**3GPP TSG SA WG3 Security — S3#22** **S3-020090**

**February 25th– February 28th, 2002**

**Bristol, UK**

| | |
|---|---|
| **Agenda Item:** | 7.3 |
| **Source:** | Ericsson |
| **Title:** | On P-CSCF behavior at Integrity check failures |
| **Document for:** | Discussion and decision |

# 1. Scope and objectives

This contribution aims to clarify the behavior of the P-CSCF when integrity check fails in SM7 during a registration/authentication procedure.

# 2 Background

During S3#21bis meeting in Antwerp, Ericsson presented contribution (S3z020014), which amongst other things, discussed the Ericsson undertanding of chapter 7.3.1.1 in TS 33.203.

## *2.2. Indication from the P-CSCF to the S-CSCF - integrity protection check of (SM5) Register has failed*

*Our current understanding of chapter 7.3.1.1 in TS 33.203, is that the P-CSCF shall forward a (SM5) Register message from the UE to the S-CSCF, even if the (SM7) Register message failed the integrity protection check in the P-CSCF. …. If this assumption is incorrect then chapter 7.3.1.1 needs to be clarified.*

During the discussion of this point, looked like the common understandoing of the group was that P-CSCF shall always discard SIP requests when integrity check fails. For the case of the registration procedure specified in chapter 7.3.1.1, timers shall take care of resolving any potential state S-CSCF and/or UE may enter during the registration/authentication procedure.

# 3 Discussion

During a Registration/Authentication procedure, SM7 which is already integrity protected with the IK derived from the challenge RAND, includes the response to the challenge RES. In the case of a user authentication failure, where RES derived from RAND at the UE is invalid, one could also assume that the IK (also derived from RAND) will be invalid as well.

This leads to the situation that P-CSCF detects the integrity check failure before S-CSCF has the chance to examine RES. If at this point of time P-CSCF discards SM7 (according to conclusions in Antwerp meeting) this means that S-CSCF will never have the chance to detect the wrong RES (SM8 and SM9), and will never have the chance to issue the Authentication Failure Response (4xx Auth_Failure in SM10) as specified in TS 33.203, Chapter 6.1.2.1.

It is assumed that upon expiration of timers at S-CSCF and UE, the registration and authentication procedures are considered as aborted.

Changes like the ones proposed below would be required in order to accommodate this new requirement into TS 33.203.

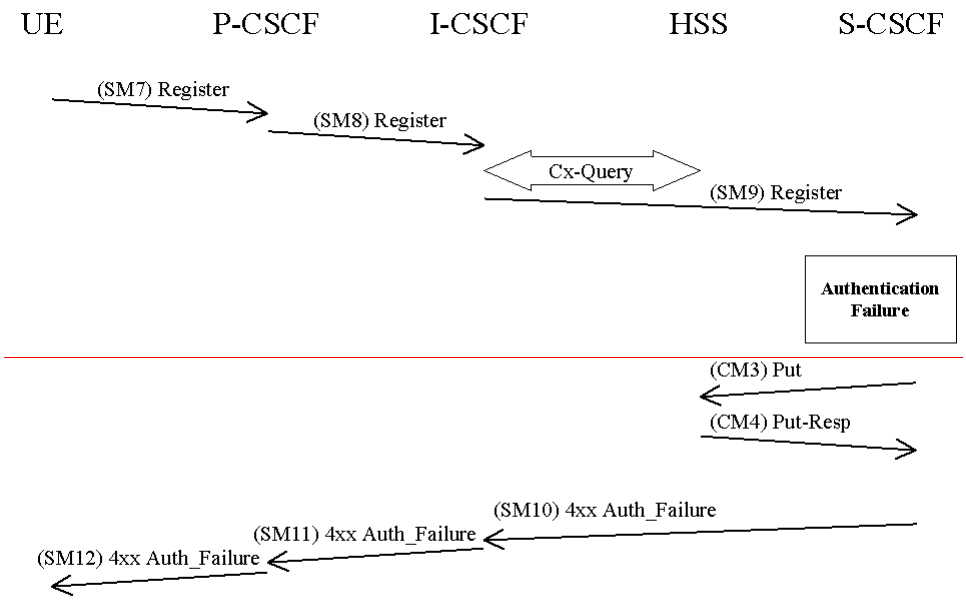
# 4 Proposed Changes to 33.203

### 6.1.2.1 User authentication failure

In this case the authentication of the user should fail at the S-CSCF due an incorrect RES (received in SM9). However, in this case when RES is incorrect, the IK used to protect SM7 will be incorrect as well and integrity check at P-CSCF will fail before RES can be verified at S-CSCF.

P-CSCF in this case shall discard SM7 and the registration and authentication procedures shall be then aborted.

~~When the check of the RES in the S-CSCF fails the user can not be authenticated and hence registration fails. The flow is identical as for the successful registration in 6.1.1 up to SM9.~~




~~CM3:~~

~~Cx-AV-Put(IMPI, Clear S-CSCF name)~~

~~The S-CSCF sends a Cx-Put (CM3) to the HSS, which indicates that authentication failed and that, the S-CSCF should be cleared for that particular IMPU. The HSS responds with a Cx-Put-Resp in CM4. In SM10 the S-CSCF sends a 4xx Auth_Failure towards the UE indicating that the authentication failed, no security parameters shall be included in this message.~~

~~SM10:~~

~~4xx Auth_Failure~~

~~Upon receiving SM10 the I-CSCF shall clear any registration information related to the IMPU.~~

~~*[Editors Note: It is FFS if the IMPI shall be included in SM10.]*~~

#### 7.3.1.1 ~~User authentication failure~~Integrity check failure in the P-CSCF

In this case, SM7 containing a potentially wrong RES fails integrity check at P-CSCF (IK derived from RAND at UE is wrong as well). ~~the authentication of the user fails in the network due an incorrect RES.~~ The P-CSCF shall discard SM7 and the registration and the authentication procedures shall be aborted (see also 6.1.2.1. ~~The S-CSCF will send a 4xx Auth_Failure message SM10, which will pass through the already established SA to the UE as SM12.~~

~~Note, that this failure will already occur in SM7, when the UE does not use the correct integrity key IK. In this situation, the P-CSCF will receive protected packets that cannot be verified.~~

~~It may seem from the above discussion that there is no requirement to check the RES at the S-CSCF since a false RES sent by a UE will never reach the S-CSCF. However, it is still necessary to check RES at the S-CSCF since this prevents a P-CSCF from registering a UE without performing user authentication. It therefore reduces S-CSCF trust in the P-CSCF.~~

# 5 Conclusion

S3 is kindly asked to evaluate the potential impacts the conclusions reached during S3#21bis in Antwerp may have in TS 33.203.

It is still unclear for Ericsson whether this is the desired behavior of the system for an optimal termination of the authentication procedure.