3GPP TSG SA WG3 Security — S3#23 **S3-020388**

9 - 12 July 2002

Helsinki, Finland

ETSI SAGE **SAGE (02) 26**

4 July 2002

Title:	Use of Kasumi-based functions for Group release security solution
Response to:	LS S3-020287 “Reply LS on Group release security solution”
Source:	ETSI SAGE
To:	SA3
Cc:	RAN2

Contact Person:

Name:	**Steve Babbage**
Tel. Number:	+ 44 1635 676209
E-mail Address:	steve.babbage@vodafone.com

Attachments: None

Suitability of the f9 function for the purpose specified

f9 chips produce 32-bit output, so using f9 with a 64-bit output would of course require new development anyway.

And f9 with untruncated, 64-bit output does *not* give 64-bit security; the best analysis known gives a forgery attack using 2^{48} chosen messages. Although this is presumably not a practical concern, taken together with the previous statement it suggests that f9 with 64-bit output is not a good choice for the group release authentication function.

A preferred alternative

A better choice would be to use f8 — or, better still, a variant on f8. (The new A5/3 and GEA3 algorithms can be viewed as members of a family that also includes f8; this f8-variant would be another member of the same family.) So we would have:

- Group Release Indicia C (*n* bits, where *n* could be 64, although 128 seems more appropriate)
- Group Release Key K (*m* bits, where *m*=128 seems most appropriate, although any *m* between 64 and 128 inclusive could readily be accommodated by the design), such that C = f(K)
- An additional input M of up to 32 bits can readily be accommodated if desired, so that instead C = f(K,M)
- f(K) is a function along the lines of “first *n* bits of f8-variant keystream, with all unused input parameters fixed”.

SAGE could define such a function; it would be a natural addition to the Kasumi-based family of algorithms including f8, A5/3 and GEA3.

IPR on Kasumi

SAGE does not anticipate any problems with the use of another member of the Kasumi-based family of algorithms for the purpose specified.

Conclusion

SAGE recommends that a new member of the Kasumi-based function family that already includes f8, A5/3 and GEA3 be defined; this function would derive an *n*-bit Group Release Indicia from a 128-bit Group Release Key.

n can be 64 if this is felt suitable; however, in the context of 3G security generally, SAGE encourages S3 to consider specifying *n*=128.