Tele
Norwegian
Telecommunications Administration

NORDIC MOBILE TELEPHONE GROUP

Date
6 October 1989

Our reference
MS 89 - 32
NMT-doc. 89 - 2216

To
Manufacturers of
NMT-900 mobile stations

Utsendt/ released 09 OKT. 1989

NMT-SIS. SUBSCRIBER IDENTITY SECURITY

Revised time schedule. Corrections and clarifications of the NMT-SIS specification.

Dear Sirs,

Based on comments from the MS manufacturers and discussions between the NMT operators and the national MS dealers' organizations, there is a need to revise the NMT-SIS time schedule, and to make some corrections and clarifications of the NMT-SIS specifications (ref. letters MS 88-26 dated 21 July 1988, MS 88-27 dated 11 October 1988 and MS 88-29 dated 30 November 1988).

A. TIME SCHEDULE FOR NMT-SIS

The time schedule for implementation of the NMT-SIS function in the MS has been postponed.

The revised NMT-SIS time schedule is as follows:

- Denmark, Finland, Norway, Sweden and Switzerland will make the NMT-SIS specifications mandatory on all NMT-900 mobile stations, excluding reused equipment, sold from 1 October 1990, and on NMT-900 mobile stations submitted for type testing after 1 September 1989 However, Denmark will accept non-SIS mobile stations submitted for type testing until 28 February 1990.

Address: Postboks 6701 St. Olavs pl. N-0130 Oslo 1
Office: Universitetsgata 2
Telephone: National (02) 48 89 90 International + 47 2 48 89 90
Telegrams: Gentel Oslo
Telex: 71203 gentel n
Telefax: National (02) 48 87 20 International + 47 2 48 87 20

- The Netherlands has already made the NMT-SIS specifications mandatory in their NMT-900 network.

B. CORRECTIONS

1. **Specification for NMT-SIS key management in NMT-900, para 4.4 (page 12):**

   Replace first sentence "Reprogramming ...not be possible" with the following text:
   "SIM modules may be reprogrammable. In this case the previously installed SAK shall be erased completely, and the new SAK shall completely replace the previous SAK. The requirements for reprogramming SIM modules are the same as for initial programming, i.e. programming by the manufacturer, and transfer of reference number and encrypted SAK to the administration(s). When reprogramming, the SIM module shall be given a new reference number."

2. SIS Addendum to NMT Doc. 900-1, item 29 - 32:

   The MS shall also be able to transmit unencrypted digits in the authentication procedure, if the MTX orders so by transmitting 5a (L=3) instead of 5a (L=11).

3. **SIS Addendum to NMT Doc. 900-1, item 31, para 4.4.1.7 (MS with priority), state 11a:**

   Transmission of frame 7 shall continue (with a minimum of 4 frames) until the next sequence of frame 5a (L=9), or until frame 13a (L=14) is received.

C. **CLARIFICATION**

1. **SIS Addendum to NMT Doc 900-3, item 13 and 15, including enclosure 2 (flowchart A), and SIS Addendum to NMT Doc 900-1, para 4.4.1.1, 4.4.1.6 and 4.4.1.11:**

   The following clarification shall be applied:

"The MS shall start transmission of frame 10b/12 after analysis of the frame following next to frame 3b. The MS shall accept the first correctly received frame 7 from MTX, received within T after start transmit frame 10b, or until frame 5a (L=3/11) is received."

2. Definition of BKEY

The BKEY is used for encryption and decryption of the B-number. It is the hex numbers C_1 - C_6 defined in SIS Addendum to NMT Doc 900-1, Enclosure 1, para 4.3.3.15.3 (NB! Misprinting: C_1 = x DIV 16, ref. MS 88-27.)

3.

Availability of the SIM reference number

The SIM reference number installed in an MS shall be readable by the mobile subscriber in the form as stated in our letter MS 88-29.

The corrections and clarifications are valid with immediate effect.

Yours faithfully

Hans Myhre

Hans Myhre
Chairman of the Nordic Mobile Telephone Group

NMT-SIS

AUTHENTICATION REGISTER

Functional specification of an Authentication Register for NMT-900

LIST OF CONTENTS

1. INTRODUCTION

The introduction of subscriber identity security makes it necessary to extend the functionality of the MTXs.
An MTX must be able to sent challenges and check received signed responses. For practical and security reasons, it has been decided to introduce an new functional entity, called the authentication register (AR). This AR will carry out security functions which are needed to support the MTX. In particular the AR contains ID-SAK pairs and supplies the MTXs with RAND - SRES - BKEY triples which can be used to authenticate users.
The functionality of the AR will be standardized and therefore is the same in all countries.

In this paper first the functional description of an AR is given (chapter 2). In chapter 3, the communication procedures for an AR are given and in chapter 4 requirements for an AR are listed. Finally, implementation aspects of an AR are discussed.

2. FUNCTIONAL DESCRIPTION

The AR is an intermediate between the administration and a number of MTXs. The AR is introduced in order to keep key management controllable and secure.

In each country a number of ARs can exist simultaneously. Each AR supports one or more MTXs. MTXs can not be supported by more than one AR at same time. The most general configuration is given in figure 1.

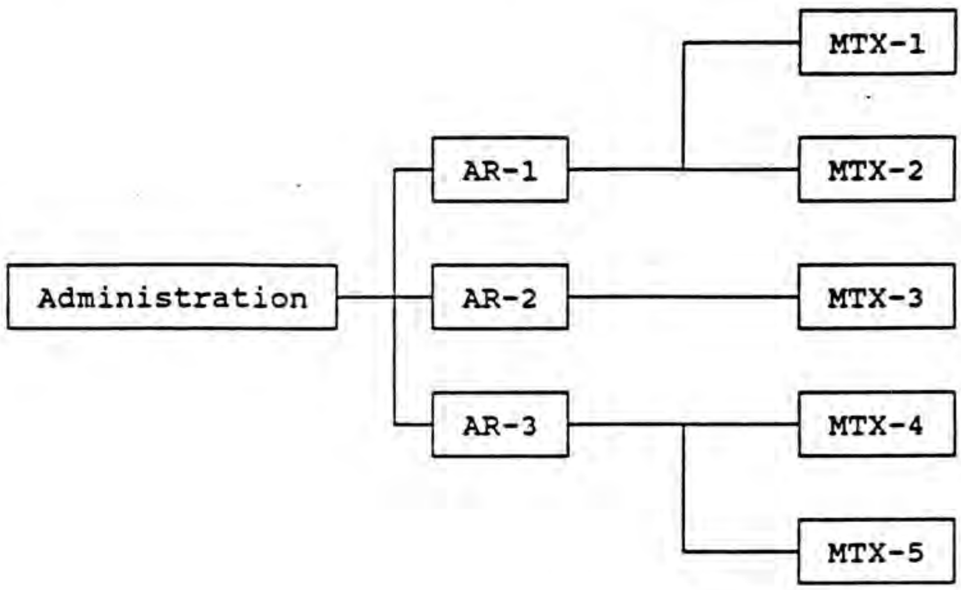


Figure 1.

When a secret authentication key (SAK) is coupled to an user identity (ID) this ID-SAK pair is, depending on the administrations policy, installed in one or more of the ARs. These pairs are stored in the AR in a secure way.

Within the AR, random numbers are generated and the ID-SAK combinations are used to produce triples containing RAND, SRES and B-KEY.

On request, these triples can be sent to MTXs where they can be used for authentication. Normally, each of these triples is used by the MTX only once. The MTX asks the AR for a set of new triples if within the MTX a certain minimum level of unused triples is reached.

The purpose of this mechanism is that SAKs only are stored in clear text in the AR. Therefore, the AR needs a strong protection.
If, for any reason, it is not possible to update an MTX with authentication triples, the responsibility for allowing call set up is left to the administration.

3. COMMUNICATION PROCEDURES

Procedures have to be defined for the communication between AR and administration and the communication between AR and MTXs. The administration can be divided in two functional parts. The first is a national database, containing pairs consisting of the reference number of a security module and the corresponding enciphered SAK.
The second part is an administrative system, containing apart from general operational data, also information concerning security modules operating in the country.
The relations between the functional entities, i.e the two parts of the administration, the AR and the MTXs, are detailed in figure 2 below.

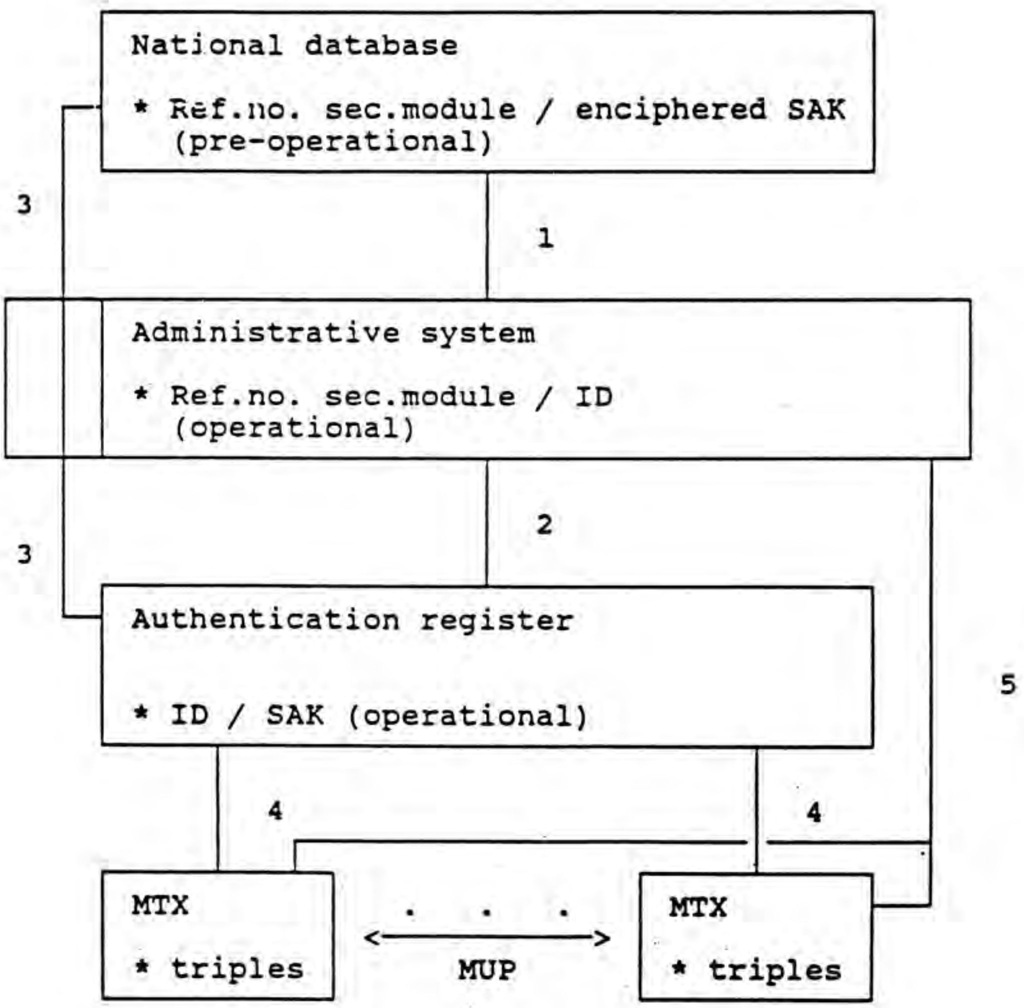


Figure 2

The administrative system can check via communication channel 1 if an (enciphered) SAK corresponding to a certain reference number is available in the database.
The keys for deciphering SAKs will be stored in the AR.

For putting an ID into operation two possible functional options are available. Serving both options is a requirement for the system configuration.

Option 1

If an ID is put into operation, the administrative system sends the corresponding reference number of the security module to the national database via channel 1. The enciphered SAK will be send from the database to the administrative system via channel 3. Via channel 3, the administrative system installs the ID/enciphered SAK relation in the AR, and sends the identification of the decipher key. The AR deciphers the SAKs and stores the SAK/ID pairs.
Via channel 5, the administrative system sends the ID and relevant subscriber data to the MTX. In this option, in principle channel 3 can be integrated in channel 1 and 2.

Option 2

If an ID is put into operation, the administrative system sends the ID and the corresponding reference number of the security module to the AR via channel 2. By sending the reference number to the national database, the AR directly requests and receives the enciphered SAK and the identification of the decipher key via channel 3. After deciphering the SAK, the AR stores the ID/SAK pairs.
Via channel 5, the administrative system sends the ID and relevant subscriber data to the MTX.

In the following tables the two options are summarized.

Option 1

Interface	Direction	Data
1	adm.sys.-> datab.	request for (SAK)
	datab.-> adm.sys.	available yes no (SAK)
2	adm.sys.-> AR	ID/encip.(SAK) pair + decip. key identification
3	-	part of interface 1 and 2
4	MTX -> AR	request for triples
	AR -> MTX	triples
5	adm.sys.-> MTX	ID + relevant subscriber data

Option 2

Interface	Direction	Data
1	adm.sys.-> datab.	request for (SAK)
	datab.-> adm.sys.	available yes no
2	adm.sys.-> AR	ID/ref.no. pair
3	AR -> datab.	request for SAK
	datab.-> AR	Encip.SAK and decipher key identification
4	MTX -> AR	request for triples
	AR -> MTX	triples
5	adm.sys.-> MTX	ID + relevant subscriber data

In the final solution, a visited MTX will use the MUP to ask a home MTX for RAND/SRES/B-KEY triples. While the MUP is not available, interim solutions on a national level are possible.

4. REQUIREMENTS FOR THE AUTHENTICATION REGISTER

4.1 General requirements

* The SAKs should be stored in the AR in a secure way. It shall in no way be possible to read out the SAKs from the AR.

* The AR will contain the keys for deciphering of SAKs. The AR should be able to store at least 1024 deciphering keys.
  It shall in no way be possible to read out these keys from the AR.

* The default number for the requested number of triples (RAND/SRES/BKEY) is set to [7]. It should be possible to adjust this number in the MTX on any value between 1 and 20.
  The MTX will request for such a set if a certain adjustable number, between 0 and 19, of unused triples is reached.

* An AR should be able to handle at least [300.000] IDs (which could be divided over a certain number of MTXs).

* In normal operation, an AR should be able to calculate and distribute at least [20] triples (RAND/SRES/BKEY) per day for each ID which could be stored in the AR.

4.2 Requirements Administration - AR communication

4.2.1 Requirements in case of option 1 (chapter 3).

* The administrative system sends pairs consisting of an ID, an enciphered SAK and decipher key identification to the AR.

* All communication concerning SAKs and decipher keys for SAKs should be protected.

4.2.2 Requirements in case of option 2 (chapter 3).

* The administrative system sends pairs consisting of an ID and a reference number to the AR.

* The AR sends the reference number to the national database as a direct request for the enciphered SAK and the identification of the decipher key.

* All communication concerning SAKs and decipher keys for SAKs should be protected.

4.3 Requirements AR - MTX communication

* The communication between the AR and an MTX will be protected. The administration determines the level and method of protection.

* The communication protocol between an AR and an MTX will be standardized.

5. REFLECTIONS ON THE IMPLEMENTATION OF AN AUTHENTICATION REGISTER

There are several ways to actually implement an authentication register.

The first method is to have one AR supporting all MTXs. In this case the AR, physically, is very close to the administrative system. This might be a good solution if only a limited number of MTXs exists in a country. Also the AR must be able to handle the management for all users. In this solution management overhead for the administrations is relatively small.

A second method is to give each MTX its own AR. In this case the AR, physically, is very close to the MTX. An advantage of this solution could be that the MTX and AR could be integrated and as one unit could be manufactured by MTX manufacturers. (This could e.g. simplify handling of error situations.)

The two solutions described above are extremes. Several solutions between these two extremes are possible, as illustrated in figure 1.

6. SOME FIGURES

This chapter gives some figures with respect to the authentication register and the MTX. The first paragraph is dedicated to the AR and the second to the MTX.
The figures are based on estimates for the GSM system.

6.1 Figures with respect to the AR

The processing power needed for the AR depends on several variables. For modelling purposes, several assumptions have to be made:

- total number of subscribers which the AR has to service: n = 300000
- subscriber identity size: IDsize = 4 bytes
- communication protocol overhead: overhead = 40 bytes
- number of authentications per subscriber per day: call-setups = 6
- table size in MTX per subscriber: tablesize = 10 entries
- triplet length: 13 bytes

These assumptions lead to the following formula's:

- Request: overhead + IDsize = 44 bytes
- Answer: overhead + tripletlength*tablesize + IDsize = 174 bytes

This implies that on every request for a new table a total of 218 bytes have to be transferred between the MTX and the AR. Since the number of authentications per subscriber per day is 6, and the number of table entries is 10, there is a need for a new table once a day for every subscriber. This covers most of the needed tables, only for subscribers which make more than 6 calls a day, an extra table is needed.
This implies a total of n*218 = 65 Mbytes per day. Most of the traffic will be during working hours (8 hours per day). During these 8 hours, this leads to a data flow of:

$$(65{,}000{,}000 * 8)/(3{,}600 * 8) = 18000 \text{ bps}$$

A new table per subscriber per day implies that the AR has to calculate the algorithm (n*tablesize) times a day. Again these calculations will be concentrated during working hours. The maximum time available for the algorithm therefore is:

$$(8*3600)/(300000*10) = 0.01 \text{ sec.}$$

6.2 Figures with respect to the MTX

The MTX must be able to store the table of triples in its memory. The memory space needed for this storage can be calculated with the following formula:

$$X = (IDsize + (tripletsize * tablesize))n$$

X = number of bytes needed
IDsize = number of ID bytes
tripletsize = number of bytes needed to store a triplet in MTX
tablesize = number of entries in the MTX's table
n = number of subscribers at the MTX

Example: $X = (4 + (9 * 10))65000 = 6$ Mbytes.

DRAFT Addendum to NMT Doc 4 (450) 1990-05-09
Revised 1990-09-06

DRAFT ADDENDUM TO NMT Doc. 4 1981

Technical specification for the base station equipment.

Annex 1: Draft specification for high rate data channel in NMT-system 1990-07-23 (enclosed).

Annex 2: Draft specification of the interface between the BS and the SSE 1990-08-07 (enclosed).

Annex 3: Compander (included).

Annex 4: Interleave channels (included).

Paragraph	Page	
1.3.8	16	Replace the paragraph with:

Safety requirements

The equipment shall fulfil the relevant requirements in IEC Publication 215 Third edition, 1987 "Safety requirements for radio transmitting equipment" and relevant requirements in IEC Publication 65 "Safety requirements for mains operated electronic and related apparatus for household and similar general use".

Regarding IEC Publication 215, following items have to be fulfilled due to national regulation:

DANGEROUS MATERIALS, paragraph 23.

When dangerous materials, such as beryllium, are used in the manufacturing of components, full instruction for handling, storage and disposal of such components shall be given in the equipment handbook, together with a note explaining the hazards associated with the material contained in the component.

The manufacturer shall state that cadmium is not used in solder alloys, as coloring agents, as stabilizers or in surface treatment. Any other use of cadmium in any form in the equipment must be declared.

The use of polychlorobiphenyl in any form in teh equipment is prohibited.

1.3.9	16	Add to the paragraph:

Maximum current drain at power start-up and the angle of phase difference for each input terminal shall be specified by the manufacturer.

The manufacturer shall state the total power consumption for a cabinet with 8 channels and for a full cabinet, if it consists of more than 8 channels.

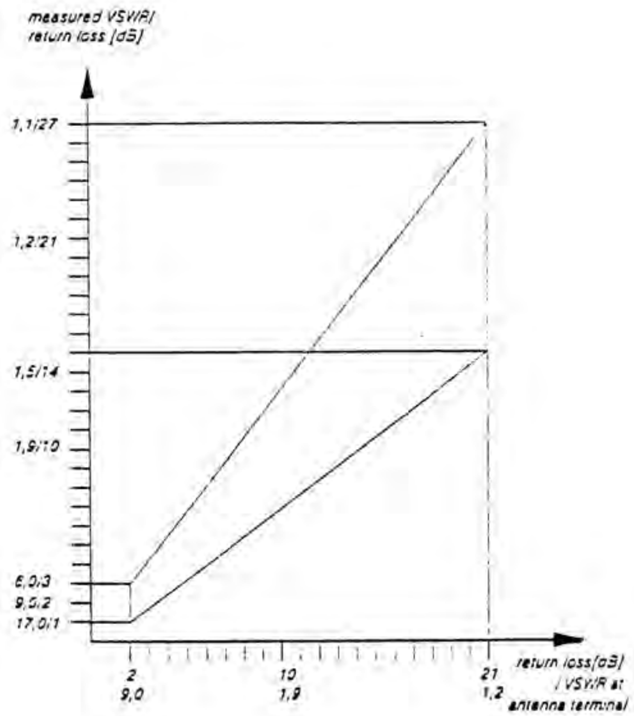
Paragraph	Page	
		Change in paragraph: - Nominal mains voltage is 230V, 50 Hz.
1.3.10	9	Replace second section, beginning with "The equipment shall ..." with: The equipment shall be clearly marked with the following: - The name of the manufacturer - The name of the unit - The revision of the unit - The serialnumber - Space to mark Status/modifications - The bar code. Add last in paragraph: The bar code shall be of type 39 or possibly 49. The bar code information must include the following: - The name of the Manufacturer - The name of the Unit - The serialnumber It is preferred that the bar code label is placed on the front of the unit. The unique bar code shall also be placed on the package easily reached for personnel at stores.
1.3.12	16	Revised paragraph Construction - Cabinet and equipment It is preferred that the base station equipment is built to fit into a cabinet with standard 490 mm (19") rack mounting. The maximum dimension of the cabinet shall be: 2200 mm (height), 600 mm (wide) and 600 mm (depth). Preferable heigth/depth of the cabinet is 2000 mm/300 mm respectively.

Paragraph	Page	
		The cabinet shall be designed in such a way so that the floor space are minimized. It shall be possible to mount the cabinets back-to-back or against the wall, i.e. no access to the backside of the cabinet is required. Preferable weigth of the cabinet is 40 kg or less.
		It shall be possible to install at least a complete 8-channel basestation with high power including transmitter combiner in one cabinet. Preferable is 16 channel.
		No unit, except the cabinet, shall be heavier than one person can handle. Total floor load of cabinet including equipment shall be maximum 2000 kg/square meter.
		The cabinet and equipment shall be designed in such a way so that the power consumption are minimized.
		The maintainability of the complete basestation equipment shall be optimized.
		Based on the manufactures philosophy regarding maintainability and reliability, other optimized solutions for floor space, weight, maintenance and power consumption may be proposed.
		- Cabling in cabinet and equipment.
		The cabling, used in the cabinet and equipment shall be of flame retardant halogen free calbe. Requirements and tests for the cables, see clause 1.3.13.9.
1.3.13.9	19	New paragraph
		Flame retardant halogen free cable.
		The tests shall be carried out and fulfil following requirements:
		FLAME RETARDANCY
		The test shall be carried out according to the IEC 332 Publication, Tests On Cables· Under Fire Conditions.

Paragraph	Page	
		Part 1 in this publication specifies a test for the flame propagation characteristics of a single vertical insulated wire or cable and part 3 a test on bunched wires and cables.
		LOW SMOKE PRODUCTION
		The test shall be carried out according to the new IEC Publication which will be issued. The test is a measurement of smoke density of electric cables burning under defined conditions. The specification (draft IEC 178) is worked out by Working Group 12 (WG 12) in the Technical Committee (TC 20).
		CORROSIVENESS OF COMBUSTION GASES
		The test shall be carried out according to following publications:
		- IEC Publication 754-1 for determination of amount of halogen acid gas evolved during the combustion of polymeric materials taken from cables.
		- German standard VDE 0472 Part 813 for determination of not only halogens, but oxides for phosphorus, sulphur, nitrogen as well as strong organic acids.
1.3.15	20	Change first section in paragraph to:
		Acoustic noise shall be measured according to ISO 6081 (which includes ISO 3743). The emitted sound power shall not exceed 60 dB (A) relative to 1 pW.
3.1.13	31	Correction regarding test features
		Replace the last section with:
		Furthermore a fault alarm (two levels) shall be given to the control unit at unallowable low reflection attenuation at the TX-antenna terminal of the radio cabinet (antenna fault). The settings for antenna fault alarms shall be adjustable between reflection attenuation 21,0 dB (VSWR 1,2) and 2,0 dB (VSWR 8,0).

It shall be possible to suppress the fault level 1 and level 2 alarms independently.
The reflection attenuation alarm level shall not vary more than ± 1,0 dB from the setting level within the transmitter frequency band.

The measuring accuracy shall be within the limits defined in the figure below with antenna output power 0,3 W or higher. The TX-antenna supervising equipment shall not malfunction with any capable output power levels.



3.2.16 New paragraph

RX-antenna supervision

The base station shall be provided with instruments for supervision of RX-antenna refelction attenuation.

Furthermore fault alarm (two levels) shall be given to the control unit at unallowable low reflection attenuation at the RX-antenna.

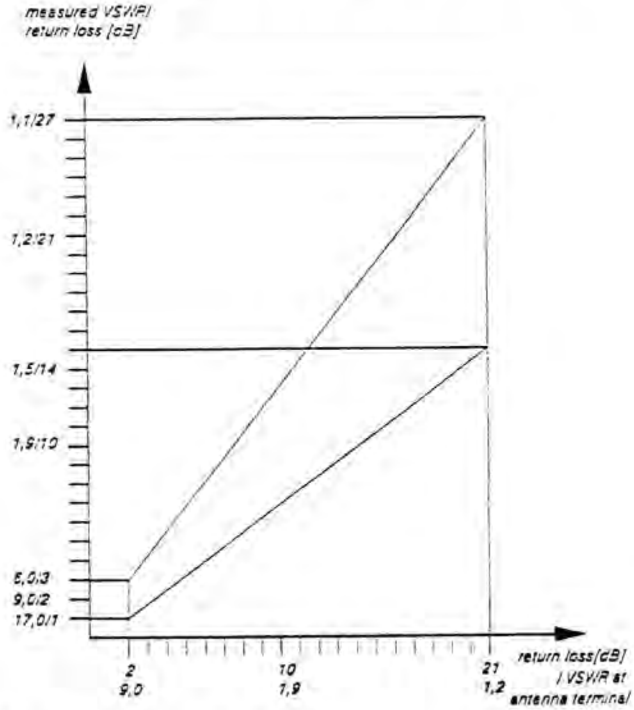
Paragraph Page

It shall be possible to suppress the fault level 1 and level 2 alarms independently. The settings for antenna fault alarms shall be adjustable between reflection attenuation 21,0 dB (VSWR 1,2) and 2,0 dB (VSWR 8,0). The measuring accuracy shall be within the limits defined in the figure below.

The reflection attenuation level shall not vary more than ± 1.0 dB from setting level within the receiver frequency band.

The RX-antenna supervising function shall be done automatically at least once/every hour. This test shall not interfere the normal operation of BS. In every case RX-antenna fault shall be indicated by RX-antenna alarm.

In case of diversity both RX-antennas shall be supervised.



4.23 57 New paragraph

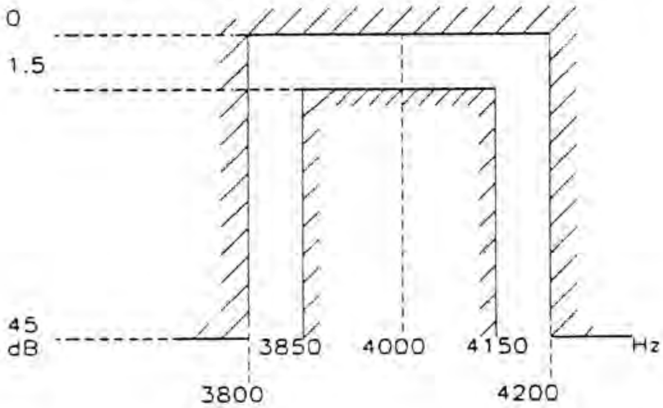
INTERFERENCE IN THE ϕ-SIGNAL FREQUENCY BAND

4.23.1 Definition

The interference level is the ratio, expressed in dB, of the level of unwanted components of the output signal, caused by the presence of a modulation signal as a result of nonlinearity in the transmitter, to the level of the wanted ϕ-signal measured at the output of the transmitter.

4.23.2 Method of measurement

The radio frequency signal produced by the transmitter is applied, by means of a suitable coupler, to a linear demodulator equipped with a filter according to the figure below, and measured with a RMS voltmeter. Alternatively an audio spectrum analyzer may be used.



The ϕ-signal is started corresponding to ± 0,3 kHz deviation and the level of the ϕ-signal at the output of the linear demodulator (including filter) is measured. Thereafter the sending of ϕ-signal is stopped.
An audio frequency signal of 1000 Hz is applied to the transmitter line input terminal.

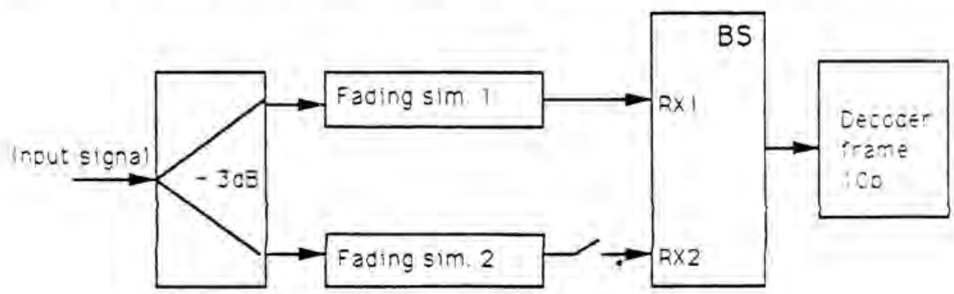
The level is adjusted so that a peak frequency deviation of the RF-carrier of ± 3,0 kHz is obtained. The input level shall be within the range given in paragraph 4.18.3.
Now the frequency is varied between 300 and 5000 Hz and the output level of the demodulator is measured.

The measurement is repeated with the level of the modulation input signal increased 6 dB.

4.23.3 Requirement

The interference level in the ϕ-signal frequency band shall not exceed -15 dB relative to the ϕ-signal level.

Paragraph	Page	
4.3.3	41	Repolace last sentence: (In Addendum dated 1988-04-15 replace the first two lines: "During the carrier ... . See clause 4.5.3") "During the carrier rise time and decay time specified in clause 4.5.3 the follwoing requirement applies." During the carrier rise time the frequency error shall be less than +/- 2,5 kHz. One framelength (138 ms) after the end of frame 20 A(14 or 15) the error shall be less than +/- 1,0 kHz. During the carrier decay time the frequency error shall be less than 1,0 kHz."
5.26	74	Replace paragraph 5.26 with: DIVERSITY (OPTION)
5.26.1		Definition The diversity gain is verified by checking that the frame reception probability is not degraded when the diversity is introduced at the same time as the input signal strength level is lowered.
5.26.2		Method of measurement A carrier with a nominal frequency of a BS receiver shall be applied to the radio cabinet antenna inputs via a divider and two Rayleigh fading simulators. The input signal shall be modulated with a continuous stream of frame 10b (see para 2.2.4.2). For each measurement 1000 frames shall be sent.



The LF signal at the line output of the receiver shall be analyzed via the demodulator (see para 4.6.1 NMT-doc 450-1) and a decoder. The received frames are corrected if necessary and possible, according to specification in Doc 450-1.
The fraction of correct frames received (including the corrected frames) related to total number of sent frames is calculated and noted.
The measurement shall be performed for two cases.

- First one of the two simulators shall be connected to the antenna input of one of the receiver units. In this case the RMS level of the RF-signal at the input shall be 8 dB (1μV) E.M.F. (-105 dBm). This shall be done for both the receiver units, one at a time.

- Thereafter the two fading simulators shall be connected to one input terminal each. In this case the input RMS level shall be 3 dB (1μV) E.M.F. (-110 dBm) at both input terminals.

All the measurement shall be performed for fading speeds of 3, 50 and 100 km/h and the correlation between the fading simulators shall be 0,8.

The frame reception probabilities with one and two receivers connected are compared for each fading speed.

5.26.3 Requirement

For each fading speed the frame reception probability when two receivers (diversity) are used, may not be lower than in any of the cases when one receiver is used

5.26.4 Other requirements for the diversity receiver.

For the diversity reception the measurements of para 5.1-5.25 and 5.27 are repeated by coupling the RF-signals to both receiver branches via 3 dB-coupler, at the two input terminals of the radio cabinet. The specified RF-signal levels shall be measured after the 3 dB coupler, at the two input terminals of the radio cabinet.

Paragraph	Page	
		When using the diversity equipment with only one RF-branch connected the ordinary receiver requirements shall be fulfilled. This shall be valid for both the RF-branches.
5.27	74	Replace section 5 (the frame 25 A(7)..) and 6 (The frame 25 A(8)...) of this paragraph with:
		Specification for signalling of handover request and RF-link disconnection is stated in paragraph 8.2.
5.28	74	Additions to paragraph
		INFLUENCE OF FADING
		This paragraph will no longer be a recommendation but a requirement.
5.28.1.2		Change paragraph:
		The alarm level 1_H and 1_L shall be set to values according to NMT doc 1 paragraph 4.3.3.10.2, e.g. 1_H=30 dBμV (-83 dBm) and 1_L=0 dBμV (-113 dBm). Therafter a start order e.g. frame 20 (A=14) is sent. Adjust the RF level until the frame 25 (A=7)/25 (A=8) is obtained with a succes rate of 80 % without fading, see up-doen method below. The frame must be received within the time limits in paragraph 5.27. This RMS level is noted. Before the next measurement the channelunit is reset by frame 20 (A=2).
		The measurement shall be repeated with the Raylight fading simulator set to 3, 50 and 100 km/h. The RMS level for 80 % succes rate are noted.
		For diversity reception the measurements shall be done for one as well as simultaneosly for both receiver branches. The RF-signal is coupled to both antenna input terminals of the radio cabinet via a 3 dB coupler and two fadingsimulators. The correlation between the simulators shall be 0,8.
		Measurement methode to be used.

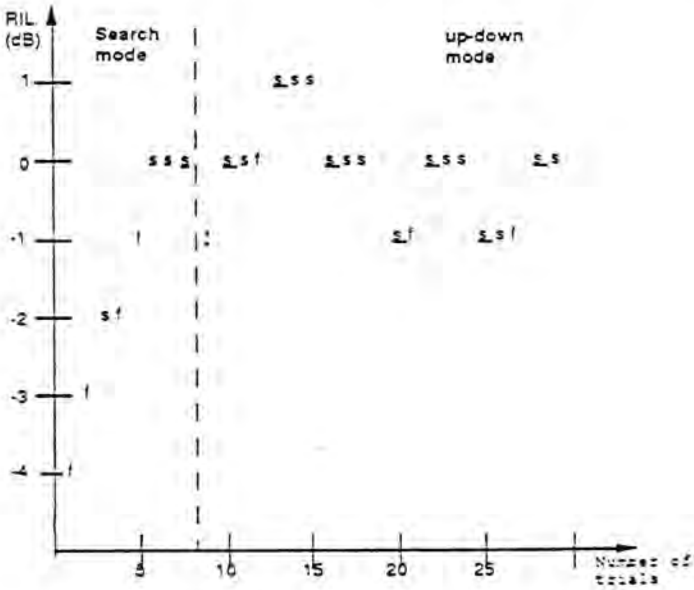
Up-down method

Measurement recommendation to be used in para 5.28.1.2 and 5.28.4.2.

The up-down method is an extension of the first multiple success method. Following the proceddure to establish the N:th consecutive success, an up-down method procedure is performed in order that the averaged RIL (Receiver Input Level) values approach more cosely the RIL_{wanted}. Essentially a fixed number of trials T are conducted and for each trial the input signal is increased by one step in the event of failure and reduced by one step in the event of N consecutive successes.

The estimate of RIL_{wanted} is determined by averaging the RIL values corresponding to the trials underlined in the figure. That is, the value of the first multiple success and the levels resulting from each step change only.

For the measurement N=3 and T=20 is applied.



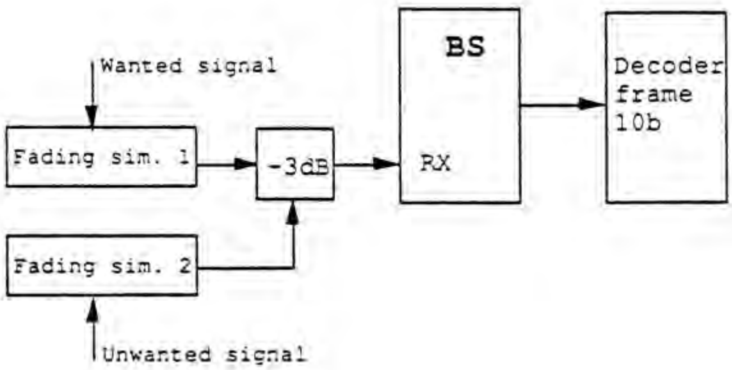
The figure illustrates the case for N=3 and T=20 and a step size of 1 dB.

Paragraph	Page	
5.28.2.2		Change the fading speeds in the second section to:
		...3, 50 and 100...
		Correct the last line in the second section to:
		...SR is adjusted to a level 1 dB above the RMS-level to SR without fading.
		Replace the last section of the paragraph with:
		For each case 1000 signal strength measurements results, R_{out}, shall be stored. Calculate mean value, upper and lower decile.
5.28.2.3		Replace the first section with:
		The difference in mean value of R_{out} with and without fading (fading margin) may not exceed 2 units.
5.28.3.1		Remove the first section, beginning with "The signal strength ...".
		Add the following section last in the paragraph:
		The calculated upper and lower decile from measurements in para 5.28.2.2 are used. The difference between the deciles are calculated.
5.28.3.2		Replace the paragraph with:
		Requirement

Fading speed (km/h)	3	50	100
Output deviation max dB	12	5	4

5.28.4.2		Insert first in the paragraph:
		Each measurement is started by adjusting the RF-level. Thereafter a start order is sent e.g. frame 20 (A=14).
		If frame 25 (A=7)/25 (A=8) is received within the specified time limits in para 8.1.5.2, the response is positive.

Paragraph	Page	
		Before the next measurement the equipment is reset by frame 20 (A=2). Other method giving equal result may be used.
		Add to the second sentence in the second section:
		... success rate of 80% without fading, see paragraph 5.28.1.2.
		Replace the fading speeds in the third section with:
		...3, 50 and 100...
5.29	74	New paragraph
		CO-CHANNEL REJECTION UNDER INFLUENCE OF FADING.
5.29.1		Method of measurement.
		A wanted and an unwanted signal shall be applied to the receiver antenna input terminal of the radio cabinet through two independent Rayleigh fading simulators via a combining network , see figure.



Paragraph	Page	
		The wanted signal shall be modulated with a continuous stream of frame 10b (see para 2.2.4.2). The unwanted signal shall be modulated (see para 2.2.4.2) with continuous pseudo-random bitstream of the 511 bits defined in CCITT Recommendation V.52. For each measurement 1000 frames shall be sent. The LF signal at the line output of the receiver shall be analyzed via the demodulator (see para 4.6.1 in Doc-1) and decoder. The received frames are corrected if necessary and possible, according to specification in Doc 450-1. The frame reception probability of the wanted signal shall be measured as the fraction of correct frames 10b received (including the corrected frames) related to the total number of sent frames. The RMS-level of the wanted signal shall be adjusted to 20 dB (1 μV) E.M.F. (-93 dBm) and the level of the unwanted signal shall be adjusted until a frame reception probability of 95% is obtained. The measurement shall be made for the speed of 50 km/h and the corresponding level of the unwanted signal is noted (see para 2.2.5) The measurements shall be made with an unwanted signal at the nominal frequency of the receiver.
5.29.2		Requirement CO-channel interference: RMS-level of the unwanted signal shall not be less than 0 dB (1μV) E.M.F. (-113 dBm).
7.2.3	77	Change of range. Change the upper and lower level in the figure to: upper: 63±6 dB (1μV) E.M.F. (-50 ± 6 dBm) lower: 0±3 dB (1μv) E.M.F. (-113 ± 3 dBm) Replace first sentence under figure with: All values below 0±3 dB (1μv) E.M.F. (-113 ± 3 dBm) shall be sent as 0 (heaxadecimal value) and

Paragraph Page

all values above 63±6 dB (1µV) E.M.F. (-50 ± 6 dBm) shall be sent as 3F (heaxadecimal value) to the MTX.

7.2.4 77 RX used as Signal strength receiver.

If a fault occurs in the SR it shall be possible to remotely from MTX to order any of the receivers (RX) to operate as an SR. When the CU/RX receives a signalstrength measurement order frame 21.b or 21.c with N1N2N3 equal to FFF the RX shall start acting as an SR, and return the measurement result in frame 26. In other respects the transformed channel unit CU/RX/TX shall be idled corresponding to frame 20A (0). If the same CU/RX/TX again receives another activation order from the MTX it shall operate as an ordinary channel unit.

It is also allowed to utilize the RX as SR when receiving signalstrength measurement orders with N1N2N3 equal to any ordinary channel number. Thus there are no requirement for interconnection between CU and the ordinary SU/SR in this case.

In this case the Channel unit except the RX shall maintain the status before the measurement order, and will operate as idle, free marked traffic channel or traffic channel actually used. The RX shall have returned to the channel, as ordered in the latest received frame 20A (14) or 20A (15), within 277 ms (2 frames) after the end of the last signalstrength measurement order.

8.1.3.1 79 Replace the whole paragraph with:

NMT alarms

When a fault occurs, the CU shall send fault alarm once to MTX (one frame 28) at:

- TX-antenna fault, when the reflection attenuation measured at the TX-antenna terminal of the radio cabinet exceeds a preset level. There shall be two levels and they shall be adjustable within the reflection attenuation range 21,0 dB (VSWR 1,2) and 2,0 dB (VSWR 8,0). It shall be possible to suppress the fault level 1 and level 2 alarms independently The alarm interface between CU and transmitter combiner is specified in paragraph 3.1.14.

Paragraph Page

Note 1. See clause 3.1.13 "Test features".

Note 2. Fault alarm shall be sent on all affected channels.

- Combiner alarm level 1 when the reflection attenuation at the transmitter combiner filter exceeds a preset level 3,0 dB ± 1 dB. The fault alarm shall be sent only on the corresponding channel.

  Alternative method:

  Combiner alarm level 1 when the attenuation of the combiner filter exceeds a preset level (decreased output power from the combiner filter relative to TX output power). Level shall be adjustable within the attenuation range 3,0 dB - 15,0 dB. The fault alarm shall be sent only on the corresponding channel.

- Combiner alarm level 2 when the reflection attenuation at the transmitter output exceeds a preset level 4,0 dB. The fault alarm shall be sent only on the corresponding channel.

- RX-antenna fault, when the reflection attenuation at the RX-antenna terminal of the radio cabinet exceeds a preset level. There shall be two levels and they shall be adjustable within the refelction attenuation range 21,0 dB and 2,0 dB. It shall be possible to suppress the fault level 1 and level 2 alarms independently.

  In case of diversity both RX-antennas shall be supervised.

Note 1. See clause 3.2.16 "RX-antenna supervision".

- Transmitter fault level 1, when the carrier output power is below a preset level 1. The level 1 shall be adjustable within the range (-15 dB, -3 dB) relative to nominal output power.

- Transmitter fault level 2, inter alia when:

- the carrier output level is below a preset level 2. The level 2 shall be adjustable within the range (-15 dB, -3 dB) relative to nominal output power.

- the synthesized frequency is unlocked (not during channel switching time and power start up period).

- any of DC-voltages is below a preset level.

- Deviation fault. This alarm is sent if the modulating signal level in the TX-modulation has decreased below a preset level (relative to the incoming signal). The incoming signal is detected by the following criterea:
  TX activated and nodeviation for at least 5 of the last 10 frames sent from the MTX. The frames detected shall contains correct $N_1N_2N_3$.

- Receiver fault, inter alia when:

  - the synthesized frequency is unlocked (not during channel switching time and power start up period).

  - any of DC-voltages is below a preset level.

- Redundant master oscillator fault. This alarm is sent if the frequency stability requirements are still fulfilled. In other case transmitter fault alarm level 2 and RX-alarm are sent from all channels connected to the master oscillator.

- Cooling fan fault. This alarm shall be sent only on affected channels.

- Power supply fault, inter alia when any of the output voltages are below a preset level.

Note 1. The fault alarm shall be sent on all channels which are connected to this power supply.

Note 2. Power supply fault shall not cause any other alarms.

- Redundant power supply fault. This alarm is sent if full operation of channels connected to this power supply is possible.

Paragraph Page

- Receiver multicoupler fault, inter alia when power failure or amplifier failure occurs.

Note 1. See clause 3.2.14

Note 2. Fault alarm shall be sent on all channels, even in other cabinets which are connected to this receiver multicoupler.

- Redundant amplifier fault in the receiver multicoupler.

- Temperature fault, inter alia when the temperature in transmitter is above preset level.

- CU fault, if possible.

Note See clause 8.1.6

- Supervisory signal test loop fault alarm according to paragraph 8.1.5.3.

- SU/SR faults, see chapter 9.

- Channel unit fault level 2. (OPTION)

  This alarm is sent in case of integrated channel unit (TX, RX and CU in same unit) when one (or more) of the following alarms occurs:

  - TX 2 alarm
  - RX-alarm
  - CU-alarm
  - ϕ-loop-alarm
  - Deviation alarm

  In this case the alarm register (below) is a requirement.

- Alarm register. (OPTION)

  The channel unit shall have an alarm register where the detailed information of at least ten latest alarms can be found locally or remotely via modem and PC. It shall be possible to erase this alarm register with local or remote control.
  If channel unit fault option is used this alarm register function is a requirement.

Paragraph	Page	
		- In case of diversity (option) following alarms shall be sent: - If a fault occure in one of the receiver multicouplers the "redundant amplifier fault in the receiver multicoupler" shall be sent on all channels even in other cabinets which are connected to this receiver multicoupler. - If a fault occure in one of the branches in the receiver the "diversity alarm" shall be sent only on the corresponding channel.
8.1.3.2	80	Correction regarding house alarms Add new alarm - Environment temperature alarm.
8.1.7	83	Correction regarding local control Add new sentence: It shall be possible to set channels (one or all at the same time) into preblock mode, i.e. channels where traffic occurs are automatically local-blocked when the channel is released. CC, AC, TC and idle channels shall be local-blocked immediately. Preblock state shall be indicated i.e. with flashing (repeatedly) channel number display at the channel unit.
8.1.10	84	Clarification of measurement of diversity with multicoupler included. Add between 15:th and 16:th line. In case of diversity the two receiverbranches shall be tested separately, but in sequence for each selftest order. The measurement period can be up to 7 sec. Add to the section starting with "If the selftest ...": "... at the BS, but not sent to the MTX."

Paragraph	Page	
		Add after the last sentence in the paragraph: The multicoupler shall be included in the measurement. Add new sentence. Rx-antenna supervision may be a part of the selftest.
9.1.3	87	New paragraph <u>RX used as SR.</u> See paragraph 7.2.4. If the RX are used as SR also for signalstrength measurement orders sent from MTX on idle, free marked traffic channel and traffic channel actually used there are no requirement for interconnection between the CU's and the ordinary SU/SR. In this case the ordinary SU/SR will communicate with MTX only via the dedicated data line for signalstrength measurements.
11	88	New paragraph (OPTION) <u>SUPERVISION OF FREEMARKED CC AND TC</u> The BS shall supervise that there always are at least one freemarked CC and one TC at the actual basestation site. The supervision shall include up to at least 40 channels. If dedicated frequency bands for CC and AC/TC are used, the supervision shall normally only include the channels inside the actual bands. This setting may be done locally and/or remote by use of the channel information and the additional information given in the frames from the MTX to the MS. If freemarked CC or AC/TC are not found inside the dedicated frequency band, the whole BASIC band shall be scanned before any alarm is sent to the MTX.

If freemarked CC-indication or related signalling sent from the MTX (frame 1a, 1b, 2a, 2b, 2c,) are not detected at any of the channels of the BS for more than 90 % of the last time "t", the BS shall send one alarm to the MTX (frame 28, "Missing CC-indication"). The time "t" shall be setable in steps of 30 seconds starting from 30 secs. to 5 minutes.

If freemarked AC- or TC-indication or related signalling sent from the MTX (frame 4, 4b, 3a, 3b, 3c, 3d) can not be detected according the limits given above the BS shall send one alarm to the MTX (frame 28, "Missing AC- or TC-indication").

The alarm shall be sent on two channels with respect to redundancy.

If the BS again detects the actual frames for at least 90 % of the time "t" the BS shall send frame 28, "Missing CC-indication ceasing" and "Missing AC/TC-indication ceasing" at the same channels.

The alarm may be sent again after an alarm ceasing with out first initiating alarm reset.

The alarm(s) shall not be indicated on the base station.

The supervision of the actual channel shall be supressed by initiating "Local blocking", and activated by "Local deblocking".
The supervision shall be supressed when receiving the frame 22V1(7) from the MTX. The supression shall be cancelled when receiving the frame 22V1(10).

The supervision may be implemented as a S/W-solution in the basestations. If so, it is important that supervision of the actual transmitters output power and modulation is included.

The supervision of freemarked CC and TC/AC may also be implemented in such a way that it could be added to older BS-equipment which do not have this function (i.e. by use of RF-monitoring and the external alarm inputs).

Paragraph	Page	
12	88	New paragraph (OPTION)

DIGITAL INTERFACE FOR BASE STATIONS.

The Base Station may as an option include a 2048 kbit/s PCM interface equipment.

In this case the Base Station shall be equipped with a PCM interface to multiplex the audio output and inputs in the Base Station to a 2.048 Mbit/s HDB 3 code (High Density Bipolar, 3. order) line.

The maximum of speech channels which shall be connected to the 2048 kbit/s line is 30.

The PCM interface equipment shall fulfil the following CCITT (blue book) recommendations :

- G.703 Physical/Electrical characteristics of hierarchical digital interface
- G.704 Functional characteristics of interface associated with networks nodes (basic frame structure)
- G.706 Frame synchronization etc.
- G.711 Pulse code modulation (PCM) of voice frequencies
- G.712 Performance characteristics of PCM channel between 4-wire interface at voice frequencies
- G.713 Performance characteristics of PCM chann between 2-wire interface at voice frequencies
- G.714 Separate characteristics of a 4-wire interface of the transmit and receive directions
- G.732 Characteristics of primary PCM multiplex equipment operating at 2048 kbit/s
- G.735 Characteristics of primary PCM multiplex equipment operating at 2048 kbit/s and offering digital access at 384 kbit/s and/or synchronous digital access at 64 kbit/s

Paragraph Page

- G.823 The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

It shall be possible to select the time slots for each channel in the 2048 kbit/s signal.

The equipment shall include a digital 2048 kbit/s through connection (multidrop) so that unused 64 kbit/s channels at the 2048 kbit/s line can also be distributed to other Base Station and/or system.

The PCM interface shall be able to transfer mains break-down alarm in the case where mains break down occurs.

The PCM interface shall be equipped with an internal alarmindication.

13 88 New paragraph (OPTION)

REMOTE CONTROL.

Remote control interface shall offer facilities for remote control of the Base Station.
The remote control interface is either directly connected to a PC via a V.24 interface or connected to a PC via a telephone modem.

With the remote control interface and IBM AT/XT PC or other compatible PC, it should be possible to control the Base Station.

On call establishment it shall be possible to identify the manufacturer and the communications protocol.

The remote control interface shall be fitted with some kind of protection to prevent unauthorized person from getting access to the Base Station. The method used shall be agreed by the operator.

As a minimum it shall be possible to carry out the same adjustments and measurements on the Base Station as it is possible in local control (see paragraph 8.1.7) and in service functions (see paragraph 8.1.9).

Paragraph Page

It shall be possible to have the type (designation) number,the serial number and software version over the V.24 interface (other item e.g. last day of warranty may also be included).

It shall be possible to change settings in the Base Station equipment.

It shall be possible to transfer measurement points from the equipment to the PC.

It shall be possible to connect several cells on the same position (site) to the same modem.

For communication through the switched telephone network the speed of the modem shall be at least 1200 baud.

If the Base Station is equipped with a digital interface (see paragraph 12), it shall also be possible to transfer the remote control commu-nication through this. It shall be possible to place the communication in an arbitrary time slot.

14 88 New paragraph (OPTION).

INTRODUCTION TO ANNEX 1 AND 2 TO NMT DOC 900-4/ DOC 4(450).

14.1 ANNEX 1.

A new unit called SLUX (Switching Unit External) will be implemented in the NMT-system. The aim is to increased capacity and quality in the system. This unit will require more information from the BS than today. Signalling from/to the BS will therefore be increased and the capacity of the data channel implemented in the NMT-system today, will not be enough.

A high rate Data Channel, HDC, between the MTX/SLUX at one end and the BS/SSE on the other is therefore specified in annex 1. The messages that the BS shall send/receive via this interface are also specified in annex 1.

Paragraph Page

The High rate Data Channel, when connected, is a replacement to the normal data channel (DC). The control message to the BS for connection/disconnection of the HDC is sent via the DC/HDC. This means that each BS must have the functionality to interface both the normal DC and the HDC, but not simultaneously. The DC shall function as backup to HDC. When the HDC is connected the messages "Handover request" shall be sent via the HDC.

The BS shall not send any messages via the interface between the SSE and the BS until the BS receives a message from OMC that the SSE is connected (specified in annex 1 paragraph 6.1.1.1). If the BS receives the message from OMC that the SSE is disconnected, the BS shall stop the signalling to the SSE.

14.2 ANNEX 2.

SLUX will also require a supervisory scanning equipment, SSE, which will be specified separately. The specification will include the functionality of scanning a number of channels in the system and detect the ϕ-signal. The SSE shall be physically installed at the BS. The interface between the SSE and the BS is specified in annex 2. The messages that the BS shall send/receive via this interface are also specified in annex 2.

15 New paragraph (OPTION)

The method for signal strength measurement and ϕ-signal detection described in paragraph 9.1.1 and 7 shall be replaced by this chapter.

SIGNAL STRENGTH MEASUREMENT

The mean value of the signal strength shall be measured for a time period of 300 ms and shall be quantified in 64 levels.
All the values below 0±3 dB (1 μV) E.M.F. (-113 ± 3 dBm) shall be coded as 0000 0000 ($R_1(0)R_2(0)$) and all the values above 63 ± 6 dB (1 μV) E.M.F. (-50 ± 6 dBm) shall be coded as 0011 1111 ($R_1(3)R_2(15)$).

Paragraph Page

The signal strength output shall fulfil the specification stated in para 7.2.3, both with and without fading. The signal strength measuring receiver shall fulfil the requirements in paragraph 5 "Receiver".

The base station receives the measuring order (frame 21b or 21c) from MTX via idle traffic channel, actual channel or data channel.
The signal strength measurement result (frame 26) shall then be sent from the base station equipment to MTX within 552 ms from the reception of measurement order.

Signal strength measurement results shall be sent to MTX via the same connection as the corresponding signal strength measurement order.

When the measuring order is sent via idle traffic channel or the data channel the measurement orders may be given in a continous stream of frames 21b or 21c (one order/ 138 ms).

In this case the measurement results shall be sent to the MTX as a continious stream of frames 26. There shall be no space between the frames and the result must be sent in the same order as the corresponding measurement orders have come.

Otherwise, if the measuring order is sent via the HDC, there may be up to 4 orders/138 ms. The results must be sent in the same order as the corresponding measurement orders have come.
The received ϕ-signal frequency looped by the actual MS shall be detected. If the ϕ-signal frequency number is incorrect the measured signal strength shall be sent and the information of the incorrect ϕ-signal (f_ϕ=0101) shall also be sent. If no ϕ-signal number is given in the frame 21b and 21c the f_ϕ=0000 and the measured result R_1R_2 shall be sent to MTX.

Paragraph	Page	
16	88	New paragraph (OPTION)

COMBINER, ALTERNATIVE EQUIPMENT

Possible to select between 16.1 and 16.2 or 16.3.

16.1 ACTIVE COMBINER

Paragraph 3 is valid with the following additions:

In case of an integrated and/or active combiner para 3.1.7 shall be exchanged with the specification according to para 4.4.3 "Carrier power".

The attenuation specified in para 3.1.12 shall be measured between any amplifier output and the combiner output.
Fault alarms defined in 3.1.13 (e.g. power failure) shall be given to the CU of each affected channel.

16.2 AUTOMATIC TUNED COMBINER (fast version)

16.2.1 General requirements from the NMT recommendations

The requirements stated in paragraph 3 shall be fulfilled by the equipment.

The equipment shall comply with the reliability requirement specified in para 1.3.6. It will belong to group B equipment, and the MTBF shall be based on a retuning occurrance of 60 times per hour.

In order to be able to replace 3 dB couplers, at connection of a number of transmitters in areas with small cell basestations, it is required that the power loss from any of the input terminals to toe output terminal, isolators included, does not exceed 5.5 dB at combining 16 transmitters at minimum, with a frequency separation of 125 kHz.

16.2.2 Power requirements

The equipment shall operate with correct tuned channels at input levels of the following range in to different segments.

(+15 dBm, +35 dBm) (+30 dBm, +50 dBm)

Input levels below [0 dBm, +20 dBm] respectively shall be treated as transmitter in off condition, at which the combiner resets according to timelimits given in the control unit. The segments will be choosen at installation.

16.2.3 Requirments for tuning time

The total time needed for tuning the transmitter and the combiner at start of the transmitter shall not exceed 138 ms, measured according to para 4.5.3. This time includes the carrier rise time at carrier on. At channel order to a randomly choose channel the power shall be applied to the antenna within one frame time after order from MTX, corresponding to one idle frame in the signalling.

16.2.4 Functions in the control unit

The combining equipment shall in normal operation have the possibility to tune to the actual frequency of the transmitter by the incoming RF-singal, or by control from the channel unit.

Following functions shall be fulfilled by control signals by every single cavity unit:

1. The cavity is immediately tuned outside the frequency band and will follow the transmitter to the new channel at carrier on.
2. Cavity is locked outside the frequency band as long as the control signal is active.
3. Cavity is locked to latest tuned channel, independant of TX carrier frequency.

[Frequency band 463,000 - 467,475].

When no control signal has been activated the cavity shall stay tuned to the last frequency a time T after TX carrier has been switched of. The time T shall be programmable in steps in the interval (10 min, 24 h).

This means that it can be selected for how long a cavity stays tuned at the frequency, before another cavity can be tuned to the same frequency without any interference. The position of the combiner outside frequency band, below or above will be choosen at installation.

16.2.5 Alarms

Alarm shall be given if improper operation occurs according to paragraph 3.1.14. (Combiner larm)

Combiner alaram level 1 and 2 shall exist.

Alarm level 2 shall be sent when a major fault occurs. The alarm shall be sent on the corresponding channel.

16.2.6 Power supply

The combiner unit shall be supplied from all the power supplys in cabinet, which supplys the transmitters connected to the combiner. The combiner shall not loose its tuning at short mains interuptions.

16.3 AUTOMATIC TUNED COMBINER (slow version)

16.3.1 The requirements stated in paragraph 3 shall be fulfilled by the equipment except in:

- Case of integrated combiner then paragraph 3.1.7 shall be exchanged with the specification according to paragraph 4.4.3 "Carrier power".

16.3.2 See paragraph 16.2.2.

16.3.3 As paragraph 16.2.3. except for the tuning time which is 5 s instead of 138 ms.

16.3.4 See paragraph 16.2.4.

16.3.5 See paragraph 16.2.5.

16.3.6 See paragraph 16.2.6.

Paragraph Page

ANNEX 3 COMPANDER (OPTION)

4.25 57 New paragraph.

Add new paragraph as follows:

SYLLABIC COMPRESSOR REQUIREMENTS (OPTION)

The base station shall be equipped with syllabic compandors. (Reference: Recommendation G.162, CCITT VIIth Plenary Assembly, Geneva, 10-21 November 1980, Yellow Book, Vol. III. 1). The compression ratio shall be 2:1. The compressor part shall be located between the line input terminal at the control unit (CU) and the pre-emphasis network.

The companders hsall be activated by the CU when the parameter d is frame 20A (3) equals F (see para 4.3.3.6 doc -1) or locally at the BS.

The compander shall be deactivated (by passed when the ϕ-signal is stopped as ordered from MTX (frame 20A (0) or A(12)) or locally at the basestation. It shall also be able to deactivate the compander by setting the parameter d in frame 20A (3) to 0 (see para 4.3.3.6 doc -1). For measurement purposes in chapter 4 and 5 it shall be possible to activate/ deact-ivate the compandors irrespective of whether the ϕ-signal is started or not.

The measurements described in this paragraph shall be performed by using a measuring set-up consisting of four parts (see figure below).

- Coupler/attenuator
- Deviation meter (modulation analyser)
- 6 dB/octave de-emphasis network

The expander part of a 2:1 syllabic compander with a nominal attack time of 3,0 msec and a nominal recovery time of 13,5 msec. The compandor shall meet the requirements in CCITT Rec. G.162.

However, the compandor parameters shall be calibrated to an accuracy in line with laboratory instruments. The expander part shall be based on the integrated circuit NE570.
In paragraph 4.25 the term "reference tone" shall mean a tone, transmitted through the system including the compressor, with a frequency of 1000 Hz and producing a peak frequency deviation of ± 3,0 kHz. The term "reference level" (unaffected level) shall, at any point, mean the level of the test tone at that point. The φ-signal shall not be started during the measurements.

When the compressor is bypassed the normal test modulation of ± 3,0 kHz deviation shall correspond to an audio frequency level of the 1000 Hz tone at the line input terminal 2,2 dB below the reference level. In this way the FFSK-signalling with an audio level of -4,4 dB at the input terminal relative to the reference level shall give the same deviation irrespective of whether the compressor is activated or not.

4.25.1 Compression linearity

4.25.1.1 Definition

The compression linearity is the deviation from the linear relation between the input amplitude of the compressor and the output amplitude of an ideal mobile station.

4.25.1.2 Method of measurement

A test signal with a frequency of 1000 Hz shall be applied to the line input terminal. Its amplitude shall be adjusted to the reference level. The ratio D0 in dB between the amplitude of the input test signal and the amplitude at Point 1 of the measuring set-up in figure above shall be measured. The input amplitude shall subsequently be varied from +3 dB to -55 dB relative to its initial value. The ratio D between the input and the output amplitudes shall be recorded as a function of input amplitude.

Paragraph Page

Note The compression ratio of the compressor of the base station is 2:1. This compression ratio is compensated by the expansion ratio of 1:2 of the expander of the measuring set-up.

4.25.1.3 Requirements

The maximum difference between D and D0 shall be ± 1,0 dB.

4.25.2 Transient response of the compressor

4.25.2.1 Definition

The definition of transient response shall be as in CCITT Rec. G.162,clause 7.

4.25.2.2 Method of measurement

The transient response of the compressor shall be measured with a 12 dB step of a test signal of 2000 Hz applied to the line input terminal.

The high and low level of the signal shall be respectively -22 dB and -34 dB relative to the reference level.

The envelope of the signal at Point 1 of the measuring set-up shall be recorded for an upward step.

The procedure shall be repeated for a downward step.

Note The high and low level recommended in CCITT Rec. G.162, clause 7, are respectively -4 dB ... and -16 dB ... relative to the reference level. The values in this specification are chosen in order to avoid possible peak limiting in the radio path.

4.25.2.3 Requirements

The overshoot (positive or negative) shall be less than 20% of the final value.

Paragraph Page

4.25.3 Attack time and recovery time of the compressor

4.25.3.1 Definition

The definition of attack time and recovery time shall be as in CCITT Rec. G.162, clause 7.

4.25.3.2 Method of measurement

The attack time and recovery time of the compressor shall be measured with a 12 dB step of a test signal of 2000 Hz applied to the line input terminal. The high and low level of the signal shall be -22 dB and -34 dB relative to the reference level.

The envelope of the signal at Point 2 of the measuring set-up shall be recorded for an uppward step of the test signal. The attack time as defined in CCITT Rec. G.162, clause 7 shall be measured.

The procedure shall be repeated for a downward step. The recovery time as defined in CCITT Rec. G162, clause 7 shall be measured.

The measurement shall be repeated with the high and low level equal to -4 dB and -16 dB relative to the reference level.

4.25.3.3 Requirements

The attack time shall be 3,0 ± 1,0 msec. The recovery time shall be 13,5 ± 5,0 msec.

4.25.4 Harmonic distortion including compressor part

4.25.4.1 Definition

See paragraph 4.15.1.

4.25.4.2 Method of measurement

See paragraph 4.15.2.
The measurement shall be repeated with the compandor activated.

The harmonic distortion at Point 1 of the measuring set-up above shall be measured. At 300 Hz and 500 Hz modulation frequency the deviation shall be ± 2.0 kHz and ± 2,5 kHz respectively.

4.25.4.3 Requirement

The harmonic distortion factor shall not exceed 5%.

4.25.5 Transmission idle noise

4.25.5.1 Definition

The transmission idle noise is the psophometrically weighted noise r.m.s amplitude in dB at the output of the ideal mobile station relative to the r.m.s amplitude of the reference tone.

4.25.5.2 Method of measurement

The reference tone shall be applied to the line input terminal, and the reference level at Point 1 of the measuring set up shall be measured. The modulating signal shall be removed and the psophometrically weighted idle noise r.m.s at Point 1 of the measuring set-up shall be measured.

4.25.5.3 Requirement

The psophometrically weighted idle noise r.m.s amplitude shall not exceed -70 dB.

Paragraph	Page	
4.10.2	47	Clarification regarding Limiting characteristic of the modulator. In case the option "Syllabic compressor" is implemented the following measurement shall be performed: The level shall be adjusted so that the frequency deviation is ± 3,0 kHz. The level is then increased by 20 dB and the compandor shall be activated. The frequency deviation is again measured.
4.10.3	47	Correction regarding Limiting characteristic of the modulator. Requirements b) The frequency deviation shall be between ± 4,3 kHz and ± 4,7 kHz. Add new meaning to paragraph 4.10.3: "c) The frequency deviation shall be between ± 4,0 kHz and ± 4,7 kHz.
5.25	74	New paragraph.
	74	SYLLABIC EXPANDER REQUIREMENTS (OPTION) Se paragraph 4.25 regarding reference to CCITT Recommendation and the activating/deactivating of the compandors. The expander shall be located between the de-emphasis network and the line output terminal. The measurements described in this paragraph shall be performed by using a measuring set-up consisting of four parts (see figure below): - Coupler - The compressor part of a 2:1 syllabic compander with a nominal attack time of 3.0 msec and a nominal recovery time of 13.5 msec. The compandor shall meet the requirements in CCITT Rec.G.162. However, the compandor parameters shall be calibrated to an accuracy in line with laboratory instruments. The compressor part shall be based on the integrated circuit NE570.

Paragraph Page

- A 6 dB/octave pre-emphasis network.
- A linear modulator/radio frequency signal generator providing an FM-modulated radio frequency signal with a peak frequency deviation proportional to its input amplitude. The RF-level at the receiver input terminal shall be 60 dBμV.

In paragraph 5.26 the term "reference tone" shall mean a tone, transmitted through the system, with a frequency of 1000 Hz and producing a peak frequency deviation of ± 3,0 kHz. The term "reference level" (unafected level) shall, at any point, mean the level of the test tone at that point.

When the expander is bypassed the normal test modulation of ± 3,0 kHz deviation shall correspond to an audio frequency level of the 1000 Hz tone at the line output terminal of 2,2 dB below the reference level.

In this way an RF-signal modulated with the FFSK-signalling (4.2 kHz peak deviation, 1800 Hz tone) shall give the same audio frequency level at the line output terminal irrespective of whether the expander is activated or not.

5.25.1 Expansion linearity

5.25.1.1 Definition

The expansion linearity is the deviation from the linear relation between the input amplitude of an ideal mobile station and the output amplitude of the expander of the base station.

5.25.1.2 Method of measurement

A test signal with a frequency of 1000 Hz shall be applied to Point 1 of the measuring set-up in figure above. Its amplitude shall be adjusted to the reference level. The ratio D0 in dB between the amplitude of the input set signal and the amplitude of the signal at the line output terminal shall be measured. The input level shall subsequently be varied from + 3 dB to - 55 dB relative to its initial value. The ratio D between the input amplitude and the output amplitude shall be recorded as a function of input amplitude.

Note The expansion ratio of the expander of the base station is 1:2. This expansion ratio is compensated by the compression ratio of 2:1 of the compressor of the measuring ratio.

5.25.1.3 Requirements

The maximum differece between D and D0 shall be ± 1,0 dB.

5.25.2 Transient response of the expander

5.25.2.1 Definition

The definition of transient response shall be as in CCITT Rec.G.162, clause 7.

5.25.2.2 Method of measurement

The transient response of the expander shall be measured with a 12 dB step of a test tone of 2000 Hz applied to Point 1 of the measuring set-up. The high and low level of the signal shall be respectively -22 dB and -34 dB relative to the reference level.

The envelope of the signal at the line output terminal shall be recorded for an upward step.

The procedure shall be repeated for a downward step.

Note The high and low level recommended in CCITT Rec.G.162, clause 7 are respectively - 4 dB and -16 dB relative to the reference level. The values in this specification are chosen in order to avoid possible peak limiting in the radio path.

Paragraph   Page

5.25.2.3   Requirements

The overshoot (positive or negative) shall in both of the above cases be less thatn 20% of the final value.

5.25.3   Receive harmonic distortion

5.25.3.1   Definition

See paragraph 5.16.1.

5.25.3.2   Method of measurement

See paragraph 5.16.2.
The measurement shall be repeated with the compandor activated, and using the measuring set-up above. The harmonic distortion at the line output terminal shall be measured.

With 300 Hz and 500 Hz tone the frequency deviation shall be ± 2,0 kHz and ± 2,5 kHz respectively.

5.25.3.3   Requirement

The harmonic distortion factor shall not exceed 5%.

5.25.4   Receive idle noise

5.25.4.1   Definition

The receive idle noise is the psophometrically weighted noise r.m.s amplitude in dB at the line output terminal, when the modulating signal to the ideal mobile station is removed, relative to the r.m.s amplitude of the reference tone.

5.25.4.2   Method of measurement

The base station receiver shall be connected to the measuring set-up above and the ideal mobile station modulated with the reference tone. The

Paragraph Page

corresponding reference level at the line output terminal is measured. The modulating signal is then removed and the psophometrically weighted idle noice r.m.s at the line output terminal is measured.

5.25.4.3 Requirement

The psophmetrically weighted idle noise r.m.s amplitude shall not exceed -70 dB.

ANNEX 4. INTERLEAVE CHANNELS (OPTION)

In case of interleaved channels the following changes shall be done in the specifikation

1.3.2 Replace second section of the paragraph with:

The channel spacing is 25 kHz at the same basestation and the frequency separation beween the transmit and receive channels is 10 MHz. The equipment shall however be designed for use of interleaved channels i.e. channels with 12.5 kHz channel separation from the ordinary channels.

Channel No	TX-frequency (MHz)	RX-frequency (MHz)
1	463,0000	453,0000
2	463,0250	453,0250
.		
.		
.		
180	467,4750	457,4750

Interleaved channels:

201	463,0125	453,0125
202	463,0375	453,0375
.		
.		
379	467,4625	457,4625

4.1 Interleaved channels.

Add:

...., with the possibility to use interleaved channels separated 12.5 kHz from the ordinary channels.

Paragraph	Page	
4.2		Interleaved channels. Replace 180 channels with: .... 359 channels...
4.3		Frequency accuracy: The frequency error of the transmitter shall not exceed ± 250 Hz. This requirement includes the effect of aging for a period of one year. The amount of annual aging shall be stated by the manufacturer. This requirement shall be fulfilled also during the carrier rise time and decay time specified inclause 4.5.
5.1		Interleaved channels. Add: ...., with the possibility to use interleaved channels separated 12.5 kHz from the ordinary channels.
5.2		Interleaved channels. Replace 180 channels with: .... 359 channels...
5.5		New headline: ADJACENT CHANNEL SELECTIVITY, SELECTIVITY IN THE INTERLEAVED CHANNEL.
5.5.1		Rename the paragraph to 5.5.1.1
5.5.2		Rename the paragraph to 5.5.1.2 ·

Paragraph	Page	
5.5.3		Rename the paragraph to 5.5.1.3
5.5.1		New paragraph. Adjacent channel selectivity.
5.5.2		New paragraph. Adjacent channel selectivity in the interleved channel (± 12.5 kHz)
5.5.2.1		Definition The adjacent channel selectivity in the interleaved channel is a measure of the capability of the receiver to receive a wanted modulated signal without exceeding a given degradation due to the presence of an unwanted signal which differs 12.5 kHz in the frequency from the wanted signal.
5.5.2.2		Method of measurement. Two signals shall be applied to the receiver antenna input terminal via a combining network. The wanted signal shall be tuned to the nominal frequency of the receiver and be modulated with normal test modulation. The unwanted signal shall be at the nominal frequency of the upper adjacent interleaved channel (+ 12.5 kHz) and be modulated with a 400 Hz tone to a frequency deviation of ±3kHz. Initially the unwanted signal shall be switched off and the level of the wanted signal shall be adjusted to 1 dB (1 µV) E.M.F. (-112 dBm) under normal test conditions. The unwanted signal shall then be switched on and its level adjusted until SND/ND-ratio, measured at the line output terminal, is reduced to 20 dB.
5.5.2.3		Requirement The adjacent channel selectivity in the interleaved channel shall not be less then 36 dB (1 µV) E.M.F. (-77 dBm) under normal test condition.

Paragraph	Page	
5.29		Change headline to: CO-channel rejection and adjacent channel selectivity under influence of fading.
5.29.1		Add interleaved channels to the last section: ...co-channel and adjacent interleaved channel (±12.5 kHz) as unwanted signal.
5.29.2	•	Add interleaved channels as a new section: Adjacent channel (±12.5 kHz) interference: RMS-level of the unwanted signal shall not be less than 20 dB (1 μV) E.M.F. (-93 dBm) for upper and lower adjacent interleaved channel.

Paragraph Page

CORRECTIONS IN DOC 450-1 FEB -80 AS A RESULT OF CHANGED SPECIFICATIONS FOR THE BASE STATION.

2.2.1 5 Add new text after the last sentence:

"In the future, however, it is possible that interleaved channels i.e. channels weith 12,5 kHz channel separation from the ordinary channels will be used."

4.3.2.3 23 Replace the description of frame 20 by:

"Chan.No Prefix TA No BS ind Idle Activ.order

$N_1N_2N_3$ P(15) Y_1 Y_2 Z(15) JJJ A(0-2,4-15) $f_\phi f_\phi f_\phi f_\phi f_\phi$
$N_1N_2N_3$ P(15) Y_1 Y_2 Z(15) JJJ A(3) d $f_\phi f_\phi f_\phi f_\phi$"

4.3.3.1 26 Replace all text on page 26 by the following text:

"Note 1)

In digits N_1 and N_a, the least significant bit (bit no. 4) denotes the hundreds digit in the channel number. Bits no. 2 and 3 contain information about power level, high power 11, medium power 10 and low power 01, 00. Bit no. 1 is set to 0 for normal channels (1 to 180) and 1 for interleaved channel (201 to 379).

Regarding MS output power, add the following:

Examples of information in $N_1N_2N_3$:

$N_1N_2N_3$ = 0111 0000 0101
means high power indication, channel number 105.

$N_1N_2N_3$ = 0010 0000 0001
means low power indication, channel number 1 (f_0)

$N_1N_2N_3$ = 1010 0000 0001
means low power indication, channel number 201 (f_0 + 12,5 kHz)

Paragraph	Page	
		Please observe that these options are valid only for BS. (Note 3) The function of interleaved channels is possible for future use. In case of interleaved channels, the channel number shall be noted as stated in the table below.

N_1	Channel number
0xx0	0 - 99
0xx1	100 - 199
1xx0	200 - 299
1xx1	300 - 399

Examples:

$N_1N_2N_3$ = 1111 0000 0101
means high power indication, interleaved channel number 305

$N_1N_2N_3$ = 0010 000 0001
means low power indication, channel number 1 (f_0)

$N_1N_2N_3$ = 1010 0000 0001
means low power indication, interleaved channel number 201 (f_0 + 12,5 kHz)

4.3.3.6 31 Add to the end of the paragraph:

"Note: Coding and meaning of parameter d in frame 20(A=3).

Notation	Coding	Meaning
d(0)	0000	Deactivate compander
d(1-14)	0001-1110	No action with compander
d(15)	1111	Activate compander

4.3.3.7 Change in paragraph:

V1(7)	0111	Supress supervision of freemarked CC/TC/AC
V1(10)	1010	Cancel supression of supervision of freemarked CC/TC/AC

Paragraph	Page			
4.3.3.8		Change in paragraph:		
		V1(8)	1000	Acknowledge supress supervison of freemarked CC/TC/AC
		V1(11)	1011	Acknowledge cancel supression of supervision of freemarked CC/TC/AC
4.3.3.9		Replace the whole paragraph with:		

- Other maintenance information from BS (frame 28)

Notation	Coding	Meaning in direction BS-MTX (frame 28)
V1(10)	1010	Don't care
V1(11)	1011	Don't care
V1(6)	0110	Block the channel
V1(9)	1001	Deblock the channel
V1(12)	1100	SU/SR alarm via channel line
V1(15)	1111	Shall not be used
V2(15)	1111	NMT-alarms
V2(1)	0001	House-alarms
V2(8)	1000	External alarms

Notation	Meaning in direction BS-MTX (frame 28)
V1(10) V2(15) V3(0)	TX-antenna fault level 1
V1(10) V2(15) V3(1)	Transmitter level 1
V1(10) V2(15) V3(2)	Selftest failed
V1(10) V2(15) V3(3)	Channel unit fault level 1
V1(10) V2(15) V3(4)	RX-antenna fault level 1
V1(10) V2(15) V3(5)	RF receiver blocking alarm
V1(10) V2(15) V3(6)	Combiner alarm level 1
V1(10) V2(15) V3(7)	High temperature fault
V1(10) V2(15) V3(8)	RF receiver blocking alarm ceasing
V1(10) V2(15) V3(9)	Diversity alarm
V1(10) V2(15) V3(12)	Redundant power supply
V1(10) V2(15) V3(13)	Redundant master oscillator
V1(10) V2(15) V3(14)	Cooling fan fault
V1(10) V2(15) V3(15)	Redundant amplifier in receiver multicoupler

Notation			Meaning in direction BS-MTX (frame 28)
V1(6)	V2(15)	V3(0)	RX-antenna fault level 2
V1(6)	V2(15)	V3(1)	Missing deviation
V1(6)	V2(15)	V3(2)	ϕ-signal test loop
V1(6)	V2(15)	V3(3)	Spare
V1(6)	V2(15)	V3(4)	Channel unit fault level 2
V1(6)	V2(15)	V3(5)	Spare
V1(6)	V2(15)	V3(6)	Local blocking
V1(9)	V2(15)	V3(6)	Local deblocking
V1(6)	V2(15)	V3(7)	Receiver
V1(6)	V2(15)	V3(8)	Combiner alarm level 2
V1(6)	V2(15)	V3(9)	CU
V1(6)	V2(15)	V3(10)	SU, via data line
V1(12)	V2(15)	V3(10)	SU, via channel line and CU
V1(6)	V2(15)	V3(11)	SR, via data line
V1(12)	V2(15)	V3(11)	SR, via channel line and CU
V1(6)	V2(15)	V3(12)	Power supply
V1(6)	V2(15)	V3(13)	Receiver multicoupler
V1(6)	V2(15)	V3(14)	Transmitter level 2
V1(6)	V2(15)	V3(15)	TX-antenna fault level 2
V1(10)	V2(1)	V3(0)	Fire alarm
V1(6)	V2(1)	V3(1)	Mains break-down alarm
V1(10)	V2(1)	V3(2)	Intruder alarm
V1(10)	V2(1)	V3(3)	Obstruction light alarm
V1(9)	V2(1)	V3(4)	Mains return
V1(10)	V2(1)	V3(5)	Mains break-down alarm at channel with battery back-up
V1(10)	V2(1)	V3(6)	Enviroment temperature alarm
V1(10)	V2(1)	V3(7)	Spare
V1(10)	V2(1)	V3(8)	Spare
V1(10)	V2(8)	V3(8)	Missing CC indication
V1(10)	V2(8)	V3(9)	Missing CC indication ceasing
V1(10)	V2(8)	V3(10)	Missing TC or AC indication
V1(10)	V2(8)	V3(11)	Missing TC or AC indication ceasing
V1(10)	V2(8)	V3(12)	Alarm unit alarm
V1(10)	V2(8)	V3(13)	MUX alarm
V1(10)	V2(8)	V3(14)	Spare
V1(10)	V2(8)	V3(15)	Spare

All other combinations of V1 V2 V3 shall be spare.

Parameter V4 can be used in case of manufacturer/operator defined alarms but shall not be interpreted by the MTX.

Paragraph Page

Note 1 Character V4 not specified in the alarm above shall have the value 0000.

Note 2 Level 1 Degradation which not requires an immediate service action.

Level 2 Not in function.

Note 3 Blocking, deblocking, don't care (see also NMT DOC. 2 (450) / NMT DOC. 900-2 (900) chapter 8 Maintenance of BS).

Three different categories of alarm information shall be sent to the MTX from the base station.

- Blocking, the MTX shall block the channel when it receives this information, i.e. the channel is no longer available for traffic. A blocked channel shall be indicated at the base station. The blocking is initiated by frame 28 from the base station.

- Deblocking, the MTX shall deblock the channel when it receives this information, i.e. the channel is now available for traffic again.

- Don't care, the MTX shall not act on this information.

Note 4 Different classes of alarms

The alarms from the BS are divided in three classes.

- NMT-alarms; includes the alarms which are released by the equipment that is included in the NMT system.

- House alarms; includes the alarms which are released from common equipment at the base station such as fire alarm and intruder alarm.

- External alarms; includes the alarms which are released by all other equipment on the station by using the NMT signalling system for alarm information.

It shall be possible to forward information in frame 28 together with circuit identity both to remote and to local I/O-devices.

Paragraph	Page	
Note 5		Idling of radio channel at blocking alarm. After the CU has sent an alarm containing V1(6), block the channel, the radio channel equipment shall be idled locally. This has the same function as reception of frame 20(A=0) from the MTX.

ADDENDUM TO NMT Doc. 4 1981

Technical specification for the base station equipment.

ADDENDUM TO NMT DOC. 450-4

Corrections and clarifications.

Contents:

ADDENDUM TO NMT DOC. 450-4

Corrections and clarifications.

Contents:

ADDENDUM TO NMT DOC. 450-4

Corrections and clarifications.

Contents:

ADDENDUM TO NMT DOC. 450-4

Corrections and clarifications.

Contents:

ADDENDUM TO NMT DOC. 450-4

Corrections and clarifications.

Contents:

Ref Paragraph	Page	
1.3.4	15	Clarification regarding Transmitter-cabinet intermodulation components. Add new meaning: "In case the combiner is integrated in the radio cabinet the specification shall be exchanged with the specification given in paragraph 3.1.9".
1.3.5	15	Correction regarding Cabinet radiation. Cabinet radiation The radiated power in transmitter off condition from the equipment and cables conntected to it shall not exceed 2,0 nW in the frequency band 30-2000 MHz. In transmitter on condition the radiated power shall not exceed 2,0 nW in the receiver band 453,000 -457,475 MHz Elsewhere the requirements in paragraph 4.6 shall be fulfilled. The measurement shall be performed in accordance with clause 4.6.3.
1.3.6	15	Correction regarding Reliability: Change the 10'th line to "The MTBF shall be at least 20 000 hours for the total channel equipment." and the 18'th to: "For each of these individual equipments the MTBF shall be at least 50 000 hours."
1.3.12	17	Correction regarding Construction Delete the chapter starting with the sentence: "As an option a mechanical arrangment.......... Add following sentence: "Based on the manufactors philosophi regading maintainability and reliability other mechanical solutions than mentioned in this chapter 1.3 may be proposed. (For exampel an integrated solution with transmitter combiner and radio equipment in the same cabinet or a larger number of radioequipment in the cabinet).
1.3.13.2	17	Correction regarding Power source voltage. Correct 3:rd line to "... 50 Hz $\pm$ 2 Hz".
1.3.13.3	17	Correction regarding Mains transients. Correct 2:nd line to ".......an amplitude of + 30% from normal........"

Ref Paragraph	Page	
1.3.13.5	18	Correction regarding Noise from DC-power source Correct 2:nd line to ".......... up to 0,3 V rms within....."
1.3.15	20	Correction regarding Acoustic noise. Change the 2:nd sentence to: "The radiated sound power L_W from the equipment shall not exceed 60 dB (A) relative to 1 pW." and the 3rd sentence to: "------ sound power L_W from the equipment shall not exceed 50 dB (A) relative to 1 pW."
3.1.5	29	Correction regarding Voltage standing wave radio. Correct 2:nd line. "... not exceed 1.8 and at all ..." Correct 4:th line. "... not exceed 2.0 at the output ..."
R 3.1.7	30	Correction regarding Carrier power. Add new last sentence: "In the case of an integrated combiner this paragraph shall be exchanged with the specification according to paragraph 4.4.3 Carrier power."
3.1.9	30	Clarification regarding Intermodulation attenuation in transmitter combiner. Delete line 8 to 13, and add new meaning: In case of an integreated transmitter combiner in the radio cabinet this specification shall be exchanged with the following requirement. "With two or more transmitters in operation the intermodulation products shall not exceed -36dBm at the output to the antenna, except for intermodulation products within the frequency band 453,0 to 457,5 MHz which shall not exceed - 96 dBm".
3.1.14	31	Add new last sentence: "If integerated solution the interface will not be specified".

	Ref Paragraph	Page	
R	3.2.5	32	Correction regarding Connectors. "Correct the sentence: Antenna input terminal(s) of the radio cabinet shall be of type N (female). The connectors at all other terminals shall be off type N (female) or TNC (female)."
	3.2.7	33	Net gain in the passband.
R			The first three lines in this paragraph shall be exchanged with the specification according paragraph 5.3 RF-sensitivity.
	3.2.9*	33	Noise factor.
			This paragraph shall be exchanged with the specification according paragraph 5.3 RF-sensitivity.
	3.2.10	33	Intermodulation.
			This paragraph shall be exchanged with the specification according paragraph 5.7 Intermodulation rejection.
	3.2.11	33	Blocking
			This paragraph shall be exchanged with the specification according paragraph 5.8 Blocking.
	3.4.10	39	Correct first line "The attenuation in the receiver branch........"
	4.3.3	41	Replace the 4:th sentence with:
			"During the carrier rise time and decay time the frequency error shall not exceed ± 2,5 kHz. See clause 4.5.3.
R			In case of using "OCXO" the following will apply:
			a) At mains interruption of more than 2 minutes the following warming up periods are allowed: - equal or less than ± 2,5 kHz within 4 minutes - equal or less than ± 1,0 kHz within 5 minutes
			b) At short mains interruption equal or less than 2 minutes the following warming-up periods are allowed: - equal or less than ± 2,5 kHz within 40 seconds - equal or less than ± 1,0 kHz within 5 minutes
			In case a) and b) the mains return alarm shall be delayed according to the paragraph 8.1.3.2."

Ref paragraph	Page	
4.4.1	42	Add new last sentence: "In case of an integrated transmitter combiner the transmitter carrier power shall be measured at the antenna output terminal of the radio cabinet."
4.4.2	42	Add new last sentence: "With an integrated transmitter combiner the transmitter carrier power shall be measured at the antenna output terminal of the radio cabinet."
4.4.3	42	Replace the first sentence with: "The nominal output power into 50 ohms unbalanced shall be selectable manually as follows: 50 W 12 W 3 W In case of an integrated transmitter combiner the nominal output power at the output terminal of the radio cabinet shall be selectable as follows: 20 W 5 W 1,25 W Concerning a small cell base station it is possible to delete the highest power level, i.e. 50 W in the ordinary base station and 20 W in the integrated solution.

R The manufacturer shall state the corresponding power at the output terminal of the transmitter unit.

R For the purpose of optimizing the system balance it shall be possible to manually reduce the output power
R from the levels given above to at least 3 db below these levels. In case the reduction is made stepwise the steps shall not be greater than 1 dB.

When using an integrated transmitter combiner the power consumption to the eight channel radio cabinet with all the transmitters activated shall be below
R 1700 W for the highest power level.

R Correct 3:rd line:

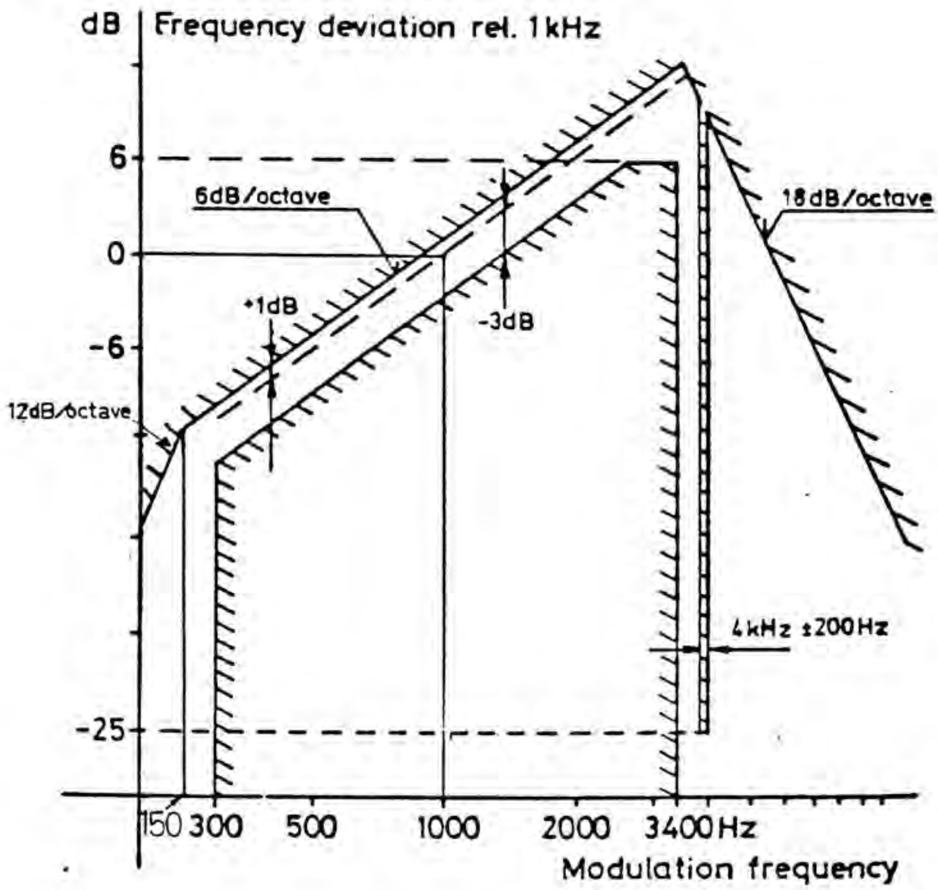
"... carrier output power shall be within ± 1dB, and in case of an integrated combiner within + 1 dB and -2 dB of the nominal output power."

R Correct last line:

"... within + 1 dB and -2 dB, and in case of an integrated combiner within + 1 dB and - 3 dB of the nominal output power."

Ref paragraph	Page	
4.5.3	43	Add new last sentence: "The carrier decay time shall not exceed 50 ms."
4.6.2	43	Correct the heading: "... conducted power level."
4.6.2	43	Correct the first sentence: "... be measured as the power of a discrete signal ..."
4.6.2	43	Add new item after 5:th line: "When the transmitter combiner is integrated in the radio cabinet the measurement shall be done at the antenna output terminal of the radio cabinet."
4.6.4	44	Correct the last sentence and add item: "For case c) the spurious emission shall not exceed 2,0 nW. Regarding spurious emissions within receiver band see paragraph 4.13."
4.7.1	44	Add new item after 5:th line: "In case of an integrated transmitter combiner paragraph 4.7 shall be replaced by paragraph 3.1.9."
4.12.2	48	Add new item after 7:th line: "When the transmitter combiner is integrated in the radio cabinet the measurement shall be done at the antenna output terminal of the radio cabinet."
4.13.2	50	Add new item after 5th line from the top of the page: "When the transmitter combiner is integrated in the radio cabinet "the output of the transmitter" shall be raplaced by "the antenna output terminal of the radio cabinet"."
4.13.3	50	Correct first sentence and add new sentence: "... not exceed 2,0 nW (-57 dBm). In case of an integrated transmitter combiner the noise power within any receiver channel shall not exceed -102 dBm."

Ref paragraph	Page	
4.14.3		Replace the figure with this new figure:

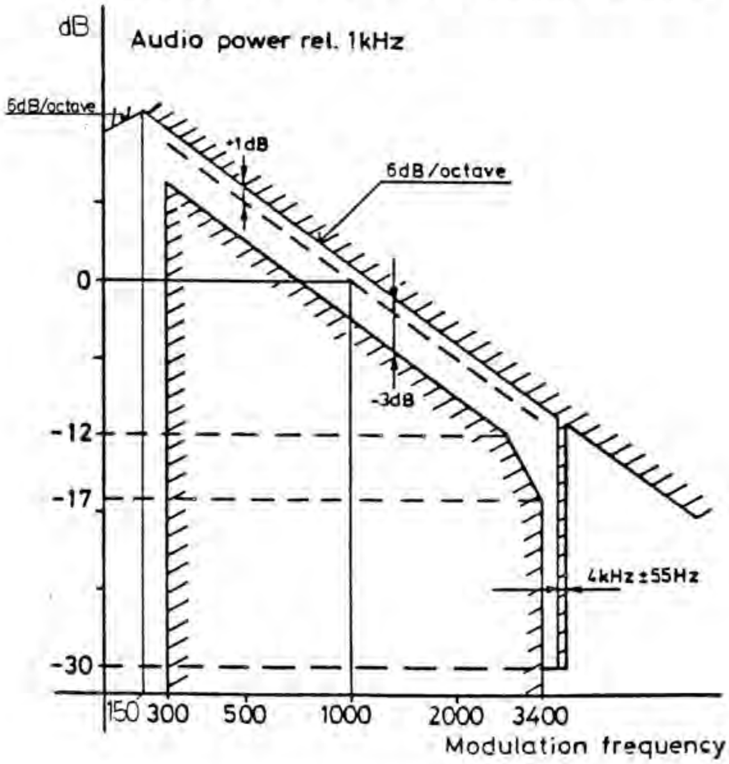


	4.16.2	53	Correct third line in b) "Frequency deviation at a modulating frequency F1 of 1000 Hz."
	4.17.2	54	Correct in b) "The same method as a) above but without the psophometric filter..."
R	4.23	57	RESERVED
R	4.24	57	New paragraph. Add new paragraph as follows:
R	4.24		INFLUENCE ON DEVIATION CAUSED BY HIGH AUDIO FREQUENCIES
R	4.24.1		Definition This clause expresses the transmitters capability not to be influenced by any frequencies outside the normal modulation frequencies.

	Ref paragraph	Page	
R	4.24.2		<u>Method of measurement</u> An audio frequency test signal of 1000 Hz is applied at the transmitter line input terminal. The level of the test signal is adjusted until ±3,0 kHz deviation is obtained. The audio level shall be within the range given in paragraph 4.18.3. Another signal with a level of -20dB below the test signal of 1000 Hz in then applied at the transmitter line input terminal (see paragraph 4.16.2). The frequency of this signal varies from 5 kHz to 40 kHz.
R	4.24.3		<u>Requirements</u> The resulting deviation shall be within ± (3,0±0,2) kHz.
	5.	58	Correction regarding simulation of duplex operation at receiver measurements. Correct 4:th line: "...........measured at the receiver antenna input terminal of the radio cabinet (including receiver multicoupler)." Add new sentence: "For measurements made at the receiver antenna input terminal of the radio cabinet the requirements shall be fulfilled even when all the transmitters in the cabinet are operating.
	5.3	58	The method of measurement/requirement according para 5.3 "RF-sensitivity" shall be corrected as below:
	5.3.1	58	Correct first sentence to: "The sensitivity of the receiver including receiver multicoupler is the minimum level of signal (E.M.F) at the receiver antenna input terminal of the radio cabinet which at the nominal frequency...."
	5.3.2	59	Correct first sentence and add second sentence: ".... modulation, according to paragraph 2.2.4, shall be applied to the receiver antenna input terminal of the radio cabinet. Thus including the receiver multicoupler and cables in the cabinet".
	5.3.3	59	Add new sentence: "The manufacturer shall state the corresponding RF-level at the input connector of the receiver unit".

Ref paragraph	Page	
5.4	59	The method of measurement/requirement according para 5.4 "Co-channel rejection" shall be corrected as below:
5.4.2	59	Correct first sentence and add second sentence:
		"Two input signals shall be applied to the receiver antenna input terminal of the radio cabinet via a combining network. Thus including the receiver multicoupler and cables in the cabinet."
		Correct the last sentence:
		".... of the wanted signal at the receiver antenna input terminal of the radio cabinet for which......."
5.5	60	The method of measurement/requirement according paragraph 5.5 "Adjacent channel selectivity" shall be corrected as below:
5.5.2	60	Correct first sentence and add second sentence:
		"Two signals shall be applied to the receiver antenna input terminal of the radio cabinet via a combining network. Thus including the receiver multicoupler and cables in the cabinet."
5.6	60	The method of measurement/requirement according paragraph 5.6 "Spurious response rejection" shall be corrected as below:
5.6.2	61	Correct first sentence and add second sentence:
		"Two input signals shall be applied to the receiver antenna input terminal of the radio cabinet via a combining network. Thus including the receiver multicoupler and cables in the cabinet."
		Correct the last sentence:
		"........of the unwanted signal at the receiver antenna input terminal of the radio cabinet when......"
5.7	61	The method of measurement/requirement according paragraph 5.7 "Intermodulation rejection" shall be corrected as below:
5.7.2	61	Correct first sentence and add new second sentence:
		"..... applied to the receiver antenna input terminal of the radio cabinet via a combining network. Thus including the receiver multicoupler and cables in the cabinet.

Ref Paragraph	Page	
		Correct the last sentence:
		"......... unwanted signals at the receiver antenna input terminal of the radio cabinet when ...."
5.8	62	The method of measurement/requirement according paragraph 5.8 "Blocking" shall be corrected as below:
5.8.2	62	Correct first sentence and add new second sentence:
		"....... applied to the receiver antenna input terminal of the radio cabinet via a combining network. Thus including the receiver multicoupler and cables in the cabinet.
5.15.3	67	Correction regarding audio frequency response of the receiver.
		The figure shall be changed below 300 Hz as follows:



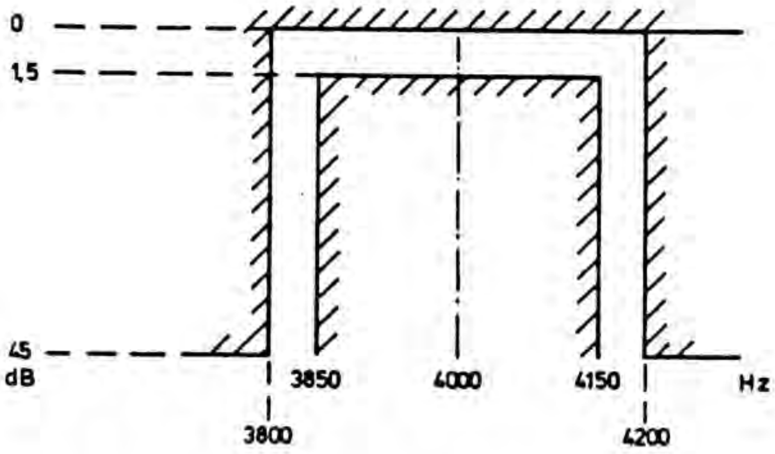
5.18.2	70	Correct second line in c)
		"level of 10 dB (1µV) E.M.F."
5.18.3	70	Correct in case c)
		"..... shall not exceed - 30 dB."

Ref Paragraph	Page	
5.20.1	71	Correction regarding squelch opening and closing levels.
		Correct first sentence:
		"... with normal test modulation at the receiver antenna input terminal of the radio cabinet shall be -2 dB (1µV) E.M.F. ± 2 dB at normal ..."
R		Correct 8:th line and move to after 11:th line:
•		"... closing level shall always be 1 to 2 dB below ...."
5.20.2.3	72	Correction regarding squelch opening and closing delays.
		Correct 11:th line:
		"... to a level of 2 dB above the ..."
5.20.2.4	73	Correct second line
		"Opening delay t_o = 5 + 2/- 4 ms."
5.22	74	Add new paragraph.
5.22	74	RF-LEVEL INDICATOR
		The receiver shall be equipped with a signal strength indicator giving information to CU when the RF-signal exceeds 10 ± 4 dB µV EMF (See 8.1.3.5).
5.23	74	Add new paragraph.
5.23	74	INTERFERENCE IN THE Ø-SIGNAL FREQUENCY BAND
5.23.1		Definition
		The interference level is the ratio, expressed in dB, of the level of unwanted components of the output signal, caused by the presence of the modulation in the received signal as a result of nonlinearity in the receiver, to the level of the wanted Ø-signal measured at the output of the receiver excluding the filter according to paragraph 5.15.3.

Ref Paragraph | Page

5.23.2 Method of measurement

A filter according to the figure below is applied to receiver output in such a way to exclude the filter for the Ø-signal frequency band according paragraph 5.15.3, and the audio frequency level is measured with a R.M.S. voltmeter. Alternatively an audio spectrum analyser may be used.



A radio frequency signal at the nominal frequency of the receiver and with a level of 60 dB (1 uV) E.M.F. is applied to the receiver input terminal. The radio frequency signal is modulated with the Ø- signal to ±0,3 KHz deviation and the level of the Ø-signal is measured. Thereafter the Ø-signal modulation is removed.

The receiver input radio frequency signal is then modulated to ± 1,5 kHz deviation and the modulation frequency is varied between 300 Hz and 3400 Hz. The interference in the Ø-signal channel is measured.

The measurement is repeated at the deviation 3 dB above and 3 dB below ± 1,5 kHz deviation.

5.23.3 Requirement

The interference level in the Ø-signal frequency band shall not exceed -10 dB relative to the Ø-signal level.

Ref Paragraph	Page	
5.24	74	Add new paragraph.
5.24	74	RELATIVE AUDIO FREQUENCY INTERMODULATION PRODUCT LEVEL IN THE Ø-SIGNAL FREQUENCY BAND
5.24.1		Definition

The relative intermodulation product level is the ratio, expressed in dB, of the level of unwanted components in the Ø-signal frequency band caused by the presence of two modulating signals as a result of nonlinearity in the reciever, to the level of the wanted Ø-signal measured at the output of the receiver excluding the filter for the Ø-signal frequency band according paragraph 5.15.3.

5.24.2 Method of measurement

A filter according to paragraph 5.23.2 is applied to the receiver output in such a way to exclude the filter for the Ø-signal frequency band according paragraph 5.15.3, and the audio frequency level is measured with a R.M.S. voltmeter. Alternatively an audio spectrum analyzer may be used.

A radio frequency signal at the nominal frequency of the receiver and with a level of 60 dB (1uV) E.M.F. is applied to the receiver input terminal. The radio frequency signal is modulated with Ø-signal to ± 0,3 kHz deviation and the level of the Ø-signal is measured. Thereafter the Ø-signal modulation is removed.

Two audio frequency generators, A and B, shall be connected via a combining device to the modulation input of the radio frequency signal generator.

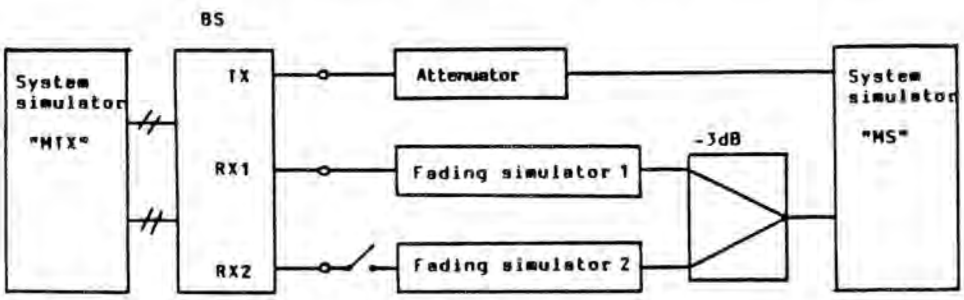
Adjust the radio-frequency test signal to the nominal frequency of the receiver and the test signal level successively to 20 dB, 60 dB and 100 dB (1 uV) E.M.F.

In the absence of an output from audio-frequency generator B, adjust the audio-frequency generator A to produce a ± 2,1 kHz frequency deviation at a modulation frequency of 1200 Hz. Record the output level of generator A.

Reduce the output of generator A to zero and adjust the output of generator B to produce a ± 2,1 kHz frequency deviation at a modulation frequency of 2800 Hz.

Restore the output of generator A to the level recorded and measure the intermodulation products in the Ø-signal frequency band.

Ref Paragraph	Page	
5.24.3		Requirement
		The intermodulation product level in the Ø-signal frequency band shall not exceed -10 dB relative to the Ø-signal level.
5.25	74	RESERVED
5.26	74	Add new paragraph.
5.26	74	DIVERSITY (Option)
		In case of a diversity receiver is implemented the following specification shall be fullfilled:
5.26.1		Definition
		The diversity gain is the mesure for the improvement on the lowest signal strength level with fading where the frame reception propability is at least 95%.
5.26.2		Method of measurement.
		A carrier with a nominal frequency of a BS receiver and modulated with a normal data test modulation (see para 2.2.4.2) shall be applied to the receiver antenna input terminal(s) of the radio cabinet through the Rayleigh fading simulator(s), see figure.



The frame reception probability with one receiver antenna input terminal connected to the fading simulator shall be measured as the propability of received frames 10a at the "MTX" sent by the "MS" as a response of
R received frames 2a. The space between 2a frames shall not be a multiple of the frame length. The "MS" output level shall be set so that a frame reception probability of 95% is obtained. The measurement shall be made for speeds of 1, 10 and 100 km/h and corresponding "MS" output levels are noted.

The measurements shall be repeated with both receiver antenna input terminals connected to the fading simulators.
R The correlation factor between the two fading simulators shall be 0,5. The corresponding "MS" output levels are noted.

Ref Paragraph	Page	
		The levels measured with corresponding speeds are compared with each other to get the diversity gain.
5.26.3		Requirement
		In each case the diversity gain shall be at least 5 dB.
5.26.4		Other requirements for the diversity receiver.
R		For the diversity reception the measurements of para 5.1-5.25 and 5.27 are done by coupling the RF-signals to both receiver branches via a 3-dB-coupler.The specified RF-signal levels shall be measured after 3 dB-coupler, that is at the two input terminals of the radio cabinet.
R		When using the diversity receiver with only one RF-branch connected this shall fullfill the ordinary receiver requirements. The branch to use may be stated by the manufacturer.
5.27	74	Add new paragraph.
R		SR-FACILITIES IN THE RECEIVER
		The receiver shall include signal strength measurement facilities according to section 7, except the requirements for channel switching time, para 7.2.2.
		The signal strength level limits shall be settable locally at BS according to the set limits given below. The limits set must be maintained after power-off and shall not be overruled by any information from the MTX.
		The signal strength from MS is measured and evaluated in relation to the set limits (see below). The evaluation is started by the frame 20(A=(3) and stopped by the frames 20(A=0), 20(A=2) and 20(A=12).
		The signal strength shall be related to the receiver antenna input terminal of the radio cabinet. Regarding the tolerances for the specified I_H- and I_L-limits these shall be in accordance to paragraph 7.2.3.
R		In the case of fading, these limits shall be widened by the fading margin specified in paragraph 5.28.1.
		The frame 25(A=7) is sent to MTX if the received signal strength averaged over 5 sec. is below the higher limit but above the lower limit. The frame 25 (A=7) is then repeated every 20 or 60 sec. (selectable as t in paragraph 8.1.5.2) if the criterias are still fullfilled.

Ref Paragraph | Page

The frame 25 (A=8) is sent to MTX if the received signal strength averaged over 20 sec. is below the lower limit. The frame 25 (A=8) is repeated every 20 sec. if the criteria is still fullfilled.

In case of diversity reception the SR-alarm limits shall be based on the combined receiver input RF-signal level.

Setting of the alarm levels for received MS signal strength in the BS:

(Coding)	Meaning	
(Binary)	High level, 1_H	Low level, 1_L
0000	Suppress the function	Suppress the function
0001	30 dB (1µV) E.M.F.	20 dB (1µV)E.M.F
0010	25 "	16 "
0011	20 "	12 "
0100	16	08 "
0101	12	4 "
0110	8 "	0 "
0111	4 "	-4
1000	0 "	Spare
1001	40 "	"
1010	35 "	"
1011	Spare	"
.	"	"
.	"	"
.	"	"
1111	Spare	Spare

The alarm limits 0111 to 1010 are only recommended.

High level and low level, including suppression of the function, shall be settable independently of each other.

5.28 74 Add new paragraph:

R 5.28 74 INFLUENCE OF FADING.

This paragraph may be changed based on further investigations.

5.28.1 Signal strength alarm fading margin. (RECOMMENDATION)

Ref Paragraph Page

5.28.1.1 Definition

Signal strengt fading margin is the rms value of the BS receiver RF-input signal level under Rayleigh fading conditions relative to the corresponding value without fading for the CU to send the quality level alarms (A7 or A8) due to signal strength to MTX.

5.28.1.2 Method of measurement

A signal of carrier frequency equal to the nominal frequency of the BS receiver and modulated only with a supervisory tone (see paragraph 4.9) shall be applied to the receiver RF-input terminal through a Rayleigh fading simulator.

The receiver rms RF-input level of this signal shall be set at ca 30 dB (µV) emf and adjusted so that is obtained with a success rate of 80% without fading. This rms levels are noted.

The measurement shall be repeated with the Rayleigh fading simulator set for simulated vehicle speeds of 1, 10 and 100 km/h. These rms levels are noted.

For diversity reception the measurements are done for one branch as well as simultaneously for both receiver branches by coupling the RF-signal to both receiver RF-input terminals (see paragraph 2.2.5) via 3-dB-coupler and another uncorrelated Rayleigh fading simulator.

R The measurements are repeated for quality level alarm 2 (frame 25 (A=8)) with the rms RF-input level set at ca 20 dB (µV) emf.

5.28.1.3 Requirement

The signal strength fading margin shall not exceed 3 dB.

For diversity reception the requirement for measurements with one branch as well as with two branches simultaneously are the same referred to one of the receiver RF-input terminals (see paragraph 2.2.5).

5.28.2 Signal strength result (frame 26) fading margin (RECOMMENDATION)

5.28.2.1 Definition

Signal strength result fading margin is the change in the mean value of the Rout when the signal strength is measured under fading conditions relative to the Rout when the measuring is done without fading. The rms value of the RF-signal to SR is kept constant under both conditions.

Ref Paragraph | Page

5.28.2.2 Method of measurement

A signal of carrier frequency equal to the nominal frequency of the SR and modulated with normal test modulation (see para 2.2.4.1) shall be applied to the SR RF-input terminal througt a Rayleigh fading simulator.

R Without fading the RF-level to SR shall be adjusted to give R(n1)R(n2)=28. The rms level to SR is now measured with a true RMS power meter and noted. The fading simulator is now set to fading speed of 10,50 and 90 km/h and the RF rms level to SR is adjusted to give the same as without fading.

For diversity reception the measurements are done for one branch as well as simultanously for both receiver branches by coupling the RF-signal to both SR RF-input terminals (see para 2.2.5) via 3-dB-coupler and another uncorrelated Rayleigh fading simulator.

The measurements are repeated for R(n1)R(n2)=14.

The calculation of the mean signal strength result should be based upon at least 1000 frames 26.

5.28.2.3 Requirement

The signal strength result fading margin shall not exeed 2 dB.

For diversity reception the requirement for measurements with one branch as well as with two branches simulanously are the same referred to one of the receiver input terminals (see para 2.2.5).

5.28.3 Signal strength result devation (RECOMMENDATION)

5.28.3.1 Definition and Method of measurement

The signal strength result deviation is the distance in dB from 10 to 90% in the accumulativ propability density when measuring signal strength under fading conditions.

The method of measurement is equal to measuring signal strength result fading margin, se para 5.28.2.

5.28.3.2 Requirement

Fading speed km/h:	10	50	90
Output devation max dB:	9.5	5.5	4.5

Ref Paragraph	Page	
5.28.4		Supervisory (Ø-) signal fading margin. (RECOMMENDATION)
5.28.4.1		Definition

Supervisory signal fading margin is the rms value of the BS receiver RF-input signal level under Rayleigh fading conditions relative to the corresponding value without fading for the CU to send the quality alarmlevel 1 resp. 2 (20(A=7) resp. (A=8)) due to signal to noise ratio to MTX.

5.28.4.2 Method of measurement

A signal of carrier frequency equal to the nominal frequency of the BS receiver and modulated only with a supervisory tone (see paragraph 4.9) shall be applied to the receiver RF-input terminal throuth a Rayleigh fading simulator.

The receiver RF-input level of this signal shall be set so that the quality alarm level 1(A7) is obtained with a success rate of 80% without fading. This rms level is noted.

The measurement shall be repeated with a Rayleigh fading simulator set of simulated vehicle speeds of 1, 10 and 100 km/h. These rms levels are noted.

For diversity reception the measurements are done for one branch as well as simultaneously for both receiver branches by coupling the RF-signal to both receiver RF-input terminals (see paragraph 2.2.5) via 3-dB-coupler and another uncorrelated Rayleigh fading simulator.

The measurements are repeated for quality alarm level 2 (A8).

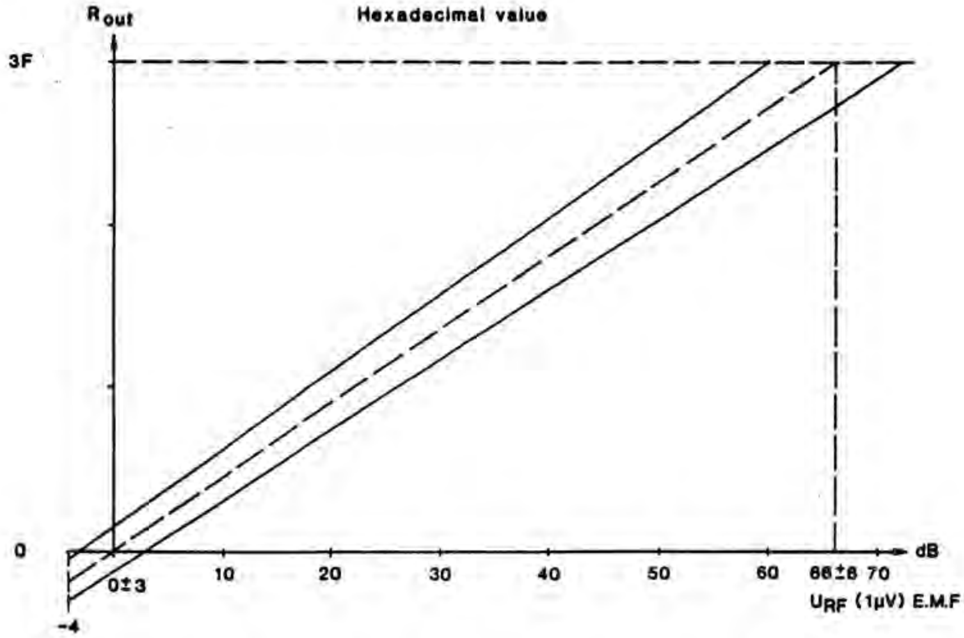
5.28.4.3 Requirement

The supervisory signal fading margin shall not exceed 7 dB.

For diversity reception the requirement for measurement with one branch the margin shall not exceed 7 dB, and with two branches simultaneously the margin shall not exceed 4 dB referred to one of the receiver RF-input terminals (see paragraph 2.2.5).

Ref Paragraph	Page	
R 7.2.3	72	Replace the whole paragraph with:
7.2.3	72	<u>Signal strength measurement output.</u>

The signal strength measurement output (ROUT) as a function of the RF input signal level at the receiver antenna input terminal of the cabinet U_{RF} shall have a characteristic as below:



R "All the values below 0+3 dB (1µV) EMF shall be sent as 0 (hexadecimal value) and all the values above R66+6 dB (1µV) EMF shall be sent as 3F (hexadecimal value) to the MTX.

The level -4 dB (1µV) EMF is used only in connection with sending I_L (ref para. 5.27).

R 8.1.1 78 Correction regarding channel activation order by MTX.

Add after 5:th line:

"One frame 15 (idle) shall be sent before frame 25A (8) for synchronization purposes.

8.1.2 78 Correction regarding Response on other management/maintenance orders.

Correct first sentence:

"The CU shall activate the BS equipment as ordered by MTX in frame 22 and send acknowledgement frame 27".

	Ref paragraph	Page	
R	8.1.3.1	79	Correction regarding NMT-alarms.

Correct in 3:rd and 4:th line:

- "Antenna fault, when the VSWR towards the antenna measured at the TX-combiner output exceeds a preset level."

Add new item after 10:th line:

R
R "Antenna fault level 1 shall also be sent to the MTX when the VSWR at the transmitter combiner filter input exceeds X (to be decided). In this case the fault alarm shall be sent only on the corresponding channel.

80 Add following text after last sentence:

- Redundant power supply fault. This alarm is sent if full operation of channels connected to this power supply is possible.
- Redundant master oscillator fault. This alarm is sent if the frequency stability requirements are still fullfilled. In order case transmitter fault alarm level 2 is sent from all channels connected to the master oscillator.
- Cooling fan fault.
- Redundant amplifier fault in the receiver multicoupler.

In case of diversity (option) following alarms shall be sent:

- If a fault occure in one of the receiver multicouplers the "redundant amplifier fault in the receiver multicoupler" shall be sent on all channels connected to this receiver multicoupler.

R - Deleted

8.1.3.2 80 Correction regarding house alarms.

R Line 4 in this paragraph shall be changed as follwos:

- Mains return alarm. Ref. paragraph 4.3.3. In case a) the alarm shall be delayed until the frequency error is equal or less than ± 2,5 kHz (maximum 4 minutes). In case b) this alarm shall be deleyed 40 seconds after power on or mains return.

Ref paragraph	Page	
R		Add in line 16:
		"... influenced of the fault, including the dataline (if the SU/SR are influenced)."
		Correct the 26:th line:
R		"Mains break-down alarm: the battery voltage is below 41 ± 2 V."
R		Correct the 27:th line:
		"Mains return alarm: the battery voltage has returned above 46 ± 1 V."
R 8.1.3.4	81	Correction regarding alarm indication.
		Correct 3:rd line after ... "shall be red" as follows:
		"If the two arlam levels are indicated by a single indicatior, alarmlevel one shall be flashing and alarmlevel two shall be continous indicated.
8.1.3.5		RF receiver blocking alarm (New paragraph)
		This alarm shall be activated if i.e. a faulty MS transmits continously on a calling channel, a combined calling and traffic channel, free marked traffic channel or an idle channel.
		The CU shall send the alarm (frame 28) to MTX if the following conditions are fulfilled:
		the Ø-signal test loop (See 8.1.5.3) is connected and at the same time information from the RX indicates a received RF-signal above a certain level for more than the last t minutes. t shall be setable between 1 and 30 minutes. See clause 5.22.
		If the RF-signal decreases below the alarm level for more than t minutes CU sends frame 28, "RF receiver blocking alarm ceasing", to MTX.
		Frame 22 V_1 (3) shall suppress the RF receiver blocking alarm and frame 22 V_1 (12) cancels the suppression. This alarm shall not be indicated on the base station.
		The MS fault alarm may be sent again after an alarm ceasing without alarm reset.

	Ref paragraph	Page	
R	8.1.5.2	82	Correction reg. detection of Ø-signal.
R			Correct 3:rd line:
			0 dB (adjustable between -5 and 10 dB).
			Exchange all text from Note 2 with following:
			Message 25A(7) to MTX shall be repeated after time t as long as the criteria for sending the alarm is still fullfilled. The time t shall be settable to 20s or 60s at the base station. In case of 60s period MTX will still order signal strength measurement every 20s if the measured signal strength is below a certain level.
			Message 25 A (8) to MTX shall be repeated after 20s periods as long as the evalutated value does not pass the alarm limit again.
			If no supervisory signal on the transmitted Ø-signal frequency (S/N ratio in speech channel below limit 2) is received within 3s after reception of frame 20A(3) from MTX, frame 25A(8) shall be sent to MTX.
			The Ø-signal detector shall measure the S/N of the looped Ø-signal. The Ø-signal shall be measured within the frequency range f ± 10 Hz (3 dB bandwidth), and the noise at least within the Ø frequency range f ± 100 Hz but not outside the frequency range 3800 to 4200 Hz (35 dB bandwidth).
	8.1.6	82	Correction regarding Channel line loop.
			Change the 1:st sentence to:
			"....... order from the MTX (frame 20 (5)) and when such faults occure in the CU that no frames can be sent to MTX.
	8.1.9	84	Correction regarding service functions.
R			Correct the sentence:
			"The measuring accuracy shall be enough for good maintainability.
			Correct the three last sentences to:
			"The base station shall be equipped with handset (with push-to-talk switch) or loudspeaker (with volume control)."

Ref paragraph | Page

R 8.1.10 **Channel selftest** (New paragraph)

The CU shall perform a channel selftest as ordered from the MTX (frame 22 $V_1(4)$, acknowledge frame 27 $V_1(5)$) or when initiated locally at the base station. In the selftest the CU shall:

- start the transmitter
- activate the RF test loop
- send a 1200 Hz testsignal from the CU, corresponding to ± 3 kHz deviation, through the RF test loop and back to the CU where it is evaluated

- start the Ø-signal and evaluate the result
- initiate a signal strength measurement in the actual receiver on the used radio channel and evaluate the result. In case of diversity the two receiver branches shall be tested separately.

Within 5s after the selftest was initiated or when a fault is detected the CU shall stop the Ø-signal, stop the test signal, deactivate the RF test loop and stop the transmitter and send the alarm frame 28, $V_1(10)V_2(15)V_3(2)$, "selftest failed" if one or several of the following conditions occur:

- the level of the detected test signal deviates more than X dB from the expected. X shall be adjustable from 3 to 8 dB, nominal 6 dB.
- the criteria for sending frame 25A(8) is fullfilled
- the signal strength, measured by the actual receiver, is below 2 dB (1uV) E.M.F. or above 14 dB (1uV) E.M.F.

In other case the frame 27 $V_1(6)$ "selftest completed" is sent.
If the selftest is locally initiated the result shall be indicated at the base station.

8.1.11 **Signal strength receiver (SR) selftest** (New paragraph)

R It is recommanded also to have a selftest functions even for the common signal strength receiver function. This can be ordered from one or several CU's and be added to the selftest for the actual channel.

It must be taken into acount that no collission with the normal signal strenght measurements is the SU/SR as ordered from the MTX is allowed.

R	9.1.1	86	Correction regarding signal strength measurements.

Exchange the text starting at 5:th line with "At 100% of Rout ..." to line 10 with following:

"The quantified binary value, representing the RF input level, shall be sent to MTX.
The figure in clause 7.2.3 shows the relation between RF input level at the antenna input terminal of the cabinet and the coded value (hexadecimal) with given tolerances.

That is, as an example, with an RF-input level at 34 dB(1µV) EMF the nominal coded value sent to MTX shall be (R_1 (2) R_2 (0)) equal to 0010 0000".

	9.1.2	87	Correction regarding fault alarm via SU.
R		•	Correct 10:th line:

... alarm shall be sent once via that CU through which the first measuring order is received after the fault accurred.
Add new senteces:

"The SU/SR alarms are reset as ordered from MTX. Frame $22V_1(1)$ will be used in case of data line, and frame 22 $V_1(2)$ will be used via channel line/CU in case of no data line is used. Frame 22 shall be acknowledged by frame 27. If the fault(s) remains the SU/CU shall therafter send the alarm(s) frame 15 and 28 to the MTX.

When data line is connected to the SU and a common power supply fault occurs which influence on SU/SR the SU shall send "Power supply fault" on the data line.

Regarding "Mains break down alarm" and "Mains return alarm" the SU shall send the alarms on the data line corresponding to paragraph 8.1.3.2."

CORRECTIONS IN DOC 1 REGARDING THE NMT-450 BASE STATION SPECIFICATION.

Ref Paragraph	Page	
4.3.3.6	30	Correction regarding Channel activation order in frame 20 and Channel status information in frame 25.

Add to the meaning of frame 20A(0):

", mute receiver, cancel suppression of frame 25A(7)".

Delete "spare" and add new meaning to frame 20A(2):

"General channel reset. This frame gives the same result as the frames 20A(0), $22V_1(1)$ and $22V_1(9)$ together".

Correct the meaning of frame 20A(4) to:

"Supress frame 25A(7) from BS".

Correct the meaning of frame 20A(10) to:

"Cancel suppression of frame 25A(7)".

Add to the meaning of frame 20A(12):

", cancel suppression of frame 25A(7)".

Correct the meaning of frame 20A(15):

R "Start BS-transmitter, deactivate muting."

Delete "spare" and add new meaning to frame 25A(3):

"Acknowledge general channel reset".

Correct the meaning of frame 25A(5) to:

"Acknowledge "supress frame 25A(7)"."

Correct the meaning of frame 25A(11) to:

"Acknowledge" cancel suppression of frame 25A(7)"."

4.3.3.7	31	Correction regarding other management/maintenance orders.

Correct the meaning of frame 22 $V_1(2)$ to:

"SU/SR alarm reset via channel line and CU".

	Ref Paragraph	Page	
R	4.3.3.6	31	Deleted
	4.3.3.7	31	Additional definitions regarding other management/maintenance orders.

$V_1(3)$	0011	Suppress RF receiver blocking alarm
$V_1(4)$	0100	Selftest
$V_1(12)$	1100	Cancel suppression of RF receiver blocking alarm

4.3.3.8 31 Correction regarding response on other management/maintenance orders.

Delete first sentence and add the following meaning of frame 27:

	"$V_1(2)$	0010	Acknowledge alarm reset
	$V_1(3)$	0011	Acknowledge SU/SR alarm reset via CU.
R	$V_1(4)$	0100	Acknowledge surpress RF-receiver blocking alarm.
	$V_1(5)$	0101	Acknowledge selftest.
	$V_1(6)$	0110	Selftest completed.
	$V_1(7)$	0111	Acknowledge RF test loop in.
	$V_1(10)$	1010	Acknowledge RF test loop out".
R	$V_1(13)$	1101	Acknowledge cancel supression of RF receiver blocking alarm.

4.3.3.9 31 Additional definitions regarding other maintenance information.

$V_1(10)$ $V_2(15)$ $V_3(2)$	Selftest failed
$V_1(10)$ $V_2(15)$ $V_3(5)$	RF receiver blocking alarm
$V_1(10)$ $V_2(15)$ $V_3(8)$	RF receiver blocking alarm ceasing

Ref Paragraph	Page				
R			$V_1(10)\ V_2(15)\ V_3(12)$	1100	Redundant power supply
R			$V_1(10)\ V_2(15)\ V_3(13)$	1101	Redundant master oscillator
R			$V_1(10)\ V_2(15)\ V_3(14)$	1110	Cooling fan fault
R			$V_1(10)\ V_2(15)\ V_3(15)$	1111	Redundant amplifier in receiver multicoupler

4.7.3 Add new paragraph.

4.7.3 • <u>False frame synchronization in BS</u>

Any number of false frame synchronization words within a frame shall be handled. The occurence of false frame synchronization words shall not cause frames to be lost.

However there exist a minor possibility that decoding of a frame after synchronization to a false synchronization word, will produce meaningful information. In such situations the above stated requirement need not to be fullfilled.

1988-07-01

SPECIFICATION FOR NMT-SIS KEY MANAGEMENT IN NMT-900

This specification specifies the requirements that are to be satisfied implementing security functions in the NMT-900 environment. Operational aspects such as the structure, generation, loading, storage and utilization of key variables are all treated together with cryptographical equipment controls.

LIST OF CONTENTS

1. PREFACE

The goal of this document is to specify key management for the subscriber identity security which will be introduced in NMT-900. Also some guidelines are given which could make the implementation of the security functions easier.

In this document the functional specification of a key management system for the NMT-900 system is given. The functional specification is based on the specification of the requirements for key-management, described in NMT-SIS Report: Descriptions of security functions in NMT-900.
It is described how the secret authentication keys (SAKs) are generated by the manufacturers, how they are installed in special security modules and how the SAK information is handed over to the administrations.

The main demand on a key management scenario for NMT-900 is that it should be infeasible to obtain corresponding ID-SAK pairs during the installation of the SAKs and IDs in MSs.

It is essential to design the system in a way that the overall security is maintained. A solution for a function in the key management system may look simple and attractive but it is very important to take the overall security in consideration before decision.

2. SCENARIO

The scenario chosen by NMT-SIS is shown in figure 1.
Two algorithms are used in the scenario. One, the so-called RSA algorithm, is used for enciphering the information which is sent to the administration and the other is used in the signalling procedures on the radiopath.
The scenario consists of the following steps.

1. On request of an MS-manufacturer, a unique RSA public key (manufacturers key), which is used to encipher SAKs, is sent to this manufacturer. The request should be addressed to the chairman of the NMT group. The MS-manufacturers key can be the same for all administrations.

2. The MS-manufacturers are responsible for generating SAKs and programming them together with the authentication algorithm in a security identity module (SIM). Each SIM shall be identified by a unique and non-SAK related reference number. This reference number shall also be programmed in the SIM. For testing purposes a common SAK shall be programmed into each SIM (see chapter 4.3).
   The SAKs are enciphered immediately after installation in a SIM using the MS-manufacturers key and the RSA algorithm in order to make them unreadable during the transportation from the manufacturers to the administrations.

3. A list with reference numbers and enciphered SAKs is sent by the MS-manufacturers to the administration(s), where the SAKs are stored to be deciphered at any convenient time. The administration(s) will to acknowledge the receipt of such a list. The MS-manufactures shall always be able to provide copies of any list sent by them to the administrations.

4. MSs with a SIM installed are sent to the retailers/local dealers.

5. For each MS which is sold, the retailer/local dealer sends an ID or an ID_Request together with the reference number of the SIM to the administration.

6. The administration selects and/or registers the ID. In the authentication centre the ID is coupled to a SAK. Triples (RAND,SRES,B-KEY) for this ID can then be generated.

7. Within the administration, the authentication centre uses the SAK to produce triples of RAND, SRES and B-KEY. These triples are sent to the MTX(s) to serve as authentication information.

8. The retailers/local dealers install the IDs (which are determined according to the normal procedure) in the MSs.

9. The subscriber receives his MS from the retailer/local dealer. The equipment is now ready for operation.

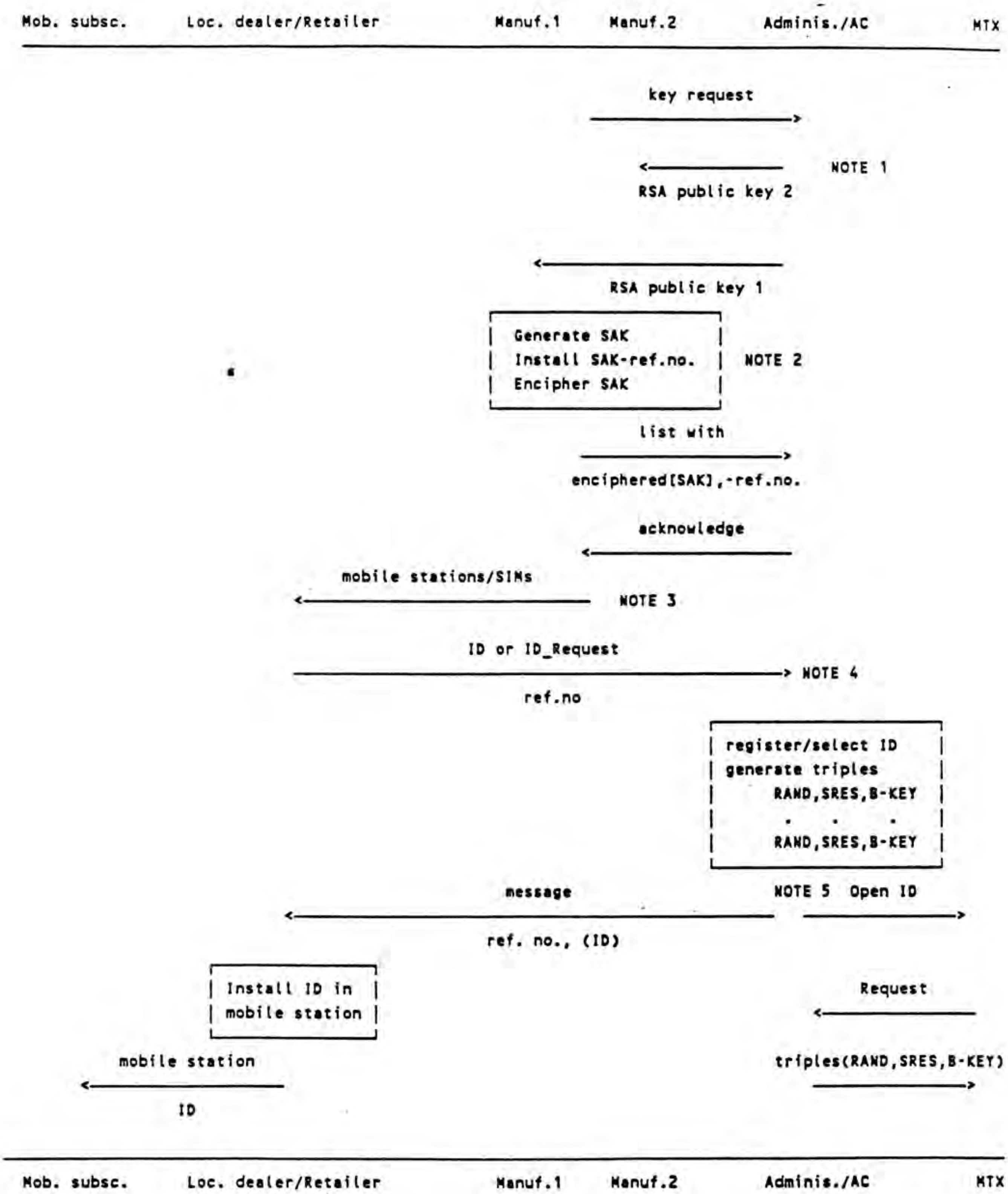

Mob. subsc.
Loc. dealer/Retailer
Manuf.1
Manuf.2
Adminis./AC
MTX
key request
NOTE 1
RSA public key 2
RSA public key 1
Generate SAK
Install SAK-ref.no.
Encipher SAK
NOTE 2
list with
enciphered[SAK],-ref.no.
acknowledge
mobile stations/SIMs
NOTE 3
ID or ID_Request
NOTE 4
ref.no
register/select ID
generate triples
RAND,SRES,B-KEY
. . .
RAND,SRES,B-KEY
message
NOTE 5
Open ID
ref. no., (ID)
Install ID in
mobile station
Request
mobile station
triples(RAND,SRES,B-KEY)
ID
Mob. subsc.
Loc. dealer/Retailer
Manuf.1
Manuf.2
Adminis./AC
MTX

Figure 1

NOTES

NOTE 1

1. On request, each manufacturer receives an RSA public key (manufacturers key) from the administrations. The request should be to the chairman of the NMT group, which will select the key. In principle, this key consists of two 512 bit numbers.
   There is no need to keep this key secret.

2. Each manufacturer uses the RSA algorithm to encipher lists of SAKs (see chapter 5 and appendix B).

3. The life time of the keys and the parameters of the algorithm may be limited. The administrations determine the life time of the keys and parameters.

NOTE 2

1. The MS-manufacturers will ensure that the SAKs are generated using the prescribed procedures (see chapter 4 and 5).

2. The SAKs should stay "inside" the device in which they are generated. This device should also be used to load SIMs with the SAK and to encipher the SAKs before transportation to the administration.

3. The SAKs should not be readable from the SIMs.

4. The reference numbers should be programmed in the SIM. It shall be possible to read out the reference number in a simple way, e.g. via the MS display.

5. List of enciphered SAKs and reference nos. are stored on a storage medium; (the SAKs are enciphered by means of the RSA algorithm and the MS-manufacturers key).

6. The MS-manufactures should keep a backup of each list sent by them to the administrations. They should always be able to provide the administrations with these backups.

NOTE 3

During the transportation of MSs from manufacturer to retailer the security of the SAKs is guaranteed, since the SAKs are not readable from the MSs.

NOTE 4

In the administration an ID is selected. This identity is, by means of the reference number, coupled to the SAK.

NOTE 5

The first triples (RAND,SRES,B-KEY) will be sent to the MTX on request of the MTX.

3. THE AUTHENTICATION CENTRE AND ITS INTERFACES

Procedures are defined for the communication between AC and administration and the communication between AC and MTXs. The administration can be divided in two functional parts. The first is a national subset or copy of an international database containing pairs consisting of the reference number of a security module and the corresponding enciphered SAK.
The second part is an administrative system containing, amongst general operational data, information on installed and in the country pre-operational security modules.
The communication structure between these two parts of the administration, the AC and the MTXs is detailed in figure 2 below.

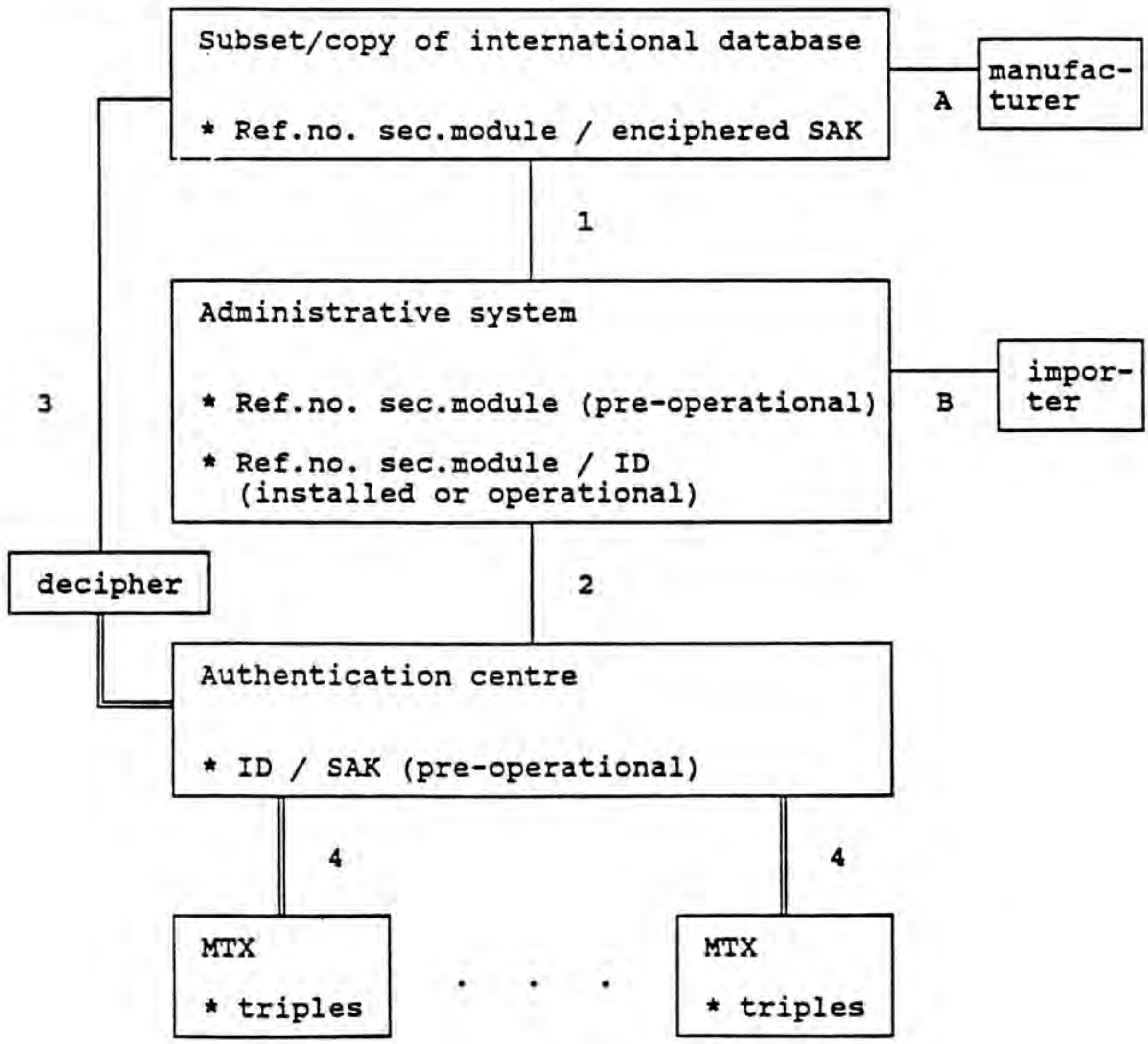


Figure 2

The national database gets its input from manufacturers of security modules via interface A and/or possibly from other administrations.
The administrative system gets its information on pre-operational reference numbers of security modules via importers, local dealers, etc. Furthermore the importers should link the reference numbers of the SIMs to the corresponding serial numbers of all the MSs imported by them. This information will be available for the administrations via interface B and will be used on a national basis for certain administrative functions.

Via interface 1, the administrative system is able to check if the (enciphered) SAK corresponding to a certain reference number is available in the database.

If an ID is put in to operation, the ID and the corresponding reference number of the security module are sent to the AC via interface 2. If the AC supports more than one MTX, at the same time it is indicated in which MTX(s) the ID has to be installed. Via interface 3 the AC sends the reference number to the database. The corresponding enciphered SAK is deciphered and sent back to the AC. This deciphering is done somewhere along this communication path. After deciphering the communication has to be secured (denoted by a double line in figure 2).

The ID / SAK is then installed in the AC.
The AC then calculates a initial number of (RAND / SRES / BKEY) triples for each MTX in which the ID has to be installed. These triples are sent to the MTX via interface 4.
Each MTX which is supported by an AC can request for a new triples for a certain ID either if a minimum level of triples is reached or if a not in the MTX installed ID reports for the first time. The communication between MTX and AC has to be secured (denoted by a double line in figure 2).

4. THE GENERATION, PROGRAMMING AND ENCIPHERING OF SAKS

The manufacturers should generate the SAK using a random generator (see appendix C). The total length of the SAK is 120 bits. The SAKs are programmed in SIMs. Lists of SAKs are enciphered at the SIM-manufacturers and then sent to the administration(s) by the MS manufacturers who will install these SIMs. These lists will be transferred by means of a generally accepted industrial standard storage medium, e.g. a floppy disk. The administrations will define standardised ways of input.

4.1 General requirements for generating, programming and enciphering SAKs

1. Generating SAKs, programming SAKs and enciphering SAKs should only be possible with special programming tools designed by the manufacturers and approved by the administrations. The programming procedures should only be known to people authorized to operate the programming tools.

2. Generating SAKs, programming SAKs and enciphering SAKs should be done in a consecutive order without unnecessary time delay.

3. With regard to the list of reference numbers and enciphered SAKs, the administration(s) will only recognize an interface with the MS-manufacturers (and not with SIM-manufacturers). The MS-manufacturers will receive the MS-manufacturers keys and will sent the list with enciphered SAKs. Whether or not the MS-manufacturers produces the SIMs themselves, they will be responsible that the SAKs are programmed, generated and enciphered according to the requirements stated in this report.

4.2 Generation of the SAK

The SAK is divided into six parts

$$SAK = (K1 \mid K2 \mid K3 \mid K4 \mid K5 \mid K6) .$$

In this description the left most bit is the most significant. The following requirements should be fulfilled.

1. The length of K1 is 16 bits.

2. The length of K2 is 32 bits.

3. The length of K3 is 48 bits.

4. The length of K4, K5 and K6 is 8 bits.

5. The first bit (i.e. the most significant bit) of K1, K2 and K3 is fixed to 1.

6. The SAKs should be generated by a good random generator.

7. K1 should contain at least 2 zeros and at least 2 ones.

8. K2 should contain at least 4 zeros and at least 4 ones.

9. K3 should contain at least 6 zeros and at least 6 ones.

10. The value of K3 should not be divisible by any prime less then 5000.

4.3 Testing authentication function

In order to test the proper functioning of a SIM, in each module a test SAK will be installed. This test SAK will be common for all SIMs. Selection of an MS test mode to select this test SAK shall become available.
The value of this test SAK is been set to

$$K1 = 2^{15} + 1 = (8001)_{hex}$$
$$K2 = 2^{31} + 1 = (80000001)_{hex}$$
$$K3 = 2^{47} + 1 = (800000000001)_{hex}$$
$$K4 = K5 = K6 = 0 = (00)_{hex}$$

4.4 Reprogramming of the SAK

Reprogramming of the SAK in a SIM shall not be possible. If the SAK in a mobile station, for some reason, has to be replaced, a new SIM shall be installed in the MS.

5. DATA FORMATS

In this chapter the format of data, which will be needed in the key management, is specified.

5.1 MS-manufacturers number

Each MS-manufacturer gets an identification number, the manufacturers number. The MS-manufacturers numbers will be specified by international agreement. The MS-manufacturer number consists of a 10 bit number between 0 and 1023:

manu. no.	
9	0

uniquely identifying the manufacturer.

5.2 Key indicator for manufacturers key

Each manufacturers key should be uniquely identified by a key indicator which is established by the administrations. The key indicator will be a 28 bit number:

manu. no.				check sum	
27	18	17	8	7	0

The first 10 bits (27-18) represent the manufacturers number. The following 10 bits (17-8) represent a number between 0 and 1023.
The last byte (bit 7-0) is a check sum which is formed by adding modulo 256 the three information bytes formed by respectively the bits 15 to 8, the bits 23 to 16 and the bits 27 to 24 preceded by four zeros.
Here, the left most bits, i.e. the bits with the highest indices, are the most significant bits. (Note that the third of the three information bytes always has a value less then 16.)

5.3 Reference number

Each SIM will be identified by a unique reference number. This reference number is a 48 bit number:

manu. no.		day		month		year				chk.sum	
47	38	37	33	32	29	28	22	21	8	7	0

The first 10 bits (47-38) represent the MS-manufacturers number. The following 16 bits (37-22) represent the date: position 37-33 the day (value 00-31), position 32-29 the month (value 00-12) and position 28-22 the year (value 00-99).
The following 14 bits (21-8) represent a number between 0 and 16383. The manufacturers must use this field in such a way, that the reference number uniquely identifies a specific SAK (e.g. by using the production sequence number of this SIM).
The last byte (bit 7-0) is a check sum which is formed by adding modulo 256 the five information bytes formed by respectively the bits 15 to 8, the bits 23 to 16, the bits 31 to 24, the bits 39 to 32 and the bits 47 to 40.
In this description, the left most bits, i.e. the bits with the highest indices, are the most significant bits.

5.4 SAK

Before the SAK is enciphered an check byte shall be added, The SAK will have the following data format.

K1		K2		K3		K4		K5		K6		chk.sum	
127	112	111	80	79	32	31	24	23	16	15	8	7	0

The first 120 bits (127-8) contain the key parts K1, K2, ... K6 as described in 4.2.

The last byte (bit 7-0) is a check sum which is formed by adding modulo 256 the fifteen information bytes formed by respectively the bits 15 to 8, the bits 23 to 16, the bits 31 to 24, ... , the bits 119 to 112 and the bits 127 to 120.
In this description, the left most bits, i.e. the bits with the highest indices, are the most significant bits.

5.4 List with reference number - enciphered SAK

The list with reference number - enciphered SAK which is sent by the manufacturer to the administration as an ASCII file and should contain a heading and a number of records of the following form:

Heading				
Ref. no. 1	Cryptogram 1	chk	cr	lf
Ref. no. 2	Cryptogram 2	chk	cr	lf
Ref. no. 3	Cryptogram 3	chk	cr	lf
.	.			
.	.			
.	.			
.	.			
Ref. no. r	Cryptogram r	chk	cr	lf
hexadecimal check digits		chk	cr	lf

The heading should be in "readable" ASCII. In the following, the heading is described in detail. It begins with the text "START HEADING" and ends with the text "END HEADING". The format, layout and underlined text should be taken over literally.

```
0   0    1    1    2    2    3    3    4    4    5    5    6    6
1...5....0....5....0....5....0....5....0....5....0....5....0....5

START HEADING
nnnn          manufacturer number
fff           floppy number
yy/mm/dd      date
kkkkkkkk      key indicator
rrrrr         number of records

eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
END HEADING

0   0    1    1    2    2    3    3    4    4    5    5    6    6
1...5....0....5....0....5....0....5....0....5....0....5....0....5
```

Here,

- nnnn is the 4-digit MS manufacturer number between 0000 and 1023 described in 5.1,
- fff is unique number between 000 and 999 determined by the manufacturer,
- yy, mm, dd are the normal two digit representations for respectively, the year, month and day of production of the floppy,
- kkkkkkkk is the decimal representation of the key indicator described in 5.2; the first 4 digit should be the MS-manufacturers number and the last four a number between 0000 and 1023,
- rrrrr is the number of ref.no/cryptogram records to follow, a number between 00001 and 99999,
- the string of 8*64=512 e's is the RSA exponent which was used (see appendix B); each e represents a 0 or a 1; the first e is the most significant,

- the string of 8*64=512 M's is the RSA modules which was used (see appendix B); each M represents a 0 or a 1; the first M is the most significant,
- the first ref.no/cryptogram record is placed on the first line after the line with the text "END HEADING".

A cryptogram is obtained by enciphering the following entry with the manufacturers key and the RSA algorithm (see appendix B):

begin	SAK	ref.no.	SAK	key ind.	SAK	end
503 480	479 352	351 304	303 176	175 148	147 20	19 0

Here, "begin" and "end" should contain random information which, in principle, should be different for every entry.
"Ref.no." and "key ind." are the reference number and the key indicator.
"SAK" is the actual SAK which is installed in the SIM identified by the reference number with the check byte (see 5.4)
The length of the cryptogram will be between 504 and 512 bits depending on the length of the parameters of the RSA algorithm.

A ref.no./cryptogram record is stored in the following way. The string ref.no/cryptogram has a length of 560 bits. These are divided in 160 groups of 4 bits. The corresponding hexadecimal value of a four bit group (0,1,2,...,9,A,B,...,F) is then stored in ASCII on the storage medium. Again, the left most bits are most significant. A hexadecimal check digit is added to this record. This check digit is obtained by adding modulo 16 the values of the 160 hexadecimal information digits. The record is completed by the carriage return and line feed ASCII characters.

The file ends with a record of 161 hexadecimal check digits. Each of these check digits is obtained by adding modulo 16 the values of the hexadecimal digits of all the rrrrr records in the corresponding column. (Note that the last hexadecimal digit is a check digit for both the row and column check digits.)

APPENDIX A LIST OF ABBREVIATIONS

NMT	Nordic Mobile Telephone
MS	Mobile Station
ID	IDentity of mobile station
SAK	Secret Authentication Key
AC	Authentication Centre
SIM	Security Identity Module

APPENDIX B DESCRIPTION OF THE RSA ALGORITHM

The RSA algorithm is a so-called public key algorithm for which it is not necessary to keep the enciphering key secret.

To use the RSA algorithm, first two large prime numbers (about 256 bits), p and q, have to be established.
The product of these primes, m=p*q, should have a length of at most 512 bits (i.e. should be less than 2^{512}).
Futhermore, the number m should be larger than 2^{504}.

Secondly a number e, with 0 < e < (p-1)*(q-1), is chosen such that e is relatively prime to (p-1)*(q-1) and then a second number d satisfying

$$e*d = 1 \bmod (p-1)*(q-1) .$$

These two operations can be combined and very fast be carried out using modifications of Euclid's Algorithm [1].

The pair (e,m) is the public key which is used by the manufacturers to encipher the SAK information as described in 4.4. There is no need to keep this key secret.
If x is the information to be enciphered, the cryptogram y becomes

$$y = x^e \bmod m$$

Deciphering can be done with the secret key d:

$$x = y^d \bmod m$$

Example.
Choose p=5, q=11. Then m=55 and (p-1)*(q-1) =40 and (e=3, d=27) is a key pair.
Let x=4, then the cryptogram becomes x^e = 64 = 9 mod m.
This is deciphered as 9^{27} which indeed is 4 mod m.

Establishing keys.
The problem of establishing keys is finding large primes.
As stated above p and q should be primes in the order of 2^{256}

such that $2^{504} < m=p*q < 2^{512}$. Furthermore, p-1 and q-1 should contain large prime factors. The best choice is p = 2*P+1 and q= 2*Q+1, where P and Q are also prime.
The best way to find suitable primes, is to randomly choose a number of the right magnitude and then to test if it is prime. For numbers in the order of 2^{256}, on the average one out of each 125 odd numbers is a prime.

Several fast primality test for large numbers exist ([2], [3]). One practical one is Miller's test [4] which is based on the following theorem.*

THEOREM. Suppose 2 <= b < m and let $m-1 = 2^{s}*Q$, with Q odd. If b^{Q} is not equal 1 mod m and if, for all i=0,1,2,...,s-1, $b^{2^{i}Q}$ is not equal to m-1 mod m, then m is not a prime.

To test if m is prime, n random numbers b between 2 and m are chosen and the test described by the theorem is applied. It can be proven that the chance of a non-prime number passing the test, is at most 4^{-n}. Therefore a number of 20 choices for b should sufficient to determine wether a number is prime or not with enough certainty.

Several software and hardware tools (e.g. PC cards) supporting the RSA algorithm are available.

[1] Knuth, D. E., "The art of computer programming vol 2/ Seminumerical Algorithms 2nd ed." Addison Wesley, 1981.

[2] Kranakis, E., "Primality and Cryptography" Wiley, New York, 1986.

[3] Riesel, H., "Prime Numbers and Computer Methods for Factorization" Birkhauser, Boston, 1985.

[4] Miller, G.L., "Riemann's hypothesis and tests for primality" J. Comput. System Sci., vol. 13, pp. 300-317, 1976.

APPENDIX C DESCRIPTION OF A RANDOM GENERATOR

As stated in Section 3, the 120-bit SAK has to be generated randomly, with the exception of the most significant bits of K1, K2 and K3 which are set to one. In this Appendix a possible method for generating the remaining 117 bits of the SAK is described. It should be noted that there exist better random generators than the one described below. However, they are more complex and probably not suitable for this application.

C.1 The linear congruential method.

The generator for 120-bit integers is based on the well-known linear congruential generator (LCG). A short description of this generator is given here. For more details see D.E. Knuth, The Art of Computer Programming, part 2: Seminumerical Algorithms (Addison-Wesley, Reading Mass., 1981).

First of all the following four integers are chosen:

$m > 0$: the modulus of the sequence,
$1 < a < m$: the multiplier of the sequence,
$0 <= c < m$: the increment of the sequence and
$0 < X_0 < m$: the seed of the sequence.

The desired linear congruential sequence (X_n) of random numbers is then obtained by setting

$$X_n := (a * X_{n-1} + c) \bmod m, \; n > 0. \tag{1}$$

Because the elements of the sequence can only take values between 0 and m-1, it is clear that after a certain value of n the sequence will repeat itself. This value of n is called the period of the sequence. The following property is of importance.

PROPERTY: Let m be a prime and assume that $c = 0$, $a > 1$ and $X_0 > 0$. Then the sequence generated by (1) will have period m-1.

It this application the following sequence will be used:

$$X_n := a * X_{n-1} \bmod (2^{127}-1), \; n > 0, \qquad (2)$$

where a and X_0 are chosen randomly. By the property above this sequence will have period $2^{127}-2$, which is about $1.7*10^{38}$, because $2^{127}-1$ is a prime. Also it should be noted that arithmetic modulo $2^{127}-1$ is very easy. Let y be the result of the integer multiplication $a*X_{n-1}$. Clearly y will consist of at most 254 bits and thus it can be written as

$$y = y_1 + 2^{127} * y_2, \; 0 <= y_1, \; y_2 < 2^{127}. \qquad (3)$$

Because $2^{127} \bmod (2^{127}-1) = 1$, it follows from (2) and (3) that

$$X_n = (y_1 + y_2) \bmod (2^{127}-1), \qquad (4)$$

which is easy to compute.

C.2 A random generator for 117-bit integers.

As stated above, the generator will use the linear congruence sequence (X_n) defined by (2). The sequence (X_n) consists of 127-bit integers. To reduce these integers to 117-bit integers the following functions will be needed.

Let $0 <= u < 15$ be an integer. A 127-bit integer is written as

$$x = x_0 + x_1 * 256 + x_2 * 256^2 + \ldots + x_{15} * 256^{15}, \qquad (5)$$

where $0 <= x_i < 256$, i=0,1,..15 are the bytes of x (note that x_{15} is less than 128). The function f_u maps x onto the 117-bit integer that is obtained by deleting the u-th byte of x and the 2 most significant bits of x. The function g_u maps x onto the 10-bit integer obtained by concatenating the u-th byte of x and the 2 most significant bits of x. More precisely,

$$\begin{aligned} f_u(x) := \; & x_0 + x_1 * 256 + \ldots + x_{u-1} * 256^{u-1} + \\ & + x_{u+1} * 256^u + x_{u+2} * 256^{u+1} + \ldots + x_{14} * 256^{13} + \\ & + (x_{15} \bmod 32) 256^{14}. \end{aligned}$$

$g_u(x) := x_u + (x_{15}$ div $32)*256$.

Now let N be the number of keys to be generated and let k, r and s be fixed integers. The random 117-bit integers Z_n (n=1,2,...,N) are computed as follows.

INITIALISATION

1. Choose randomly the following integers:
   $0 <= j < k$, $0 <= u < 15$, $2^{126} <= a < 2^{127}-1$ and
   $1 < X_0 < 2^{127}-1$.
2. Make a table V[0..k-1] by defining
   $V[0] := X_0$;
   $V[i] := X_i = a*X_{i-1} \bmod (2^{127}-1)$, $0 < i < k$.

STEP FOR n = -(s-1),-(s-2),...,0,1,...,N

1. Let Y:= V[j] and compute
   $X_{n+k+s-1} := a*X_{n+k+s-2} \bmod (2^{127}-1)$.
2. Put $V[j] := X_{n+k+s-1}$,
   $Z_n := f_u(Y)$,
   $j := (k*g_u(Y))$ div 2^{10}.
3. If (n - s) mod r = 0 then generate a new integer 0 <= u < 15.

The steps for n = -(s-1),-(s-2),...,0 can be seen as part of the initialisation procedure. The parameter k should be odd and of order 100, for example k = 99 is a good choice. The parameter s can be taken as s = 3k. The integer u, 0 <= u < 15 is changed after r steps. It is advisable to take r reasonably small, say r = 10. The integer u can be obtained in the following way. Let f be the 6 least significant bits of the fraction in milliseconds of the system time of the computer system when a new u has to be generated. The new u is then defined as u := (15*f) div 64.

The starting values j, a and X_0 should be changed regularly, for example once every three months. A way to generate these values using the system time of the computer system is explained below.

Type the alphabet twice on a terminal and record each time a key is stricken the fraction in milliseconds of the system time. By taking the 6 least significant bits of these fractions one obtains 52 random numbers d_0, d_1, ..., d_{51} with $0 <= d_i < 64$. We then can define

$$a := d_0 + d_1*64 + ... + d_{20}*64^{20} + 2^{126},$$
$$X_0 := d_{21} + d_{22}*64 + ... + d_{40}*64^{20} + (d_{41} \bmod 2)*2^{126}.$$
$$j := (k*d_{42}) \operatorname{div} 64.$$

Note that these values must satisfy the conditions stated in block 1 of the initialisation above. If one or more of these values do not satisfy these conditions one can generate new values the same way as described above. Also, one has to check whether the SAK's obtained this way satisfy the conditions of Section 3.