3GPP TSG SA WG3 Security — S3#14 **S3-000408**

31st-4th August, 2000

Oslo, Norway

Source: Ericsson, Nokia, Siemens

Ciphering for GSM/EDGE RAN

1 Introduction

This document suggests a few ciphering working assumptions for the GSM/EDGE radio access network. This document is not reflecting a formal position in SMG2 but rather reflects the opinion of the companies listed as source. However those companies were the main one being involved into the discussion in SMG2.

Adopting the functional split of the Iu interface will require that ciphering is performed in the radio access network and not in the core network as in (E)GPRS. Depending on how this is implemented in the BSS it will increase the complexity in the BSC or BTS.

Apart from the protocol considerations there are security aspects as well to take into account. From a security point of view the ciphering should be done before channel encoding (and after source coding) since the redundancy of the channel encoding can be used to break the crypto. However, all the ciphering algorithms that are in use in GSM/GPRS or in UMTS are designed to be resistant against this kind of attacks.

In GSM and EDGE, the ciphering algorithm that is implemented uses a ciphering key (Kc) and a count variable as input to get the crypto message which is modulo-2 added to the payload. The same count variable should only be used for one payload since otherwise the two encrypted messages can be added and enough information is obtained to reveal the original messages in plaintext although the algorithms are designed to be resistant against "known plaintext" attacks, it is a good practice to use the same count variable whenever a payload is retransmitted. Note however, that in this case the retransmitted payload must be exactly the same as the original; since otherwise the attack described above applies for the part that is different in the original and in the retransmitted payload.

Also some legal considerations have to be taken into account. For ciphering equipment there are export restrictions considering the length of the ciphering key when exporting equipment to certain countries. These issues have to be considered carefully as well so that legal difficulties are avoided.

2 The UMTS ciphering algorithm

For UMTS, the ciphering is done at the RLC [1] or MAC [2] layer. The payload part of a packet is modulo-2 added with the ciphering bits. For the non-transparent services there is a sequence number present at the RLC layer, which can be used as input to the ciphering algorithm. The payload part of a packet can be between 24-5000 bits. For the transparent services, the ciphering is done at the MAC layer. There is no sequence number present at the MAC layer for transparent services so a radio frame number which is updated every 10 ms is introduced here for this case.

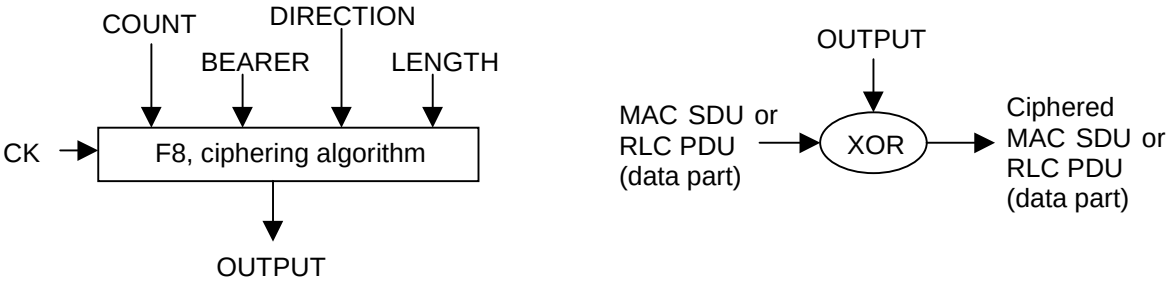

Figure 1. Ciphering for the UMTS, RLC and MAC respectively.

3 The PDCP, RLC, and MAC layers in GSM/EDGE RAN

In GSM/EDGE RAN the radio protocols are PDCP, RLC and MAC layer as described in the stage 2 description for GERAN [3] and depicted below.

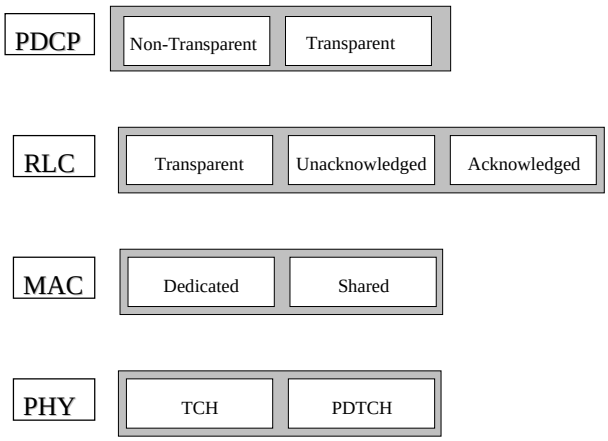

Figure 2: GERAN user plane protocol stack

The PDCP layer has a transparent mode and several non-transparent modes. The RLC layer has three modes, one acknowledged mode, one unacknowledged mode, and one transparent mode. The MAC layer is divided into one shared mode and one dedicated mode.

The above mentioned modes can be combined in different ways to achieve different bearers. To align with UMTS, four radio access bearer classes are proposed for the GMS/EDGE RAN. These four classes are conversational, streaming, interactive, and background.

The ciphering algorithm needs some kind of sequence number to generate the ciphering bits. This sequence number has to be known at both the transmitting and the receiving side. In the case of transparent RLC, there is no sequence number present at the RLC and MAC layers, so to be able to have ciphering for these cases some kind of numbering has to be introduced.

4 Proposed solution for GERAN

4.1 Ciphering algorithm

In order to align with UMTS and to allow service transparency also from a security point of view it is proposed to use the UMTS 128bit f8 algorithm also for GERAN. The UMTS algorithm is designed to handle blocks of up to 5000 bits.

4.2 Ciphering location

Regarding the ciphering location it is proposed to implement the ciphering algorithm at the RLC protocol layer for non-transparent services and at the MAC protocol layer for the transparent services. The main advantage of this is the alignment with UMTS. Proposed solution for GERAN

5 Conclusion

A working assumption regarding ciphering is proposed to 3GPP S3 allowing full alignment with UMTS and offers full service transparency also from a security aspect.

The next GERAN Adhoc will be 7th-11th of August. If S3 has other issues to raise regarding GERAN security it would be beneficial to raise them for this meeting.

6 References

[1] 3GPP 25.322, “Radio Link Control protocol specification”.

[2] 3GPP 25.322, “Medium Access Control protocol specification”.

[3] ETSI 03.51, “Stage 2 description: GERAN overall description”