3GPP TSG SA WG3 Security — S3#14 **S3-000463**

1-4 August, 2000

Oslo, Norway

From: Chairman GSM2000 SA WG3 and GSMA SG Joint Working Party
Charles Brookson

To: SA WG3

Date: 14 July 2000

SUBJECT: Use of Kasumi for A5/3

The GSM2000 Group, the joint Working Party between 3GPP SA WG3 and the GSM Association Security Group met on the 10th July 2000 in Dusseldorf.

Mitsubishi has kindly offered their IP on Kasumi for use as A5/3 (and possibly GEA3). At a subsequent meeting between the GSM Association and ETSI it was thought appropriate for a formal agreement to be made on the use of Kasumi for this purpose. The final decision will be made after SAGE has carried an initial feasibility study.

SA WG3 is therefore formally asked to approve the use of Kasumi for A5/3 and other GSM purposes such as EDGE and GEA3.

Attached: Input document form Mitsubishi on Kasumi for A5/3.

GSM2000 Joint GSMA TSG SA WG3 Working Party **TD**

Dusseldorf, Germany

10 July, 2000

Utilisation of Kasumi for the GSM A5/3 Encryption Algorithm

Source: Mitsubishi Electric

Date: 7 July 2000

GSM Association, jointly with ETSI SMG10/3GPP TSG SA WG3, has produced a Requirement Specification for the GSM A5/3 Encryption Algorithm, ref. SMG P-00-310.

This specification is intended to be a mandatory standard for GSM, in addition to the already used A5/1 and A5/2 algorithms. A5/3 shall also be capable of use for EDGE and GPRS.

During development and selection phase of this new algorithm, following facts should be taken into account:

1. The algorithm shall satisfy the Requirements of the above mentioned Specifications.
2. Development, selection and evaluation time should be as short as possible.
3. Development and evaluation costs should be as low as possible.
4. Implementation complexity and cost should be as low as possible, particularly for dual mode GSM/UMTS terminals.

The use of a 3G adopted Encryption Algorithm "Kasumi", based on Mitsubishi's "Misty" fully satisfies the above criteria:

1. It is compliant to the Requirements Specifications.
2. Already developed, selected and evaluated for high security performance for 3G/UMTS, thus timing is not an issue.
3. No development and evaluation costs, as already covered within 3G selection.
4. Use of a common Encryption Algorithm in a dual mode terminals has lowest cost and complexity involved

Proposal:

Adopt 3G/UMTS selected Encryption Algorithm Kasumi as a new GSM A5/3 Algorithm

Intellectual Property:

As Kasumi is based on the Mitsubishi's Misty algorithm, the IPR in the new A5/3 Algorithm will be jointly owned both by Mitsubishi, 3GPP and GSM Association.

MELCO will offer Misty license on a non-discriminatory basis to those intending to make, use or sell products that are compliant with GSM Standard, and grant such licenses under separate written license agreements **without any license fee/royalty** and subject to other terms and conditions that it believes fair and commercially reasonable. MELCO reserves the right to refuse or withdraw Misty license to/from the parties that refuse to license, or claim unfair, unreasonable or discriminatory royalty rates for their

essential GSM/3G IPRs from MELCO.