3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010107**

14 September, 2001

Sophia Antipolis, France

3GPP TSG SA WG3 Security — S3#20 **S3-010432**

16 - 19 October, 2001

Sydney, Australia

3GPP TSG CN WG4 Meeting #09 **Tdoc N4-010968**
Dresden, GERMANY, 9th - 13th July 2001

Source:	**TSG CN WG4**
Title:	**LS response to SA3 on "Using a generic authentication scheme for SIP"**
To:	**S3**
CC:	**S2, N1**

Contact Person:
Name: Miguel-Angel Pallares López
E-mail Address: **miguel-angel.pallares-lopez@ece.ericsson.se**

CN4 thanks SA3 for asking CN4 opinion on this matter. CN4 has analysed the use of EAP and Diameter NASREQ in the Cx interface and has come to the following conclusions.

As the authentication point is in the S-CSCF, the standard EAP model breaks in Cx interface. The EAP can be only used to encapsulate the security parameters and download parameters in the EAP format to the S-CSCF.

Encapsulating the authentication parameters inside EAP payloads has the advantage of making the Cx interface more generic and it is possible to re-use some of the existing AVPs, e.g. EAP-Payload and NAS-Session-Key AVP, from the NASREQ.

Although recognising that the model proposed by EAP is not fully applicable for 3GPP architecture, CN4 can see, from a protocol point of view, a possibility to transport authentication information on EAP payloads. It is CN4's intention to develop a protocol with the widest scope possible. In case that new authentication schemes were introduced in the future (e.g. due to the introduction of another access technologies or new authentication methods in 3GPP) the impacts in the protocol (Diameter application for the Cx interface) would be minimised if a generic authentication framework were supported. The 3GPP system may also lead to similar interoperation issues as with the UMTS and GSM authentication had if new authentication method is introduced in 3GPP. In this case the EAP may not anymore secure against 'bidding-down' attacks from the S-CSCF where the S-CSCF may be able to negotiate a lower authentication method with the HSS.

The use of NASREQ also breaks. Therefore, the re-use of the NASREQ command codes is not reasonable. However, the re-use of the some of the NASREQ AVPs is still possible and CN4 is investigating this approach.