3GPP TSG SA WG3 Security — S3#17 **S3-010003**

27 February - 02 March, 2001

Gothenberg, Sweden

LIAISON STATEMENT

To: **3GPP S3, ETSI SAGE**
From: **Wap Security Group**
CC:
Date: **October, 2000**

Using Kasumi in WAP specification

WAP Forum WSG(WAP Security Group) is now developing a specification for WAP NG(Next Generation) TLS(Transport Layer Security) profile towards the end of this year. It intends to ensure an end-to-end secure communication between a wireless handset and an origin server on the Internet.

This specification is based on the TLS specification developed by the IETF, and some extensions are going to be made to accommodate to "wireless" communication. This extension includes adding algorithms to the current TLS cipher suites, and one candidate of them is Kasumi. The addition of algorithms to TLS has not been done by WSG, but independently by parties directly contacting the IETF.

If Kasumi is included in the TLS cipher suites, it can be used for both air link level ciphering and data communication level ciphering. It will save cost and resources for designing and implementing ciphers in a small handset. However, it is necessary to get 3GPP and ETSI permission to use Kasumi for our specification.

To explore the possiblity to include Kasumi in WAP NG TLS cipher suites, WAP WSG asks 3GPP S3 and ETSI SAGE to study and consider about permitting this.

Yours sincerely,

WAP Security Working Group