3GPP TSG SA WG3 Security — S3#31 **S3-030671**
18 - 21 November 2003
Munich, Germany

3GPP TSG CN WG3 Meeting #30 N3-030830
Bangkok, Thailand, 27th – 31st October 2003

Title: **LS on security of the Diameter protocol for the Gq interface**
Source: CN3
To: SA2, SA3
Cc:

Contact Person:
Name: **Constance GUILLERAY**
Tel. Number: +33.1.45.29.62.08
E-mail Address: constance.guilleray@francetelecom.com

Attachments: none

1. Overall Description:

In the CN3#29 meeting, CN3 decided to use the Diameter protocol as a working assumption for the Gq interface. During the CN3#30 meeting, some concerns were raised regarding the security requirements for this interface.
The Gq interface is defined between the PDF (Policy Decision Function) that belongs to the 3GPP operator network and the AF (Application Function) that can be in another 3GPP operator network in case of roaming.It is up to SA2 to decide if the AF can belong to a third party network.

Therefore, the Gq interface has to be considered as an inter-domain interface. There is then a critical issue on how to secure the Diameter signalling path between the AF and the PDF in a configuration where the AF is in a third party network. CN3 would like SA2 to clarify whether the third party AF is located in a 3GPP trusted domain or not.

The Diameter protocol supports the use of proxies. CN3 would like SA2 to clarify if the support of untrusted proxies is required for the Gq interface.

If the third party AF is not located within the 3GPP trusted domain, Diameter endpoints (i.e. AF and PDF) may communicate through Diameter proxy agent(s) that are outside the 3GPP trusted domain. The presence of Diameter proxy agent(s) outside of the 3GPP trusted domain in the signalling path may break the end-to-end security because integrity of the Diameter message can not be ensured.

This potential issue is raised within the Diameter base protocol specification in the security considerations section (RFC 3588):

"The Diameter base protocol assumes that messages are secured by using either IPSec or TLS. This security mechanism is acceptable in environments where there is no untrusted third party agent. In other situations, end-to-end security is needed." CN3 would like to ask SA3 how tohandle configurations with untrusted third party agent.

The end-to-end security includes integrity and confidentiality of the AVPs exchanged between the Diameter endpoints.

Actually, the Diameter base protocol relies on the draft "Diameter CMS (Cryptographic Message Syntax) Security application" to provide end-to-end security functionality but this specification is still under discussion within the IETF.

CN3 would like to have SA3 confirmation that end-to-end security is needed on the Gq interface when the AF is outside the 3GPP trusted domain with or without untrusted proxies.

CN3 would like to ask SA3 whether it would be advisable to rely on the IETF work in progress on Diameter CMS Security application for end-to-end security. Also, CN3 has concerns whether the Diameter CMS Security Application draft would become an RFC within the Release 6 timeframe.

2. Actions:

To SA2 group.

ACTION:

CN3 kindly asks SA2 to clarify

- if the support of third party AFs in an untrusted domain is required;
- If the support of untrusted proxies is required.

To SA3 group.

ACTION:

CN3 kindly asks SA3 to give guidance on the following security issues with the Diameter protocol:

- requirement of end-to-end security if the third party AF is located within an untrusted domain,
- use of the Diameter CMS Security Application draft for end-to-end security and availability of the RFC in the Release 6 timeframe.

3. Date of Next CN3 Meetings:

CN3#31	16-20 February 2004	USA, Atlanta
CN3#32	10-14 May 2004	Zagreb, Croatia