3GPP TSG-CN Meeting #22 **NP-030561**
10th - 12th December. Maui, Hawaii.

Source: **CN3**

Title: **All LSs send from CN3 since CN#21 Meeting**

Agenda item: **6.3.1**

Document for: **INFORMATION**

Introduction:

This document contains all the LSs APPROVED and sent by CN3 since the last CN Plenary.

Tdoc #	Tdoc Title	LS to	LS cc	Attachment
N3-030828	LS on Inter-network accounting for BS30 based services such as video telephony	CN, SA	-	N3-030821, N3-030713
N3-030830	LS out to SA2 and SA3 on Security concerns of DIAMETER over Gq interface	SA3, SA2	-	-
N3-030811	LS on SBLP handling of Session modification without adding or removing media lines	CN1	-	N3-030764

3GPP TSG-CN WG3 Meeting #30 **N3-030811**
Bangkok, Thailand. 27th - 31st October 2003.

Title: **LS on SBLP handling of Session modification without adding or removing media lines**

Release: **Rel-5**

Source: **CN3**

To: **CN1**

Contact Person:
Name: Thomas Belling
Tel. Number: +49 89 636 75207
E-mail Address: Thomas.Belling@siemens.com

Attachments: **N3-030764** Discussion Document "Comments on Session modification without adding or removing media lines"

---

1. Overall Description:

CN3 would like to inform CN1 how a previously bidirectional media component ("sendrecv SDP attribute") becoming unidirectional ("sendonly" or "recvonly" SDP attribute) is handled whith respect to SBLP, as CN3 discovered a problem and intends to amend their specifications in the next meeting.

This modification may be triggered in two scenarios:

1. media are put on hold
   (In the LS N3-030682/N1-031286 CN1 kindly informed CN3 that media are put on hold in the IMS as described in RFC 3264. The offerer that wants to put a bidirectional media component on hold will make it sendonly.)
2. media component is permanently made unidirectional

CN3 thinks that for scenario 1 a closing of the gates is most appropriate, whereas for scenario 2 a modification of the PDP context (either initiated by the UE or otherwise enforced by the GGSN) is most appropriate, and their spcificactions TS 29.207 and TS 29.208 are currently written with that understanding.

However, the P-CSCF/PDF is not able to distinguish between the scenario 1 and 2. According to the current version of TS 29.207 and TS 29.208, both a closing of gates and a network-enforced modification of the PDP context will be triggered for both scenarios. CN3 agreed that only a network-enforced modification of the PDP context shall be triggered if a previously bidirectional media component becomes unidirectional. CN3 intends to modify their specications accordingly.

This decision may affect CN1´s specifications. CN1 may want to take one of the following decisions and add clarifications they may find necessary to their specifications to avoid the uncertainty expressed above:

A. CN1 accepts that when bidirectional media is put on hold, this will trigger a PDP context modification.
B. CN1 recommends to use "inactive" to put bidirectional media components on hold within the IMS.

2. Actions:

To CN1 group.

ACTION: CN3 asks CN1 to consider the sitiuation described in this LS, and inform CN3 on which of the possibilities listed (A or B) they choose to solve the problem.

3. Date of Next CN3 Meetings:

CN3_31	16th - 20th February 2004	Atlanta, USA.
CN3_32	10th - 14th May 2004	Zagreb, Croatia.

3GPP TSG-CN WG3 Meeting #30 **N3-030828**
Bangkok, Thailand, 27th - 31st October 2003.

Title: **LS on Inter-network accounting for BS30 based services such as video telephony**

Source: **CN3**

To: **CN, SA**

Contact Person:
Name: Stefan Koppenborg
Tel. Number: +49 228 936 18449
E-mail Address: stefan.koppenborg@t-mobile.de

Attachments: **N3-030821** CR to TS 29.007 Backward signaling of service information between VMSC and GMSC for MTC

N3-030713 Discussion paper on inter-networking accounting for BS30 services

---

1. Overall Description:

CN3 has been requested by CN#21 to study the issue of Inter-network accounting for BS30 based services such as video telephony (cf. NP-030431 and SP-030527).
CN3 has reviewed two documents on that matter proposing solutions:

- **N3-030821**, a CR to TS 29.007 introducing backward signaling from the VMSC to the GMSC making use of the Access Transport parameter in the ISUP Answer message to carry the requested information,
- **N3-030713**, a discussion paper proposing a new parameter to be used for that purpose which has to be standardized by ITU-T.

Both papers have in common that the need for providing the requested information to the GMSC for accounting purposes is recognized as requested by SA1.

The first paper, N3-030821, was supported by a broad majority of delegates. However, one company expressed their reservations against this CR and argued that the CR would not follow the ITU-T principles of accounting in the originating network and would not allow for all interconnection cases. The CR was reviewed and considered technically correct for its limited scope.

The second paper, N3-030713, is proposing an ITU-T based solution to be established via appropriate changes to ITU-T Q.762, Q.763 and Q.764. Although CN3 supported this proposal as a longer-term solution it was felt by a majority of that group that this would run the risk of more time needed to get agreed and thus may not serve the need to have a short-term solution for mobile operators.

This LS is copied to SA since SA#21 has reserved their rights to decide on the release applicability.

2. Actions:

To CN and SA:

ACTION: CN3 kindly asks CN and SA to decide whether a short-term solution should be specified and whether a longer-term solution involving ITU-T should be specified.

3. Date of Next CN3 Meetings:

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

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 to handle 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