GSM 03.20 - EXT
Version: 3.0.0
Date: 25 June 1993

Work Item No:

Key words:

European digital cellular telecommunication system (phase 1);

Security Related Network Functions Part 2

ETSI

European Telecommunications Standards Institute
ETSI Secretariat: Route des Lucioles, F-06921 Sophia Antipolis Cedex . France
TP. + 33 92 94 42 00 TF. + 33 93 65 47 16 Tx. 47 00 40 F

Preface:

This specification is an addendum to GSM 03.20 version 3.3.2 and shall only be read in connection with that specification.

The page numbers used in this document is equivalent to those used in GSM 03.20 version 3.3.2 and can be seen as a page by page replacement.

Changes with GSM 03.20 version 03.3.2 as reference are marked as follows:

Double Underline	:	New added text.
Strikethrough	:	Deleted text.
Vertical Bar in margin	:	Changes occur in the corresponding line.

The support of the additional functionality specified in this addendum is not mandatory, however if the functionality is supported, it shall be supported completely in accordance with this specification.

ETSI/TC GSM

Title : **Recommendation GSM 03.20 - EXT**

Security Related Network Functions, part 2

Version : 3.0.0

Date : June 1993

List of contents:

Language of original : English

TABLE OF CONTENTS

0. SCOPE

This recommendation specifies the network functions needed to provide the security related service and functions specified in Recommendation GSM 02.09.

This recommendation does not address the cryptological algorithms that are needed to provide different security related features. This topic is addressed in Annex 3 Wherever a cryptological algorithm or mechanism is needed, this is signalled with a reference to Annex 3 The references refers only to functionalities, and some algorithms may be identical or use common hardware.

This delta recommendation only includes modified parts concerning the short term solution (phase 1) for support of dual ciphering algorithms (A5/1 and A5/2).

1. GENERAL

The different security related service and functions that are listed in Recommendation 02.09 are grouped as follows :

- Subscriber identity confidentiality;
- Subscriber identity authentication;
- Signalling information element and connectionless user data confidentiality;
- Data confidentiality for physical connections.

All functions must be implemented with minimum assumptions about the cryptologial algorithms that are used, and it must be possible that these algorithms are changed during the system life time. Any change in these algorithms must not change the format of the messages exchanged via the interfaces of the system. The system must be prepared for a parallel operation of more than one algorithm during a transitional period.

The security procedures must include mechanisms to enable recovery in event of signalling failures. These recovery procedures must be designed in such a way that they cannot be used to breach the security of the system.

General note on figures :

1- In the figures below, signalling exchanges are referred by functional names. The exact messages and message types are specified in Rec. GSM 04.08 and Rec. GSM 09.02.

2- No assumptions are taken for function splitting between MSC (Mobile Switching Centre), VLR and BS (Base Station). Signalling is hence described directly between MS and the local network (i.e. MSC, VLR, and BS, denoted in the figures by BS/MSC/VLR). The splitting in Annex 1 is only given for illustrative purpose.

3- Addressing fields are not given; all information relate to the signalling layer. The TMSI allows addressing schemes without IMSI, but the actual implementation is specified in the 04. series.

4- The term HPLMN in the figures below is used as a general term which should be understood as HLR (Home Location Register) or AR (Authentication Centre).

5- What is put in a box is not part of the described procedure but it is relevant to the understanding of the figure.

4.7 [Spare]

4.8 Negotiation of A5 algorithm

Not more than two versions of the A5 algorithm will be defined for the short term solution (phase 1).

When an MS wishes to establish a connection with the network, the MS shall indicate to the network the version(s) of the A5 algorithm it is prepared to use.

The network shall compare its ciphering capabilities and preferences with those indicated by the MS and shall act according to the following rules:

1 If the MS and the network have no versions of the A5 algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.

2 If the MS and the network have at least one version of the A5 algorithm in common, then the network shall select one of the mutually acceptable versions of the A5 algorithm for use on that connection.

3 If the MS and the network have no versions of the A5 algorithm in common and the network is willing to use an unciphered connection, then an unciphered connection shall be used.