**3GPP TSG SA WG3 Security** **S3-020091**

**February 25 - 28, 2002**

**Bristol, England**

| | |
|---|---|
| **Agenda Item:** | 7.3 |
| **Source:** | Ericsson |
| **Title:** | Unprotected REGISTER messages |
| **Document for:** | Discussion and decision |

## 1. Introduction

Already at SA3 #21 bis in Antwerpen, Nokia presented a contribution in Tdoc S3z020011 discussing unprotected re-registration initiated by the UE during SA lifetime. This problem was acknowledged by SA3 in that meeting. This paper attempts to extend the discussion a bit further from a UE perspective to also consider the case when the UE is moving out of radio coverage and back within radio coverage again of the selected PLMN. It is assumed that the PDP context for IMS signalling most likely will survive these scenarios, as it is an interactive bearer.

## 2. Discussion

### 2.1 UE power off

The Nokia contribution discussed that at some circumstances the UE is not able to deregister for IMS services before powering off. It was mentioned that this could be the case when the battery has been removed, but could also be cases as the UE happens to be out of radio coverage when user decides to power off the UE.

When the UE is powered on again, it has no security association stored in the UE to protect the initial Register message to the P-CSCF in order to register for IMS services in the network. In fact the UE has no knowledge of whether the P-CSCF has any valid SA stored for this particular UE. In addition when a new PDP context is established between the UE and the network, a new P-CSCF might be selected for this particular UE (i.e. different from the previous one).

### 2.2 Periodic re-registration timer expires in the UE during loss of radio coverage

There are also the scenarios when the UE moves out of radio coverage of the selected PLMN when the periodic re-registration timer expires. The SIP client in the UE is not aware of whether the UE happens to be within radio coverage or not. This means that the SIP client will not behave differently while being out of radio coverage or while being within radio coverage of the selected PLMN.

The periodic re-registration timer in the UE is shorter than the periodic timers in the P-CSCF and S-CSCF. The UE will attempt to perform the first re-registration already when half of the periodic re-registration timer value in the P-CSCF and S-CSCF has elapsed, in order to ensure that the UE will be able to re-register successfully for IMS services in the network, before the SA has expired in the P-CSCF. TS24.229 is currently stating that the UE shall perform 3 retransmissions of the re-register procedure. Hopefully the UE will return into radio coverage before the UE has attempted these attempts. It is not currently defined in 24.229 or 24.228 how the SIP client will proceed after 4 failed attempts. Such a mechanism might need to be defined.

When the SA has expired in the UE, the UE should assume that the P-CSCF has no valid SA for this UE. The SIP client in the UE should delete the stored SA before initiating a further re-transmission of the re-register procedure, which will in fact be an initial REGISTER, as it will be sent unprotected to the P-CSCF.

When returning back into radio coverage, those media flows, which have used a high QoS, will most likely be lost. If the SA has expired in the UE, an initial REGISTER needs to be initiated in order to get access to IMS services and establish a new SA between the UE and the P-CSCF, before any new sessions can be re-established.

## 3. Summary

In summary it is proposed that TS33.203 is clarified so that the following can be applied:

1. after the UE has powered on, the first initial (SM1) Register message initiated by the UE has to be sent unprotected, as the UE has no stored SA;
2. the UE shall send re-register message protected, if the UE has a valid SA;
3. if the SA has expired in the UE, then the UE shall delete the SA and accordingly send the next (SM1) Register message unprotected, in order to get access for IMS services;
4. the P-CSCF has to accept and handle unprotected (SM1) Register messages from the UE, even if the P-CSCF has a valid SA stored for this particular UE, as already pointed out by Nokia in Antwerpen. In addition, the P-CSCF shall keep the SA for this UE, if any available, in case the unprotected (SM1) Register message is sent by an attacker. The P-CSCF shall forward the re-register message to the S-CSCF and include an indication to the S-CSCF to trigger the S-CSCF to challenge the subscriber with the execution of a new IMS-AKA procedure.

It is proposed that TS33.203 is updated according to the text below.

******** Proposed change to TS33.203 version 1.1.0 *******

## 7.3.3 Authenticated re-registration

If the registration is a re-registration, a pair of security associations between UE and P-CSCF is already active. The authenticated re-registration shall initially utilize the existing SA.

In normal conditions, both the UE and P-CSCF shall use the existing SA to protect re-register messages (e.g. SM1/SM4). However, in the event the UE originates the (SM1) Register message using no protection, the P-CSCF shall still accept it and forward the request to the S-CSCF, indicating that the register message was not integrity protected. This shall trigger the S-CSCF to challenge the subscriber with the execution of a new IMS-AKA procedure as described in chapter 6.1.

~~*[Editors Note: It is under investigation if unprotected re-registration shall be allowed during the SA-Lifetime.]*~~

Before SM7 is sent by the UE, both peers shall replace the existing SA by the new SA negotiated during these first two messages.