3GPP TSG SA WG3 Security **S3-020510**

8th – 11th October, 2002

Munich, Germany

Agenda Item: 7.4 UTRAN network access security

Source: Ericsson

Title: Group Release Authentication algorithm

Document for: Discussion/Decision

1 Introduction

TSG RAN WG 2 has discussed the group release function of several UEs with a single RRC message that would include a security solution preventing an attacker to force many UEs to falsely go into IDLE mode. This feature was discussed at SA3#22 in the LS from RAN WG 2 (S3-020178).

Although the function itself has not yet been approved by RAN WG 2 Ericsson seeks support from SA3 to agree on that HMAC SHA-1 is used to create the Group Indicia and that the indicia as well as the key are 128 bit long.

Given that SA3 approves these working assumptions Ericsson suggests that SA3 sends an LS with the requirements to RAN WG 2. The LS should also inform RAN WG 2 that SA3 expects to approve a CR against TS33.102 at SA3#26 should RAN WG 2 adopt the Group Release function.

2 Discussion

2.1 Group Release Authentication overview

1. In situations when the network lost information about UEs in connected mode, such as after an RNC, MSC or SGSN reset, the RNC(s) should bring all affected UEs down to idle mode, in order to keep the UEs reachable for terminating traffic. The most efficient way is to send a message to all or a group of terminals, forcing them back to idle mode. This function is called Group Release. The message can not be protected using the existing ciphering or integrity protection mechanisms since the security contexts may be lost or would require a release of the UEs one by one.

2. To avoid attacks where an adversary sends a false Group Release messages, the UEs need to be able to authenticate the message. A shared secret between the RNC and all connected mode UEs does not work, as all UEs (even the adversary's) would know it.

3. The solution is that the RNC generates a secret, random, Group Release Key, (K). K is common for a group of UEs. For each UE in connected mode, the RNC generates a Group Release Indicia (I) by:

$I = f(K, U)$,

where f() is a one-way hash function and U is the U-RNTI, a (public) identifier for each UE. I is therefore different for each UE. I is sent with integrity protection (in order to avoid Man-in-the-middle attacks.) The RNC may generate new Group Release Keys periodically, and would then need to calculate and send a new Group Release Indicia to the UEs. Similarly, if the U-RNTI of a UE changes, e.g. at SRNS relocation, a new Group Release Indicia is also calculated and sent.

4. In situations such as those mentioned under 1 above, the RNC sends a Group Release message to all affected UEs with K included, addressed to the group of UEs which share the same K. (This is the first time that K leaves the RNC.) All UEs run I=f(K,U), and compares the result to their stored I. If they are equal, the message is considered authenticated and the UE enters idle mode.

2.2 Key and Indicia length

Group Release Key and Group Length Indicia must be of sufficient length to withstand an attack. As an UE typically is not in connected mode more than minutes or possibly hours, the security of the algorithm need only be able to protect that long. For UEs that stay in connected mode longer, the Group Release Indicia is refreshed periodically, based on operator policy. In [7], SAGE suggests a 128 bit Group Release Key and Group Release Indicia. In [3], a hash value of 80+ bits is suggested for a related usage. In [6], a hash value of 96 bits is used.

2.3 Algorithms

In [8], section 2.2.2, there is a proposal on using KASUMI[1] to derive the Group Release Indicia. The U-RNTI is fed into the message input and the Group Release Key is fed into the key input. The Key is 128 bits and the Indicia is 64 bits. In [11], it was suggested that a modified f9[2] algorithm should be used instead of KASUMI. The modification consists of using the full 64 bits output that f9 uses internally, instead of truncating it as is does today. [9] also suggests using f9. A reason is that manufacturers may have chosen to implement f8 and f9 in hardware, with no direct interface to KASUMI. [10] suggests using HMAC-SHA1 to derive the Indicia.

In [7], SAGE notes that the use of f9 with the full 64 bits output would require new development. Instead, they suggest the development of a new algorithm, based on f8[2].

Developing a new cryptographic algorithm is a major task. It requires a fair amount of evaluation, in order to assess its strength. SAGE has the experience developing algorithms based on KASUMI, but Ericsson understands that SAGE would require enough time to evaluate the algorithm making it difficult for them to deliver according to RAN2 Release 5 time scale. Using an existing, proven algorithm would reduce the development effort while assuring good security.

An existing, proven algorithm is HMAC-SHA1. HMAC-SHA1 is a variant of the HMAC[3] algorithm, using SHA-1[4] internally. This algorithm has several advantages.

1. It is well known, understood and well analysed.
2. It can be ready for Release 5.
3. The Group Release Key length is not determined by the algorithm. It can be of any convenient length. The Group Release Indicia can be up to 160 bits.
4. It is fast, an order of magnitude faster than the f9 proposal.
5. It unencumbered by IPR issues.
6. Reference code is available [4], [5].
7. It is less complex than a f8 or f9 alternative.
8. SHA-1 is already available in all UEs using the WAP protocol.

3 Proposal

Ericsson proposes that SA3 adopts:

1) HMAC-SHA1 is used to derive the group Release Indicia, and that it shall be captured in TS 33.102.

2) The Group Release Key shall be 128 bits long.

3) The Group Release Indicia shall be 128 bits long.

4 References

[1] 3GPP TS 35.202 **3rd Generation partnership Project; Technical Specification Group Services and Systems Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification**.

[2] 3GPP TS 35.201 **3rd Generation partnership Project; Technical Specification Group Services and Systems Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification**.

[3] RFC 2104, **HMAC: Keyed-Hashing for Message Authentication**

[4] RFC 3174, **US Secure Hash Algorithm 1 (SHA1)**

[5] RFC 2202, **Test Cases for HMAC-MD5 and HMAC-SHA-1**

[6] RFC 2404, **The Use of HMAC-SHA-1-96 within ESP and AH**

[7] R2-021866, **Use of Kasumi-based functions for Group release security solution**, 4 July 2002

[8] R2-020734, **Actions at RNC reset**, Ericsson

[9] S3-020205, **Comment on R2 Group Release Security Solution**, Qualcomm

[10] S3-020206, **Group Release Security Solution Analysis (S3-020178),** Siemens

[11] S3-020287, **Reply LS on Group release security solution**, SA3.