3GPP TSG SA WG3 Security#30 **S3-030554**
6 – 10 October, 2003
Povoa do Varzim, Portugal

Agenda Item: **5.2 of joint SA3-CN1 session**
Source: **Siemens**
Title: **Handling of Security Associations**
Document for: **Discussion and Decision**

Introduction

This discussion paper wants to clarify the behaviour of the P-CSCF in case a REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid (indicated by the AUTS parameter in the REGISTER).

Additionally this discussion paper wants to clarify the necessary parameters for IPSec in a reREGISTER request.

Proposal

1. Synchronization Failure during Authentication

In the case that the REGISTER request from the UE containing an authentication response indicate that the sequence number in the authentication challenge was invalid (synchronization failure, indicated in the AUTS parameter) the S-CSCF will fetch new authentication vectors and shall either

- send a 401 (Unauthorised) response to initiate a further authentication attempt, using these new vectors ; or
- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned.

When the P-CSCF receives a REGISTER request from the UE containing an authentication response indicate that the authentication challenge was invalid (synchronisation failure, indicated in the AUTS parameter) the P-CSCF shall delete the newly created SAs and store the parameters (*SPI_C, SPI_S, PORT_C, PORT_S*) from the Security-Client header. On the reception of a 401 from the S-CSCF the P-CSCF shall establish new security associations based on the keys derived from the received CK and IK as a result of this new challenge. For these new SAs the P-CSCF shall use the stored parameter values *SPI_C, SPI_S, PORT_C, PORT_S* form the Security-Client header (sec-client_1 in the following figure) and the parameters from the Security-Server header (sec-server_1 in the following figure) received in this 401 response.

The described behaviour results in the following flow:

UE P-CSCF

---- 1.REGISTER (sec-client_1)---------->

<--- 2.401 (challenge1, sec-server_1) ----------

-----3. REGISTER (sec-client_1, sec-verify_1,AUTS) >

Synchronisation Failure

<--- 4. 401(challenge2, sec-server_1) ----------

-----5. REGISTER (sec-client_1, sec-verify_1) ---->

< ---6. 200OK----------

If the described behaviour of the P-CSCF can be agreed Siemens volunteers to write the necessary CR against TS 24.229. No CR against TS 33.203 is deemed necessary.

2. Parameter Values of Security-Client header in reregistration

On user initiated re-registration 3GPP TS 24.229 sub-clause 5.1.1.4 states the following

"On sending a REGISTER request, the UE shall populate the header fields as follows:
...

g) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

However, no further details on the content of the Security-Client header field are specified in the case of re-registration, especially the content of *SPI_C, SPI_S, PORT_C, PORT_S* is open.

On sending a REGISTER request for re-registration the UE shall populate the Security-Client header as follows:
The Security-Client header field shall contain new parameter values for *SPI_C, SPI_S, PORT_C, PORT_S*, i.e. these parameter values are different to those used in the previous registration.

If the request is answered with 200OK from the S-CSCF then these new parameter values will not be used for security association set-up because this means that the re-registration is not authenticated. Consequently, these new parameter values can be deleted in the P-CSCF.

If the request is challenged with 401 response from the S-CSCF then the new parameter values will be used to set-up new security associations.

The Security-Verify header is not needed in the first REGISTER request sent for re-registration.

If the above proposal can be agreed, SIEMENS volunteers to write the necessary CR against TS 24.229. No CR against TS 33.203 is deemed necessary.