SLOVENSKI STANDARD
SIST EN 50094:1999

01-april-1999

Access control system for the MAC/packet family: EUROCRYPT

Access control system for the MAC/packet family: EUROCRYPT

Zugriffskontrollsystem für die MAC/Paket-Familie: EUROCRYPT

Système d'accès conditionnel pour la famille MAC/paquet: EUROCRYPT

Ta slovenski standard je istoveten z: **EN 50094:1992**

ICS:

33.170	Televizijska in radijska difuzija	Television and radio broadcasting

SIST EN 50094:1999 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50094

December 1992

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

Système d'accès conditionnel pour la famille MAC/paquet: EUROCRYPT

Zugriffskontrollsystem für die MAC/ Paket-Familie: EUROCRYPT

This European Standard was approved by CENELEC on 9 December 1992. CENELEC members are bound to comply with the requirements of 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 and 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).

Following patent holders subscribed the above conditions:

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

CONTENTS

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 recommandations 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 refering 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 modifiyng keys associated with the service

Legend of Figure 2.1

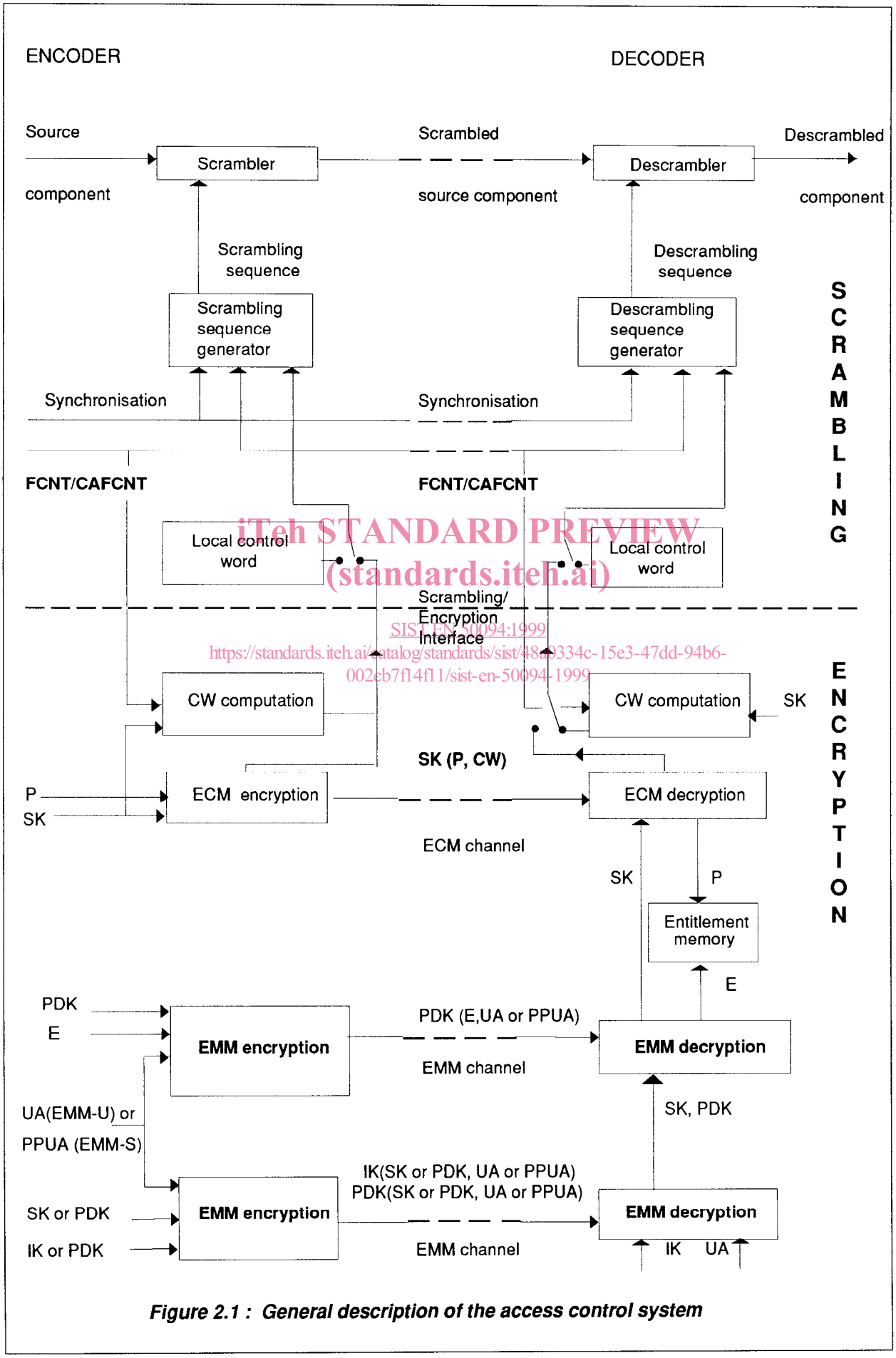

Figure 2.1 : General description of the access control system

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 programm 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 maturarity 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.