ETSI TS 101 638 V8.0.1 (2000-04)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Packet Data on Signalling channels service (PDS)
Service description;
Stage 3
(GSM 04.63 version 8.0.1 Release 1999)

Reference
RTS/SMG-030463Q8

Keywords
Digital cellular telecommunications system,
Global System for Mobile communications (GSM)

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights 5
Foreword 5
1 Scope 6
2 References 6
3 Definitions and abbreviations 6
3.1 Definitions 6
3.2 Abbreviations 7
4 Applicability 7
5 Main concepts 7
6 Elementary procedures for PDSS1 8
6.1 Overview 8
6.2 Procedures for establishment of a PDSS1 connection 8
6.3 Procedures for release and termination of a PDSS1 connection 9
6.4 Procedures for the information phase of a PDSS1 connection 9
6.4.1 Resumption of a connection 10
7 Elementary procedures for PDSS2 10
7.1 Overview 10
7.2 Procedures for establishment of a PDSS2 connection 11
7.3 Procedures for release and termination of a PDSS1 connection 12
7.4 Procedures for the information phase of a PDSS2 connection 12
8 Handling of unknown, unforeseen, and erroneous protocol data 13
8.1 General 13
8.2 Message too short 13
8.3 Unknown or unforeseen transaction identifier 14
8.4 Unknown or unforeseen message type 14
8.5 Non-semantical mandatory information element errors 14
8.5.1 Special cases 15
8.6 Unknown and unforeseen information elements in the non-imperative message part 15
8.6.1 Information elements unknown in the message 15
8.6.2 Out of sequence information elements 15
8.6.3 Repeated Information elements 16
8.7 Non-imperative message part errors 16
8.7.1 Syntactically incorrect optional Information elements 16
8.8 Messages with semantically incorrect contents 16
9 MESSAGE FUNCTIONAL DEFINITIONS AND CONTENTS 16
9.1 DATA 18
9.1.1 Data 18
9.2 IMMEDIATE SETUP 19
9.2.1 Ciphering key sequence number 19
9.2.1 Data 19
9.3 RELEASE COMPLETE 20
9.3.1 Data 20
9.3.2 Cause 2 20
9.4 SETUP 21
9.4.1 Data 21
9.5 SETUP ACKNOWLEDGE 22
9.5.1 Data 22
9.6 RESUME 23
9.6.1 Ciphering key sequence number 23
9.7 RESUME ACK 24
9.8 STATUS 24

9.8.1 Cause 2 24
10.1 Overview 25
10.2 Protocol Discriminator 25
10.3 Transaction identifier 25
10.4 Message Type 25
10.5 Other information elements 25
10.5.1 Application 25
10.5.2 Cause 26
10.5.3 Data 27
10.5.4 Mobile identity 2 27
10.5.5 Spare Half Octet 28

Annex A (informative): Change Request History 29

History 30

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by the Special Mobile Group (SMG).

The present document provides a mechanism giving reliable transfer of signalling messages within the digital cellular telecommunications system (Phase 2/Phase 2+).

The contents of the present document is subject to continuing work within SMG and may change following formal SMG approval. Should SMG modify the contents of the present document it will be re-released with an identifying change of release date and an increase in version number as follows:

Version 8.x.y

where:

8 indicates Release 1999 of GSM Phase 2+.

x the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

y the third digit is incremented when editorial only changes have been incorporated in the specification.

1 Scope

The present document specifies the protocols for connection management of packet data on signalling channels which is applied on the air interface, the PDSS1 protocol and the PDSS2 protocol.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1999 document, references to GSM documents are for Release 1999 versions (version 8.x.y).

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM 02.63: "Digital cellular telecommunications system (Phase 2+); Packet Data on Signalling channels service (PDS) Service description, Stage 1".

[6] GSM 03.63: "Digital cellular telecommunications system (Phase 2+); Packet Data on Signalling channels service (PDS) Service description, Stage 2".

[3] GSM 04.06: "Digital cellular telecommunications system (Phase 2+); Mobile Station - Base Station System (MS - BSS) interface Data Link (DL) layer specification".

[4] GSM 04.07: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface signalling layer 3 General aspects".

[5] GSM 04.08: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".

[7] GSM 08.56: "Digital cellular telecommunications system (Phase 2+); Base Station Controller - Base Transceiver Station (BSC - BTS) interface Layer 2 specification".

3 Definitions and abbreviations

3.1 Definitions

Definitions used in the present document are also defined in GSM 02.63 and GSM 04.07.

Idle phase: A protocol entity is in the idle phase when.

TI flag: See GSM 04.07.

Transaction Identifier (TI): See GSM 04.07.

3.2 Abbreviations

Abbreviations used in the present document are also listed in GSM 01.04 [1].

For the purposes of the present document, the following abbreviations apply:

CM:	Connection Management
MM:	(See GSM 04.07)
PDSS1:	Packet Data on Signalling channels Service 1
PDSS2:	Packet Data on Signalling channels Service 2
RR:	(See GSM 04.07)
TI:	Transaction Identifier

4 Applicability

Support of the PDSS1 protocol is optional in the mobile station and in the network. Support of the PDSS2 protocol is optional in the mobile station and in the network.

If a mobile station supports the PDSS1 protocol, it must support it on both the main and the slow associated data link.

5 Main concepts

The present document specifies the protocols for connection management of packet data on signalling channels which is applied on the air interface: the

- PDSS1 (Packet Data on Signalling channels Service 1) protocol, and the
- PDSS2 (Packet Data on Signalling channels Service 2) protocol.

Both are protocols of the Connection Management (CM) sublayer (see GSM 04.07).

PDSS1 and PDSS2 transactions can be active in parallel to other CM transactions.

A PDSS1 transaction may be initiated by the mobile station or the network. A PDSS2 transaction shall only be initiated by the mobile station.

The present document describes the PDSS1 and PDSS2 protocols with regard to two peer entities, one in a mobile station, the other one in the network. The call control entities are described as communicating finite state machines which exchange messages across the radio interface and communicate internally with other protocol (sub)layers.(see note[In the model, for PDSS1, for each Transaction Identifier (TI) value there are two protocol entities in the mobile station and two protocol entities in the network: one which may originate a transaction and one which may use the transaction originated bt its peer entity; the protocol entity receiving messages with a given TI and TI flag value x may send messages with equal TI value and with TI flag value (1-x) mod 2. The originator uses TI flag value 0. A protocol entity is idle (also called: in the idle phase) until it has received a message from its peer entity or lower or higher layers have passed an abstract service primitive to it.

[NOTE: Text not yet approved for this version].

In particular, the

- PDSS1 protocol uses the MM and RR sublayer specified in GSM 04.08, and the
- PDSS2 protocol uses the RR sublayer specified in GSM 04.08.

This description in only normative as far as the consequential externally observable behaviour is concerned.

Certain sequences of actions of the two peer entities compose "elementary procedures" which are used as a basis for the description in the present document. These elementary procedures are defined in section 6 and 7.

NOTE: Whereas PDSS1 provides connections between mobile station and MSC, PDSS2 provides connections between the mobile station and the PDSS2 support node, see GSM 03.63.

The mobile station receives on lower sublayers information from the network whether the mobile station is allowed to establish a PDSS1 and/or PDSS2 connection. The network is informed by the mobile station in the classmark whether the mobile station supports PDSS1 and/or PDSS2.

The PDSS1 and PDSS2 protocols may use the main signalling link or the slow associated signalling link for communication, always on the SAP with SAPI=0 and in acknowledged mode (for the definition of these terms, see GSM 04.06). It is informed by the network whether it is allowed to establish a PDSS1 and/or PDSS2 connection by sending the SETUP and/or the IMMEDIATE SETUP message on the main signalling link and/or slow associated signalling link. If the mobile station supports PDSS1 and/or PDSS2, it shall be able to receive messages of the supported protocol(s) on both data links. Once a protocol entity in the mobile station has received a message, the mobile station shall send any further message pertaining to the same transaction on the data link on which it had received the last message.

6 Elementary procedures for PDSS1

6.1 Overview

The elementary procedures for PDSS1 may be grouped into the following classes:

- PDSS1 establishment procedures.
- PDSS1 termination procedures.
- PDSS1 information phase procedures.

6.2 Procedures for establishment of a PDSS1 connection

The PDSS1 protocol entity in the mobile station or network in the idle phase shall on request of higher layers to establish a connection, analyse the request: the request contains all information necessary for the SETUP message and an indication whether the main or slow associated data link is to be used. The PDSS1 protocol entity shall then verify whether:

1) use of the indicated link for PDSS1 is possible and allowed;

and ask the MM sublayer whether:

2) establishment of a PDSS1 connection is possible and allowed.

   - If one of these conditions is not fulfilled, the request is rejected.
   - If the MM connection establishment is possible and allowed and the use of the indicated link is possible and allowed, the PDSS1 protocol entity asks the MM sublayer to establish an MM connection. The request contains a SETUP message to be transferred to the peer entity. The request from higher layers may already contain data to be transferred which does not exceed a maximum allowed length. In this case the data is included in the SETUP message.
   - If the MM connection establishment fails or is rejected, the PDSS1 protocol entity aborts the establishment and gives an appropriate information to higher layers; it then returns to the idle phase.

An idle PDSS1 protocol entity shall on receipt of a SETUP message inform higher layers. If the SETUP message contained a data part, it passes the data part to higher layers and then continues as follows:

- If higher layers accept the establishment, the PDSS1 protocol entity shall send a SETUP ACKNOWLEDGE message to its peer entity and enter the PDSS1 information transfer phase. The acceptance from higher layers may already contain data to be transferred which does not exceed a maximum allowed length. In this case the data is included in the SETUP ACKNOWLEDGE message.

- If higher layers reject the establishment, the PDSS1 protocol entity shall send a RELEASE COMPLETE message with appropriate cause to its peer entity.

When a PDSS1 has transferred a SETUP message to its peer entity and receives as an answer a SETUP ACKNOWLEDGE message, it informs higher layers and enters the PDSS1 information transfer phase.

Abnormal cases

1) If during the establishment of a PDSS1 connection higher layers decide to abort the establishment, the PDSS1 protocol entity shall react as specified in subclause 6.3.

2) If during the establishment of a PDSS1 connection a lower layer failure occurs, the PDSS1 protocol entity shall abort the establishment and inform higher layers.

3) If the request from higher layers to establish a connection contained data with more than the maximum allowed length, the protocol entity shall reject the request with appropriate cause.

4) If the response from higher layers to accept a connection contained data with more than the maximum allowed length, the protocol entity shall reject the response with appropriate cause and then wait for further action from higher layers.

5) If after having informed higher layers that a SETUP has been received, no valid response was received from higher layers within 5 seconds, the protocol entity shall send a RELEASE COMPLETE message to its peer entity and inform higher layers that the connection establishment has been aborted.

6) If after having sent the SETUP message, no valid response was received from the peer entity within 10 + 10·T200·(N DIV N201) seconds (where N is the number of octets the SETUP message consisted of and T200 and N201 are as defined in GSM 04.06 for the used channel), the protocol entity shall send a RELEASE COMPLETE message to its peer entity and inform higher layers that and why the connection establishment has been aborted.

6.3 Procedures for release and termination of a PDSS1 connection

If during the establishment or information phase of a PDSS1 connection higher layers request to abort the establishment or to terminate the connection, the PDSS1 protocol entity:

- if it has sent or received the SETUP message, shall send a RELEASE COMPLETE message and then ask MM to release the MM connection; the request from higher layers may contain data to be transferred which does not exceed a maximum allowed length; in this case the data shall be included in the RELEASE COMPLETE message;

- otherwise shall ask MM to release the MM connection.

If during the establishment or information phase of a PDSS1 connection a PDSS1 protocol entity receives a RELEASE COMPLETE message from its peer entity, it shall inform higher layers and ask MM to release the MM connection. If the RELEASE COMPLETE message contains a data part, the data part is passed to higher layers.

Abnormal cases:

If the request from higher layers to abort or terminate the connection contained data with more than the maximum allowed length, the protocol entity shall send a RELEASE COMPLETE message without data part to its peer entity, and inform higher layers about the situation.

6.4 Procedures for the information phase of a PDSS1 connection

During the information phase of a PDSS1 connection, higher layers may request the transfer of data which does not exceed a maximum allowed length. The PDSS1 protocol entity then sends the data to its peer entity in a DATA message.

NOTE: Higher layers may apply activity supervision and, e.g., release a PDSS1 connection when it has been idle for a longer period.

Abnormal cases:

1) If during the information phase of a PDSS1 connection, a lower layer failure occurs, the PDSS1 protocol entity informs higher layers that the data transfer is suspended; if possible and allowed, the PDSS1 protocol entity asks MM to re-establish the MM connection. If the re-establishment is successful, the PDSS1 protocol entity proceeds as defined in subclause 6.4.1. If the re-establishment is unsuccessful, higher layers are informed that the connection is aborted.

2) If during the information phase of a PDSS1 connection, the PDSS1 protocol entity becomes aware that too much data is waiting for transmission ("congestion condition"), it informs higher layers that the data transfer is suspended. If the PDSS1 protocol entity later becomes aware that the congestion condition no more exists, it informs higher layers that data transfer can be resumed.

3) If the request from higher layers to transfer data contained data with more than the maximum allowed length, the protocol entity shall reject the request with appropriate cause.

6.4.1 Resumption of a connection

During a connection, after a radio link failure the MS shall try to initiate CM re-establishment. If a cell supporting re-establishment has been found and the CM re-establishment has been accepted by MM, the MS shall try to resume the PDSS1 connection:

- When the MS receives a message with the transaction identifier of the PDSS1 connection, it shall:
  - if it is a PDSS1 DATA message, implicitly resume that connection;
  - if it is a PDSS1 SETUP message, release that connection and treat the SETUP as the first message of a new transaction;
  - if it is a PDSS1 RELEASE COMPLETE message, release that connection;
- if it did not yet perform such a release or implicit resumption, send a PDSS1 RESUME REQUEST which may be:
  - explicitly acknowledged by the network with a PDSS1 RESUME ACK, or
  - implicitly accepted by the network with transmission of a DATA message, or
  - implicitly rejected by the network with the transmission of a PDSS1 SETUP, or
  - explicitly rejected by the network with the transmission of a PDSS1 RELEASE COMPLETE message;

  (all these messages with the same transaction identification).

7 Elementary procedures for PDSS2

7.1 Overview

The elementary procedures for PDSS2 may be grouped into the following classes:

- PDSS2 establishment procedures.
- PDSS2 termination procedures.
- PDSS2 information phase procedures.

7.2 Procedures for establishment of a PDSS2 connection

The PDSS2 protocol entity in the mobile station in the idle phase shall on request of higher layers to establish a connection, analyse the request: the request contains all information necessary for the IMMEDIATE SETUP message and an indication whether the main or slow associated data link is to be used. The PDSS2 protocol entity shall then verify whether:

1) use of the indicated link for PDSS2 is possible and allowed;

and whether

2) establishment of a PDSS2 connection is possible and allowed.

- If one of these conditions is not fulfilled, the request is rejected.

- If the PDSS2 connection establishment is possible and allowed and the use of the indicated link is possible and allowed, the PDSS2 protocol entity asks the RR sublayer to establish an RR connection. The request contains an IMMEDIATE SETUP message to be transferred to the peer entity. The request from higher layers may already contain data to be transferred which does not exceed a maximum allowed length. In this case the data is included in the IMMEDIATE SETUP message.

  If the RR connection establishment fails or the PDSS2 connection establishment is rejected, the PDSS2 protocol entity aborts the establishment and gives an appropriate information to higher layers; it then returns to the idle phase.

An idle PDSS2 protocol entity in the network shall on receipt of an IMMEDIATE SETUP message inform higher layers. If the IMMEDIATE SETUP message contained a data part, it passes the data part to higher layers and then continues as follows:

- If higher layers accept the establishment, the PDSS2 protocol entity shall send a SETUP ACKNOWLEDGE message to its peer entity and enter the PDSS2 information transfer phase. The acceptance from higher layers may already contain data to be transferred which does not exceed a maximum allowed length. In this case the data is included in the SETUP ACKNOWLEDGE message.

- If higher layers reject the establishment, the PDSS2 protocol entity shall send a RELEASE COMPLETE message with appropriate cause to its peer entity.

When a PDSS2 protocol entity in the mobile station has transferred an IMMEDIATE SETUP message to its peer entity and receives as an answer a SETUP ACKNOWLEDGE message, it informs higher layers and enters the PDSS2 information transfer phase.

Abnormal cases

1) If during the establishment of a PDSS2 connection higher layers decide to abort the establishment, the PDSS2 protocol entity shall react as specified in subclause 6.3.

2) If during the establishment of a PDSS2 connection a lower layer failure occurs, the PDSS2 protocol entity shall abort the establishment and inform higher layers.

3) If the request from higher layers to establish a connection contained data with more than the maximum allowed length, the protocol entity shall reject the request with appropriate cause.

4) If the response from higher layers to accept a connection contained data with more than the maximum allowed length, the protocol entity shall reject the response with appropriate cause and then wait for further action from higher layers.

5) If after having informed higher layers that an IMMEDIATE SETUP has been received, no valid response was received from higher layers within 5 seconds, the protocol entity shall send a RELEASE COMPLETE message to its peer entity and inform higher layers that the connection establishment has been aborted.

6) If after having sent the IMMEDIATE SETUP message, no valid response was received from the peer entity within 10 seconds, the protocol entity shall send a RELEASE COMPLETE message to its peer entity and inform higher layers that and why the connection establishment has been aborted.

7.3 Procedures for release and termination of a PDSS1 connection

These procedures are identical to those specified for PDSS1 in subclause 6.3.

7.4 Procedures for the information phase of a PDSS2 connection

During the information phase of a PDSS2 connection, higher layers may request the transfer of data which does not exceed a maximum allowed length. The PDSS2 protocol entity then sends the data to its peer entity in a DATA message.

NOTE: Higher layers may apply activity supervision and, e.g., release a PDSS2 connection when it has been idle for a longer period.

Abnormal cases:

1) During a PDSS2 connection;

(A) after a change of the radio channel (assignment or handover) and the corresponding L2 SAPI 0 establishment or re-establishment (at return to the old channel) the MS shall regard the PDSS2 connection as suspended. It shall then try to resume the connection:

- When the MS receives a message with the transaction identifier of the PDSS2 connection, it shall
  - if it is a PDSS2 DATA message, implicitly resume that connection;
  - if it is a PDSS2 RELEASE COMPLETE message, release that connection.
- If the MS did not yet perform such a release or implicit resumption, it shall send a PDSS2 RESUME REQUEST which may be:
  - explicitly acknowledged by the network with a PDSS2 RESUME ACK, or
  - implicitly accepted by the network with transmission of a DATA message, or
  - explicitly rejected by the network with the transmission of a PDSS2 RELEASE COMPLETE message;

  (all these messages with the same transaction identification).

NOTE: After having transferred the HANDOVER COMPLETE or ASSIGNMENT COMPLETE message, layer two will schedule the remaining part of an PDSS2 message, if there is any, for transmission, so that the network layer 3 may receive a PDSS2 message after the change of radio channel which was required to be transferred by the mobile station PDSS2 protocol entity before it received the indication about the channel change. Cf. GSM 04.06.

(B) after a radio link failure the MS shall regard the PDSS2 connection as suspended. It shall then decide to abort the connection or to resume it.

In order to resume it, the RR sublayer is requested to establish an RR connection. There may be further requests for RR connection establishment, e.g. for CM re-establishment; these shall prevail. The further proceeding is as described below:

- If there are only request from the PDSS2 sublayer, the MS shall send a PDSS2 RESUME REQUEST relating to one of the requesting PDSS2 protocol entities as first layer 3 message.
- Otherwise, and for further PDSS2 entities requesting the resumption. after establishment of the RR connection, the MS continues as in (A).

NOTE: The messages sent by a PDSS2 protocol entity after resumption still use the same transaction identifier and TI flag as before.

2) If during the information phase of a PDSS2 connection, the PDSS2 protocol entity becomes aware that too much data is waiting for transmission ("congestion condition"), it informs higher layers that the data transfer is suspended. If the PDSS2 protocol entity later becomes aware that the congestion condition no more exists, it informs higher layers that data transfer can be resumed.

3) If the request from higher layers to transfer data contained data with more than the maximum allowed length, the protocol entity shall reject the request with appropriate cause.

8 Handling of unknown, unforeseen, and erroneous protocol data

8.1 General

This section specifies procedures for the handling of unknown, unforeseen, and erroneous protocol data by the receiving PDSS1 or PDSS2 protocol entity. These procedures are called "error handling procedures", but in addition to providing recovery mechanisms for error situations they define a compatibility mechanism for future extensions of the protocols.

Subclauses 8.1 to 8.8 shall be applied in order of precedence.

Most error handling procedures are mandatory for the MS.

Detailed error handling procedures in the network are implementation dependent and may vary from PLMN to PLMN. However, when extensions of this protocol are developed, networks will be assumed to have the error handling that is indicated in this section as mandatory ("shall") and that is indicated as strongly recommended ("should").
Subclauses 8.2, 8.3, 8.4, 8.5 and 8.7.2 do not apply to the error handling in the network applied to the receipt of initial layer 3 message: If the network diagnoses an error described in one of these sections in the initial layer 3 message received from the mobile station, it shall either:

- try to recognize the classmark and then take further implementation dependent actions, or
- release the RR-connection.

Also, the error handling of the network is only considered as mandatory or strongly recommended when certain thresholds for errors are not reached during a dedicated connection.

In this section the following terminology is used:

- An IE is defined to be syntactically incorrect in a message if it contains at least one value defined as "reserved" in subclause 10, or if its value part violates rules of subclause 10. However it is not a syntactical error that a TLV encoded IE specifies in its length indicator a greater length than defined in subclause 10.
- A message is defined to have semantically incorrect contents if it contains information which, possibly dependant on the state of the receiver, is in contradiction to the resources of the receiver and/or to the procedural part of sections 6 and 7.

8.2 Message too short

When a message is received that is too short to contain a complete message type information element, that message shall be ignored, see GSM 04.07.

8.3 Unknown or unforeseen transaction identifier

The mobile station and network shall answer to a message received with TI value "111" by sending a RELEASE COMPLETE message with same TI value and cause "invalid transaction identifier value". For a call control message received with TI different from "111", the following procedures shall apply:

a) Whenever a message except a SETUP or RELEASE COMPLETE is received specifying a transaction identifier which is not recognized as relating to an active transaction, the receiving entity shall send a RELEASE COMPLETE message with cause #81 "invalid transaction identifier value" using the received transaction identifier value and remain idle.

b) When a RELEASE COMPLETE message is received specifying a transaction identifier which is not recognized as relating to an active transaction, the MM connection associated with that transaction identifier shall be released.

c) When a SETUP message is received with:

- a transaction identifier which is not recognized as relating to an active transaction, and
- TI flag value 1;

the receiving entity shall send a RELEASE COMPLETE message with cause "invalid transaction identifier value" and not including diagnostics using the received transaction identifier value and remain idle.

d) When a SETUP message is received specifying a transaction identifier which is recognized as relating to an active call or to a call in progress, this SETUP message shall be treated as a message not compatible with the protocol state, see subclause 8.4.

8.4 Unknown or unforeseen message type

If the protocol entity in the mobile station receives a message with message type not defined for the PD or not implemented by the receiver, it shall ignore the message except for the fact that, if an RR connection exists, it shall return a STATUS message with cause "message type non-existent or not implemented" and including as diagnostics the message type of the message received.

If the protocol entity in the network receives a message with message type not defined for the PD or not implemented by the receiver, it shall ignore the message except that it should return a STATUS message with cause "message type non-existent or not implemented" and including as diagnostics the message type of the message received.

NOTE: A message type not defined for the PD in the given direction is regarded by the receiver as a message type not defined for the PD, see GSM 04.07.

1) If the protocol entity in the mobile station receives a message not compatible with the protocol state, the mobile station shall ignore the message except for the fact that, if an RR connection exists, it returns a STATUS message with cause "message type not compatible with protocol state" and including as diagnostics the message type of the message received.

If the network receives a message not compatible with the protocol state, the network actions are implementation dependent.

8.5 Non-semantical mandatory information element errors

When on receipt of a message:

- an "imperative message part" error, or
- a "missing mandatory IE" error;

is diagnosed or when a message containing:

- a syntactically incorrect mandatory IE, or

- an IE unknown in the message, but encoded as "comprehension required" (see GSM 04.08, subclause 10.5), or
- an out of sequence IE encoded as "comprehension required" (see GSM 04.08, subclause 10.5);

is received;

- the mobile station shall proceed as follows:

  When the message is not one of the messages listed in section 8.5.1, the mobile station shall ignore the message except for the fact that, if an RR connection exists, it shall return a STATUS message with cause "invalid mandatory information" and including, if possible, as diagnostics the complete message received (this may not be possible, e.g., due to length restrictions).

- the network shall proceed as follows:

  When the message is not one of the message listed in section 8.5.1 the network shall either:

  - try to treat the message (the exact further actions are implementation dependent), or
  - ignore the message except that it should return a STATUS message with cause "invalid mandatory information", possibly including as diagnostics the complete message received.

8.5.1 Special cases

1) If the message is a SETUP message and received by the mobile station, a RELEASE COMPLETE message shall be returned with cause "invalid mandatory information" and including, if possible, as diagnostics the complete message received (this may not be possible, e.g., due to length restrictions).
2) If the message is a SETUP message and received by the network, a RELEASE COMPLETE message shall be returned with cause "invalid mandatory information" and possibly including as diagnostics the complete message received.
3) If the message is a RELEASE COMPLETE message, it shall be treated as a normal RELEASE COMPLETE message.
4) If the message is a STATUS message and received by the network, a RELEASE COMPLETE message may be returned with cause value "invalid mandatory information" and possibly including as diagnostics the complete message received.

8.6 Unknown and unforeseen information elements in the non-imperative message part

8.6.1 Information elements unknown in the message

The protocol entity shall ignore all information elements unknown in a message which are not encoded as "comprehension required".

8.6.2 Out of sequence information elements

The MS shall ignore all out of sequence Information elements in a message which are not encoded as "comprehension required".

The network should take the same approach.

8.6.3 Repeated Information elements

If an information element with format T, TV, or TLV is repeated in a message in which repetition of the information element is not specified in section 9 of the present document, only the contents of the information element appearing first shall be handled and all subsequent repetitions of the information element shall be ignored. When repetition of information elements is specified, only the contents of specified repeated information elements shall be handled. If the limit on repetition of information elements is exceeded, the contents of information elements appearing first up to the limit of repetitions shall be handled and all subsequent repetitions of the information element shall be ignored.

The network should follow the same procedures.

8.7 Non-imperative message part errors

This category includes:

- syntactically incorrect optional Information elements;
- conditional IE errors.

8.7.1 Syntactically incorrect optional Information elements

The protocol entity shall treat all optional Information elements that are syntactically incorrect in a message as not present in the message.

8.8 Messages with semantically incorrect contents

When a message with semantically incorrect contents is received, the foreseen reactions of the procedural part of sections 6 and 7 are performed. If however no such reactions are specified, the MS shall ignore the message except for the fact that, if an RR connection exists, it returns a STATUS message with cause value "semantically incorrect message" and including, if possible, as diagnostics the complete message received (this may not be possible, e.g., due to length restrictions).

The network should follow the same procedure except that a status message is not normally transmitted.

9 MESSAGE FUNCTIONAL DEFINITIONS AND CONTENTS

This section defines the structure of the messages of those layer 3 protocols, that is the PDSS1 and PDSS2 protocols. Both protocols mostly use the same messages, but have different protocol discriminators, cf. GSM 04.07.

NOTE: Two different protocol discriminators are used in order to allow the network different routing.

When a message is only defined for one protocol in one protocol or has restricted use in one protocol (i.e. it is only defined in one direction in one protocol but in both directions in the other protocol), this is defined in the subclause specifying the message. All messages are standard L3 messages as defined in GSM 04.07.

Each definition given in the present subclause includes:

- a brief description of the message direction and use;
- a definition in which protocol(s), PDSS1 and/or PDSS2 the message is defined and in which direction;

- a table listing the information elements permitted to be in that message and their order of their appearance in the message. All information elements that may be repeated are explicitly indicated. Neither the network nor the mobile station is allowed to include information elements in a message which are not specified for the message or to include the information elements in the message in an order different from the specified order. (V and LV formatted IEs, which compose the imperative part of the message, occur before T, TV, and TLV formatted IEs which compose the non-imperative part of the message, cf. GSM 04.07.) In a (maximal) sequence of consecutive information elements with half octet length, the first information element with half octet length occupies bits 1 to 4 of octet N, the second bits 5 to 8 of octet N, the third bits 1 to 4 of octet N+1 etc. Such a sequence always has an even number of elements.

  For each information element the table indicates:

  1. if the IE has format T, TV, or TLV, the IEI used by the IE at the indicated position in the message, in hexadecimal notation. If the IEI has half octet length, this is specified by a notation representing the IEI as a hexadecimal digit followed by a "-" (example: B-);

  2. the name of the information element (which may give an idea of the semantics of the element). The name of the information element (usually written in italics) followed by "IE" or "information element" is used in GSM 04.08 as reference to the information element within a message;

  3. the name of the type of the information element (which indicates the coding of the value part of the IE), and generally, the referenced subsection of subclause 10 describing the value part of the information element;

  4. the presence requirement indication (M or O) for the IE as defined in GSM 04.07. (Presence requirement indication C is not used in the present document);

  5. the format of the information element (T, V, TV, LV, TLV) as defined in GSM 04.07;

  6. the length of the information element (or permissible range of lengths), in octets, in the message. This indication is normative. However, further restrictions to the length of an IE may be specified elsewhere.

c) subsections specifying, where appropriate:

  - the meaning of, and

  - conditions for;

  absence, repeated occurrence, and/or presence for IEs with presence requirement O in the relevant message which together with other conditions specified, define when the information elements shall be included or not, what presence, repeated occurrence, and absence of such IEs means.

Table 9.1/GSM 04.63 summarizes the messages for PDSS1 and PDSS2. A letter D ("downlink") in the column corresponding to one of the two protocols specifies that the message is defined in the direction network to mobile station for that protocol, a letter U ("uplink") specifies that the message is defined in the direction mobile station to network for that protocol; the word "no" specifies that the message is not defined at all for that protocol.

Table 9.1/GSM 04.63: Messages for PDSS1 and PDSS2

Message	Reference	defined for PDSS1	defined for PDSS2
DATA	9.1	D,U	D,U
IMMEDIATE SETUP	9.2	no	U
RELEASE COMPLETE	9.3	D,U	D,U
SETUP	9.4	D,U	no
SETUP ACKNOWLEDGE	9.5	D,U	D,U
RESUME	9.6	U	U
RESUME ACK	9.7	D	D
STATUS	9.8	D,U	D,U

9.1 DATA

This message is used to send data to the peer entity. See Table 9.2/GSM 04.63.

Message type: DATA.

Protocol/direction: PDSS1 in both directions.

PDSS2 in both directions.

Table 9.2/GSM 04.63: DATA message

IEI	information element	type / reference	presence	format	length
	protocol discriminator	protocol discriminator GSM 04.07, 11.2.1	M	V	1/2
	transaction identifier	transaction identifier GSM 04.07, 11.2.3	M	V	1/2
	message type	message type 10.4	M	V	1
	data	data 10.5.3	M	LV	1-249

9.1.1 Data

The length of the *data* information element (including the length indicator) in the DATA message shall not exceed 251 - L octets where L is the number of octets occupied by all other IEs in the message.

NOTE: This is due to restrictions of layer 2 (which result from restrictions in GSM 08.56). Due to some reasons, usage of long data IE is not recommendable e.g. on the SACCH or if the A or A_p interface has stronger length restrictions.

9.2 IMMEDIATE SETUP

This message is sent by the mobile station to the network in order to initiate the establishment of a PDSS2 connection. See Table 9.3/GSM 04.63.

Message type: IMMEDIATE SETUP.

Protocol/direction: PDSS2 mobile station to network.

Table 9.3/GSM 04.63: IMMEDIATE SETUP message

IEI	information element	type / reference	presence	format	length
	protocol discriminator	protocol discriminator GSM 04.07, 11.2.1	M	V	1/2
	transaction identifier	transaction identifier GSM 04.07, 11.2.3	M	V	1/2
	message type	message type 10.4	M	V	1
	spare half octet	spare half octet 10.5.5	M	V	1/2
	ciphering key sequence number	ciphering key sequence number GSM 04.08, 10.5.3.2	M	V	1/2
	mobile station classmark	mobile station classmark 2 GSM 04.08, 10.5.1.6	M	LV	4
	mobile identity	mobile identity 10.5.4	M	LV	2-9
	application	application 10.5.1	M	V	1
	data	data 10.5.3	M	LV	1-10

9.2.1 Ciphering key sequence number

The ciphering key sequence number shall be set to the value “111“ (no key is available).

9.2.1 Data

The length of the *data* information element (including the length indicator) in the IMMEDIATE SETUP message shall not exceed N201 - L, where L is the number of octets all other information elements occupy in the message and N201 is as defined in GSM 04.06 for the signalling link used for the transmission of the message.

9.3 RELEASE COMPLETE

This message is sent to the peer entity in order to release the PDSS1 or PDSS2 connection. See Table 9.4/GSM 04.63.

Message type: RELEASE COMPLETE.

Protocol/direction: PDSS1 in both directions.

PDSS2 in both directions.

Table 9.4/GSM 04.63: RELEASE COMPLETE message

IEI	information element	type / reference	presence	format	length
	protocol discriminator	protocol discriminator GSM 04.07, 11.2.1	M	V	1/2
	transaction identifier	transaction identifier GSM 04.07, 11.2.3	M	V	1/2
	message type	message type 10.4	M	V	1
	cause	cause 10.5.2	M	LV	2-248
	data	data 10.5.3	M	LV	1-248
08	cause 2	cause 10.5.2	O	TLV	3-248

9.3.1 Data

The length of the *data* information element (including the length indicator) in the RELEASE COMPLETE message shall not exceed 251 - L octets where L is the number of octets occupied by all other IEs in the message.

NOTE: This is due to restrictions of layer 2 (which result from restrictions in GSM 08.56). Due to some reasons, usage of long data IE is not recommendable e.g. on the SACCH or if the A or A_p interface has stronger length restrictions.

9.3.2 Cause 2

This IE is included in the message, if more than one cause has to be reported; it may be repeated in the message, if further causes have to be reported.

9.4 SETUP

This message is sent by a PDSS1 protocol entity in order to establish a PDSS1 connection. See Table 9.5/GSM 04.63.

Message type: SETUP.

Protocol/direction: PDSS1 in both directions.

Table 9.5/GSM 04.63: SETUP message

IEI	information element	type / reference	presence	format	length
	protocol discriminator	protocol discriminator GSM 04.07, 11.2.1	M	V	1/2
	transaction identifier	transaction identifier GSM 04.07, 11.2.3	M	V	1/2
	message type	message type 10.4	M	V	1
	application	application 10.5.1	M	V	1
	data	data 10.5.3	M	LV	1-248

9.4.1 Data

The length of the *data* information element (including the length indicator) in the SETUP message shall not exceed 251 - L octets where L is the number of octets occupied by all other IEs in the message.

NOTE: This is due to restrictions of layer 2 (which result from restrictions in GSM 08.56). Due to some reasons, usage of long data IE is not recommendable e.g. on the SACCH or if the A or A_p interface has stronger length restrictions.

9.5 SETUP ACKNOWLEDGE

This message is sent by a PDSS1 or PDSS2 protocol entity in order to accept establishment of a connection. See Table 9.6/GSM 04.63.

Message type: SETUP ACKNOWLEDGE.

Protocol/direction: PDSS1 in both directions.

PDSS2 in both directions.

Table 9.6/GSM 04.63: SETUP ACKNOWLEDGE message

IEI	information element	type / reference	presence	format	length
	protocol discriminator	protocol discriminator GSM 04.07, 11.2.1	M	V	1/2
	transaction identifier	transaction identifier GSM 04.07, 11.2.3	M	V	1/2
	message type	message type 10.4	M	V	1
	data	data 10.5.3	M	LV	1-249

9.5.1 Data

The length of the *data* information element value part in the SETUP message shall not exceed 251 - L octets where L is the number of octets occupied by all other IEs in the message.

NOTE: This is due to restrictions of layer 2 (which result from restrictions in GSM 08.56). Due to some reasons, usage of long data IE is not recommendable e.g. on the SACCH or if the A or A_p interface has stronger length restrictions.

9.6 RESUME

This message is sent to the peer entity in order to resume the connection. See Table 9.7/GSM 04.63.

Message type: RESUME.

Protocol/direction: PDSS1 in mobile to network direction.

PDSS2 in mobile to network direction.

Table 9.7/GSM 04.639.6: RESUME

IEI	information element	type / reference	presence	format	length
	protocol discriminator	protocol discriminator GSM 04.07, 11.2.1	M	V	1/2
	transaction identifier	transaction identifier GSM 04.07, 11.2.3	M	V	1/2
	message type	message type 10.4	M	V	1
	spare half octet	spare half octet 10.5.5	M	V	1/2
	ciphering key sequence number	ciphering key sequence number GSM 04.08, 10.5.3.2	M	V	1/2
	mobile station classmark	mobile station classmark 2 GSM 04.08, 10.5.1.6	M	LV	4
	mobile identity	mobile identity 10.5.4	M	LV	2-9

9.6.1 Ciphering key sequence number

The ciphering key sequence number shall be set to the value "111" (no key is available) in case of PDSS2.

9.7 RESUME ACK

This message is sent to the peer entity in order to acknowledge resumption of the connection. See Table 9.8/GSM 04.63.

Message type: RESUME ACK.

Protocol/direction: PDSS1 in network to mobile direction.

PDSS2 in network to mobile direction.

Table 9.8/GSM 04.63: RESUME ACK

IEI	information element	type / reference	presence	format	length
	protocol discriminator	protocol discriminator GSM 04.07, 11.2.1	M	V	1/2
	transaction identifier	transaction identifier GSM 04.07, 11.2.3	M	V	1/2
	message type	message type 10.4	M	V	1

9.8 STATUS

This message is sent by a PDSS1 or PDSS2 protocol entity in order to inform its peer entity about an error situation. See Table 9.7/GSM 04.63.

Message type: STATUS.

Protocol/direction: PDSS1 in both directions.

PDSS2 in both directions.

Table 9.9/GSM 04.63: STATUS message

IEI	information element	type / reference	presence	format	length
	protocol discriminator	protocol discriminator GSM 04.07, 11.2.1	M	V	1/2
	transaction identifier	transaction identifier GSM 04.07, 11.2.3	M	V	1/2
	message type	message type 10.4	M	V	1
	cause	cause 10.5.2	M	LV	2-248
08	cause 2	cause 10.5.2	O	TLV	3-248

9.8.1 Cause 2

This IE is included in the message, if more than one cause has to be reported; it may be repeated in the message, if further causes have to be reported.

10.1 Overview

Within the Layer 3 protocols defined, every message is a standard L3 message as defined in GSM 04.07.

10.2 Protocol Discriminator

The Protocol Discriminator (PD) and its use are defined in GSM 04.07. GSM 04.08 defines the protocols relating to the PD values:

bits 4 3 2 1
0 0 1 0 PDSS1 protocol
0 1 0 0 PDSS2 protocol.

10.3 Transaction identifier

Bits 5 to 8 of the first octet of every message belonging to the PDSS1 and PDSS2 protocols contain the transaction identifier (TI). The transaction identifier and its use are defined in GSM 04.07.

10.4 Message Type

The message type IE and its use are defined in GSM 04.07. Table 10.1/GSM 04.63 define the value part of the message type IE used in the PDSS1 and PDSS2 protocols.

Table 10.1/GSM 04.63: Message types for PDSS1 and PDSS2

8 7 6 5 4 3 2 1	
0 x 1 1 0 0 0 0	DATA
0 x 1 1 0 0 0 1	IMMEDIATE SETUP
0 x 1 1 0 0 1 0	RELEASE COMPLETE
0 x 1 1 0 0 1 1	SETUP
0 x 1 1 0 1 0 0	SETUP ACKNOWLEDGE
0 x 1 1 0 1 0 1	RESUME
0 x 1 1 0 1 1 0	RESUME ACK
0 x 1 1 0 1 1 1	STATUS

Bit 8 is reserved for possible future use as an extension bit, see GSM 04.07.

Bit 7 is reserved for the send sequence number in PDSS1 and PDSS2 messages sent from the mobile station. In PDSS1 and PDSS2 messages sent from the network an, bit 7 is coded with a "0". See GSM 04.07.

10.5 Other information elements

For coding of other IEs, the rules defined in GSM 04.08 apply.

10.5.1 Application

The purpose of the *application* information element is to indicate the application that requested the PDSS1 or PDSS2 connection to the peer entity.

The *application* information element value part has a length of 1 octets. The value part is coded as shown below:

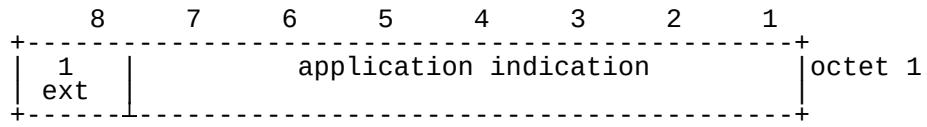

Figure 10.1/GSM 04.63: *application indication* information element

Table 10.2/GSM 04.63: *application indication* information element

application indication (7 bits) bit 7 6 5 4 3 2 1 0 0 0 0 0 0 0 X.25 0 0 0 0 0 0 1 IP all other values indicate unknown applications

10.5.2 Cause

The purpose of the *cause* information element is to describe the reason for generating certain messages and to provide diagnostic information in the event of procedural errors.

The *cause* information element value part has a minimal length of 1 octets. No upper length limit is specified except for that given by the maximum number of octets in a L3 message (see GSM 04.06); further rules in the present document may further restrict the length of the IE in a message.

The value part is coded as shown below:

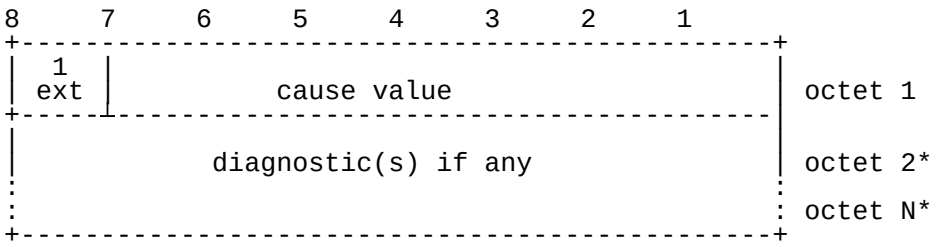

Figure 10.2/GSM 04.63: *cause* information element

Table 10.3/GSM 04.63: *cause* information element

Cause value (octet 1)	
Bits	
7 6 5 4 3 2 1	
0 0 0 0 0 1 1	Illegal MS
0 0 0 0 1 0 1	IMEI not accepted
0 0 0 0 1 1 0	Illegal ME
0 0 0 1 0 0 0	Service not authorized
0 0 0 1 0 0 1	Application not supported on the protocol
0 0 0 1 0 1 0	RR connection aborted
0 0 1 0 0 0 1	Network failure
0 0 1 0 1 1 0	Congestion
0 1 0 0 0 0 0	Service option not supported
0 1 0 0 0 0 1	Requested service option not subscribed
0 1 0 0 0 1 0	Service option temporarily out of order
0 1 0 0 1 1 0	Call cannot be identified
0 1 1 0 0 0 0	}
to	} retry upon entry into a new cell
0 1 1 1 1 1 1	}
1 0 1 1 1 1 1	Semantically incorrect message
1 1 0 0 0 0 0	Invalid mandatory information
1 1 0 0 0 0 1	Message type non-existent or not implemented
1 1 0 0 0 1 0	Message type not compatible with the protocol state
1 1 0 0 0 1 1	Information element non-existent or not implemented
1 1 0 0 1 0 1	Message not compatible with the protocol state
1 1 0 1 1 1 1	Protocol error, unspecified
Any other value received shall be treated as an unspecific information	
Diagnostics (octet 2 ff) This field may contain a message or information element	

10.5.3 Data

The purpose of the *data* information element is to transport data to the peer entity. Within the scope of the present document the content of the *data* information field is an array of octets.

The *data* information element has a minimum length of 0 octets. No upper length limit is specified except for that given by the maximum number of octets in a L3 message (see GSM 04.06); further rules in the present document may further restrict the length of the IE in a message.

10.5.4 Mobile identity 2

The purpose of the *mobile identity* information element is to provide either the international mobile subscriber identity, IMSI, the temporary mobile subscriber identity, TMSI, the international mobile equipment identity, IMEI, the international mobile equipment identity together with the software version number, IEMISV or the Anonymous Mobile Station Identity (AMSI).

The IMSI shall not exceed 15 digits, the TMSI and The AMSI is 4 octets long.

The *mobile identity 2* IE is used in the establishment of a PDSS2 connection. The mobile station shall select the mobile identity type as follows: If the application requests it, the AMSI is used. Otherwise the TMSI shall be used if it is available. The IMSI shall be used in cases where no TMSI is available.

The *mobile identity* information element is coded as shown below:

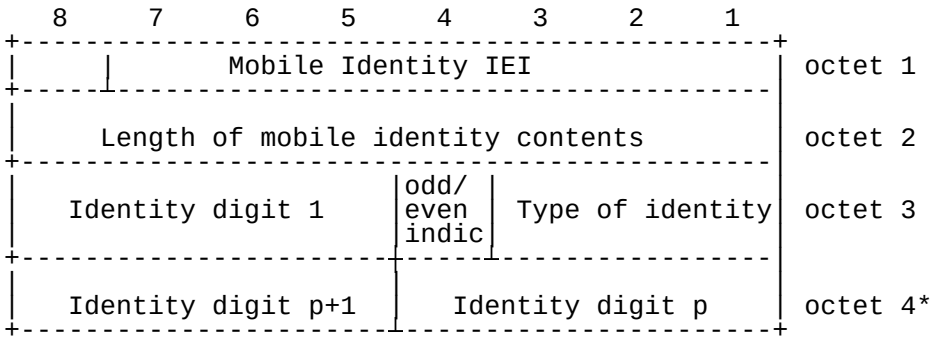

Figure 10.3/GSM 04.63: *Mobile Identity 2* information element

Table 10.4/GSM 04.63: *Mobile Identity* information element

Type of identity (octet 3)
Bits
3 2 1
0 0 1 IMSI
1 0 0 TMSI
1 0 1 AMSI

All other values are reserved.

Odd/even indication (octet 3)
Bit
4
0 even number of identity digits and also when the TMSI is used
1 odd number of identity digits

Identity digits (octet 3 etc.)
For the IMSI this field is coded using BCD coding. If the number of identity digits is even then bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111".

If the mobile identity is the TMSI then bits 5 to 8 of octet 3 are coded as "1111" and bit 8 of octet 4 is the most significant bit and bit 1 of the last octet the least significant bit. The coding of the TMSI is left open for each administration.

If the mobile identity is the AMSI then bits 5 to 8 of octet 3 are coded as "1111" and bit 8 of octet 4 is the most significant bit and bit 1 of the last octet the least significant bit.The coding of the AMSI is further defined in TS GSM 03.03.

10.5.5 Spare Half Octet

This element is used in the description of messages in section 9 when an odd number of half octet type 1 information elements are used. This element is filled with spare bits set to zero and is placed in bits 5 to 8 of the octet unless otherwise specified.

Annex A (informative): Change Request History

Change history					
SMG No.	**TDoc. No.**	**CR. No.**	**Section affected**	**New version**	**Subject/Comments**
SMG#18				5.0.0	ETSI Publication of GTS 04.63
SMG#27				6.0.0	Release 1997 version
SMG#29				7.0.0	Release 1998 version
SMG#31				8.0.0	Release 1999 version

History

Document history		
V8.0.1	April 2000	Publication