

Access control system for the MAC/packet family: EUROCRYPT

The European Standard EN 50094 : 1992 has the status of a
British Standard

ICS 33.160.20

Cooperating organizations

The European Committee for Electrotechnical Standardization (CENELEC), under whose supervision this European Standard was prepared, comprises the national committees of the following countries:

Austria	Italy
Belgium	Luxembourg
Denmark	Netherlands
Finland	Norway
France	Portugal
Germany	Spain
Greece	Sweden
Iceland	Switzerland
Ireland	United Kingdom

This British Standard, having been prepared under the direction of the Electronic Equipment Standards Policy Committee, was published under the authority of the Standards Board and comes into effect on 15 October 1993

© BSI 1997

The following BSI references relate to the work on this standard:
Committee reference EEL/25
Draft for comment 91/31136 DC

ISBN 0 580 22546 1

Amendments issued since publication

Amd. No.	Date	Text affected
9667	December 1997	Indicated by a sideline in the margin

Summary of pages

The following table identifies the current issue of each page. Issue 1 indicates that a page has been introduced for the first time by amendment. Subsequent issue numbers indicate an updated page. Vertical sidelining on replacement pages indicates the most recent changes (amendment, addition, deletion).

Page	Issue	Page	Issue
Front cover	2	2	2
Inside front cover	2	3 to 195	original
a	1	196	2
b	blank	197 and 198	2
i	2	199 to 213	1
ii	blank	214	blank
EN title page	2	Inside back cover	original
		Back cover	2

Contents

	Page
Cooperating organizations	Inside front cover
National foreword	i
Foreword	2
Text of EN 50094	3
National annex NA (informative)	Inside back cover

National foreword

This British Standard has been prepared by Technical Committee EPL/100 (formerly EEL/25) and is the English language version of EN 50094 : 1992 *Access control system for the MAC/packet family: EUROCRYPT* including amendment A1 : 1995, published by the European Committee for Electrotechnical Standardization (CENELEC).

For the purposes of this British Standard, appendices 1, 2, 3, 4 and annex 5 are informative.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

UDC 621.396 : 534.86 : 621.397

Descriptors: Radiocommunications, television broadcasting, sound broadcasting, telecasting, user network access, specifications

English version

Access control system for the MAC/packet family: EUROCRYPT

(includes amendment A1 : 1995)

Système d'accès conditionnel pour la famille
MAC/paquet: EUROCRYPT
(inclut l'amendement A1 : 1995)

Zugriffskontrollsystem für die
MAC/Paket-Familie: EUROCRYPT
(enthält Änderung A1 : 1995)

This European Standard was approved by CENELEC on 9 December 1992. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B-1050 Brussels

Foreword

At the request of CENELEC Technical Committee TC 106, MAC receiving equipment, the text of this European Standard was submitted to the CENELEC members for formal vote in August 1992 and was approved by CENELEC on 9 December 1992 as EN 50094.

The following dates were fixed:

- latest date of publication of an identical national standard (dop) 1993-06-30
- latest date of withdrawal of conflicting national standards (dow) 1993-06-30

The EUROCRYPT system, as described in this standard, is subject to patent rights.

In accordance with CEN/CENELEC Memorandum 8 on Standardization and Intellectual Property Rights (IPR), a statement from the patent holders of the EUROCRYPT system was obtained, confirming their willingness to negotiate licences under the following conditions:

- no exclusivity;
- they apply for the conditional access system related to the MAC/Packet family called 'EUROCRYPT';
- the territory comprises the CEC, EFTA and other countries which receive the MAC signal from a European satellite;
- the conditions are to be reasonable and non-discriminatory (the term 'reasonable' will be interpreted by referring to the customs in the electronic large users domain, the term 'non discriminatory' refers to licensing conditions not depending on the identity or the nationality of the licensee).

The following patent holders subscribed to the above conditions:

BULL CP8
CANAL+
FRANCE TELECOM
GEMPLUS CARD INTERNATIONAL
GIE MAC PACKET
INNOVATRON
ITT COMPOSANTS ELECTROMECHANIQUES
MATRA COMMUNICATION
NOKIA
PHILIPS INTERNATIONAL B.V.
SCHLUMBERGER INDUSTRIES
SGS-THOMSON MICROELECTRONICS
TELEDIFFUSION DE FRANCE
THOMSON CONSUMER ELECTRONICS

Foreword to amendment A1

This amendment was prepared by the Technical Committee CENELEC TC 106, Broadcast receiving equipment.

The text of the draft was submitted to the Unique Acceptance Procedure as prAA and prAB and was approved by CENELEC as amendment A1 to EN 50094 : 1992 on 1994-12-06.

The following dates were fixed:

- latest date by which the amendment has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 1995-12-01
- latest date by which the national standards conflicting with the amendment have to be withdrawn (dow) 1995-12-01

CONTENTS

1. SUBJECT	7
2. GENERAL DESCRIPTION OF THE ACCESS CONTROL SYSTEM	8
2.1 The scrambling and encryption systems	8
2.2 Initialising and updating service keys (management or operation)	11
2.3 Functionalities	11
3. SCRAMBLING SOUND, DATA AND PICTURE	13
3.1 Introduction	13
3.2 Description of the sound and data scrambling processes	13
3.3 Generating descrambling sequences	13
3.4 Synchronising descrambling sequences	14
4. SIGNALS CROSSING THE ACCESS CONTROL INTERFACE	23
4.1 Receiver-ACS interface	23
4.1.1 Configuring the receiver-ACS interface	23
4.1.2 Signals received by the ACS	23
4.1.3 Signals from the ACS	26
4.1.3.1 Locally-generated control messages	26
4.1.3.2 Locally-generated messages for display	26
4.2 Service identification and relation to control words	27
4.3 Generation and assignment of control words	29
4.3.1 Generation of control words	29
4.3.2 Assignment and synchronisation of control words	29
5. GENERAL DESCRIPTION OF ENTITLEMENT MANAGEMENT MESSAGES (EMM)	30
5.1 Message formats	30
5.2 Customer addresses	33
5.3 Command identifier CI	36
5.4 Length indicator CLI	37
5.5 Parameter identifier PI	37
5.5.1 List of parameters available in EMM messages	37
5.5.2 Grouping of parameters in the EMM	41
5.5.3 Parameter sequencing rules in the EMM-U and EMMG	42
5.5.4 Software data SOFT	43
5.5.5 Programme provider identification PPID	43
5.5.6 Random number (for address field descrambling) RND-ADF	43
5.5.7 Random number (for confidential data descrambling) RND-CONF	44
5.5.8 Programme provider or issuer authentication	44
5.5.9 Address field ADF	44
5.5.10 Control CTRL	45
5.5.11 Identification of data to update IDUP	47
5.5.12 Descriptor DESCR	47

5.5.13 General purpose data FAC	48
5.5.14 Unique address UA	49
5.5.15 Programme provider user address PPUA	49
5.5.16 Group customer address GCA	49
5.5.17 LABEL parameter	50
5.5.18 DATES + Theme/Level TH/LE	50
5.5.19 DATES + List of classes CUSTWD	52
5.5.20 Initial and final programme numbers INUMB + FNUMB	53
5.5.21 DATE + CREDIT	54
5.5.22 DATE + Total amount TOTAM	55
5.5.23 DATE + Authorised overdraft OVER	55
5.5.24 SURVEY	57
5.5.25 DATES	57
5.5.26 Receiver modem control parameters	57
5.5.27 Modem activation coordinates MOD	58
5.5.28 Wakeup coordinates WAK	60
5.5.29 Authentication control parameters	61
5.5.30 Individual messages INDMES	61
5.5.31 Personal identification number PIN (Parental code)	62
5.5.32 Secret key CLE	62
5.5.33 HASH signature	63
5.5.34 Group address GA	63
5.5.35 Teletext service SEI-TXT	64
5.5.36 Video signal replacement TTP1	64
5.5.37 TV sound replacement RCI-R1	65
5.5.38 Additional service replacement RCI-02, RCI-R2	65
5.5.39 Teletext page for fingerprinting TPP2	66
5.5.40 Fingerprinting control FCTRL	66
5.6 Fixed format messages (F = 0 in the CI parameter)	67
6. UNIQUE CUSTOMER ENTITLEMENT MANAGEMENT MESSAGES (EMM-U)	68
6.1 Data format	68
6.1.1 Command identifier CI	68
6.1.2 Command length indicator CLI	68
6.2 EMM-U messages used for over-the-air addressing	68
6.2.1 List of parameters available in EMM-U messages	69
6.2.2 Description of parameters	71
6.2.3 Illustration of EMM-U messages with examples	72
6.2.3.1 Initial connection of a customer to the programme provider management centre	72
6.2.3.1 Individual entitlements	72
6.2.3.2 Invalidating or deleting entitlements	75
7. MESSAGES FOR THE ENTIRE AUDIENCE (EMM-G)	76
7.1 Introduction	76
7.2 Data format	76
7.2.1 Command identifier CI	76
7.2.2 Command length indicator CLI	76
7.3 EMM-G messages used for over-the-air addressing	76
7.3.1 List of parameters available in EMM-G messages	77
7.3.2 Use of EMM-G messages	79
7.3.2.1 Free initial entitlement or entitlement common to the entire audience	79
7.3.2.2 Shared entitlement	79

7.3.3 Description of parameters	80
7.3.3.1 Free initial entitlement or entitlement common to the entire audience	80
7.3.3.2 Shared entitlement	80
7.3.4 Illustration of EMM-G messages with examples	81
7.3.4.1 Free initial entitlement or entitlement common to the entire audience	81
7.3.4.2 Shared entitlements	82
8. MESSAGES FOR SHARED GROUPS (EMM-S).....	83
8.1 Introduction	83
8.2 Data format	83
8.2.1 Command identifier CI	83
8.2.2 Command length indicator CLI	84
8.3 EMM-S messages used for over-air addressing	84
8.3.1 List of parameters available in EMM-S messages	84
8.3.1.1 Fixed format EMM-S	84
8.3.1.2 Variable format EMM-S	84
8.3.2 Description of parameters	84
8.3.2.1 Fixed format EMM-S	84
8.3.2.2 Variable format EMM-S	84
8.3.3 Illustration of EMM-S messages with examples	85
9. COLLECTIVE ENTITLEMENT MANAGEMENT MESSAGES (EMM-C).....	87
9.1 Data format	87
9.1.1 Command identifier CI	87
9.1.2 Command length indicator CLI	87
9.2 EMM-C messages for over-air addressing	87
9.2.1 List of parameters available in EMM-C messages	88
9.2.2 Use of EMM-C messages	88
9.2.3 Description of parameters	89
9.2.4 Illustration of EMM-C messages with examples	89
10. DESCRIPTION OF ENTITLEMENT CONTROL MESSAGES (ECM)	90
10.1 Message format	90
10.2 Command identifier CI	92
10.3 Command length indicator CLI	92
10.4 Parameter identifier PI	92
10.4.1 List of parameters available in ECM messages	93
10.4.2 Grouping of parameters in the ECM	94
10.4.3 Parameter sequencing rules in the ECM	94
10.4.4 Software data SOFT	95
10.4.5 Programme provider identifier PPID	95
10.4.6 Global group address GGA	96
10.4.7 Control CTRL	98
10.4.8 Broadcast date CDATE + Theme/Level THEME/LEVEL	99
10.4.9 Broadcast date CDATE + Programme class LINK	100
10.4.10 Programme number PNUMB	100
10.4.11 Programme number PNUMB and Programme cost PPV/P	101
10.4.12 Programme number PNUMB + Cost per time unit PPV/T	101
10.4.13 Even control word cryptogram ECW	102
10.4.14 Odd control word cryptogram OCW	102
10.4.15 Odd and even control words cryptograms ECW/OCW	103
10.4.16 HASH signature	103

10.5	Illustration of ECM messages with examples	104
10.5.1	Subscription per theme/level	104
10.5.2	Subscription per class with blackout enabled	104
10.5.3	Impulse pay-per-view per programme	105
10.5.4	ECM message for different access conditions	105
11.	DETAILS CONCERNING THE IMPLEMENTATION OF THE ACCESS CONTROL PROCEDURES DESCRIBED IN THE SPECIFICATION	107
11.1	Part 1	107
11.1.1	Introduction	107
11.1.2	Section 5.3 - Static data frame (SDF)	107
11.1.3	Section 5.3 - Repeated data frame (RDF)	108
11.2	Part 2	109
11.2.1	Section 7 - Enlarged format pictures	109
11.3	Part 5	109
11.3.1	Introduction	109
11.3.2	Section 2.3 - Description of service components	109
11.3.3	Section 3.1 - Instructions and parameters	111
11.3.4	Table 1	111
Appendix 1 :	Coding examples of the service identification channel with the PGI parameter group identifier	112
12.	SWITCHING TIMING DIAGRAMS	107
12.1	Introduction	114
12.2	Content of switching timing diagrams	114
12.3	Create a component in controlled access mode	115
12.4	Switch a component to controlled access mode	116
12.5	Change the access condition for a component	117
12.6	Switch a component from controlled access mode to clear or free access mode	118
12.7	Reorganize component and access conditions	119
12.7.1	Regroup 2 components with different access conditions on the access condition of the first component	120
12.7.2	Separate 2 components, one of them preserving the initial access condition	121
12.7.3	Regroup 2 components with different access conditions on a new access condition	122
12.7.4	Separate 2 components, with change of access condition for both components	123
GLOSSARY		124
REFERENCE		130
APPENDIX 1 :	External specifications of the PC2 smart card	131
APPENDIX 2 :	Operating regulations for the broadcasting of D2-MAC/packet services	178
APPENDIX 3 :	Recommandations for the development of a EUROCRYPT D2-MAC/packet receiver	184
APPENDIX 4 :	Specifications of the PC-EUROCRYPT cards	192

1. SUBJECT

This document describes an access control system designated EUROCRYPT which can be applied to the systems in the MAC/packet family. The access control system is responsible for ensuring that television, radio programmes, or data services are accessible only to those customers who have satisfied clearly specified conditions, usually payment related. For its application to the D2-MAC/packet system it refers to the document Ref. 1.

In Part 6 of the document (Ref. 1), sections 2 to 5 contain a general description of the access control system, without including the internal format of the data signals which depend on the system being used. For ease of understanding, sections 2 to 4 of this document review the information contained in Part 6 of the document (Ref. 1), and sections 5 to 10 supplement this information with details of the components specific to the EUROCRYPT access control system specification. The application of these components in relation to a sample implementation (the PC2 smart card) is used in the specification by way of illustration.

Section 2 describes the basic principles of the access control system ; it also describes the functions of the system. The access control system may, schematically, be divided into two part : the **scrambling system** and the **encryption system**. The scrambling system mainly involves the programme signals whereas the encryption system processes the keys and data signals required to access the programme.

Section 3 contains the specifications of the sound, data and video scrambling procedure. Section 4 describes the interface used to transmit security data and control signals to the receiver, the format and addresses of the entitlement management messages, and the service identifiers.

Section 5 gives a general description of the entitlement management messages (EMM) and sections 6 to 9 respectively specify the format of the entitlement messages for «unique», «global», «shared», and «collective» audiences. Section 10 specifies the format of the entitlement control messages (ECM).

Section 11 details the setting up of the access control procedures described in the specification (Ref. 1) and introduces a new functionality: called «panning».

Section 12 details the basic timing diagrams that apply during switchings.

By way of example, appendix 1 contains the external specifications of an entitlement medium, the PC2 smart card, which represents a sample implementation of an entitlement storage device conforming to the specification. All entitlement storage devices designed to use the access methods described in the specification are generically know as PC EUROCRYPT.

Appendix 2 contains the operating regulations for the broadcasting of services using the D2-MAC/packet specification and the EUROCRYPT access control system.

Appendix 3 describes the recommendations for the development of a D2-MAC/packet receiver in accordance with the D2-MAC/packet specification described in document Ref. 1, using the EUROCRYPT access control system and referring to the operating regulations described in appendix 2.

Appendix 4 describes the PC-EUROCRYPT cards specifications and the way of using them with a D2-MAC/packet receiver such as described in appendix 2.

2. GENERAL DESCRIPTION OF THE ACCESS CONTROL SYSTEM

2.1 The scrambling and encryption systems

Figure 2.1 provides the functional block diagram of the access control system. Some of the functions (e.g. demultiplexing) are omitted in the interest of clarity, and *Figure 2.1* gives only a global representation of the system. The **source component** of *Figure 2.1* might be a video picture, a sound or a data signal for which the programme provider wishes to restrict access. A scrambler renders the component unintelligible, using a scrambling sequence derived from a constantly changing pseudo-random binary sequence generator. In the receiver, the reverse process is applied by the **descrambling sequence generator**, the **descrambling sequence** (the process of reversing the scrambling sequence) and the **descrambler**.

The scrambling sequence generator is a pseudo-random binary sequence generator with a very long cycle time. Its output is made unpredictable by the use of a **control word** and a **cyclic, 8-bit frame counter FCNT**, which has a cycle time of about ten seconds (25 frames/second). The descrambling system must be synchronised on the source and on the receiver. The scrambled source component, the frame counter and the synchronising signal are derived from signals transmitted in the same channel.

The service operator can choose to send the signal **unscrambled** (in clear) or **scrambled**. If scrambled, the programme provider can use a **local control word**, which is constant and stored in the receiver, or a **regenerated control word** originating from the encryption system. If a regenerated control word is used, the customer's receiver will not be able to generate the correct control word internally unless the appropriate service access conditions have been satisfied.

When the local control word is not used, the control word is supplied by the security processor incorporated in the access control system (ACS).

In order to do so, the control word (CW) is generated at the point of transmission and sent encrypted to the receiver using the operation key SK (cf. *Figure 2.1*). The control word changes every 256 TV frames (i.e. approximately every 10 seconds), but its cryptogram is transmitted at approximately 0.5-second intervals to allow rapid descrambling for receivers which are tuned to the channel. The cryptogram SK (CW) is sent in an entitlement control message, ECM, which is transmitted in the same channel as the service itself. The message also contains data concerning the use of the control word.

New control words are loaded into the descrambler at approximately 10-second intervals, provided that the operation key is available in the receiver and authorised to generate the control word.

The purpose of the access control system (ACS), which may be internal to the receiver or detachable, is to decide whether or not it can compute the control word. It is provided with a security processor which has both storage memory and computation capabilities. The security processor stores the secret keys and associated entitlements. Only non-secret data can be read in the security processor. Secret data remains internal to the processor. The entitlements describe the parameters of the customer in a variety of forms : validity period, consumable units, geographical area, and so on. The processor checks these parameters before computing any control word with an operation key.

These parameters are management parameters which can be loaded into the ACS by entitlement management messages EMM comprising data transmitted in clear or scrambled, and cryptograms. These messages constitute the over-air addressing service and may be unique (specific to a particular customer) or shared (specific to a group of customers).

Before writing any parameter into the ACS, the processor checks the integrity of the message, that the message is correctly addressed to it, that it has not already been processed and that the authority sending it is one of the authorities entitled to enter data into the ACS. This process is controlled by a management key, PDK (which may in certain circumstances be an operation key) belonging to the programme provider.

The management and, when appropriate, operation keys are loaded into the ACS under the control of a higher level key : the issuer key. This key can be used to invalidate existing service keys (management or operation) if the service is not locked, or load new keys, as required, to enable new operators to access the ACS of a given customer. The system can be used to modify the group of operators with access to a receiver. Existing service keys can be modified using the issuer key or a management key of the service itself.

Shared EMM messages are used to reduce the entitlement broadcasting time. These messages must be broadcast at regular intervals to ensure that the message has been received at least once by the entire audience. Given that groups can be made up of 256 customers, millions of customers can be addressed in less than a minute.

All of these items of information and parameters, whether in clear or secret, are associated with a particular programme provider and stored under the operator's service identifier. The EMM can be sent independently of the physical RF channel because the programme provider identifier is independent of the transmission channel.

Entitlement management messages can also be used to distribute messages to individuals or to groups of customers. These same messages can equally be used to configure replacement functions for specified groups or to submit special management messages. A replacement configuration may be, for example, a special teletext page to replace the video signal in case of a blackout affecting a specific group of customers. A replacement page can also be used in conjunction with fingerprinting, that is, the addition of a given customer's signature to predetermined frames of the video signal. Replacement of other services (e.g. radio, teletext, etc.) is also possible.

And finally, individual or shared entitlement management messages can also be used to transmit specific configuration data to the customer's receiver (modem telephone number, date and time of modem call, remote controlled emergency call, etc.).

ECM =	entitlement control message
EMM =	entitlement management message
CW =	control word
SK =	operation key
FCNT =	frame counter (8-bit)
CAFCNT =	256-frame counter (20-bit)
E =	customer entitlement
IK =	issuer key
UA =	unique address
P =	current programme parameter
SK (P, CW) =	CW encrypted by SK
PDK =	service management key
PDK (E, UA or PPUA) =	E encrypted with PDK
IK (SK or PDK, UA or PPUA) or PDK (SK or PDK, UA or PPUA) =	SK or PDK encrypted with IK or PDK ; PDK can be used only for modifying keys associated with the service

Legend of Figure 2.1

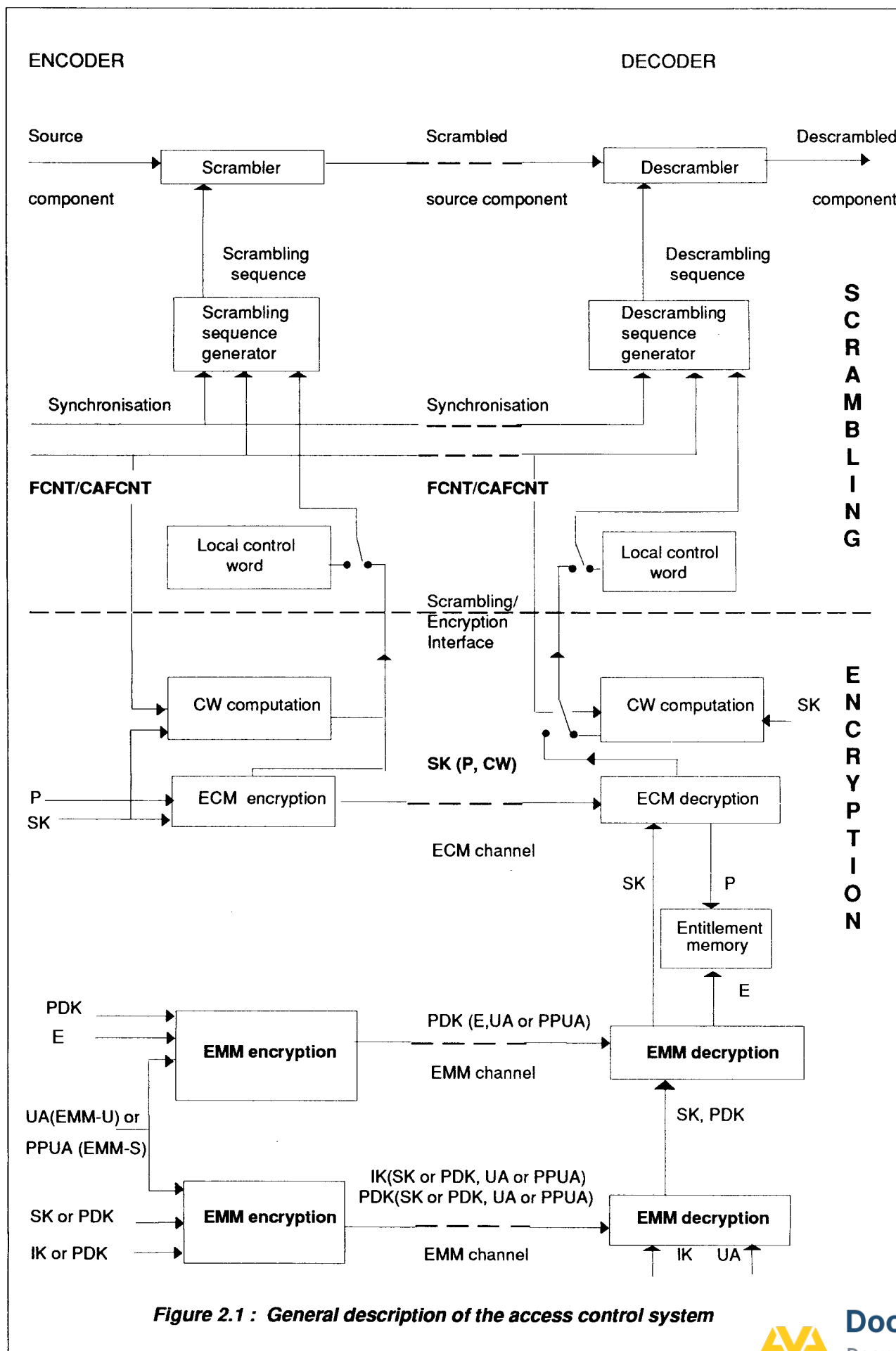


Figure 2.1 : General description of the access control system

2.2 Initialising and updating service keys (management or operation)

When first put into service, the ACS is programmed only with a unique address and the issuer key. As described above, only the holder of the issuer key can load the first management key for any service, corresponding to a service identifier.

A operation key can be entered or an operation or management key modified by any appropriate service management key or by an issuer key. The facility for entering or modifying service keys by the issuer can however be parametered ; a programme provider may ask for his service to be locked out to prevent any action on the part of the issuer on his keys once the first key has been entered.

When the keys have been entered, any authority receiving a service key together with the corresponding service identifier can load entitlements into those ACS which have received the same key. This authority may, if it wishes, enter a special address in the ACS reserved for this particular service. The purpose of this is to ensure maximum efficiency in the use of shared messages.

The role of the issuer holding the issuer key is to distribute service keys to the operators and to load them into the ACS. The issuer can also invalidate service keys. This means that he may be considered as a general service organiser, with his role kept to a minimum since most of the operations concerning the ACS are performed by the programme providers themselves, once the service management keys have been entered.

2.3 Functionalities

This specification describes five access control methods :

- Subscription per theme and level, whereby customers are allowed access to programmes for a period described by a beginning date and a finishing date. The subscription is also characterised by a level, specifying the highest level of programmes which can be accessed by the customer (each programme has a level reference), and a theme specifying the theme of the programmes which can be accessed (each programme also has a theme reference).
- Subscription per class, whereby customers are allowed access to programmes for a period defined by a beginning date and a finishing date. The period is also related to a defined list of classes of programmes ; for each class, the list specifies whether or not the customer is allowed access, each programme being referenced by a class.
- Pre-booked pay-per-view per programme, whereby customers are allowed access to one or more programme items, or to a set of programmes defined by an initial and a final programme number, each programme being referenced by its number.
- Impulse pay-per-view per programme, whereby customers are assigned a credit ; the credit is debited by the cost of the programmes as they are accessed. Each programme is identified by a programme number and a cost. This method is particularly suited for payment per programme because it provides feedback information concerning programmes purchased by customers.
- Impulse pay-per-view per time, whereby customers are also assigned a credit. This credit is debited on a time basis (price of the programme per time unit). Each programme is identified by a programme number. This method provides feedback information concerning programmes purchased by customers.

An additional parameter is introduced to supplement the access control system, covering copyright protection. Irrespective of the access method, each customer is assigned a group address associated with a service identifier. This parameter divides the customers into groups, so that, where appropriate, the programmer can blackout or select one or more groups by sending the corresponding signals. This parameter is assigned the highest level priority, and, where a customer belongs to a blacked-out group, he will not be allowed access to the programme irrespective of his own entitlements.

These access methods can be used in combination to define the conditions of access to the various components which constitute the programme. Such definition entails the continuous transmission of entitlement control messages (ECM) in the MAC/packet signal.

Local, customer-oriented, control of ACS is also possible by programming a maturity rating. Each programme broadcast within a service can be assigned a maturity rating which defines the minimum age required in order to watch the programme. Where a programme has a rating which is higher than that programmed by the customer, the parental, or PIN, code must then be submitted. The customer can also lock access to his ACS for impulse pay-per-view (per programme or time). Each purchase is then conditional on submission of the PIN code. Finally, if the ACS is locked from impulse pay-per-view or for a given maturity rating, the customer can store a number of programmes which will not be subject to this rule when they are received. This can be used for pre-programmed video recording or for selectively receiving programmes in the absence of the owner of the ACS.

For these various access methods, the customers are given an entitlement storage device containing one or more service keys. A service key can be used for a given period (in the subscription methods) or for a given number of programmes numbered consecutively (in the pre-booked pay-per-view method). In the impulse pay-per-view methods, a service key is valid up to a maximum cost. This validity can be renewed (for a further period, for a further set of consecutively numbered programmes, or for further credit) by sending entitlement management messages (EMM) intermittently in the MAC/packet signal. All entitlements are stored by the ACS and the same service key can be used for different access modes.

The entitlement storage device is managed by the access control system (ACS) connected to the receiver via a receiver-ACS interface (which may be a virtual interface if the ACS is buried in the receiver).

The entitlement management and control messages required for the various access methods described above are detailed in sections 5 to 10.

Available entitlements can be consulted locally by the customer through his receiver. This is done by reading the entitlements entered in the security processor. This means that the customer can check periods, credits, etc. which are available under each service. The exact type and format of the messages displayed in this case are left to the access control system so that the man/machine dialogue can be made as customer-friendly as possible and tailored to the type of system.

3. SCRAMBLING SOUND, DATA AND PICTURE

3.1 Introduction

Services for which no subscription or other type of payment is needed are considered to be in **free access mode**. In **controlled access mode**, sound, data and pictures are always scrambled ; they can also be scrambled in free access mode. For those free access services which are scrambled prior to broadcasting, the appropriate control word (the «local control word») needed to descramble the various components is available in the receiver (see Section 3.3).

In free access mode, the picture signal can be scrambled or not, as chosen by the service operator. The corresponding wave shapes are described in Part 2 of document Ref. 1.

The digital sound and data signals are first scrambled for access control purposes and then subjected to bit interleaving and transmission scrambling (in order to shape the signal spectrum). Section 3.2 describes the scrambling procedure for access control purposes.

3.2 Description of the sound and data scrambling process

To scramble sound and data, a pseudo-random binary sequence (PRBS) is added modulo 2 to the **useful data** of the sound or data service packets. This operation is added to the bit interleaving and transmission scrambling specified in sections 3.6 and 3.7 of Part 1 in document Ref. 1.

Note that :

- the sound encoding blocks are scrambled **after** being subjected to error protection ; this means that, in the receiver, error detection or correction takes place **after** descrambling.
- the packet headers, packet type bytes (PT), interpretation blocks (BI) and service identification data (SI) are not scrambled.

3.3 Generating descrambling sequences

Descrambling sequences are generated by a pseudo-random binary sequence (PRBS) system. The schematic block diagram in *Figure 3.1* shows the effective configuration for the main television service (picture and associated sound).

All services can be subject to scrambling, but in the case of free access scrambled mode, the control word is locally available in the receiver.

A 60-bit control word is required for descrambling. In free access scrambled mode, all the bits of this word are set to logic '1' and the control word is stored in the receiver. In controlled access mode, the 60-bit control words are provided from the access control system.

The schematic block diagram in *Figure 3.1* shows three PRBS generators. They are described in *Figures 3.2, 3.3 and 3.4*.

The PRBS system requires an 8-bit frame count ; the specification and location of this information on line 625 are given in section 5.4 of Part 1 in document Ref. 1 (FCNT code). As can be seen from *Figure 3.1*, the PRBS generator initialising words are generated by combining the control words and the 8-bit frame count FCNT. The PRBS generators are synchronised with the frame count as described in the next section.

3.4 Synchronising descrambling sequences

Take, for example, two consecutive frames F_n and F_{n+1} . During line 625, at the end of F_n , a new frame count value, FCNT, is received with the value n . This value n is combined with control words CW1 and CW2 (*Figure 3.1*) to create two new values IW1 and IW2 for the initialisation words which are loaded into PRBS generators 1 and 2 respectively. Notice, too, that the first 61 bits generated by the PRBS generator 1, once it has been loaded, are used by PRBS generator 3 to descramble the first packet received during frame F_{n+1} . Similarly, the first 16 bits generated by PRBS generator 2, once it has been loaded, are used to descramble line 1 of frame F_{n+1} .

Every 256 frames, the PRBS system receives a new control word for which the validity period

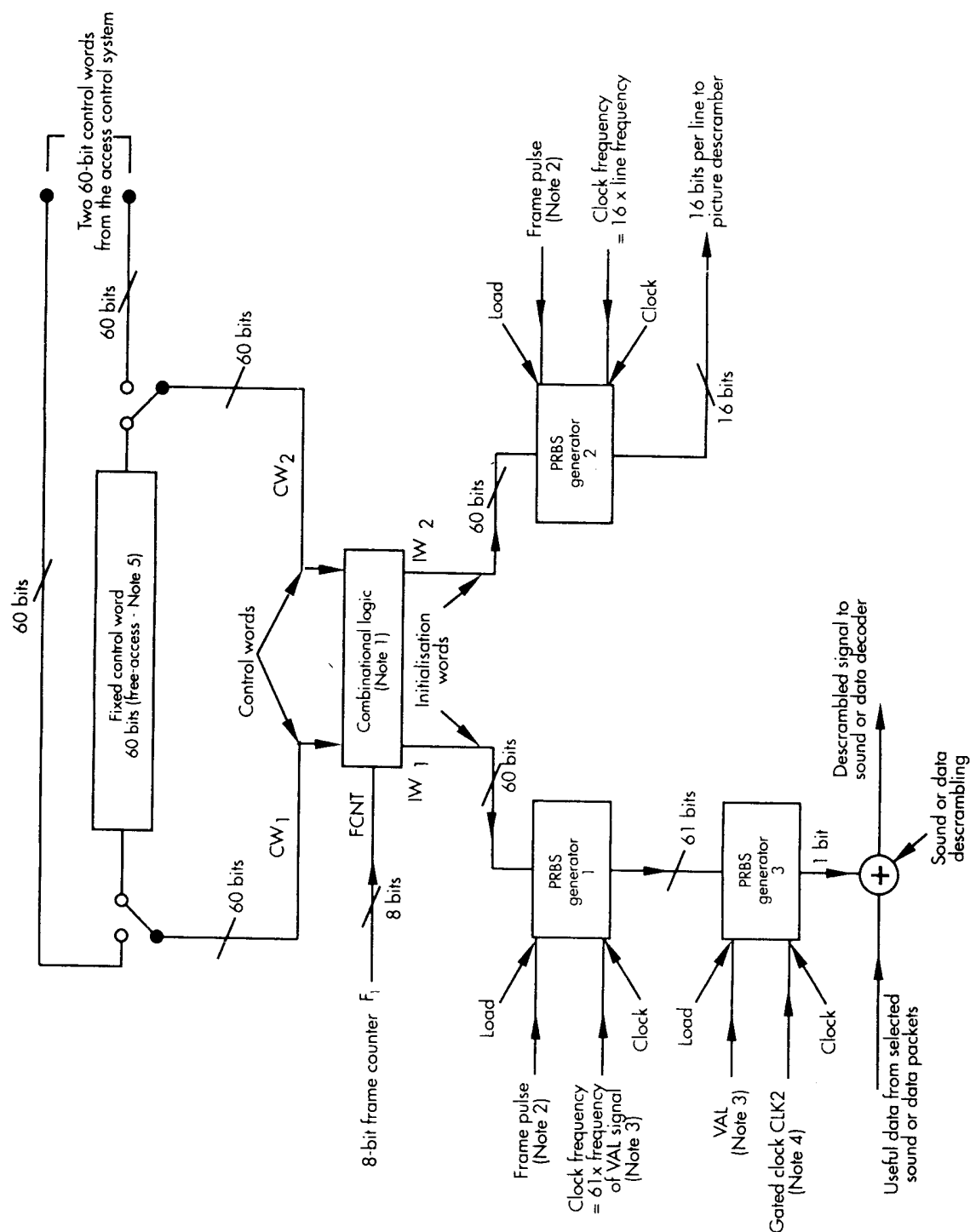


Figure 3.1 : PRBS system for access control system
(shown for picture and one sound component only)

Note 1

The combinational logic functions used to combine the two 60-bit control words CW_1 and CW_2 with the 8-bit frame count FCNT, to give the two 60-bit initialisation words IW_1 and IW_2 are the same in both cases and are defined as follows :

The 8-bit frame count (FCNT) is written as $F_0, F_1, \dots, F_7$.

The 60-bit control word (CW) is written as follows :

$C_0 C_1 \dots C_7$	$C_8 C_9 \dots C_{15} \dots C_{48} C_{49} \dots C_{55}$	$C_{56} C_{57} C_{58} C_{59}$
CW0	CW1 ... CW6	CW7

Then the 60-bit initialisation word (IW) is then written as follows :

$I_0 I_1 \dots I_7$	$I_8 I_9 \dots I_{15} \dots I_{48} I_{49} \dots I_{55}$	$I_{56} I_{57} I_{58} I_{59}$
IW0	IW1 ... IW6	IW7

IW can be deduced from CW and FCNT as follows :

$IW0 = CW0 \oplus FCNT$	$IW1 = CW1 \oplus \overline{FCNT}$	$IW2 = CW2 \oplus FCNT$	$IW3 = CW3 \oplus \overline{FCNT}$
$IW4 = CW4 \oplus FCNT$	$IW5 = CW5 \oplus \overline{FCNT}$	$IW6 = CW6 \oplus FCNT$	$IW7 = CW7 \oplus \overline{FCNT}$

It should be noted that :

- $\overline{FCNT}$ is the logical complement of FCNT (i.e. $FCNT \oplus \overline{FCNT} = 11111111$)
- When CW7 is transformed into IW7, only the least significant half byte of $\overline{FCNT}$ is used.

Note 2

The frame pulse occurs once per frame and its leading edge (rising edge) indicates the limits of the frame.

Note 3

VAL is a clock signal functioning at the same rate as the packets in the given sub-frame. The PRBS 1 generator is clocked 61 times between two validation signals VAL.

Note 4

CLK 2 is a gated clock such that PRBS 3 generator transmits 720 bits per packet and is synchronised by the useful data burst which arrives in the descrambling modulo-2 adder.

Note 5

In free access scrambled mode, all the bits in the control words are set to logic '1'.

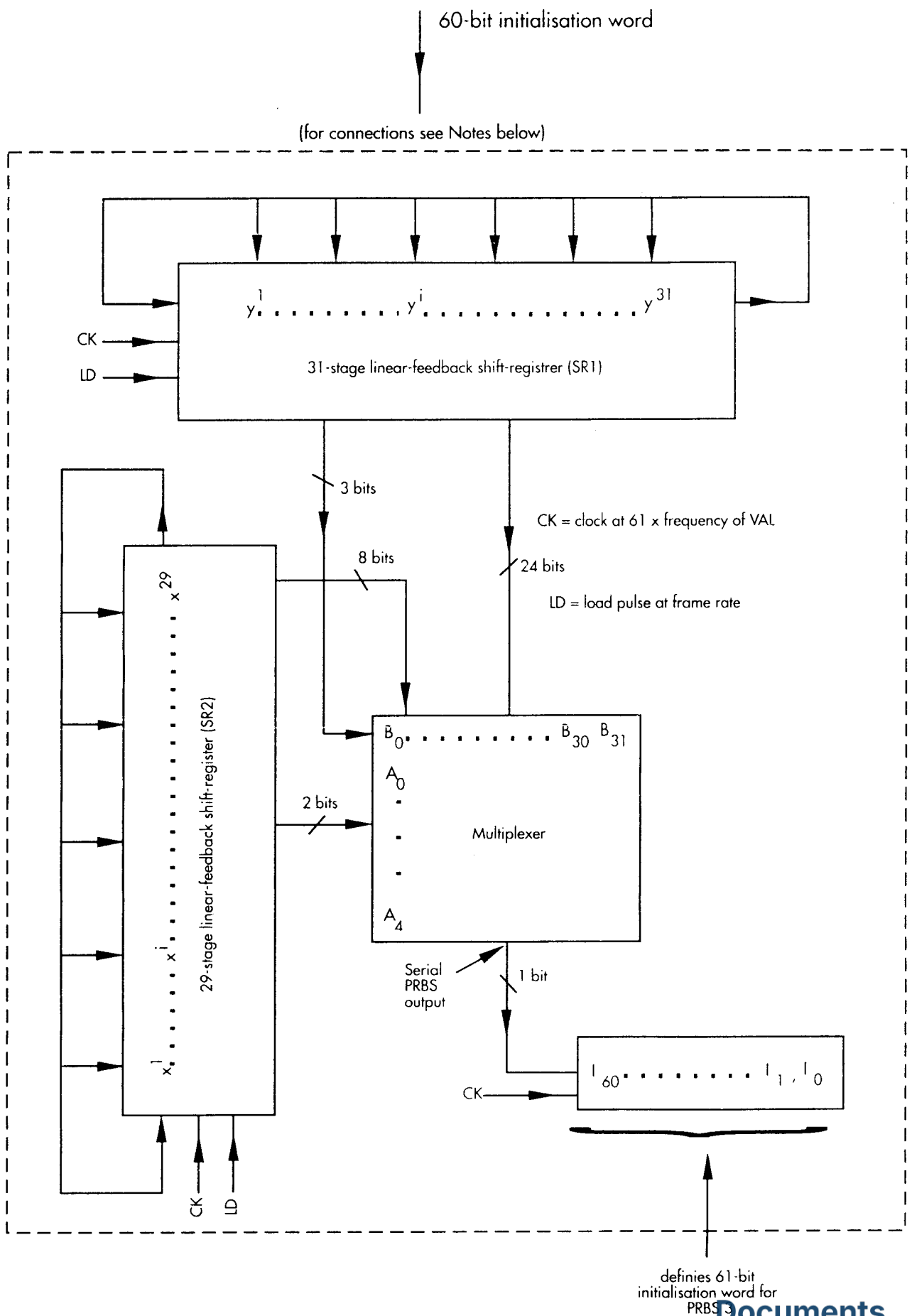


Figure 3.2 : PRBS generator 1 in Fig. 2

Notes

The interconnections of the block diagram in *Figure 3.2.* are as follows :

The PRBS generator has two multi-stage linear-feedback shift-registers SR1 and SR2. The polynomials defining the feedback configurations are as follows :

$$\text{SR1 : } 1 + y + y^2 + y^3 + y^7 + y^{14} + y^{19} + y^{25} + y^{31}$$

$$\text{SR2 : } 1 + x^2 + x^3 + x^4 + x^8 + x^{11} + x^{16} + x^{20} + x^{29}$$

The initialisation word is loaded in SR1 and SR2 as follows : the 60-bit initialisation word is defined by the list $I_{59} - I_0$, where I_i represents each bit and i varies between 0 and 59.

$$\text{SR1 : } I_i \text{ is loaded in } y^{(31-i)} \text{ for } i = 0 \text{ to } 30$$

$$\text{SR2 : } I_i \text{ is loaded in } x^{(60-i)} \text{ for } i = 31 \text{ to } 59$$

The shift register outputs are input to a multiplexer. The inputs to the multiplexer are represented as A_0 to A_4 and B_0 to B_{31} . The connections are defined as follows :

$$x^1 \text{ is loaded in } A_0$$

$$x^2 \text{ is loaded in } A_1$$

$$x^i \text{ is loaded in } B_{(i-3)} \text{ for } i = 3 \text{ to } 10$$

$$y^1 \text{ is loaded in } A_2$$

$$y^2 \text{ is loaded in } A_3$$

$$y^3 \text{ is loaded in } A_4$$

$$y^n \text{ is loaded in } B_{(n+4)} \text{ for } n = 4 \text{ to } 27$$

The signal A is a 5-bit word $A_4 \dots A_0$ which defines the address of the index of signal B (binary number corresponding to 0-31 for $B_{31} - B_0$). The 61 consecutive values of signal B, as defined by address A, are output to form the initialisation word for PRBS 3 generator at the rate of one per packet (i.e. the VAL signal frequency). The least significant bit in the initialisation word (I_0) is output first.

Notes of Figure 3.2

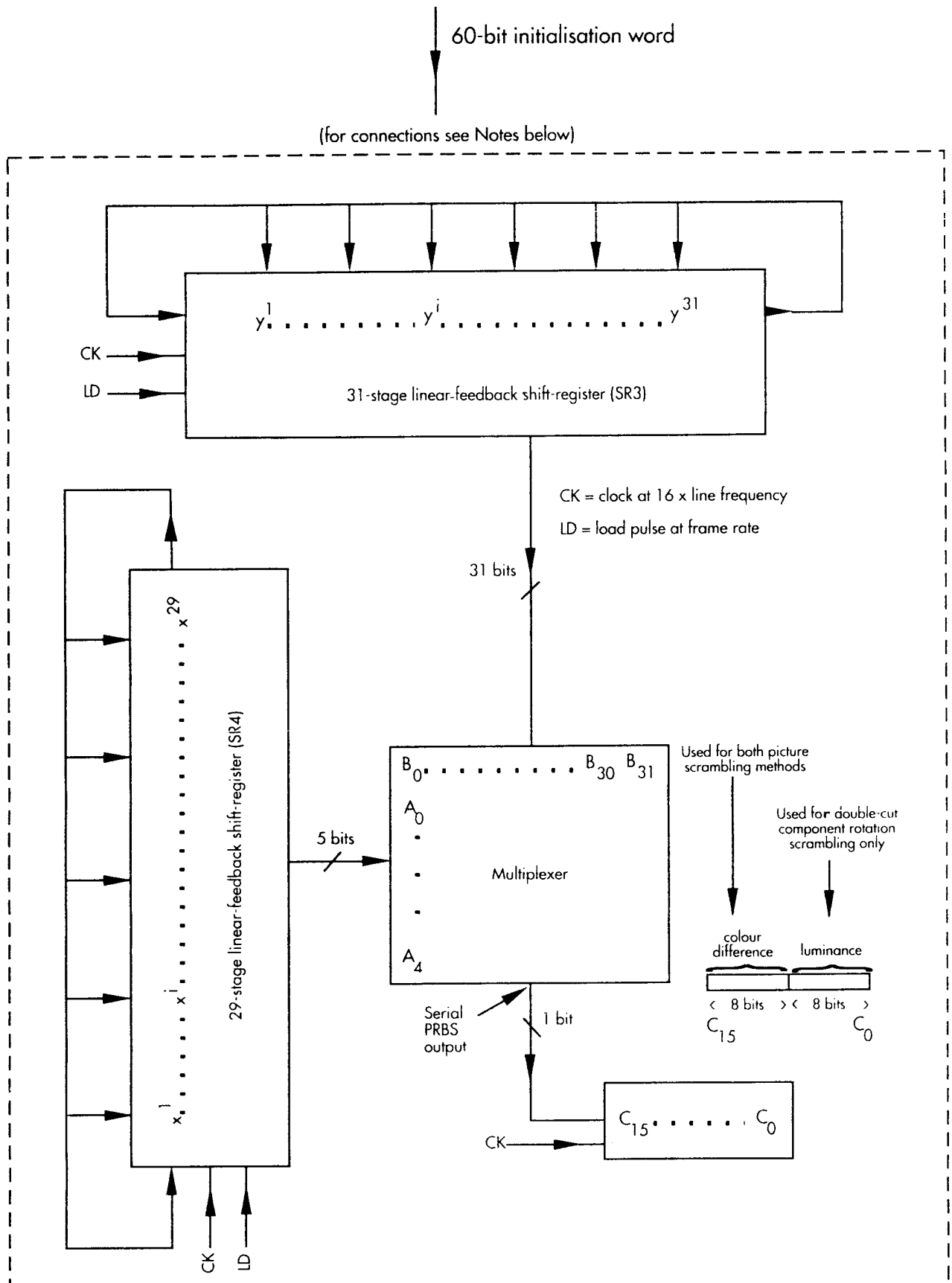


Figure 3.3 : PRBS generator 2 in Fig. 3.1

Notes

The interconnections of the block diagram of *Figure 3.3* are as follows :

The PRBS generator has two multi-stage linear-feedback shift-registers SR3 and SR4. The polynomials defining the feedback configurations are as follows :

$$\text{SR3 : } 1 + y + y^2 + y^3 + y^5 + y^6 + y^7 + y^9 + y^{10} + y^{11} + y^{15} + y^{19} + y^{23} + y^{27} + y^{31}$$

$$\text{SR4 : } 1 + x^2 + x^3 + x^4 + x^5 + x^7 + x^{11} + x^{13} + x^{14} + x^{20} + x^{29}$$

The initialisation word is loaded in SR3 and SR4 as follows : the 60-bit initialisation word is defined by the list $I_{59} \dots I_0$, where I_i represents each bit and i varies between 0 and 59.

SR3 : I_i is loaded in $y^{(31-i)}$ for $i = 0$ to 30

SR4 : I_i is loaded in $x^{(60-i)}$ for $i = 31$ to 59

The shift register outputs are input to a multiplexer. The inputs to the multiplexer are represented as A_0 to A_4 et B_0 to B_{31} .

The connections are defined as follows :

x^i is loaded in $A_{(i-1)}$ for $i = 1$ to 5

y^i is loaded in $B_{(i-1)}$ for $i = 1$ to 31

In addition, B_{31} is strapped to B_{30}

The signal A constitutes a 5-bit word $A_4 \dots A_0$ which defines the address of the index of signal B (binary number corresponding to 0-31 for $B_{31} \dots B_0$). Sixteen consecutive values of the relevant signal B are output to form the 16-bit image descrambling word at line rate.

For the double-cut component rotation system, the luminance component cut-point number (in the range 0 to 255) is the binary number $C_7 \dots C_0$ given by the 8 bits furthest to the right on the 16-bit shift register at the output of the PRBS 2 generator.

The colour-difference component cut-point number (in the range 0 to 255) is the binary number $C_{15} \dots C_8$ given by the 8 bits furthest to the left on the 16-bit shift register at the output of the PRBS 2 generator.

For the single-cut line rotation system, only the colour-difference cut-point number described above is used.

Notes of Figure 3.3

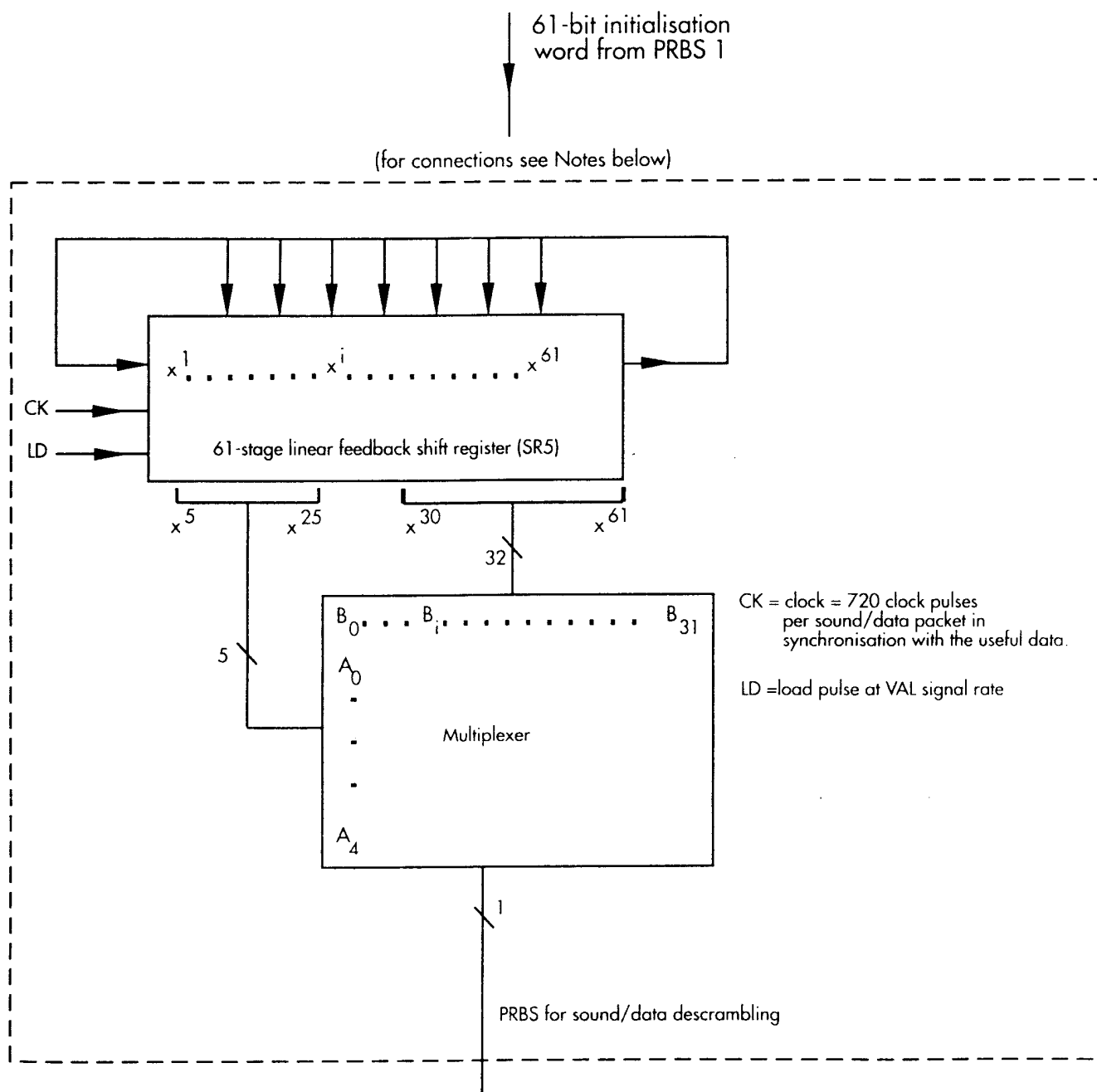


Figure 3.4 : PRBS generator 3 in Fig. 3.1

Notes

The interconnections of the block diagram in *Figure 3.4* are as follows :

The PRBS generator has one 61-stage linear-feedback shift-register SR5. The polynomial defining the feedback configuration is as follows :

$$\text{SR5 : } 1 + x^2 + x^3 + x^7 + x^8 + x^9 + x^{10} + x^{12} + x^{15} + x^{19} + x^{20} + x^{22} + x^{24} + x^{25} + x^{28} + x^{30} + x^{33} + x^{34} + x^{37} + x^{40} + x^{43} + x^{44} + x^{46} + x^{54} + x^{56} + x^{60} + x^{61}$$

The initialisation word is loaded in SR5 as follows.

The 61-bit initialisation word is defined by the list $I_{60} - I_0$, where I_i represents each bit and i varies between 0 and 60.

SR5 : I_i is loaded in $x^{(60-i)}$ for $i = 0$ to 60

The shift register outputs are input to the multiplexer. The inputs to the multiplexer are represented as A_0 to A_4 and B_0 to B_{31} . The connections are defined as follows :

$x^{5(i+1)}$ is loaded in A_i for $i = 0$ to 4

$x^{(30+i)}$ is loaded in B_i for $i = 0$ to 31

The signal A is a 5-bit word $A_4 \dots A_0$ which defines the address of the index of signal B (binary number corresponding to 0-31 for $B_{31} - B_0$). The value of signal B, at the address defined by A, is switched to the output at clock instants (CLK 2) to form a serial output data stream at the same rate as the useful data.

Notes of Figure 3.4

4. SIGNALS CROSSING THE ACCESS CONTROL INTERFACE

4.1 Receiver-ACS interface*

4.1.1 Configuring the receiver-ACS interface

Receivers with access control can be divided into modules and systems as shown in *Figure 4.1*. The access control system (ACS) is connected to the rest of the receiver via a receiver-ACS interface.

The functions associated with data demultiplexing, packet selection, and man/machine dialogue (for VDU module management only) are external to the access control system.

The access control system may be buried in the receiver, or detachable and connected via an external receiver-ACS interface. There may be more than one ACS available on one receiver. The choice of access control system is based on an ACS type information field and on the programme providers identifiers available in the ACS.

The ECM and EMM messages are sent to the access control system in the data multiplex. The entitlement management messages are, in most cases, addressed to individual customers or to specific groups of customers ; they are then identified by a customer address which is a unique address for a message to a particular customer or a shared address for a message to a group of customers. In this case, only those EMM packets which have a correct customer address (unique, shared or collective) cross the receiver-ACS interface. The result of this is that the access control system submits its customer addresses to the receiver EMM receiving circuit before selection can be implemented.

The signals which cross the receiver-ACS interface are illustrated in *Table 4.1* and annotated in sections 4.1.2 and 4.1.3, below.

4.1.2 Signals received by the ACS

Entitlement management messages EMM are used to provide each customer with the means of accessing the services he is authorised to receive. The EMM can be sent by the MAC/packet signal on a special over-air addressing service, represented by the LISTX parameter value '04 in the service identification channel (cf. section 2.1 in Part 5 of document Ref.1). The ACCM parameter indicates the channel address of the EMM packets in the data multiplex (cf. section 11). Four different types of EMM message (EMM-U, EMM-S, EMM-C and EMM-G) are specified ; all of them (except EMM-G) contain a customer address which indicates to the receiver (and consequently to the ACS) to whom they are addressed. Only those EMM packets addressed to the ACS cross the receiver-ACS interface.

EMM-U can also be transmitted by other means (mail, telephone, etc.). Similarly, the information conveyed in EMM-S and EMM-G messages can be transmitted on networks other than the broadcasting network, except for messages conveying information which needs to be synchronised with programme broadcasting and which is dependent on operational decisions, i.e. replacement and fingerprinting (EMM-C), etc.

ECM (entitlement control messages) are applied to all customers, but are specific to a service or a set of services. ECM can be transmitted only over the broadcasting network. The ACCM parameter(s) described in the service identification channel indicates the presence or absence of ECM and their corresponding channel address(es) (cf. section 2.3 in Part 5 of document Ref.1).

* The specification of the characteristics of an elementary simplified and non system specific interface in case of a detachable Access Control System is under consideration

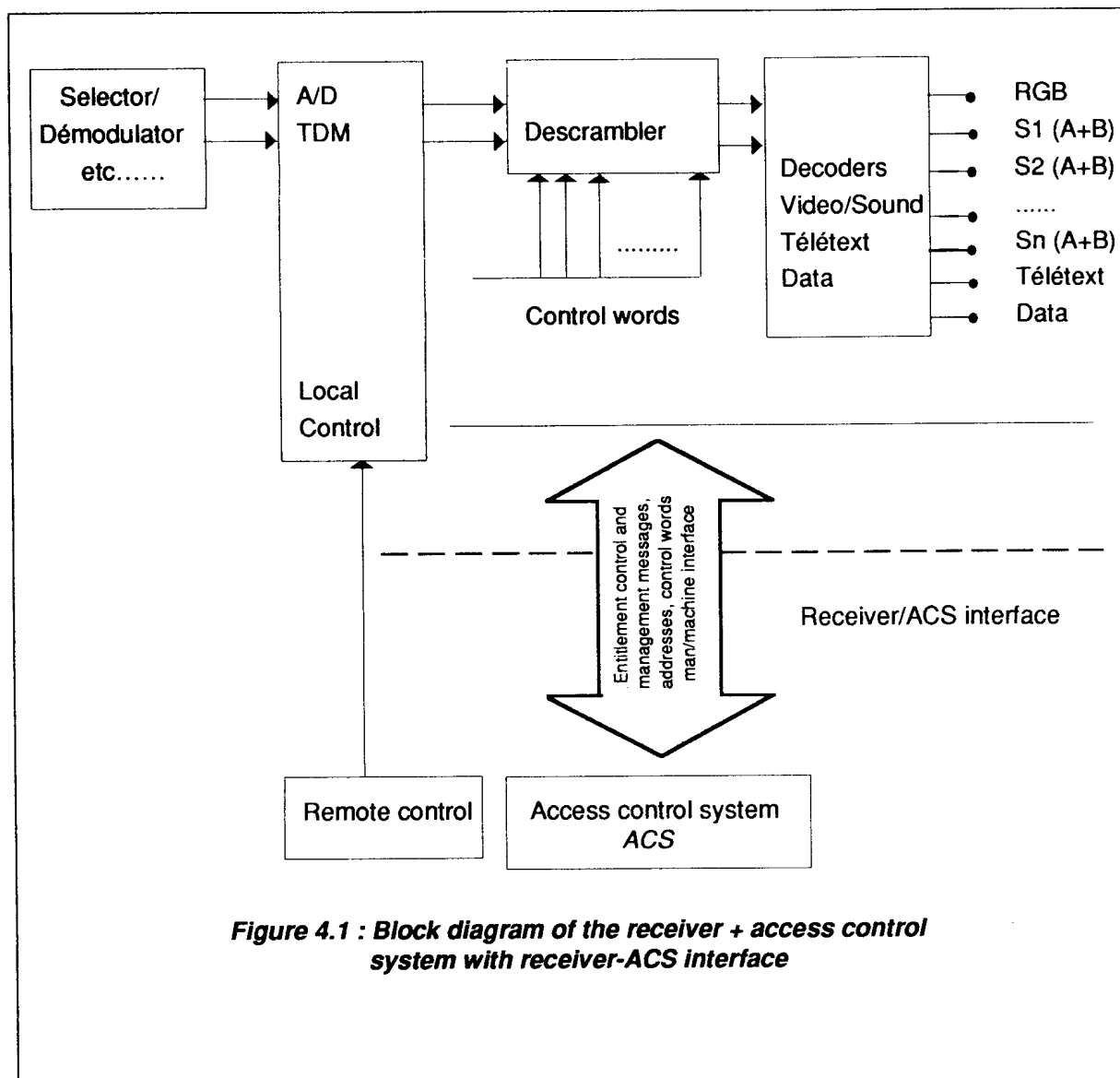


Figure 4.1 : Block diagram of the receiver + access control system with receiver-ACS interface

The ACS is selected by the CI code described in section 10.1 for ECM and section 5.1 for EMM. If there are two ACS of the same type, the selection process is then based on the presence of service identifiers (inasmuch as a service identifier can only be available in one ACS). Keys and entitlements within the ACS are selected by the PPID parameter described in sections 5.5.3 and 10.4.3. These parameters are pointers to the required key. The key identification and corresponding control word generation processes are described in sections 4.2 and 4.3.

The access control related man/machine dialogue is in two parts : management of VDU modules that are external to the ACS, and internal ACS dialogue contents (messages displayed, type of keyboard input, etc.).

For each service, the following options are provided by the ACS via a menu and a command from the receiver keyboard (remote control) :

- display available service access modes (subscription, pre-booked or impulse pay-per-view per programme, impulse pay-per-view per time),
- display service or programme access mode selected by customer,

GENERAL LIST OF MESSAGES CROSSING THE RECEIVER-ACS INTERFACE	DATA SIGNALS CROSSING THE RECEIVER-ACS INTERFACE
From receiver to ACS Content of selected packets Man/machine dialogue information Initialisation	From receiver to ACS EMM-U packets EMM-S packets EMM-C packets EMM-G packets ECM packets Transmission of keyboard input Initialisation
From ACS to receiver Control words Customer addresses Configuration data Data for use by the receiver extracted from EMM Man/machine dialogue information	From ACS to receiver Even and odd control words Unique address Shared address Collective address Group address Configuration data Modem telephone number Call date and time Individual messages Authentication parameters Display data

Table 4.1 : Principal exchanges across the receiver-ACS interface

- display selected service label (mnemonic),
- display price per programme or price per unit time,
- purchase programme,
- purchase time units (tokens),
- display remaining credit,
- display programmes bought on pay-per-view basis : number and cost of programmes, number of tokens used (pay-per-view per time),

- display unique customer address,
- display programm provider user address,
- display group customer address (specific to each service).

A general description of the packets sent to the ACS is given in sections 5.1 and 10.1 ; the various EMM formats are described in sections 5 to 9.

4.1.3 Signals from the ACS

4.1.3.1 Locally-generated control messages

The ACS supplies the following information to the rest of the receiver :

- the unique costumer address (UA, see section 5.2),
- the shared customer address (PPUA, see section 5.2) corresponding to the current PPID,
- the group customer address (GCA, see section 5.2) corresponding to the current PPID, and the collective customer address (CCA, section section 5.2),
- the command identifiers CI (ACS type) indicating which packets can be interpreted by the ACS (see section 5.3) and the type of access control system CA (see section 11.3.2),
- the control words available for the service(s) or service components selected,
- the data configuration for replacement and fingerprinting.

4.1.3.2 Locally-generated messages for display

The following information can be displayed for each service, if requested by the customer :

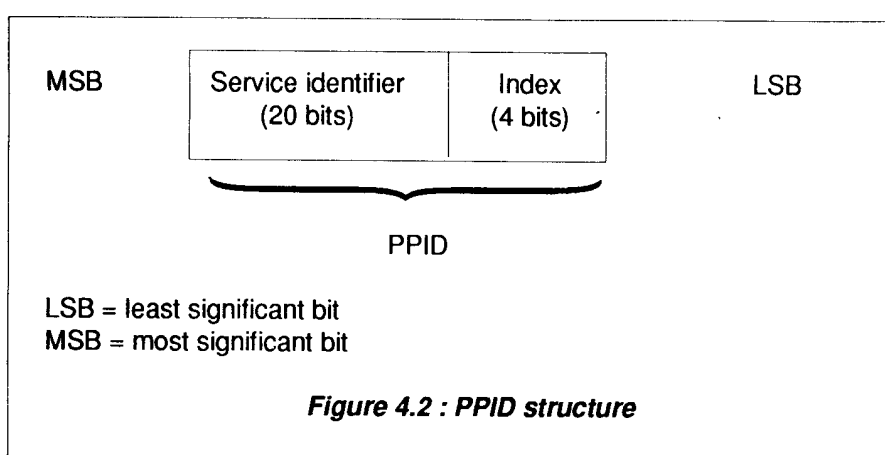
- available service access modes (free acces, subscription available, purchase made, pay-per-view per programme or per time, etc.),
- access mode used for the current programme (subscription, pay-per-view per programme or per time, etc.),
- cost of programme or of time unit,
- available credit,
- programme number and associated cost or tokens used for the programme purchased,
- unique address (UA) and shared address derived from PPUA,
- geographical code (GC) and subject code (SC),
- memory availability on entitlement storage device (per service or overall),
- maturity rating, receiver lock status.

The receiver manufacturer may consider adding diagnostic information for the customer.

4.2 Service identification and relation to control words

The various services are accessible on the basis of the following parameters :

PPID (24 bits) : identifies the service operator (programme provider). Points to the key in use for the service or component. The four least significant PPID bits (LSB) specify the index of the key used. To demonstrate implementation of the PC2 card, the PPID length is set at 24 bits (see *Figure 4.2*). In addition, for this ACS, the index can be used to define two service keys per operator (an operation key used only for computing control words and a management key used for computing control words and entering entitlements). In this case, the MSB of the index indicates whether it is an operation key (index '8 to 'F) or a management key (index '0 to '7).



- CDATE (16 bits)** : defines the broadcasting date of the service or component if accessed by subscription.
- THEME/LEVEL (16 bits)** : defines the theme/level of a service or component if accessed via a subscription per theme/level.
- LINK (8 bits)** : defines the class of a service or component if accessed via a subscription per class. This parameter points to a bit taken from the list of classes stored in the entitlement storage device (the length of the list of classes can range from 8 to 256 positions, in multiples of 8 bits).
- PNUMB (24 bits)** : defines the programme number when pay-per-view is offered by the programme provider.
- PPV/P (16 bits)** : defines the cost of the programme. Once purchased, the programme is accessible throughout its transmission time.
- PPV/T (16 bits)** : defines the cost of access to a programme during the validity period of a control word.
- RCI (16 bits)** : identifies a replacement service for a blacked-out programme.
- CTRL (8 bits)** : indicates the use of blackout and defines the maturity rating of the programme. This byte also specifies whether the computation of the control words is conditional on checking specified criteria or if all that is needed is to have the current operation key in order to perform the computation.

Each scrambled service or component is linked to its control word by the address of the channel containing the ECM messages, the address being defined by the ACCM parameter in the service identification channel (cf. section 4.1.2). An ECM message is thus sent for each service, component or set of services or components with different control words.

The control words are not computed by the ACS unless the corresponding service key is available and the parameters defining the programme access conditions are loaded in one of the entitlements in the customer storage device. Assuming that the service key is present, the checks carried out by the storage device differ slightly according to the programme access modes :

- **If the programme is accessible in subscription per theme/level**, the CDATE parameter must be included in the subscription validity period (beginning date - finishing date), the LEVEL parameter must be less than or equal to the level (LE) and the THEME must be equal to one of the themes (TH). The beginning date (BD), finishing date (FD), LE and TH are stored under the operator's PPID.
- **If the programme is accessible in subscription per class**, the CDATE parameter must be included in a period defined by BD and FD and the LINK parameter must point to a valid entitlement in the list of classes (CUSTWD). The list of classes and validity period are stored under the operator's PPID.
- **If the programme is accessible in pay-per-view per programme**, the programme number parameter PNUMB must be stored in the security processor. If the PPV/P method with the impulse option is offered by the programme provider, the customer can buy the programme provided his remaining credit (CREDIT) exceeds the price indicated by the PPV/P or PPV/T parameters. PNUMB and CREDIT are stored under the operator's PPID.

The service keys associated with an operator are also stored under a PPID. A number of service keys may be stored for one operator, in which case only the «index» part of the PPID will vary, with the 20-bit «service identifier» part remaining constant. This feature is offered to allow for the coexistence of a number of keys for one operator (operation key, management keys whether diversified or not), and for the renewal of keys. The entitlements associated with a particular operator are entered in transaction blocks and, for these blocks, only the «service identifier» part is analysed ; the index is ignored.

The definition and use of the PPID may be completely independent of the RF transmission channel.

- **a group of RF channels** may be assigned the same PPID. All the services offered by these channels will be controlled by the same service key, even if the services or components can be scrambled by different control words, based on the definition of different access conditions for different programme elements (subscription, PPV/P, etc.).
- **a RF channel** can be assigned a PPID. This channel will then be controlled by its own service key, even if the services or components can be assigned different control words, by defining different access conditions as described above.
- **service operators whether sharing the same RF channel or present on several RF channels** can be assigned their own PPID, each controlled by its own service key and able to have services or components scrambled with control words corresponding to different access conditions.

4.3 Generation and assignment of control words

4.3.1 Generation of control words

Even and odd control words are transmitted in the form of cryptograms in entitlement control messages ECM referring to the service and components selected by the customer (see section 4.2).

The service keys used for decrypting the control words are stored under the corresponding PPID.

4.3.2 Assignment and synchronisation of control words

The control words are assigned to the descrambler(s) used by the service to which the customer is tuned.

Control words must be transmitted sufficiently early, before the effective use of the control word, in order to cover the ECM reception time and the security processor checking and computation times, and to ensure synchronisation of the descrambling sequences, (see section 3.3).

5. GENERAL DESCRIPTION OF ENTITLEMENT MANAGEMENT MESSAGES (EMM)

Entitlement management messages are used :

- for the over-air addressing service when it is implemented for distributing entitlements or modifying keys,
- for distributing replacement configurations when these are used.

5.1 Message formats

Figure 5.1 shows the four possible formats of entitlement management messages (EMM).

The first two fields, PH and PT, are common to all packets. The packet header (PH) contains a 10-bit address field identifying the packet in the data multiplex and a 2-bit continuity index (I). EMM packets of the same type can be linked using the continuity index (I) of the packet header. The first synchronizing packet of a message always has a zero continuity index (I=0), while subsequent packets have continuity index values in the range [1,3], the value of I being incremented by 1 in modulo 3 sequence each time a packet of the same type is transmitted (see Figure 5.2). The PH field is protected by a (23,12) Golay code.

The message type is given by the packet type field (PT) which is protected by a (8,2) code as described in section 7.1 of Part 3 of document Ref.1. The four values of the PT parameter for EMM are defined in Figure 5.1.

After the PT parameter, all packets contain an error-protected data field. Protection is provided by a (24,12) Golay code ; the data block then consists of 30 (24,12) Golay words, which corresponds to a useful data field length of 360 bits once the protection is removed. The 24-bit code words are formed by the (23,12) code specified by the packet headers (cf. the appendix to Part 3 of document Ref.1), the 24th bit specifying an overall odd parity.

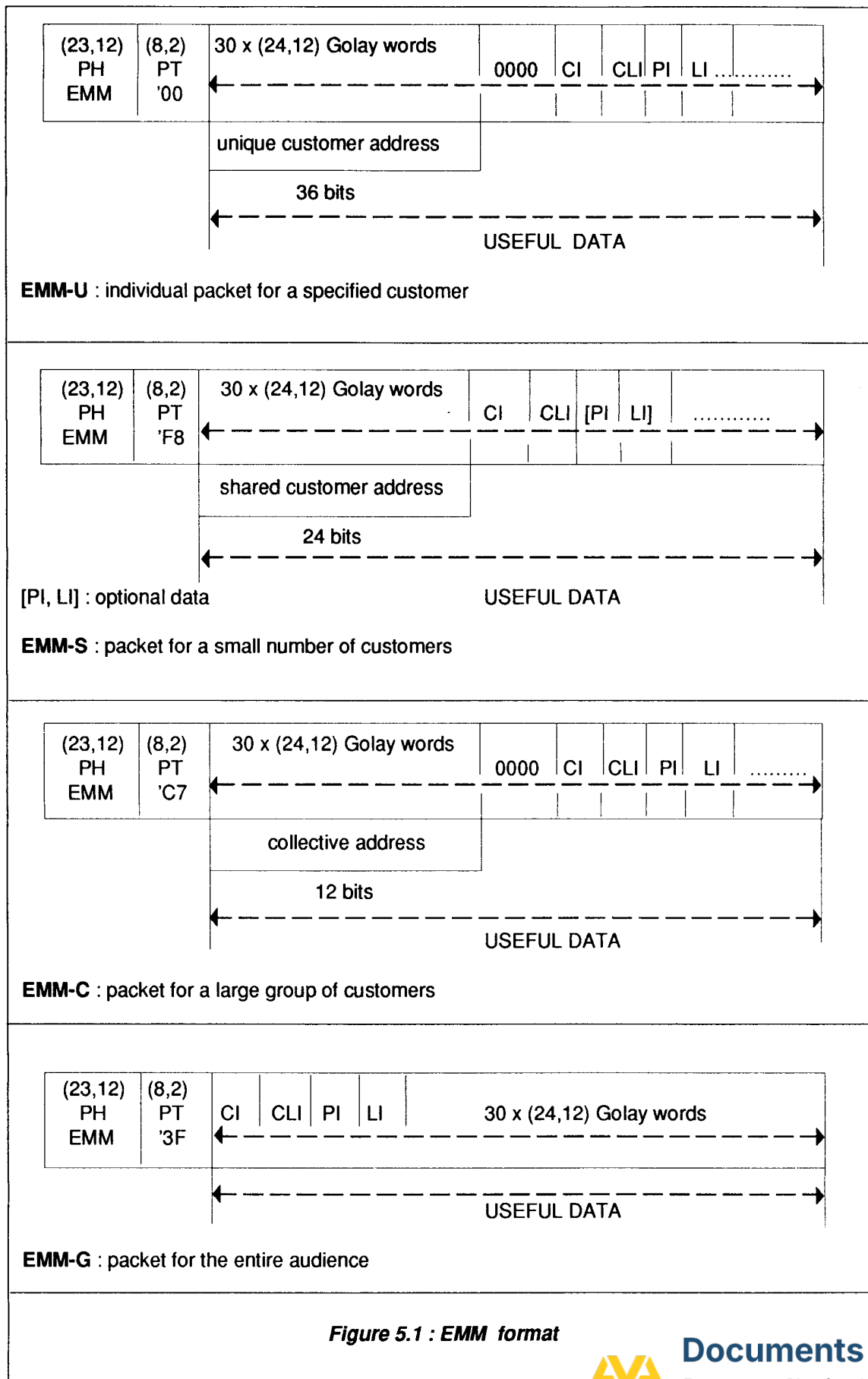
All synchronizing packets contain a clear command identifier (CI) specifying the type of data contained in the EMM, the crypto-algorithm type used and the format of the data within the EMM. If present, the parameter identifiers (PI) specify the content of subsequent data which follow (the parameter data field).

Three possible types of EMM are specified with a customer address field located **before** the CI parameter, while the fourth format begins with the CI parameter (this last type may include a group address **after** the CI parameter). The contents of the entitlement management messages are described below and apply to the EMM-U, EMM-G, EMM-S and EMM-C messages described in sections 6, 7, 8 and 9.

Entitlement management messages are protected by a (24,12) Golay code. The hexadecimal notation described in sections 5, 6, 7, 8 and 9 specifies the value of the data field of the message, **with** the Golay code removed. All subsequent references to sizes in bytes apply to the useful message data.

Only the CI and PI values specified in this document will be recognized by the sample implementation of PC2 (described in appendix 1).

Note : In the following parts of this document, the ' character is set before the hexadecimal values (for example : '00 and 'A8).



All messages containing an unrecognised CI parameter will be ignored. Unrecognised PI parameters introducing a variable format data field (see *Figure 5.2*) will be ignored (as will the associated data field), but this will not cause the message to be rejected. The parameters defined in the document are reserved for the use corresponding to their definition. All the parameters introduced by a parameter identifier (PI) have a variable format data field flagged by the length indicator LI.

In the remainder of the document (sections 5, 6, 7, 8 and 9) the length and contents of the data field for these parameters correspond to the sample ACS implementation (detailed in appendix 1). For other implementations, the length of the data field for the parameters defined may be extended or shortened provided the use of that part of the field currently specified is retained. Further parameters may also be introduced on condition that they comply with the following rules which are applicable to the EUROCRIPT specification :

- the PPID parameter must be present in all variable format EMM,
- the HASH parameter must be present in all EMM-U, EMM-G for entering common or free initial entitlements, and EMM-S.

The address fields preceding the CI code are transmitted with the least significant bit first ; when necessary, they are followed by four zero bits in order to use an integer number of bytes.

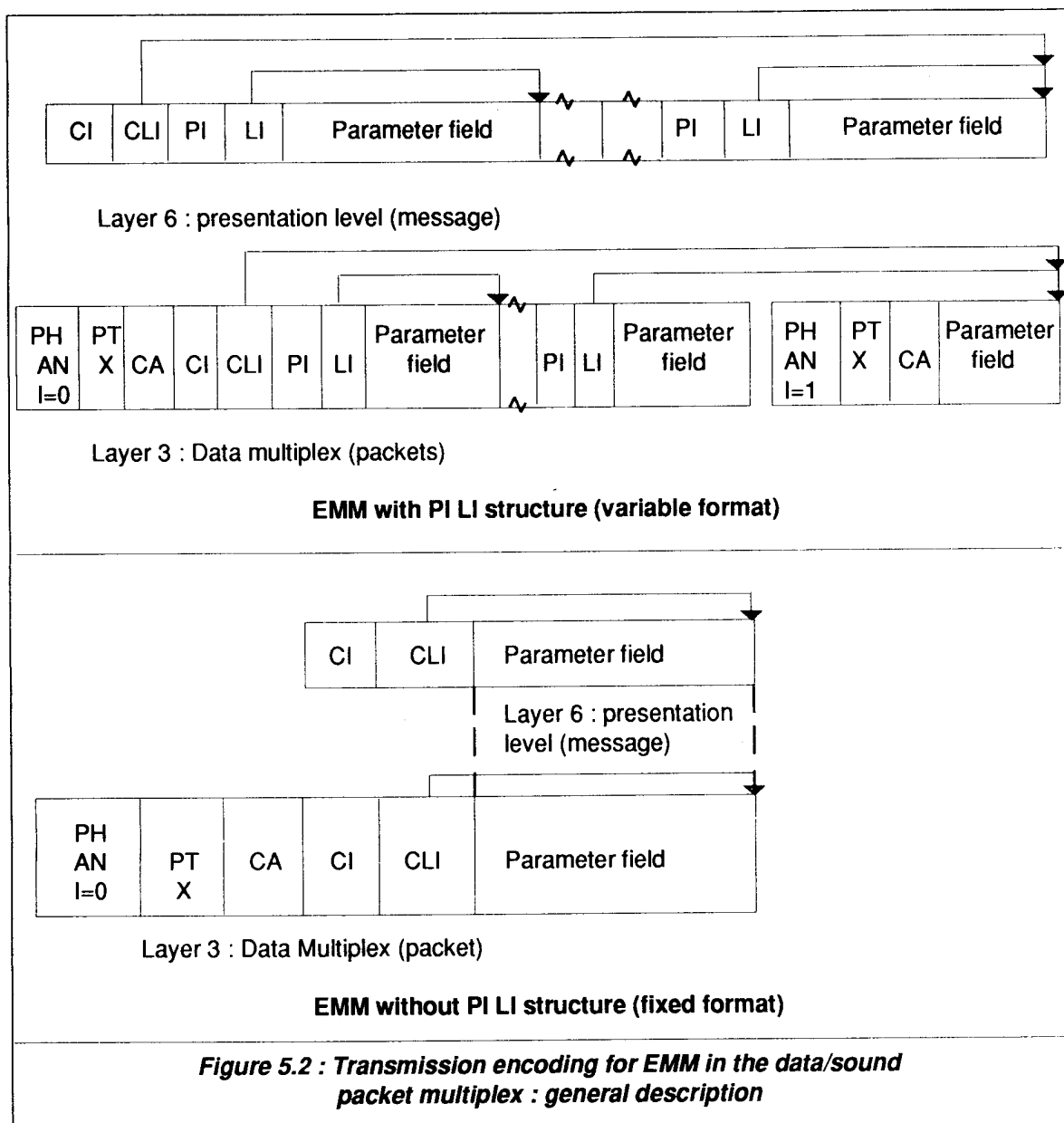
The parameter data fields contain an integer number of bytes. The most significant byte is the one containing the most significant bit (MSB). The least significant byte is the byte containing the least significant bit (LSB). The bytes of a parameter data field are transmitted most significant byte first and least significant byte last.

All the bytes of the message (see *Figure 5.2*), as from and including the CI code, are transmitted least significant bit first and most significant bit last.

When a parameter field contains numbered bits, the least significant bit (LSB) is designated b0.

Notes about *Figure 5.2* :

- PH Packet Header ; this contains the continuity index I (2 bits) and the address AN (10 bits) of the dedicated data channel for entitlement management messages as described in the service identification channel.
- PT Packet Type (2 bits), see *Figure 5.1* (X = '00, 'F8, 'C7 or '3F for EMM).
- CA Customer Address field (0-36 bits depending on the value of PT, padded, where necessary, by zeros to an integer number of bytes), see *Figure 5.1*.
- CI Command Identifier (8 bits) ; this specifies the format of the parameter field and the crypto-algorithm type.
- CLI Length Indicator (8 bits) for the parameter field associated with CI.
- PI Parameter Identifier (8 bits), optional.
- LI Length Indicator for the parameter field associated with PI (8 bits).
- The presence of the PI LI structure depends on the value of CI. The PI LI structure is used for EMM-U, EMM-G, EMM-C and for some EMM-S. The fixed format structure is used for other EMM-S.
- There is no packet suffix at the end of the packets.



5.2 Customer addresses

The ACS can provide up to four types of addresses to the receiver :

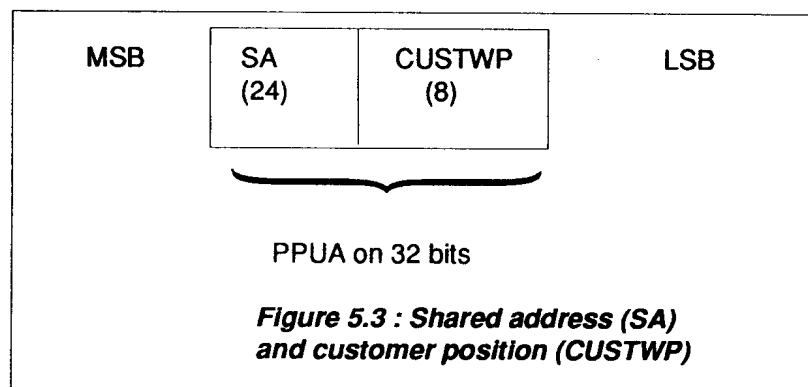
— A unique address on 36 bits (UA)

The UA is common to all PPID. It is loaded in the ACS when the security processor is manufactured and stored in non-erasable and non-modifiable memory.

— **A shared address on 24 bits (SA) for each PPID**

This address defines a group of 256 customers for the purpose of entitlement transmission. It is derived from the programme provider user address (PPUA) on 32 bits comprising the SA on the 24 most significant bits and the position of the customer within the group (CUSTWP) on the eight least significant bits. This last parameter, CUSTWP, points to a customer within the group sharing the same SA, as described in *Figure 5.3*.

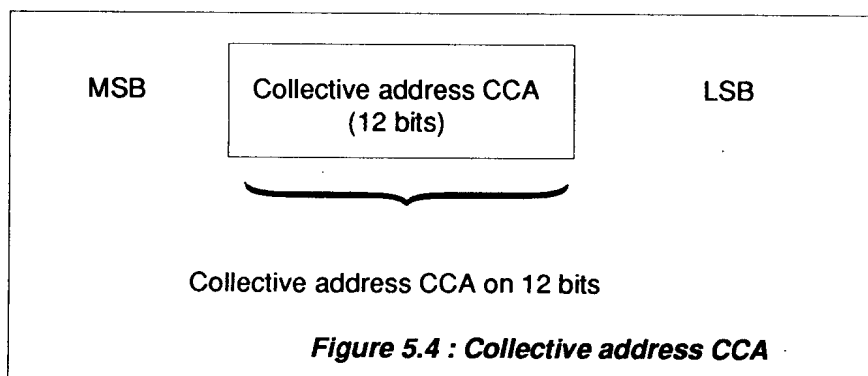
Each group is referenced by its SA and contains 256 customers. The position of a customer in the group is given by the pointer CUSTWP (8 bits).



— **A collective address on 12 bits (CCA)**

The collective address CCA is illustrated in *Figure 5.4*.

The EMM-C format is reserved for transmitting replacement configurations for blacked-out areas. The collective address value CCA is set to 0.



— **A group customer address on 32 bits (GCA) for each PPID**

The GCA comprises two parts, GC and SC, and is used for addressing groups defined in terms of geographical location and category (common interests, profession, etc), see *Figure 5.5*.

The 32 bits of the GCA parameter represent an 8-digit hexadecimal coded number, abcdefgh. The 24 most significant bits represent the geographical code (GC = abcdef) while the eight least significant bits represent the subject code (SC = gh).

The stored GC code (abcdef) can be allocated in accordance with the six most significant digits of the customer's international telephone number, or the number of the telephone exchange to which he is connected. Any other meaning of national significance may be specified in the national part of the number, where the national telephone numbers do not correspond to clearly defined geographical areas.

The stored SC code (gh) is one item selected from the 255 existing subject codes.

The GA parameter included in EMM-C packets or the GGA parameter included in ECM packets is compared with the GCA parameter stored in the receiver. The transmitted packet will not be analysed unless the following conditions are satisfied :

- the subject codes match or the transmitted category code is 'FF,
- **and** the characters of the transmitted GC parameter match the characters of the stored GC parameter, or the value of the transmitted character is 'F (hexadecimal), see *Figure 5.5*.

Examples :

GC = 'FFFFFF, SC = 'FF : global address 'FF (the entire audience),

GC = 'FFFFFF, SC = 'CD : global address of group 'CD (e.g. all bridge players),

GC = '78FFFF, SC = 'FF : address of all receivers located in the (telephone) area with numbers beginning '78,

GC = '7883FF, SC = 'FF : address of all receivers located in the (telephone) area with numbers beginning '7883,

GC = '7883FF, SC = 'CD : address of the specified group of receivers (e.g. bridge players) located in the (telephone) area with numbers beginning '7883.

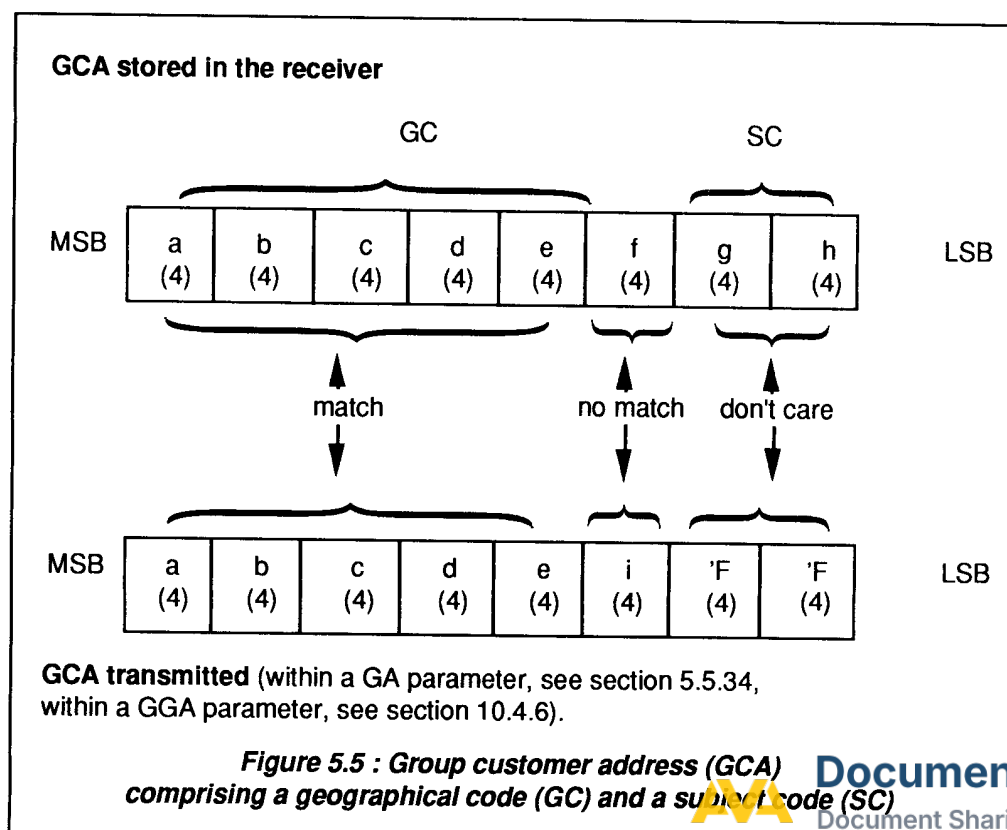


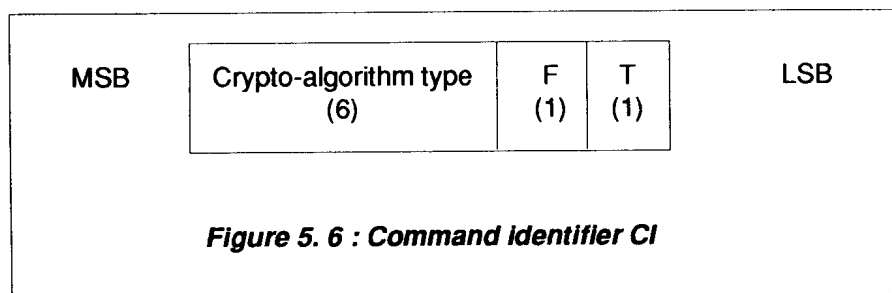
Figure 5.5 shows an example in which the five most significant nibbles of the stored GC code (abcdef) and the transmitted GC (abcdei) match, but not the sixth. Because the SC code has the value 'FF (don't care)' this field is not analysed

All EMM packets which, on comparison, do not show a match on the customer address are disregarded until a match is found to indicate that the packet concerns the ACS.

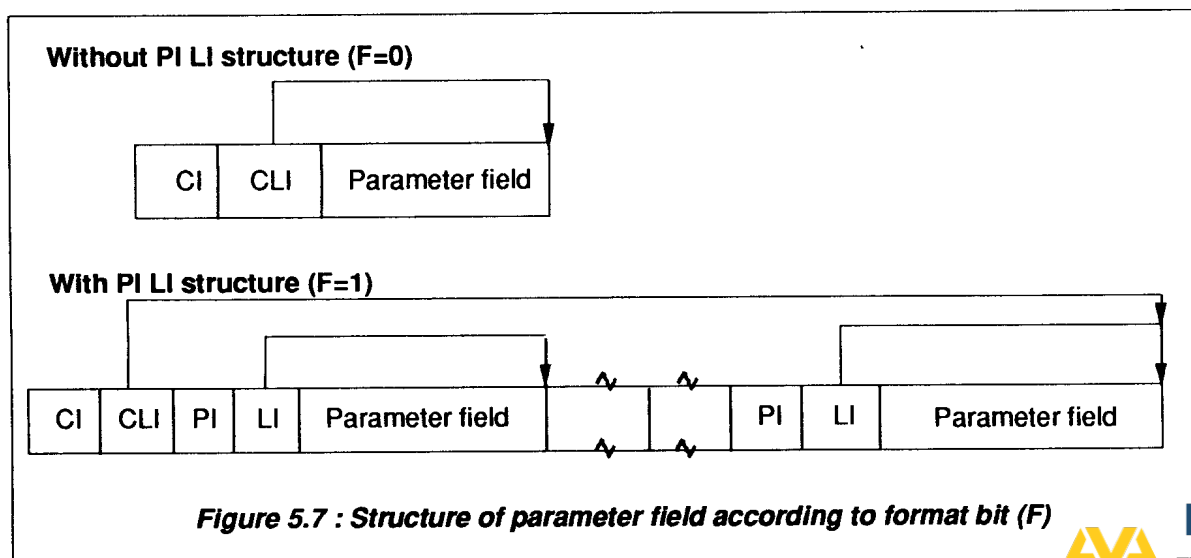
UA, SA, GCA and CCA are stored in a non-volatile memory in the security processor.

5.3 Command identifier CI

The CI parameter comprises 8 bits. This parameter describes the format being used for the parameter field and the type of cryptographic algorithm used for decryption. It is included in all EMM messages and located in the message synchronising packet. Its contents are described below and illustrated in Figure 5.6.



- T is used in EMM-G and EMM-C to indicate a change in the information contents of the messages (toggle bit). It is also used in fixed format EMM-S messages to indicate whether or not the address field ADF is scrambled (T = 1 : ADF is scrambled, T = 0 : ADF is in clear). It has no meaning for EMM-U. This bit is also used as a toggle bit in ECM messages (see section 10.2).
- F is the format bit specifying whether the next parameter field is in fixed format (F=0) or variable format (F = 1), as illustrated in Figure 5.7.
- Type of crypto-algorithm (6 bits). The hexadecimal value '20 is currently defined for this field ; it corresponds to the sample implementation of the entitlement storage device (PC2) described in appendix 1.



5.4 Length indicator CLI

The CLI parameter comprises 8 bits. It indicates the number of bytes in the EMM data field. This parameter is always included in an EMM message after the CI parameter.

5.5 Parameter identifier PI

The PI codes are included only if the CI parameter introduces a variable format parameter field (F=1), (see section 5.3). The PI code is followed by a byte LI specifying the length of the parameter field in bytes.

The EMM carry all the information needed to update or configure the customers' security processors. These parameters are used to specify :

- The programmer provider user address (PPUA) comprising the shared address (SA) and the position of the customer within the group (CUSTWP).
- The group customer address (GCA) comprising the geographical code (GC) and the subject code (SC).
- The operation keys (SK) used for computing the control words.
- The management keys (PDK, which can also be used as operation keys), used for entering new entitlements for the customer.
- The parental code (PIN code).

The EMM are also used to renew entitlements and send individual messages. Finally, these messages can convey the information needed to configure blackout and fingerprinting.

5.5.1 List of parameters available in EMM messages

The list of parameters below describes all the available PI parameters (values expressed in hexadecimal notation). The parameters actually included in each EMM depend on the nature of the information transmitted.

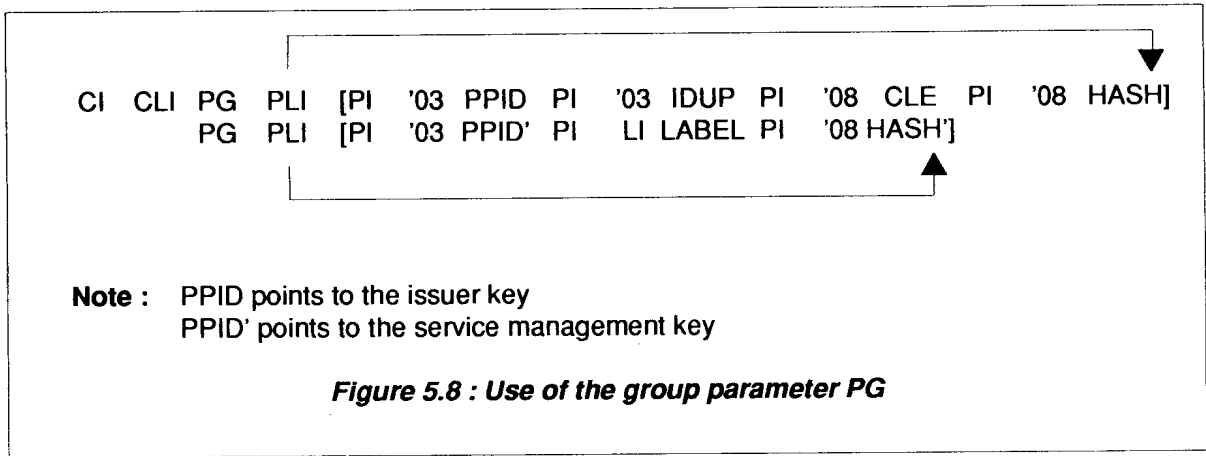
- PI = '70 : Software parameter (SOFT) used when software is to be added to process the subsequent parameters ; this parameter can be used only by an ACS capable of downloading software in order to complement a resident application.
- PI = '90 : Programmer provider identifier (PPID) representing the operator generating the EMM.
- PI = '91 : Random number (RND-ADF) used as a basis of cryptographic computation for descrambling the address field ADF.
- PI = '92 : Random number (RND-CONF) used as a basis of cryptographic computation for descrambling confidential data (entitlements introduced by the PC parameter, described below, or purchase surveys).
- PI = '93 and '94 : Programme provider authentication control parameters used prior to purchase survey or read-out of customer credit.

- PI = '9E : Address field (ADF) ; this parameter is used to indicate the status (authorised or barred) of each customer in a group of 256 customers referenced by the shared address (SA). Each customer is in turn referenced by his SA and CUSTWP which points to the corresponding bit of ADF.
- PI = 'A0 : Control (CTRL) ; this parameter is used when invalidating or deleting entitlements from the security processor. It is also used when transmitting free initial entitlements or to lock out a service.
- PI = 'A1 : Identifier of the block of data to be updated (IDUP), used when entering or invalidating/deleting a key, a descriptor or a service.
- PI = 'A2 : Descriptor (DESCR) ; this parameter is used to enter the memory allocation and control descriptor of a programme provider. This descriptor must be included in the security processor for a programme provider to operate, and precedes all other information (key, etc.). The descriptor specifies the maximum amount of memory allocated to the programme provider, service locking authorisation and the access methods which can be used, such as subscription, pay-per-view per programme, etc.
- PI = 'A3 : Facility data (FAC) ; this parameter is used to enter general purpose data loaded under a specific PPID. This data can be used by the terminal for certain specific operations such as automatic calls, entering an authentication value, and so on. This parameter is also used to delete these same items of data.
- PI = 'A4 : Unique customer address (UA) ; this parameter is used to update the unique address of the customer in the security processor. Once stored in the processor, this address is used to filter EMM-U messages.
- PI = 'A5 : Programme provider user address (PPUA) ; this parameter is used to enter or update PPUA by EMM.
- PI = 'A6 : Group customer address (GCA) ; this parameter is also related to a programme provider. It is included when entering or updating GCA by EMM.
- PI = 'A7 : Label (LABEL) ; this parameter is specific to each programme provider (PPID). It is used to name and identify the programme provider in the man/machine dialogue with the customer. It comprises up to sixteen characters from the CCITT No. 5 alphabet (example : CANAL+, SKY, etc.).
- PI = 'A8 : Dates (DATES) + theme/level (TH/LE) ; this parameter is included when defining a subscription per theme/level in the EMM.
- PI = 'A9 : Dates (DATES) + list of classes (CUSTWD) ; this parameter is included when defining a subscription per class in the EMM.
- PI = 'AA : Initial programme number (INUMB) and final programme number (FNUMB) ; this parameter is included when purchasing one or more consecutive programmes in pre-booked pay-per-view mode, or when deleting programme numbers already recorded. Programmes with numbers included in the INUMB to FNUMB range inclusive will be acquired (or deleted). This parameter is used in pre-booked pay-per-view mode to allocate a programme or a set of programmes from a series (serials, etc.) to a given customer (each component of the series will be allocated a PNUMB which is incremented by 1 after each item).

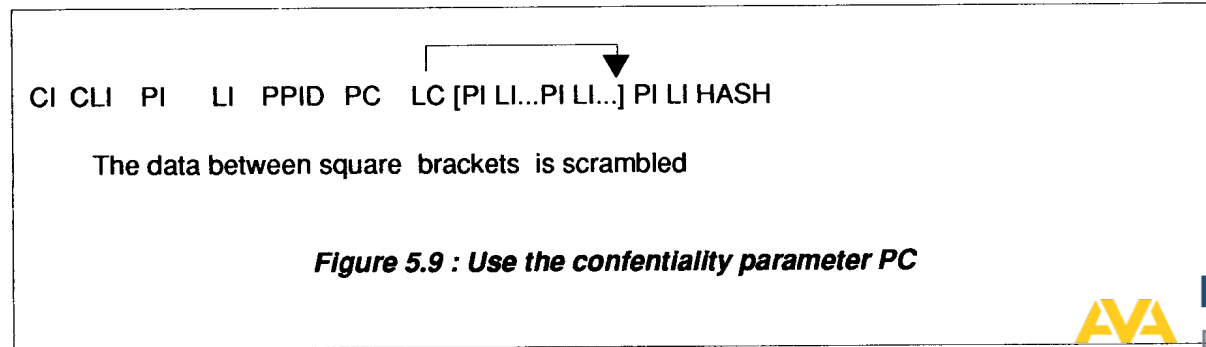
- PI = 'AB : Date (DATE) + credit (CREDIT) ; this parameter is used where additional credit is allocated to a customer. It is added to the remaining credit to constitute the new credit available to the customer. This credit can be used in impulse pay-per-view per programme or per time modes.
- PI = 'AC : Date (DATE) + total amount allocated (TOTAM) ; this parameter specifies the total amount of credit allocated to the customer since being connected to the programme provider. This represents another form of customer accreditation ; when a customer requests additional credit, it can be granted in the form of CREDIT or in the form of TOTAM.
- PI = 'AD : Date (DATE) + authorised overdraft (OVER) ; if included, this parameter specifies, the maximum amount by which a customer may overdraw for a given programme provider. It is included to offset carelessness on the part of the customer in forgetting to purchase more credit when his remaining credit is almost used up, in order to allow continued access to a current programme. The amount of overdraft used is naturally deducted from the next re-accreditation value.
- PI = 'AE : Date (DATE) + purchase survey (SURVEY) ; this parameter is included only where access is possible via an interactive network between the management centre and the customer's security processor. The purchase survey is required for customers using the impulse pay-per-view per programme or per time modes, to provide a retrospective method of determining royalties due.
- PI = 'AF : Dates (DATES) ; this parameter is included when deleting previously recorded subscriptions and defines a range of dates.
- PI = 'C0, 'C2 to 'C8 et 'CA to 'CF : Control parameters of the receiver modem.
- PI = 'C1 : Modem activation coordinates (MOD) for connection to the management centre during the receiver idle periods.
- PI = 'C9 : Wakeup coordinates (WAK) for the acquisition of entitlement management messages during the receiver idle periods.
- PI = 'D0 to 'D7 : Control parameters for authenticating the security processor by the receiver. These parameters are used to reconfigure or where appropriate, to inhibit the authentication procedure.
- PI = 'D8 : Individual message (INDMES) used when text is to be displayed for the customer.
- PI = 'EE : Parental code (PIN) ; this parameter is used for entering or updating the parental code (personal identification number).
- PI = 'EF : Secret key (CLE) ; this parameter is used for entering or updating a secret key.
- PI = 'F0 : Signature (HASH) ; this parameter provides a cryptographic compression of all sensitive data (in clear or encrypted) contained in the EMM. The EMM will not then be analysed and executed by the security processor unless it finds a match between the transmitted signature and the internally generated result of its own message compression procedure. It therefore entails cryptographic redundancy of the EMM parameters.
- PI = 'F1 : Group address (GA) ; this parameter is used during implementation of blackout or fingerprinting and provides a list of the groups of customers concerned. The parameter must match GCA parameter stored in the security processor.

- PI = 'F2 : Teletext service (SEI-TXT) ; this parameter indicates the reference for the teletext service used for replacement or fingerprinting.
- PI = 'F3 : Video signal replacement (TPP1) ; this parameter specifies the teletext page used to replace the video signal.
- PI = 'F4 : TV sound replacement (RCI-R1) ; this parameter describes the identification of the sound service replacing the TV sound.
- PI = 'F5 : Additional digital radio or teletext replacement (RCI-02, RCI-R2) ; this is used to configure the digital service used to replace an additional service.
- PI = 'F6 : Teletext page for fingerprinting (TPP2) ; this parameter is used when the finger-printing of the video signal by a specific teletext page is enabled.
- PI = 'F7 : Fingerprinting control (FCRL) ; this parameter comprises three separate data fields, FMOD, LOCUA, FDUR, which respectively represent the fingerprinting mode, the location of the unique address and the fingerprinting duration.

A group parameter PG, encoded '80, is introduced in order to combine the PI parameters described above. The associated length indicator PLI points to the end of the group of parameters which it covers. This parameter is used whenever a message requires more than one signature. This might apply, for example, when transmitting in the same message the first key of a service, followed by the service LABEL (see *Figure 5. 8*) :



A confidentiality parameter PC, encoded '81, is introduced for the purposes of scrambled data transmissions (to comply with privacy regulations). In this case, all the data in the message is scrambled (it consists of parameters with codes within the range 'A0 to 'EF). The length LC specifies the length of the scrambled data field (see *Figure 5.9*).



5.5.2 Grouping of parameters in the EMM

Four parameter groups are defined :

- Group 1 :

PG parameter (PGI = '80)

- Group 2 :

Parameters generating specific PC-EUROCRYPT commands.

- Subset 2.1 : this group is comprised of the following parameters :

PPID (PI = '90)

RND-ADF (PI = '91)

RND-CONF (PI = '92)

- Subset 2.2 : parameters having a PI comprised between '93 and '9F,

- Subset 2.3 : PC parameter (PCI = '81).

- Group 3 :

Parameters having a PI comprised between 'A0 and 'F0 inclusive, defined or undefined in this document.

- Group 4 :

Other parameters defined or undefined in this document.

- Subset 4.1 : parameters having a PI comprised between '00 and '7F,

- Subset 4.2 : parameters having a PI comprised between '82 and '8F,

- Subset 4.3 : parameters having a PI comprised between 'F8 and 'FF.

Parameters included between 'F1 and 'F7 are exclusively for EMM-C.

5.5.3 Parameter sequencing rules in the EMM-U and EMMG

– Rule A :

Only group 3 parameters are inserted between the PC parameter and the next HASH parameter.

– Rule B :

Two PG parameters are separated by a HASH parameter and vice-versa.

– Rule C :

In the absence of a PG parameter, between two PG parameters and following the last transmitted PG parameter, rules C-1, C-2, C-3, C-4 and C-5 apply.

- **Rule C-1** : group 2 parameters are transmitted in the 2.1, 2.2, 2.3 order, without inserting parameters from the other groups, before group 3 parameters and in strict increasing order within each subset,

- **Rule C-2** : the PPID parameter is mandatory and unique,

- **Rule C-3** : group 3 parameters are transmitted without inserting parameters from the other groups,

- **Rule C-4** :

- * Case of EMM-U and EMM-G common to the entire audience (with no associated EMM-S) :

- If group 3 parameters other than HASH are transmitted, the HASH parameter is mandatory and is necessarily the last one to be transmitted among group 3 parameters.

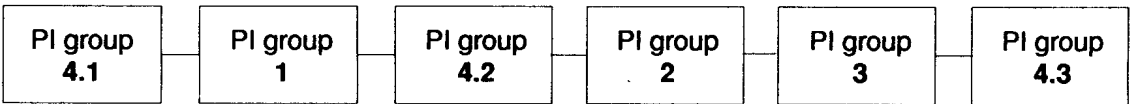
- * Case of EMM-G/EMM-S association :

- The HASH parameter is not included in the EMM-G. It is conveyed by the EMM-S.

- In the EMM-G, group 3 parameters are the last to be transmitted.

- **Rule C-5** : group 4.1 parameters are transmitted before parameters from other groups, those from group 4.2 are transmitted before the parameters from group 2 and those from group 4.3 are transmitted after parameters from other groups.

In conclusion, an EMM-U or EMM-G structure must conform to the following structure :



5.5.4 Software data SOFT

PI = '70
LI = length of software data
value = application number + software code
name = SOFT

This parameter is used where additional software is required to analyse the subsequent parameters. The software code transmitted updates the locally resident software. This function is implemented only if the ACS features software downloading capabilities. It is not used in the sample implementation of PC2, described in appendix 1.

- Application number (1 byte) : this parameter specifies the number of the application corresponding to the software code transmitted. This parameter may be used for execution by a local application.
- Software code : the subsequent data describe the software code which must be loaded into the ACS associated with the application number reference.

5.5.5 Programme provider identification PPID

PI = '90
LI = '03
value = programme provider identification
name = PPID

This parameter identifies the programme provider generating the EMM. This parameter is compulsory in EMM-U, EMM-G, and EMM-C.

The way in which this parameter is used differs slightly according to the type of operation carried out in the EMM message :

- if entering entitlements or updating customer addresses (see sections 6, 7 and 8), the parameter points to the memory area assigned to the programme provider in the ACS.
- the parameter points to the current key to provide secret word encryption or integrity checking functions.
- the parameter identifies the programme provider for replacement or fingerprinting (see section 9).

5.5.6 Random number (for address field descrambling) RND-ADF

PI = '91
LI = '08
value = random number
name = RND-ADF

This parameter is used to initialise the descrambling process on the address field ADF. It is not usually transmitted in EMM ; its (default) value is set to NOT(HASH) by the ACS.

5.5.7 Random number (for confidential data descrambling) RND-CONF

PI = '92
LI = '08
value = random number
name = RND-CONF

This parameter is used to initialise the confidential data descrambling process. Descrambling can be applied to the transmission of entitlements in EMM, or to the purchase survey via the modem. This parameter is not usually transmitted in EMM ; its (default) value is set to HASH by the ACS. In the purchase survey function, the random number is set to HASH.

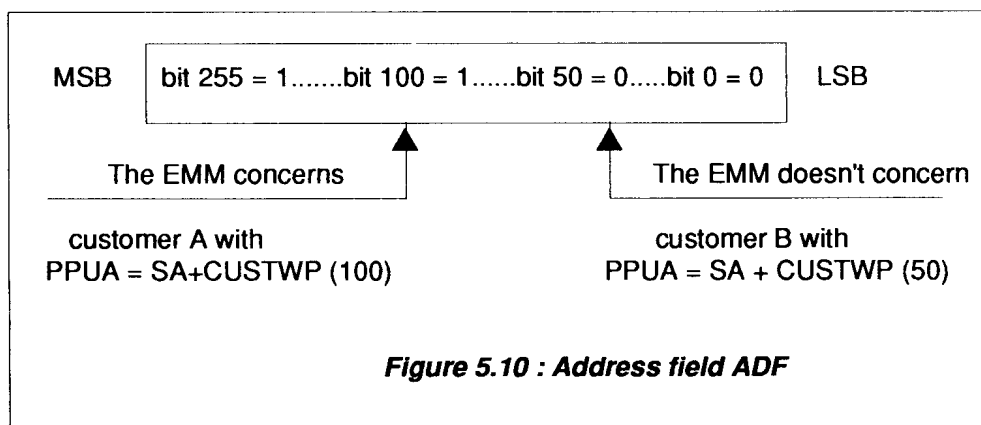
5.5.8 Programme provider or Issuer authentication

Programme provider authentication mandatorily precedes access via the modem to the audience survey function or to customer credit information. The process is in two stages: generation of the random number by the security processor and transmission to the programme provider, followed by computation based on the programme provider's service key. The result of the computation is sent to the security processor for verification. If there is a match with the computation performed internally by the security processor, the authentication phase is deemed successfully completed and the ACS accepts the instruction to run the audience survey function or to read the customer credit information. The exact definition of these parameters will be provided later.

5.5.9 Address field ADF

PI = '9E
LI = '20
value = address field
name = ADF

This 256-bit parameter specifies, for each customer in the group sharing the SA address of the EMM-S, whether the EMM-S concerns that customer or not. The customer's security processor points to the corresponding bit in the address field using the value of CUSTWP. The CUSTWP and SA fields are derived from the PPUA of the programme provider, PPID. The address field is used as described in *Figure 5.10*.



This field may also be scrambled before transmission. The ADF field is included (without PI LI format) in fixed format EMM-S.