3GPP TSG SA WG3 Security — S3#22 **S3-020132**

25 - 28 February 2002

Bristol, UK

Source: Siemens

Title: Security association management in the UE and the P-CSCF

Document for: Discussion/ Approval

Agenda item: 7.3, IP multimedia subsystem security

---

1. Introduction

The purpose of this contribution is to contribute to the consolidation of section 7 of TS 33.203. It starts from the new structure proposed in S3-020107 on "SA handling and use" (Hutchison 3G UK), but tries to include the greater level of detail in the handling of the security associations from the old text in TS 33.203, section 7.3. It further proposes the simplifying assumption that a UE is involved in only one registration procedure at a time.

The contribution also relates to the contributions S3-020091 and S3-020092 in the following way:

Relation with contribution S3-020091 on "Unprotected registrations during SA lifetime" (Nokia): this contribution takes into account the need for unprotected re-registration messages in certain failure situations, which was identified in S3-020091.

Relation with contribution S3-020092 on "Requirements and a proposed solution for SA_ID" (Ericsson, Nortel Networks, Nokia): the need to distinguish between old and new SAs by means of SA_IDs is highlighted, cf. last sentence before section 7.4.1.1 and Note in 7.4.1.2.

2. Proposed changes to TS 33.203v110:

It is proposed to replace section 7.3.3 with the following new section 7.4:

7.4 Management and Use of Security Associations

Every successful registration or re-registration procedure that includes a user authentication produces a new pair of security associations (SAs). These new SAs shall then replace the previous SAs. This section describes how the UE and P-CSCF shall handle this replacement and which SA to apply to which message. The section also specifies how the lifetime of security associations can be limited.

7.4.1 Management of security associations

Security associations may be unidirectional or bi-directional. This section assumes that security associations are unidirectional, as this is the general case.
For release 5, at any one time, there shall be at most two security associations stored at a UE, and at most two security associations per UE stored at a P-CSCF, for each direction.

Whenever a user is registered there is a **current SA** for each direction. In addition, there may be a **registration SA** for each direction. Their use is explained in the following. They are denoted as follows:

SA_in_cur	current inbound SA
SA_out_cur	current outbound SA
SA_in_reg	registration inbound SA
SA_out_reg	registration outbound SA

This notation has local significance only. That means that SA_in_cur at the UE equals SA_out_cur at the P-CSCF,and similarly for the other SAs.

The current and the registration SAs shall be distinguished by different SA_IDs.

7.4.1.1 Management of security associations in the UE

The text in this subsection makes reference to the messages in Figure ?? of section 7.2.

The UE shall be involved in only one authenticated registration procedure at a time. Upon starting a new registration procedure, the existing registration SAs are deleted.

The registration proceeds in the following steps:

1) The UE sends SM1 to register with the IMS. SM1 should be integrity-protected using SA_out_cur if available. In initial registrations or in certain failure cases, SM1 is sent unprotected.

2) The UE receives SM6 from the P-CSCF. SM6 shall be integrity-protected using SA_in_cur if SM1 was integrity-protected using SA_out_cur.

3) If SM6 can be successfully processed by the UE, the UE creates the new SAs SA_in_reg and SA_out_reg, which are derived according to section 7.2. The UE then sends SM7 to the P-CSCF. SM7 is protected with SA_out_reg.

4) The UE receives SM12 from the P-CSCF, which shall be protected using SA_in_reg.

5) After the successful processing of SM12 by the UE, the re-registration is complete.

After the completion of the registration procedure, the SAs are handled as follows:

6) SA_out_reg becomes the new SA_out_cur and there is no more SA_out_reg.

7) When a further SIP message protected with SA_in_reg is successfully received from the P-CSCF, SA_in_reg becomes the new SA_in_cur and there is no more SA_out_reg.

The UE applies the current SAs to all SIP messages unless specified otherwise in this subsection.

7.4.1.2 Management of security associations in the P-CSCF

The text in this subsection makes reference to the message in Figure ?? of section 7.2.

The P-CSCF shall be involved with a given UE in only one authenticated registration procedure at a time. When the P-CSCF receives a message from the UE starting a new registration procedure, the existing registration SAs for that UE are deleted.

The registration proceeds in the following steps:

1) The P-CSCF receives SM1. SM1 should be integrity-protect using SA_in_cur if available. In initial registrations or in certain failure cases, SM1 is received unprotected.

2) The P-CSCF sends SM6 to the.UE. SM6 shall be integrity-protected using SA_out_cur if SM1 was integrity-protected using SA_in_cur.

3) The P-CSCF then creates the new SAs SA_in_reg and SA_out_reg, which are derived according to section 7.2.

4) The P-CSCF receives SM7 from the UE. SM7 shall be protected using SA_in_reg.

5) The P-CSCF sends SM12 to the UE. SM12 shall be protected using SA_out_reg. This completes the registration procedure for the P-CSCF.

After the completion of the registration procedure, the SAs are handled as follows:

6) The P-CSCF continues to use SA_out_cur for outbound traffic to the UE until it receives a further SIP message protected with SA_in_reg from the UE.

Note: In case the UE did not successfully receive SM12 the P-CSCF will receive further SIP message from te UE protected with SA_ in_cur. In order for the P-CSCF to be able to efficiently decide which SA to apply there have to be different SA_IDs for the registration SA and the current SA.

7) When the P-CSCF successfully receives a further SIP message protected with SA_in_reg from the UE, then SA_in_reg and SA_out_reg becomes the new SA_in_cur and SA_out_cur respectively, and there are no more registration SAs.

The P-CSCF applies the current SAs to all SIP messages unless specified otherwise in this subsection.

The P-CSCF associates the IMPI given in the registration procedure and all the successfully registered IMPUs related to that IMPI with the current SAs.

7.4.2 Security association lifetimes

The UE shall delete any SA whose expiry time is exceeded.

The expiry time of the current SA must be kept later than the expiry time of all registered IMPUs,

In the case of a UE-initiated re-registration, the UE may set a timer T-U according to the security policies of the UE as follows: the UE deletes SA2 after the expiry of T-U. This is to make sure that the old SA can be used once more to avoid service disruption, but cannot be used indefinitely.

Note: in Release 6, there will be network-initiated re-registrations. In the case of a network-initiated re-registration the P-CSCF may set a timer T-P according to the security policies of the P-CSCF as follows: the P-CSCF deletes the old SAs after the expiry of T-P. This is to make sure that the old SAs cannot be used indefinitely. In order to avoid disruption of service, the UE should take care to make another re-registration attempt before the expiry of T-U.