3GPP TSG SA WG3 Security — S3#23 **S3-020206**

14 - 17 May 2002

Victoria, Canada

Source: **Siemens**

Title: **Group Release Security Solution Analysis (S3-020178)**

Document for: **Discussion**

Agenda Item: **T.B.D**

Abstract

This contribution discusses the 'Group release security solution' as provided by a Liaison Statement from RAN2 (R2-020797) to SA3 (S3-020178).

1) Introduction

Within S3-020178, SA3 is asked by RAN2 to verify the presented solution for 'group release'. This contribution evaluates the security aspects of the proposed (not agreed within RAN2) solution.

2) Evaluation

A) The 'preferred alternative 2' of section 2.2.2 [R2-020797] uses KASUMI.

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}.

Alternative algorithms to derive the indicia could be to use HMAC-SHA-1.

B) The use of C = KASUMI $(M)_{KEY}$ as a one-way function needs further specification.

KASUMI [TS 35.202] is defined as taking a 64-bit input and producing a 64-bit output under control of a 128-bit-key, whereas in the alternative 2 of section 2.2.2 [R2-020797] all M, KEY and C are having 64-bits.

If KASUMI is used, than the 'authentication key' shall be 128-bits long, and a rule shall be specified to derive a shorter length Indicia (if needed) from the 64-bits output produced by KASUMI (i.e. Take the highest order bits)

An alternative function to generate the release indicia C could be defined by using a non-keyed hash function that takes the 'authentication key' as input (I.e SHA-1), i.e. it is not clear how the use of U_RNTI as input brings more security.

C) What is a sufficient output length for the Release Indicia C to provide a reasonable level of security?

A 32-bit length of the indicia is considered long enough. The security is dependent on the one-way strength of the hash function and the true randomness of the 'authentication key'.

D) 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 pseudo random generator function on the RNC (I.e the key shall be unpredictable and independently from previous keys). 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).

E) 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 a more meaningfull names.

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

SAGE-specification might be needed (when using KASUMI) but also TS 33.102 and TS 33.103 shall be updated after an agreement on the needed 'group release' feature.

G) The Authentication 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.

An attacker may have both *Indicia (C)* and *the input to derive the indicia (M)* available when the Indicia are not transferred over a confidentiality protected channel. Mounting a brute force attack to derive a 128-bit key will not be completed within reasonable time, even if success is expected after probing the half of the key space.

3) Conclusion

It is proposed that SA3 considers the above security remarks on the ‘Group Release solution’, and provide an answer to RAN2, that is also meeting this week. In addition, RAN2 shall be asked to inform SA3 about any further proposals for the group release feature, such that the security can be evaluated.

4) References

[TS 35.201]: 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: *f8* and *f9* Specification".

[TS 35.202]: 3GPP TS 35.202: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification (Release 4).

[TS 33.102]: 3G TS 33.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture".