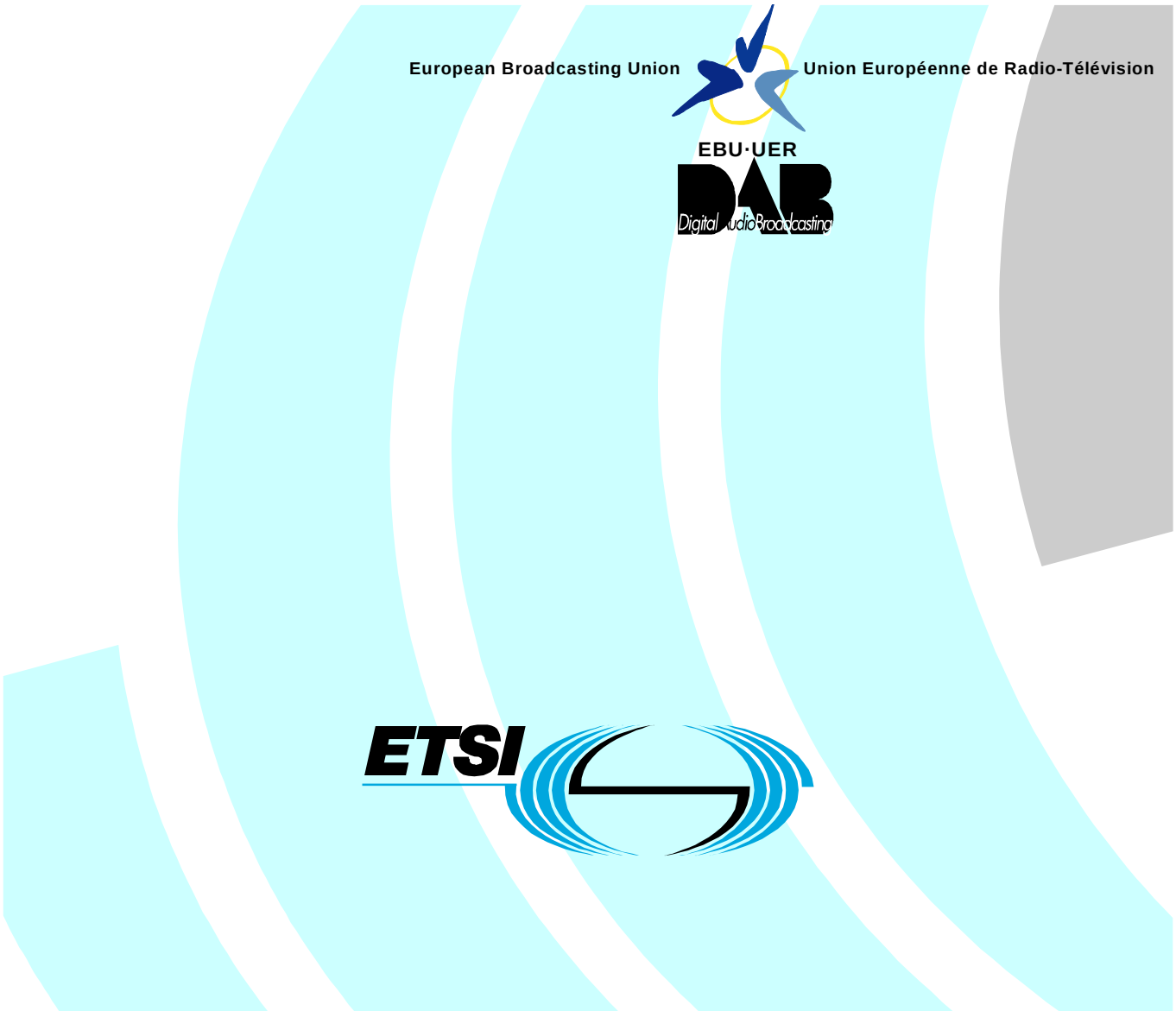
ETSI TS 102 367 V1.1.1 (2005-01)

Technical Specification

Digital Audio Broadcasting (DAB); Conditional access



Reference
DTS/JTC-DAB-35

Keywords
audio, broadcasting, DAB, data, digital,
packet mode

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

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

NOTE 1: The EBU/ETSI JTC Broadcast was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadcast 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
CH-1218 GRAND SACONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

The Eureka Project 147 was established in 1987, with funding from the European Commission, to develop a system for the broadcasting of audio and data to fixed, portable or mobile receivers. Their work resulted in the publication of European Standard, EN 300 401 [1], for DAB (see note 2) which now has worldwide acceptance. The members of the Eureka Project 147 were drawn from broadcasting organizations and telecommunication providers together with companies from the professional and consumer electronics industry. In 1995, the European DAB Forum (EuroDAB) was established to pursue the introduction of DAB services in a concerted manner world-wide, and it became the World DAB Forum (World DAB) in 1997.

NOTE 2: DAB is a registered trademark owned by one of the Eureka Project 147 partners.

Introduction

The Conditional Access specification provides DAB with the ability to deliver encrypted services, both audio and data, both stream mode and packet mode, within a standardized framework.

1 Scope

The present document specifies how to use Conditional Access within the Digital Audio Broadcasting (DAB) system.

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI EN 300 401: "Radio Broadcasting Systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers".

[2] ETSI ETS 300 174 (1992): "Network Aspects (NA); Digital coding of component television signals for contribution quality applications in the range 34-45 Mbit/s".

[3] CENELEC EN 50094 (1992): "Access control system for the MAC/packet family: EUROCRYPT".

3 Definitions, abbreviations and conventions

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EN 300 401 [1] and the following apply:

Access Control System (ACS): particular set of rules for managing entitlement checking and conditional access messages

blackout state: denial of access to a service because it is restricted for some reason (for example, targeted only to a particular geographical region)

Conditional Access (CA): mechanism by which the user access to service components can be restricted

Control Word (CW): secret part of the IW that depends on the ACS used

Entitlement Checking Messages (ECM): these messages contain information about the conditions required for accessing service components, which are intended for restricted access, and for descrambling the data

Entitlement Management Messages (EMM): these messages contain information about the conditions required for accessing service components which are intended for restricted access and for descrambling the data

Initialization Modifier (IM): openly available and continually-changing part of the IW that provides information to synchronize the generation of de-scrambling parameters to the received scrambled data

Initialization Word (IW): data string that is used to periodically reset the state of the pseudo-random bit sequence generator used to scramble the data

replacement: presentation of another service to a customer for whom a "blackout state" applies

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in EN 300 401 [1] and the following:

ACS	Access Control System
CA	Conditional Access
CAId	Conditional Access Identifier
CAOrg	Conditional Access Organization
CustAd	Customer Address
CW	Control Word
DGCA	Data Group Conditional Access
ECM	Entitlement Checking Message
EMM	Entitlement Management Message
FIDCCA	Fast Information Data Channel Conditional Access
IM	Initialization Modifier
IMW	Initialization Modifier Word
IW	Initialization Word

3.3 Convention

Unless otherwise stated, the following notation, regarding the order of bits within each step of processing is used:

- in figures, the bit shown in the left hand position is considered to be first;
- in tables, the bit shown in the left hand position is considered to be first;
- in byte fields, the Most Significant bit (MSb) is considered to be first and denoted by the higher number. For example, the MSb of a single byte is denoted "b_7" and the Least Significant bit (LSb) is denoted "b_0";
- in vectors (mathematical expressions), the bit with the lowest index is considered to be first.

NOTE: Due to time-interleaving, this order of bits is not the true transmission order.

4 Conditional Access (CA)

The Conditional Access system used in the DAB 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 ensemble.

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, level 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 ensemble as the scrambled services or by some other means.

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 DAB multiplex. Clause 4.1 describes the scrambling/descrambling procedures for data in Stream and Packet modes and in the FIDC. These procedures are completely independent of any other scrambling procedures that may also be performed on the signal (for example energy dispersal scrambling). Clause 4.2 describes the parameters which are used to provide signalling and synchronization for access control. Clause 4.3 describes the different possibilities that can be used to send the access control messages (ECMs and EMMs).

4.1 Scrambling audio and data

4.1.1 Introduction

For each service component, a Conditional Access flag (CA flag) and/or a Conditional Access Identifier (CAId, see clause 4.2.1) 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 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.

4.1.2 Description of the audio and data scrambling processes

To scramble audio and data, a Pseudo-Random Binary Sequence (PRBS) shall be added modulo 2 to the audio or data bytes, that shall be scrambled according to the mechanism described in clauses 4.1.4.2 to 4.1.4.4. The PRBS generator shall be the same as defined in ETS 300 174 [2], clause 12.2. In some cases, some particular bytes which remain unscrambled (for example, packet headers) are also defined. For these particular bytes, the PRBS generator is not activated.

4.1.3 Generating scrambling and descrambling sequences

An Initialization Word (IW) shall be used to initialize the PRBS generator. The IW bytes shall be inserted in the PRBS, most significant byte first, byte by byte. In this clause, the formation of the IW is defined and phasing considerations are described.

4.1.3.1 Generation of the initialization word

The Initialization Word is a bit string which shall be used to initialize the PRBS generator. It contains two parts, the Initialization Modifier (IM) and the Control Word (CW):

a) The Initialization Modifier (IM) varies very often (every logical frame or every MSC data group) 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 descramblers, and to prevent the output of very long scrambling/descrambling sequences. The Initialization Modifier comprises a number (logical frame count, MSC data group counter value, notional packet counter value) and sometimes a service component Identifier. This last parameter should be used to prevent two service components using the same ECMs and being scrambled with the same scrambling sequences.

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 8 bytes long. In free access mode, the Control Word shall be fixed, it shall have all 64 bits set to "1". In controlled access mode, the Control Word shall be provided by the Access Control System (ACS).

4.1.3.2 Phasing

The period during which a CW 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.

4.1.4 Scrambling/descrambling processes

This clause specifies three different Conditional Access signalling configurations and the way Conditional Access is incorporated into the different data transport mechanisms (see [1], clause 5.3 for audio data, data in Stream and Packet mode, and [1], clause 5.2.2.3 for the FIDC).

4.1.4.1 Conditional Access signalling configurations

Three different configurations are available for signalling CA information. Configuration 1 is suitable for all data transport mechanisms which are synchronized to the CIF counter. Configuration 2 is suitable for data in Packet mode or for data sent in the FIDC but not for data in Stream mode. Configuration 3 is suitable only for data in Packet mode.

Configuration 1

In configuration 1, all the parameters which are necessary to descramble a service component are carried separately from the service component. The following conditions apply:

- The initialization Modifier (IM) and the phase parity shall be derived from the logical frame count (see [1], clause 5.3), the phase parity shall be changed every 250 logical frames and so the parity flag shall be signalled using bit b_8 of the logical frame count and the IM using bits b_7 ... b_0 of the logical frame count.

- The scrambling mode and the updating bits of the service component shall be sent in the parameter CAOrg in the FIC (see clause 4.2.2).

- The ECMs containing the Control Words shall be sent either in the FIG type 6 or in sub-channel 63.

Configuration 2

The following conditions apply:

- The Initialization Modifier, the phase parity, the scrambling mode and the updating bits shall be sent with the Service component. This shall be either at the beginning of each MSC data group (DGCA: see clause 4.2.3) in the scrambled sub-channel, in the case of data carried in the Packet mode, or at the beginning of each FIG type 5 (FIDCCA or FIDCCA_Ext: see clause 4.2.4), in the case of data carried in the FIC.

- The ECMs containing the Control Words are sent either in the FIG type 6 or in sub-channel 63.

Configuration 3

In configuration 3, all the parameters which are necessary to descramble a service component are carried with the service component. The following conditions apply:

- The Initialization Modifier, the phase parity, the scrambling mode and the updating bits shall be sent at the beginning of each MSC data group (DGCA: see clause 4.2.3) in the scrambled sub-channel.

- The ECMs containing the Control Words shall be sent in command packets (see clause 4.3.2.1) inserted inside the Packet stream of the service component.

The signalling locations for CA information are summarized in table 1.

Table 1: CA signalling locations

CA signalling configuration	FIC or sub-channel 63	With service component
1	IM (derived from the logical frame count); Phase parity (derived from the logical frame count); Scrambling mode in CAOrg; Update in CAOrg; ECM in FIG 6 or sub-channel 63	
2	ECM in FIG 6 or sub-channel 63	IM Phase parity Scrambling mode Update
3		IM Phase parity Scrambling mode Update ECM

4.1.4.2 Scrambling/descrambling of service components in stream mode

For stream mode, only configuration 1 is possible. For audio data, scrambling shall be performed before energy dispersal scrambling (see figure 1).

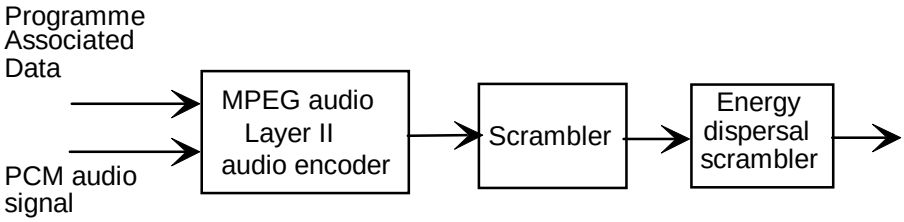


Figure 1: Scrambling of audio in Stream mode

For general data, scrambling is performed before energy dispersal scrambling (see figure 2).

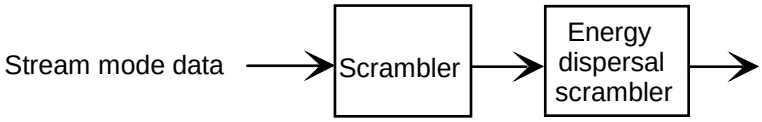


Figure 2: Scrambling of general data in stream mode

In both cases, at each new logical frame, the PRBS generator is initialized with an Initialization Word (MSB first) structured as shown in figure 3.

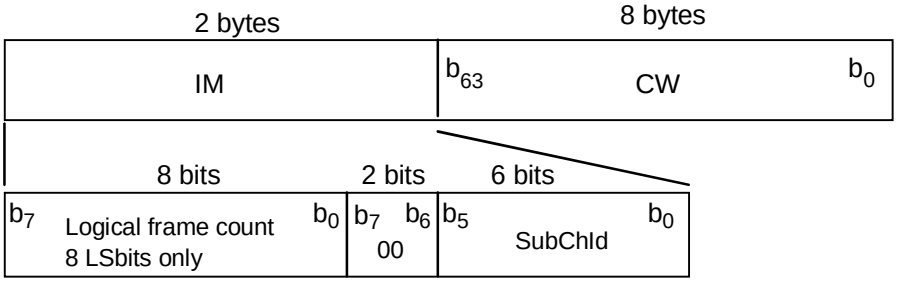


Figure 3: Structure of the IW for general data in stream mode

The following definitions apply:

IM, **CW:** see clause 4.1.3.1.

Logical frame count: see [1], clause 5.3.

SubChId: see [1], clause 6.2.

The 10 bytes of IW shall be inserted in the PRBS generator, most significant byte first, byte per byte.

4.1.4.3 Scrambling/descrambling of service components in packet mode

For service components in Packet mode, all the three CA signalling configurations are possible.

Configuration 1

When configuration 1 is chosen, scrambling shall be performed after the packet multiplex assembler and before the energy dispersal scrambler as shown in figure 4.

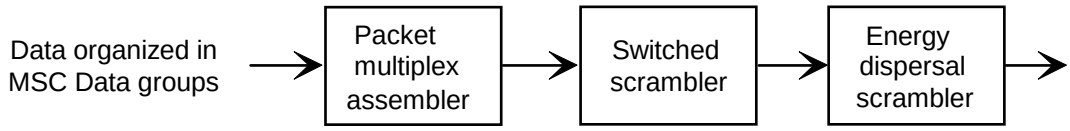


Figure 4: Scrambling in the packet mode in configuration 1

The PRBS generator shall be initialized at the beginning of each packet with an Initialization Word (MSB first) structured as shown in figure 5.

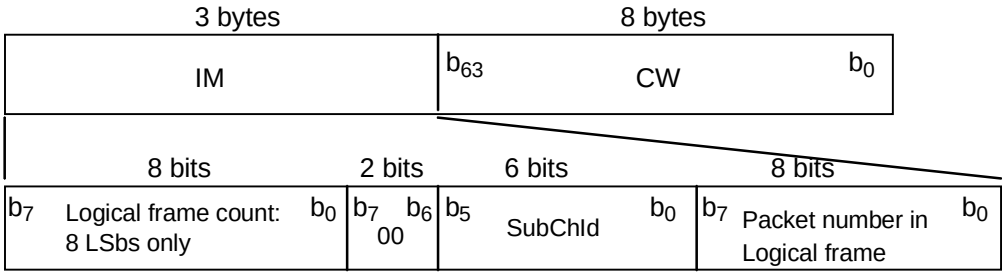


Figure 5: Structure of the IW for packet mode in configuration 1

The following definitions apply:

IM, **CW:** see clause 4.1.3.1.

Logical frame count: see [1], clause 5.3.

SubChId: see [1], clause 6.2.

Packet number in Logical frame: this 8-bit field shall be a notional counter value defined in the following way. At each new logical frame, the number of the first packet sent in the sub-channel shall be zero. This packet number is incremented (modulo 256) at each new packet in the logical frame of the sub-channel (independently of its address).

Padding packets, padding bytes (if any), packet headers and the packet CRC shall not be scrambled. The packet CRC shall be calculated on the unscrambled packet header and the unscrambled data field.

The 11 bytes of IW shall be inserted in the PRBS generator, most significant byte first, byte per byte.

Configurations 2 and 3

In these two configurations, data (already organized in MSC data group data fields) shall be scrambled as shown in figure 6. The Initialization Modifier, the phase parity, the scrambling mode and the updating bits shall be sent at the beginning of each of these MSC data groups in the Data Group Conditional Access parameter (DGCA: see clause 4.2.3). Scrambling is performed on the Data group data field only, for MSC data group "0010" and "0101". The MSC data group header and the session header (see [1], figure 9) are not scrambled. The Data group CRC is performed on the unscrambled MSC data group header, the unscrambled DGCA field, the optional unscrambled Session header and the scrambled MSC data group data field.

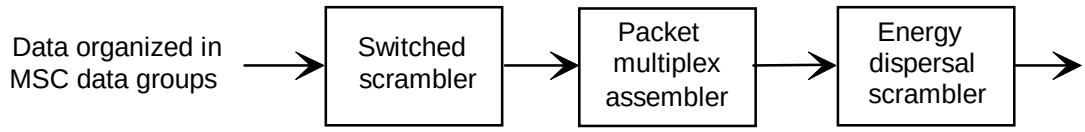


Figure 6: Scrambling in the packet mode in configurations 2 and 3

The PRBS generator shall be initialized at the beginning of the MSC Data group with an Initialization Word (MSB first) structured as shown in figure 7.

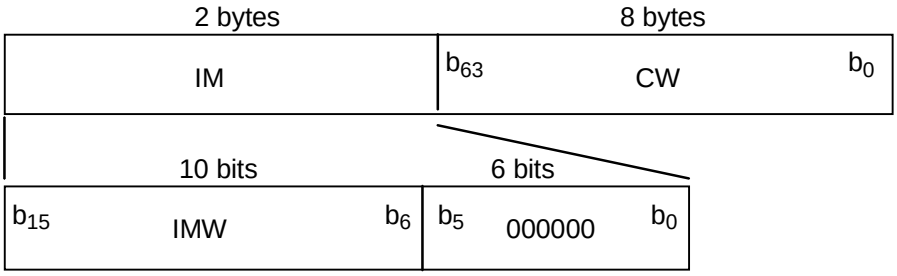


Figure 7: Structure of the IW for packet mode in configurations 2 and 3

The following definitions apply:

IM, **CW:** see clause 4.1.3.1.

IMW (Initialization Modifier Word): this 10-bit field shall signal a number which should be varied frequently. This number need not be related to other DAB counters such as the logical frame count.

The 10 bytes of IW shall be inserted in the PRBS generator, most significant byte first, byte per byte.

4.1.4.4 Scrambling/descrambling of service components in the FIDC

For service components sent in FIDC, only CA signalling configurations 1 and 2 are possible. Scrambling is performed before the Fast Information Block assembler.

Configuration 1

In configuration 1, scrambling shall be performed on data already organized in the FIG type 5 format (see figure 8).

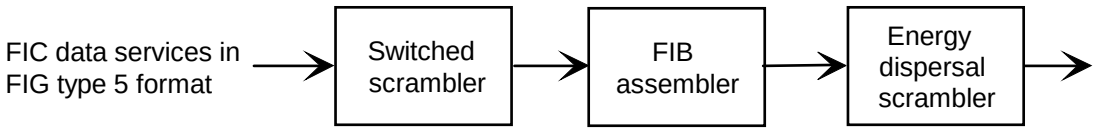


Figure 8: Scrambling in the FIDC in configuration 1

The 8 LSbs of the CIF counter shall be used, as a part of the IM, for all scrambled FIGs sent in FIBs, which are assigned to the same CIF.

The PRBS generator shall be initialized, for each new FIG, with an Initialization Word (MSB first) structured as shown in figure 9.

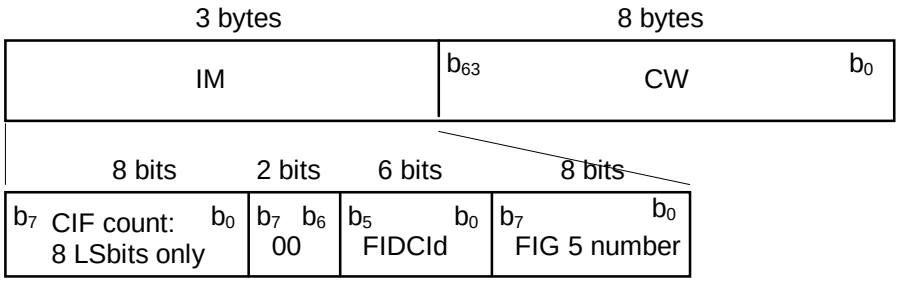


Figure 9: Structure of the IW for the FIDC in configuration 1

The following definitions apply:

IM, **CW:** see clause 4.1.3.1.

CIF count: see [1], clause 5.3.

FIDCId: see [1], clause 6.3.1.

FIG 5 number: this 8-bit field shall be a notional counter value defined in the following way. For every new IM, the first FIG type 5 field shall have a number equal to zero. This FIG type 5 number shall be incremented by 1 (modulo 256) at each new FIG type 5 field (independently of its Extension field and TCId).

Only the type 5 field is scrambled: the FIG type 5 header and the following byte (D1, D2, TCId and Extension) shall always be unscrambled.

The 11 bytes of IW shall be inserted in the PRBS generator, most significant byte first, byte per byte.

The FIB CRC shall be calculated on all FIGs, scrambled or unscrambled, contained in the FIB data field.

Configuration 2

In this configuration, scrambling is performed individually on each FIC data service, before data is organized in the FIG type 5 format (see figure 10).

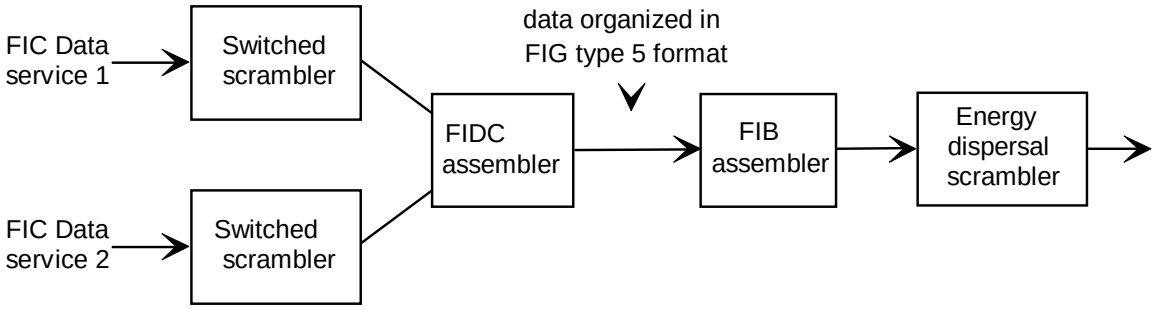


Figure 10: Scrambling in the FIDC in configuration 2

The Initialization Modifier, the phase parity, the scrambling mode and the updating bits shall be sent in the parameters FIDCCA or FIDCCA_Ext. (see clause 4.2.4). These bits are not scrambled. The situation after scrambling and after the FIG type 5 assembler is shown in figure 11.

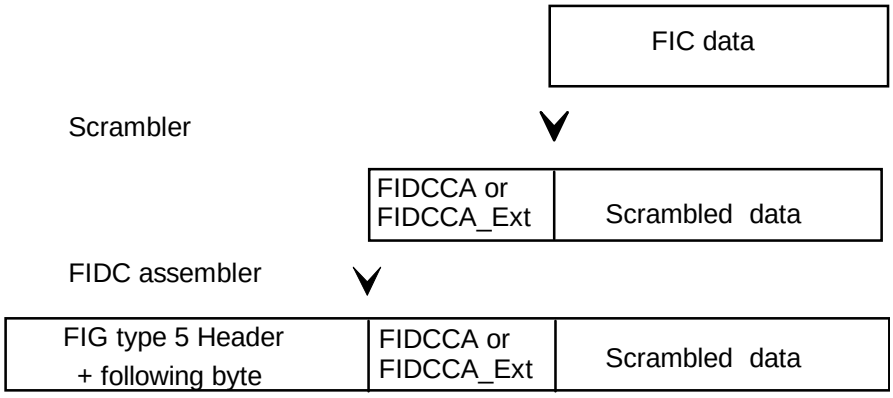


Figure 11: Insertion of FIDCCA in the FIDC in configuration 2

The PRBS generator shall be initialized, for each new FIG, with an Initialization Word (MSB first) structured as shown in figure 12.

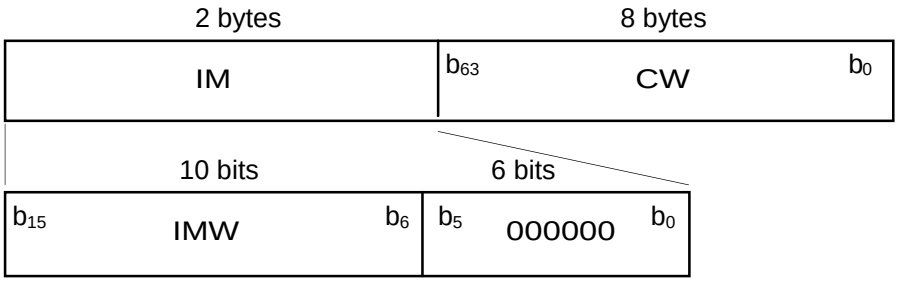


Figure 12: Structure of the IW for FIDC in configuration 2

The following definitions apply:

IM, **CW:** see clause 4.1.3.1.

IMW: see clause 4.1.4.3.

The FIB CRC shall be calculated on all FIGs, scrambled or unscrambled, contained in the FIB data field.

The 10 bytes of IW shall be inserted in the PRBS generator, most significant byte first, byte per byte.

4.2 CA signalling and synchronizing data

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

4.2.1 Conditional Access Identifier (CAId)

This 3-bit field shall identify the Conditional Access system used for all the service components of a service. The interpretation of this field is given in table 2.

Table 2: CAId

b_6	b_5	b_4	CAId
0	0	0	No access control for all the components of the service
0	0	1	NR-MSK
0	1	0	Eurocrypt EN 50094 [3]
0	1	1	*rfu*
1	0	0	*rfu*
1	0	1	*rfu*
1	1	0	*rfu*
1	1	1	*rfu*

4.2.2 Conditional Access Organization (CAOrg)

For each access controlled service component, the CAOrg contains the information necessary for descrambling as shown in figure 13.

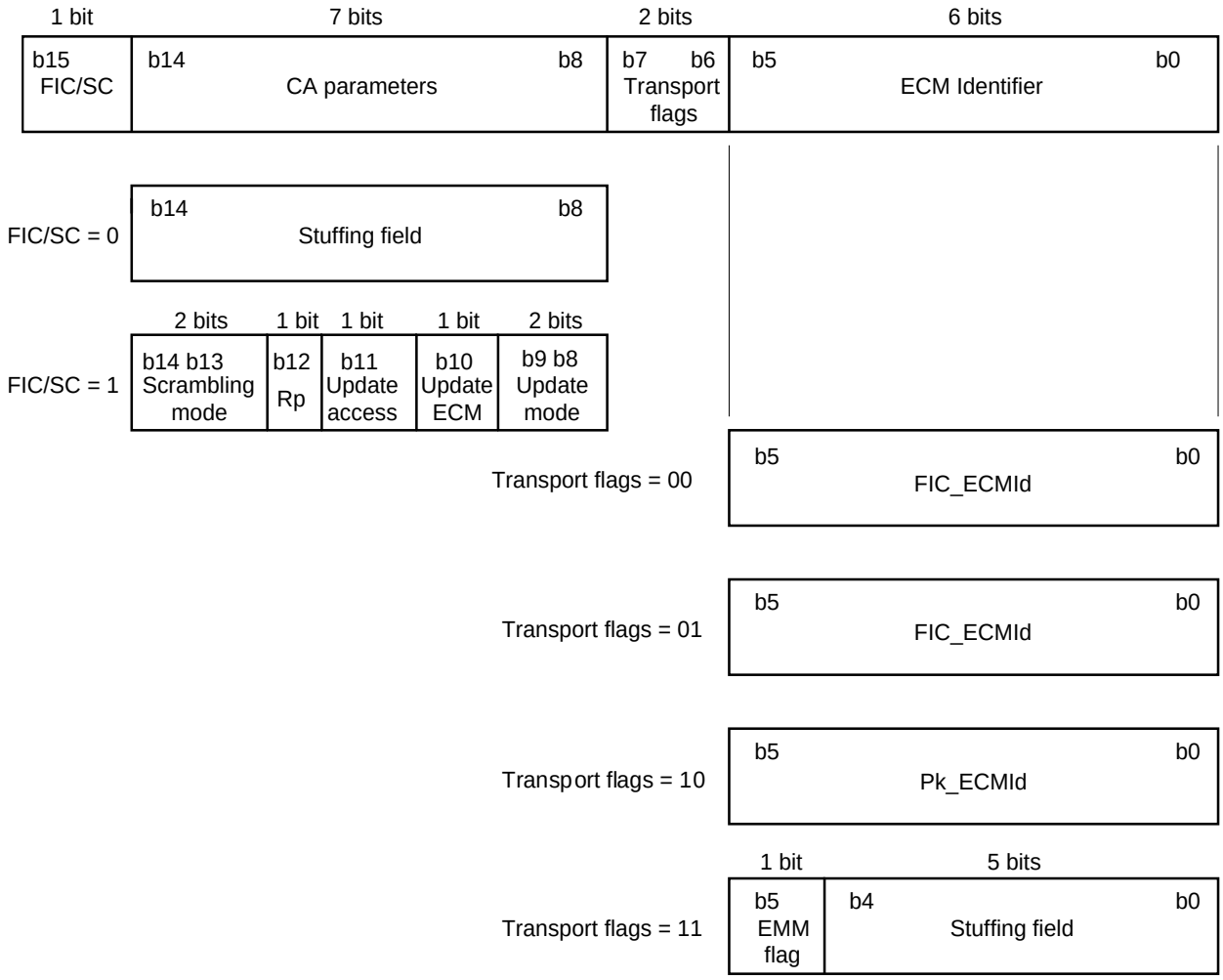


Figure 13: Structure of the CAOrg field

The following definitions apply:

FIC/SC flag: this 1-bit flag shall indicate whether the scrambling mode, replacement function and CA update possibilities are signalled elsewhere or within the CAOrg as follows:

0 : CA parameters signalled elsewhere;

1 : CA parameters signalled in this CAOrg.

The CA parameters may only be signalled elsewhere for Service components in Packet mode or Service components sent in FIDC.

FIC/SC = 0:

- **Stuffing field:** this 7-bit field shall contain stuffing bits which are set to "0".

FIC/SC = 1:

- **Scrambling mode:** this 2-bit field shall identify the scrambling mode as follows:

  b_6 - b_5

  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).

- **Rp (Replacement) flag:** this 1-bit flag shall indicate replacement operations 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) [3].

  The replacement flag indicates to the receiver when to take into account the replacement characteristics given by the ACS if it is in a blackout state [3].

- **Update access:** this 1-bit flag shall indicate a change in the access conditions (signalled in the ECM) which become effective when the four least significant bits of the logical frame count are zero, as follows:

  0 : no update;

  1 : update access.

- **Update ECM:** this 1-bit flag shall indicate a change in the ECM transmission and forces the descrambler to read the next ECM, as follows:

  0 : no update;

  1 : update ECM. Next ECM shall be sent to the ACS.

- **Update mode:** this 2-bit field shall indicate a change in the scrambling mode as follows. The future scrambling mode should be taken into account when the four least significant bits of the logical frame count are zero:

  b_1 - b_0

  0 0 : no update;

  0 1 : update imminent; future mode is "unscrambled";

  1 0 : update imminent; future mode is "scrambled with a local Control Word";

  1 1 : update imminent; future mode is "scrambled with a Control Word regularly transmitted and changed with ECMs.

Transport flags: this 2-bit field shall indicate where to find the ECMs and the possible EMMs of the access controlled service component.

The ECMs or EMMs shall be sent in FIG type 6, in sub-channel 63 or in the same sub-channel as the service component itself. This last option is possible only for service components sent in Packet mode.

Transport flags = "00" (Case 1).

In this case, the ECMs and the EMMs shall be sent in FIG type 6.

- **FIC_ECMId:** this 6-bit field shall indicate the value of the ECM Identifier which is used to identify the structure containing the ECM message in FIG type 6. The value "000000" is not allowed (because it is reserved for the EMM).

Transport flags = "01"(Case 2).

In this case, the ECMs shall be sent in FIG type 6, using the FIC_ECMId), and the EMMs shall be sent in sub-channel 63.

- **FIC_ECMId:** this 6-bit field shall indicate the value of the ECM Identifier which is used to identify the structure containing the ECM message in FIG type 6. The value "000000" is not allowed.

Transport flags = "10" (Case 3).

In this case, both the ECMs and the EMMs shall be sent in sub-channel 63.

- **Pk_ECMId:** this 6-bit field shall indicate the value of the ECM Identifier which is used to identify the structure containing the ECM message. The Pk_ECMId shall comprise the 6 least significant bits of the address of the packets transporting the ECMs. The value "000000" is not allowed (because it is reserved for the EMM).

Transport flags = "11" (Cases 4 and 5).

In these cases, the ECMs shall be sent in the same sub-channel as the service component. This option can only be used for service components carried in Packet mode.

- **EMM flag:** this 1-bit flag shall indicate whether the EMMs are carried in the same sub-channel as the service component or in sub-channel 63, as follows:

  0 : same sub-channel as the service component (Case 4);

  1 : sub-channel 63 (Case 5).

- **Stuffing field:** this 5-bit field shall contain stuffing bits which are set to "0".

Table 3 summarizes all the possible transport possibilities within the ensemble.

Table 3: Allowed ECM/EMM transport mechanisms within the ensemble

EMM	ECM		
Carried in:	**FIG type 6**	**Service component**	**Sub-channel 63**
FIG type 6	Case 1	not allowed	not allowed
Service component	not allowed	Case 4	not allowed
Sub-channel 63	Case 2	Case 5	Case 3

4.2.3 Data Group Conditional Access (DGCA)

This 16-bit parameter is used to transport the IMW and the other CA parameters in the headers of the MSC data groups carrying the service component.

This parameter shall be carried in the Extension field of MSC data groups with type = "0010" and "0101". Consequently, the Extension flag for the MSC data group header is set to "1". The Command bit of packet headers shall be set to "0" (data) (see [1], clause 5.3.2). Figure 14 shows the structure of the DGCA field.

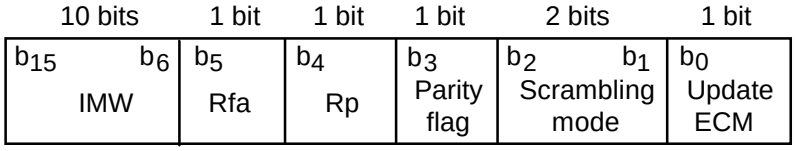


Figure 14: Coding of the Data Group Conditional Access (DGCA) field

The following definitions apply:

IMW: see clause 4.1.4.3.

Rfa: this bit shall be reserved for future additions. The bit shall be set to "0" until it is defined.

Rp (Replacement) flag: see clause 4.2.2.

Parity flag: this 1-bit flag shall be used to indicate the parity of the control word used for the current MSC data group, as follows:

0 : even parity;

1 : odd parity.

Scrambling mode: this 2-bit field shall identify the scrambling mode, as follows:

b_2 - b_1

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: see clause 4.2.2.

4.2.4 Fast Information Data Channel Conditional Access (FIDCCA and FIDCCA_Ext)

4.2.4.1 FIDCCA

FIDCCA is a 16-bit parameter which is used to transport the IMW and the other CA parameters at the start of the FIG type 5 field (see [1], figure 6) transporting the service component. This parameter shall exist if the CA flag of the service component is set to "1" and/or the CAId is not equal to zero. Figure 15 shows the structure of the FIDCCA field.

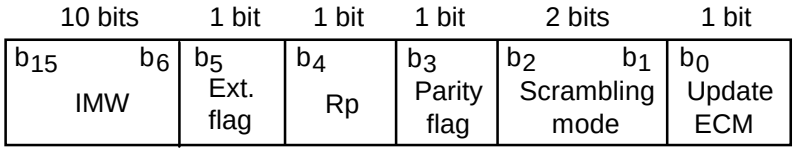


Figure 15: Coding of the Fast Information Data Channel Conditional Access (FIDCCA) field without extension

The following definitions apply:

IMW: see clause 4.1.4.3.

Ext. (Extension) **flag:** this 1-bit flag shall distinguish between FIDCCA and FIDCCA_Ext, as follows:

0 : FIDCCA;

1 : FIDCCA_Ext.

Rp (Replacement) flag): see clause 4.2.2.

Parity flag: see clause 4.2.3.

Scrambling mode: see clause 4.2.3.

Update ECM: see clause 4.2.2.

4.2.4.2 FIDCCA_Extended

FIDCCA_Extended is a 24-bit parameter which combines the FIDCCA with the information provided in the second byte of CAOrg (the CAOrg indicates where the ECMs of the service component can be found). Figure 16 shows the structure of the FIDCCA_Ext field.

10 bits	1 bit	1 bit	1 bit	2 bits	1 bit	2 bits	6 bits
b_{23} b_{14} IMW	b_{13} Ext. flag	b_{12} Rp	b_{11} Parity flag	b_{10} b_9 Scrambling mode	b_8 Update ECM	b_7 b_6 Transport flags	b_5 b_0 ECM Identifier

Figure 16: Coding of the Fast Information Data Channel Conditional Access - Extended field

The definition of the parameters contained in the first two bytes are the same as for FIDCCA (see clause 4.2.4.1). The remaining parameters are defined as follows:

Transport flags = "00":

- In this case, the ECMs and the EMMs shall be sent in the FIG type 6.
- **ECM Identifier:** this 6-bit field shall identify the structure containing the ECM message in FIG type 6, using the FIC_ECMId (see clause 4.2.2). The value "000000" is not allowed (because it is reserved for the EMMs).

Transport flags: = "01":

In this case, the ECMs shall be sent in the FIG type 6 and the EMMs shall be sent in sub-channel 63.

- **ECM Identifier:** this 6-bit field shall identify the structure containing the ECM message in the FIG type 6, using the FIC_ECMId (see clause 4.2.2). The value "000000" is not allowed.

Transport flags: = "10":

In this case, both the ECMs and the EMMs shall be sent in sub-channel 63.

- **ECM Identifier:** this 6-bit field shall identify the structure containing the ECM message, using the Pk_ECMId (see clause 4.2.2). The value "000000" is not allowed (because it is reserved for the EMMs).

Transport flags = "11": this case shall be reserved for future use of the ECM Identifier field.

4.3 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 clause describes the coding of ECMs and EMMs and their transport mechanisms.

4.3.1 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.

4.3.1.1 ECM and EMM coding

The ECM identifier (ECMId) shall be used to point to a specific ECM. The ECM and the EMM are coded as shown in figure 17.

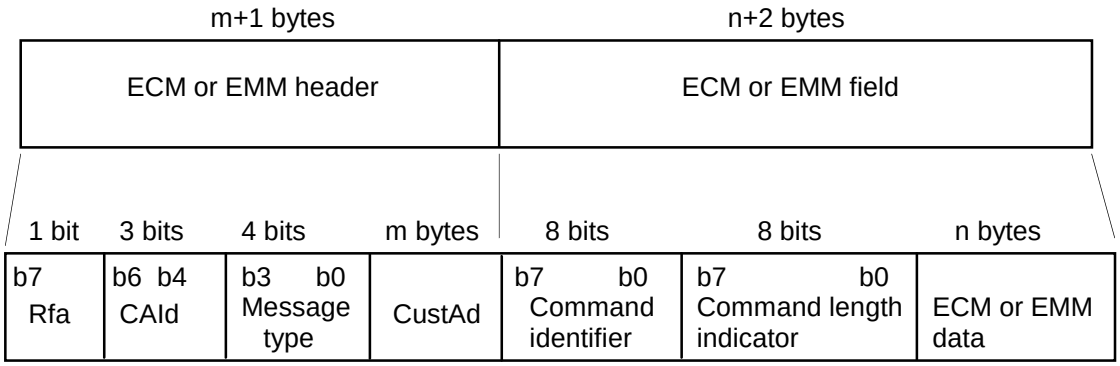


Figure 17: ECM or EMM coding field

The following definitions apply:

ECM or EMM header:

- **Rfa:** this bit shall be reserved for future additions. The bit shall be set to zero until it is defined.
- **CAId:** see [1], clauses 6.3.1 and 4.2.1.
- **Message type** (type of message): this 4-bit field shall specify the type of message, as follows (the remaining types are reserved for future use of the message type field:

  b_3 - b_0

  0 0 0 0 : ECM;

  0 0 0 1 : reserved for specific ECM;

  0 0 1 0 : reserved for specific ECM;

  0 0 1 1 : reserved for specific ECM;

  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).

- **CustAd** (Customer Address): this parameter is optional for ECMs but mandatory for all EMMs, except EMM-G. The length of the Customer Address field is defined for the following applications:

  UA (Unique Address): 40 bits (for ECMs and EMM-U);

  SA (Shared Address): 24 bits (for ECMs and EMM-S);

  CCA (Collective Code Address): 16 bits (for ECMs and EMM-C).

ECM or EMM field:

- **Command Identifier:** this 8-bit field shall specify the toggle bit and the crypto-algorithm type (see clause 4.3.1.2).
- **Command Length Indicator:** this 8-bit field (expressed as an unsigned binary number) shall indicate the number of bytes in the ECM or EMM data field.
- **ECM (Entitlement Checking Messages) data:** this field shall contain the complete ECM information.
- **EMM (Entitlement Management Messages) data:** this field shall contain the complete EMM Information.

4.3.1.2 Command Identifier coding

The Command Identifier describes the toggle bit and the type of cryptographic algorithm used for decryption. It shall be included in all EMMs and ECMs. Its structure is shown in figure 18.

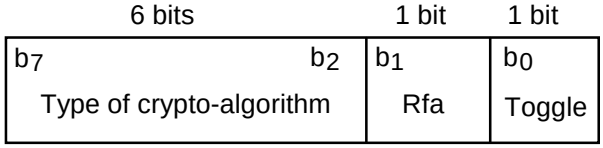


Figure 18: Coding of the Command Identifier field

The following definitions apply:

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 "0" until it is defined.

Toggle: this 1-bit flag 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.

4.3.2 Transport of ECM and EMM

The following clauses describe how the ECMs and EMMs are transported in the MSC (sub-channel 63), in the FIC or in the same sub-channel as the service component.

4.3.2.1 Transport in the MSC

The ECM or EMM shall be carried in the MSC data group as shown in figure 19 (see also [1], figure 9).

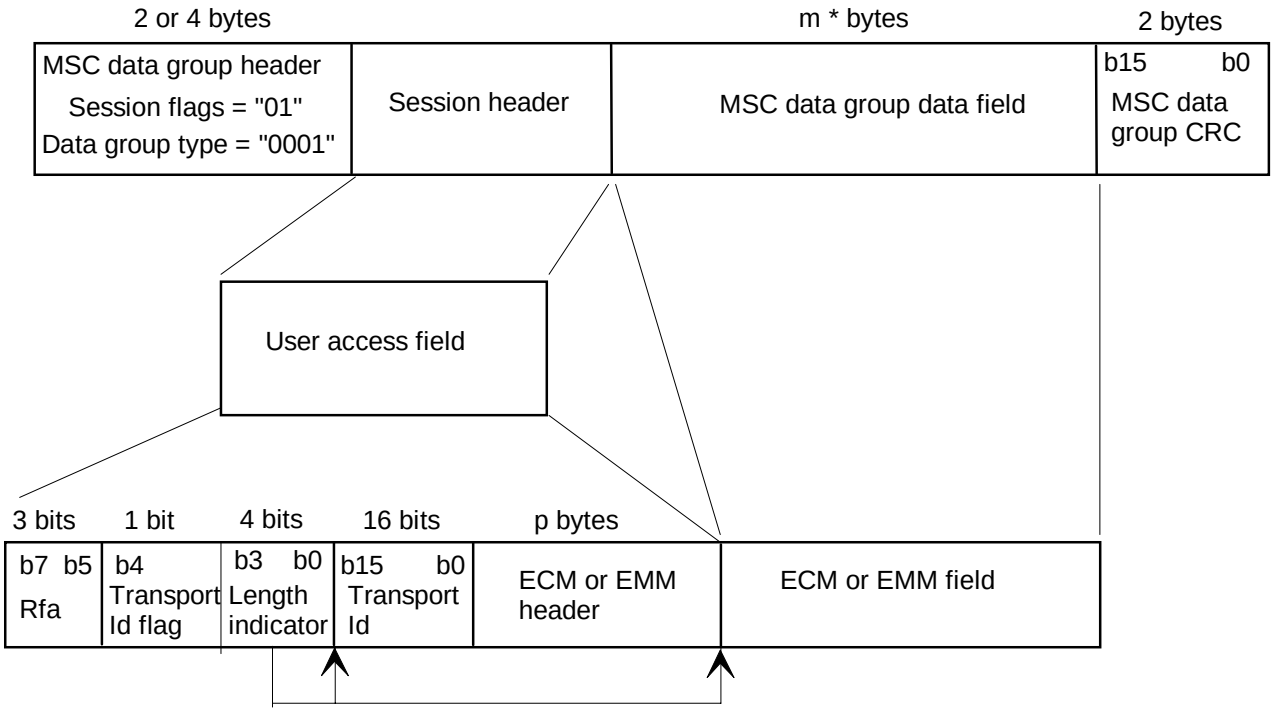


Figure 19: ECM or EMM transport using MSC data group

The following definitions apply:

MSC data group header: see [1], clause 5.3.3.1. The session flags (segment flag and user access flag) shall be set to indicate no segment field present but the user access field present ("01"). The data group type shall be set to "CA messages" ("0001");

Session header: the Segment field is absent, the user access field is present - see [1], clause 5.3.3.2;

- **Rfa:** this 3-bit field is reserved for future additions. The bits shall be set to zero until they are defined.
- **Transport Id flag, Transport Id:** see [1], clause 5.3.3.2.
- **Length indicator:** this 4-bit field shall indicate the length in bytes of the ECM (or EMM) header and the Transport Id field. It is coded as an unsigned binary number in the range 0 to 15.
- **ECM or EMM header:** see clause 4.3.1.1.

MSC data group data field: see [1], clause 5.3.3.3;

- **ECM or EMM field:** see clause 4.3.1.1.

MSC data group CRC: see [1], clause 5.3.3.4;

At the network level, each MSC data group containing one ECM or one EMM shall be carried in one or several packets having the same address (see [1], clause 5.3.2).

The ECMs of each access controlled service component shall be carried in packets with addresses described in table 4. The EMMs of all the access controlled service components shall be carried in packets having the same address.

Table 4: Packet address allocated for ECMs and EMMs

Type of message	Packet address (10 bits)	
	b9 b6	**b5 b0**
ECM	0 0 0 1	Pk_ECMId
EMM	0 0 0 1	0 0 0 0 0 0

4.3.2.2 Transport in the FIC

The FIG type 6 is used to send the control and management information about a scrambled service component. This information is referred to as CA messages. The structure of the FIG type 6 data field is shown in figure 20.

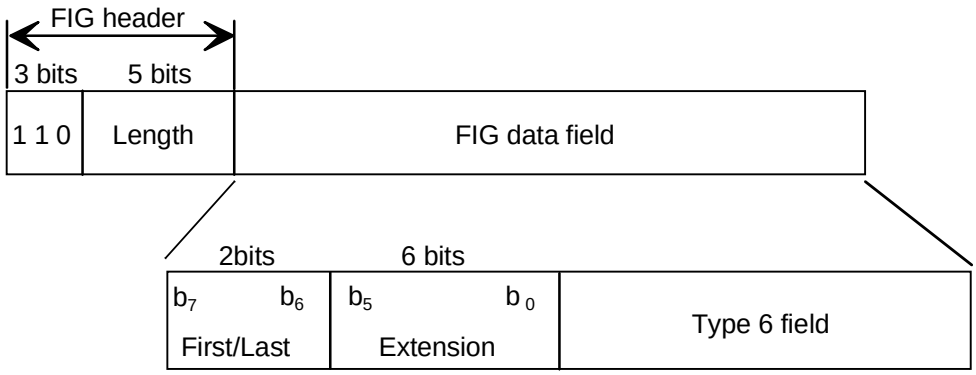


Figure 20: Structure of the FIG type 6 data field

The following definitions apply:

First/Last: this 2-bit field shall indicate how CA messages are managed if they have to be split into more than one FIG type 6 field. The flags are set according to table 5.

Table 5: First/Last flags for FIG type 6 data fields

First b_7	Last b_6	The FIG type 6 data field is the:
0	0	intermediate FIG type 6 data field of a series
0	1	last FIG type 6 data field of a series
1	0	first FIG type 6 data field of a series
1	1	one and only one FIG type 6 data field

Extension: this 6-bit field, expressed as an unsigned binary number, shall identify one of 64 interpretations of the FIG type 6 field. Those extensions, which are not defined, are reserved for future use.

The ECMs and the EMMs shall be carried in FIG type 6 as shown in figure 21 (see also [1], figure 7).

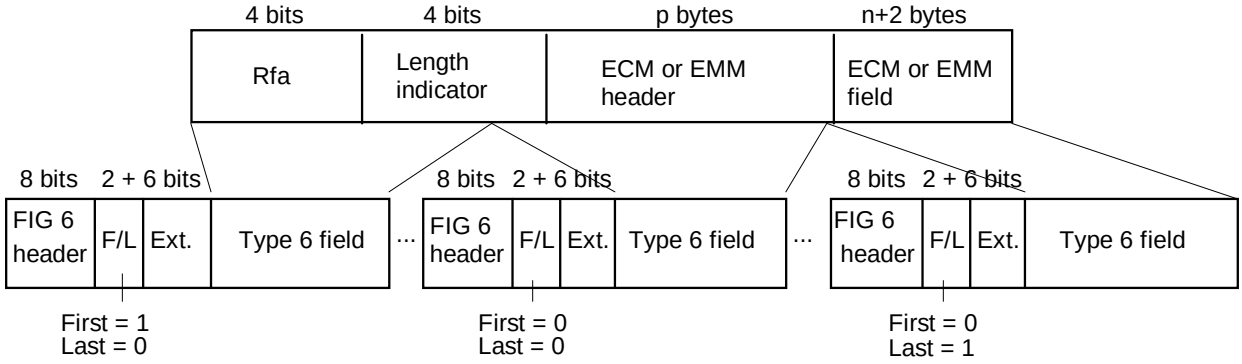


Figure 21: ECM or EMM transport using FIG type 6

The following definitions apply:

Rfa: this 4-bit field is reserved for future additions. The bits shall be set to zero until they are defined.

Length indicator: this 4-bit field shall indicate the length in bytes of the ECM (or EMM) header.

ECM header, EMM header: see clause 4.3.1.1.

ECM or EMM field: (see clause 4.3.1.1 and figure 17).

F/L (First/Last): see table 5.

Ext. (Extension): except for the value "000000", this 6-bit field shall contain the FIC_ECMId (FIC_ECM Identifier) which identifies the ECM or the portion of the ECM data carried in the Type 6 field. The FIC_ECMId cannot take the value "000000". The value "000000" indicates that the Type 6 field contains EMM data.

4.3.2.3 Transport together with service component

The ECMs and EMMs shall be coded in the same way as that described for sub-channel 63 in clause 4.3.2.1.

At the network level, each MSC 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.

History

Document history		
V1.1.1	January 2005	Publication