EUROPEAN TELECOMMUNICATION STANDARD

FINAL DRAFT
pr **ETS 300 751**

November 1996

Source: EBU/CENELEC/ETSI JTC

Reference: DE/JTC-SWIFT

ICS: 33.020

Key words: FM, radio, data, broadcasting, multimedia

European Broadcasting Union 

Union Européenne de Radio-Télévision

Radio broadcast 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

Contents

Blank page

Foreword

This final draft European Telecommunication Standard (ETS) has been produced by the Joint Technical Committee (JTC) of the European Broadcasting Union (EBU), Comité Européen de Normalization ELECtrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI), and is now submitted for the Voting phase of the ETSI standards approval procedure.

NOTE: The EBU/ETSI JTC was established in 1990 to co-ordinate the drafting of ETSs 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 SACONNEX (Geneva)
Switzerland

Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Blank page

1 Scope

This European Telecommuncation 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] Contributions on ITU-R Recommendation BS 1194 [7] from Japan (10B/25-E) and from Sweden (10B/35-E) about protection ratios.

3 Definitions and abbreviations

3.1 Definitions

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 packet channel PaCh, for big files with low priority.

Each logical channel carries a lot of **subchannels** distinguishable by an address and/or a type. Every subchannel may be allocated to one **service component**. Each service may involve one or several **components**. When a service has only one component, it is referred to as the service itself. Components of a service are data streams with common presentation characteristics from the user point of view.

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

3.2 Abbreviations

For the purpose 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 (Japanese RDS standard)
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 (DAB) [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
SCCA	Service Component 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 may operate either on a service basis or on a component basis;
- to multiplex the components of one service and/or components of several services;
- 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 component of the service is described when needed (type of data, coding algorithm, type of segmentation and reassembling technique, type of error correction/detection, etc.). No information relative to the physical mux is carried here: each component is identified thanks to a logical number. 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 component 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 component 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,...). 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;

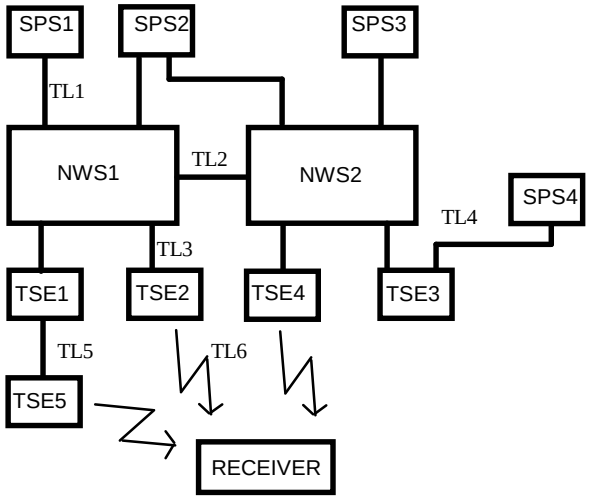
9) **frame generation/delineation:** for a frame based transmission, it is the capability to recover the boundaries;

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 rooting and relaying. Routing 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 et 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+l) entities and those above by the functionality of Layers (l) to (N) below it.

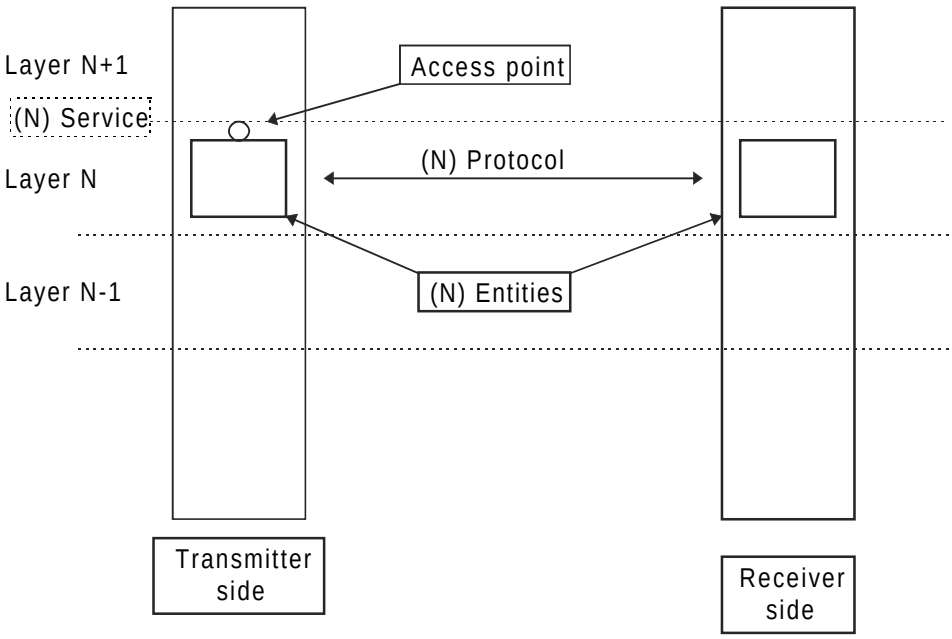


Figure 2

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 INDication primitive type sent by a lower layer;
4) the **CON**firm 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 ± 7,6 Hz (0,01 %) and the phase difference shall not exceed ± 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.

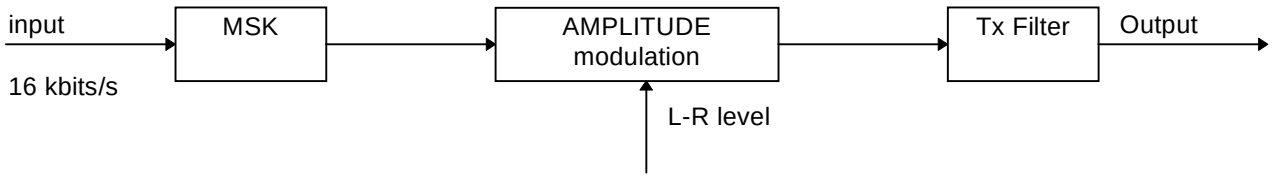


Figure 3

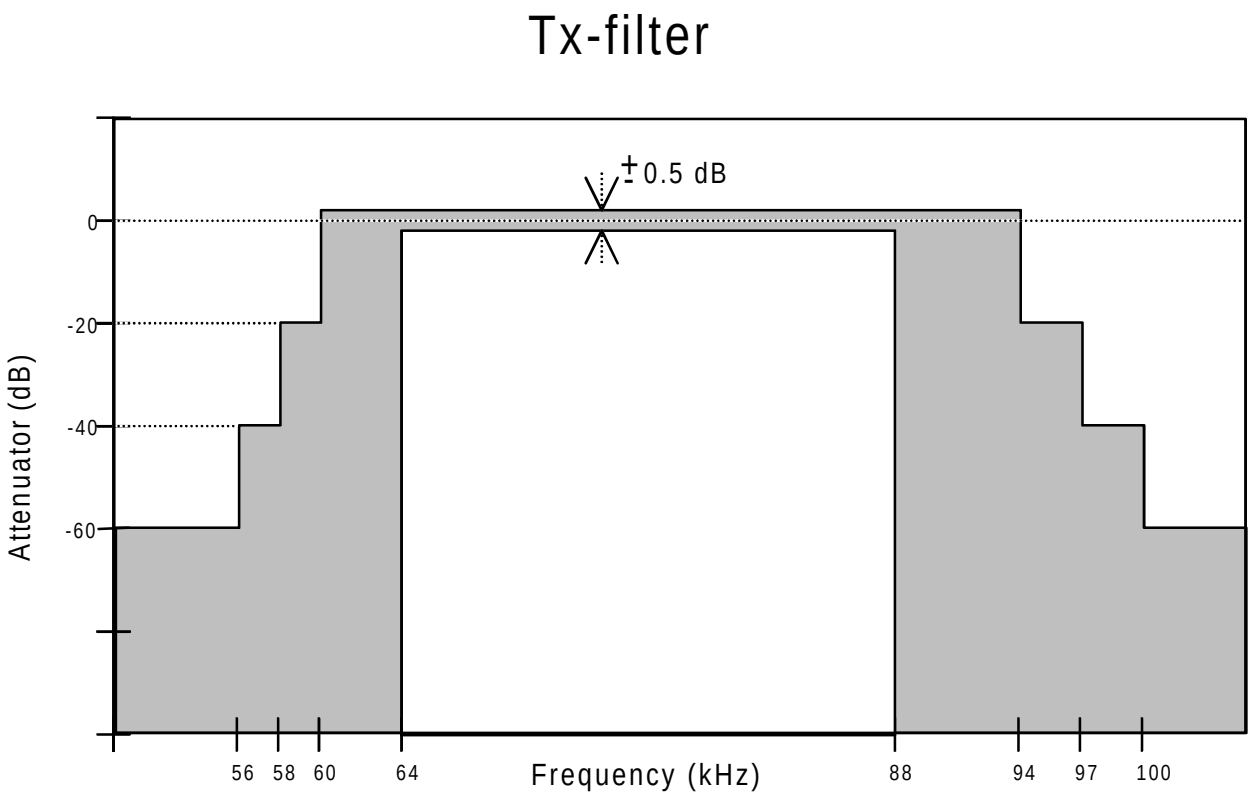


Figure 4

Table 1

Upper bound:	
- 60 dB	(Freq.< 56 kHz, 100 kHz ≤ Freq.)
- 40 dB	(56 kHz ≤ Freq.< 58 kHz, 97 kHz ≤ Freq.< 100 kHz)
- 20 dB	(58 kHz ≤ Freq.< 60 kHz, 94 kHz ≤ Freq.< 97 kHz)
0,5 dB	(60 kHz ≤ Freq.< 94 kHz)
Lower bound:	
- 0,5 dB	(64 kHz ≤ Freq.< 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 4). 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.

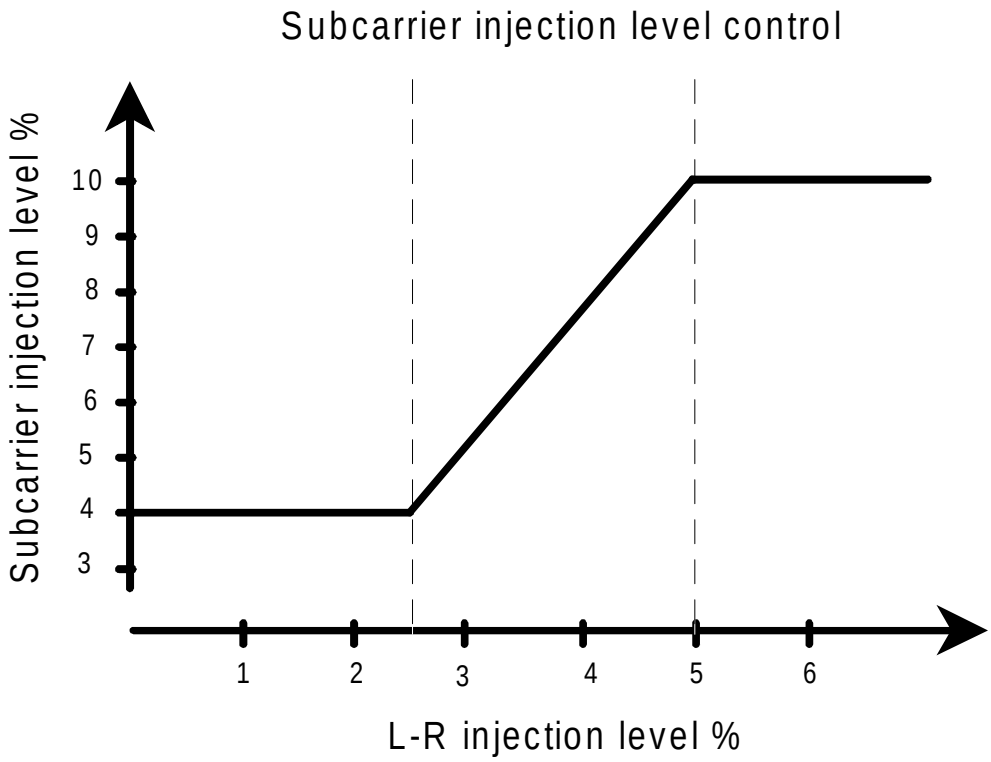


Figure 5

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% (+/-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].

The effect of the addition of the SWIFT subcarrier system to the stereo multiplex is given in [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:

L2_data.RES (L3-Block) the Layer 3 sends a L3-block of data (22 bytes) to the Layer 2.

L2_ready.IND no parameters. The Layer 2 is ready to receive a L2_data.RES containing a L3-Block and the Layer 3 should send it.

L2_reset.REQ 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:

L2_data.IND (L3-Block) 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.

L2_no_synch.IND no parameters.

L2_reset.REQ 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 A

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.

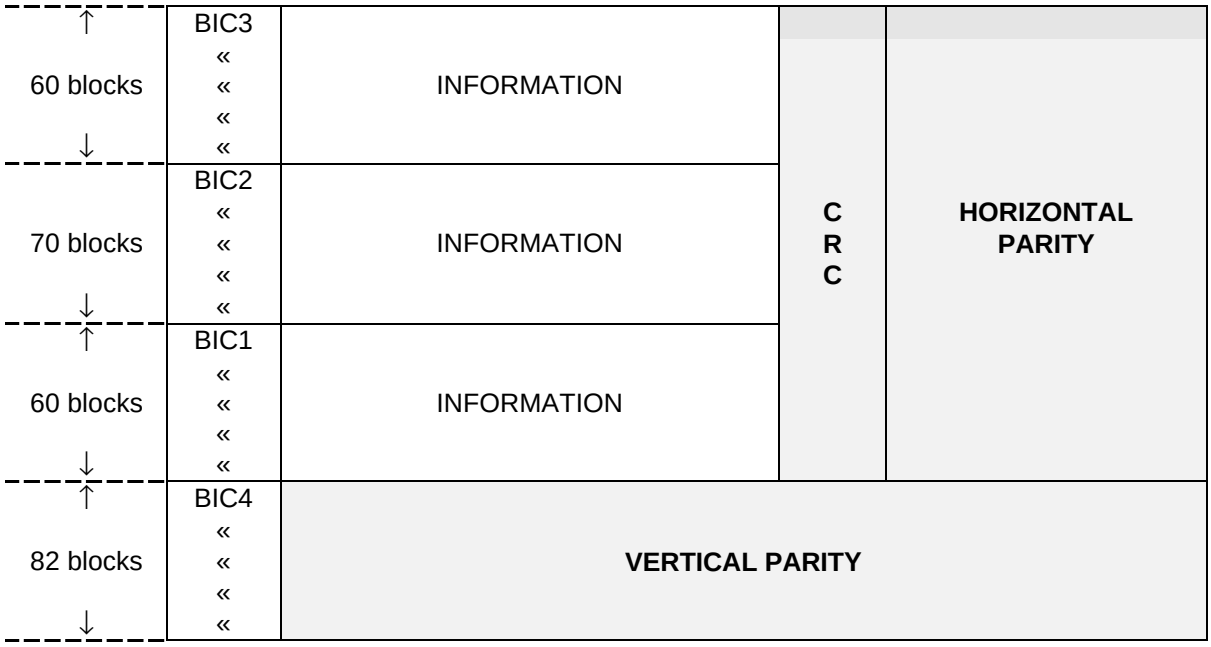


Figure 6

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 at the end of the frame. 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 6. In this case, total of blocks from a frame start to the next 272 + 12 blocks. The Bloc Identification Code (BIC) for inserted blocks is BIC2.

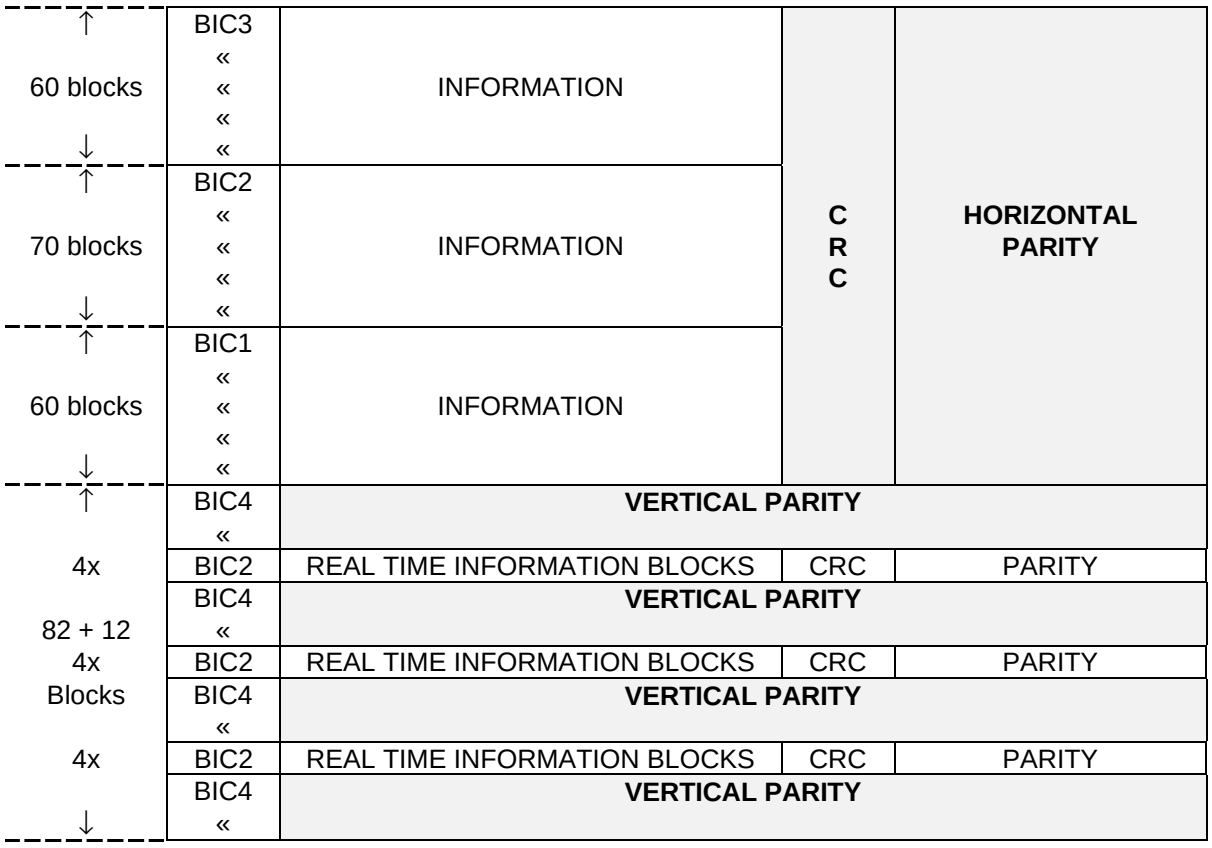


Figure 7

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 can be sent in the service channel. It is important that the change of structure appears very seldom.

7.3.2.2.1.2 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**
	«	«	«	«
	BIC1	INFORMATION 13	CRC	**PARITY**
	BIC3	INFORMATION 14	CRC	**PARITY**
	BIC3	INFORMATION 15	CRC	**PARITY**
	BIC4	**PARITY 1**		**PARITY**
	BIC3	INFORMATION 16	CRC	**PARITY**
	BIC3	INFORMATION 17	CRC	**PARITY**
123 blocks	**BIC4**	**PARITY 2**		**PARITY**
	BIC3	INFORMATION 18	CRC	**PARITY**
	«	«	«	«
	BIC4	**PARITY 40**		**PARITY**
	BIC3	INFORMATION 95	CRC	**PARITY**
	BIC3	INFORMATION 96	CRC	**PARITY**
	BIC4	**PARITY 41**	**7/**	**PARITY**
	BIC2	INFORMATION 97	CRC	**PARITY**
13 blocks	«	«	«	«
	BIC2	INFORMATION 109	CRC	**PARITY**
	BIC3	INFORMATION 110	CRC	**PARITY**
	BIC3	INFORMATION 111	CRC	**PARITY**
	BIC4	**PARITY 42**		**PARITY**
	BIC3	INFORMATION 112	CRC	**PARITY**
	BIC3	INFORMATION 113	CRC	**PARITY**
123 blocks	**BIC4**	**PARITY 43**		**PARITY**
	BIC3	INFORMATION 114	CRC	**PARITY**
	«	«	«	«
	BIC4	**PARITY 81**		**PARITY**
	BIC3	INFORMATION 189	CRC	**PARITY**
	BIC3	INFORMATION 190	CRC	**PARITY**
	BIC4	**PARITY 82**		**PARITY**

Figure 8

7.3.2.2.1.3 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.

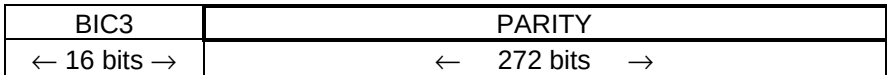


Figure 11: Parity Block with leading BIC

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)

BIC1	0001	0011	0101	1110
BIC2	0111	0100	1010	0110
BIC3	1010	0111	1001	0001
BIC4	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:

L3_LgMsg.RES (Id, LgMsg) the Layer 4 sends a long message (max. length: 8 bytes for the header, 252 bytes for the data) to the Layer 3 associated to the identities of the service and the component it belongs;

L3_ShMsg.RES (Id, ShMsg) the Layer 4 sends a short message (max. length: 6 bytes for the header, 114 bytes for the data) associated to the identities of the service and the component it belongs;

L3_Table.RES (TNI, Table) 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 TNI parameter which includes the country code, the network identification number and the transmitter identification number;

L3_ready.IND 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;

L3_reset.REQ 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:

L3_LgMsg.IND (Id, LgMsg, BQA) the Layer 3 sends a long message to the Layer 4 with a block quality array and the identity of the service/component. 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);

L3_ShMsg.IND (Id, ShMsg, BQA) as L3_LgMsg.IND but for short messages;

L3_error.IND cause of the error;

L3_reset.REQ no parameters.

8 Multiplex organization (Layer 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 packet mode at Layer 4 can be built over the Layer 3 block specification of the DARC system. A DATA GROUP structure may also be used over the packet mode for upper layers protocol units but the packet mode can be used without the Data Group Structure. However, in packet mode, the Conditional Access system is only defined at the data group level.

8.2 Definition of logical channel

Logical channels can be implemented in the Layer 3. A mapping of the Layer 3 sub-frames shall be sent from the central management entity (network sender) to the management entity of Layer 3 in the TSEs. A link table shall also be sent, defining which applications to use which logical channels. Layer 3 shall be able to run several parallel processes (one per logical channel) feeding in each logical channel with its pre-defined data frame.

The link of the distribution network between the network server and the TSE shall have an higher rate than the useful rate of the radio channel to guaranty:

- no transmission delay into the distribution network for real time applications (problem of real time data waiting in the network server the transmission of data from other multiplexed applications);
- the parallel feeding of the logical channels in the TSE.

First of all the sub-Layer 3 will be defined as Layer 3. SI and DI will be untouched to ensure compatibility with the protocol defined by NHK. The SI defines SI/LCh where LCh corresponds with Logic Channels. With LCh four different logic channels can be defined.

These are the proposed logic channels:

- service Channel "SeCh";
- short Message Channel "SMCh";
- long Message Channel "LMCh";
- reserved for future use.

A dynamic allocation of capacity, for these channels, shall be done depending on what the services within the logic channels require but a minimum capacity shall always be left for the service channel (SeCh). The total capacity is never more than the DARC's capacity. The SWIFT system requires a minimum service channel capacity of X block/second to get adequate function for the receivers.

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

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 can not synchronize with the accurate physical channel. The structure of a service message is shown in figure 12.

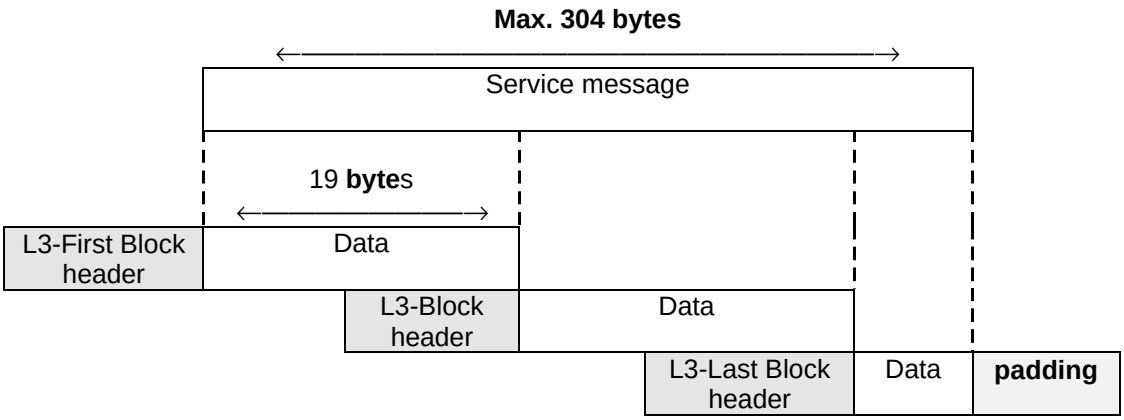


Figure 12: Partition of service messages into L3-blocks

Each Service Blocks (SeB) consist of a header and 19 bytes 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 301 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 improve the robustness of the service channel. When the receiver do not receive a complete service message the receiver save the correct blocks in order to wait for the new correct blocks that are missing to build the complete service message. For this mechanism a block number is defined for each L3 header.

The receive may use the Data Update (DUP) for knowledge if the service message of a specific service message type is updated since last reception. Country ID (CID) and Network ID (NID) are used for the receiver to synchronies to the correct channel.

The service block (L3) is defined as follows:

L3-Header

←——→

SI/LCh	LF	DUP	RFA	NID	TYPE	CID	BLN	DATA
←4 bits→	←1 bit→	←2 bits→	←1 bit→	←4 bits→	←4 bits→	← 4 bits →	←4 bits→	←19 BYTEs→

Figure 13: Format of Service Blocks (SeB)

Table 3: Format of L3-Header for a service block

b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
SI/LCh				RFA	LF	DUP		byte 1
CID				TYPE				byte 2
NID				BLN				byte 3

SI/LCh = Logical Channel field, set to 1000 (binary) to define the service channel. This field ensure a compatibility with the NHK protocol.

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

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.

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.

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

NID = Network Identification. The Network Identification distinguish different network in each country.

DUP = Data Update, indicates if the service message are updated or not. This 2-bit modulo-4 counter shall be incremented by one for each time the service message type are updated. A service message is normally not updated very frequently.

DATA = 19 bytes of service message data.

Table 4: 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 Table (TDP)
Others	Reserved for Future Addition (RFA)

8.3.3 Service message format

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

The general information (called ETS) is defined as follows:

Table 5: General information

b7	b6	b5	b4	b3	b2	b1	b0	
Extended Country Code (ECC)								byte 1
TSE Identification (TSEID)							Service..	byte 2
… Message Length (SML)								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.

SML = Service Message Length. SML describes the total message length. The maximum length is 16×19 bytes or 304 bytes.

The maximum length of the type specific information for each service type is $16 + (15 \times 19)$ bytes or 301 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 of its associated components in the multiplex. The Channel Organization Table shall have highest priority and shall be sent frequently.

Table 6: COT table

b7	b6	b5	b4	b3	b2	b1	b0	
Extended Country Code (ECC)								byte 1
TSE Identification (TSEID)							Service..	byte 2
... Message Length (SML)								byte 3
Service Identity 1...								byte 4
...(SID)						CA flag	SA	byte 5
SCCA (if CA flag=1)								byte 6
Service Identity 2...								byte 7
...(SID)						CA flag	SA	byte 8
SCCA (if CA flag=1)								byte 7
.....								» »
....								» »
Service Identity n								» »
...(SID)						CA flag	SA	» »
SCCA (if CA flag=1)								Up to
End marker/Padding								byte 301

Service Identity: On 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 component if set to "1". If CA flag equals "0", the SCCA 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.

SCCA: Service Component Conditional Access.

End marker/Padding: If the service table will not be filled, these bytes should fill the rest of the table. This byte is always equal to "0".

8.3.3.2 Alternative Frequency Table (AFT)

Alternative frequency lists are concatenated, up to 281 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 7: AFT table

RFA	RFA	AF_NUMBER (0-62 decimal)						byte 1
TUNING_FREQUENCY								byte 2
AF1								byte 3
AF2								...
...								...
AFi								byte 2 + i
RFA	RFA	AF_NUMBER (63 in decimal)						byte 3 + i
TUNING_FREQUENCY								byte 4 + i
		AF1						byte 5 + i
					AF2			...
			AF3			AF4		...
...	...	...	...	...	...	...	...	...
		AFj		RFA	RFA	RFA	RFA	byte 30 + i
RFA	RFA	AF_NUMBER						**and so on**
TUNING_FREQUENCY								**up to**
...								**byte 301**

RFA: Reserved for Future Addition.

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 nb 1). A value of 63 (decimal) means that the AFs are coded on a bitmap field of 26 bytes (format nb 2).

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

The coding is summarized in table 8.

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

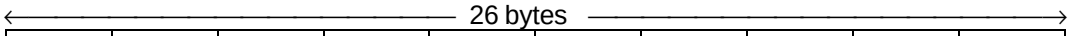
Number (decimal)	Carrier frequency (MHz)
0	RFA
1	87,6
2	87,7
...	...
...	...
204	107,9
205	RFA
...	...
255	RFA

AF: Alternative Frequency, possible frequency on which the receiver can switch on, if the quality of the tuning frequency decreases to much.

If the number of AFs for one tuning frequency is lower than 63 (AF_NUMBER<=62), the AFs are coded using the tuning frequency coding (format nb 1), or the bitmap coding (format nb 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 the MSB (bit 1) and ending with frequency 107,9 MHz on the 204th bit. Bits 205, 206, 207 and LSB are reserved.

Table 10: Bitmap AF coding



MSB	bit 2	bit 3	...	...	bit 204	bit 205	bit 206	bit 207	LSB
87,6	87,7	87,8	...	...	107,9	RFA	RFA	RFA	RFA

The bit value is:

0: not an AF frequency
1: AF frequency

8.3.3.3 Service Alternative Frequency Table (SAFT)

The SAFT contains, for each service, the Alternative Frequencies where it can be found. The SAFT is used in relation with the Alternative Frequency Table (AFT). By default, the SAFT and the AFT tables are equal. If not, the SAFT gives the difference between the AFT and SAFT tables.

Service Alternative Frequency (SAF) lists are concatenated up to 301 bytes.

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

- service identity;
- number of partial SAF lists for the service;

where the partial SAF lists have the general format:

- subtraction or addition operator;
- number of frequencies to subtract or add;
- sequence number of the related AF list;
- list of frequencies to subtract or add to the related AF list.

In the protocol, the partial SAF lists are grouped in pairs.

Table 11: SAFT table

b7	b6	b5	b4	b3	b2	b1	b0	
Extended Country Code (ECC)								byte 1
Transmitter Identification (TID)							Service..	byte 2
... Message Length (SML)								byte 3
Service..								byte 4
..Identity 1		Reserved						byte 5
Number of frequencies to add		Number of frequencies to subtract						byte 6
Freq 1 to add								byte 7
» » »								» » »
Freq n to add								» » »
Freq 1 to subtract								» » »
» » »								» » »
Freq n to subtract								» » »
...								» » »
...								» » »
Service								» » »
..Identity n		Reserved						» » »
Number of frequencies to add		Number of frequencies to subtract						» » »
Freq 1 to add								» » »
» » »								» » »
Freq n to add								» » »
Freq 1 to subtract								» » »
» » »								» » »
Freq n to subtract								» » »

8.3.3.4 Time/Date Table (TDT)

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

8.3.3.4.1 Modified Julian Date (MJD)

Table 12: MJD format

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

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

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

Table 14: TDT table

b7	b6	b5	b4	b3	b2	b1	b0	
Extended Country Code (ECC)								byte 1
Transmitter Identification (TID)							Service..	byte 2
... Message Length (SML)								byte 3
DATE/TIME Field								byte 4 byte 5 byte 6
RFA								byte 7
RFA								» » »
RFA								» » »
RFA								» » »
RFA								» » »
RFA								» » »

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

The Short Message Channel (SMCh) is compatible with the Fast Information Channel (FIC) of the DAB specification ETS 300 401 [4] and SMCh provides a protocol for messages up to 117 bytes data field.

It is composed with consecutive Short Message Blocks (SMB) that corresponds to 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).

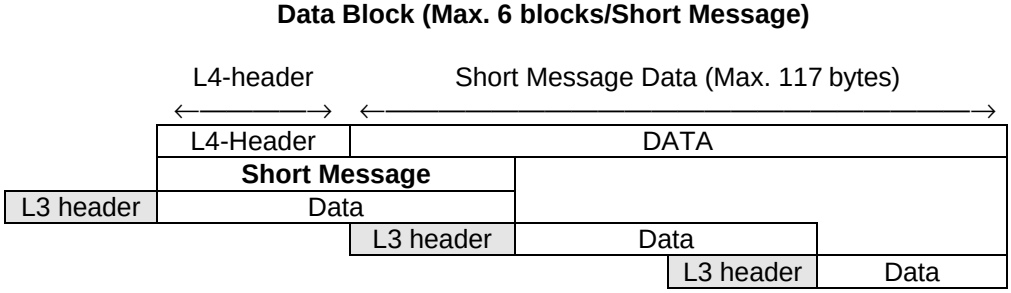


Figure 14: Short Message Channel Data Unit

8.4.1 L4 short message format

EXT	RFA	ADD	EXT ADD	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 56bits) in the Short Message Channel

ETX: 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 1 to 3).

EXT ADD: Extended Address field. Present if the EXT flag is set to 1 (see notes 1 to 3).

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 can be extended. See subclause 9.2.5.

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

NOTE 2: The ADD field on 6 bits permits to code service identifiers from 0 to 63. In this case, the EXT ADD field is not required (EXT flag set to 0). The 6 bits of the ADD field correspond to the 6 LSBs of the service identifier. To rebuilt the service identifier on 14 bits, 0 are set in place of the 8 MSBs of the service identifier.

NOTE 3: Service identifiers upper 63 are coded on both ADD and EXT ADD fields (EXT flag set to 1). ADD and EXT ADD are concatenated to form a 14 bits field supporting directly the service identifier (LSB right justified).

8.4.2 L3 short message channel block format

SI/LCh=1001	DI	LF	SC	CRC on L3-Header
← 4 bits →	<1 bit>	<1 bit>	← 4 bits→	← 6 bits →

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 9.

DI: Decode Indicator.

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).

Up to 6 SMB can be used to carry one short message.

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.

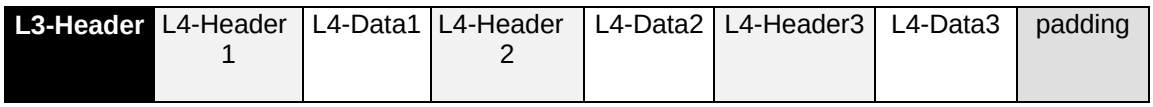


Figure 17: An example for L3 - Block within SMCh

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

The padding byte shall be zero.

8.5 Long Message Channel "LMCh" (SI/LCh = 0xA)

In the Long Message Channel, data are sent in variable length packet, called long message, with a header and a data field. These packets are transmitted after their partition into consecutive fixed length L3-Blocks of type 0xA (2 bytes L3-Header, 20 bytes data field).

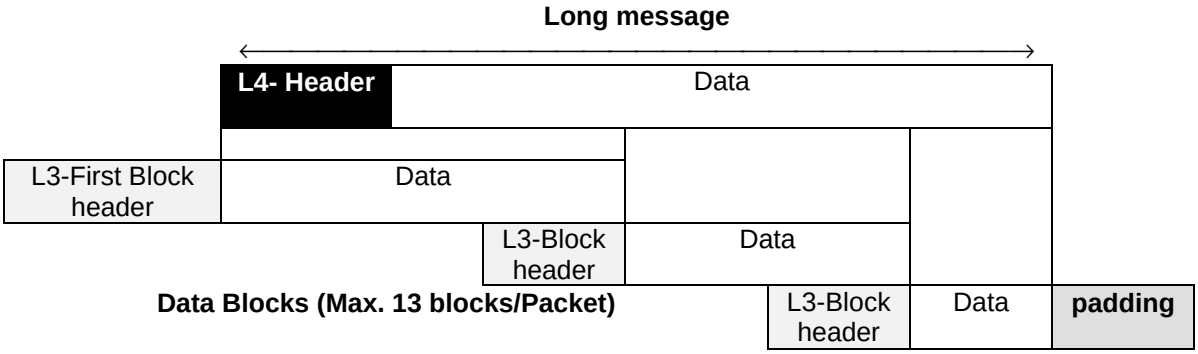


Figure 18: Partition of long messages into L3-blocks

8.5.1 L4 Long message format

The header of a long message is coded as follows:

RFA	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)

CI: Continuity Index, this 2-bit modulo-4 counter shall be incremented by one for each successive message in a series having the same address. It provides the link between successive messages, carrying the same service component, 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). Table describes the significance of these flags.

Table 15: 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

ETX: Extended address flag, signals, if set to 1, that the extended address field (EXT ADD) is present. 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 1 to 3).

EXT ADD: Extended Address field. Present if the EXT flag is set to 1 (see notes 1 to 3).

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.

LMMCA: Conditional Access field which can be extended (see subclause 9.2.4). It is possible to have this field only in the first messages of a data stream.

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

NOTE 2: The ADD field on 6 bits permits to code service identifiers from 0 to 63. In this case, the EXT ADD field is not required (EXT flag set to 0). The 6 bits of the ADD field correspond to the 6 LSBs of the service identifier. To rebuilt the service identifier on 14 bits, 0 are set in place of the 8 MSBs of the service identifier.

NOTE 3: Service identifiers upper 63 are coded on both ADD and EXT ADD fields (EXT flag set to 1). ADD and EXT ADD are concatenated to form a 14 bits field supporting directly the service identifier (LSB right justified).

8.5.2 L3 long message channel block format.

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

SI/LCh=1010	DI	LF	SC	CRC on SI, DI, FS, SC, NB
←4 bits→	←1 bit→	←1 bit→	←4 bits→	←6 bits→

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

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).

The padding bytes shall be set to zero.

The Long Message Channel can be used to transport the following services:

- broadcasting (Digital News Paper, Hot News Sheets);
- mailing (X.400);
- transfer with high bit-rate guaranty (still image, sound);
- broadcast general file transfer (Tele-software, Broadcast Fax, New Price List, List of blocked Account, Gambling Information);
- Addressed text and Graphic messages (Road Information Sign, Calculated Bus, Arrival, Commercial Advertisement Board).

8.6 Data Group structure over long messages

Service information may be structured into Data Groups for transport in one or more packets. 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. The generation shall be based on the polynomial $G(x)= x^{16} + x^{12} + x^5 + 1$ (ITU-T Recommendation X.25). At the beginning of each CRC word calculation, all shift register stage contents shall be initialized to "1". The CRC word shall be complemented (1s complement) prior transmission.

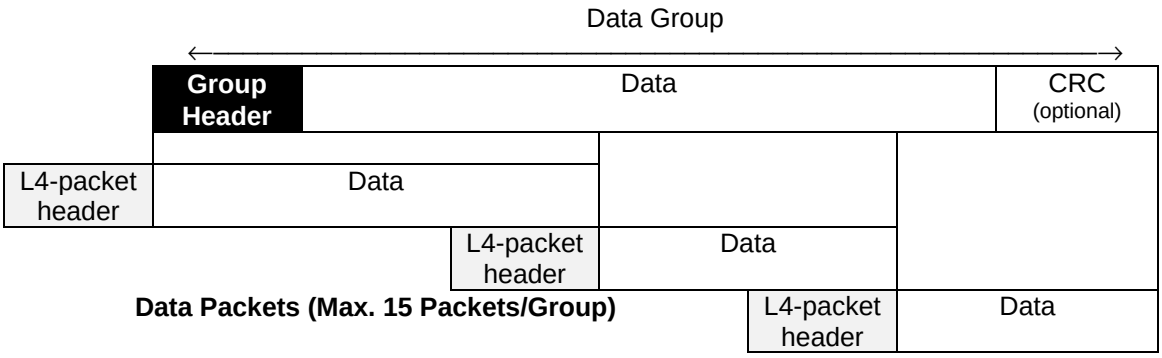


Figure 21: Data units within LMCh

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

DGCA Flag	CRC Flag	Session flags	Data group type	Continuity index	Repetition index	DGCA field	Session Header
1 bit	1 bit	2 bits	4 bits	4 bits	4 bits	16 bits	16 bits

Figure 22: Data Group header (32 bits)

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 flags: These two bits indicate the presence of a segment field and/or of an End User Address field. It is coded as follows:

Table 16

b5	b4	Meaning
0	0	no Session Header
0	1	no Last flag, no Segment Number but End User Address field present
1	0	Last flag and Segment Number present but no End User Address field
1	1	Last flag, Segment Number and End User Address 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 17

b3 b0	Meaning
0 0 0 0	General Data
0 0 0 1	Conditional Access Messages (ECM and EMM)
0 0 1 0	General Data with Conditional Access according to configuration 1 or 2 of table 8.1
0 0 1 1	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.

DGCA field: Data Group Conditional Access field (see subclause 9.2.3).

Session header: it is a 16-bit field composed as follows:

Last Flag	Segment Number	End User Address Field
1 bit	15 bits	n bytes

Figure 23

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.

End User Address field: the EUA field is coded as follows:

EXT flag	RFA	EUA length (=n)	Link field	address field	address list extension field
1 bit	←3 bits→	←4 bits→	←16 bits→	← (n-2) × 8 bits→	

Figure 24

EXT flag: this flag indicates whether the address list extension fields are present or not, as follows:

0: no address list extension field;
1: address list extension field present.

RFA: Reserved for Future Additions.

EUA length: this 4 bits field codes the length in bytes of both link field and address field (from 0 to 15). If it equals 0 none of these fields is present. The link field is always two bytes long. It associates the current Data Group with the File transfer description Data Group with the same link field. The real length of the address field is 2 bytes shorter than the EUA length. It codes also the length of the each address in the extension field. The EUA length is coded as an unsigned binary number in the range 0-15.

Address field: this field, when present, indicates the address of the end user on one or more bytes (up to 13) coded as an unsigned binary number, or a temporary address if the EXT flag is set.

Address list extension field: the address list extension field is coded as follows:

Address number	1st list address	2nd list address	.....	nth list address
8 bits	n × 8 bits	n × 8 bits		n × 8 bits

Figure 25

Address number: this field is present when the list flag is set and indicates the number of end user addresses of the address list.

nth address: this field when present (list flag set) indicates the address of the nth end user of the address list on one or more bytes (up to 13) coded as an unsigned binary number.

One constraint exists between the **EUA length** field and the **length of list** field in order to restrict the length of the data group header to the maximum length of one data packet (248 bytes). This is summarized in the table below.

Table 18

EUA length value	Address number maximum value
3	239
4	119
5	79
6	59
7	47
8	39
9	33
10	29
11	25
12	23
13	20
14	19
15	17

RFA: Reserved for Future Additions.

EUA length: this 4 bits field codes the length in bytes of the address field (from 0 to 15 bytes). It is coded as an unsigned binary number in the range 0-15.

Address field: this field when present indicates the address of the End User on one or more bytes (up to 15) coded as an unsigned binary number.

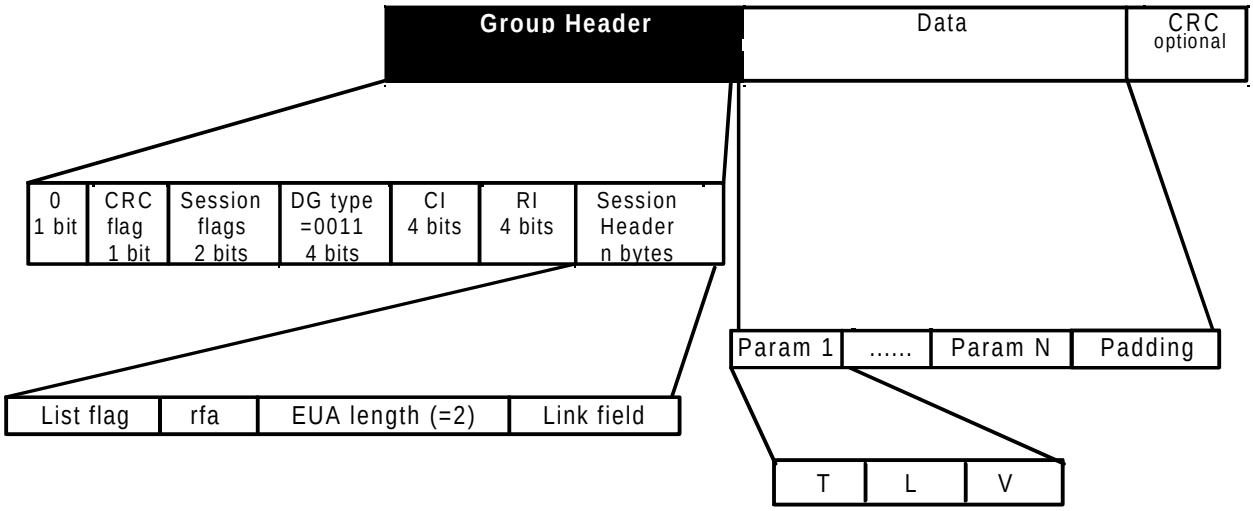


Figure 26: Coding of File Transfer Description Data Groups

Link Field: shall match the Link filed of the associated DG.

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 = 0xFF, 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). Scrambling can be applied to service components, either using a common Control Word or using separate Control Words for each component.

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.

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

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

When Conditional Access mechanisms are used, the service component 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 component is said to be in free access mode.

In scrambling mode c), a subscription is required to recover the encrypted control word. The component 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/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 component. 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 (CA) signalling configurations

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

Table 19: Configurations for ECM and EMM locations

Config.	SCCA content (see subclause 8.2.2)	ECM Location	EMM Location
1	not transmitted	In LMCh, with: - Data Group type =0001 - command packets - same packet address and IND as data packets - One subchannel per component	In LMCh, with: - Data Group type =0001 - command packets - same packet address and IND as data packets - One subchannel per component
2	not transmitted	In LMCh, with: - Data Group type =0001 - command packets - same packet address and IND as data packets - One subchannel per component	In a common LMCh subchannel with: - Data Group type =0001 - command packets - address=111000000 and IND=0
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=111000000 and IND=0
4	MM=01 SMC_ECMId (ECM short message address)	in SMCh short messages with address identified by SMC_ECMId and same IND as the scrambled data messages	In a common LMCh subchannel with: - Data Group type =0001 - command packets - address=111000000 and IND=0
5	MM=00 SMC_ECMId	in SMCh short messages with address identified by SMC_ECMId and same IND as the scrambled data messages	in SMCh short messages with: ADD=000000 and IND=0
6	MM= 11 EMM flag=0	In LMCh, with: - Data Group type =00010001 - command packets - same packet address and IND as data packets - One subchannel per component	In LMCh, with: - Data Group type =00010001 - command packets - same packet address and IND as data packets - One subchannel per component
7	MM=11 EMM flag=1	In LMCh, with: - Data Group type =00010001 - command packets - same packet address and IND as data packets - One subchannel per component	In a common LMCh subchannel with: - Data Group type =0001 - command packets - address=111000000 and IND=0

Table 20: Allowed configurations depending on data location

Data Location	SCCA location	IM, Flags Location	Allowed configurations for ECM and EMM locations
Data Group with type=0000	Service description table	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	Service description table	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 et 5
Short Message	not transmitted	SMCCA in the short message header	not allowed case
Short Message	Service description table	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 et 5

NOTE 1: Conditional Access at long message level using indirect signalling in service description table is not allowed for compatibility reasons with Conditional Access at data group level.

NOTE 2: In configuration 6 and 7, SCCA is exclusively transmitted in service description table.

NOTE 3: 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 component level.

9.1.3.2 Scrambling/descrambling service components in DG

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 (DG) 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):

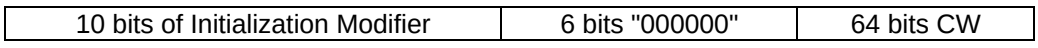


Figure 27

9.1.3.3 Scrambling/descrambling service components in LMCh

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):

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

Figure 28

9.1.3.4 Scrambling/descrambling service components in SMCh

For service components 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 111111 and IND=0 is dedicated for this purpose. Temporary addresses may be used if the DAB format is signalled in the channel organization table.

The structure of FIG type 5, when scrambled, is shown in figure 29.

←——————— FIG type 5 header + added bytes ———————→

101	Length	D1	D2	TCId	Extension	FIDCCA(_ext)	Type 5 data field
3 bits	5 bits	1 bit	1 bit	3 bits	3 bits	2 or 3 bytes	up to 29 bytes

Figure 29

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 30.

←——————— FIG type 6 header ———————→

110	Length	First/Last	Identifier	Type 6 data field
3 bits	5 bits	2 bits	6 bits	up to 31 bytes

Figure 30

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.	SCCA content (see subclause 8.2.2)	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=111000000
9	MM=00 FIC_ECMId	in FIG type 6 messages identified by FIC_ECMId	in FIG type 6 messages with Id=000000

Only these two configurations are allowed for the ECMs and EMMs locations when scrambled data are 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 31

For service components 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 all the service components of a 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 all the service components of the service;
0 0 1	NR-MSK;
0 1 0	EUROCRYPT;
other	reserved for future definition.

9.2.2 Service Component Conditional Access (SCCA)

For each access controlled service component, the SCCA contains the parameters necessary for descrambling. The SCCA 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 component. The SCCA is sent either in the service description table, or in SMCCA_Ext or in LMCCA_Ext.

The ECMs can be sent:

- in SMCh messages with address given by SCCA content;
- in a LMCh subchannel with address given by SCCA content;
- in the same LMCh subchannel as the service component itself (in command packets with same address as related data packets of the component).

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

The EMM can be sent:

- in SMCh messages with address ADD=000000 and IND=0;
- in a common LMCh subchannel with address ADD=111000000 and IND=0;
- in the same LMCh Subchannel as the service component 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 32 describes the different parameters of SCCA:

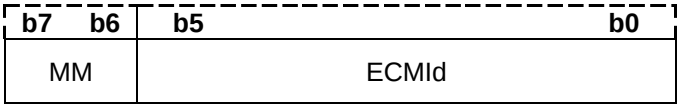


Figure 32

MM defines the Messaging Modes and ECMId is the address of the ECM subchannel:

- in the LMCh (LMC_ECMId);
- in the SMCh (SMC_ECMId);
- in FIG type 6 (FIC_ECMId).

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 "000000" 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: "111000000 ". 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 address "000000" is not allowed.
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. The EMM shall be sent in the LMCh in a common subchannel identified by the address: "111000000 ".
11	In this case: - ECMs are sent in the same subchannel as the service component (only when transmitted in LMCh) - SCCA is exclusively transmitted in the service description table - Bit b5 of SCCA shall be considered as an EMM flag which signals: if set to 1, that EMMs are sent in the same subchannel as the service component (config. 6) if set to 0, that EMMs are sent in a common LMCh subchannel with ADD=111000000 and IND=0.

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 component. The command bit of packet headers shall be set to 0 (data). The coding of DGCA is described in figure 33:

b15...b6	b5	b4	b3	b2 b1	b0
IM	RFA	Rp	Parity flag	Scrambling mode	Update ECM
10 bits	1 bit	1 bit	1 bit	2 bits	1 bit

Figure 33: 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 component. This parameter shall exist if the CA flag of the service component is set to 1.

The coding of LMCCA is described in figure 34:

b15...b6	b5	b4	b3	b2 b1	b0
IM	Ext. flag	Rp	Parity flag	Scrambling mode	Update ECM
10 bits	1 bit	1 bit	1 bit	2 bits	1 bit

Figure 34: 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 SCCA indicating where the ECMs of the service component can be found.

The coding of LMCCA_Ext is described in figure 35.

b15...b6	b5	b4	b3	b2...b1	b0	b7...b6	b5...b0
IM	Ext. flag	Rp	Parity flag	Scrambling mode	Update ECM	MM	ECMId
10 bits	1 bit	1 bit	1 bit	2 bits	1 bit	2 bits	6 bits

Figure 35: 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. The value "000000" is 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: "111000000 ";
- 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 3 MSB are set to "1" to complete the address. The EMMs shall be sent in the LMCh subchannel identified by the packet address: "111000000 ".

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 component. This parameter shall exist if the CA flag of the service component is set to 1 and/or if CAId is not equal to zero.

The coding of SMCCA is described in figure 36:

b15...b6	b5	b4	b3	b2...b1	b0
IM	Ext. flag	Rp	Parity flag	Scrambling mode	Update ECM
10 bits	1 bit	1 bit	1 bit	2 bits	1 bit

Figure 36: 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 SCCA indicating where the ECMs of the service component can be found.

The coding of SMCCA_Ext is described in figure 37:

b15...b6	b5	b4	b3	b2...b1	b0	b7...b6	b5...b0
IM	Ext. flag	Rp	Parity flag	Scrambling mode	Update ECM	MM	ECMId
10 bits	1 bit	1 bit	1 bit	2 bits	1 bit	2 bits	6 bits

Figure 37: 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. The value "000000" is 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: "111000000";
- 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 the ECM message (6 least significant bits of the address of the packets transporting these ECMs). The value "000000" is not allowed. The 3 most significant bits are set to "1" to complete the address. The EMMs shall be sent in the PaCh Sub-channel identified by the packet address: "111000000".

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 38:

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 38: 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 39:

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 39: 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 40.

b7 b2	b1	b0
Type of crypto-algorithm	Rfa	T
6 bits	1 bit	1 bit

Figure 40: 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 41:

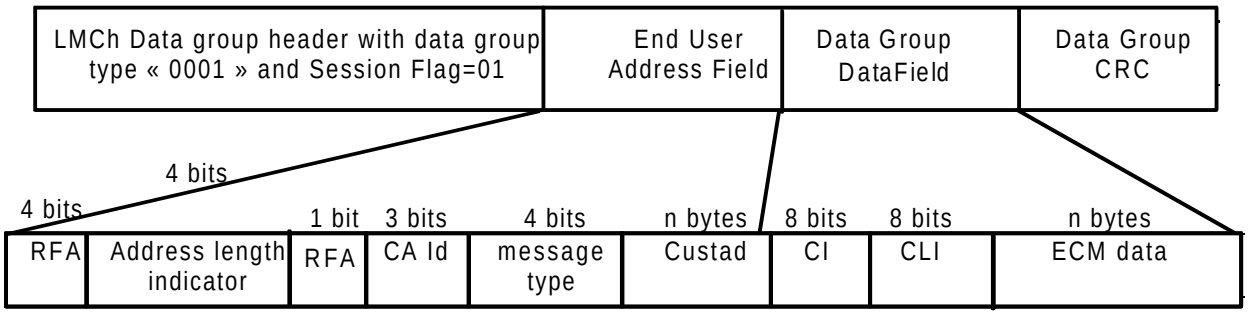


Figure 41: Data group structure containing an ECM

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 42:

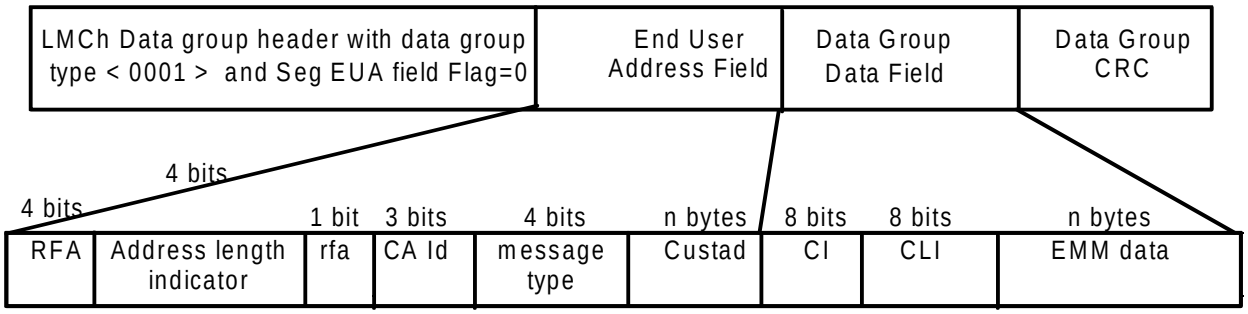


Figure 42: Data group structure containing an EMM

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 all the access controlled service components shall be carried in messages having the same address (see table 29).

The ECMs of each access controlled service component 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 (9 bits)	
	MSB	LSB
	b9...b6	b5...b0
ECM	111	LMC_ECMId (6 bits)
EMM	111	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 43 and 44.

For ECMs, address shall be different from 000000 and contains SMC_ECMId.

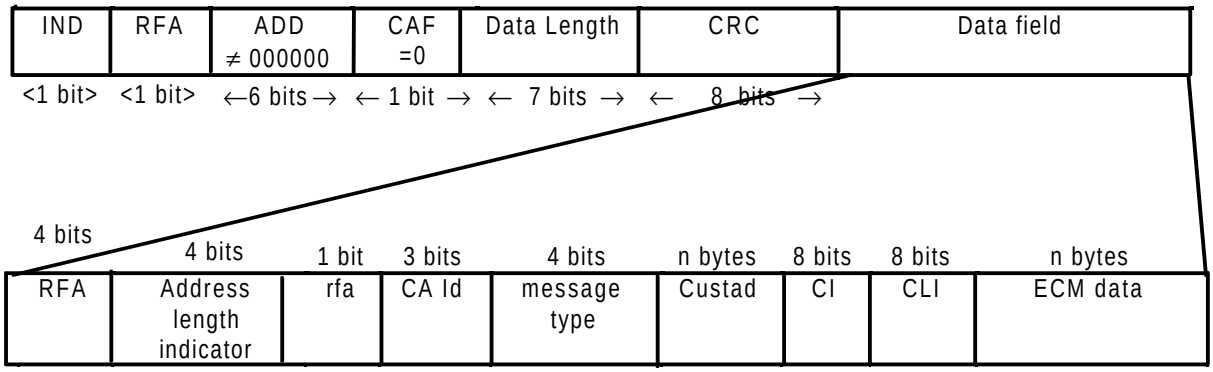


Figure 43: ECM coding in SMCh

The data field contains all or part of one ECM identified by SMC_ECMId;

For EMMs, Address (ADD) is equal to 000000.

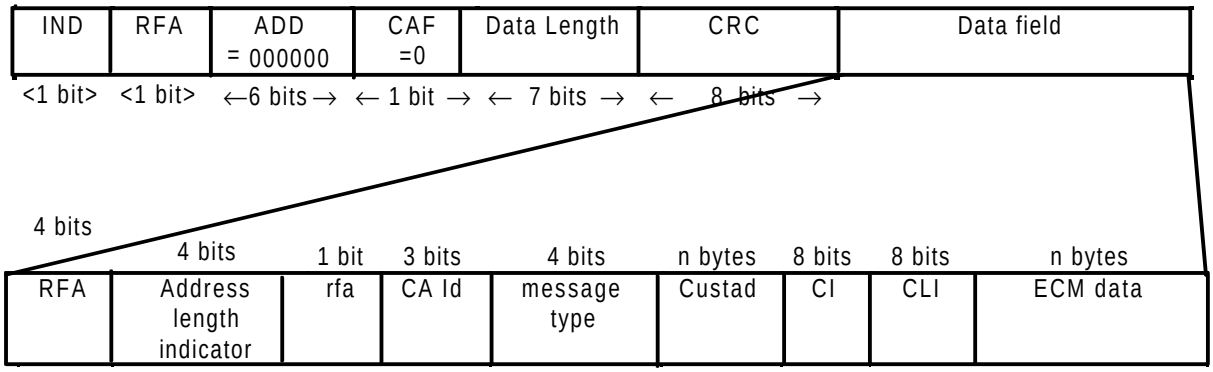


Figure 44: EMM coding in SMCh

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 = 000000: the data field contains all or part of one EMM;
- CAId, message type, CustAd, CI, CLI, data: see subclause 9.3.1.2.

9.3.2.3 Together with service component

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 component.

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 BLOCK PARITY is calculated using the generator polynomial:

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

10.2 Other layers error detection strategy

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).

In practice, four different CRCs are used:

- CRC with a 6 bits parity length for SeCh and L3-headers. The generator polynomial is given by the expression: $x^6 + x^3 + 1$;
- CRC with a 8 bits parity length for SMCh and LMCh L4-headers. The generator polynomial is given by the expression: $x^8 + x^5 + x^4 + x^3 + 1$;
- CRC with a 14 bits parity length for SeCh and L3-headers;
- CRC with a 16 bits parity length for SeCh and L3-headers.

11 Quality of service

11.1 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.

11.2 Expected capabilities of a CA system

The aim of this subclause is to present the expected capabilities of a CA 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.

11.2.1 From the user's point of view

11.2.1.1 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.

11.2.1.2 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.

11.2.2 From the service operator's point of view

11.2.2.1 Bit rate needed to broadcast CA 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.

11.2.2.1.1 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_{ecm}) needed to send the ECMs of one scrambled component 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 components. This simplification is no longer possible if scrambling is done at the source.

11.2.2.1.2 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: Np;
- 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 Ng of EMMs that have to be sent (which is closely related to the number of customers or groups of customers).

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

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

1) If it should 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 it should 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, etc.);
- 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.

11.2.2.2 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.

11.2.2.3 Transcontrol

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

11.2.2.4 Scrambling by components

A programme or service can be made up of several components (video, sound, Teletext, etc.). The very possibility of associating different access conditions with each of the components has consequences on access control and multiplex organization. These access methods can be used in combination to define the conditions of access to the various components. Such definition entails the continuous transmission of Entitlement Control Messages (ECM) in signal.

11.2.2.5 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.

11.2.2.6 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.

11.2.2.7 Hierarchical coding and scrambling

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

12 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
Examples	**X.400**	**Operator**	**Times, Le Monde**	**TMC, Weather**	**dGPS**	**Sound, Still pictures**	**Tele** software
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 kbytes		< 10 Mbytes	1-15 blocks	1-5 blocks	< 1 Mbytes	< 10 Mbytes
Average bit-rate	large	low		low	1 200 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 1997-01-17