3GPP TSG SA WG3 Security **S3-020361**

9th – 12th July, 2002

Helsinki, Finland

Agenda Item:	TBD
Source:	Ericsson
Title:	SA handling
Document for:	Discussion and decision

1. Introduction

SA3 is currently discussing the number of security associations (SAs) needed between the UE and P-CSCF.

The current version of TS33.203 proposes that there will be at least 2 x 2 x 2 = 8 SAs (two directions, two temporarily SAs for re-registrations, and two transport protocols). It has also been proposed that since the re-registrations use existing SAs, and because there are some potential error situations, additional three SAs are needed for each inbound/outbound/existing/new SA quartet [S3-020292] (one for UE and two for P-CSCF). This concludes all together 12 SAs.

In general, the SA handling procedure is becoming overcomplicated. This paper discusses how it could be simplified, and how the number of needed SAs could be kept in minimum.

The proposal is to tie the SA-handling to registration messages only.

Accompanied CR to 33.203 has been submitted.

2. SA handling

According to S3-020292, it is possible to have the following kind of SAs between the UE and P-CSCF:

- Two SAs, one for each direction (inbound and outbound).
- At the time of SA creation, the number of SAs is sometimes temporarily doubled (existing and new SAs).
- Three additional SAs are needed for specific error cases, one for UE, two for P-CSCF.
- All of the previous SAs must be received for UDP and TCP separately.

Complex SA handing procedure might cause problems in security basically because it is difficult to understand and analyse. There may always be some security problems that are not found, for example. Even if the procedure was secure, interoperability between different implementations may still cause problems if the software designers have difficulties understanding the scheme.

All the SAs presented in [S3-020292] are most probably needed in order to make the procedure secure for every possible situations. It is not easy to see alternative solutions that would not danger the security but would still meet all the assumed requirements. However, the solution will lead to situation in which P-CSCF must check the status of SAs with every SIP message. This is because the SA handling procedures are extended outside the registration. For example, old SAs can only be deleted after the next message after the SM12 (last response to REGISTER message).

Ericsson believes that the SA handling procedure may become too complicated, and that some simplifications can be done. The following sub-sections describe concepts and procedures for SA handing when only eight SAs are used. The SA handling is restricted to registration messages only.

The major difference of this approach to the current version of 33.203 is that while doing authenticated re-registration using already existing SAs, the old SAs are removed already after SM10 (P-CSCF) and SM12 (UE). This procedure will open a possibility for an attacker to remove existing SAs if the re-registration is sent unprotected. For this reason, re-registrations should always be sent protected if there already is a valid SA in use.

2.1 Definition of security associations

This paper uses the following names for the SAs in UE and P-CSCF:

SA_in_{udp} – inbound SA for UDP
SA_out_{udp} – outbound SA for UDP
SA_in_{tcp} – inbound SA for TCP
SA_out_{tcp} – outbound SA for TCP

UE and P-CSCF refer to one particular SA using the opposite naming because what is inbound for UE is outbound for P-CSCF:

$UE(SA\_in_{udp}) = P\text{-}CSCF(SA\_out_{udp})$

Each SA has a state. Figure 1 demonstrates all possible states of an SA: ‘negotiated’, ‘used’, and ‘deleted’.

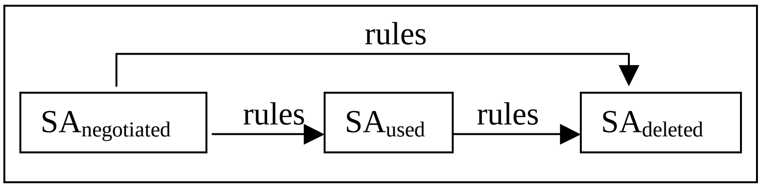

Figure 1: A state diagram for a SA

Transition between the states is guided using some specific rules.

2.2 Re-registration messages sent unprotected

Re-registration messages may be sent using the existing SA, or unprotected. Sending re-registration messages unprotected is not recommended if valid SAs exist. This sub-section describes what would happen if this was done anyway.

If the existing SAs are not used, the first REGISTER message (SM1) is sent unprotected. The second REGISTER is protected using the SA negotiated in SM1 and SM6. Figure 2 demonstrates the situation from P-CSCF perspective.

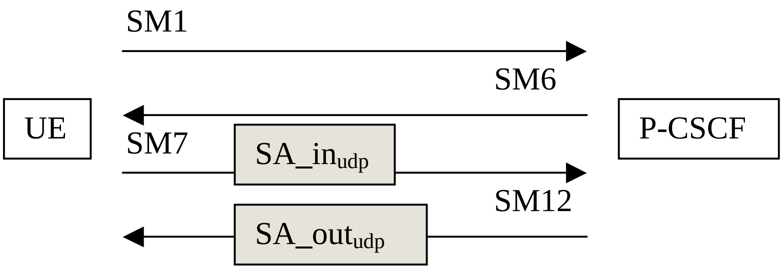

Figure 2: Unprotected registration from P-CSCF perspective

The procedure for updating the states of the SAs goes as follows:

- Rules for P-CSCF:
    - After receiving SM4, P-CSCF will create new SAs with state ‘negotiated’.
    - If P-CSCF does not receive SM7, it will (after the time-out) change the status of the new SAs from ‘negotiated’ to ‘deleted’.

- After receiving SM7, P-CSCF will know that the new inbound SA is valid. It will change the state of new inbound SA from ‘negotiated’ to ‘used’.
- After receiving SM10, P-CSCF will know that the home network is able to authenticate the UE, and it will change the state of new outbound SA from ‘negotiated’ to ‘used’. P-CSCF will also change the state of old inbound and outbound SAs from state ‘used’ to ‘deleted’.

- Rules for UE:
  - After receiving SM12, UE will know that both the inbound and outbound SAs were valid. UE change the state of all old SAs from ‘used’ to ‘deleted’, and update the state of the new SAs from ‘negotiated’ to ‘used’.
  - If UE is not able to receive SM12, and after re-transmitting SM7 several times, UE will change the state of all SAs with state ‘used’ or ‘negotiated’ to ‘deleted’.

The strength of this procedure is that the UE and P-CSCF will delete the old SAs already during the registration procedure. 33.203 currently specifies that UE and P-CSCF must wait until P-CSCF receives the next message from UE using the new SA.

The weakness of this procedure is that an attacker may modify the unprotect message SM1, and consequently UE and P-CSCF cannot use either the new or the old SAs (new SAs does not work, and old SAs have been removed). For this reason, re-registration should always be sent using an existing SA. If the existing SAs can not be used because they do not work, the attack has no effect to the use of the system because the existing SAs should be removed anyway.

2.3 Re-registration messages sent over an existing SA

In normal, UE will send a re-registration message over an existing SA. Assuming that S-CSCF will challenge the first REGISTER message, the procedure from the P-CSCF perspective is as in the figure 3. There are no changes to the SAs if S-CSCF does not challenge the re-registration message.

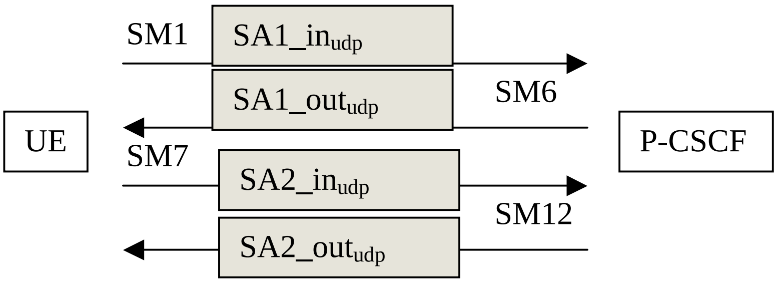

Figure 3: Protected registration from P-CSCF perspective

The procedure for updating the states of the SAs goes as follows:

- Rules for P-CSCF:
  - After receiving SM4, P-CSCF will create new SAs with state ‘negotiated’.
  - If P-CSCF does not receive SM7, it will (after the time-out) change the status of the new SAs from ‘negotiated’ to ‘deleted’.
  - After receiving SM10, P-CSCF will know that the new inbound and outbound SAs are valid because 1) UE and P-CSCF know the same key IK, 2) the home network was able to authenticate the user, and 3) messages SM1 and SM6 were protected and consequently no attacker could have modified the SA parameters under negotiation. P-CSCF will change the state of new SAs from ‘negotiated’ to ‘used’. At the same time, P-CSCF will also change the state of old inbound and outbound SAs from state ‘used’ to ‘deleted’.

- Rules for UE:
  - If UE needs to send non-register messages to P-CSCF during the registration procedure, UE shall change the status of the new outbound SA from ‘negotiated’ to ‘used’. Note that at this phase the status of the old outbound SA is also ‘used’, however, the new outbound SA is preferred.
  - If the UE does not receive SM12, and after re-transmitting SM7 a number of times, the UE shall change the status of the new SAs from ‘negotiated’ to ‘deleted’.
  - After receiving SM12, UE will know that both the inbound and outbound SAs were valid. UE change the state of all old SAs from ‘used’ to ‘deleted’, and update the state of the new SAs from ‘negotiated’ to ‘used’.

3. Conclusions

The SA handling procedures are becoming more and more complicated. They are hard to understand and analyse which may cause problems for detailed protocol design and interoperability of different implementations.

It is proposed that SA3 adopts the principles presented in this document in order to clarify and simplify the SA handling process. This SA handling process is able to operate with 8 SAs in maximum. It does include a possibility for an attack if the re-registration message is for some reason sent unprotected even when valid SAs exists. If the existing SAs are broken, the attack does not exist.

Accompanied CR to 33.203 is included.

References

[S3-020292] Hutchison 3G UK: *Update of SA handling procedures*, 3GPP, SA3#23, Change Request, document no. S3-020292, 14 – 17 May 2002, Victoria, Canada.

3GPP TSG-SA3 Meeting #24
Helsinki, Finland, Date

Tdoc DocNumber

CR-Form-v5.1

CHANGE REQUEST

⌘	**33.203**	**CR**	**CRNum**	⌘ **rev**	**-**	⌘	Current version:	**x.y.z** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM □ ME/UE ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Rules for changing SAs.		
Source:	⌘	Ericsson		
Work item code:	⌘	IMS-ASEC	***Date:*** ⌘	
Category:	⌘		***Release:*** ⌘	Rel-5
		Use one of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*Use one of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *REL-4 (Release 4)* *REL-5 (Release 5)*

Reason for change:	⌘	33.203 does not specify the exact mechanism for changing SAs.
Summary of change:	⌘	The changes specify explicitly when the existing SAs can be removed. Accompanied discussion paper describing the principle behind this approach has also been submitted (see Ericsson contribution to SA3#24 on “SA handling”).
Consequences if not approved:	⌘	IMS SA handling will not work if the missing mechanisms are not defined.

Clauses affected:	⌘		
Other specs affected:	⌘	□ Other core specifications	⌘
		□ Test specifications	
		□ O&M Specifications	
Other comments:	⌘		

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

7.4 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. This is the normal case. However, in the event the UE originates the (SM1) Register message using no protection, the P-CSCF shall still accept it and forward the request to the S-CSCF, indicating that the register message was not integrity protected. This shall trigger the S-CSCF to challenge the subscriber with the execution of a new IMS-AKA authentication procedure as described in clause 6.1.1.

~~[Editors Note: The exact mechanism for changing SAs is currently under investigation.]~~

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

~~[Editors Note: The exact mechanism when to change SA1 to SA2 under certain error conditions is FFS.]~~

7.4.1 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. Sending SM1 unprotected in the case where SA1 and SA2 exist is not allowed. 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~~SM6 are included. SM7 is protected with the new SA11. If UE needs to send non-register messages to P-CSCF during the registration procedure, UE starts using SA11 instead of SA1 at this phase.

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. P-CSCF deletes the old (inbound) SA1 and the old (outbound) SA2.

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. It also deletes the old SA1 and SA2.

~~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.~~

7.4.2 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 exist and have not yet expired. If the UE has no valid SAs the UE can only register and create new SAs via an initial REGISTER.

~~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.~~