Source:	Ericsson and Nokia
Title:	IETF-53: Key transport in SIP
Agenda item:	TBD
Document for:	Information

1   Scope and objectives

This document summarise the status of key agreement discussed in SIPPING Working Group in IETF-53, Minneapolis, 17th –22nd, 2002.

2   Key agreement in SIP

Requirements related to key agreement in SIP have been discussed in SIPPING WG in IETF53, as well as in [SIPPING-DEL].

SIPPING 3GPP Ad-hoc meeting indicated that key agreement could not be solved by IETF in time, and that the matter might be controversial in IETF.

3GPP was unofficially encouraged to find its own solution to the problem without involving IETF. A suggested solution included the addition of "unspecified" parameters e.g. to the remote party identifier or the Digest AKA headers. Both headers have a syntax, which allows extra parameters to be carried and ignored by receivers who do not understand them. This makes it possible to use these existing headers also for this other purpose without breaking the SIP syntactic rules. This behaviour is not documented in any Internet Draft or RFC, but is rather specified in the 3GPP CN1 specifications only. This allows 3GPP equipment to interwork. This means that IETF will tolerate a minor 3GPP specific feature providing that it is only used between two 3GPP specific proxies. Mechanisms involving SIP clients, laptops or other end-user equipment must still be specified in IETF in order to provide interoperability.

The unofficial solution approach was also confirmed in a private discussion with a SIP WG chair.

3   References

[SIPPING-DEL] Arkko et al., "Requirements for Delegation of Message Protection for SIP", IETF, Work in progress, February 2002, draft-uusitalo-sipping-delegation-00.txt.