Title:	**Correction and Alignment of SA handling procedures**
Source:	**3**
Document for:	**Discussion/Approval**
Agenda Item:	
Attachments:	**None**

Introduction

This contribution proposes a couple of small corrections to the Security Association (SA) handling procedures in TS 33.203. It also notes that the text in TS 24.229 on SA handling is not inline with TS 33.203. It proposes changes that could be made to TS 24.229 to align it with TS 33.203.

Clarification to SA3 procedures

A CR approved at the last SA plenary contained the following behaviour for the UE

"For further SIP messages sent from UE, the new outbound SAs are used, with the following exception: when a SIP message is part of a pending SIP transaction it is still sent over the old SA."

This text forces pending SIP transactions to be completed on the old SA. This seems strange as mandating the use of old SAs partly defeats the point of having the new SAs. Also using the new SA, as early as possible, allows a quicker transfer to the new SAs. Finally a strict reading the TS gives the following conclusion. Messages in pending transactions must be sent on the old SAs. Messages sent on the wrong SA must be discarded. Suppose the old SAs expire in the middle of a transaction and the UE and P-CSCF share new SAs. The new SAs can not be used to send the remaining messages in the transaction. So we are in a situation where the UE and P-CSCF could send messages securely but the TS forbids it.

This situation could be avoided by changing the "is" to a "may". A similar change would be needed in the P-CSCF section.

There is a further minor issue with the P-CSCF section, which does not make it explicit that the P-CSCF shall start using the new SAs if the old ones expire. This can be corrected by a small addition to the text.

This contribution proposes making the following changes to TS 33.203. If it is agreed, **3** will draft the appropriate CRs.

Text in clause 7.4.1a is changed as follows;

" After the successful processing of this message by the UE, the registration is complete. The UE sets the lifetime of the new SAs using the maximum of registration timer in the message and the lifetime of the old SAs. For further SIP messages sent from UE, the new outbound SAs are used, with the following exception: when a SIP message is part of a pending SIP transaction it may~~is~~ still sent over the old SA. A SIP transaction is called pending if it was started using an old SA. When a further SIP message protected with a new inbound SA is successfully received from the P-CSCF, then the old SAs shall be deleted as soon as either all pending SIP transactions have been completed, or have timed out. The old SAs shall be always deleted when the lifetime is expired. This completes the SA handling procedure for the UE."

Text in clause 7.4.2a is changed as follows;

"After SM12 is sent, the P-CSCF handles the UE related SAs according to following rules:

If there are old SAs, but SM1 is received unprotected, the P-CSCF considers error cases happened, and assumes UE does not have those old SAs for use. In this case the P-CSCF shall remove the old SAs.

If SM1 is protected with an old valid SA, the P-CSCF keeps this inbound SA and the corresponding three SAs created during the same registration with the UE active, and continues to use them. Any other old SAs are deleted. When a further SIP message protected with a new inbound SA is successfully received from the UE or the old SAs expire, the P-CSCF starts to use the new SAs for outbound messages with the following exception: when a SIP message is part of a pending SIP transaction it ~~is~~ may still sent over the old SA. A SIP transaction is called pending if it was started using an old SA. The old SAs are then deleted as soon as all pending SIP transactions have been completed, or have timed out. The old SAs are always deleted when the old SAs lifetime are expired. This completes the SA handling procedure for the P-CSCF.".

Alignment of SA handling procedures

Currently there is a mis-alignment in the SA handling procedures at the P-CSCF between TS 33.203 and TS 24.299. This is true whether the above clarification to the TS 33.203 SA handling procedure is agreed or not.

Currently TS 33.203 states (in clause 7.4.2a);

"After SM12 is sent, the P-CSCF handles the UE related SAs according to following rules:

If there are old SAs, but SM1 is received unprotected, the P-CSCF considers error cases happened, and assumes UE does not have those old SAs for use. In this case the P-CSCF shall remove the old SAs.

If SM1 is protected with an old valid SA, the P-CSCF keeps this inbound SA and the corresponding three SAs created during the same registration with the UE active, and continues to use them. Any other old SAs are deleted. When a further SIP message protected with a new inbound SA is successfully received from the UE, the P-CSCF starts to use the new SAs for outbound messages with the following exception: when a SIP message is part of a pending SIP transaction it is still sent over the old SA. A SIP transaction is called pending if it was started using an old SA. The old SAs are then deleted as soon as all pending SIP transactions have been completed, or have timed out. The old SAs are always deleted when the old SAs lifetime are expired. This completes the SA handling procedure for the P-CSCF.";

whereas TS 24.229 states (in clause 5.2.2)

"The P-CSCF shall:

If new security associations are established and there are no old security associations, start using the new security associations towards the UE after the 200OK has been sent out.

If a request protected within the newly established security associations is received from a UE, which has old security associations, delete the old security associations and related keys when all SIP transactions that use the old security associations are completed.

If the newly established security associations has not been taken into use by the UE and the UE sends request protected on the old security associations, delete the new security associations.

If the newly established security associations are a result of an unprotected REGISTER request being received from the UE, then delete the old security associations which may exist towards the UE."

The case of unprotected REGISTER is covered in both and the documents are inline, although which bullets apply to the unprotected REGISTER case is unclear in TS 24.229. This can be made clearer by combining bullets 1 and 4 together as the first bullet.

For protected REGISTERs, TS 24.229 does not discuss deleting old SAs so this needs to be added. It also does not mention continuing to use the old SAs until a request protected with the new SA is received and hence this should be added. It should also be mentioned that the old SA can be used for existing transactions once the new SAs are being used. Finally the third bullet in the CN1 specification needs to be deleted, as this is not specified in TS 33.203.

The following text is proposed to align the two specifications. It is written assuming the changes proposed to TS 33.203 earlier in the document are accepted. It is discussed below how to modify the text below if they are not.

"The P-CSCF shall:

~~If new security associations are established and there are no old security associations, start using the new security associations towards the UE after the 200OK has been sent out.~~

If the newly established security associations are a result of an unprotected REGISTER request being received from the UE, then delete the old security associations, which may exist towards the UE and use the new ones to protect traffic towards the UE.

If the newly established security associations are a result of a protected REGISTER request being received from the UE, then the P-CSCF shall

Keep the inbound SA used by the UE to protect the REGISTER and the corresponding three SAs created by the same registration and continue to use the old SAs towards the UE.

If a message~~request~~ protected within the newly established security associations is received from a UE which has old security associations or the old SAs expire, then the P-CSCF shall

use the new SAs to protect requests to the UE,

delete the old security associations and related keys when all SIP transactions that use the old security associations are completed

send and receive responses on the new SAs, expect when the associated request was sent on an old SA when the old SA may be used. ~~.~~

~~If the newly established security associations has not been taken into use by the UE and the UE sends request protected on the old security associations, delete the new security associations.~~

~~If the newly established security associations are a result of an unprotected REGISTER request being received from the UE, then delete the old security associations which may exist towards the UE."~~

If the proposed changes to TS 33.203 are not accepted, then the last sentence should be changed to read "send or receive responses over a security association created at the same time as the security association that the associated request was sent over".

Given the proposed changes to TS 33.203 are accepted, then text in clause 5.1.1.5.1 of TS 24.229 should be changed to something like the following:

"On receiving the 200 (OK) response for the integrity protected REGISTER request, the UE shall:

set the security association lifetime to the longest of either the previously existing SA lifetime, or the lifetime of the just completed registration plus 30 seconds;

send subsequent requests towards the P-CSCF using the new security associations;

send the responses toward the P-CSCF over a~~the same~~ new security association, except when ~~that~~ the associated request was received over an old SA when an old SA may be used; and

receive the responses from the P-CSCF over a~~the~~ new~~same~~ security association, except when ~~that~~ the associated request was sent over an old SA when an old SA may be used."

If the proposed changes are not accepted, then a change is needed to this text anyway, as a response is not returned over the **same** security association, as the associated request because security associations in this case are uni-directional.

This contribution proposes some changes to TS 24.229. If any of the proposed changes are agreed, **3** will draft the appropriate CR(s) for discussion at the next CN1 meeting.