3GPP TSG SA WG3 Security — S3#30 **S3-030570**
06 - 10 October 2003
Povoa de Varzim, Portugal

Source: Nokia

Title: Security issues

Document for: Discussion

Agenda Item: 5.2

WI / Topic: IMS-ASEC

1. Introduction

1. Introduction

SA3 has agreed on their last meeting a bunch of new procedures for managing the SAs in the P-CSCF, at SIP level. In some cases the agreed text is going into too much detail, resulting in unnecessary and heavy procedures for the P-CSCF.

2. Discussion

1. S3-030461 says: "**TCP case:** the P-CSCF receives requests and sends responses protected with ESP from and to any UE on the port *port_ps*. The P-CSCF sends requests and receives responses protected with ESP to and from a UE on the port *port_pc* (the "protected client port").

This is an unnecessary restriction. Once there are two pair of SAs towards the UE, the P-CSCF could use any of them to send the request to the UE. For TCP it makes no difference whether it carries a SIP request or SIP response. Nor does for an SA.

2. "Same problem as above for the UE: "**UDP case:** the UE receives requests and responses protected with ESP on the port *port_us* (the"protected server port"). The UE sends requests and responses protected with ESP on the port *port_uc* (the "protected client port"). For every protected request towards the P-CSCF, the UE shall insert the protected server port *port_us* into the Via header. The protected responses from the P-CSCF are then sent to port_us at the UE.
TCP case: the UE receives requests and sends responses protected with ESP on the port *port_us*. The UE sends requests and receives responses protected with ESP on the port *port_uc* (the "protected client port")."

3. The same agreed contribution together with S3-030445 defines the parameters the security-client and security-server headers should contain (in SM1 and SM6). It then says that SM7 (the protected REGSITER carrying RES) should contain the parameters from both headers (i.e. replicating the parameters sent in the unprotected register, security-client header). This is an additional procedure to the RFC3329, is this additional procedure agreeable for CN1? In case the protected register is re-challenged, the same security parameters would need to be reused.

SA3 does not specify what the content of the security-verify header should be in subsequent requests. What parameters that header should contain? It is noted that the purpose of the security-verify header is the detection of the MITM attacks. For detecting these kind of attacks, only the algorithm list is needed, the rest of the parameters is not relevant.

Nokia considers that it is enough if the security-verify header only contains the list of algorithms, both in registration and non-registration requests.

4. S3-030461 says: "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."

There must be a time period when both the new and the old SAs are valid. If the old SA expires before the pending transactions are completed, then the transaction times out. It is proposed that the old SA is deleted 64*T1 period after its expiration, therefore new transactions can be initiated with new SAs and old transactions can be completed on the old SA.

5. N1-030461 says: "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."

It is assumed that the text should read:

"If there are old SAs, but SM1 ~~is~~ was 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."

The above assumes the P-CSCF to be stateful over two consecutive transactions (the challenged REGISTER and the REGISTER carrying RES).

This has been discussed in CN1, people were not happy, but other solutions may not exist.

6. N1-030461 says: "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"

This rule and the rule quoted in bullet above (5) implicitly make a difference between SAs created as a result of an unprotected REGISTER and a protected REGISTER:

a) an SA set up as a result of an unprotected REGISTER will result in an SA which right away has to be taken into use and all possible old SAs to be deleted.

b) an SA set up as a result of a protected REGISTER will result in an SA which will be taken into use after a new message is received from the UE protected on this new SA or when the old SA expires.

Is it seen necessary to make such distinctions between SAs?

3. Proposal

Discuss the above and the relevant CRs.