3GPP TSG SA WG3 Security — S3#29 **S3-030417**

15 – 18 July 2003

San Francisco, USA

Source: **Siemens**

Title: **Delta Changes to TS 33.203 on Security Association Handling in Re-authentications**

Document for: **Discussion**

Agenda Item: **7.1 IMS**

Abstract

This contribution is to be read in conjunction with two change requests also submitted to SA3#29 by Siemens, the first entitled "Alignment of security association handling and behaviour of SIP over TCP*" and the second* " Security association handling, behaviour of SIP over TCP and re-authentication*". The first change request implements the changes necessary to address the fact that SIP over TCP may sometimes require two different TCP connections between UE and P-CSCF. These changes were discussed over the SA3 mailing list and are expected to be not contentious.*

This contribution shows which changes need to be implemented (relatively few) in addition to those in the first change request so that the problem with the use of UE ports in re-authentications identified in S3-030258 (Lucent) is addressed. The proposed solution is to always keep the server ports fixed, and change the client ports at the UE and the P-CSCF in a re-authentication. At the time of writing this solution was not yet agreed on the SA3 mailing list. This is why the corresponding changes are presented separately here. The changes are not implemented as a stand-alone CR as they use terminology from the first CR. It would not make much sense to approve the delta CR on its own. The second change request combines the changes from the first change request and from this contribution. An approval of the second change request would imply approval of the first CR.

***** Begin of Change ****

7.4 Authenticated re-registration

Every registration that includes a user authentication attempt produces new security associations. If the authentication is successful, then these new security associations shall replace the previous ones. This clause describes how the UE and P-CSCF handle this replacement and which SAs to apply to which message.

When security associations are changed in an authenticated re-registration then the protected server ports at the UE (*port_us*) and the P-CSCF (*port_ps*) shall remain unchanged, while the protected client ports at the UE (*port_uc*) and the P-CSCF (*port_pc*) shall change. For the definition of these ports see section 7.1.

If the UE has an already active pair of security associations, then it shall use this to protect the REGISTER message. If the S-CSCF is notified by the P-CSCF that the REGISTER message from the UE was integrity-protected it may decide not to authenticate the user by means of the AKA protocol. However, the UE may send unprotected REGISTER messages at any time. In this case, the S-CSCF shall authenticate the user by means of the AKA protocol. In particular, if the UE considers the SAs no longer active at the P-CSCF, e.g., after receiving no response to several protected messages, then the UE should send an unprotected REGISTER message.

Security associations may be unidirectional or bi-directional. This clause assumes that security associations are unidirectional, as this is the general case. For IP layer SAs, the lifetime mentioned in the following clauses is the lifetime held at the application layer. Furthermore deleting an SA means deleting the SA from both the application and IPsec layer. The message numbers, e.g. SM1, used in the following clauses relate to the message flow given in section 6.1.1.

7.4.1 Void

7.4.1a Management of security associations in the UE

The UE shall be involved in only one registration procedure at a time, i.e. the UE shall remove any data relating to any previous incomplete registrations or authentications, including any SAs created by an incomplete authentication.

The UE may start a registration procedure with ~~an~~ two existing pairs of SAs. These~~is~~ will be referred to as the old SAs. The authentication produces two ~~a~~ pairs of new SAs. These new SAs shall not be~~y~~ used to protect non-authentication traffic until noted during the authentication flow. In the same way, certain messages in the authentication shall be protected with a particular SA. If the UE receives a message protected with the incorrect SA, it shall discard the message.

A successful authentication proceeds in the following steps:

- The UE sends the SM1 message to register with the IMS. If SM1 was protected, it shall be protected with the old outbound SA.
- The UE receives an authentication challenge in a message (SM6) from the P-CSCF. This message shall be protected with the old inbound SA if SM1 was protected and unprotected otherwise.
- If this message SM6 can be successfully processed by the UE, the UE creates the new SAs, which are derived according to section 7.1. The lifetime of the new SAs shall be set to allow enough time to complete the registration procedure. The UE then sends its response (SM7) to the P-CSCF, which shall be protected with the new outbound SA. Meanwhile, if SM1 was protected, the UE shall use the old SAs for messages other than those in the authentication, until a successful message of new authentication is received (SM12); if SM1 was unprotected, the UE is not allowed to use IMS service until it receives an authentication successful message (SM12).
- The UE receives an authentication successful message (SM12) from the P-CSCF. It shall be protected with the new inbound SA.
- 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 ~~traffic~~ requests sent from UE, the new outbound SAs ~~is~~ are used. Responses received over an old SA are still sent over the old SA. When no more responses are to be sent over an old SA, ~~T~~the old outbound SAs ~~is~~ are are now deleted. The old inbound SAs ~~is~~ are kept for receiving messages from P-CSCF. In particular, responses to requests sent over the old SA shall be received over the old SA.~~It~~ They shall be deleted when either lifetime is expired, or a further SIP message protected with ~~the~~ a new inbound SA is successfully received from the P-CSCF, and no more responses to be received over the old SA are expected. The new SAs are used to protect all traffic.

A failure in the authentication can occur for several reasons. If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SA. If SM1 was protected, the old SAs shall be used to protect the failure messages. In both cases, after processing the failure message, the UE shall delete the new SAs.

The UE shall monitor the expiry time of registrations without authentication and adjust the lifetime of SAs it holds to ensure that they live longer than the expiry time given in the registration.

The UE shall delete any SA whose lifetime is exceeded.

7.4.2 Void

7.4.2a Management of security associations in the P-CSCF

When the S-CSCF initiates an authentication by sending a challenge to the UE, the P-CSCF may already contain existing SAs from previously completed authentications. It may also contain ~~an~~ two existing pairs of SAs from an incomplete authentication. These will be referred to as the old and registration SAs respectively. The authentication produces two~~a~~ pairs of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication flow. Similarly certain messages in the authentication shall be protected with a particular SA. If the P-CSCF receives a message protected with the incorrect SA, it shall discard the message.

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

A successful authentication proceeds in the following steps:

- The P-CSCF receives the SM1 message. If SM1 is protected, it shall be protected with the old inbound SA.
- The P-CSCF forwards the message containing the challenge (SM6) to the UE. This shall be protected with the old outbound SA, if SM1 was protected and unprotected otherwise.
- The P-CSCF then creates the new SAs, which are derived according to section 7.1. The expiry time of the new SAs shall be set to allow enough time to complete the registration procedure. The registration SAs shall be deleted if they exist.
- The P-CSCF receives the message carrying the response (SM7) from the UE. It shall be protected using the new inbound SA. If SM1 was protected, the old SAs are used to protect messages other than those in the authentication.
- The P-CSCF forwards the successful registration message (SM12) to the UE. It shall be protected using the new outbound SA. This completes the registration procedure for the P-CSCF. The P-CSCF sets the expiry time of the new SAs equal to the maximum of registration timer in the message and the lifetime of the old SAs.
- 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 ~~outbound~~ three SAs created during the same registration with the UE active, and continues to use them. . In particular, responses to requests sent/received over the old SA shall be received/sent over the old SA. Any other old SAs are deleted. The kept old SAs are deleted when either the old SAs lifetime are expired, or a further SIP message protected with ~~the~~ a new inbound SA is successfully received from the UE, and no more responses to be sent or received over the old SAs are expected.. Then further messages are protected with new SAs. This completes the SA handling procedure for the P-CSCF.

A failure in the authentication can occur for several reasons. If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SAs. If SM1 was protected, the old SAs shall be used to protect the failure messages. In both cases, after processing the failure message, the P-CSCF shall delete the new SAs.

The P-CSCF shall monitor the expiry time of registrations without authentication and adjust the lifetime of SAs it holds to ensure that they live longer than the expiry time given in the registration.

The P-CSCF shall delete any SA whose lifetime is exceeded.

******End of Change ***