3GPP TSG SA WG3 Security — S3#22 **S3-020030**

25 - 28 February 2002

Bristol, UK

3GPP TSG-CN1 Meeting #SIPadhoc0201 ***Tdoc N1-020154***

Phoenix, USA, 14. –18. January 2002

Title: Liaison Statement on transportation of SIP session keys from S-CSCF to P-CSCF

Source: CN1

To: SA3

Cc:

Response to: LS N1-012011 (S3-010669) on IMS Security requirements and transportation of SIP session keys from SA3

Contact Person:

Name: Duncan Mills

Tel. Number: +44 1635 676074

E-mail Address: duncan.mills@vf.vodafone.co.uk

Attachments: None

1. Overall Description:

CN1 thanks SA3 for the above liaison statement, and is pleased to respond.

SA3 highlighted the following three actions on CN1:

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.

Firstly, with respect to action number 1, CN1 will certainly continue to review the stage two specification 33.203 and raise any issues that may arise with SA3.

Secondly, regarding action number 2, CN1 feels that the number of re-attempts to authenticate is something that greatly affects UE behaviour. It is important that a UE knows exactly what to expect from the network and exactly what to do if that expectancy is not met.

CN1 believes that for both aspects of mutual authentication failure (the UE continues to provide an incorrect RES or the network continues to provide an incorrect RAND+AUTN) the number of re-attempts should be limited.

For example, if the number of re-attempts is set by the operator, then the UE always has to expect and allow a further attempt (incorrect RAND+AUTN) or the UE is always allowed to retry a further time (when the network continues to provide challenges, even though the UE is sending incorrect RES). As far as the UE is concerned, the network has obviously decided to perform a very high number of re-attempts- as per the specification- and so the UE will continue to respond.

CN1 sees the above example as unacceptable, and prefers to follow the UMTS model and limit the number of re-attempts. This has the advantage of giving genuine UEs and genuine networks a further opportunity to authenticate correctly, in case the original failure was due to an error. It also means that after a pre-defined number of re-attempts, both the UE and the network can safely abort the procedure and assume 'foul play'.

The current number of re-attempts is specified as three. CN1 asks SA3 to decide whether or not they still require CN1 to alter this.

Finally, in response to action number 3, CN1 can report that it has agreed upon the following working assumption:

Session keys CK and IK will be passed from the S-CSCF to the P-CSCF in the EAP header of the 401 UNAUTHORISED response (along with the RAND and AUTN). The P-CSCF shall remove and store the CK and IK, before forwarding the 401 UNAUTHORISED response to the UE.

It is expected that detailed CRs will be agreed at the next CN1 meeting.

2. Actions:

To SA3 group.

ACTION: CN1 asks SA3 to reconsider specifying the number of authentication re-attempts as being an operator choice.

3. Date of Next CN1 Meetings:

CN1_22	28th January – 1st February 2002	Sophia Antipolis, France
CN1_22bis	19th – 21st February 2002	Oulu, Finland