3GPP TSG SA WG3 Security — S3#21 **S3-010669**

27 - 30 November, 2001

Sophia Antipolis, France

Source: **TSG-SA WG3**

To: **TSG-CN WG1**

Title: **IMS Security requirements and transportation of SIP session keys**

Contact person: **Krister Boman**
Krister.Boman@emw.ericsson.se

SA3 would kindly like to inform CN1 on the current requirements in TS33.203v070 for authenticated re-registrations.

Furthermore SA3 would kindly like to encourage CN1 to inform SA3 whenever CN1 detects a security requirement is missing in TS33.203 before solutions are implemented in related CN1 Technical Specifications. This in order to minimise the risk of implementing security deficiencies in the IMS architecture.

SA3 also kindly asks for information on how session keys are transported in SIP.

Network initiated re-authentication

In TS24.229v080 CN1 has implemented solutions in section *11.4.1.5 Network-initiated reauthentication* that are tailored to authenticated re-registrations. It is e.g. required that "In the case that the response from the UE is incorrect three consecutive attempts then the S-CSCF shall deregister the user and terminate any ongoing sessions for all public identities associated with the private identity being authenticated, and release resources allocated to those sessions". SA3 encourages CN1 to consider that SA3 has not specified the number of attempts since the number of attempts should be defined by the policy of the operator. However SA3 will closely review the current requirements in TS33.203v070 related to Network-initiated re-authentication in order to identify if and how the requirements need to be updated such that adequate solutions can be defined.

Transportation of session keys in SIP

Currently SA3 is closely monitoring IMS Security related IETF drafts e.g. EAP AKA authentication and Security Mechanism Agreement for SIP connections. However according to the current knowledge in SA3 it is not clear how the Session Keys IK and CK are transported from the S-CSCF to the P-CSCF by SIP. SA3 kindly asks CN1 to provide SA3 with information on how the mechanism for SIP key transportation is defined.

Actions:

1. CN1 to inform SA3 whenever CN1 detects a security requirement is missing in TS33.203 before solutions are implemented in related CN1 Technical Specifications.
2. CN1 to remove the restriction on 3 re-authentication attempts.
3. CN1 to inform SA3 on how session keys are transported in SIP.

SA3 looks forward to very close cooperation with CN1 on SIP and the development of secure IMS signaling for the IM CN SS.