## 3GPP TSG SA WG3 Security — S3#22 S3-020287

## 14 - 17 May 2002

## Victoria, Canada

**Title:** Reply LS on Group release security solution

**Response to:** LS *R2-020797* on Group release security solution from RAN 2

**Source:** SA3

**To:** RAN2, ETSI SAGE

**Cc:**

**Contact Person:**
**Name:** **Marc Blommaert**
**Tel. Number:** + 32 14 25 3411
**E-mail Address:** Marc.Blommaert@Siemens.atea.be

**Attachments:** None

### 1. Overall Description:

This is a reply-LS to RAN2 LS R2-020797 (S3-020178) that includes R2-020734.

SA3 thanks RAN2 for providing the opportunity to analyse the group release security solution. This LS provides remarks related to alternative 2 of section 2.2.2 of R2-020734 and additional comments on the concept. Alternative 1 was not considered as it was already pointed out by RAN2 that it was insecure.

#### A) Output length for the ‘Release Indicia’.

SA3 recommends using a minimum of 64-bit as length for the indicia. SA3 discussed also a 32-bit length but it was found not to be sufficient.

#### B) The ‘Release Indicia’ shall be integrity protected, but confidentiality protection by the channel on which it is transferred cannot be guaranteed.

Section 2.2.2 principle 3 mentions that *‘The authentication release Indicia should be sent on an encrypted channel (DCCH)’. If the channel is not encrypted, an integrity protection mechanism can be used. ‘*
Confidentiality protection of the air interface is optional for the operator, and is already established between UE and RNC or not, when the RNC wants to sent the ‘release indicia’. Using confidentiality protection only for the ‘group release’ feature is not possible as suggested in principle 3 of section 2.2.2.
From a security point of view the integrity protection of the ‘Authentication release indicia’ is enough. Confidentiality protection does not add any security to the mechanism. The integrity protection of the Layer 3 RRC commands ensure that the release indicia cannot be modified by a man in the middle.

#### C) It is unclear if KASUMI can be used for deriving the ‘Release Indicia’.

KASUMI seems to be an obvious choice as it is already present in the MT and the RNC, but it is not certain that the KASUMI algorithm may be used outside the already defined use within f8 and f9.

KASUMI is a block cipher that forms the heart of the 3GPP confidentiality algorithm ***f8***, and the 3GPP integrity algorithm ***f9***.

[TS 35.202] Contains following text on the Intellectual Property Rights of the KASUMI algorithm:
*‘The f8 & f9 Algorithms Specifications may be used only for the development and operation of 3G Mobile Communications and services. Every Beneficiary must sign a Restricted Usage Undertaking with the Custodian and demonstrate that he fulfills the approval criteria specified in the Restricted Usage Undertaking.*

*Furthermore, Mitsubishi Electric Corporation holds essential patents on the Algorithms. The Beneficiary must get a separate IPR License Agreement from Mitsubishi Electronic Corporation Japan.*
*For details of licensing procedures, contact ETSI, ARIB, TTA or T1.'*

Currently SAGE is specifiying to use KASUMI as the core algorithm for A5/3, GEA3 and a variant of A5/3 for GSM EDGE. Because of the licencing aspect it seems prudent to involve ETSI on whether a different use might be allowed. If it would be allowed, than the use could be documented by ETSI SAGE in a separate TS 35.xxx as algorithm $f_{xy}$.

**D) Instead of using KASUMI directly, the message authentication function *f9* should be considered, with constant values for the other required inputs to *f9*.**

Following reasons are favouring the use of the function f9

1) The required functionality is that of message authentication, not encryption.

2) Some manufacturers may have chosen to implement *f8* and *f9* as hardware units without directly exposing the functionality of KASUMI.

3) No interface to KASUMI is directly available in existing standards.

But as the f9 function only produces a 32-bit output and a 64-bit output is required (as mentioned in bullet A), changes will be required to f9. So ETSI SAGE needs to be consulted anyhow. It must be mentioned that f9 generates internally a 64-bit result but truncates this to a 32-bit output.

**E) The generation and use of the 'authentication key' needs further specification.**

The 128-bit 'authentication key' (belonging to a U_RNTI group) needs to be generated by a suitable key generation function. A key can only be used once, as it traverses the air when used for a group release. Consequently, after using this at RNC reset, a new 'authentication key' needs to be generated. The 'authentication key' may not leave the SRNC, unless used immediately for the 'group release (f.i. to be used in a DRNC).

**F) An 'authentication key' refresh mechanism needs to be considered.**

If the time between using a new 'authentication key' (i.e sending the first time the release indicia to a UE) and using the group release mechanism (i.e. sending the 'authentication key' over the air) would become too long, an attacker could still be in the possibility to mount a brute force attack to retrieve the 'authentication key'.

**G) The name 'authentication key' is misleading.**

A reader might think at the UMTS authentication. 'Group release key' and 'Group Release Indicia' are considered to be more meaningful names.

**H) The 'group release' algorithm needs to be documented in 'S3-specifications'.**

ETSI SAGE-specification might be needed (using a 64-bit f9 function) but also TS 33.102 and TS 33.103 shall be updated after an agreement on the needed 'group release' feature.

Finally SA3 would like to advise RAN2 that specifying security for the group release feature is a significant task and that we are very concerned to be doing it in time for Release 5.

## 2. Actions:

**To RAN2 group.**

**ACTION: SA3 asks RAN2 to consider the above remarks and to keep SA3 informed about alternative solutions and final RAN2-agreed proposals.**

**To ETSI SAGE group.**

**ACTION: SA3 asks ETSI SAGE to investigate if the f9-function can make a 64-bit output available.**

## 3. Date of Next TSG-SA3 Meetings:

| | | |
|---|---|---|
| SA3-24 | 9th – 12th July 2002 | Helsinki, Finland |
| SA3-25 | 8th – 11th Oct 2002 | Munich, Germany |