3GPP TSG SA WG3 Security **S3z010003**

Meeting S3#17bis, Ad-hoc IMS

Madrid, 24 – 26 April, 2001

Source: Siemens AG

Title: Alternatives for terminating authentication in the home domain of the IM Subsystem

Document for: Discussion / Decision

Work item: Access security for IP-based services

Agenda item: tbd

Abstract

At S3#17 (Göteborg, 27 Feb – 2 March 2001) it was decided that authentication in the IMS should be carried out in the IMS home network, but that it is ffs whether HSS or S-CSCF terminates authentication between user and IM CNSS. An information flow with the HSS as termination point has been included by the editor in the latest version of TS 33.203. This contribution presents an alternative information flow with the S-CSCF as termination point. It is tentatively concluded that it is more appropriate to terminate authentication in the S-CSCF. However, before a final decision on the termination point for authentication can be taken all information flows possibly involving authentication should be examined.

1 Introduction

At S3#17 (Göteborg, 27 Feb – 2 Mar, 2001) 3G SA3 took the following decisions on IMS security [S3-010100]:

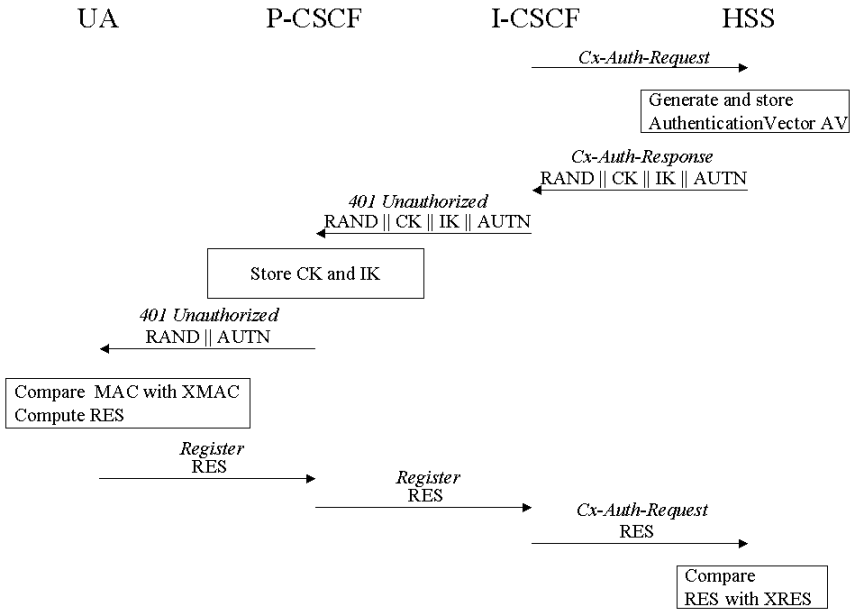
- P-CSCF terminates IMS access integrity/confidentiality protection of SIP messages from the UE. Security associations are user specific here and are established by the 3G AKA mechanism.
- Security associations between P-CSCF and S-CSCF are established via Network Domain Security mechanisms and are not user specific.
- Authentication is performed in the home network. It is ffs whether it is performed in the HSS or the S-CSCF.

This document addresses the last bullet.

2 IMS authentication terminating in the HSS

In the new version of [3G TS 33.203, section 6.1], the editor incorporated a part of an information flow for IMS authentication which shows the IMS authentication terminating in the HSS . It should be noted here, however, that it is still for further study if the decision on successful authentication is carried out

in the S-CSCF or in the HSS (cf. also [3G TS 33.203], section 4) and that therefore this information flow is only an example.



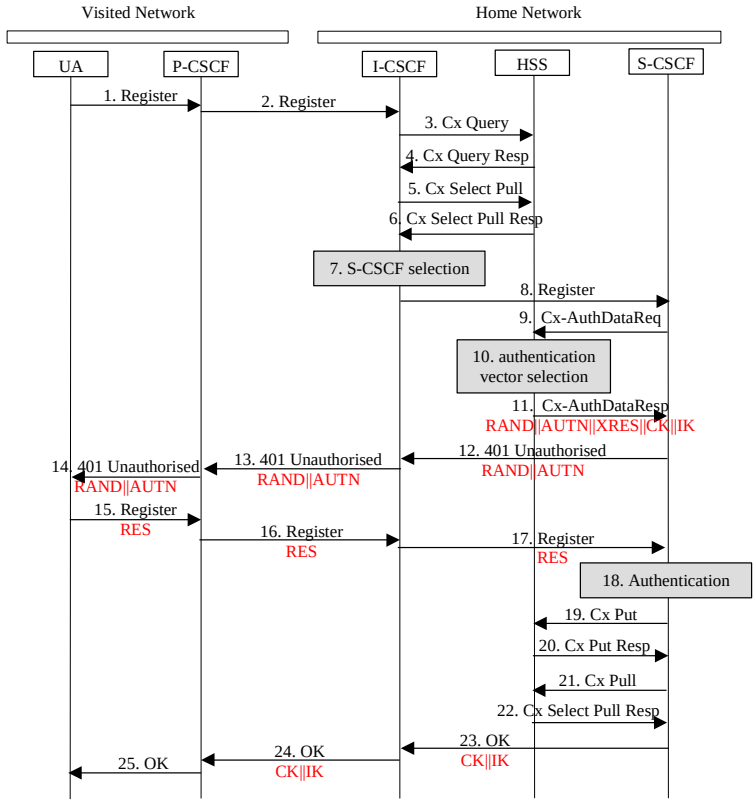
In the second message, i.e. the *Cx-Auth-Response* message, the parameters *RAND*||*CK*||*IK*||*AUTN* are sent from the HSS to the I-CSCF. *RAND* and *AUTN* have to be forwarded further on to the user agent UA in this message for the purpose of mutual authentication between user and HSS, whereas the session keys *CK* and *IK* are only forwarded to the P-CSCF in order to protect SIP messages between UE and P-CSCF in subsequent SIP transactions (e.g. INVITE, Re-REGISTER).

A comment on the point in time the keys *CK* and *IK* are sent: From a security point of view, sending *CK, IK* to the P-CSCF before the user has been authenticated does not seem to be appropriate for the following reason: it was decided in the last SA 3 meeting to carry out authentication in the IMS in the home and not in the visited network. The main reason was that it was argued that this reduces the trust in the visited IMS required by the home IMS. But if the visited IMS is not trusted, then session keys should not be revealed to the P-CSCF in the visited IMS before the user is authenticated. This can, however, be avoided, when *CK, IK* are sent to the P-CSCF later in the information flow, i.e. after comparison of *RES* and *XRES* is successfully completed.

A further discussion of the pros and cons of this approach can be found in section 4.

3 IMS authentication terminating in the S-CSCF

Below an information flow is shown where the S-CSCF terminates IMS authentication.



Description of the Information flow:

Up to message 8 the information flow does not differ from the one without security given in [3G TS 23.228], section 5.3.

9. The S-CSCF sends a request for authentication data *Cx-AuthDataReq* to the HSS.

10. The HSS selects a quintuple with user specific authentication data *RAND||AUTN||XRES||CK||IK*.

11. In an *Cx-AuthDataResp* message the HSS sends the quintuple *RAND||AUTN||XRES||CK||IK* to the S-CSCF.
    Note, that it is also possible to send a batch of pre-computed quintuples to the S-CSCF, if desired. This would facilitate that even in further SIP transactions (e.g. re-registration) which require authentication, steps 9 to 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 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 forwards the received message (including the parameter *RES*) to the S-CSCF.

18. 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.

19. - 22. As in course of a registration transaction without security (cf. [3G TS 23.228], section 5.3)

S-CSCF and HSS exchange a set of Cx-Put and Cx-Pull requests and responses.

23. The S-CSCF indicates to the I-CSCF that authentication was successfully completed by sending an *OK* message, which includes the session keys *IK* and *CK* for integrity/confidentiality protection of SIP signalling.
24. The I-CSCF forwards the received message (including the parameters *CK*||*IK*) to the P-CSCF.
25. The P-CSCF sends an *OK* to the UA (which does not include the parameters *CK*||*IK*).

4 Pros and cons of authentication decision in S-CSCF

In the following advantages and disadvantages of terminating IMS authentication in the S-CSCF (section 3) are discussed compared to terminating IMS authentication in the HSS (section 2).

Pros:

- Stateless paradigm for HSS can be preserved (from UMTS and GSM):

  If the AKA is terminated in the S-CSCF the paradigm for the HSS applied so far in UMTS and GSM could be preserved: the HSS would just be a (transaction-)stateless server which responds to queries.

  If the AKA was terminated in the HSS the HSS would have to send out requests and wait for responses, for a potentially large number of users simultaneously. This could reduce HSS performance significantly. (The HSS would have to keep the state of the registration transaction of each UA from the point in time it receives the Cx-Auth-Request message until it sends the UA specific keys CK, IK to the I-CSCF. Cf. section 2.)

- HSS becomes more vulnerable to DoS attacks:

  The fact that the HSS has to keep the state of the actual running SIP registration transactions of a possibly large number of users could make the HSS more vulnerable to the DoS attacks.

- HSS can send a batch of authentication vectors to the S-CSCF:

  In step 10 of the description of the information flow in section 3 above it is possible to pre-compute more than one authentication vector (quintuple) and to send a batch of pre-computed quintuples to the S-CSCF, if desired.

  This could enable the S-CSCF to handle SIP transactions which require re-authentication autonomously without the need to contact the HSS each time.

  It could e.g. be facilitated that even in further SIP transactions (e.g. re-registration) which require authentication, steps 9 to 11 of the information flow could be omitted. Furthermore, and possibly more importantly, if authenticated SIP INVITE messages would optionally require authentication, this could be facilitated without contacting the HSS. Note, that the HSS is usually not involved in the INVITE information flow when no authentication is required. This may reduce load on the HSS.

Cons:

- Home network more vulnerable to DoS attacks:

  The S-CSCF is selected before the UA is authenticated. This may make the home network more vulnerable to DoS attacks. But on the other hand, as already mentioned under "pros" above, the decision on authentication in HSS makes the HSS itself more vulnerable to DoS attacks.

- S-CSCF temporarily needs to store authentication related information:

  This not the case, when authentication is carried out in the HSS. But: the S-CSCF has to keep user state anyhow, so the additional burden may not be too large. In general, the HSS is considered a more precious resource than the S-CSCF as there are few HSSs handling a very large number of users.

5 Conclusions

The above discussion shows on the one hand, that the information flow included by the editor in the latest version of [3G TS 33.203] may be inconsistent with the security assumptions underlying the termination of IMS authentication in the home. This, however, could be easily remedied by a minor change to the information flow. In section 3 an alternative approach is presented where the S-CSCF is the authentication termination point. Section 4 suggests that the pros for this alternative solution outweigh the cons. However, before a final decision on the termination point for authentication can be taken all information flows possibly involving authentication should be examined. These information flows include re-registration, session set-up (INVITE) and re-synchronisation. Corresponding slides will be provided by Siemens for the S3#17bis ad-hoc meeting.

6 References

[3G TS 23.228] 3GPP TSG SA WG2 Architecture, TS 23.228: *IP Multimedia (IM) Subsystem - Stage 2;* v. 2.0.0, March 2001.

[3G TS 33.203] 3GPP TSG SA WG3 Security, TS 33.203: *Access security for IP-based services (Release 5)";* v 0.2.0, March 2001.

[S3-010100] 3GPP TSG SA WG3 Security, S3-010100: *Proposal on IM domain access security;* SA WG3 #17, Göteborg, 27 Feb – 2 March 2001.