3GPP TSG SA WG3 Security — S3#16 **S3-000691**

28-30 November, 2000

Sophia Antipolis, France

Source:	**Vodafone**
Title:	**Emergency call handling**
Document for:	**Discussion/Decision**
Agenda Item:	**10.1**

1 Introduction

This document discusses issues relating to emergency call handling in the 3GPP R99 specifications and proposes that S3 should consider applying the same security procedures to emergency calls as for non-emergency calls.

2 Clarification of emergency call handling specifications in 33.102

There is currently some confusion over how to interpret the recent changes to the emergency call handling specifications in 33.102, section 6.4.9. There are two interpretations:

(A) As a serving network option, emergency calls may *only* be established without security procedures being applied in four specific cases (USIM not present, valid USIM not present due to USIM being barred or no roaming agreement, fresh authentication vectors not available in serving network due to network failure, USIM authentication failure).

(B) As a serving network option, emergency calls may be established without security procedures being applied but it is *recommended* that emergency calls may only be established without security procedures being applied in four specific cases (USIM not present, valid USIM not present due to USIM being barred or no roaming agreement, fresh authentication vectors not available in serving network due to network failure, USIM authentication failure).

Although interpretation (A) is clearly stronger from a security perspective, it appears that some S3 participants will not accept interpretation (A) since they seem to require the possibility for emergency calls to be established without security procedures in cases that are not currently listed.

The risk in accepting interpretation (B) is that it is more likely that serving network operators will never apply security procedures to emergency calls. However, we can never prevent this even if interpretation (A) is adopted, we just make it less likely.

N1 cannot approve the stage 3 specifications in 24.008 until S3 remove the ambiguity. Currently it is understood that N1 have assumed interpretation (B).

Rather than deciding between the two interpretations, Vodafone believe that S3 must take a closer look at the consequences of allowing emergency calls to be established without security procedures being applied.

3 Consequences of allowing emergency calls without security

Originally, the intention in S3 was to apply the same security procedures for emergency calls and non-emergency calls. However, a requirement was raised for certain serving network operators to be able to disable security procedures for emergency calls. The apparent motivation behind this was to ensure that operators could take all reasonable steps to ensure that an emergency call can be connected as a priority. For example, there was a belief that it should be possible to connect emergency calls even when the application of security is impossible or the application of security would result in the call being rejected because of a security failure.

To fulfil this requirement some changes were made to 33.102 to allow security procedures to be disabled as a serving network option under certain conditions. The result is the text in 33.102 v3.5.0, section 6.4.9.

It is important to acknowledge the consequences for operators who choose not to apply security to emergency calls. Some of these consequences are listed below:

1) Operators who do not apply security to emergency calls will not be able to reliably identify malicious callers using the IMSI and therefore cannot bar those users (note that barring the IMEI would also be ineffective).

2) Operators who do not apply security to emergency calls will not be able to reliably identify callers to emergency services. Identification of emergency callers may be a regulatory requirement in some jurisdictions.

Unfortunately the provision of this capability also has an impact on *all* users and as a result *all* operators; not just those who choose not to apply security to emergency calls. This is due to the fact that *all* mobiles must be capable of establishing an emergency call without security being applied. Some of the effects are described below:

3) An active attacker could eavesdrop an emergency call.

4) An active attacker could block an emergency message and force the mobile to think that it has been successfully transmitted/acknowledged.

Although these active attacks may be quite sophisticated, they would be prevented if emergency calls were treated in the same way as non-emergency calls where the application of security procedures is mandatory[1]. The cipher indicator would help the user detect whether they are subject to these attacks, but this is clearly not as "user friendly" nor as effective as preventing the attack in the first place.

The second effect, in particular, seems to conflict with the original requirement to ensure that operators take all reasonable steps to ensure that an emergency calls can be connected as a priority. It must therefore be questioned whether the facility to turn off security for emergency calls helps or hinders attempts by operators to meet the original requirement.

Note also that these effects, if not corrected now, will persist even if all operators apply security for all emergency calls which we believe will eventually be the case in practice due to the risks identified in (1) and (2) above.

Vodafone believe that S3 should consider removal of the facility to allow operators to establish emergency calls without applying security procedures.

Note that if this proposal is approved then any ‘old’ mobiles which do still accept emergency calls without security will work in ‘new’ RNCs, however ‘old’ RNCs will not be able to establish emergency calls without security for ‘new’ mobiles.

[1] Ciphering is not mandatory but this does not affect the ability to prevent these attacks. Note that an active attacker is prevented from turn off ciphering because of mandatory integrity protection on the relevant signalling messages.