

Zugriffskontrollsysteme für die MAC/Paket-Familie: EUROCRYPT

Deutsche Fassung EN 50094 : 1992/A1 : 1995

DIN

EN 50094/A1

ICS 33.160.20

Deskriptoren: Fernseh Rundfunk, Rundfunk, EUROCRYPT, Zugriff, Kontrolle

Access control systems for the MAC/packet family: EUROCRYPT;

German version EN 50094 : 1992/A1 : 1995

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

Version allemande EN 50094 : 1992/A1 : 1995

Die Europäische Norm EN 50094 : 1992/A1 : 1995 hat den Status einer Deutschen Norm.

Nationales Vorwort

Für die vorliegende Norm ist das nationale Arbeitsgremium UK 742.4 "Rundfunk-Empfangsgeräte und verwandte Geräte und Systeme der Unterhaltungselektronik" der Deutschen Elektrotechnischen Kommission im DIN und VDE (DKE) zuständig.

Der Norm-Inhalt war veröffentlicht als E DIN EN 50094/AA : 1994-07 und E DIN EN 50094/AB : 1994-07.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist nachstehend wiedergegeben.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Zum Zeitpunkt der Veröffentlichung dieser Norm waren die angegebenen Ausgaben gültig.

Europäische Norm	Deutsche Norm
ETS 300250 : 1993	DIN ETS 300250 : 1994-08

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ETS 300250

Fernseh-Systeme — Festlegung des D2-MAC/Paket-Systems; Englische Fassung ETS 300250 : 1993

Fortsetzung 18 Seiten EN

Deutsche Elektrotechnische Kommission im DIN und VDE (DKE)

ICS 33.160.20

Deskriptoren: Rundfunkübertragung, Fernseh-Rundfunk, Ton-Rundfunk, Fernsehsendung, Netzwerkzugriff für Benutzer, Spezifikation

Deutsche Fassung

**Zugriffskontrollsysteme
für die MAC/Paket-Familie: EUROCRIPT**

Access control systems for the MAC/
packet family: EUROCRIPT

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

Diese Änderung A1 modifiziert die Europäische Norm EN 50094 :1992. Sie wurde von CENELEC am 1994-12-06 angenommen.

Die CEN/CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Änderung besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen. CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien und dem Vereinigten Königreich.

CENELEC

EUROPÄISCHES KOMITEE FÜR ELEKTROTECHNISCHE NORMUNG
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

Vorwort

Diese Änderung wurde vom CENELEC/Technischen Komitee TC 106 "Rundfunk-Empfangseinrichtungen" erarbeitet.

Der Text des Entwurfs wurde als prAA und prAB dem Einstufigen Annahmeverfahren (UAP) unterworfen und am 1994-12-06 von CENELEC als Änderung A1 zur EN 50094:1992 genehmigt.

Folgende Daten wurden festgelegt:

- spätestes Datum der Veröffentlichung
einer identischen nationalen Norm (dop): 1995-12-01
- spätestes Datum der Zurückziehung
entgegenstehender nationaler Normen (dow): 1995-12-01

**- ANHANG 5 -
(INFORMATIV)**

KLARSTELLUNGEN UND ANTWORT AUF FRAGEN BEZÜGLICH DER NORM EN 50094

1 Gegenstand

Dieser informative Nachtrag enthält Klarstellungen und Antwort auf Fragen, die bei der Veröffentlichung der Norm EN 50094 aufkamen. Er bezieht sich auf die EUROCRYPT-Spezifikation, soweit nichts anderes angegeben ist.

2 Auf MAC/Paket bezogene Aspekte

2.1 Zugriffsverfahren

Bei der Entscheidung über das Zugriffsverfahren (zwischen Klartext, Verschlüsselung mit freiem Zugriff und Verschlüsselung mit kontrolliertem Zugriff) muß der Empfänger der Echtzeit-Information, wie sie in der D2-MAC/Paket-Spezifikation (Lit. 1, Teil 5, Abschnitt 3.1) beschrieben ist, die höchste Priorität geben. Diese Information ist enthalten:

- in der Komponente selbst: BI und BC1/BC2 für die Ton-Komponente sowie PT für Teletext,
- in Zeile 625 für die Video-Komponente (VSAM).

Eine niedrigere Priorität ist den SI-Parametern zu geben, die weniger häufig aktualisiert werden (VCONF für die Video-Komponente und DCINF für die Ton-Komponenten).

Wenn ein ACCM-Parameter mit Komponenten innerhalb eines Befehls oder einer Parameter-Gruppe verknüpft ist, dann muß der Dekoder die zugehörige ECM verarbeiten, auch wenn die Echtzeit-Information angibt, daß die Komponente in Klartext oder freiem Zugriff ist (siehe Abschnitte 11.3.2 und 12).

2.2 SI-Kanal-Information

Beschreibung und Status der SI-Kanal-Information, im Rahmen von frei wählbar oder verbindlich, sind in der D2-MAC/Paket-Spezifikation (Lit. 1, Teil 5, Abschnitt 2, und Teil 8, Abschnitt 6) angegeben.

2.3 Daten in Zeile 625

Beschreibung und Status der Daten in Zeile 625, im Rahmen von frei wählbar oder verbindlich, sind in der D2-MAC/Paket-Spezifikation (Lit. 1, Teil 1, Abschnitt 5, und Teil 8) beschrieben.

3 Auf die EUROCRYPT-Spezifikation bezogene Aspekte

Abschnitt 4 Signale an der Schnittstelle der Zugriffskontrolle

Abschnitt 4 gibt die Prinzipien der Schnittstelle des Empfänger-ACS an, nicht aber eine besondere Ausführung, wie z. B. bei der Schnittstelle zwischen der PC-EUROCRYPT-Karte und dem Empfänger. In der PC-EUROCRYPT-Ausführung enthält das ACS den Karten-Leser einschließlich seiner Software und die PC-EUROCRYPT-Karte. Die PC-EUROCRYPT-Smart-Card, die im Anhang 1 beschrieben ist, stellt die Sicherheitseinrichtung des ACS dar. Die ACS-Software schließt das Smart-Card-Austauschprotokoll und den auf die Zugriffskontrolle bezogenen Mensch/Maschine-Dialog ein. Die Empfänger-ACS-Schnittstelle unterstützt die Prinzipien, wie sie in Abschnitt 4 beschrieben sind.

Abschnitt 5.3 Befehlskennung CI - Algorithmus-Werte

Andere Algorithmen als '20 können verwendet werden. Der Algorithmus-Anzeigewert '20 ist für die PC2-Karte zugewiesen. Der Algorithmuswert der PC-EUROCRYPT-Karte ist in einem FAC-Block der Karte enthalten, wie im Anhang 4, Abschnitt 3.1, beschrieben. Dieser Wert muß dem angezeigten Algorithmuswert angepaßt werden, wenn er in den ACCM- und ACMM-Parametern bzw. im CI-Byte der ECM und EMM vorhanden ist.

Abschnitt 5.5.4 Softwaredaten SOFT

Der SOFT-Parameter ist ein empfängerbezogener Parameter. Er wurde für die Software-Nachladung im Empfänger festgelegt. Heutzutage wird er nicht benutzt, und er muß vom Empfänger ignoriert werden, was aber nicht dazu führt, daß die Nachricht zurückgewiesen wird, wie im Abschnitt 5.1 beschrieben.