

Title: Proposed Reply LS to "Protection of GTP Messages using IPsec"
Source: TSG SA WG3 Ad-Hoc
To: TSG CN WG4
Contact Person:

Name: Geir M. Køien

email: Geir-myrdahl.koien@telenor.com

Reply LS to "Protection of GTP Messages using IPsec"

This reply LS is sent by an SA3 ad-hoc meeting and CN4 is asked to bear this in mind when considering the reply.

The SA3#15bis ad-hoc thanks CN4 for the LS (N4-000847) on "Protection of GTP Messages Using IPsec".

The SA3 #15bis Ad-Hoc would like to comment on the issues raised in N4-000847.

We completely agree with CN4 that use of IPsec is an operator option. Indeed, there are countries where use of encryption is forbidden so to require mandatory use of IPsec is clearly not advisable.

It is also clear that operator agreements, bilateral or multilateral, should cover security requirements. Such agreements should cover security for all protocols used for interoperability, but it is not necessarily so that the same policies apply to all protocols. There are several reasons for this, including practical real-world deployment issues of the infrastructure to support secure protocols.

In LS N4-000847, CN4 specifically draws attention to one sentence from LS S3-000607 that has caused some concern in CN4.

“GTP-C protection should be mandatory for TS 29.060 R00, and all releases going forward.”

The consensus at the SA3#15bis Ad-Hoc and on the SA3 mailinglist is that this is a vendor requirement. So all R00(R4) compliant implementations of GTP as defined in TS 29.060 **shall** support IPsec for GTP-C. It is an operator option whether or not IPsec is to be used for intra-PLMN traffic and it is a roaming agreement issue whether or not IPsec is to be used for inter-PLMN traffic.

The SA3#15bis ad-hoc hopes that this clarifies the issue. Should CN4 for any reason want or need a formally approved LS from the SA3 plenary, it can be provided by our next plenary meeting in Sophia Antipolis (28-30.11.2000).