3GPP TSG SA WG3 Security **S3-000689**
Meeting S3#16

Sophia Antipolis, 28-30 November, 2000

Source: Siemens AG

Title: IMS authentication and integrity/confidentiality protection

Document for: Discussion / Decision

Work item: Access security for IP-based services

Agenda item: tbd

Abstract

This contribution is un update of the Siemens contribution Sz00022 proposes that the P-CSCF shall perform the IMS AKA with the UE by re-using the UMTS AKA mechanism through SIP and that the P-CSCF terminates integrity/confidentiality protection of SIP messages from the UE. For the further SIP hops in the network, integrity/confidentiality protection shall be provided by network domain security features using IPSec.

1 Introduction

This document is based on [S3z000022]. The basic ideas of the IMS security architecture described there are still the valid in this contribution. Additional arguments are only incorporated into section 3, where the consequences of the security architecture described in section 2 are discussed and a comparison with the Ericsson contribution [S3z000010] is made.

The scope of this document is to provide an answer to two questions, which will have major impact on the security architecture of the IMS:

- Which network entity should perform authentication and key agreement (AKA) with the UE for SIP registration of a (roaming) user?
- Which network entity should terminate the access integrity/confidentiality protection of SIP messages with the UE?

We base our discussion on the following 3GPP SA 3 working assumption [3G TR 33.8xx, section 8]:

- For the provision of access network security in the IM domain the UMTS authentication and key agreement (AKA) protocol [3G TS 33.102] is performed through the SIP protocol (IMS AKA mechanism). To achieve this a new authentication mode for SIP has to be standardised.

The scenario described in section 2 provides a solution for both questions. Section 3 discusses the pros and cons of the scenario compared to an alternative scenario of Ericsson in [S3z000010]. Section 4 contains the conclusions from the discussion and proposes new working assumptions for the further work in 3G SA3 on IMS security.

2 Proposal for IMS access security

It is proposed that the P-CSCF performs IMS AKA but also terminates integrity/confidentiality to the UE. Figure 1 below shows the information flow for a SIP register message, in the case that no authentication information for this user is available at the P-CSCF and authentication has to be performed. If authentication information for the user is available at the P-CSCF the information flow is simplified: messages 2 to 6 can then be omitted. Note, that authentication information for the user may be available at the P-CSCF from a previous registration because in our proposal it is possible to send a batch of authentication vectors from the HSS to the P-CSCF.

Note also, that the I-CSCF needs to distinguish between the *Register* messages received from the P-CSCF in message 2 and in message 10. For this purpose, a corresponding parameter in the *Register* message has to be defined, and specific values have to be assigned to the different *Register* message types by 3GPP. Besides the pre-defined values for *Auth Info Indication* and *Proceed Indication* e.g. at least a pre-defined value for *Re-Synchronation Indication* will be required (for message 10).

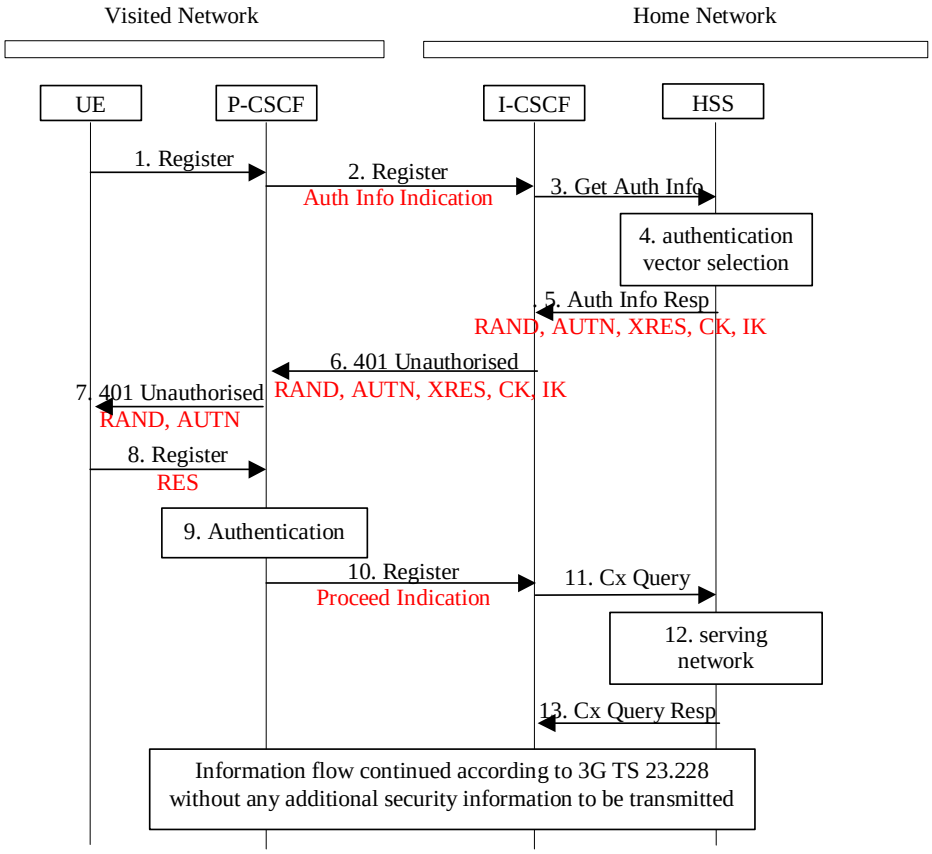

Figure 1: P-CSCF performs IMS AKA and terminates integrity/confidentiality to the UE

Description of the information flow:

1. The mobile node sends a SIP *Register* message to the P-CSCF.
2. The P-CSCF detects that it has no subscriber authentication information available (from previous protocol runs, e.g. initial registration) and authentication has to be performed. It therefore forwards the SIP *Register* message to the I-CSCF in the user's home network.
3. The I-CSCF notices that the SIP *Register* message contains an *Auth Info Indication* and requests the UMTS authentication vector, i.e. the quintet *(RAND, AUTN, XRES, CK, IK)*, by sending a *Get Auth Info* messages to the HSS.
4. The HSS selects the authentication vector. (The HSS may either calculate this authentication vector in real-time in the AuC or may retrieve the pre-calculated values from storage.)
5. The HSS responds with an *Auth Info Resp* message to the I-CSCF, which contains the quintet *(RAND, AUTN, XRES, CK, IK)*.

6. The I-CSCF forwards the security information quintet in a SIP *401 Unauthorised* message to the P-CSCF.

   Note: In order to carry the UMTS AKA parameters within SIP, document [3G TR 33.8xx, section 8.1] already specifies a new authentication mode. This mode allows to transmit the two parameters *RAND*, *AUTN* within a SIP 401 Unauthorised message. This new specification would simply have to be extended in order to carry the quintet *(RAND, AUTN, XRES, CK, IK)* from the I-CSCF to the P-CSCF.

   This extension may also be further extended to allow for a transmission of more than one quintet (in analogy to the UMTS CS- and PS-domains). This would avoid that the visited network would have to contact the home network for each authentication attempt.

7. The P-CSCF stores the received quintuple, extracts the data elements *(RAND*, *AUTN)* and sends them in a SIP *401 Unauthorised Authentication* message to the UE.
8. The UE computes its security information from the received data elements, checks if the network is authentic and sends its authentication value *RES* in a new SIP *Register* message to the P-CSCF.
9. The P-CSCF checks the received value *RES* for validity by comparing it with the stores value *XRES* and thereby authenticates the UE.
10. The P-CSCF sends a *Register* message with a *Proceed Indication* to the I-CSCF.
11. Now the information flow is continued according to [3G TS 23.228]. The I-CSCF sees the *Register* message with the *Proceed Indication* and decides to subsequently send a *Cx Query* to the HSS; the HSS responds with a *Cx Query Resp* to the I-CSCF, ...

In the information flows in figure 1, it is implied that the P-CSCF terminates the integrity/confidentiality protection of SIP messages from the UE. For this reason, the session keys *IK*, *CK* are sent to the P-CSCF together with the other security information needed for authentication.

3 Discussion

In the following we list the pros and cons for the case that the P-CSCF

- performs the IMS AKA with the UE and
- is the point of termination for integrity/confidentiality protection of SIP messages from the UE.

3.1 Location of integrity/confidentiality protection functionality for the IMS

(1) Confidentiality and integrity protection should be co-located in the same network entity. Otherwise the following drawbacks are seen:

- Two different network entities have to be provided with the appropriate security functionality, including additional mechanisms for control of access to the entity, secure storage of the secret key material, reliability, etc.
- In order to agree on the parameters for the security associations for integrity and confidentiality protection, an equivalent to the security mode set-up procedure in the UMTS PS- and CS-domain is needed. (This feature still has to be defined for the IM domain!) This security mode procedure would have to be implemented in both network entities, and the UE would have to carry out this procedure twice, once with each of the two network entities involved.
- The key management for the integrity and confidentiality keys could become complicated:

  For UMTS, document [3G TS 33.102, section 6.4.1] mentions the possibility of a network-initiated re-authentication which may e.g. also be performed during an ongoing connection. In UMTS this re-authentication is initiated by the VLR or the SGSN, respectively. An analogous seems to be required for the IMS. The change of *CK* and *IK* in the course of such an IMS network-initiated re-authentication procedure requires a synchronisation between both network entities holding *CK* and *IK*, respectively. Otherwise, the UE may have to perform the change

from the old to the new session keys for ciphering and integrity protection at different times which again would introduce additional complexity into the UE.

(2) Access network integrity/confidentiality protection with the UE should be terminated in the P-CSCF for the following reasons:

- Access network confidentiality protection with the UE should be terminated in the visited network, at least for lawful interception reasons. The only network entity which is always available in the visited network, is the P-CSCF. We therefore propose to terminate confidentiality protection in the P-CSCF.
- As a result of the discussion above this implies that also integrity protection has to be terminated in the P-CSCF.

(3) Comparison of the proposal in section 2 above with the contribution from Ericsson [S3z000010]:

Ericsson proposes in this contribution, to terminate integrity in the S-CSCF and to terminate confidentiality protection as well as an additional integrity protection mechanism in the P-CSCF. Apart from the drawbacks already mentioned above, of having the two security mechanisms (i.e. integrity and confidentiality) performed in different network entities, we see the following additional drawbacks:

- The S-CSCF may be located in the visited or in the home network. Depending on this property, two different security related information flows have to be specified. In contrast, in the Siemens proposal in section 2 above the security related information flow is always the same.
- It seems odd to integrity-protect SIP messages twice: once at the application layer between the UE and the S-CSCF and a second time (optionally) by means of WTLS between the UE and the P-CSCF. In addition, it should be questioned whether WTLS is the right choice: WTLS necessitates another handshake to derive confidentiality and integrity keys for WTLS from the CK which is used as a master key for WTLS which seems unnecessary. Furthermore, it is not clear why one should have two different mechanisms, one at the application layer and one at the transport layer. Even if confidentiality was to be performed at an entity different from that which performs integrity it would seem more natural to define also a confidentiality mechanism at the application layer.

3.2 Location of IMS AKA functionality

Authentication information is only computed in the AuC (part of the HSS) and in the USIM. The question to decide is which network entity determines that the outcome of the user authentication has been successful. This involves comparing parameters received in an authentication vector from the HSS with the parameters received from the UE. The same entity must also be capable of handling the re-synchronisation procedure. (This feature still has to be defined for the IM domain!)

But still, the implementation effort for handling of the IMS AKA appears considerably lower than for the implementation of the confidentiality and integrity functions and the corresponding security mode set-up procedure. Moreover, the resource required to execute the IMS AKA mechanism between the appropriate network entity and the UE also appears to be a considerably lower effort than the handling of integrity/confidentiality protected SIP messages. These facts contribute to the suggestion proposed in (1) below.

(1) The P-CSCF should perform the IMS AKA with the UE for the following reasons:

- The P-CSCF has to be enhanced to handle the confidentiality and integrity functions anyway, according to our proposal in section 3.1 above, so the handling of the AKA seems to be a tolerable additional burden for the P-CSCF. (For justification cf. to the facts mentioned in the preceding paragraph.)
- If the AKA is handled in the P-CSCF the paradigm for the HSS applied so far in UMTS and GSM could be preserved: the HSS would just be a database which responds to queries. If the AKA was handled in the HSS the HSS would have to send out requests and wait for responses, for a

potentially large number of users simultaneously. (Cf. also information flows in [S3z000010, section 4.5.1].) This could reduce HSS performance.

The latter fact could also make the HSS more vulnerable to denial of service attacks, as (compared to the [S3z000022] proposal) it is determined later in the protocol run, that authentication of a user has failed and, moreover, in the meantime the HSS has to keep the state of each of these users.

- Since all IMS security (AKA as well as integrity/confidentiality protection) is carried out in the same entity no procedure to transfer the integrity/encryption keys is required.
- The visited network may want to control the lifetime of *CK* and *IK* by triggering a re-authentication. If it (i.e. the P-CSCF) has stored an additional quintuple it can do so without having to contact the home network. In any case, if the AKA is located in the HSS re-authentication seems more complicated as the HSS has to be triggered by the visited network and the result has to be distributed to two different entities in the visited network.
- The IMS AKA is analogous to UMTS authentication. Therefore a re-use of the mechanisms e.g. for generating the security information in the HSS/AuC but also in the USIM is possible.
- The visited network has control over mobiles roaming in its network.
- In the Ericsson proposal the home network HSS has to be contacted for each authentication attempt, whereas in the proposal made here authentication information for a user may be available at the P-CSCF from a previous registration because in our proposal it is possible to send a batch of authentication vectors from the HSS to the P-CSCF. Therefore the Ericsson proposal may imply a higher network load in the home network.

(2) The proposal in section 2 above is compatible with access independence:

If a user wants to access IM domain services via a non-UMTS visited network there will be, of course, no P-CSCF with the desired security functionality in that non-UMTS visited network. In that case, the user must access a P-CSCF with the desired security functionality at the boarder of the (UMTS) home network. The address of that P-CSCF could e.g. be known to the UE as the default address of a SIP proxy for access over a non-UMTS network. P-CSCF entities are available in the home network anyway for the case that the user wants to access services from his home network.

Moreover all security information flows for access to the IMS could be identical no matter whether the access network is a UMTS or a non-UMTS network.

(3) General remark on mechanisms for confidentiality and integrity

The mechanism to be used for confidentiality and integrity is unaffected by the above discussion. In the Siemens contribution [S3-000447] the mechanisms available from the IETF SIP group were examined, and it was concluded that IPSec (AH and ESP) was the only one worth to investigate further. It was therefore proposed to use IPSec as a working hypothesis. We would like to clarify here that this hypothesis should not preclude the investigation of other mechanisms for confidentiality and integrity, in particular mechanisms at the application layer.

4 Conclusions

From the discussion of the pros and cons discussed above the following working assumption is proposed for further investigations in 3G SA3:

- The P-CSCF performs the IMS AKA with the UE.
- The P-CSCF terminates access network integrity/confidentiality protection of SIP messages from the UE.

  For the further SIP hops in the network, integrity/confidentiality protection shall be provided by network domain security features using IPSec.

It is additionally proposed to incorporate these working assumptions into [3G TR 23.228] and the information flows description into [3G TS 33.2xx].

Note, that in contrast to what is stated to date in [3G TR 33.8xx], end-to-end integrity between UE and S-CSCF is not a requirement for the IM domain. The justification for this can be found in the companion contribution [S3z000023].

5 References

[S3z000010] 3GPP TSG SA WG3 Security, S3z000010: *Authentication and protection mechanisms for IM CN SS;* Source Ericsson; contribution to the ad-hoc meeting S3#15bis, Munich, 8th - 9th November 2000.

[S3z000022] 3GPP TSG SA WG3 Security, S3z000023: *IMS authentication and integrity/confidentiality protection;* Source Siemens; contribution to the ad-hoc meeting S3#15bis, Munich, 8th - 9th November 2000.

[S3z000023] 3GPP TSG SA WG3 Security, S3z000023: *Comments on 3G TR 33.8xx;* Source Siemens; contribution to the ad-hoc meeting S3#15bis, Munich, 8th - 9th November 2000.

[S3-000446] 3GPP TSG SA WG3 Security, S3-000446: *Requirements on access security for IP-based services;* Source Siemens, July 2000.

[S3-000447] 3GPP TSG SA WG3 Security: *Overview of security mechanisms for access security for IP-based services;* July 2000.

[3G TR 33.8xx] 3GPP TSG SA WG3 Security, TR 33.8xx: *Access security for IP-based services (Release 2000);* v 0.2.0, October 2000.

[3G TS 33.2xx] 3GPP TSG SA WG3 Security, TS 33.2xx: *Access security for IP-based services (Release 4)";* v 0.1.0, October 2000.

[3G TR 23.228] 3GPP TSG SA WG2, TR 23.228: IP multimedia (IM) subsystem - Stage 2; v 1.2.0, October 2000.