



# EUROPEAN TELECOMMUNICATION STANDARD

**ETS 300 751**

August 1997

Source: EBU/CENELEC/ETSI JTC

Reference: DE/JTC-SWIFT

ICS: 33.020

**Key words:** Broadcasting, radio, FM, Multimedia



## Radio broadcasting systems; System for Wireless Infotainment Forwarding and Teledistribution (SWIFT)

### ETSI

European Telecommunications Standards Institute

#### ETSI Secretariat

**Postal address:** F-06921 Sophia Antipolis CEDEX - FRANCE

**Office address:** 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE

**X.400:** c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

**Copyright Notification:** No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1997.

© European Broadcasting Union 1997.

All rights reserved.



## Contents

Foreword .....	7
1 Scope .....	9
2 Normative references .....	9
3 Definitions and abbreviations .....	10
3.1 Definitions .....	10
3.2 Abbreviations .....	10
4 Multiplex requirements .....	11
5 Functions of the multiplexing unit .....	11
6 Reference model .....	12
7 Layers organization OSI reference model .....	13
7.1 Functional layers .....	13
7.1.1 Physical layer (Layer 1) .....	13
7.1.2 Data link layer (Layer 2) .....	13
7.1.3 Network layer (Layer 3) .....	13
7.1.4 Transport layer (Layer 4) .....	13
7.1.5 Session layer (Layer 5) .....	14
7.1.6 Presentation layer (Layer 6) .....	14
7.1.7 Application layer (Layer 7) .....	14
7.2 Services and protocols .....	14
7.3 Detailed description of Layers 1 to 5 .....	15
7.3.1 Layer 1 .....	15
7.3.1.1 Service provided by Layer 1 .....	15
7.3.1.1.1 Service on the transmitter side .....	15
7.3.1.1.2 Modulation characteristics .....	15
7.3.1.1.3 Protection ratios .....	17
7.3.1.2 Service on the receiver side .....	17
7.3.2 Layer 2 .....	17
7.3.2.1 Service provided by Layer 2 .....	17
7.3.2.1.1 Service on the transmitter side .....	17
7.3.2.1.2 Service on the receiver side .....	18
7.3.2.2 Layer 2 protocol .....	19
7.3.2.2.1 Frame structure .....	19
7.3.2.3 Information Block .....	21
7.3.2.4 Parity Block .....	22
7.3.2.5 Block Identification Code (BIC) .....	22
7.3.2.6 Scrambling .....	22
7.3.3 Layer 3 (Network layer) .....	22
7.3.3.1 Service provided by Layer 3 .....	22
7.3.3.1.1 Service on the transmitter side .....	22
7.3.3.1.2 Service on the receiver side .....	23
8 Multiplex organization (Layer 3 & 4) .....	24
8.1 Principles .....	24
8.2 Definition of logical channel .....	24
8.3 Service Channel "SeCh" (SI/LCh = 8 Hex) .....	24
8.3.1 Definition .....	24
8.3.2 Service Channel - Layer 3 .....	25
8.3.2.1 L3-Header SeCh format. ....	25
8.3.3 Service message format .....	26

	8.3.3.1	Channel Organization Table (COT) .....	27
	8.3.3.2	Alternative Frequency Table (AFT) .....	28
	8.3.3.3	Service Alternative Frequency Table (SAFT).....	30
	8.3.3.4	Time, Date, Position and Network name Table (TDPNT)...	31
	8.3.3.4.1	MJD, Modified-Julian-Date .....	31
	8.3.3.4.2	Time reference .....	31
8.4		Short Message Channel "SMCh" (SI/LCh =9 Hex) .....	33
	8.4.1	L4-Header SMCh format .....	33
	8.4.2	L3-Header SMCh format .....	34
8.5		Long Message Channel "LMCh" (SI/LCh = A Hex).....	35
	8.5.1	L4-Header LMCh format .....	35
	8.5.2	L3-Header LMCh format .....	36
8.6		Data Group Structure over long messages.....	36
	8.6.1	L5-Data group header LMCh format.....	37
	8.6.1.1	Fields description of the data group minimum header.....	38
	8.6.1.2	Description of the DGCA field .....	38
	8.6.1.3	Fields description of the session header.....	38
	8.6.1.3.1	User Access field .....	39
	8.6.2	Coding of the data group type 12.....	39
9		Conditional Access (CA).....	40
	9.1	Scrambling data .....	41
	9.1.1	Introduction .....	41
	9.1.2	Generating scrambling and descrambling sequences.....	41
	9.1.2.1	Initialization Word (IW).....	41
	9.1.2.2	Phasing .....	42
	9.1.3	Scrambling/descrambling processes.....	42
	9.1.3.1	Conditional Access signalling configurations .....	42
	9.1.3.2	Scrambling/Descrambling of the service in Data Groups ...	43
	9.1.3.3	Scrambling/Descrambling of the service in the Long Message Channel .....	43
	9.1.3.4	Scrambling/Descrambling of the service sent in SMCh.....	44
	9.1.3.5	DAB compatibility .....	44
	9.2	Signalling and synchronizing data .....	45
	9.2.1	Conditional Access Identifier (CAId) .....	45
	9.2.2	Service Conditional Access (SCA) .....	45
	9.2.3	Data Group Conditional Access (DGCA).....	47
	9.2.4	Long Message Channel Conditional Access (LMCCA and LMCCA_Ext) ....	47
	9.2.4.1	LMCCA.....	47
	9.2.4.2	LMCCA_Extended .....	48
	9.2.5	Short Message Channel Conditional Access (SMCCA and SMCCA_Ext)...	49
	9.2.5.1	SMCCA .....	49
	9.2.5.2	SMCCA_Extended .....	50
	9.3	ECM and EMM transmission.....	51
	9.3.1	General description.....	51
	9.3.1.1	ECM coding.....	51
	9.3.1.2	EMM coding .....	52
	9.3.1.3	Command Identifier (CI) coding .....	53
	9.3.2	Transport .....	53
	9.3.2.1	LMCh.....	53
	9.3.2.2	SMCh .....	54
	9.3.2.3	Together with service data .....	55
10		Error correction strategy .....	55
	10.1	Layer 2 error detection and correction .....	55
	10.2	Error detection strategy at other layers .....	56
	10.2.1	L3 short message header CRC .....	56
	10.2.2	L3 long message header CRC .....	56
	10.2.3	L4 short message header CRC .....	56
	10.2.4	L4 long message header CRC .....	57
	10.2.5	L5 (data group) CRC .....	57
11		Bit-order of transmission.....	57

12	Service addressing mechanism .....	59
12.1	Global services .....	59
12.2	Country wide services .....	59
12.3	Network specific services .....	59
12.4	Local services of single transmitters .....	60
12.5	Address allocation for global services .....	60
13	Quality of service .....	60
13.1	Useful bit-rate .....	60
13.2	Expected capabilities of a Conditional Access system .....	60
13.2.1	From the user's point of view .....	60
13.2.1.1	Access time of a newly connected user .....	60
13.2.1.2	Zapping time .....	60
13.2.2	From the service operator's point of view .....	60
13.2.2.1	Bit rate needed to broadcast Conditional Access messages .....	60
13.2.2.1.1	Bit rate for the ECMs .....	61
13.2.2.1.2	Bit rate for the EMMs .....	61
13.2.2.2	Maximum time for changing the access mode .....	61
13.2.2.3	Transcontrol .....	62
13.2.2.4	Length of a scrambling cycle .....	62
13.2.2.5	Repetition frequency .....	62
13.2.2.6	Hierarchical coding and scrambling .....	62
14	Classes of services .....	62
	History .....	64

Blank page

## Foreword

This European Telecommunication Standard (ETS) has been produced by the Joint Technical Committee (JTC) of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECtrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

NOTE: The EBU/ETSI JTC was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters is in Geneva \*.

\* European Broadcasting Union  
Case Postale 67  
CH-1218 GRAND SACCONNEX (Geneva)  
Switzerland  
  
Tel: +41 22 717 21 11  
Fax: +41 22 717 24 81

Transposition dates	
Date of adoption:	8 August 1997
Date of latest announcement of this ETS (doa):	30 November 1997
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 May 1998
Date of withdrawal of any conflicting National Standard (dow):	31 May 1998

Blank page



## 1 Scope

This European Telecommunication Standard (ETS) establishes a broadcasting standard of a System for Wireless Infotainment Forwarding and Teledistribution (SWIFT) designed for delivery of data services for mobile, portable and fixed receivers in the FM band. This ETS defines the nature and content of the transmitted SWIFT signal. It describes also the organization of the multiplex for the SWIFT standard.

A multiplex is necessary to optimize the use of the radio channel by sharing it between several applications. For example, a dGPS application has some precise constraints such as real time (one message per second), size (2 kbits per message). This application requires a continuous channel of perhaps 3 kbit/s. Assuming a DARC channel has a minimum useful bit rate of 6 kbit/s, it would be interesting to use the remaining 3 kbit/s for an other application, newspapers broadcasting for example.

On the opposite, in a newspaper application, it is necessary to broadcast the news twice a day for example in a maximum time (1 hour). This is a low rate service with a big amount of data and without real time. It would be interesting to stop for some time this service if hot news have to be sent (higher service priority).

Sometimes, the network operator can offer the same application (class of application/service) to different service providers, for example, different newspapers. It would be interesting to multiplex this newspapers on the same radio channel in a transparent manner for the service provider point of view.

The multiplex can be made:

- in the Transmitter Station Equipment (TSE), for splitting the radio channel into logical channels using a given mapping at a given time. The characteristic of the logical channels is a constant bit rate enabling real time applications and/or applications requiring constant bit rate all the time;
- in the TSE, for repeating regularly or inserting some information into the multiplex. In this case, a local priority management is required;
- on the network server, based on a priority mechanism. This enables for example the mixing of several applications with different priorities, but not real time and on demand (news and hot news, pictures preloading and weather information);
- on the network server, for multiplexing different processes of an application (for example, different newspapers for the application newspapers broadcasting). This is useful if it should offer a quicker "average" service (for example, the reading of a newspaper page by page before the complete loading).

As described above, there are different multiplexing levels/functions for different reasons. Each function is necessary and it shall be possible to make them running together.

## 2 Normative references

This ETS incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

- |     |  |
|-----|--|
| [1] | EN 50067: "Specification of the Radio Data System (RDS)".  |
| [2] | ETS 300 075: "Terminal Equipment (TE); Processable data File transfer".  |
| [3] | ETS 300 174: "Network Aspects (NA); Digital coding of component television signals for contribution quality applications in the range 34 - 45 Mbit/s". |
| [4] | ETS 300 401: "Radio broadcasting systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers".                                   |

- [5] ISO 7498: "Information Processing Systems - Open systems Interconnection - Basic Reference Model".
- [6] ITU-T Recommendation X.200: "Reference model of open systems interconnection for CCITT applications".
- [7] ITU-R Recommendation BS 1194: "Data Radio Channel (DARC)".
- [8] ITU-R Recommendation 412: "Planning standard for FM broadcasting".

### 3 Definitions and abbreviations

#### 3.1 Definitions

For the purpose of this ETS, the following definitions apply:

Several carriers may be associated to one transmitter. Every carrier transports only one physical DARC channel.

This physical channel will be identified by the frequency of its carrier. It is time-divided in **Layer 2 data units (frames or blocks)** continuously broadcast with the same number of Bytes in it.

One physical channel is shared between several logical channels. Three logical channels with different broadcasting characteristics are described in this ETS:

- a) the service channel SeCh, especially dedicated to information about the local transmitter and multiplex organization;
- b) the short message channel SMCh, for low bit-rate or real time applications;
- c) the long message channel LMCh, for files with low priority.

Each logical channel carries a lot of **subchannels** distinguishable by an address and/or a type. Each subchannel corresponds to one **service**.

Services with some common broadcasting characteristics are classified in a same category, or **class of services**.

#### 3.2 Abbreviations

For the purposes of this ETS, the following abbreviations apply in the construction of system coefficient names:

ACS	Access Control System
ADD	ADdress
BIC	Block Identification Code
BPF	Band-Pass Filter
CA	Conditional Access
CAId	Conditional Access Identifier
CW	Control Word
DAB	Digital Audio Broadcasting
DARC	DAta Radio Channel
DGCA	Data Group Conditional Access
dGPS	differential Global Positioning System
ECM	Entitlement Checking Message
EMM	Entitlement Management Message
FIG	Fast Information Groups (see ETS 300 401 [4])
FM	Frequency Modulation
GPS	Global Positioning System
IM	Initialization Modifier
LMCCA	Long Message Channel Conditional Access

LMCh	Long Message Channel
LMSK	Level-controlled Minimum Shift Keying
LPF	Low-Pass Filter
MM	Messaging Mode
MSK	Minimum Shift Keying
NWS	Network Server
OSI	Open Systems Interconnection
PRBS	Pseudo-Random Binary Sequence
RFA	Reserved for Future Addition
SCA	Service Conditional Access
SMCCA	Short Message Channel Conditional Access
SMCh	Short Message Channel
SPS	Service Provider Server
SWIFT	System for Wireless Infotainment Forwarding and Teledistribution
TSE	Transmitter Station Equipment

## 4 Multiplex requirements

The multiplex system shall cope with specific requirements. A list of these requirements is given below:

- flexible usage of a given subchannel according to the requirements of each individual service;
- an optimum management of the transmission resource by dynamic reallocation of the subchannels;
- to recover any service clock at the receiver side;
- to ensure that the impact of the demultiplexing method on the decoder price is low;
- to take into account the needs of the Conditional Access system which operates on a service basis;
- to take into account class of services based upon common broadcasting characteristics at the multiplex level;
- to inform receivers on the broadcast services and carriers configuration by offering all the information required to easily select a service and change carrier especially when mobile and of course, without return channel;
- to keep under a defined value the access time to a selected service;
- to keep under a defined value the change time from one service to another, on the same or on a different carrier;
- to take into account possible power/battery saving for some services;
- to take into account possible fast access for some services;
- to take into account possible interworking with DAB services.

## 5 Functions of the multiplexing unit

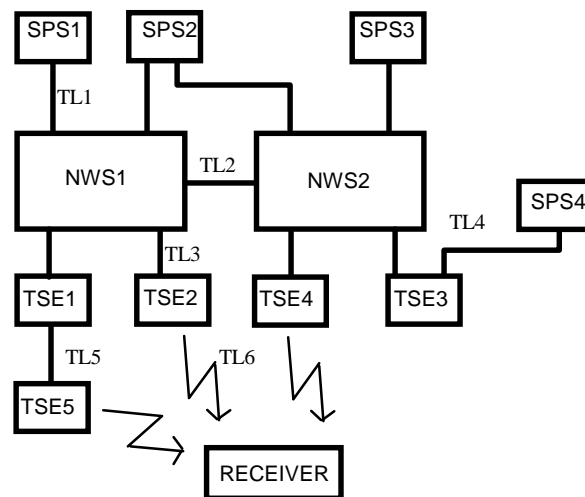
The multiplexing (demultiplexing) unit is located between the source coding (decoding) and the modulator (demodulator). The functions of the following list take place between these two functions and define what is intended by a multiplexing unit:

- 1) **source coding/decoding:** out of mux scope, on top of mux functions;
- 2) **end to end scrambling and access control management:** this scrambling function may apply all over the transmission chain;
- 3) **service multiplexing information insertion/extraction:** each service is described when needed (type of data, coding algorithm, type of segmentation and reassembling technique, type of error

- correction/detection, etc.). Information relative to the end to end scrambling or the time base of the service may also be inserted/extracted;
- 4) **error correction/detection:** optional, a service may require an improved quality (additional error correction) or error detection may be required by the above functions (source coding);
  - 5) **segmentation and reassembling:** the bit stream of each service has to be segmented in order to allow a time division multiplex;
  - 6) **multiplex technique:** several multiplexing techniques are available (position multiplex, fixed or variable length packets with headers, etc.). The most appropriate one may be chosen for each layer. It should however allow a time division multiplex;
  - 7) **transmission media scrambling and access control management:** identical to function 2) but only performed on one transmission link at the transport level, between the mux and demux functions;
  - 8) **channel multiplexing information:** at this level is inserted/extracted tables containing mapping between physical channels information and the logical organization of the services;
  - 9) **frame generation/delineation:** for a frame based transmission, it is the capability to recover the boundaries;
  - 10) **express data transfer:** It is the capability to reserve a subchannel with a high priority access to the data contained in it;
  - 11) **channel coding/decoding and modulation/demodulation:** this is out of the mux unit scope. This function may include error correction facilities in order to ensure the correct transmission quality.

The multiplexing/demultiplexing unit is expected to ensure functions 2) to 10).

## 6 Reference model



Transmission Link TL1 is between a service provider server and a network server.

Transmission Link TL2 is between two (different) network servers.

Transmission Link TL3 is between network servers and transmission station equipment TSE.

Transmission Link TL4 is between a service provider server and a TSE.

Transmission Link TL5 is between two TSE.

Transmission Link TL6 is between TSE and receivers.

**Figure 1: Reference model**

**Service organization hypothesis:**

- a service provider server can be connected to several network servers;
- two different networks can be connected via their network servers. These networks are not necessarily SWIFT networks;
- a TSE belongs to only one network;
- one TSE can be connected to several other TSE.

**Consequences:**

- TL1 and TL2 should be independent of the network organization and transmission mechanisms;
- TL3 and TL4 should permit service multiplexing and insertion at transport level;
- TL5 should permit service multiplexing and insertion at network level.

## **7 Layers organization OSI reference model**

Open Systems Interconnection reference model (OSI reference model) is a means of structuring communication between entities, which may be located at different sites. The OSI reference model is committed to ISO 7498 [5] and ITU-T Recommendation X.200 [6].

### **7.1 Functional layers**

As a main principle of structuring, the model subdivides functionality into 7 functional layers.

Layers 1 to 4 include functions needed for transferring data between computers (transport functions), and Layers 5 to 7 include functions needed to facilitate common transactions between different users at different sites (application functions).

For Layers 1 to 4, functions support the transfer of data, independently of what happens with these data after their transfer.

For Layers 5 to 7, functions should deal with establishment and release of a common understanding between users, which act as the source and sink of the data.

Application functions and transmission functions should be independent of each other, as far as possible.

#### **7.1.1 Physical layer (Layer 1)**

OSI systems are connected by a physical medium, consist of copper conductor, optical fibres, radio waves, or any other medium. The physical layer does not contain the physical medium, but ensures the transmission of data bits (synchronous or asynchronous). Of course, these functions are highly media-dependent.

#### **7.1.2 Data link layer (Layer 2)**

The data link layer adds error recovery and flow control functions to the physical layer. Especially, it processes errors non-corrected by Layer 1. The Layer 2 protocol generally organizes the data into frames.

#### **7.1.3 Network layer (Layer 3)**

The network layer serves to establish, maintain, and clear network connections or to provide connectionless transmission of data units between OSI systems. This layer implies functions such as routing and relaying. Routeing deals with establishing a route between two systems and relaying with the use of intermediate systems data transfer from one data link (or more generally speaking, sub-network) to another data link (belonging to a sub-network which is possibly dissimilar). The functions of this layer are highly dependent on the technology of those communication (sub-) networks.

#### **7.1.4 Transport layer (Layer 4)**

The transport layer serves to establish, maintain, and clear transport connections or to provide connectionless transmission of data units between applications (end-users). It is in charge of the segmentation of the Layer 5 data into packets. Depending on the class of service, the transport layer

ensures the transfer of application-relevant data between users in the right order, without any loss or duplication.

It controls the data flow between the two end-users (global flow control).

#### 7.1.5 Session layer (Layer 5)

The session layer supports the service of enabling users to agree on the beginning or the end of a session or of inserting synchronization points in the structure of a session.

#### 7.1.6 Presentation layer (Layer 6)

Although data transferred between applications can be interpreted in different ways, the presentation layer provides services which facilitate consistent interpretation of them.

#### 7.1.7 Application layer (Layer 7)

All functions to be agreed upon between applications, which are not provided by Layers 1 to 6, have to be provided by Layer 7. Therefore, the application layer includes open-ended functionality.

### 7.2 Services and protocols

A (N) service is the set of facilities provided to a (N+1) entity by the Layer N at the interface between Layer N and Layer N+1. A protocol is a set of rules and formats managing the exchanges between two entities at the same layer. The purpose of a protocol is to provide a service to users (entities) residing above the respective layer boundary. More precisely, a service which is accessible at the boundary between the Layers (N+1) and (N) is provided to (N+1) entities and those above by the functionality of Layers (1) to (N) below it.

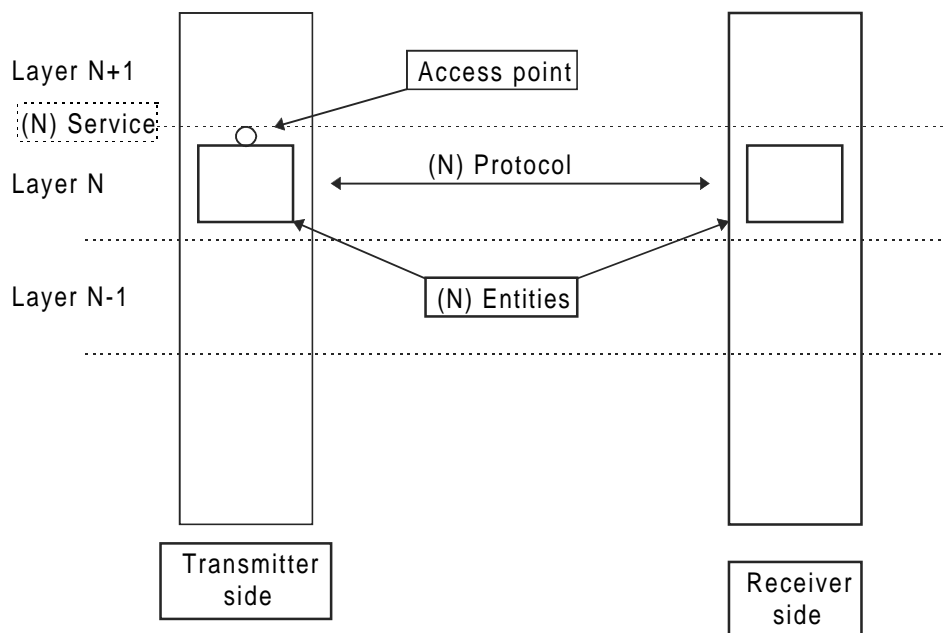


Figure 2

In practice, a service consists of primitives. These primitives can be divided into 4 categories as follows:

- 1) the **REQ**uest primitive type is used when a higher layer is requesting an activity from the next lower layer;
- 2) the **IND**ication primitive type is used by a layer providing a service to inform the next higher layer of an event which is service related;
- 3) the **RES**ponse primitive type is used by a layer to acknowledge the receipt of an **IND**ication primitive type sent by a lower layer;

- 4) the **CONFIRM** primitive type is used by the layer providing the requested service to confirm that the activity has been completed.

### **7.3 Detailed description of Layers 1 to 5**

#### **7.3.1 Layer 1**

##### **7.3.1.1 Service provided by Layer 1**

###### **7.3.1.1.1 Service on the transmitter side**

The transmitter side is responsible for modulating the subcarrier with the data received from Layer 2. The modulated subcarrier is added to the FM multiplex signal.

###### **7.3.1.1.2 Modulation characteristics**

###### **7.3.1.1.2.1 Subcarrier frequency**

The subcarrier frequency is 76 kHz, locked in phase to the fourth harmonics of pilot tone in the case of stereophonic sound. The frequency tolerance shall be within 76 kHz  $\pm$  7,6 Hz (0,01 %) and the phase difference shall not exceed  $\pm$  5 degrees for the phase of pilot tone.

###### **7.3.1.1.2.2 Method of modulation**

The modulation of the subcarrier is LMSK (Level-controlled Minimum Shift Keying) with a spectrum shaping according to figure 4 and table 1. LMSK is a form of MSK in which the amplitude of the modulated subcarrier is controlled by the level of the stereo L-R (left minus right) sound signal. The frequency 76 kHz + 4 kHz is used when the input data is 1 and the frequency 76 kHz - 4 kHz is used when the input data is 0.

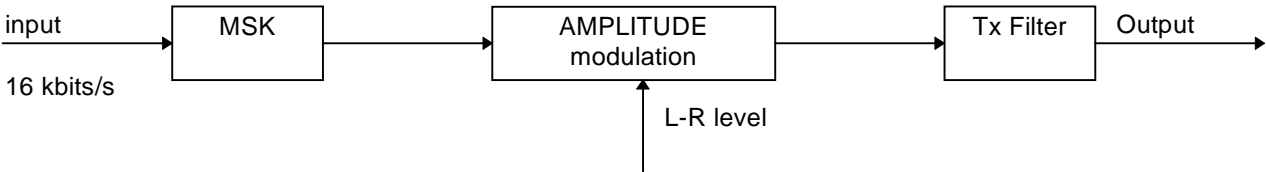


Figure 3

Tx-filter

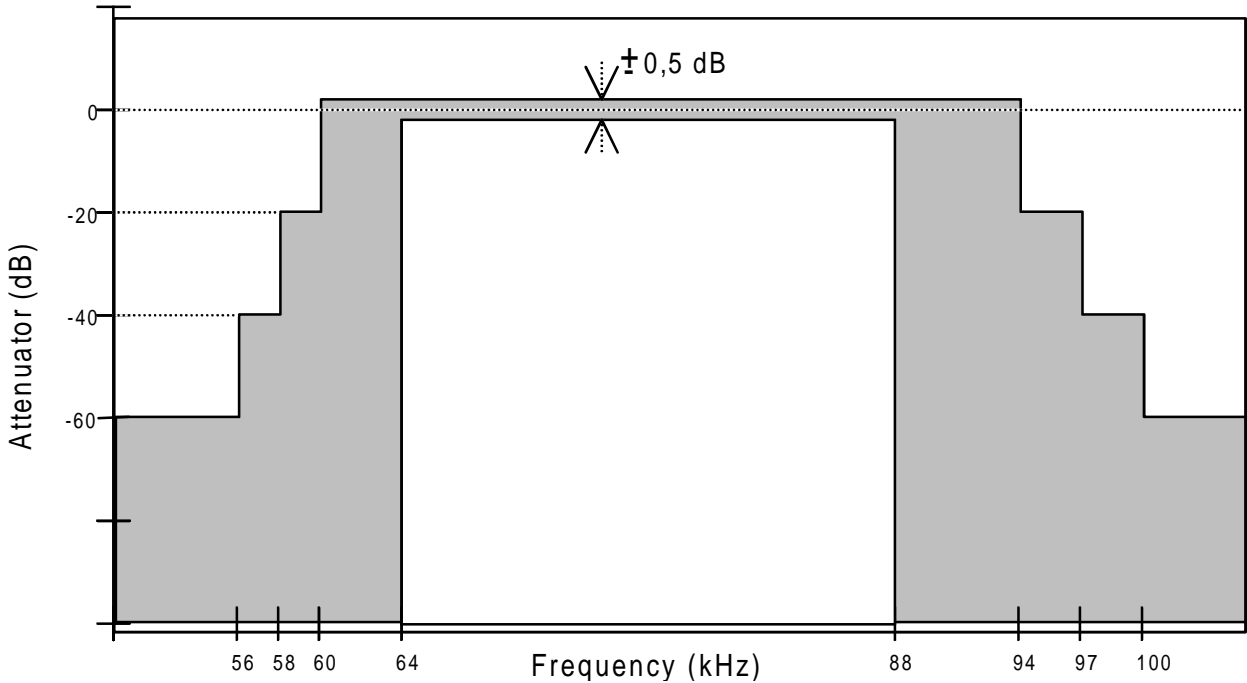


Figure 4

Table 1

Upper bound:	
-60 dB	(Frequency < 56 kHz, 100 kHz ≤ Frequency )
-40 dB	(56 kHz ≤ Frequency < 58 kHz, 97 kHz ≤ Frequency < 100 kHz)
-20 dB	(58 kHz ≤ Frequency < 60 kHz, 94 kHz ≤ Frequency < 97 kHz)
0,5 dB	(60 kHz ≤ Frequency < 94 kHz)
Lower bound:	
-0,5 dB	(64 kHz ≤ Frequency < 88 kHz)

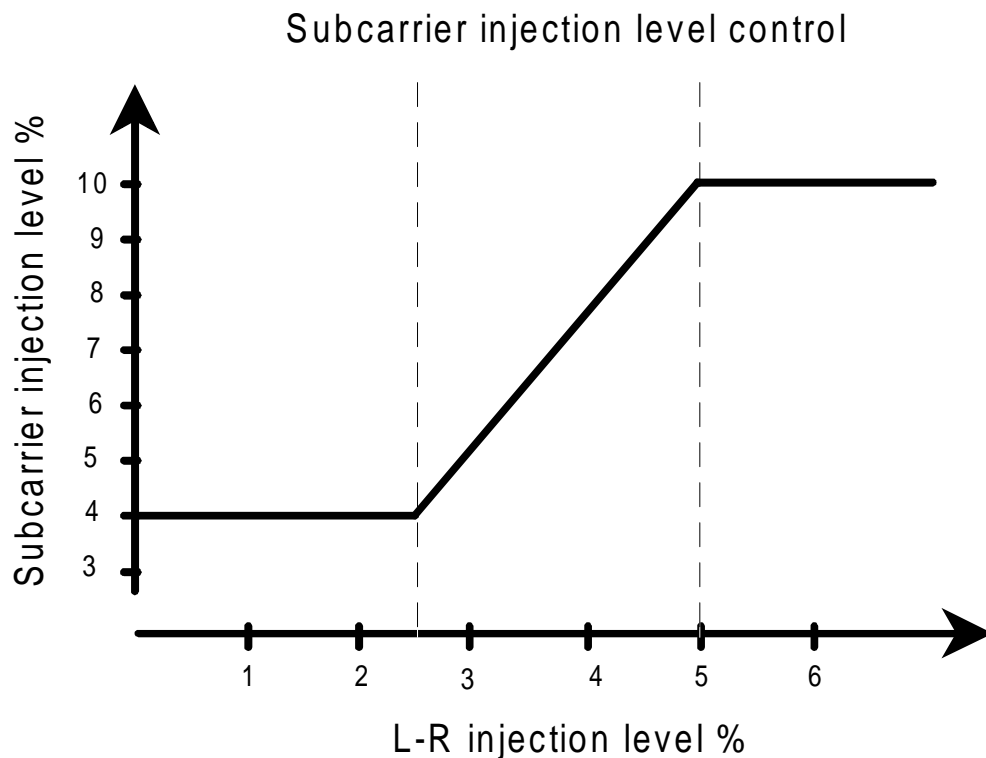
7.3.1.1.2.3 Bit rate

The gross bit rate is 16 kbit/s ±1,6 bit/s.

7.3.1.1.2.4 Subcarrier amplitude

The subcarrier amplitude (injection level) shall be varied depending on the level of the stereo L-R signals (see figure 5). When the deviation of the main FM carrier caused by the stereo L-R signals is less than 2,5 %, the sub-carrier shall cause a deviation of 4 % (± 3 kHz) of the main FM carrier. When the deviation of the main FM carrier caused by the stereo L-R signals is more than 5 %, the sub-carrier shall cause a deviation of up to 10 % (± 7,5 kHz) of the main carrier. Between these limits the subcarrier injection level a linear relation.





**Figure 5**

Where other supplementary signals are transmitted on the parent signal (e.g. the Radio Data System, EN 50067 [1]), the maximum deviation of the main carrier attributable to the subcarrier shall be reduced such that the overall deviation of the main carrier by all the subcarriers (which are not part of the stereo multiplex signal itself), does not exceed 10 % ( $\pm 7,5$  kHz).

#### **7.3.1.1.3 Protection ratios**

SWIFT uses the same Layer 1 as DARC. It fully follows ITU-R Recommendation BS 1194 [7].

Studies conducted in Japan and Sweden showed that:

- the DARC signal does not introduce audible distortion on the audio signal;
- protection ratios either for the audio signal and for the DARC signal comply with ITU-R Recommendation 412 [8].

#### **7.3.1.2 Service on the receiver side**

The receiver side is responsible for extracting the subcarrier from the FM multiplex signal and to demodulate the subcarrier. The data from the demodulated subcarrier is sent to Layer 2.

### **7.3.2 Layer 2**

#### **7.3.2.1 Service provided by Layer 2**

This layer includes logical functions related to the data transmission such as frame synchronization, data formatting, error protection and scrambling.

##### **7.3.2.1.1 Service on the transmitter side**

The transmitter side is responsible for sending Layer 2 frames. Before a frame can be sent, it shall be filled with data, which is done block by block. When Layer 2 has received all 190 blocks constituting a frame, it calculates the 82 parity blocks.

The following services shall be offered by Layer 2 to Layer 3:

- inform that Layer 2 is able to receive a new block (flow control);
- ensure a continuous transmission of blocks to the receiver side when a Layer 2 block have been filled with a data block from Layer 3.

Primitives and their contents:

<b>L2_data.RES (L3-Block)</b>	The Layer 3 sends a L3-block of data (22 Bytes) to the Layer 2.
<b>L2_ready.IND</b>	No parameters. The Layer 2 is ready to receive a L2_data.RES containing a L3-Block and the Layer 3 should send it.
<b>L2_reset.REQ</b>	No parameters.

#### 7.3.2.1.2 Service on the receiver side

The receiver side is responsible for the interpretation of the incoming continuous bit stream. The Layer 2 frames can be identified in the continuous bit-stream after synchronization on frames boundaries.

When Layer 2 has received and decoded a block, it will read the DI flag in the Layer 3 header. If the DI-flag is set, Layer 3 will be able to read the block immediately. Receiving a DARC frame is followed by a decoding of the product code which includes a correction of bit-errors.

The next step is to calculate the checksums of data blocks, and send one block at the time including a parameter that informs Layer 3 of the quality of the data block.

The following services shall be offered to the Layer 3:

- inform if Layer 2 is in a non-synchronized state;
- deliver data blocks. Each data block shall be accompanied by a parameter signalling the quality of the data;
- offer the possibility to force a reset of the DARC circuit.

Primitives and their contents:

<b>L2_data.IND (L3-Block)</b>	The Layer 2 sends a L3-block of data (22 Bytes) to the Layer 3 with a quality parameter indicating the result of the CRC calculation.
<b>L2_no_synch.IND</b>	No parameters.
<b>L2_reset.REQ</b>	No parameters.

### 7.3.2.2 Layer 2 protocol

This layer includes logical functions related to the data transmission such as block and frame synchronization, data formatting, error protection, scrambling for energy dispersal and interleaving.

#### 7.3.2.2.1 Frame structure

The largest element in the data structure is called a "frame" and consists of 78 336 bits. One frame consists of 272 rows of data. Each row contains a block of 288 bits. This block comprises a BIC (Block Identification Code) of 16 bits and a data block of 272 bits. The data blocks may be of two types: information blocks and parity blocks.

There are three specified types of frames: Frame A, Frame B and Frame C. Frame A and B comprise 190 information blocks and 82 parity blocks while frame C comprises 272 information blocks and no parity block. The different frames are distinguished by the BIC codes.

##### 7.3.2.2.1.1 Frame A0

Frame A is a coded frame with 190 information blocks and then 82 parity blocks (see figure 6).

- 60 information blocks with BIC3;
- 70 information blocks with BIC2;
- 60 information blocks with BIC1;
- 82 parity blocks with BIC4.

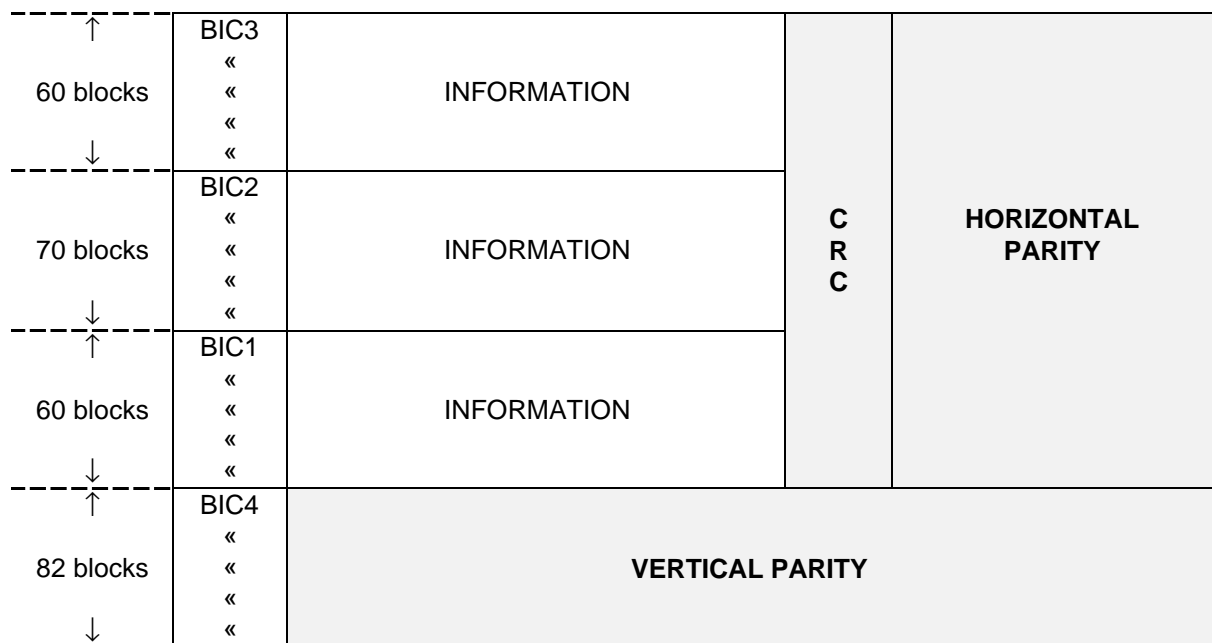


Figure 6

##### 7.3.2.2.1.2 Frame A1

To suppress the delay caused by the 82 parity blocks, information blocks are inserted (inserted blocks or real time blocks) among the 82 parity blocks. This frame is called A1. These inserted blocks are not part of the product coded frame and they are placed at fixed positions four blocks three time. The first four blocks are placed after the 20th parity blocks, next four after another 21 parity blocks and the last four blocks after 21 blocks more. The receivers filters these inserted blocks and decode them immediately. Frame A with 12 inserted blocks is shown in figure 7. In this case, total of blocks from a frame start to the next 272 + 12 blocks. The Block Identification Code (BIC) for inserted blocks is BIC2.

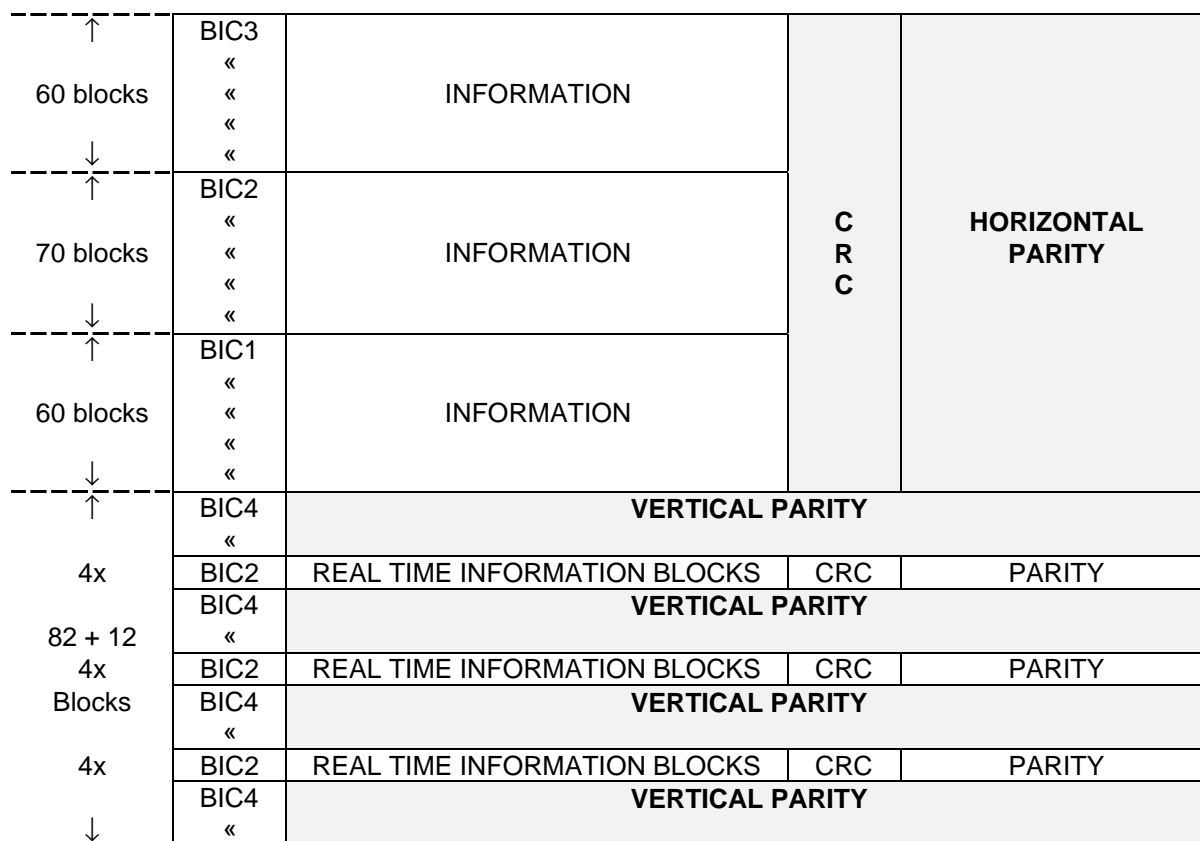


Figure 7

If a delay up to 1,5 second is acceptable, the Frame A without inserted blocks is preferable but otherwise the frame with static insertion of blocks shall be chosen. If all the capacity is used by real time services, it can be preferable to use the Frame C.

A flexible use of Frame A requires the system to inform the receivers if real time blocks are inserted among parity blocks. This type of information is sent in the service channel. It is important that the change of structure appears very seldom.

#### 7.3.2.2.1.3 Frame B

In order to be able to transmit information almost uniformly during the whole frame. Frame B is interleaved with parity blocks in the same frame (see figure 8). Frame B is the frame specified by NHK in Japan.

13 blocks	BIC1	INFORMATION 1	CRC	PARITY
	«	«	«	«
123 blocks	BIC1	INFORMATION 13	CRC	PARITY
	BIC3	INFORMATION 14	CRC	PARITY
	BIC3	INFORMATION 15	CRC	PARITY
	<b>BIC4</b>	<b>PARITY 1</b>		<b>PARITY</b>
	BIC3	INFORMATION 16	CRC	PARITY
	BIC3	INFORMATION 17	CRC	PARITY
	<b>BIC4</b>	<b>PARITY 2</b>		<b>PARITY</b>
	BIC3	INFORMATION 18	CRC	PARITY
	«	«	«	«
	<b>BIC4</b>	<b>PARITY 40</b>		<b>PARITY</b>
	BIC3	INFORMATION 95	CRC	PARITY
	BIC3	INFORMATION 96	CRC	PARITY
13 blocks	<b>BIC4</b>	<b>PARITY 41</b>	<b>7/</b>	<b>PARITY</b>
	BIC2	INFORMATION 97	CRC	PARITY
	«	«	«	«
	BIC2	INFORMATION 109	CRC	PARITY
	BIC3	INFORMATION 110	CRC	PARITY
	BIC3	INFORMATION 111	CRC	PARITY
	<b>BIC4</b>	<b>PARITY 42</b>		<b>PARITY</b>
	BIC3	INFORMATION 112	CRC	PARITY
	BIC3	INFORMATION 113	CRC	PARITY
	<b>BIC4</b>	<b>PARITY 43</b>		<b>PARITY</b>
	BIC3	INFORMATION 114	CRC	PARITY
	«	«	«	«
123 blocks	<b>BIC4</b>	<b>PARITY 81</b>		<b>PARITY</b>
	BIC3	INFORMATION 189	CRC	PARITY
	BIC3	INFORMATION 190	CRC	PARITY
	<b>BIC4</b>	<b>PARITY 82</b>		<b>PARITY</b>

Figure 8

#### 7.3.2.2.1.4 Frame C

Frame C contains 272 information blocks of 288 bits. These information blocks consist of:

- a BIC of 16 bits;
- an information field on 176 bits;
- a CRC on 14 bits;
- a parity field on 82 bits (see figure 9).

BIC3	INFORMATION	CRC	PARITY
------	-------------	-----	--------

Figure 9: Frame C only Block code

#### 7.3.2.3 Information Block

The Information Block comprises:

- 176 Information bits;
- 14 CRC bits;
- 82 parity bits.

BIC3	INFORMATION	CRC	PARITY
← 16 bits →	← 176 bits →	← 14 bits →	← 82 bits →

Figure 10: Information Block with leading BIC

The Information Block is coded with the (272,190) block code, which is a shortened majority logic decodable difference set cyclic code. The generator polynomial for the (272,190) code is given in clause 10.

14 bits of CRC (Cyclic Redundancy Check) are used to enable the receiver/decoder to detect errors. From the 176 information bits, a CRC is calculated using the generator polynomial given in clause 10.

Only information bits can be used for message transport by higher layers.

#### 7.3.2.4 Parity Block

The Parity Block comprises 272 parity bits.

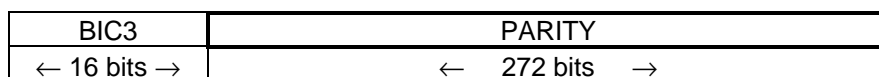


Figure 11: Parity Block with leading BIC

#### 7.3.2.5 Block Identification Code (BIC)

There are four different types of BIC. They have poor cross-correlation with each other, while their auto-correlation function make them suitable for synchronization.

The BIC are used to distinguish Parity Blocks from Information Blocks. They are also used to retrieve frame and block synchronization. The BIC words are fixed and cannot be manipulated by higher layers.

Table 2: BIC coding (16 bits)

<b>BIC1</b>	0001	0011	0101	1110
<b>BIC2</b>	0111	0100	1010	0110
<b>BIC3</b>	1010	0111	1001	0001
<b>BIC4</b>	1100	1000	0111	0101

#### 7.3.2.6 Scrambling

To avoid restrictions on the data input format and to spread the modulation spectrum, data should be scrambled by the PN sequence specified by:

$$g(x) = x^9 + x^4 + 1$$

The starting sequence for the scrambler is 101010101. The scrambler is restarted for each block. The BIC code shall not be scrambled.

### 7.3.3 Layer 3 (Network layer)

#### 7.3.3.1 Service provided by Layer 3

The network service provides data transmission services to the transport layer entities. The following services shall be offered to these entities.

##### 7.3.3.1.1 Service on the transmitter side

- Inform that Layer 3 is able to take care of new messages (flow control);
- transmit message to the receiver side;
- offer the possibility to reset the lower layers.

Primitives and their contents:

<b>L3_LgMsg.RES (LgMsg)</b>	The Layer 4 sends a long message (max. length: 260 Bytes) to the Layer 3.
<b>L3_ShMsg.RES (ShMsg)</b>	The Layer 4 sends a short message (max. length: 120 Bytes).
<b>L3_Table.RES (TNI, Table)</b>	Optionally, the Layer 4 may inform the Layer 3 of the content of the service tables (see subclause 8.3.1 for tables definition). Every table should be accompanied by the Transmitter and Network Identification (TNI) parameter which includes the country code (CID and ECC), the network identification number (NID) and the TSE identification number (TSEID).
<b>L3_ready.IND</b>	No parameters. The Layer 3 is ready to receive a L3_LgMsg.RES, L3_ShMsg.RES or L3_Table.RES containing a long or short message or a table.
<b>L3_reset.REQ</b>	No parameters.

#### **7.3.3.1.2 Service on the receiver side**

- Deliver received messages according to the pre-defined quality of service. The application can choose to deliver messages to the layer above depending on the quality of the received data;
- signal a reception or synchronization problem;
- offer the possibility to reset the lower layers.

Primitives and their contents:

<b>L3_LgMsg.IND (LgMsg, BQA)</b>	The Layer 3 sends a long message to the Layer 4 with a block quality array. The first bit of the block quality array corresponds to the first received block of the message. A binary "0" indicates that the first segment is correct, a binary "1" indicates a fault (the quality of the blocks are given in the primitive L2_data.IND).
<b>L3_ShMsg.IND (ShMsg, BQA)</b>	As L3_LgMsg.IND but for short messages.
<b>L3_error.IND</b>	Cause of the error.
<b>L3_reset.REQ</b>	No parameters.

## 8 Multiplex organization (Layer 3 & 4)

### 8.1 Principles

The basic service is at Layer 4. The end to end addressing, permitting the selection of an application by the users, is made at this level. A long message packet at Layer 4 can be built over the Layer 3 block specification of the DARC system. A DATA GROUP structure is also used over the long message packet for upper layer protocol units.

### 8.2 Definition of logical channel

The first four bits of a Layer 3 block are used as a Service Identity and Logical Channel identifier (SI/LCh) and ensures compatibility at Layer 3 between different systems (SWIFT and other systems using DARC). SWIFT reserves 4 values for implementation as logical channels, 3 of which are at present defined as below.

- The Service Channel "SeCh", SI/LCh = 8 Hex, handling L4 service messages, used to transmit network and service information to the receivers, so that they behave correctly in the SWIFT network.
- The Short Message Channel "SMCh", SI/LCh = 9 Hex, handling L4 short messages, used to transmit data, with real time capabilities.
- The Long Message Channel "LMCh", SI/LCh = A Hex, handling L4 long messages, used to transmit data files.
- The fourth undefined channel, SI/LCh = B Hex, is reserved for future use.

Channel capacity for the services in the logical channels is allocated dynamically but a minimum capacity shall always be left for the service channel (SeCh).

### 8.3 Service Channel "SeCh" (SI/LCh = 8 Hex)

#### 8.3.1 Definition

The Service Channel is divided into 16 different service message types. A service message consist of 1 to 16 L3-blocks where each block corresponds to the information part in an L2-block. The service channel is a Layer 3 link between transmitter and receiver on Layer 3. The service channel transfer service and channel information to the receivers and without this information the receivers cannot synchronize with the accurate physical channel. The structure of a service message is shown in figure 12.

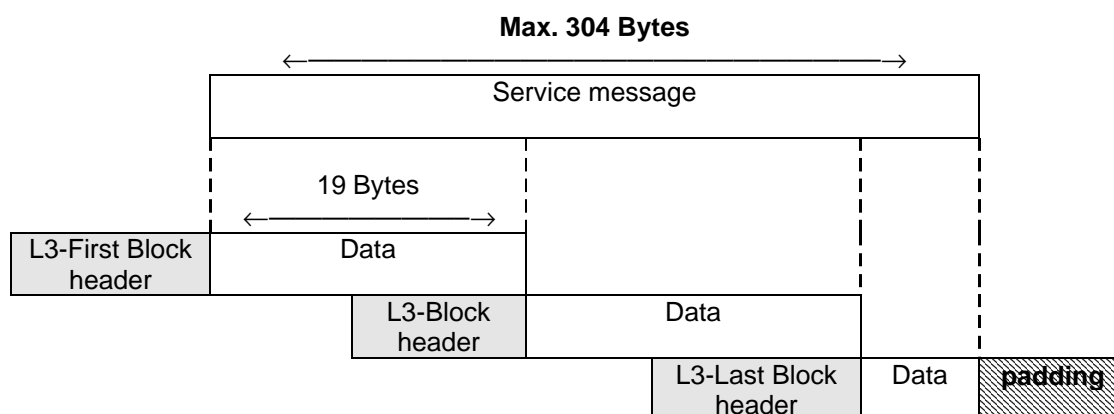


Figure 12: Partition of service messages into L3-blocks

Each Service Block (SeB) consists of a header and 19 Bytes of data. Padding Bytes are added to the last block if needed to complete it. The Service message consists of a maximum number of 16 blocks allowing a maximum length of 304 Bytes.



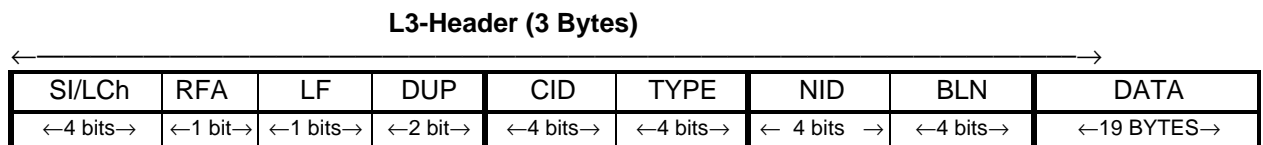
### 8.3.2 Service Channel - Layer 3

The Service Channel L3 structure is designed to enable rebuilding (if needed) of a service message from several service messages using correctly received L3 blocks from different service messages with the same data. This improves the robustness of the service channel. A block number is defined for each L3 header in the service message in order to identify the block's position in the message. If the receiver does not receive a complete service message it may save the correct blocks and use correctly received blocks from further service messages to build the complete message.

The receiver may use the Data UPdate (DUP) field to determine if the service message of a specific service message type has been updated since it was last received. Country ID (CID) and Network ID (NID) are used by the receiver to synchronize to the correct channel.

#### 8.3.2.1 L3-Header SeCh format.

The service block (L3) is defined as follows:



**Figure 13: Format of Service Blocks (SeB)**

**SI/LCh:** Logical Channel field, set to 8 Hex to define the service channel.

**RFA:** Reserved for Future Addition.

**LF:** Last Fragment, flag set to 1 when the block contains the last fragment of Service Message.

**DUP:** Data Update, indicates if the service message has been updated or not. This 2-bit modulo-4 counter is incremented by one each time the service message of this type is updated.

**CID:** Country Identification. The format can be found in EN 50067 [1]. It is the same as the Country Identification (first four bits) in the RDS PI-code.

**TYPE:** Type field (4 bits) takes 16 different values (0-15) and permits to distinguish the nature of the information contained in the data field.

**NID:** Network Identification. The Network Identification allows different networks in a country to be identified.

**BLN:** Block number (4 bits), indicates which block in a specific service message type that it belongs to. Maximum number of blocks is 16. BLN = 0 indicate the first block.

**DATA:** 19 Bytes of service message data.

**Table 3: TYPE significance**

TYPE (binary)	Information
0000	Channel Organization Table (COT)
0001	Alternative Frequency Table (AFT)
0010	Service Alternative Frequency Table (SAFT)
0011	Time, Date, Position & Network nameTable (TDPNT)
Others	Reserved for future addition

### 8.3.3 Service message format

The service message consists of two parts, general information and type specific information.

The general information is defined as follows:

**Table 4: General information**

b7	b6	b5	b4	b3	b2	b1	b0	
Extended Country Code (ECC)								Byte 1
TSE Identification (TSEID)							Message	Byte 2
Length (ML)								Byte 3

**ECC:** Extended Country Code. The format can be found in EN 50067 [1].

**TSEID:** TSE Identification. In a network TSEID gives each TSE within the receiving area a unique number.

**ML:** Message Length. ML describes the message length of the specific information for each service type. The maximum length is  $16 + (15 \times 19) = 301$  Bytes.

The maximum length of a service message, including the general information is  $16 \times 19 = 304$  Bytes.

### 8.3.3.1 Channel Organization Table (COT)

This table contains the services available on the current frequency. It describes, for each service, the addresses and characteristics in the multiplex. The COT shall have highest priority and shall be sent frequently.

**Table 5: COT table**

b7	b6	b5	b4	b3	b2	b1	b0	
Extended Country Code (ECC)								Byte 1
TSE Identification (TSEID)						Message..		Byte 2
... Length (ML)								Byte 3
Service Identity 1...								Byte 4
...(SID)					CA flag	SA		Byte 5
SCA (if CA flag=1)								Byte 6
Service Identity 2...								Byte 7
...(SID)					CA flag	SA		Byte 8
SCA (if CA flag=1)								Byte 7
.....								» »
....								» »
Service Identity n.								» »
...(SID)					CA flag	SA		» »
SCA (if CA flag=1)								Up to
								Byte 304

**Service Identity:** 14 bits. Gives the service a unique address in the system. The value 0 is not allowed.

**CA flag:** Signals a possible use of a conditional access system for this service if set to 1. If CA flag equals 0, the SCA field is not present.

**SA:** Service actuator flag:

- 0 This service is not currently available;
- 1 indicates that the service will shortly be available or is currently available.

**SCA:** Service Conditional Access (see subclause 9.2.2).

### 8.3.3.2 Alternative Frequency Table (AFT)

Alternative frequency lists are concatenated, up to 304 Bytes.

Each list presents the general format:

- number of AFs;
- tuning frequency;
- list of AFs.

Two different formats are defined for coding a list. One format uses less resources for lists with less than 26 frequencies and an other format uses less resources for lists with more than 25 frequencies.

**Table 6: Alternative Frequency Table**

b7	b6	b5	b4	b3	b2	b1	b0	
Extended Country Code (ECC)								Byte 1
TSE Identification (TSEID)							Mes-	Byte 2
... sage Length (ML)								Byte 3
FT		AF_NUMBER (0-62 decimal)						Byte 4
TUNING_FREQUENCY								Byte 5
AF1								Byte 6
AF2								...
...								...
AFi								...
FT		AF_NUMBER (63 in decimal)						...
TUNING_FREQUENCY								...
		AF1						...
					AF2			...
			AF3			AF4		...
...	...	...	...	...	...	...	...	...
		AFi		RFA				...
FT		AF_NUMBER						and so on
TUNING_FREQUENCY								up to
...								Byte 304

**FT:** Frame Type indicates the type of frame that is transmitted on current FM tuning frequency.

**Table 7**

Value	Type of frame
00	A0
01	A1
10	B
11	C

**AF\_NUMBER:** Alternative Frequency Number (6 bits field), the number of alternative frequencies for the tuning frequency presented in the following Byte. A value between 0 and 62 (decimal) included represents the exact AF number and the AFs are coded on one Byte each (format 1). A value of 63 (decimal) means that the AFs are coded on a bitmap field of 26 Bytes (format 2).

For lists shorter than 63 AFs, both formats 1 and 2 can be used. For lists longer than 62 AFs, format 2 shall be used.

The coding is summarized in next table.

**Table 8: Number of AF in the list**

Value (decimal)	Meaning
0	no AF follows
1	1 AF follows
2	2 AFs follow
...	...
62	62 AFs follow
63	AFs bitmap coding

**TUNING\_FREQUENCY:** the frequency for which the following AF list is valid.

The coding is as follows:

**Table 9: AF coding**

Number (decimal)	Carrier frequency (MHz)
0	Reserved for future addition
1	87,6
2	87,7
...	...
...	...
204	107,9
205	Reserved for future addition
...	...
255	Reserved for future addition

**AF:** Alternative Frequency, other frequency on which the same SWIFT network may be found. If the number of AFs for one tuning frequency is lower than 63, the AFs are coded using the tuning frequency coding (format 1), or the bitmap coding (format 2).

If the number of AFs for one tuning frequency is higher than 62 (AF\_NUMBER=63), the AFs are coded on 26 Bytes representing a bitmap field of 208 bits. The bit rank represents the carrier frequency, starting with frequency 87,6 MHz on bit 1 and ending with frequency 107,9 MHz on bit 204. Bits 205 to 208 are reserved.

**Table 10: Bitmap AF coding**

← 26 Bytes →									
bit 1	bit 2	bit 3	...	...	bit 204	bit 205	bit 206	bit 207	bit 208
87,6	87,7	87,8	...	...	107,9	RFA			

The bit value is:

- 0 not an AF frequency;
- 1 AF frequency.

### 8.3.3.3 Service Alternative Frequency Table (SAFT)

This table lists the differences relative to the AFT for services on the SWIFT network. The lists for each service and the SAFT itself are optional, used only if there are differences.

The SAFT consists of concatenated SAF lists. The maximum length of the SAFT is 301 Bytes.

One complete SAF list may include several partial SAF lists related to different AF lists. The complete list consists of:

- service identity;
- SAF list length in Bytes;
- partial SAF lists.

The partial SAF list has the general format:

- tuning frequency of the related AF list;
- number of frequencies to add and subtract;
- list of frequencies to add to and subtract from the related AF list.

**Table 11: SAF table**

b7	b6	b5	b4	b3	b2	b1	b0	
Extended Country Code (ECC)								Byte 1
TSE Identification (TSEID)							Message	Byte 2
Length (ML)								Byte 3
Service..								Byte 4
..Identity 1						RFA		Byte 5
SAF list length								Byte 6
Tuning frequency 1								Byte 7
Number of frequencies to add		Number of frequencies to subtract						Byte 8
Frequency 1 to add » » »								Byte 9 » » »
Frequency n to add » » »								» » »
Frequency 1 to subtract » » »								» » »
Frequency n to subtract » » »								» » »
Tuning frequency 2								» » »
Number of frequencies to add		Number of frequencies to subtract						» » »
...								» » »
Service								» » »
..Identity n						RFA		» » »
SAF list length								» » »
Tuning frequency 1								» » »
Number of frequencies to add		Number of frequencies to subtract						» » »
Frequency 1 to add » » »								» » »
Frequency n to add » » »								» » »
Frequency 1 to subtract » » »								» » »
Frequency n to subtract » » »								» » »
Tuning frequency 2								
...								

and so on  
up to  
Byte 304

**ECC, TSEID and ML:** Are defined earlier.

**Service Identity:** Gives the service for which the SAF list is applicable.

**RFA:** Reserved for future addition.

**SAF list length:** Number of Bytes before the next service identity field.

**Tuning frequency:** The tuning frequency of the AF list for which frequencies should be added and subtracted.

**Number of frequencies to add:** Number of frequencies to add to the AF list.

**Number of frequencies to subtract:** Number of frequencies to subtract from the AF list.

**Frequency to add:** Frequency to add to the AF list. Coded in the same way as in the AFT.

**Frequency to subtract:** Frequency to subtract from the AF list. Coded in the same way as in the AFT.

The same tuning frequency can occur several times for a given service. Thus the number of frequencies to add can be more than 3 and the number of frequencies to subtract can be more than 63 for a given service and a given AF list. The receiver can combine them into a complete partial SAF list.

The bitmap coding used in the AFT is not allowed in the SAFT.

#### 8.3.3.4 Time, Date, Position and Network name Table (TDPNT)

This table contains the time, date, position of the transmitter and network name.

##### 8.3.3.4.1 MJD, Modified-Julian-Date

Table 12: MJD Format

b7	b6	b5	b4	b3	b2	b1	b0	
D/T	Modified-							Byte 1
	-Julian-							Byte 2
	-Date		RFA					Byte 3

**D/T:** Date and Time flag

- 0 indicates that the remaining of the three Bytes gives the time.
- 1 indicates that the remaining of the three Bytes gives the date.

As above, information and detailed formats about these values can be found in the RDS specification EN 50067 [1].

##### 8.3.3.4.2 Time reference

Table 13: Time Format

b7	b6	b5	b4	b3	b2	b1	b0	
D/T	Hours					Mi-		Byte 1
-nutes				sec-				Byte 2
-onds		Local Time Offset						Byte 3

**D/T:** Date and Time flag

- 0 indicates that the remaining of the three Bytes gives the time.
- 1 indicates that the remaining of the three Bytes gives the date.

As above, information and detailed formats about these values (except seconds) can be found in the RDS specification EN 50067 [1].

**Table 14: Position Format**

b7	b6	b5	b4	b3	b2	b1	b0	
P/N	CF	RFA						Byte 1
Frequency of transmitter sec-								Byte 2
Latitude-								Byte 3
coarse								Byte 4
Longitude-								Byte 5
coarse								Byte 6
Latitude fine				Longitude fine				Byte 7

**P/N:** Position and Network flag

- 0 indicates that the remaining of the seven Bytes gives the position of the transmitter.
- 1 indicates that the remaining of the ON Length + 1 of Bytes gives the name of the network.

**CF:** Coarse fine flag

- 0 indicates that there is no fine coarse for the latitude and the longitude.
- 1 indicates that there is a fine coarse for the latitude and the longitude.

**Frequency of Transmitter:** This field gives the frequency of the transmitter where the SWIFT encoder is located.

**Latitude coarse:** This 16-bit field, coded as two's complement number, shall specify the coarse latitude. It shall be calculated by multiplying the value of the Latitude coarse field by  $(90^\circ/2^{15})$ . Southern latitudes shall be considered negative and northern latitudes positive.

**Longitude coarse:** This 16-bit field, coded as two's complement number, shall specify the coarse longitude. It shall be calculated by multiplying the value of the Longitude coarse field by  $(180^\circ/2^{15})$ . West of Greenwich shall be considered negative and east of Greenwich positive.

**Latitude fine:** This 4 bit field shall specify the latitude offset. This unsigned binary number multiplied by  $(90^\circ/2^{19})$  shall be added to the coarse latitude to calculate the latitude with full precision.

**Longitude fine:** This 4 bit field shall specify the longitude offset. This unsigned binary number multiplied by  $(180^\circ/2^{19})$  shall be added to the coarse longitude to calculate the latitude with full precision. Information and detailed formats about the position (Bytes 10 to 14) can be found in the DAB specification ETS 300 401 [4]. It should be noted that the accuracy of the position may be restricted by national laws. If only the coarse fields are used the transmitters are within a square of approximately  $300 \times 300$  m.

**Table 15: Network name Format**

b7	b6	b5	b4	b3	b2	b1	b0	
P/N=1	ON Length				RFA			Byte 1
Character 1								Byte 2
Character 2								Byte 3
...								...
...								...
Character n								...

**P/N:** Position and Network flag

- 0 indicates that the remaining of the seven Bytes gives the position of the transmitter.
- 1 indicates that the remaining of the ON Length + 1 of Bytes gives the name of the network.

**ON Length:** gives the length of the operator name in Bytes. If the operator name is longer than 12 a second block is used.



**Character 1 - n.** The operator name, max. 16 characters.

**Table 16: Time date table**

b7	b6	b5	b4	b3	b2	b1	b0	
Extended Country Code (ECC)								Byte 1
TSE Identification (TSEID)						Message		Byte 2
Length (ML)								Byte 3
DATE/TIME Field								Byte 4
								Byte 5
								Byte 6
Position/Network name								Byte 7
								» » »
								» » »

**ECC:** Extended Country Code. The format can be found in EN 50067 [1].

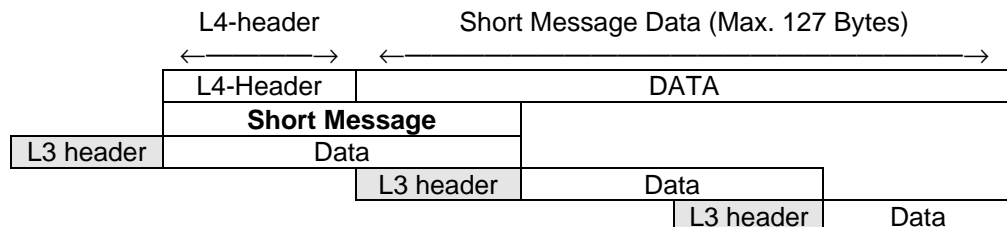
**TSEID:** TSE Identification. In a network TSEID gives each TSE within the receiving area a unique number.

**ML:** Message Length. ML describes the message length of the specific information for each service type. The maximum length is  $16 + (15 \times 19) = 301$  Bytes.

#### 8.4 Short Message Channel "SMCh" (SI/LCh =9 Hex)

The Short Message Channel (SMCh) is compatible with the Fast Information Channel of the DAB specification and SMCh provides a protocol for messages up to 127 Bytes data.

The message is split into consecutive L3-blocks of type 9. These L3-Blocks are 22 Bytes long (2 Bytes for the L3-Header, 20 Bytes for the L3-Data field).



**Figure 14: Short Message Channel Data Unit**

##### 8.4.1 L4-Header SMCh format

EXT	RFA	ADD	EXT ADD (opt.)	CAF	Data Length	SMCCA (opt.)	CRC on L4 header
<1bit>	<1bit>	←6 bits→	←8 bits→	<1bit>	← 7 bits →	←16 or 24 bits→	← 8 bits →

**Figure 15: L4-header SMCh (24,32, 40, 48 or 56 bits) in the Short Message Channel**

**EXT:** Extended address flag, signals, if set to 1, that the extended address field (EXT ADD) is present.

**ADD:** Address used to define a subchannel in the SMCh. See notes at the end of this subclause for the coding of this field.

**EXT ADD:** Extended Address field. Present if the EXT flag is set to 1. See notes at the end of this subclause for the coding of this field.

**CAF:** Conditional Access Flag, set to 1 if the SMCCA field is present.

**Data Length:** Length in Bytes of the data field.

**SMCCA:** Conditional Access field which could be extended. See subclause 9.2.5.

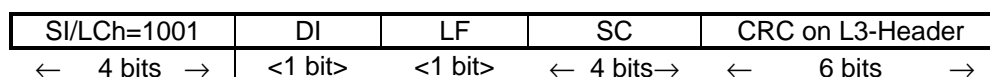
Notes on the coding of the ADD and EXT ADD fields.

NOTE 1: The service Identifier is coded in the ADD and EXT ADD field.

NOTE 2: The ADD field on 6 bits allows coding of service identifiers from 0 to 63. In this case, the EXT ADD field is not required (EXT flag set to 0).

NOTE 3: Service identifiers above 63 are coded on both ADD and EXT ADD fields (EXT flag set to 1). ADD and EXT ADD form a 14 bit field corresponding to the service identifier.

#### 8.4.2 L3-Header SMCh format



**Figure 16: L3-header SMCh (16 bits) in the Short Message Channel**

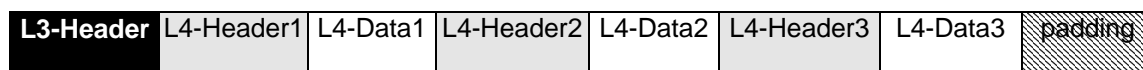
**CRC:** The generator polynomial of CRC and the corresponding shift register are defined in clause 10.

**DI:** Decode Indicator. Set to 1 for real time information.

**LF:** Last Fragment, flag set to 1 when the block contains the last fragment of a short Message.

**SC:** Sequence Counter this 2-bit modulo-4 counter shall be incremented by one for each successive block in a series within the same logical channel (same SI/LCh).

Instead of filling the leftover Bytes of a L3-block after ending of a short message with padding Bytes, it is allowed to have other short messages, probably with another address, in this area. The only stipulation is that the following messages are short enough to take place in the remaining Bytes of the L3-Block. L4 Header of the following message begins directly after the last Byte of previous message.



**Figure 17: An example for L3 - Block within SMCh**

Padding Bytes are set to zero.

## 8.5 Long Message Channel "LMCh" (SI/LCh = A Hex)

In the Long Message channel, data is sent in a variable length packet, called a Long Message, with a header and a data field. These packets are transmitted after their partition into consecutive fixed length L3-Blocks of type A Hex (2 Bytes L3-Header, 20 Bytes data field).

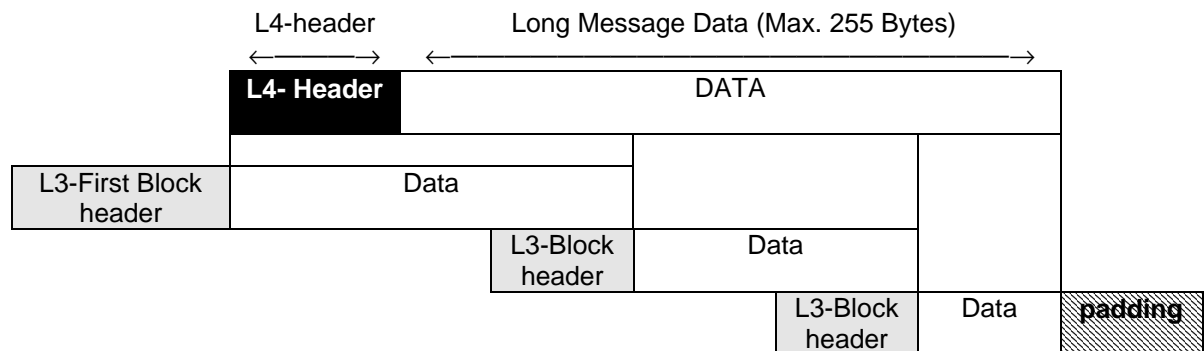


Figure 18: partition of long messages into L3-blocks

### 8.5.1 L4-Header LMCh format

The header of a long message is coded as follow:

RI	CI	F/L	EXT	ADD	EXT ADD (opt.)	RFA (opt.)	COM	CAF	Used Data Length	LMCCA (opt.)	CRC on L4 header
2bits	2 bits	2 bits	1 bit	9 bits	5 bits	3 bits	1 bit	1 bit	8 bits	16 or 24 bits	6 bits

Figure 19: L4- Long Message header in LMCh (32, 48 or 56 bits)

**RI:** Repetition Index, the binary value of this 2-bit field shall signal the remaining number of repetitions of a L4 LMCh message with the same data content. Exceptionally, the binary code 11 shall be used to signal that the repetition continues for an undefined period.

**CI:** Continuity Index, this 2-bit modulo-4 counter shall be incremented by one for each successive non repeat message in a series having the same address. It provides the link between successive messages, carrying the same service, regardless of length.

**F/L:** First/Last Flags. Data may be carried over several long messages. The F/L flag indicates the position of the current long message in a succession of messages, carrying data of the same data group (see subclause 8.6). The following table describes the significance of these flags.

Table 17: Meaning of different F/L values

F/L		
First	Last	
0	0	Intermediate message
0	1	Last message
1	0	First message
1	1	The one and only message

**EXT:** Extended address flag, signals, if set to 1, that the extended address field (EXT ADD) is present. Note that in this case, the 3 RFA bits following the EXT ADD field are also present.

**ADD:** Address used to define a subchannel in the LMCh. It identifies messages carrying a particular service within this subchannel. See notes at the end of this subclause for the coding of this field.

**EXT ADD:** Extended Address field. Present if the EXT flag is set to 1. See notes at the end of this subclause for the coding of this field.

Notes on the coding of the ADD and EXT ADD fields.

NOTE 1: The service Identifier is coded in the ADD and EXT ADD field.

NOTE 2: The ADD field on 9 bits allows coding of service identifiers from 0 to 511. In this case, the EXT ADD field is not required (EXT flag set to 0).

NOTE 3: Service identifiers above 511 are coded on both ADD and EXT ADD fields (EXT flag set to 1). ADD and EXT ADD form a 14 bit field corresponding to the service identifier.

**COM:** Command Flag used to signal special command messages associated to the general data messages of the same subchannel.

0 data message;  
1 command message.

**CAF:** Conditional access Flag, set to "1" if the LMCCA field is present.

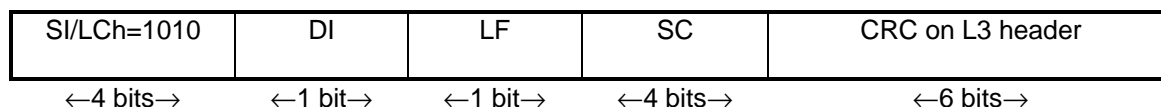
**Data Length:** Length in Bytes of the data field.

**LMCCA:** Conditional Access field which could be extended. See subclause 9.2.4.

**CRC:** The generator polynomial of CRC and the corresponding shift register are defined in subclause 10.

### 8.5.2 L3-Header LMCh format

In this logical channel (LMCh), Data Packets (DP) are divided into L3-Blocks. These Data Blocks shall be coded with the format below.



**Figure 20: L3- Block header in LMCh (16 bits)**

**DI:** Decode Indicator. Set to 1 for real time information.

**LF:** Last Fragment, flag set to 1 when the block contains the last fragment of a long Message.

**SC:** Sequence counter this 2-bit modulo-4 counter shall be incremented by one for each successive block in a series within the same logical channel (same SI/LCh).

**CRC:** The generator polynomial of CRC and the corresponding shift register are defined in subclause 10.

Padding Bytes are set to zero.

### 8.6 Data Group Structure over long messages

Data is structured into Data Groups for transport in one or more long messages (without exceeding 15 long messages per data group). A Data Group (DG) contains a group header, a group data field and optionally a CRC. The data group CRC shall be a 16-bit CRC word calculated on the data group header and data field. See clause 10 for practical implementation of the CRC. Figure 21 shows how a data group is mapped over long messages.

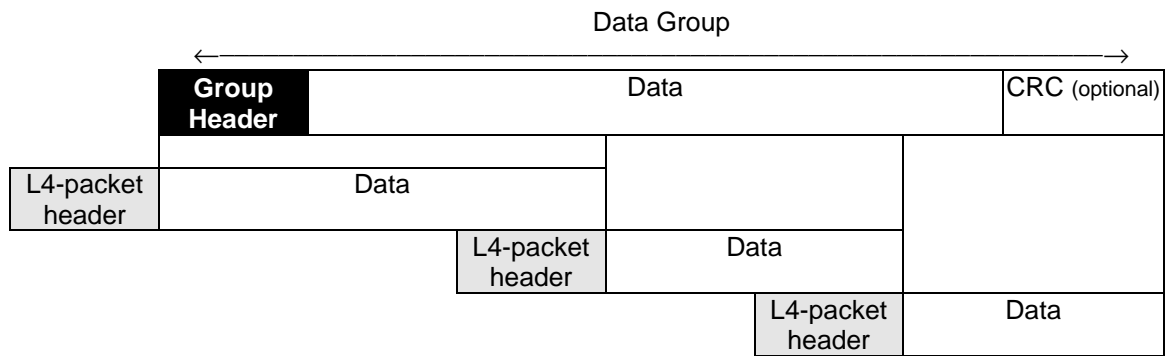


Figure 21: Data units within LMCh

### 8.6.1 L5-Data group header LMCh format

The structure of a data group header is shown in figure 22.

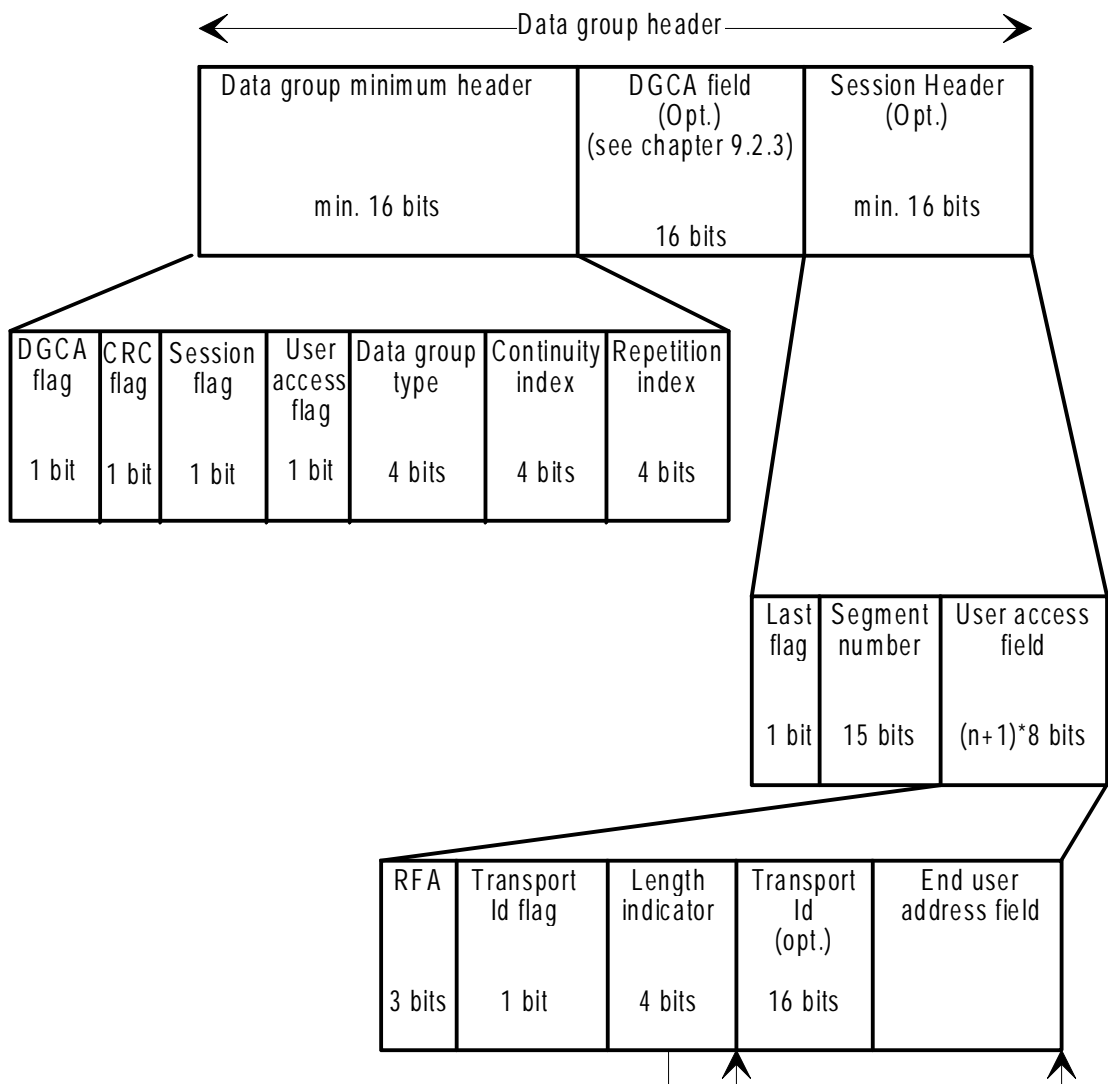


Figure 22: Data Group header (16, 32, 48 or more bits)

#### 8.6.1.1 Fields description of the data group minimum header

**DGCA Flag:** This flag indicates whether the DGCA Field is present or not, as follows:

- 0 no DGCA field;
- 1 DGCA field is present.

**CRC Flag:** This flag indicates whether there is a CRC at the end of the data field of the Data Group, as follows:

- 0 no Data Group CRC;
- 1 Data Group CRC is present.

**Session Flag:** This flag indicates whether the segment number and last flag fields are present or not, as follows:

- 0 No last flag, no Segment Number;
- 1 Last flag and Segment Number present.

**User access Flag:** This flag indicates whether the user access flag is present or not, as follows:

- 0 no User Access field;
- 1 User Access field present.

**Data Group Type:** This 4 bits field defines the type of data carried in the data group data field. The following types are defined (the remaining types are reserved for future definition):

Table 18

b3 b0	Meaning
0 0 0 0	General Data without conditional access parameters (in this case, DGCA flag should be equal to 0, if it is equal to 1, it could be used as a general extension flag)
0 0 0 1	Conditional access Messages (for example ECMs and EMMs)
0 0 1 0	General Data possibly with conditional access parameters (in this case, DGCA flag should be equal to 1 if there are actually conditional access parameters, otherwise it could be equal to 0)
0 0 1 1	MOT header information
0 1 0 0	MOT data without conditional access parameters (in this case, DGCA flag should be equal to 0, if it is equal to 1, it could be used as a general extension flag)
0 1 0 1	MOT data possibly with conditional access parameters (in this case, DGCA flag should be equal to 1 if there are actually conditional access parameters, otherwise it could be equal to 0)
1 1 0 0	SWIFT Reserved for file transfer description

**Continuity Index:** The binary value of this 4-bits field shall be incremented each time a data group of a particular type is transmitted with a content different from that of the immediately preceding data group of the same type.

**Repetition Index:** The binary value of this 4 bits field shall signal the remaining number of repetitions of a data group with the same data content, occurring in successive data groups of the same type. Exceptionally, the code "1111" shall be used to signal that the repetition continues for an undefined period.

#### 8.6.1.2 Description of the DGCA field

**DGCA Field:** Data Group Conditional Access field. This field is present if the DGCA flag is equal to 1. See subclause 9.2.3. for the complete description.

#### 8.6.1.3 Fields description of the session header

The session header is composed by three fields as follows:

Last Flag	Segment Number	User Access Field
1 bit	15 bits	n+1 Bytes

**Figure 23: Session Header**

**Last Flag:** This 1-bit flag indicates whether the segment number field is the last or whether there are more to be transmitted, as follows:

- 0 more segments to follow;
- 1 last segment.

**Segment Number:** This field is present when the corresponding flag is set.

This field is coded as an unsigned binary segment number in the range  $0-(2^{15}-1)$ . The first segment is numbered 0 and the segment number is incremented by one at each new segment, until reaching the last segment.

#### 8.6.1.3.1 User Access field

**RFA:** Reserved for Future Additions.

**Transport Id Flag:** This flag indicates whether the transport Id field is present, or not, as follows:

- 0 no Transport Id Field;
- 1 Transport Id Filed present.

**Length Indicator:** This 4 bit field codes the length in Bytes of both Transport Id field and address field (from 0 to 15). If it equals 0 none of these fields is present.

**Transport Id:** This field is always two Bytes long. It uniquely identifies one data object (file and header information) from a stream of such objects. It is used to indicate that the data carried in the data group belongs or relates to the same object.

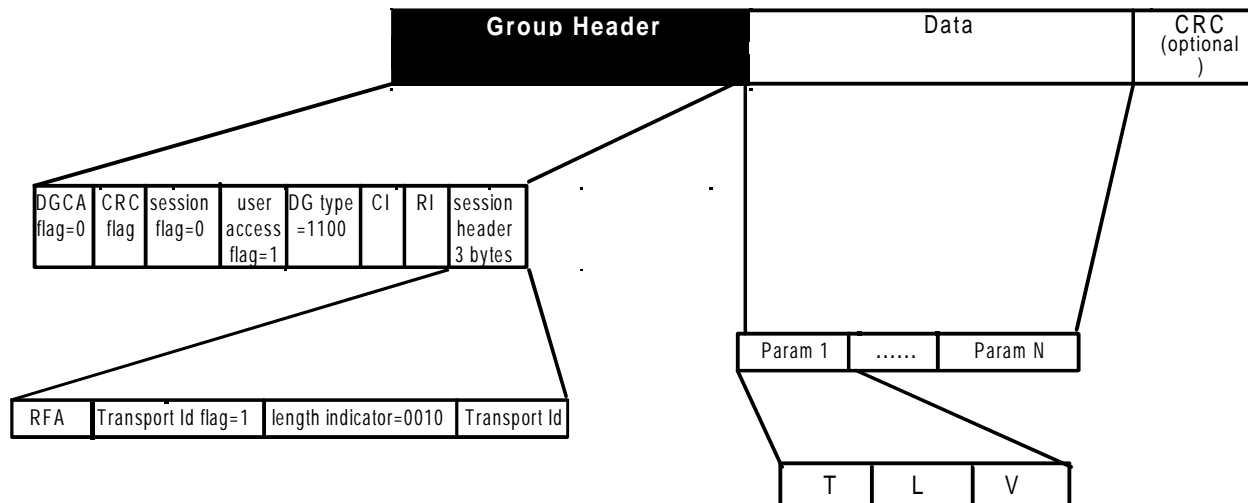
**End user address field:** This field when present indicates the address of the end user on one or more Bytes (up to 15).

#### 8.6.2 Coding of the data group type 12

File transfer information (e.g. file name) and possibly application information on a file being broadcasted could be given using data group type 12.

The link between the data group type 12 and its associated data file (data groups type 0 or 2) is provided by the Transport Id field defining a unique identifier of the two objects.

Data group type 12 has a specific format described below:



**Figure 24: Coding of File Transfer Description Data Groups**

The information field is coded using the TLV format for each parameter (information).

**T:** Parameter tag.

**L:** Length of value field on one Byte if  $L < 255$ , on three Bytes if  $L > 254$  (in that case, first Byte = FF Hex, two other Bytes = Length).

**V:** Parameter value.

TLV parameters are coded according to ETS 300 075 [2].

## 9 Conditional Access (CA)

The Conditional Access system includes three main functions: scrambling/descrambling, entitlement checking and entitlement management.

The scrambling/descrambling function aims to make the service incomprehensible to unauthorized users. Descrambling can be achieved by any receiver having an appropriate descrambler and holding a secret Control Word (CW).

The entitlement checking function consists of broadcasting the conditions required to access a service together with encrypted secret codes to enable the descrambling for authorized receivers. These codes are sent inside dedicated messages called Entitlement Checking Messages (ECMs) and these are carried in the Multiplex.

Generally, scrambling is applied to service data using separate Control Words for each service but a common Control Word may be shared by referring to common ECMs carried in a specific subchannel shared by several services.

The entitlement management function consists of distributing entitlements to receivers. There are several kinds of entitlements matching different means of subscribing to a service: subscription per theme or class, pre-booked pay-per-programme or impulse pay-per-programme, per service or per time. This information is sent inside dedicated messages called Entitlement Management Messages (EMMs) and these may be carried in the same multiplex as the scrambled services or may not.

The control and management functions require the use of secret keys and cryptographic algorithms.

This clause describes the mechanisms available to control access to service sent in the SWIFT multiplex. Subclause 9.1 describes the scrambling/descrambling procedures for data. These procedures are completely independent of any other scrambling procedures that may also be performed on the signal (for



example energy dispersal scrambling). Subclause 9.2 describes the parameters which are used to provide signalling and synchronization for access control. Subclause 9.3 describes the different possibilities that can be used to send the access control messages (ECMs and EMMs).

## **9.1 Scrambling data**

### **9.1.1 Introduction**

For each service, a Conditional Access flag (CA flag) and/or a Conditional Access Identifier (CAId) shall be used to indicate whether or not the service uses Conditional Access mechanisms and, if so, which kind of mechanism is used.

When no Conditional Access mechanism is used, the service shall not be scrambled.

When Conditional Access mechanisms are used, the service shall be sent in one of these three different scrambling modes:

- a) unscrambled;
- b) scrambled with a specific Control Word (CW), called local Control Word, which is permanently installed in the receiver;
- c) scrambled with a Control Word which is changed regularly. The new value of the CW is sent encrypted to receivers in the Entitlement Checking Messages (ECMs).

In scrambling modes a) and b), no subscription is needed. The service is said to be in free access mode.

In scrambling mode c), a subscription is required to recover the encrypted control word. The service is said to be in controlled access mode.

In order to scramble data, a Pseudo-Random Binary Sequence (PRBS) is added modulo 2 to the useful data.

Padding Bytes, packet headers and CRCs are not scrambled. Short messages headers are not scrambled.

The PRBS generator is described in the subclause 12.2 of ETS 300 174 [3].

### **9.1.2 Generating scrambling and descrambling sequences**

#### **9.1.2.1 Initialization Word (IW)**

The Initialization Word is a bit string which shall be used to initialize the PRBS generator. It includes 10 Bytes which shall be inserted in the PRBS, most significant Byte first, Byte by Byte. It involves two parts, the Initialization Modifier (IM) and the Control Word (CW):

- a) the Initialization Modifier (IM) varies very often and is used to modify the Initialization Word at each new initialization of the PRBS generator. The PRBS generator is reinitialized very often to allow fast (re)synchronization of the scrambler and the descrambler and to prevent the output of very long scrambling/descrambling sequences. The Initialization Modifier comprises a number (in DGCA, LMCCA or SMCCA);
- b) the Control Word (CW) is changed less often and provides the "secret key" used to scramble and descramble the service data. The Control Word shall be 64 bits long. In free access mode, the Control Word is fixed and stored in the receiver. In controlled access mode, the Control Word shall be provided by the Access Control System (ACS).

### 9.1.2.2 Phasing

The period during which a Control Word is valid is called a phase. Each phase shall be allocated a parity (even or odd), which toggles for each new phase. A phase parity flag shall be used to indicate the parity of the current phase. This flag is located in the DGCA, LMCCA, and SMCCA.

### 9.1.3 Scrambling/descrambling processes

This subclause specifies two different Conditional Access signalling configurations and the way Conditional Access is incorporated into the different data transport mechanisms.

#### 9.1.3.1 Conditional Access signalling configurations

The different signalling configurations authorized for one service are summarized in table 19.

**Table 19: Configurations for ECM and EMM locations**

Config.	SCA content (see subclause 9.2.2)	ECM Location	EMM Location
1	not transmitted	In LMCh, with: - Data Group type =0001 - command packets - same packet address as data packets	In LMCh, with: - Data Group type =0001 - command packets - same packet address as data packets
2	not transmitted	In LMCh, with: - Data Group type =0001 - command packets - same packet address as data packets	In a common LMCh subchannel with: - Data Group type =0001 - command packets - address=11 1111 1100 0000
3	MM=10 LMC_ECMId (ECM long message address)	In a LMCh subchannel with: - Data Group type =0001 - command packets - address identified by LMC_ECMId and IND=0	In a common LMCh subchannel with: - Data Group type =0001 - command packets - address=11 1111 1100 0000
4	MM=01 SMC_ECMId (ECM short message address)	in SMCh short messages with address identified by SMC_ECMId	In a common LMCh subchannel with: - Data Group type =0001 - command packets - address=11 1111 1100 0000
5	MM=00 SMC_ECMId	in SMCh short messages with address identified by SMC_ECMId	in SMCh short messages with: - address=11 1111 1100 0000
6	MM= 11 EMM flag=0	In LMCh, with: - Data Group type =0001 - command packets - same packet address as data packets	In LMCh, with: - Data Group type =0001 - command packets - same packet address as data packets
7	MM=11 EMM flag=1	In LMCh, with: - Data Group type =0001 - command packets - same packet address as data packets	In a common LMCh subchannel with: - Data Group type =0001 - command packets - address=11 1111 1100 0000

**Table 20: Allowed configurations depending on data location**

Data Location	SCA location	IM, Flags Location	Allowed configurations for ECM and EMM locations
Data Group with type=0000	COT	DGCA in the Data Group Header	3, 4, 5, 6 and 7
Data Group with type=0010	not transmitted	DGCA in the Data Group Header	1 and 2
Long Message	not transmitted	LMCCA in the long message header	not allowed case
Long Message	COT	LMCCA in the long message header	not allowed case (reserved for data group level)
Long Message	LMCCA_Ext (Byte 3) in the long message header	LMCCA_Ext in the long message header	3, 4 and 5
Short Message	not transmitted	SMCCA in the short message header	not allowed case
Short Message	COT	SMCCA in the short message header	3, 4 and 5
Short Message	SMCCA_Ext(Byte 3) in the short message header	SMCCA_Ext in the short message header	3, 4 and 5
<b>NOTES:</b> Conditional Access at long message level using indirect signalling in COT is not allowed for compatibility reasons with conditional access at data group level. In configuration 6 and 7, SCA is exclusively transmitted in COT. Configurations 1 and 2, are not distinguishable at the receiving end. The only difference between them concerns the location of the EMMs. Consequently, in that case, the receiving end will have to fetch them in priority in the common EMM subchannel. Simple implementations may let the Layer 5 process EMM data groups at service level.			

#### 9.1.3.2 Scrambling/Descrambling of the service in Data Groups

In this case, the data is already organized in data groups. The Initialization Modifier, the phase parity, the scrambling mode and the updating bits shall be sent at the beginning of each of these data groups in a parameter called DGCA. Scrambling is performed on the data group data field only. The data group header and the DGCA field are not scrambled. The data group CRC is performed on the unscrambled data group Header, the unscrambled DGCA field and the scrambled data group data field.

The PRBS generator shall be initialized at the beginning of the data group with the following initialization Word (MSB first):

10 bits of Initialization Modifier	6 bits "000000"	64 bits CW
------------------------------------	-----------------	------------

**Figure 25**

#### 9.1.3.3 Scrambling/Descrambling of the service in the Long Message Channel

In this case, messages are only organized in long message packets. The Initialization Modifier, the phase parity, the scrambling mode and the updating bits shall be sent at the beginning of each of these long message packets in a parameter called LMCCA (optionally in the first packet of a long message). Scrambling is performed on the packet data field only. The packet header is not scrambled.

The PRBS generator shall be initialized at the beginning of the LMCh packets with the following initialization Word (MSB first):



Figure 26

#### 9.1.3.4 Scrambling/Descrambling of the service sent in SMCh

For service sent in SMCh, scrambling is performed individually on each short message data field, before data is organized in the SMCh format.

The initialization modifier, the phase parity, the scrambling mode and updating bits shall be sent at the beginning of each of these short messages in a parameter called SMCCA or SMCCA\_Ext. Scrambling is performed on the data field only. The header is not scrambled.

#### 9.1.3.5 DAB compatibility

The compatibility between DAB and SWIFT for exchanging data is natural at Data Group level. The format is the same for this structure in the two systems.

Compatibility is also possible at the Short Message Channel (SMCh) level for the transport of DAB Fast Information Groups (FIG) (see ETS 300 401 [4]). In that case, FIG type 5 are used for carrying services and FIG type 6 for carrying ECMs and EMMs. These two kinds of FIG should be inserted in the SWIFT multiplex in the SMCh. A special subchannel with address 11 1111 1111 1111 (3FFF Hex) is dedicated for this purpose.

The structure of FIG type 5, when scrambled, is shown in figure 27.

← FIG type 5 header + added Bytes →

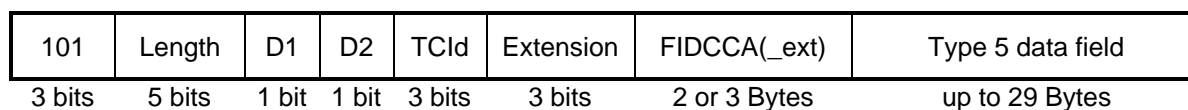


Figure 27

See ETS 300 401 [4] for details and definitions.

The structure of FIG type 6, when used for ECMs and EMMs, is shown in figure 28.

← FIG type 6 header →

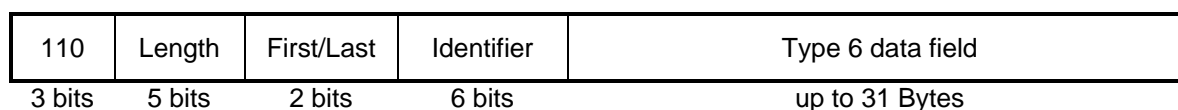


Figure 28

See ETS 300 401 [4] for details and definitions.

The FIDCCA and FIDCCA\_ext purpose, format and definition are the same as SMCCA and SMCCA\_ext described in subclause 9.2.5.

They contain mainly the Initialization modifier IM, the Messaging Mode (MM) and the FIG type 6 Identifier FIC\_ECMId (with also phase parity, scrambling mode and updating bits).

Table 21

Config.	SCA content (see subclause 9.2.2)	ECM Location	EMM Location
8	MM=01 FIC_ECMId	in FIG type 6 messages identified by FIC_ECMId	In a common LMCh subchannel with: - Data Group type =0001 - command packets - address = 11 1111 1100 0000
9	MM=00 FIC_ECMId	in FIG type 6 messages identified by FIC_ECMId	in FIG type 6 messages with: - address = 11 1111 1100 0000

Only these two configurations are allowed for the ECMs and EMMs locations when scrambled data is carried inside FIG type 5 messages.

The PRBS generator shall be initialized, for each new scrambled FIG type 5 message, with the following Initialization Word (MSB first):

10 bits of Initialization Modifier	6 bits "000000"	64 bits CW
------------------------------------	-----------------	------------

Figure 29

For service sent in SMCh, scrambling is performed individually on each SMCh service data, before data is organized in FIG type 5 format.

## 9.2 Signalling and synchronizing data

This subclause describes all the Access Control parameters which are used to provide signalling and synchronization for Conditional Access.

### 9.2.1 Conditional Access Identifier (CAId)

This 3-bits field shall identify the Conditional Access system used for a given service.

If no access control system is used for the service, CAId shall be equal to 000.

For the existing access control systems, the coding of CAId shall be as follows:

Table 22

CAId MSB LSB	Meaning
0 0 0	no CA for the service
0 0 1	NR-MSK
0 1 0	Eurocrypt
other	reserved for future definition

### 9.2.2 Service Conditional Access (SCA)

For each access controlled service, the SCA contains the parameters necessary for descrambling. The SCA comprises one Byte as described in the following two subclauses. This Byte, if significant, indicates how to find the ECMs and the possible EMMs of the access controlled service. The SCA is sent either in the COT, or in SMCCA\_Ext or in LMCCA\_Ext.

The ECMs could be sent:

- in SMCh messages with address given by SCA content;
- in a LMCh subchannel with address given by SCA content;

- in the same LMCh subchannel as the service data (in command packets with same address as related data packets of the service data).

This last option is possible only for service data sent in the LMCh.

The EMM could be sent:

- in SMCh messages with address = 11 1111 1100 0000;
- in a common LMCh subchannel with address = 11 1111 1100 0000;
- in the same LMCh Subchannel as the service itself, together with ECM.

For FIG type 5 messages in SMCh, ECMs are sent in SMCh FIG type 6 and EMMs either in SMCh FIG type 6 messages or in the common LMCh subchannel.

Figure 30 describes the different parameters of SCA:



**Figure 30**

MM defines the messaging modes and ECMId is part of the address of the ECM subchannel:

- in the LMCh (LMC\_ECMId);
- in the SMCh (SMC\_ECMId);
- in FIG type 6 (FIC\_ECMId).

Full ECM subchannel address is got as follow:

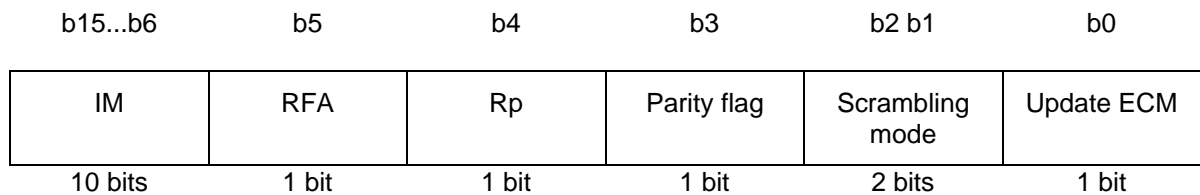
- in the LMCh: ADD= 11 1111 1100 0000 + LMC\_ECMId;
- in the SMCh: ADD= 11 1111 1100 0000 + SMC\_ECMId;
- in FIG type 6 with ID=FIC\_ECMId in SMCh with address 11 1111 1111 1111.

**Table 23**

MM	Significance
00	ECMs and EMMs are sent in SMCh short messages. The bits b5 to b0 shall indicate the value of the ECM Identifier which is used to identify the address of the ECMs (SMC_ECMId). The address: 11 1111 1100 0000 is reserved for the EMM messages.
01	The ECMs shall be sent in the SMCh and the EMMs in the LMCh in a common subchannel identified by the address: 11 1111 1100 0000. The bits b5 to b0 shall indicate the value of the ECM Identifier (SMC_ECMId) which is used to identify the address of the ECMs in the SMCh. The 000000 and 111111 values are not allowed for SMC_ECMId.
10	In this case, the ECM shall be sent in the LMCh in a subchannel identified by the value of the ECM Identifier ECMId (LMC_ECMId) which is used for the 6 LSB of the address of the packets transporting these ECMs, the 3 MSB being set to 1. The value 000000 is not allowed for LMC_ECMId. The EMM shall be sent in the LMCh in a common subchannel identified by the address: 11 1111 1100 0000.
11	In this case: <ul style="list-style-type: none"> <li>- ECMs are sent in the same subchannel as the service (only when transmitted in LMCh)</li> <li>- SCA is exclusively transmitted in the COT</li> <li>- Bit b5 of SCA shall be considered as an EMM flag which signals: <ul style="list-style-type: none"> <li>if set to 1, that EMMs are sent in the same subchannel as the service (configuration 6)</li> <li>if set to 0, that EMMs are sent in a common LMCh subchannel with address = 11 1111 1100 0000.</li> </ul> </li> </ul>

### 9.2.3 Data Group Conditional Access (DGCA)

This 16-bit parameter is used to transport the Initialization Modifier (IM) and the scrambling flags in the headers of the data groups carrying the service data. The command bit of packet headers shall be set to 0 (data). The coding of DGCA is described in figure 31:



**Figure 31: Coding of the Data Group Conditional Access (DGCA) field**

**Initialization Modifier (IM):** This 10-bit parameter shall be used together with the Control Word to form the initialization word used to initialize the PRBS generator.

**RFA:** This bit shall be reserved for future additions. The bit shall be set to zero until it is defined.

**Rp:** This bit shall be reserved for replacement operations. It indicates to the receiver when to take into account the replacement characteristics given by the ACS if it is in blackout state as follows:

- 0 replacement is inactive;
- 1 replacement is active and the receiver has to take into account the replacement characteristics given by the access control system.

**Parity flag:** This flag shall be used to indicate the parity of the current phase as follows:

- 0 even parity;
- 1 odd parity.

**Scrambling mode:** This two-bit parameter shall define the scrambling mode, as in table 24:

**Table 24**

b2 b1	
0 0	not allowed
0 1	unscrambled
1 0	free access (i.e. scrambled with a local Control Word)
1 1	controlled access (i.e. scrambled with a Control Word regularly transmitted and changed with ECMs)

**Update ECM:** This flag shall indicate a change in the ECM transmission and make the descrambler read the next ECM:

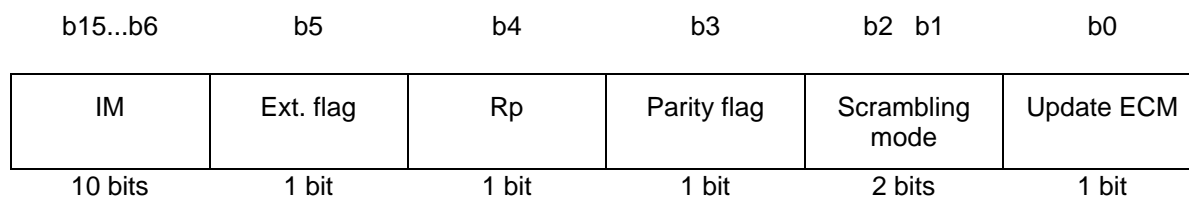
- 0 no update;
- 1 update ECM. Next ECM shall be sent to the ACS.

### 9.2.4 Long Message Channel Conditional Access (LMCCA and LMCCA\_Ext)

#### 9.2.4.1 LMCCA

LMCCA is a 16-bit parameter which is used to transport the Initialization Modifier (IM) and some scrambling flags at the start of LMCh packets transporting the service data. This parameter shall exist if the CA flag of the service Data Group is set to 1.

The coding of LMCCA is described in figure 32:



**Figure 32: LMCCA field without extension**

**Initialization Modifier:** This 10-bit parameter shall be used together with the Control Word to form the initialization word used to initialize the PRBS generator.

**Ext. flag:** This one bit flag shall distinguish between LMCCA and LMCCA\_Ext:

- 0 LMCCA;
- 1 LMCCA\_Ext.

**Rp:** This bit shall be reserved for replacement operations. It should indicate to the receiver when to take into account the replacement characteristics given by the ACS if it is in blackout state, as follows:

- 0 replacement is inactive;
- 1 replacement is active and the receiver has to take into account the replacement characteristics given by the Access Control System (ACS).

**Parity flag:** This flag shall be used to indicate the parity of the current phase as follows:

- 0 even parity;
- 1 odd parity.

**Scrambling mode:** This two-bit parameter describes the scrambling mode as in table 25:

**Table 25**

b2 b1	Meaning
0 0	not allowed
0 1	unscrambled
1 0	free access (i.e. scrambled with a local Control Word)
1 1	controlled access (i.e. scrambled with a Control Word regularly transmitted and changed with ECMs)

**Update ECM:** This flag shall indicate a change in the ECM transmission and it makes the descrambler read the next ECM:

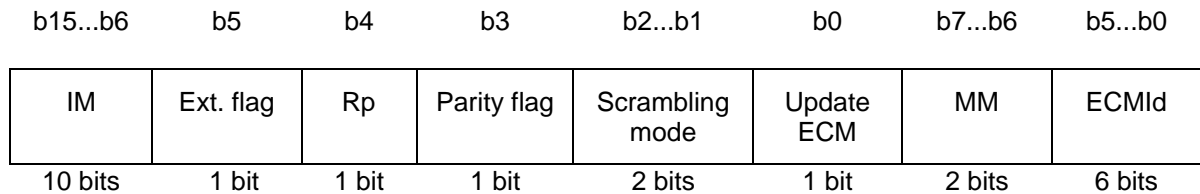
- 0 no update;
- 1 update ECM. Next ECM shall be sent to the ACS.

#### 9.2.4.2 LMCCA\_Extended

LMCCA\_Extended is a 24-bit parameter consisting of LMCCA and the Byte SCA indicating where the ECMs of the service can be found.



The coding of LMCCA\_Ext is described in figure 33.



**Figure 33: Coding of the LMCCA - Extended field**

The first two Bytes are the same as for LMCCA. The remaining parameters are defined as follows:

**MM = 00:**

- In this case, the ECMs and the EMMs shall be sent in the SMCh in message type 3.
- The bits b5 to b0 shall indicate the value of the ECM Identifier (SMC\_ECMId) which is used to identify the structure containing the ECM message. Values 000000 and 111111 are not allowed.

**MM = 01:**

- In this case, the ECMs shall be sent in the SMCh in message type 3 and the EMMs shall be sent in the LMCh subchannel identified by the packet address: 11 1111 1100 0000.
- The bits b5 to b0 shall indicate the value of the ECM Identifier (SMC\_ECMId) which is used to identify the address of the ECM message. The value 000000 is not allowed.

**MM = 10:**

- In this case, the ECM and the EMM shall be sent in the LMCh.
- The bits b5 to b0 shall indicate the value of the ECM Identifier (LMC\_ECMId) which is used to identify the address of the ECM message (6 LSB of the address of the packets transporting these ECMs). The value 000000 is not allowed. The 8 MSB are set to 1 to complete the address. The EMMs shall be sent in the LMCh subchannel identified by the packet address: 11 1111 1100 0000.

**MM = 11:**

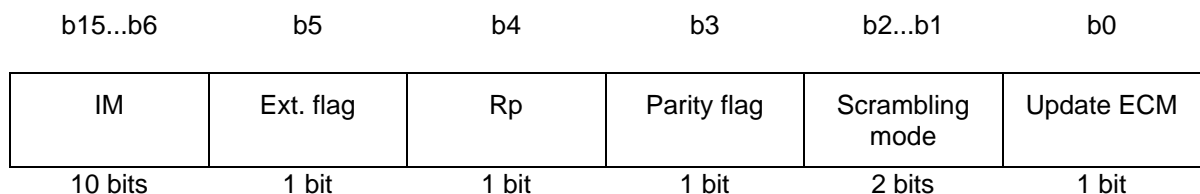
- This case shall be reserved for future use.

## 9.2.5 Short Message Channel Conditional Access (SMCCA and SMCCA\_Ext)

### 9.2.5.1 SMCCA

SMCCA is a 16-bit parameter which is used to transport the Initialization Modifier (IM) and some scrambling flags at the start of SMCh messages transporting the service. This parameter shall exist if the CA flag of the service short message is set to 1 and/or if CAId is not equal to zero.

The coding of SMCCA is described in figure 34:



**Figure 34: SMCCA field without extension**

**Initialization Modifier:** This 10-bit parameter shall be used together with the Control Word to form the initialization word used to initialize the PRBS generator.

**Ext. flag:** This one bit flag shall distinguish between SMCCA and SMCCA\_Ext:

- 0 SMCCA;
- 1 SMCCA\_Ext.

**Rp:** This bit shall be reserved for replacement operations. It should indicate to the receiver when to take into account the replacement characteristics given by the ACS if it is in blackout state, as follows:

- 0 replacement is inactive;
- 1 replacement is active and the receiver has to take into account the replacement characteristics given by the Access Control System (ACS).

**Parity flag:** This flag shall be used to indicate the parity of the current phase as follows:

- 0 even parity;
- 1 odd parity.

**Scrambling mode:** This two-bit parameter describes the scrambling mode as in table 26:

**Table 26**

b2 b1	Meaning
0 0	not allowed
0 1	unscrambled
1 0	free access (i.e. scrambled with a local Control Word)
1 1	controlled access (i.e. scrambled with a Control Word regularly transmitted and changed with ECMs)

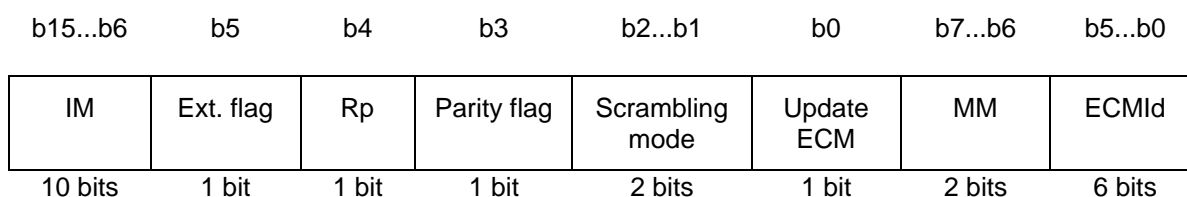
**Update ECM:** This flag shall indicate a change in the ECM transmission and it makes the descrambler read the next ECM:

- 0 no update;
- 1 update ECM. Next ECM shall be sent to the ACS.

#### 9.2.5.2 SMCCA\_Extended

SMCCA\_Extended is a 24-bit parameter consisting of SMCCA and the second Byte of SCA indicating where the ECMs of the service can be found.

The coding of SMCCA\_Ext is described in figure 35:



**Figure 35: Coding of the SMCCA - Extended field**

The first two Bytes are the same as for SMCCA. The remaining parameters are defined as follows:

#### MM = 00:

- In this case, the ECMs and the EMMs shall be sent in the SMCh.
- The bits b5 to b0 shall indicate the value of the ECM Identifier (SMC\_ECMId) which is used to identify the address of the ECM message. Value 000000 and 111111 are not allowed.

#### MM = 01:

- In this case, the ECMs shall be sent in the SMCh and the EMMs shall be sent in the LMCh Sub-channel identified by the packet address: 11 1111 1100 0000.

- The bits b5 to b0 shall indicate the value of the ECM Identifier (SMC\_ECMId) which is used to identify the address of the ECM message. Values 000000 and 111111 are not allowed.

**MM = 10:**

- In this case, the ECM and the EMM shall be sent in the LMCh.
- The bits b5 to b0 shall indicate the value of the ECM Identifier (LMC\_ECMId) which is used to identify the address the ECM message (6 least significant bits of the address of the packets transporting these ECMs). The value 000000 is not allowed. The 8 most significant bits are set to 1 to complete the address. The EMMs shall be sent in the LMCh Sub-channel identified by the packet address: 11 1111 1100 0000.

**MC = 11:**

- This case shall be reserved for future use.

### 9.3 ECM and EMM transmission

ECMs (Entitlement Checking Messages) give information about the conditions required to access a service. EMMs (Entitlement Management Messages) transport new entitlements and management data to customers. This subclause describes the coding of ECMs and EMMs and their transport mechanisms.

#### 9.3.1 General description

All access control messages shall begin with a parameter CAId identifying the Access Control System which can interpret and process the messages. The receiver only sends to the ACS the messages which the ACS can interpret and process.

##### 9.3.1.1 ECM coding

An ECM identifier (ECMId) shall be used to point to a specific ECM. The ECM is coded as in figure 36:

4 bits   4 bits                      1 bit   3 bits   4 bits                      n Bytes   8 bits   8 bits                      n Bytes

RFA	Address length	RFA	CA Id	message type	CustAd	CI	CLI	ECM data
-----	----------------	-----	-------	--------------	--------	----	-----	----------

**Figure 36: ECM coding field**

**RFA:** These bits are reserved for future additions.

**Address length indicator:** This 4 bits field codes the length in Bytes of the CAId + Message type + CustAd field. It is coded as an unsigned binary number in the range 1-15. The length 1 signals that there is no CustAd Field.

**CAId:** See subclause 9.2.1.

**Message type:** Type of message, which is defined as follows:

**Table 27**

0 0 0 0	ECM
0 0 0 1 and 0 0 1 x	reserved for specific ECM
other values	not allowed values (reserved for EMMs)

**CustAd:** This parameter is optional for ECMs. The length of CustAd shall be defined as follows:

- 40 bits. In this case, CustAd should also be called UA (Unique Address);
- 24 bits. In this case, CustAd should also be called SA (Shared Address);
- 16 bits. In this case, CustAd should also be called CCA (Collective Address).

**CI (Command Identifier):** This 8-bit field shall specify the format of the parameter field and the crypto-algorithm type (see subclause 9.3.1.3).

**CLI (Command Length Indicator):** This 8-bit field (expressed as an unsigned binary number) shall indicate the number of Bytes of the ECM data field in Bytes.

### 9.3.1.2 EMM coding

All EMMs shall be sent inside structures containing at least the parameters shown in figure 37:

4 bits   4 bits                      1 bit   3 bits   4 bits                      n Bytes   8 bits   8 bits                      n Bytes

RFA	Address length	RFA	CA Id	message type	CustAd	CI	CLI	EMM data
-----	----------------	-----	-------	--------------	--------	----	-----	----------

**Figure 37: EMM coding field**

**RFA:** These bits are reserved for future additions.

**Address length indicator:** This 4 bits field codes the length in Bytes of the CAId + Message type + CustAd field. It is coded as an unsigned binary number in the range 1-15. The length 1 signals that there is no CustAd Field.

**CAId:** See subclause 9.2.1.

**Message type:** Type of message, which is defined as in table 28:

**Table 28**

0 0 x x	not allowed values (reserved for ECMs);
0 1 0 0	EMM for a unique customer (EMM-U);
0 1 0 1	EMM for small groups of customers (EMM-S);
0 1 1 0	EMM for large groups of customers (EMM-C);
0 1 1 1	EMM for the entire audience (EMM-G);

The remaining codes are reserved for future definition.

**CustAd (Customer Address):** This parameter shall exist in all EMMs, except EMM-G. The length of CustAd shall be defined as follows:

- 40 bits for EMM-U. In this case, CustAd should also be called UA (Unique Address);
- 24 bits for EMM-S. In this case, CustAd should also be called SA (Shared Address);
- 16 bits for EMM-C. In this case, CustAd should also be called CCA (Collective Address).

**CI (Command Identifier):** This 8-bit field shall specify the format of the parameter field and the crypto-algorithm type (see subclause 9.3.1.3).

**CLI (Command Length Indicator):** This 8-bit field (expressed as an unsigned binary number) shall indicate the number of Bytes of the EMM data field in Bytes.

### 9.3.1.3 Command Identifier (CI) coding

The CI describes the format used for the parameter field and the type of cryptographic algorithm used for decryption. It shall be included in all EMMs and ECMs. Its content is described in figure 38.

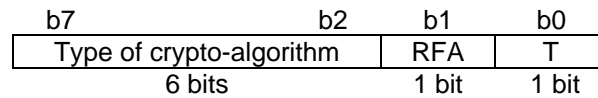


Figure 38: Coding of the Command Identifier field

**Type of Crypto-algorithm:** This 6-bit field shall be used to identify one of 64 types of crypto-algorithms.

**RFA:** This bit shall be reserved for future additions. The bit shall be set to zero until it is defined.

**T:** The toggle bit. It shall be maintained in the same state as long as the content of the message has not changed. It shall be used in EMM-G and in ECM to indicate a change in the information content of these messages. It has no meaning for the EMM-U, EMM-C and EMM-S. The toggle bit is attached to a given crypto-algorithm type; therefore, if ECMs or EMM-G corresponding to two different types of crypto-algorithm are sent, the corresponding toggle bits are kept separate.

### 9.3.2 Transport

ECMs and EMMs can be sent in the SMCh, or in the LMCh.

#### 9.3.2.1 LMCh

The ECM shall be coded as shown in figure 39:

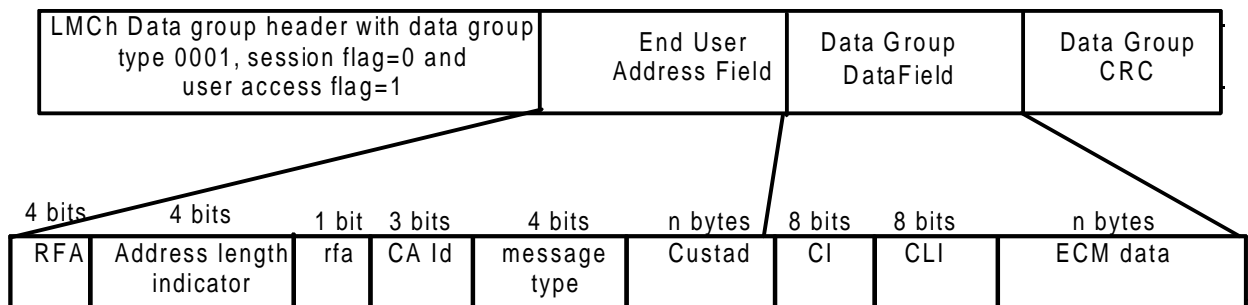


Figure 39: Data group structure containing an ECM

The parameters shall be defined as follows:

**CAId, message type, CI, CLI, ECM data:** See subclause 9.3.1.1.

The EMM shall be coded as shown in figure 40:

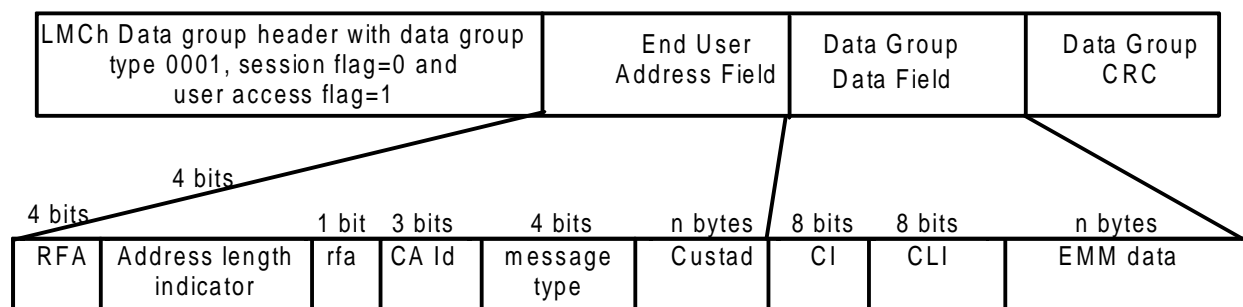


Figure 40: Data group structure containing an EMM

The parameters shall be defined as follows:

**CAId, message type, CI, CLI, EMM data:** See subclause 9.3.1.1.

At the network level, each LMCh data group containing one ECM or one EMM shall be carried in one or several messages having same address.

The EMMs of one given access controlled service shall be carried in messages having the same address (see table 28).

The ECMs of one given access controlled service shall be carried in packets with addresses described in table 29.

Table 29: Packet address for ECMs and EMMs in LMCh

Type of message	Packet address (14 bits)	
	MSB	LSB
	b13...b6	b5...b0
ECM	11111111	LMC_ECMId (6 bits)
EMM	11111111	000000

### 9.3.2.2 SMCh

The ECM and the EMM shall be coded in short messages or FIG 6 type 6 as described in figures 41 and 42.

For ECMs, address shall be 11 1111 1100 0000 + SMC\_ECMId.

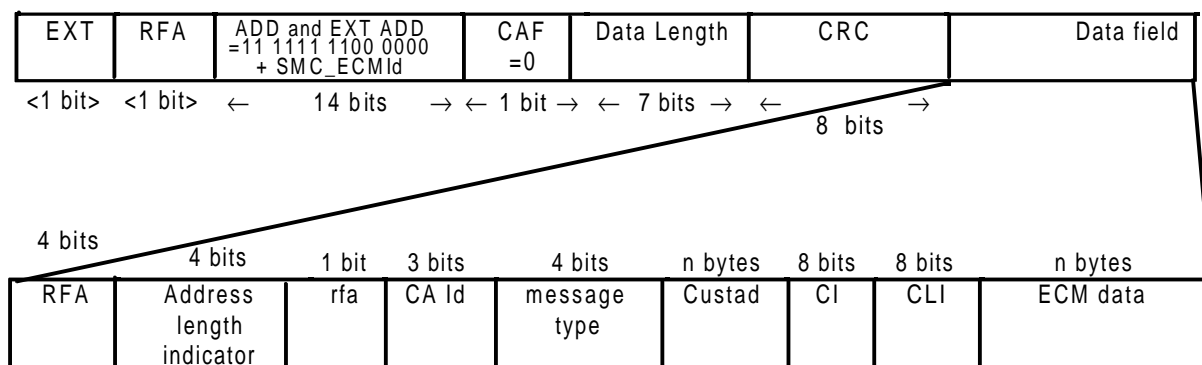


Figure 41: ECM coding in SMCh

The data field contains all or part of one ECM identified by SMC\_ECMId.

For EMMs, Address (ADD) is equal to 11 1111 1100 0000.

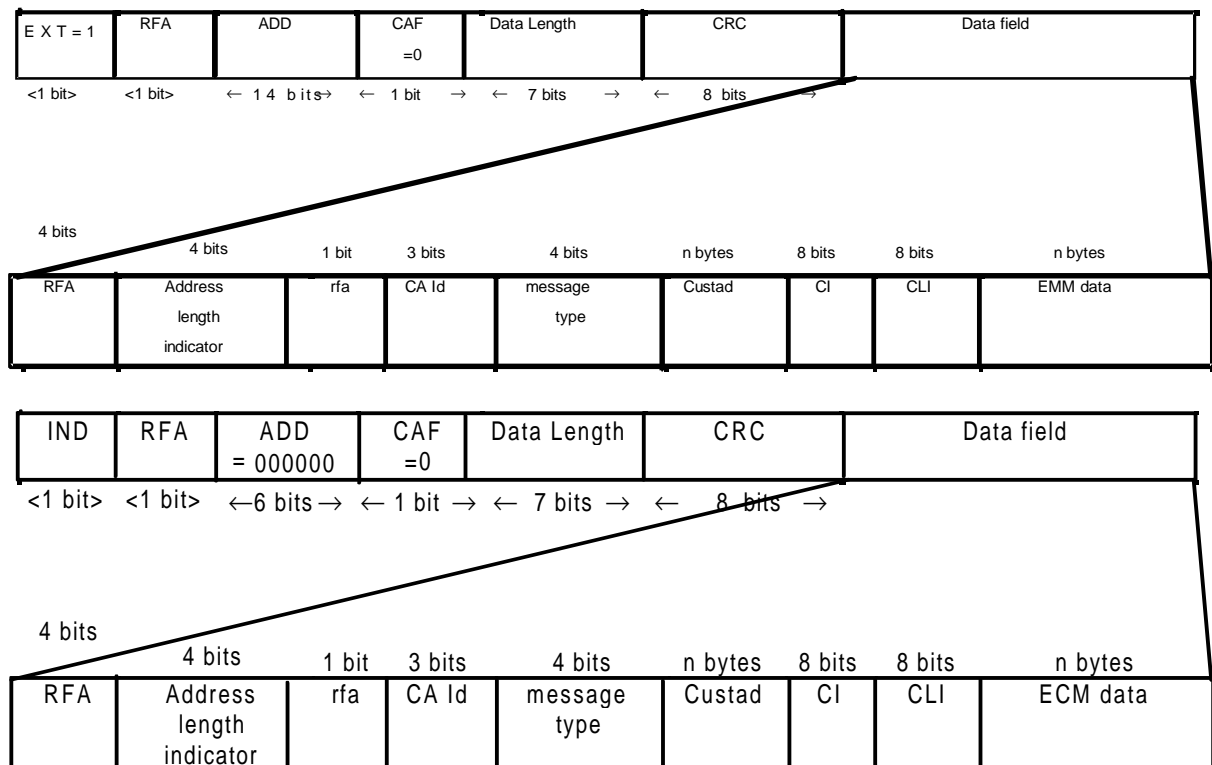


Figure 42: EMM coding in SMCh

The extension field shall qualify the CA Message field as follows:

- CAId, message type, CI, CLI, ECM data (see subclause 9.3.1.1);
- ADD = 11 1111 1100 0000: the data field contains all or part of one EMM;
- CAId, message type, CustAd, CI, CLI, EMM data (see subclause 9.3.1.2).

### 9.3.2.3 Together with service data

The ECMs and EMMs shall be coded in the same way as that described for the LMCh in subclause 9.3.2.1.

At the network level, each LMCh data group containing one ECM or one EMM, shall be carried in one or several command packets having the same address as the service data.

## 10 Error correction strategy

The main error correction processing will be made by Layer 2.

### 10.1 Layer 2 error detection and correction

The INFORMATION BLOCK CRC is calculated using the generator polynomial:  $g(x) = x^{14} + x^{11} + x^2 + 1$ .

The CRC is the remainder of the polynomial division of the transmitted bits (L3-header and data) by the generator polynomial. See example below:

DATA	CRC
40 00 80 40 EC 04 0A 4A F2 52 A2 C2 2A04 B2 82 9272 B2A272 AA	DC 10

NOTE: The CRC is 14 bits left justified so the last two bits do not care.

The BLOCK PARITY is calculated using the generator polynomial:

$$g(x)=x^{82}+x^{77}+x^{76}+x^{71}+x^{67}+x^{66}+x^{56}+x^{52}+x^{48}+x^{40}+x^{36}+x^{34}+x^{24}+x^{22}+x^{18}+x^{10}+x^4+1$$

The parity is the remainder of the polynomial division of the transmitted bits (DATA and CRC) by the generator polynomial. An example using data and CRC from above can be seen below:

DATA and CRC	PARITY
40 00 80 40 EC .....72 AA DC 10	2 42 02 A6 00 08 92 AD DF 59 7B

NOTE: The PARITY is 82 bits right justified where only the last two bits in the leftmost nibble are valid.

## 10.2 Error detection strategy at other layers

Some other mechanisms may be implemented in application layers. They are let under the responsibility of the application conceiver and not specified in this ETS.

However, in order to ensure a good synchronization on layer-3 and -4 headers which is a basic mechanism for an efficient demultiplexing, specific CRCs are introduced at these level (see clause 7).

There is also an optional CRC on L5 (data group) layer for the header and the data.

### 10.2.1 L3 short message header CRC

The short message L3 header is protected by a 6 bits CRC. The generator polynomial is given by the expression:  $x^6 + x^4 + x^3 + 1$ .

The CRC is the remaining from the polynomial division of the header bits by the generator polynomial.

Example of a L3 short message (SI/LCh = 1001) header CRC (in binary mode):

SI/LCh	DI	LF	SC	CRC
1001	0	0	1111	000101

### 10.2.2 L3 long message header CRC

The long message L3 header is protected by a 6 bits CRC. The generator polynomial is given by the expression:  $x^6 + x^4 + x^3 + 1$ .

The CRC is the remaining from the polynomial division of the header bits by the generator polynomial.

Example of a L3 long message (SI/LCh = 1010) header CRC (in binary mode):

SI/LCh	DI	LF	SC	CRC
0101	0	0	1111	110011

### 10.2.3 L4 short message header CRC

The short message L4 header is protected by a 8 bits CRC. The generator polynomial is given by the expression:  $x^8 + x^5 + x^4 + x^3 + 1$ .

The CRC is the remaining from the polynomial division of the header bits by the generator polynomial.



Example of a L4 short message header CRC (in binary mode):

EXT	RFA	ADD	CAF	Data Length	CRC
0	0	000001	0	0000011	11010111

#### 10.2.4 L4 long message header CRC

The long message L4 header is protected by a 6 bits CRC. The generator polynomial is given by the expression:  $x^6 + x^4 + x^3 + 1$ .

The CRC is the remainder of the polynomial division of the header bits by the generator polynomial.

Example of a L4 long message header CRC (in binary mode):

RI	CI	F/L	EXT	ADD	COM	CAF	Data Length	CRC
00	00	11	0	001000000	0	0	10000000	101101

#### 10.2.5 L5 (data group) CRC

The data group CRC is a 16-bit word based on division of the data group header and data field by the polynomial  $g(x) = x^{16} + x^{12} + x^5 + 1$ .

Before polynomial division the first 16 bits shall be inverted. The CRC which is remainder of the division shall be inverted prior to transmission.

Example of a L5 data group CRC (in hexadecimal mode):

header and data	CRC
B234	EC48

### 11 Bit-order of transmission

This clause will give an explanation of how Layer 2 blocks are transmitted over the SWIFT air interface. The handling of the BIC and the fields in the Layer 3-header might seem confusing, compared to the rest of the data Bytes (L3-data, CRC and Parity on Layer 2) which are transmitted lsb (least significant bit) first. The reason for handling L3-headers in this way is to keep compatibility with DARC in Japan. The calculation of CRC and parity is given in clause 10.

Normally in serial transmissions the lsb (least significant bit) is transmitted first even though many Byte oriented.

computer people seem to feel more comfortable with msb (most significant bit) first.

The receiver consists of some circuitry that reorganizes the transmitted serial bitstream into computer friendly Bytes. When serially received data is reorganized into Bytes the first received bit ends up as lsb in the first Byte and thus the transmitted Byte is received bit-reversed.

The BIC:s are four unique 16-bit data patterns that are used by Layer 2 for block and frame synchronization. They are only used as a serial bit pattern and are therefor transmitted with the leftmost bit first (see figure 43).

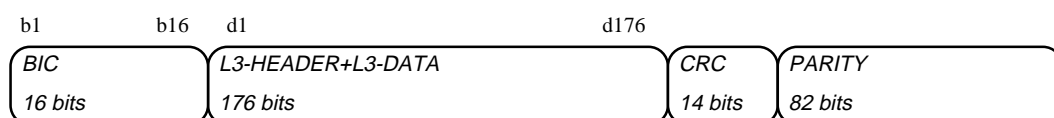


Figure 43: Layer 2-block

The crucial part of transmission order is the Layer 3-headers. They consist of 16 or 24 bits of data organized in different fields like SI/LCh (logical channel),DI, SF, SC (sequence counter) and CRC (see figure 44).

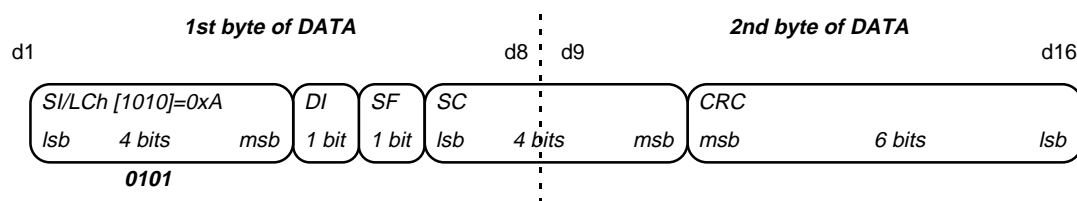


Figure 44: SWIFT/DARC Layer 3-header

The 16 or 24 bits in the L3-header and 14 bits CRC and 82 bits parity are transmitted with their leftmost bit first. The values in L3-header fields, used to select logical channel or as counters, are inserted bit-reversed i.e. these fields are transmitted lsb first on a field basis. See LMCh example in figure 46.

In the receiver this header ends up like the two Bytes in figure 45 below:

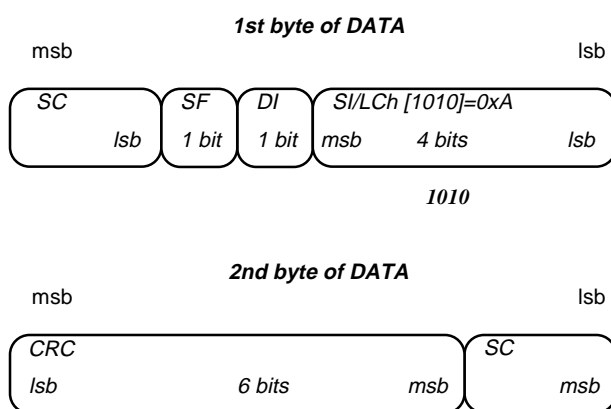


Figure 45

The Layer 3 data (Layer 4-headers and L4-data) and the 14 bits of CRC and the 82 bits of parity are segmented into Bytes that are transmitted with lsb first. See Example from LMCh in figure 46 below.

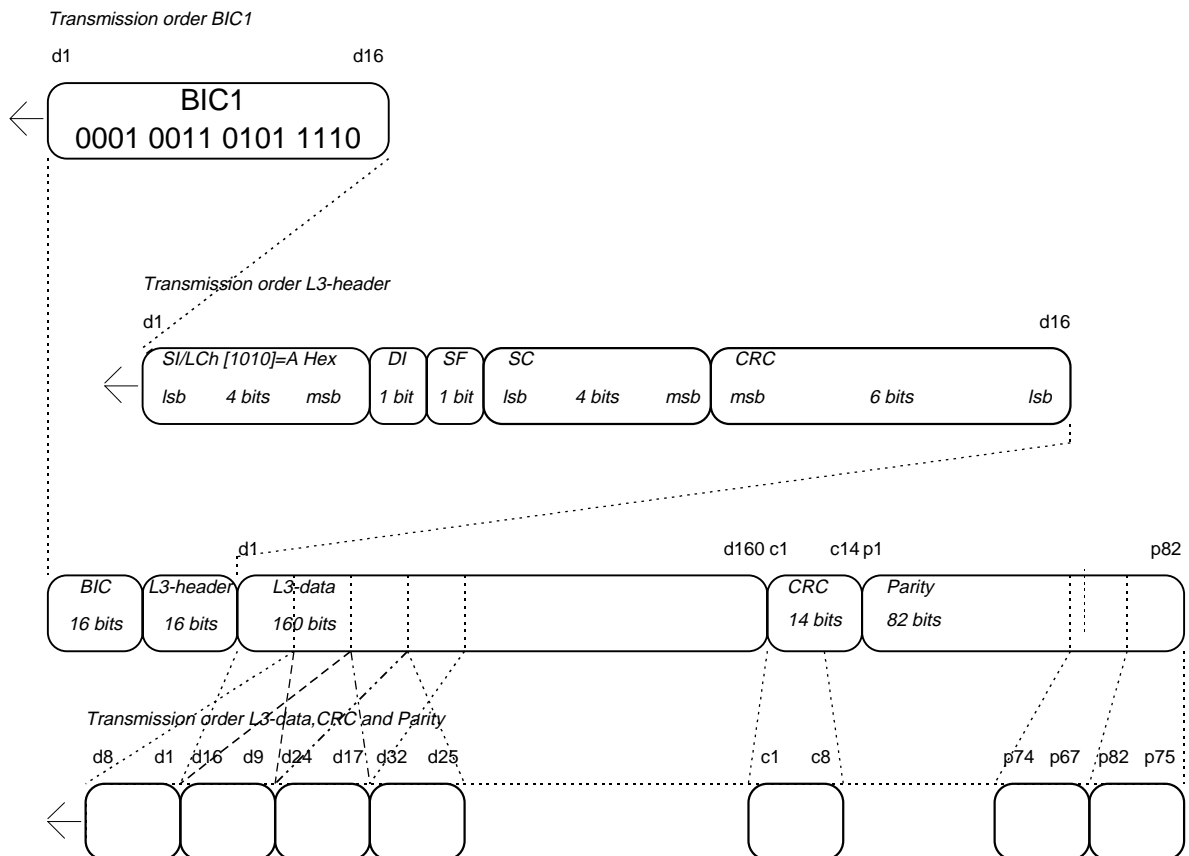


Figure 46: Transmission order

## 12 Service addressing mechanism

The SWIFT multiplex is a transport protocol where each service has a unique address. This service address may be based on:

- the Service ID (SID);
- the Service ID (SID) and country code (CID + ECC);
- the Service ID (SID), Network ID (NID) and country code (CID + ECC).

### 12.1 Global services

Global services, as program related information and community service etc. that shall be receivable in any country that operates the SWIFT system, the address shall only be based on the Service ID. Those SID have to be co-ordinated in the SWIFT group.

### 12.2 Country wide services

Country wide services, as a service that are distributed on several networks using the same application protocol, the address may be based on SID and CID. This means that the co-ordination of SID is only done in the specific country.

### 12.3 Network specific services

Network specific services, which is only transmitted in one network, the address may be based on SID, NID and CID. This means that the co-ordination of SID is only done for each network in each country.

## 12.4 Local services of single transmitters

Local services, that is transmitted on single transmitters, the address may be based on SID, NID = 0 and CID. This means that the co-ordination of SID is only done for each country. This is useful also if 16 networks is not enough.

## 12.5 Address allocation for global services

The SWIFT group have allocated the SID address field 1 - 7 (3 bits) as global services that only use the SID for the service address. This means that its possible to have 7 different services.

## 13 Quality of service

### 13.1 Useful bit-rate

Table 30 shows the overhead for different cases of data encoding.

Table 30

	SMCh						LMCh					
	best case			worst case			best case			worst case		
data size	117	115	114	18	16	15	256	254	253	17	15	14
L4-header size without CA	3			3			4			4		
L4-header size with CA case 1		5			5			6			6	
L4-header size with CA case 2			6			6			7			7
padding Bytes	0	0	0	19	19	19	0	0	0	19	19	19
L3-header size	12	12	12	4	4	4	26	26	26	4	4	4
Layer 4 overhead (%)	3	4	5	17	31	40	2	2	3	24	40	50
Layer 3 overhead (%)	10	10	11	127	144	153	10	10	10	135	153	164
Total overhead (Bytes)	15	17	18	26	28	29	30	32	33	27	29	30
Total overhead (%)	13	15	16	144	175	193	12	13	13	159	193	214
NOTE: The overhead is very important if the size of the data field is not optimized. The main overhead is produced by the Layer 3 coding.												

### 13.2 Expected capabilities of a Conditional Access system

The aim of this subclause is to present the expected capabilities of a Conditional Access system as regards services and from different points of view. Once expressed, these capabilities will allow better definition of the system's technical characteristics according to the constraints which they impose.

#### 13.2.1 From the user's point of view

##### 13.2.1.1 Access time of a newly connected user

This is the maximum time taken to acquire descrambling information and to access the service from the moment of the connection. This time is closely related to the repetition frequency of ECMs' broadcasting.

##### 13.2.1.2 Zapping time

This is the maximum time taken to access the new descrambled service from the moment when the user switched from one service to another. This time depends on the multiplex organization and capabilities. Some special mechanisms, if included in the receiver, allow to reduce it.

#### 13.2.2 From the service operator's point of view

##### 13.2.2.1 Bit rate needed to broadcast Conditional Access messages

As already described, ECMs are included in the multiplex with a repetition rate determined by the desired access time, and EMMs are also sent with a repetition rate depending on the number of customers and the average time a customer spends using a service.

### 13.2.2.1.1 Bit rate for the ECMs

The bit rate needed to transmit the ECMs depends on two features:

- the size of the ECMs, that is to say the length  $L$  (in bits) of an ECM;
- the repetition period of the ECMs, that is to say the maximum time  $T$  that a decoder has to wait for an ECM.

The bit rate ( $B_{\text{ecm}}$ ) needed to send the ECMs of one scrambled service is then equal to  $L/T$ .

EXAMPLE:  $L \geq 320$  bits and  $T = 2$  seconds. So the bit rate necessary to send the ECMs is at least equal to 160 bit/s.

NOTE: If scrambling is done inside the multiplexer, it is possible to use the same ECMs for different services. This simplification is no longer possible if scrambling is done at the source.

### 13.2.2.1.2 Bit rate for the EMMs

Contrary to the ECMs, the EMMs are not synchronized with the signal. They can be sent using another transmission channel.

The bit rate necessary for the EMMs depends on four criteria:

- the number of services:  $N_p$ ;
- the size of the EMMs, that is to say the length  $L$  (in bits) of an EMM;
- the repetition period of the EMMs, that is to say the maximum time  $T$  that a user has to wait to receive an EMM intended for him;
- the number  $N_g$  of EMMs that have to be sent (which is closely related to the number of customers or groups of customers).

The bit rate ( $B_{\text{emm}}$ ) necessary to send the EMMs of all the programmes is then equal to  $N_p \times (N_g \times L/T)$ .

EXAMPLE: When using Eurocrypt, the average size of an EMM is around 240 bits.

1. If we want to address 100 000 customers individually in one minute, then the necessary bit rate is equal to  $10^5 \times 240 / 60 = 400$  kbit/s.
2. If we want to address 10 000 customers individually in 15 minutes, then the necessary bit rate is equal to  $10^4 \times 240 / 900 = 2,7$  kbit/s.

NOTE 1: Such bit rates prove the necessity for regrouping customers. The EUROCRYPT system, for instance, allows one EMM to be sent for 256 customers. The bit rates of the EMMs is then reduced to 1,5 kbit/s in the first example and to 10,4 bit/s in the second example.

NOTE 2: The bit rate for the EMMs can be reduced by different means:

- by sending the EMMs to the customers in another way (telephone, mail, ... ?).
- by accepting large repetition period (depends on the services) and/or by leaving the receivers watching continually for the EMMs (even when the user is not using his decoder).
- by using "unused" service resources (during the night for instance) to send the EMMs.

NOTE 3: All services may use the same channel to send their EMMs. This allows a customer to receive an EMM of service 1, while he is using service 2.

### 13.2.2.2 Maximum time for changing the access mode

This is the maximum time required to change from one mode to another, and particularly from plain form to scrambled form and vice-versa. In fact, such changes can only occur at certain moments. The minimum interval between these moments can influence the service quality and the possibility of synchronization with the signal sources.

#### **13.2.2.3 Transcontrol**

This is the capability of modifying the access conditions of a service at different places on the broadcasting network without changing its scrambling.

#### **13.2.2.4 Length of a scrambling cycle**

This is the lifetime of a control word. Expanding this lifetime makes the receivers' task easier but damages security. A suitable compromise shall be found.

#### **13.2.2.5 Repetition frequency**

To have a good access time and to minimize effect of transmission errors, it is necessary to send several unchanged ECM in a cycle.

#### **13.2.2.6 Hierarchical coding and scrambling**

This is the possibility of having several levels of service capabilities and of associating different access conditions to these levels.

### **14 Classes of services**

EXAMPLES:

- Mailing.
- Paging.
- News Broadcasting.
- Cyclic Information Broadcasting.
- Real-time Transfer.
- Transfer with high bit rate guaranty and clock recovery.
- General File Transfer.

Table 31

Criteria	Mailing	Paging	News Broadcasting	Cyclic Information Broadcasting	Real Time Transfer	Transfer with high bit-rate guaranty	General File Transfer
<b>Examples</b>	<b>X.400</b>	<b>Operator</b>	<b>Times, Le Monde</b>	<b>TMC, Weather</b>	<b>dGPS</b>	<b>Sound, Still pictures</b>	<b>Tele software</b>
Receiving Delay	< 40 s	< 40 s	< 30 min	< 10 s	< 1 s	< 30 s	< 30 min
Receiving Conditions	mobile	mobile	portable	mobile	mobile	mobile	portable
Coverage area of a message	all large small	all large	all large small	small large	small	all large small	all large small
User addressing	yes	yes	no	no	no	yes or no	yes or no
Message Length	< 100 kB		< 10 MB	1-15 blocks	1-5 blocks	< 1 MB	< 10 MB
Average bit-rate	large	low		low	1200 bit/s per set	high	
Message format	X.400		RATS	ALERT+	RTCM 104	JPEG, MPEG, TCD	Binary, ASCII
Improved transmitting strategy for service header	yes	yes	yes	no	yes	yes	yes
Improved transmitting strategy for sensible data	yes	yes	yes	no	yes	yes	yes
Improved transmitting strategy for ordinary data	no	no	no	no	yes	no	no
Channel Access	on demand	on demand	on demand	continuously	continuously	on demand	on demand
Message Priority	high/low	high	low	low	high	high	low
RDS interworking	no	yes	no	yes	yes	no	no
Confidentiality Required	yes	yes	no	no	no	yes/no	yes/no
Users Charging Mode	subscription, per event	subscription, per event	subscription per event, per volume	subscription per event, per time	subscription per event, per time	subscription, per event, per time	subscription, per event, per volume
Source Charging Mode	per event	per event	subscription per event, per volume	subscription, per event, per volume	subscription, per event, per time	per event, per time	per event, per volume
Service association					yes		
Minimum bit rate guaranty during a limited period of time	no	no	no	no	no	yes	no
Desirable Single Frame Process	no	yes	no	no	yes	no	no

## History

Document history			
May 1996	Public Enquiry	PE 106:	1996-05-20 to 1996-09-13
November 1996	Vote	V 115:	1996-11-25 to 1997-02-21
May 1997	Second Vote	V 9731:	1997-05-20 to 1997-08-01
August 1997	First Edition		