3GPP TSG SA WG3 Security — S3#16 **S3-000710**

28-30 November, 2000

Sophia Antipolis, France

Source: **Nokia**

Title: **IMS authentication in both visited and home networks**

Document for: **Discussion**

Agenda Item:

There has been an on-going discussion on whether authentication between user and IMS should be executed in visited network (P-CSCF) or in home network (S-CSCF or HSS). We propose authenticating the user at two points: in P-CSCF and in S-CSCF. The first is needed to give visited network control on identities of the users that are utilizing this network's services. On the other hand, S-CSCF is the unit that controls services offered to the user and, therefore, should authenticate the user also.

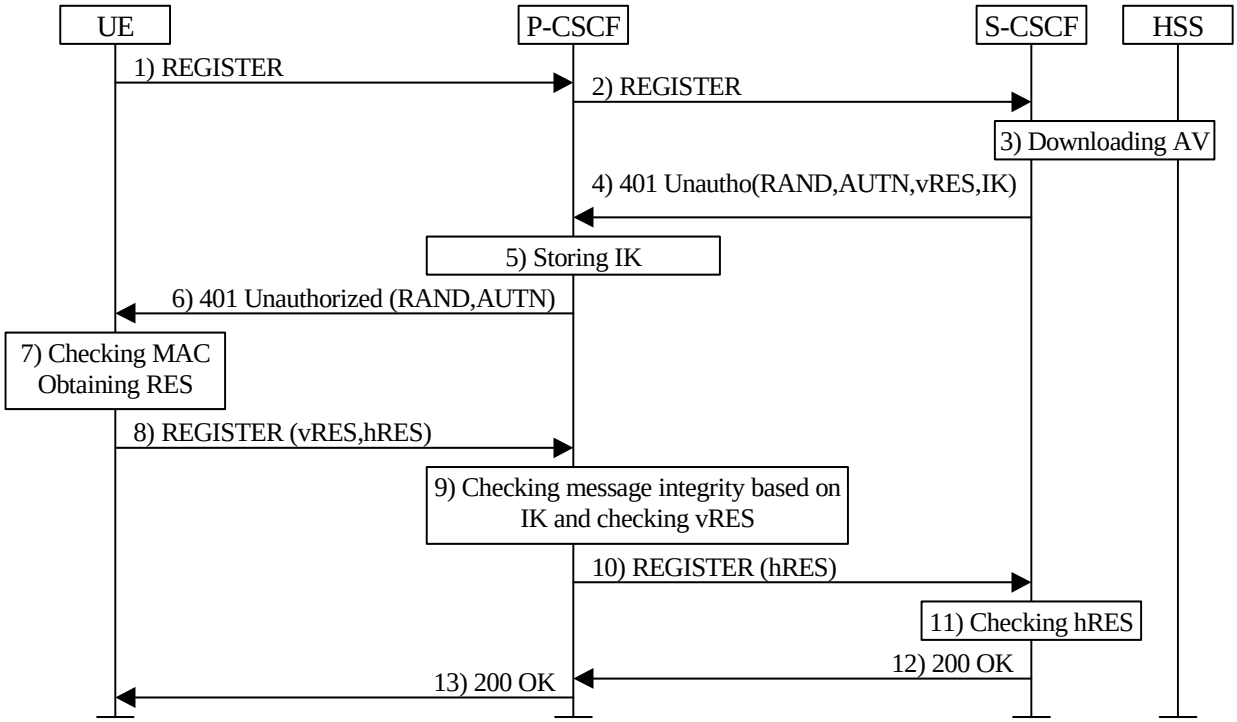
In this solution the UMTS AKA mechanism itself is slightly enhanced. Basically the enhancement can be realized for R99 UMTS networks also (and even GSM networks) if a better home control is wanted. This is the case at least in the 3GPP2 networks.

The RES parameter in UMTS AKA is so long in the maximal case that it can be divided into two halves and still checking of each half individually provides adequate security.

We denote RES = vRES | hRES. Only vRES is delivered to the P-CSCF. If P-CSCF does not implement authentication correctly, it cannot obtain hRES from the user. Hence, home network has final control over the authentication executed by the P-CSCF.

The key CK that is also generated during the UMTS AKA can be used for integrity protection of SIP messages between UE and S-CSCF. The fact that CK is used for confidentiality purposes in UMTS R99 UTRAN does not restrict its use for integrity purposes in IMS.

For the sake of simplicity, the first contact point in home network, i.e. I-CSCF is omitted from the figure below.



1. UE sends REGISTER request to the P-CSCF without authentication data.
2. P-CSCF forwards the REGISTER request to the S-CSCF.
3. The S-CSCF downloads the user profile, which includes the authentication vectors, from the HSS. The key CK is stored for further use in protection of signaling between UE and S-CSCF.
4. The S-CSCF sends back a 401 Unauthorized response to the P-CSCF with the following authentication data: RAND, AUTN, vRES and IK.
5. The P-CSCF stores the IK value and removes it from the SIP message.
6. The P-CSCF forwards 401 Unauthorized response with the authentication data (RAND and AUTN) to the UE.
7. UE authenticates the network (checks the value of the MAC) and generates the RES and the keys IK and CK.
8. UE sends a new REGISTER request that contains the RES and a message authentication code generated with IK to the P-CSCF.
9. The P-CSCF checks the integrity of the message, which also includes subscriber authentication since the message authentication code is generated with IK. At the same time, P-CSCF checks that the first part of RES matches vRES.
10. The P-CSCF forwards REGISTER request with the authentication data (RES and message authentication code) to the S-CSCF.
11. The S-CSCF accepts the REGISTER request if the latter part of RES value matches the hRES value and the message contains a valid message authentication code (calculated by IK).
12. The S-CSCF sends a 200OK response after the successful registration.
13. The P-CSCF forwards the 200OK to the UE.