3GPP TSG SA WG3 Security **S3-020231**

May 14 – May 17, 2002

Victoria, Canada

Agenda Item:	TBD
Source:	Ericsson
Title:	Incoming SIP messages at the unprotected port at the UE and integrity check failures in the UE
Document for:	Discussion and decision

1. Scope and objectives

This paper raises the problem with allowing any incoming SIP messages on the unprotected port at the UE.

The issue of how the UE shall handle incoming SIP messages, which fails the integrity check in the UE, is also brought up in this paper.

2. Introduction

A list has been defined in TS33.203 to prevent the P-CSCF to handle any incoming SIP message on the unprotected port.

Chapter D.1 in TS33.203 version 5.1.0 it is stating the following:

> *The UE may send only the following messages to the fixed port for unprotected messages:*
>
> - *initial REGISTER message;*
> - *REGISTER message with network authentication failure indication;*
> - *REGISTER message with synchronization failure indication.*

All other messages incoming on this port must be discarded by the SIP application on the P-CSCF.

3. Discussion on incoming unprotected SIP messages

If a similar list were defined for the UE as defined for the P-CSCF above, then the protection in the UE would be improved.

The only time the UE needs to accept incoming unprotected SIP messages are during an ongoing Register procedure when the UE has no stored SA. Then the P-CSCF has to be allowed to send selected SIP messages unprotected to the UE.

The SIP messages, which the P-CSCF could be allowed to send at the unprotected port at the UE could be the following:

- Authentication Challenge;

- 4xx Unacceptable_Proposal;
- 4xx Auth_Failure;
- Any more messages?

It could be further discussed which messages this list should contain. The list above is most likely not complete.

The SIP layer in the UE should only be allowed to handle this list of unprotected messages, if the UE has an ongoing Register procedure and no valid SA.

All other messages incoming on this port should be discarded by the SIP application in the UE.

4. Discussion on SIP messages which fails the integrity check in the UE

In TS33.203 we have a requirement in chapter 7.3.1.1 where the P-CSCF shall discard incoming SIP messages, which fails the integrity check in the P-CSCF:

7.3.1.1 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 clause 6.1.2.1).

A similar requirement is needed for the UE.

5. Conclusions

This paper proposes to define a new list for the UE in TS33.203 based on the discussion in chapter 3 above. This requirement would improve the protection in the UE from attackers.

In addition it is proposed to add a requirement in TS33.203 that the UE shall discard all incoming SIP messages, which fails the integrity check in the UE.

It is proposed that TS33.203 is updated according to the attached CR’s.

References

[TS33203] 3G TS 33.203: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA3; Access Security for IP-based services".