3GPP TSG SA WG3 Security — S3#22 **S3-020107**

25 - 28 February 2002

Bristol, UK

Source: **Hutchison 3G UK**

Title: **SA handling and use**

Document for: **Discussion/Decision**

Agenda Item: **7.3**

Introduction

This contribution is a revised version of S3z020026 that was submitted to the Ad-hoc in Antwerp.

The contribution proposes revised text for the handling of security associations and some new text on the use of security associations. The proposed text deals with the following issues

- Ensures that the new security associations are used after an authentication by reducing the expiry timers of the other SAs.
- Overcomes a problem with the current SA handling procedures by introducing Registration SAs.
- States which SAs to use to protect traffic and provides rules for protecting the first messages and failure messages in a registration procedure.

Discussion of Proposed Modifications

The proposed method of handling SAs builds on the method already given in the text by adding the concept of Registration SAs to overcome the following problem.

- Suppose a registration procedure including an authentication has taken place. This process generates a new pair of SAs that should be used to replace the previous SAs. This means the UE has the following SAs, SA1_p_u (the old SA for traffic to the UE), SA2_p_u and SA2_u_p (the new SAs for traffic to and from the UE respectively). The P-CSCF has the same SA plus SA1_u_p (the old SA for traffic from the UE).

  Now suppose another (re-) register procedure is initiated without integrity protection and the UE successfully receives SM6. Both the UE and P-CSCF now have SA3_p_u and SA3_u_p (the "new new" SAs for traffic to and from the UE respectively). Nothing in the specification deals with the situation of three sets of SAs at the UE or P-CSCF. At the P-CSCF, SA3_u_p and SA3_p_u should not overwrite SA2_u_p and SA2_p_u as there could still be a registration failure. Traffic to the UE must still be protected with SA1_p_u. Therefore all three sets must be kept. Hence it is proposed to introduce the concept of Registration SAs.

The proposed text is also written to deal with more than one authenticated (re-) registration at a time. This seems an unnecessary requirement if (re-) registrations without user authentications are allowed.

In registrations procedures the first messages and all failure messages can be protected by previously established SAs. The text proposes that the UE should in general protect all of these messages and the P-CSCF protects all messages once the UE has protected one. Perhaps the only exception for the UE is if it is having problems sending protected traffic to the P-CSCF and wants to negotiate new SAs.

Conclusions

This contribution proposes the changes to TS 33.200 given in the attached pseudo_CR. SA3 is asked to accept these changes.

This contribution also suggests that SA3 should consider limiting the number of registrations a UE can be simultaneously involved in.

************************ FIRST MODIFIED SECTION ****************

6.1 Authentication and key agreement

The scheme for authentication and key agreement in the IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. Figure 3. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. [3]. The HSS and the ISIM share a long-term key associated with the IMPI.

For the IMS the ISIM and the HSS keeps track of the counters SQN$_{ISIM}$ and SQN$_{HSS}$~~.~~ respectively. The handling of the SQN can be as in [1]. The HN shall choose the IMS AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g. keys generated by the IMS AKA scheme are transported by SIP.

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. For each user it is the HSS that keeps track of the counter SQN$_{HSS}$. The requirements on the SQN handling both in the Home Network i.e. the HSS and the ISIM are specified in [1]. The AMF field can be used in the same way as in [1].

Furthermore a security association is established between the UE and the P-CSCF. The subscriber may have several IMPUs associated with one IMPI. These can ~~and~~ belong to the same or different service profiles. Only one SA shall be active between the UE and the P-CSCF. This single SA shall be updated when a new successful authenticated re-registration has occurred, cf. section 7.4.1~~3.3~~.

It is the policy of the HN that decides if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles. Regarding the definition of service profiles and implicit registrations cf. [3].

******************* NEXT MODIFIED SECTION **********************

7.3.3 Authenticated re-registration

If the registration is a re-registration, a pair of security associations between UE and P-CSCF is already active. The authenticated re-registration shall initially utilize the existing SA.

[Editors Note: It is under investigation if unprotected re-registration shall be allowed during the SA-Lifetime.]

~~Before SM7 is sent by the UE, both peers shall replace the existing SA by the new SA negotiated during these first two messages.~~

~~7.3.3.1 Handling of security associations in authenticated re-registrations (successful case)~~

~~Before re-registration begins the following SAs exist:~~

~~-SA1 from UE to P-CSCF~~

~~-SA2 from P-CSCF to UE~~

~~The re-registration then is as follows:~~

~~1) The UE sends SM1 to re-register with the IMS, using the existing SA1 to the P-CSCF. As in the case of a new registration, a list of parameters to be negotiated in a security association set-up is included.~~

~~*[Editors Note: It is FFS if the SA1 shall be used for SM1 or not]*~~

~~2) The P-CSCF waits for the response SM4 from the S-CSCF and then sends SM6 to the UE, using SA2. As in the case of a new registration, the parameters selected for the new security associations are included. The P-CSCF then creates two new security associations, in parallel to the existing ones, in its database:~~

~~- SA11 from UE to P-CSCF~~

~~- SA12 from P-CSCF to UE~~

~~3) If SM6 could be successfully processed by the UE, the UE also creates the new SAs SA11 and SA12 in its database. The UE then sends SM7 to the P-CSCF. As in the case of a new registration, the authentication response and the list of parameters repeated from message 1 are included. SM7 is protected with the new SA11.~~

~~4) The P-CSCF waits for the response SM10 from the S-CSCF and then sends SM12 to the UE, using the new SA 12.~~

~~5) After the reception of SM12 by the UE, the re-registration is complete.~~

~~The UE now uses the new SAs for all subsequent messages. The old (outbound) SA1 is deleted. The old (inbound) SA2 must be kept until a further SIP message protected with the new inbound SA12 is successfully received from the P-CSCF.~~

~~The P-CSCF keeps all four SAs with the UE active until a further SIP message protected with the new inbound SA11 is successfully received from the UE. In the meantime, the P-CSCF continues to use the old SA2 for outbound traffic to the UE.~~

~~7.3.3.2 Error cases related to authenticated re-registration~~

~~Whenever an expected message is not received after a time-out the receiving entity considers the registration to have failed. The receiving entity then deletes any new security associations it may have established and continues to use the old ones if they have not yet expired.~~

~~If the registration protocol goes well up to the last message SM12, and SM12 is sent by the P-CSCF, but not received by the UE , then the UE has only the olds SAs available (after the time-out), but the P-CSCF cannot know this. Therefore, the P-CSCF continues to use the old SA2 for outbound traffic to the UE, but keeps both, old and new SAs. The new SAs are deleted when a message is received from the UE which is protected with the old SA, or if a REGISTER message is received on the port where the P-CSCF accepts specific unprotected messages.~~

************** NEXT MODIFIED SECTION *********************

7.4 Management and Use of Security Associations

Every (re-) registration procedure that includes a user authentication potentially produces a new pair of security associations (SAs). These new SAs should then replace the previous SAs. This section describes how the UE and P-CSCF should handle this replacement and which SA to use when the more than one.

7.4.1 Management of security associations

7.4.1.1 Management of security associations in the UE

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

SAs created during a (re-) registration procedure are considered **Registration** SAs until that (re-) registration procedure is complete. They should be given a short lifetime and deleted if there is some failure in the (re-) registration procedure. The UE needs to store one registration pair of SAs for each registration and re-registration the UE is currently involved in.

Upon the successful completion of an authenticated (re-) registration, the inbound/outbound SA created during that (re-) registration procedure become the **Current** inbound/outbound SA at the UE, if they are the most recent pair of SAs created based on the CSeq number of the last message in the (re-) registration procedure.

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

If the Current SAs are changed, the original inbound Current SA becomes the **Old** SA, if the original outbound Current SA was ever used to protect a message outside the (re-) registration procedure that created it or there is no Old SA.

If the UE ever receives a message protected by the Current inbound SA, it can delete the Old inbound SA.

7.4.1.2 Management of security associations in the P-CSCF

The P-CSCF should delete any SA whose expiry time is exceeded.

SAs created during a (re-) registration procedure are considered **Registration** SAs until that (re-) registration procedure is complete. They should be given a short lifetime and deleted if there is some failure in the (re-) registration procedure. The P-CSCF should be capable of storing as least as many pairs of registration SAs as the total number of registration and re-registration the UE is capable of being simultaneously involved in.

Once the P-CSCF has received an authentication successful response, the P-CSCF considers the pair of SAs created by the registration procedure to be **Valid**.

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

The P-CSCF stores the Valid SA pairs from a UE in order based on the CSeq number. The expiry timer of the new pair of SAs should be set to the maximum of the expiry time given in the successful registration message and the expiry time of all stored older Valid SAs. Older Valid SAs should have their expiry time set to expire in a short time (enough time for the UE to realise it has not received a success or failure response to its REGISTER request containing RES and perform a successful authenticated (re-) registration). This must be enforced even if messages arrive out of order.

If the P-CSCF receives a message protected with the inbound SA of a Valid pair, it make that pair of SAs the **Current** pair and deletes all the older Valid SAs. If the P-CSCF runs out of space to hold Valid SAs, it should delete the oldest pair, which is not Current, in order to store the new one. To be robust the P-CSCF needs to be able to store as many Valid pairs of SAs as the total number of registration and re-registration the UE is capable of being simultaneously involved plus one.

7.4.2 Use of the Security Associations to Protect Signalling

7.4.2.1 Signalling from UE to P-CSCF

The UE must protect SIP signalling towards the P-CSCF using an outbound SA whose expiry time has not been exceeded according to the following rules:

- Requests or Responses, that are not REGISTER requests must be protected with the Current SA.
- A REGISTER request that has its expiry time set to 0 (i.e. a de-register message) must be protected with the Current outbound SA.
- REGISTER request carrying a RES must be protected with the Registration SA created during that (re-) registration procedure.
- Other REGISTER requests can be protected with either the Current outbound SA or not protected. In general the UE should protect these requests if it has a Current outbound SA. Furthermore once it has protected a message in a registration procedure with a non-Registration SA, it shall protect all messages in that registration procedure.

If the expiry time of the SA used to protect the message has been exceeded, the P-CSCF treats the message as though integrity protection has failed.

On receiving a Request or Response, which is not a REGISTER request, the P-CSCF shall ensure that the SA used to protect it was a Valid inbound SA for that IMPU. If the wrong SA was used to protect the message or there was no SA applied, the P-CSCF treats the message as though integrity protection has failed.

On receiving a REGISTER request, the P-CSCF does the following:

- If it is a de-register message, i.e. expiry timer set to 0, then the P-CSCF shall ensure that it was protected with a Valid inbound SA for that IMPU.
- If it carries a RES, then the P-CSCF shall ensure that it was protected with the inbound Registration SA created during that (re-) registration procedure.
- Otherwise, the P-CSCF shall ensure that if it was proctected, it was done with a Valid inbound SA for the IMPI in the REGISTER request and that it was protected if any earlier REGESTER request in the registration procedure was protected with a non-Registration SA.

If the wrong SA was used to protect the message or no SA was used when one was required, the P-CSCF treats the message as though integrity protection has failed.

7.4.2.2 Signalling from P-CSCF to UE

The P-CSCF shall protect SIP signalling towards the UE using an SA whose expiry time has not been exceeded according to the following rules:

- Messages outside (re-) registration flows shall be protected with either the Current outbound SA for that IMPU or if there is not a Current SA, the most recent Valid SA for that IMPU.
- A successful registration acknowledgement shall be protected with the outbound Registration SA created during that (re-) registration procedure.

- Other messages in (re-) registration procedure shall be protected with the Current outbound SA for the IMPI if it exists and the UE has protected an earlier message in the (re-) registration with a non-Registration SA.

If the expiry time of the SA used to protect the message has been exceeded, the UE treats the message as though integrity protection has failed.

On receiving a message outside a (re-) registration procedure, the UE shall ensure it was protected with either the Current inbound SA or an Old SA. If the wrong SA or no SA was used to protect the message, the UE treats the message as though integrity protection has failed.

On receiving a successful registration acknowledgement, the UE shall ensure it was protected with the inbound Registration SA created during that (re-) registration procedure. If the wrong SA or no SA was used to protect the message, treats the message as though integrity protection has failed.

On receiving any other message from a (re-) registration procedure, the UE shall ensure it was protected with either the Current inbound SA or an Old SA if it has protected an earlier message in the (re-) registration with a non-Registration SA. If the wrong SA or no SA was used when it should have been, the UE treats the message as though integrity protection has failed.