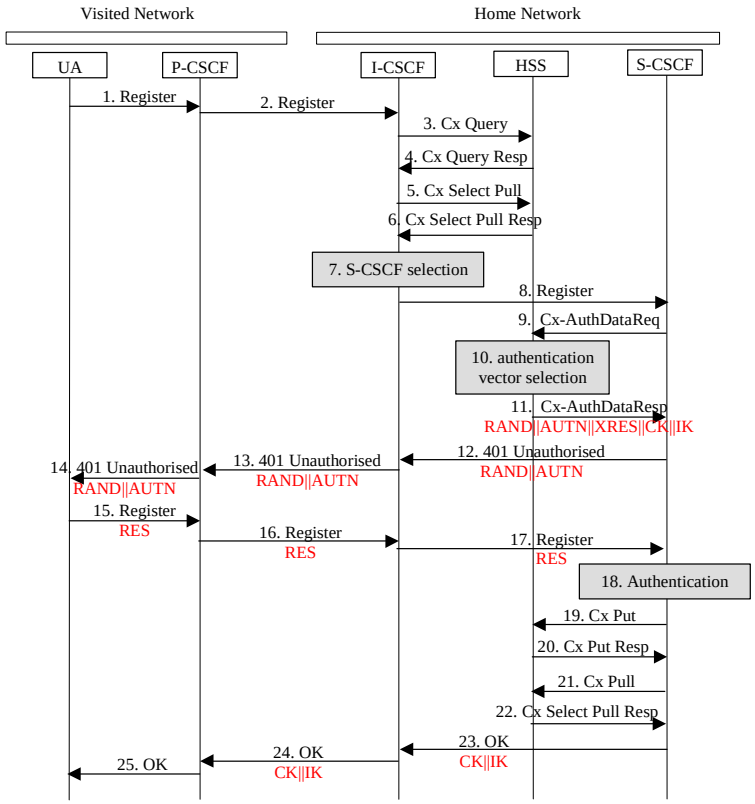

Figure 2. - Successful Registration (S-CSCF control).

First of all it should be stressed here that it is FFS whether confidentiality protection should terminate in the P-CSCF. Hence at this stage it is pre-mature to include the CK in the signalling flow. It could however be viewed as an example where to include the CK if necessary.

Is this scenario compliant with the requirements stated in chapter 2?

According to 23.228 when the I-CSCF receives the response in Step 16 it does not know to which S-CSCF to send the response i.e. {Req. 2}. Hence the I-CSCF should keep the state (Step 7) until the user has been authenticated and registered. However this is not compliant with {Req. 2} and would imply that the I-CSCF keeps state information on previous registration attempts (i.e. I-CSCF stateful). This would also mean that this alternative is not compliant with {Req. 5} either, since the P-CSCF shall have to send the SIP REGISTER message in step 16 to the same I-CSCF selected in step 2 (i.e. stateful P-CSCF).

Another alternative would be to query the HSS once again in order to find out which S-CSCF to use. In this case it should be noted that the HSS has not yet stored the name of the S-CSCF. That takes place later on in Step 19 in the flow above i.e. {Req. 3}. This means that a new full S-CSCF selection process has to take place again. But if this is feasible or not has to be analysed further since what happens if the I-CSCF comes up with another S-CSCF at this stage compared to the one in Step 7?

Furthermore note that the I-CSCF will not behave in the same way for the Register messages. At step 3 the I-CSCF queries the HSS but at step 17 the I-CSCF forwards the Register message to an S-CSCF. This adds extra complexity to the I-CSCF. The proposal from Siemens is not compliant with {Req. 1} either, since the authentication takes place at a much later stage, step 18. The consequences in doing this is that the HSS authorises any user an S-CSCF before authentication has taken place and the allocation of system resources,

from a performance but also from a security point of view, shall be only granted to valid users (i.e. once the user has been authenticated). The amount of signalling, states and processing is increased with an amount that can not be negligible, see below:

I. The I-CSCF has to send a Cx-Select pull to the HSS (Step 5)

II. The HSS has to process this information and send back the required S-CSCFs capabilities (Step 6)

III. The I-CSCF has to process this information and determine the S-CSCF address through a name resolution mechanism (Not Shown in the Flow). The I-CSCF might store the name of the S-CSCF in order to continue the flow at (Step 17) but this is NOT compliant with {Req. 2}.

IV. If the name of the S-CSCF is not stored in the I-CSCF in III above than the I-CSCF once again has to find out the address of an appropriate HSS. Then query the HSS in order to determine which S-CSCF to forward the REGISTER with the response i.e. a new S-CSCF selection has to be accomplished.

V. The S-CSCF receives the Register and sends an Authentication data requests to the HSS, which calculates the appropriate parameters and sends them to the S-CSCF (Step 9-11). The S-CSCF stores the XRES with the user id.

VI. The user is authenticated (Step 18)

This extra amount of signalling, states kept at the P/I-CSCF, processing and use of network resources is sensitive to a DoS. As it will be shown further in this document, this sensitivity to DoS attacks in the S-CSCF option is even more significant when considering Authentication Failure Report and Re-Synchronisation scenarios.

The S-CSCF also has to store, as the HSS, the XRES for some predetermined time.

Apart from the extra signalling and sensitivity to DoS attacks the analysis above has shown that the signalling flow taken from [S3z010003]is not compliant with 23.228 500 and hence can not work. The flow is not compliant with {Req. 1}, {Req. 2},{Req. 3} and {Req. 5}.

3.2 Authentication failure

3.2.1 HSS performs authentication

As proposed in figure 3, when the user can not verify the MAC he sends a SIP Register Auth Failure message to the P-CSCF which forwards it towards the HN. The HSS sends an ACK back to the I-CSCF which sends a SIP 200 towards the user.

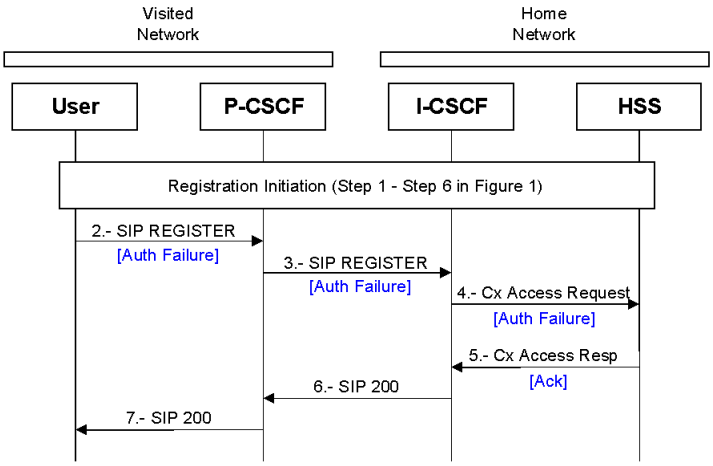

Figure 3.- Network Authentication Failure (HSS control).

As proposed in figure 4, if the HSS can not verify the user it sends a NACK back to the I-CSCF, which forwards a SIP 401 towards the user.

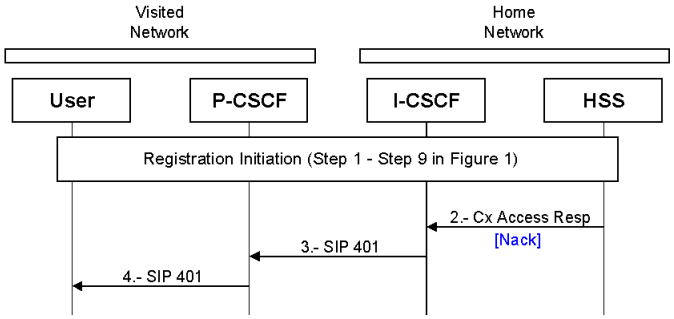

Figure 4.- User Authentication Failure (HSS control).

3.2.2 S-CSCF performs authentication

As proposed in figure 5, when the user can not verify the MAC he sends a SIP Register Auth Failure message to the P-CSCF which forwards it towards the HN. The I-CSCF forwards the message to an appropriate S-CSCF. The S-CSCF sends an authentication failure report to the HSS and then sends a SIP 200 towards the user. In order to send the authentication failure to an S-CSCF the I-CSCF can not be stateless and it has to store the address of the S-CSCF.

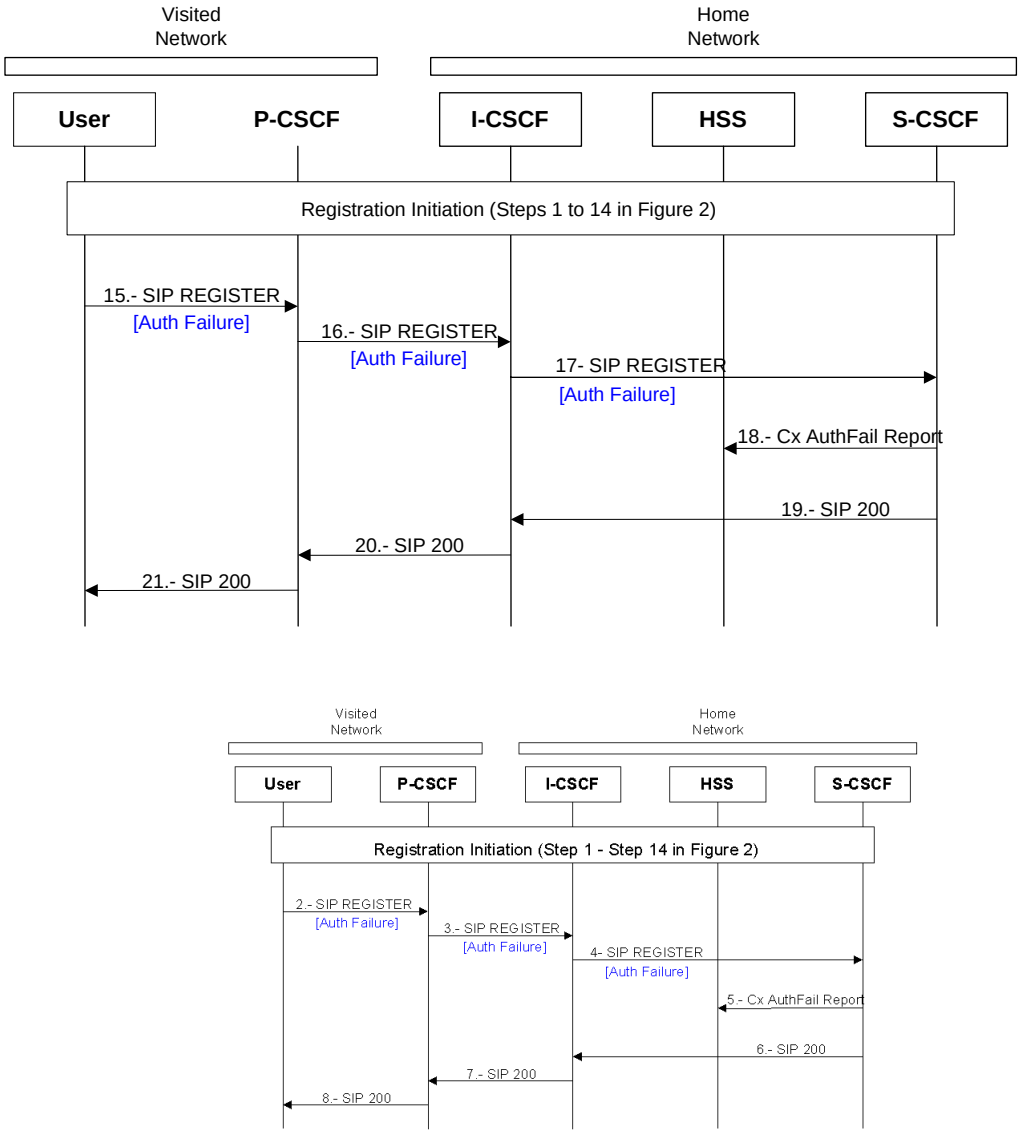

Figure 5.- Network Authentication Failure (S-CSCF control).

As it can be seen in figure 6, if the S-CSCF can not verify the user it sends an authentication failure report to the HSS and then a SIP 401 towards the user.

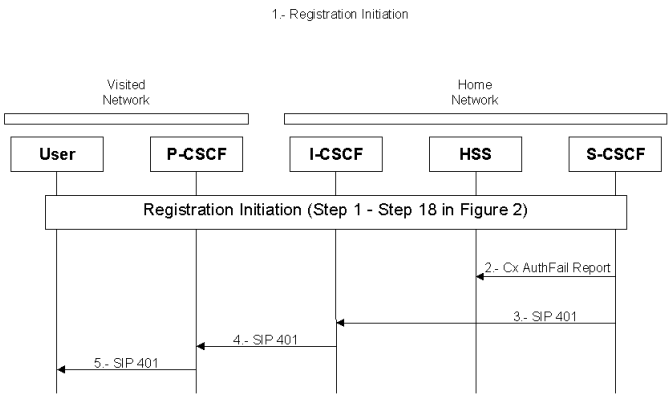

Figure 6.- User Authentication Failure (S-CSCF control).

On top of the drawbacks presented in the successful authentication scenario (stateful P/I-CSCF, extra signalling and processing), with the S-CSCF option it takes almost 10 messages more to detect and complete an Authentication Failure Report. This is mainly because the S-CSCF needs to be selected first and then the S-CSCF needs to inform the HSS of this event.

With the HSS alternative, the HSS itself informs and is informed of User and/or NW authentication failures much sooner in the process.

3.3 Re-synchronisation

3.3.1 Authentication in the HSS

When the USIM detects that the SQN is out of synch the UA shall send a SIP REGISTER including the AUTS, cf. 33.102 towards the HSS. The HSS sends a NACK to the I-CSCF and a new challenge together with the other parameters.

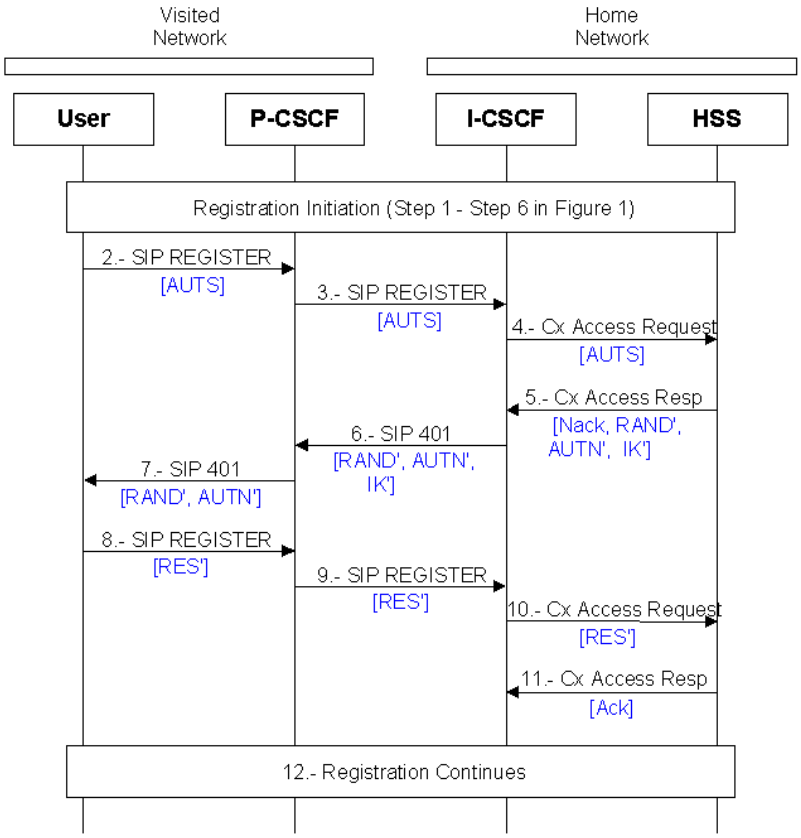

Figure 7.- Re-Synchronisation procedure (HSS control).

3.3.2 Authentication in the S-CSCF

When the USIM detects that the SQN is out of synch the UA shall send a SIP REGISTER including the AUTS, cf. 33.102 towards the HN. The I-CSCF forwards the message to an S-CSCF, which contacts the HSS and gets back new parameters to perform a new challenge. The S-CSCF sends the challenge towards the user which sends back a response. The main drawback with this alternative remains. The I-CSCF can not be stateless. At Step 4 the I-CSCF needs to know that a SIP Register containing an AUTS should be forwarded to an S-CSCF whose address is stored in the I-CSCF. The same applies at Step 12 when the SIP register contains a response.

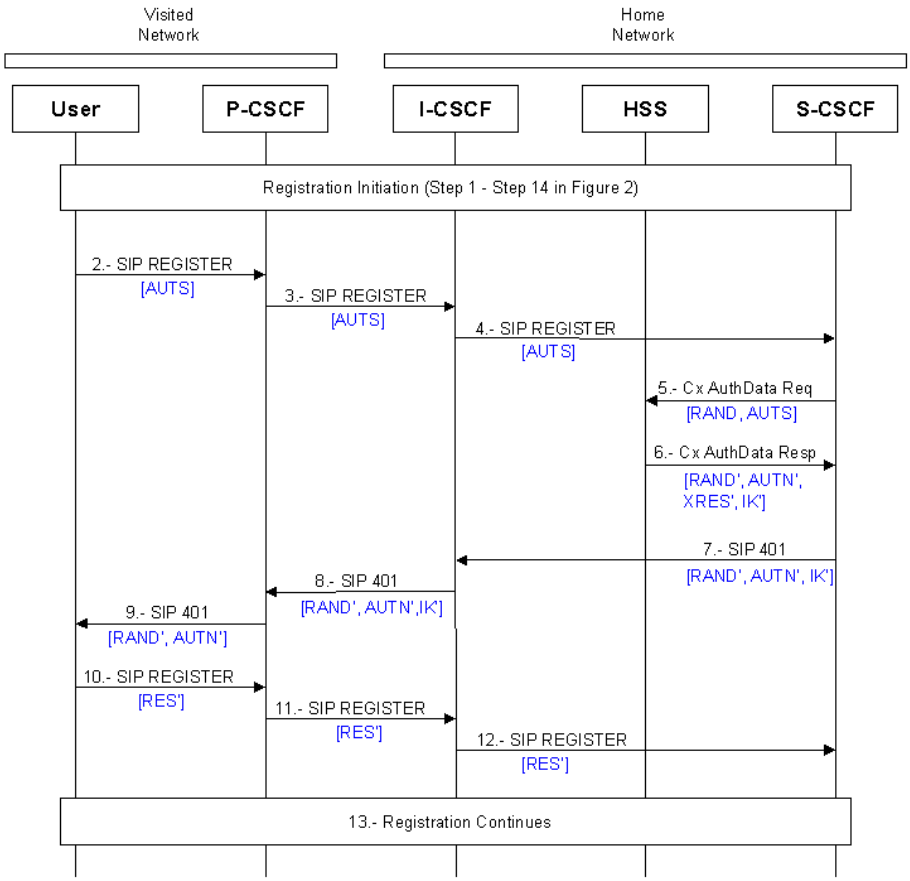

Figure 8.- Re-Synchronization procedure (S-CSCF control).

In both cases the HSS should calculate a new challenge and corresponding parameters. However, and on top of the drawbacks presented in the successful authentication scenario (stateful P/I-CSCF, extra signalling and processing), with the S-CSCF option it takes almost 10 messages more to detect and complete a re-synchronisation. This is mainly because the S-CSCF needs to be selected first and then the S-CSCF needs to inform the HSS of this event after the initial challenge has been sent.

With the HSS alternative, the HSS itself gets to know about the synchronisation failure much sooner in the process and it the HSS itself provides the new set of authentication data, so the complete procedure is simplified and optimised.

Conclusions

To terminate the authentication in the HSS is the most efficient solution in terms of signalling overhead and use of network resources. The solution is fully compliant with [3G TR 23.228] and no states are introduced to the P-CSCF and the I-CSCF.

However performing the authentication in the HSS means that the user id and the corresponding XRES have to be stored for some predetermined time in the HSS. This however has a limited impact since there will be no penalty in real time performance but some penalty on the amount of memory needed in the HSS. It should be noted that the S-CSCF should have a similar XRES mechanism.

With the proposal to perform the authentication in the S-CSCF it should be concluded that it would introduce a lots of extra signalling compared to the HSS alternative. This is valid for registration of a subscriber as well as for authentication failures etc. Furthermore an S-CSCF is assigned before the user has been authenticated which means that unnecessary use of network resources for bogus users. This together with the extra signalling creates unnecessary sensitivity to DoS attacks. It should also be noted that with this alternative there would be more signalling towards the HSS as well.

Furthermore the S-CSCF alternative and the flow described in [S3z010003] is not compliant with [3G TR 23.228] and would not work unless the P-CSCF and the I-CSCF becomes stateful. It should also be mentioned that the I-CSCF with this alternative needs a mechanism in place in order to behave differently for SIP Register messages since it sometimes should route them towards the S-CSCF and sometimes send a Cx message to the HSS.

5 References

[3G TR 23.228] 3GPP TSG SA WG2, TR 23.228: IP multimedia (IM) subsystem - Stage 2; v 5.0.0, October 2000.

[S3z010003] 3GPP TSG SA WG3 Security, S3z010003 *Alternatives for terminating authentication in the home domain of the IM Subsystem;* Source Siemens, April 2001.

Annex A

1. The user sends the register information (subscriber identity, home network domain name) to the P-CSCF.
2. The P-CSCF examines the home network domain name to find the entry point (i.e. the I-CSCF) corresponding to that home network. Then the P-CSCF forwards the register information to the discovered I-CSCF (subscriber identity, HN name, VN name, P-CSCF name).
3. The I-CSCF uses the subscriber identity to determine the corresponding HSS, and sends a Cx-Access-Request to that HSS (subscriber identity, HN name, VN name, P-CSCF name).
4. The HSS initiates the AKA procedure:

- It generates a random number RAND, an expected response XRES and an AUTN value for network authentication. Both XRES and AUTN depend on the values taken by RAND and K[1].
- The integrity key IK are also calculated as a function of RAND and K.
- The HSS responds to the received Cx-Access-Request with a Cx-Access-Response denying access and containing RAND, AUTN, CK and IK.

5. The I-CSCF issues a SIP 401 message[2] containing RAND, AUTN and IK, and sends it to the P-CSCF.
6. The P-CSCF stores IK for subsequent use, and sends a SIP 401 message containing RAND and AUTN to the user.
7. Upon receipt the user does the following:
    - Network authentication is achieved making use of AUTN.
    - The user computes RES and sends a SIP REGISTER containing RES to the P-CSCF. The user may also reject the registration attempt if there is a failure in network authentication or a synchronisation failure (see **Error! Reference source not found.** and **Error! Reference source not found.**).
    - The integrity key IK are calculated as a function of RAND and K.

---

[1] K is a secret value shared by the user and the HN.

[2] SIP 4xx messages indicate a Client Failure. Specifically, a SIP 401 message indicates “User unauthorised”.

8. The P-CSCF forwards the SIP REGISTER to the I-CSCF.
9. The I-CSCF sends a Cx-Access-Request containing RES to the HSS.
10. The HSS executes the following actions:
    - User authentication is achieved comparing RES with XRES.
    - The HSS responds to the received Cx-Access-Request with a Cx-Access-Response containing a positive result. The Cx-Access-Response may also reject the registration attempt if a failure in user authentication had occurred or if the time passed since the storage of XRES in the HSS exceeds a pre-configured time.
11. The registration procedure continues as defined in [3G TR 23.228], which includes authorisation of the user to register in the VN.