SLOVENSKI STANDARD
SIST EN 50094:1999/A1:1999

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/A1:1995**

ICS:

33.170	Televizijska in radijska difuzija	Television and radio broadcasting

SIST EN 50094:1999/A1:1999 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50094/A1

February 1995

UDC 621.396:534.86:621.397
ICS 33.160.20

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 amendment A1 modifies the European Standard EN 50094:1992; it was approved by CENELEC on 1994-12-06. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this amendment 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 amendment 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

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

- ANNEX 5 -

(INFORMATIVE)

CLARIFICATIONS AND ANSWER TO QUESTIONS

ABOUT THE EN 50094 STANDARD

1. SUBJECT

This informative annex contains clarifications and answer to questions that occured when publishing the EN 50094 standard. It refers to the EUROCRYPT specification unless otherwise stated.

2. MAC/packet RELATED ASPECTS

2.1 Access mode

When deciding the access mode (between clear, free access scrambling, and controlled access scrambling), the receiver shall give the highest priority to the real time information as described in the D2-MAC/packet specification (Ref. 1, Part 5, section 3.1). This information is contained :
- in the component itself : BI and BC1/BC2 for the sound component and PT for teletext
- in line 625 for the video component (VSAM).

A lower priority must be given to the SI parameters which are uptaded less frequently (VCONF for the video component, and DCINF for the sound components)

When an ACCM parameter is linked to components within a command or a parameter group, the decoder must process the corresponding ECM even if the real time information indicates that the component is in clear or free access (see Section 11.3.2 and 12).

2.2 SI channel information

The description and the status of the SI channel information, within optional or mandatory, are given in the D2-MAC/packet specification (Ref. 1, Part 5, section 2 and Part 8, section 6).

2.3 Line 625 data

The description and the status of the line 625 data, within optional or mandatory, are described in the D2-MAC/packet specification (Ref. 1, Part 1, section 5 and Part 8).

3. EUROCRYPT SPECIFICATION RELATED ASPECTS

Section 4. Signals crossing the Access Control Interface

Section 4 outlines the principles of the receiver-ACS interface, and not a particular implementation such as the interface between the PC-EUROCRYPT card and the receiver. In the PC-EUROCRYPT implementation, the ACS contains the card reader with its software and the PC-EUROCRYPT card. The PC-EUROCRYPT smart card described in Appendix 1 is the security device of the ACS. The ACS software includes the smart card exchange protocol and the access control-related man/machine dialogue. The receiver-ACS interface respects the principles described in Section 4.

Section 5.3. Command Identifier CI - Algorithm values

Other algorithms than '20 can be used. Algorithm indicated value '20 is allocated for the PC2 card. The algorithm value of the PC-EUROCRYPT card is contained in a FAC block of the card as described in Appendix 4, Section 3.1. This value must be matched with the algorithm value indicated when present in the ACCM and ACMM parameters, and in the CI byte of the ECM and EMM respectively.

Section 5.5.4. Software data SOFT

The SOFT parameter is a receiver-related parameter. It has been specified for software downloading within the receiver. It is not used today and must be ignored by the receiver but this will not cause the message to be rejected, as described in Section 5.1.

Section 5.5.8. Programme provider or issuer authentication

The programme provider or issuer authentication is used when a purchase survey is done by a receiver. The receiver is then connected via a modem to the programme provider or issuer management centre. The security processor provides the receiver with a random number for authentication (Appendix 1, Section 6.15.1) and the receiver transmits it to the management centre. When receiving the result of the computation from the management centre, the receiver sends it to the security processor to achieve the authentication process (Appendix 1, Section 6.15.2). The authentication process is then achieved and the security processor accepts the instruction to run the purchase survey. These functions are described in Appendix 1, Sections 5.4 and 6.15. The modem is an optional function of the receiver.

Section 5.5.10. Control CTRL - Free entitlement

The content of the man-machine dialogue, in particular for free entitlement, between the receiver and the user is manufactor-related and is not part of the specification. The receiver can also systematically acquire the free initial entitlement as described in the footnote on page 46 and in Appendix 3, Section 9.3.

Section 5.5.13. General purpose data FAC

FAC blocks broadcast over-the-air in EMM will be destinated to the PC-EUROCRYPT card, and will be processed like any EMM Group 3 parameter (see Section 5.2 and 5.3, and Appendix 3, Section 6). The receiver will be transparent for this information. The outgoing FAC blocks from the PC-EUROCRYPT card will be processed by the receiver as described in Appendix 3, Sections 9.5, 9.6, 9.7, 11.2 and in Appendix 4, Section 3.

Section 5.5.17. LABEL parameter

No language option is described in the definition of the LABEL parameter. The LABEL parameter contains the "commercial name" of the programme provider (Example : CNN, TV3, CANAL+).

Section 5.5.24. SURVEY

The SURVEY parameter is sent within an entitlement management message when completing a purchase survey operation. It is processed by the PC-EUROCRYPT card like any other EMM Group 3 parameter. The receiver will be transparent for this information (see Appendix 1, Section 6.11.11).

Section 5.5.26. Receiver modem control parameters

These parameters are reserved code values. They must be ignored by the receiver

Section 5.5.27. Modem activation coordinates MOD

When receiving a MOD parameter, the receiver that contains a modem will programm its modem call time and call number. It may find the time and date reference for programming the modem in the D2-MAC/packet signal itself (in line 625 for the real-time information) or have a local clock. The rules of implemention of the modem are described in the Appendix 2, Section 7.3.6, and the Appendix 3, Section 11.2.

Section 5.5.28. Wakeup coordinates WAK

The receiver may find the time and date reference for programming the wakeup in the D2-MAC/packet signal itself (in line 625 for the real-time information) or have a local clock. One WAK parameter is associated to one channel. The receiver must manage the corresponding tables if several wakeup times can be stored. The rules of implemention of the wakeup are described in the Appendix 2, Section 7.3.5, and in the Appendix 3, Section 11.1.

Section 5.5.29. Authentication control parameters

These parameters are reserved code values for an authentication control mechanism. They must be ignored by the receiver, as described in Section 5.1.

Section 5.5.30. Individual messages INDMES

The page reference and the teletext magazine used in the INDMES parameter are described in the CCIR system B teletext specification. The INDMES message is displayed on agreement from the customer for a letter-box stored message. The way the INDMES page shall be cleared depends on the storage capacity and is manufactor-related. The receiver implementation is described in Appendix 3, Section 9.4.

Section 5.5.36. Video signal replacement TPP1

The page reference and the teletext magazine used in the TPP1 parameter are described in the CCIR system B teletext specification.

Section 5.5.37. TV sound replacement RCI-R1

The receiver shall select the replacement sound on its LISTX parameter **and** its language code. The replacement sound (LISTX = 'AA in the SI channel) will be selected first if its language code corresponds to the language code of the RCI-R1 parameter.

Section 5.5.38. Additional service replacement RCI-O2, RCI-R2

The receiver shall select the replacement sound on its LISTX parameter **and** its language code. The replacement sound (LISTX = 'AA in the SI channel) will be selected first if its language code corresponds to the language code of the RCI-R2 parameter.

Section 5.5.40. Fingerprinting control FCTRL

The locally-generated page (FMOD = 2, or FMOD = 3) shall be displayed as a CCIR system B teletext page.

Section 7 & 8. EMM-G and EMM-S sequencing

Rules of operation are under study for the EMM sequencing.

Section 9. EMM-C

The same structure is used for all EMM. All EMM contain a CI code even if all the EMM data are processed by the receiver. Furthermore, the CI code can be used for EMM selection in case of multialgorithm broadcasting.

Section 10.4.11. Programme number PNUMB and Programme cost PPV/P

The definition of the man-machine dialogue for impulse pay-per-view is manufactor-related and is not part of the specification. The user must give his agreement to each new programme purchase. The need for agreement is signalled by the PC2 smart card by setting the bit DPPV/P. The PC2 related-information for the use of pay-per-view is described in Appendix 1, Section 6.9.

Section 10.4.12. Programme number PNUMB + Cost per time unit PPV/T

The receiver programms or modifies the Ceiling (COUTMAX) by the use of a man-machine dialogue. The definition of the man-machine dialogue for impulse pay-per-view per time is manufactor-related and is not part of the specification. The user must give his agreement for each new programme purchase or when the Ceiling is overreached till the last agreement. In that case, the PC2 smart card set the bit DPPV/T to 1. The PC2 related-information for the use of pay-per-view is described in Appendix 1, Section 6.9.

Section 10.5. Description of ECM messages with examples - PPV/P + PPV/T

Pay-per-view per programme and pay-per-view per time may occur simultaneously. The definition of the man-machine dialogue is manufactor-related and is not part of the specification.

Section 11.1.2. Static data frame - Replacement and Fingerprinting

If replacement and fingerprinting are used simultaneously by the programme provider, the replacement shall be given the highest priority.

Rp and Fp bits are allocated in the D2-MAC/packet specification (Ref. 1, Part 1, Section 5.3).

Section 11.3.2. Description of service components - ACCM and ACMM

Only the first byte of the parameter field in the ACCM and ACMM parameters shall be processed by the receiver when present, it contains the cryptoalgorithm byte, and will be compared to the cryptoalgorithm type of the security processor as described in the operating regulations (Appendix 2, Section 7.3.2). Any other byte must be ignored by the receiver.

The definition of the ACCM parameter is coherent with the D2-MAC/packet specification (Ref. 1, Part 5, Section 2.3).

Section 11.3.3. Commands and parameters - Multiple access conditions

No maximum value has been allocated to the number of access conditions that control a service. The receiver must analyse the ACCM or ACMM parameters untill it finds the corresponding CI code.

Section 11.3.4. Table 1 - Multiple ACMM

The ACMM parameter can only be present in the over-the-air adressing service command (CI = 'C0) as described in the operating regulations (Appendix 2, Section 7.3.3).

4. APPENDIX 1 : PC-EUROCRYPT RELATED ASPECTS

General remarks

The sequence and the context of the different commands are described in Appendix 1, Section 5.

The presence of an error bit indicates that the smart card can't be used for that function. Two errors bits can't be set simultaneously since that card stops the command processing when the first error occurs. The warning bits can be set simultaneously.

The receiver behaviour is described in the minimal terminal specification (Ref. 2).

Section 6.2. Reset - Historical characters

The receiver shall not interpret the historical characters in the answer to reset.

Section 6.3. Select a service or issuer

The receiver shall apply the entity selection each time a new Service Identifier is selected in ECM or EMM processing. It must select the Issuer entity when managing PIN code controlled operations (Section 6.4) or when accessing the data that are stored under the Issuer entity.

Section 6.3.3. Select entity direct - IDENT parameter

IDENT is the Service Identifier (20 MSB) in the PPID parameter of an ECM or EMM (see Section 4.2 of the specification, page 27).

Section 6.3.4. Status words - AA bit

The receiver reaction on an AA status bit depends on the processed function. When processing an ECM, the receiver shall display an error message, as described in the minimal terminal specification (Ref. 2). When processing an EMM, the receiver shall reject the EMM.

Section 6.4.5. Status words - MVAUTH, EI, IE/IL, PBABS bits

When the smart card signals the following status bits, the receiver shall react the following way :

MVAUTH : No maximum number of PIN code entering is managed by the PC2 smart card. The receiver may allow the user to enter his PIN code an other time.

EI and IE/IL : The receiver shall indicate that a smart card failure has occured as described in the minimal terminal specification.

PBABS : The receiver shall indicate that an error has occured as described in the minimal terminal specification.

Section 6.5. Modify the preselection area

The preselection area allows the PC2 card to bypass the man-machine dialogue in case of ECM processing (maturity rating and pay-per-view). The receiver must generate the corresponding man/machine dialogue.

Section 6.8.2. Status words - PBABS bit

When the PBABS status bit is set by the smart card, the receiver will be blacked-out.

Section 6.9.1. Command format - I index of the key

I is the Index (4 LSB) in the PPID parameter (see Section 4.2 of the specification, page 27).

Section 6.9.2. Status words - DENTAM, MAC, HF, SF, ADI bits

When detecting an error in the case of ECM processing, the receiver shall generate an automatic response message to the user as described in the minimal terminal specification (Ref. 2).

Section 6.10.3. Status words - PBABS bit

The PBABS status bit is set by the smart cardwhen it has no PPUA for that entity. The receiver can't read any SA for that entity, it can't select the corresponding EMM-S and must reject the EMM.

Section 6.11. Enter information - MVSQ/L status bit

In case of EMM processing, the MVSQ/L bit is set when the PPID is not the correct one in the EMM. The receiver must reject the EMM, whatever the combination of the parameters in the EMM.

Section 6.11.2. Status words common to all commands - PNI status bit, UA

The PNI bit is set when the EMM includes one or several parameters which cannot be interpreted by the card. These parameters can be receiver-related (Example : MOD, WAK, INDMES). The receiver must analyse the EMM and process these receiver-related parameters.

The card may not contain a Unique Address. This can be the case for "single-event" cards.

Section 6.11.3. Enter or modify descriptor - PBMODE, PBTAIL status bits

When the PBMODE or PBTAIL status bit is set by the smart card, the receiver must reject the EMM.

Sections 6.11.4 to 6.11.13. PBVER, PBTOTA, PBDATE, MAC, PBFAC, AA, PBDEBO status bits

When one of these status bits is set by the smart card, the receiver must reject the EMM.

Section 6.11.12. Enter a free initial entitlement - PBGRAT status bit

The PBGRAT status bit is set when an entitlement is already stored in the service entity. The free initial entitlement is not stored. The receiver must then reject the EMM.

Section 6.13.3. Delete service entity - PBINV status bit

When the PBINV status bit is set by the smart card, the receiver must reject the EMM.