

21 - 24 May, 2001

Phoenix, USA

3GPP TSG CN WG1 Meeting #17
Puerto Rico, 14th - 18th May 2001

Tdoc N1-010892

Title: Liaison Statement on " Handling of ICMP messages by 3GPP SIP Implementations"

Source: TSG CN WG1

To: TSG SA WG3

cc:

Contact Person:

Name: Milo Orsic

E-mail Address: orsic@lucent.com

Tel. Number: +1 630 713 5161

1. Overall Description:

At its meeting in Puerto Rico the CN WG1 discussed the handling of the ICMP messages in 3GPP SIP implementations. It was pointed out that the SIP - as defined in RFC 2543 - recommends that some ICMP messages acquire equivalent status as SIP response messages. Hence, the respective ICMP messages become an integral part of SIP.

In the IP networks, any entity is a legitimate source of ICMP messages. Hence, the ICMP system is intrinsically a non-secure mechanism. Therefore, the handling of ICMP messages - as recommended by SIP (RFC 2543) - represent a security problem for 3GPP implementations.

The 3GPP Security Requirements states that protecting the core network signalling protocols is a clear architectural requirement for 3G systems. The security association between the SIP-message sender and the receiver has to be established and all SIP traffic has to be protected by some security mechanism.

2. Action:

The CN WG1 is kindly requesting the guidance from the SA WG3 pertaining to handling of the ICMP messages in 3GPP SIP implementations. The question posed to the SA WG3 is: "Should the 3GPP SIP implementation handle the ICMP messages as recommended in RFC 2543, or should they be ignored by the 3GPP SIP implementation?"

3. Date of Next CN1 Meetings:

CN1#19 10th – 12th July 2001 Dresden, Germany.

CN1#20 27th – 31th August 2001.

Thank you very much for your kind attention to this matter. The CN WG1 is looking forward toward our future collaboration.