3GPP TSG SA WG3 Security — S3#18 **S3-010220**

21-24 May, 2001

Phoenix, Arizona, USA

Source:	**Nokia**
Title:	**Integrity protection of the IMS registration**
Document for:	**Discussion / Decision**
Agenda Item:	**9.3**

According to the current IMS security working assumptions, integrity protection of SIP signalling between UE and P-CSCF begins after the user response RES has been verified in the home network. It is a good security practice to begin using the keys (in this case IK and, optionally, CK) only after it is known that also the receiving party possess the same key(s).
However, in the particular case of IMS there is a down-side of this assumption. The protection does not cover critical information in the SIP REGISTER message such as the To, From and Contact fields. These fiels determine which identities are involved in the registration and also where the user can be reached, and therefore they should be protected.
A straight-forward solution to this problem is to send a new REGISTER message after the authentication procedure is completed, i.e. the user should perform re-registration. The down-side of this solution is that, as a consequence, authentication signalling flow becomes even more complex than it is now. This is difficult to tolerate since the delays in SIP signalling are already now remarkable.

Because of these reasons it is proposed that already the second REGISTER message in the authentication signalling flow is integrity protected. This is possible if:

- The IK (and optionally also CK) are delivered to P-CSCF already before the user response RES is checked. In fact, the integrity of the REGISTER message is checked in P-CSCF before RES is sent back to home network. Of course, this check has no meaning in the negative case, i.e. when the RES is not correct;
- The IK can be computed in USIM fast enough that the REGISTER message is not delayed because it is integrity protected.

As a side-effect the open issue about the IMS security mode set-up has to be solved in a particular way. Indeed, the IMS integrity protection capabilities are sent to the P-CSCF already attached to the first REGISTER message and the rest of the messages in the UTRAN security mode setup prcedure can be similarly embedded to arious messages in the authentication flow.