

Zugriffskontrollsysteme für die MAC/Paket-Familie: EUROCRYPT

Deutsche Fassung EN 50 094 : 1992

DIN
EN 50 094

Access Control System for the MAC/Package Family: EUROCRYPT; German Version EN 50 094 : 1992

Système d'accès conditionnel pour la famille MAC/paquet: EUROCRYPT; version allemande EN 50 094 : 1992

Die Europäische Norm EN 50 094 : 1992 hat den Status einer Deutschen Norm.

Nationales Vorwort

Diese Norm beinhaltet die Deutsche Fassung der vom Technischen Komitee TC 106 „Broadcast receiving equipment“ des Europäischen Komitees für Elektrotechnische Normung (CENELEC) ausgearbeitete Norm EN 50 094. Das zuständige deutsche Arbeitsgremium ist das UK 731.2 „MAC-Empfangseinrichtungen“ der Deutschen Elektrotechnischen Kommission im DIN und VDE (DKE).

Der Norm-Inhalt war veröffentlicht als Entwurf DIN EN 50 094/01.92

Fortsetzung 195 Seiten EN-Norm

Deutsche Elektrotechnische Kommission im DIN und VDE (DKE)


Documents
 Document Sharing Hub

DK 621.396 : 534.86 : 621.397

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

Deutsche Fassung

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

Access Control System for the MAC/Packet
Family:
EUROCRYPT

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

Diese Europäische Norm wurde von CENELEC am 1992-12-09 angenommen.

Die CEN-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 CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm 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 die 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

Auf Veranlassung des Technischen Komitees TC 106 "Rundfunk-Empfangsanlagen" von CENELEC wurde der Text dieser Europäischen Norm den CENELEC Mitgliedern im August 1992 zur offiziellen Abstimmung vorgelegt und von CENELEC am 9. Dezember 1992 als EN 50094 angenommen.

Folgende Termine wurden festgelegt:

- spätestes Datum der Veröffentlichung
einer identischen nationalen Norm (dop) 30.06.1993
- spätestes Datum der Zurückziehung
entgegenstehender nationaler Normen (dow) 30.06.1993

Das EUROCRYPT System, wie es in dieser Norm beschrieben wird, ist Gegenstand von Patentrechten.

In Übereinstimmung mit dem CEN/CENELEC Memorandum 8 über Normung und Rechte an geistigem Eigentum (Standardization and Intellectual Property Rights (IPR)) wurde eine Erklärung von den Patenthaltern des EUROCRYPT Systems erreicht, in der sie ihre Bereitschaft zu Lizenzverhandlungen unter folgenden Bedingungen bestätigen:

- keine Exklusivität;
- Anwendung auf das MAC/Paket bezogene Zugriffskontrollsystem EUROCRYPT;
- das Vertragsgebiet umfaßt EG, EFTA und andere Länder, die das MAC-Signal von einem europäischen Satelliten empfangen;
- die Konditionen müssen annehmbar und nicht einseitig begünstigend sein (der Ausdruck 'annehmbar' wird wie im Hauptanwendungsbereich der Elektronik üblich ausgelegt; der Ausdruck 'nicht einseitig begünstigend' bezieht sich auf Lizenzbedingungen, die nicht von der Identität oder der Nationalität des Lizenznehmers abhängig sind).

Folgende Patenthalter haben die vorstehenden Bedingungen unterschrieben:

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

INHALT

1	Gegenstand.....	7
2	Allgemeine Beschreibung des Zugriffskontrollsystems	8
2.1	Das Scrambling- und das Verschlüsselungssystem.....	8
2.2	Initialisierung und Aktualisierung der Dienst-Schlüssel (Verwaltung oder Betrieb).....	11
2.3	Funktionen	11
3	Scrambeln von Ton, Daten und Bildern.....	13
3.1	Einleitung	13
3.2	Beschreibung des Scrambling-Verfahrens für Ton und Daten	13
3.3	Erzeugung der Descramblersequenzen	13
3.4	Synchronisierung der Descramblersequenzen.....	14
4	Signale, an der Schnittstelle der Zugriffskontrolle.....	23
4.1	Schnittstelle zwischen Empfangsgerät und Zugriffskontrollsystem	23
4.1.1	Konfigurierung der Schnittstelle zwischen Empfangsgerät und ACS	23
4.1.2	Signale, die vom ACS empfangen werden.....	23
4.1.3	Signale vom ACS	26
4.1.3.1	Im ACS erzeugte Kontrollmeldungen	26
4.1.3.2	Im ACS erzeugte Bildschirm-Meldungen	26
4.2	Die Dienst-Kennung und die Verbindung zu den Kontrollwörtern	27
4.3	Erzeugung und Zuweisung von Kontrollwörtern.....	29
4.3.1	Erzeugung von Kontrollwörtern	29
4.3.2	Zuweisung und Synchronisierung der Kontrollwörter	29
5	Allgemeine Beschreibung der Berechtigungs-Verwaltungsmeldungen (EMM).....	30
5.1	Formate der Meldungen	30
5.2	Teilnehmeradressen.....	33
5.3	Befehlskennung CI.....	36
5.4	Befehlslängenangabe CLI.....	37
5.5	Parameter-Kennung PI.....	37
5.5.1	Verzeichnis der möglichen Parameter bei EMM-Meldungen	37
5.5.2	Parametergruppen bei EMM	41
5.5.3	Vorschriften zur Reihenfolge der Parameter in den EMM-U und EMM-G.....	42
5.5.4	Softwaredaten SOFT	43
5.5.5	Programmanbieter-Kennung PPID.....	43
5.5.6	Zufallszahl RND-ADF (zur Descramblung des Adreßfeldes).....	43
5.5.7	Zufallszahl RND-CONF (zur Descramblung von vertraulichen Daten)	44
5.5.8	Authentizitätsprüfung des Programmanbieters oder des Herausgebers	44
5.5.9	Adreßfeld ADF	44
5.5.10	Kontrolle CTRL.....	45
5.5.11	Identifizierung von Aktualisierungsdaten IDUP	47
5.5.12	Deskriptor DESCR	47

5.5.13	Allgemeine Daten FAC.....	48
5.5.14	Einzeladresse UA	49
5.5.15	Programmanbieter-Nutzeradresse PPUA	49
5.5.16	Gruppenteilnehmeradresse GCA.....	49
5.5.17	LABEL-Parameter.....	50
5.5.18	Datumsangaben DATES + Thema/Klasse TH/LE.....	50
5.5.19	DATES + Spartenverzeichnis CUSTWD.....	52
5.5.20	Anfangs- und Endprogrammnummern INUMB + FNUMB	53
5.5.21	DATE + CREDIT	54
5.5.22	DATE + Gesamtguthaben TOTAM	55
5.5.23	DATE + Überziehungskredit OVER	55
5.5.24	SURVEY	57
5.5.25	DATES.....	57
5.5.26	Empfängermodem-Kontrollparameter.....	58
5.5.27	Modem-Aktivierungskordinaten MOD.....	58
5.5.28	Die Weckruf-Kordinaten WAK	60
5.5.29	Authentizitätskontrollparameter.....	61
5.5.30	Individuelle Meldungen INDMES.....	61
5.5.31	Personenkennummer PIN (Eltern-Kode).....	62
5.5.32	Geheimschlüssel CLE.....	62
5.5.33	HASH-Signatur	63
5.5.34	Gruppenadresse GA	63
5.5.35	Teletext-Dienst SEI-TXT	64
5.5.36	Videosignal-Ersatz TPP1	64
5.5.37	Fernsehton-Ersatz RCI-R1.....	65
5.5.38	Ersatz für weitere Dienste RCI-02, RCI-R2	65
5.5.39	Teletext-Seite für Fingerprint TPP2.....	66
5.5.40	Fingerprint-Kontrolle FCTRL	66
5.6	Meldungen mit festem Format (F = 0 im CI-Parameter)	67
6	Verwaltungsmeldungen zur Einzelteilnehmerberechtigung (EMM-U)	68
6.1	Datenformat.....	68
6.1.1	Befehlskennung (CI)	68
6.1.2	BefehlsLängenangabe CLI.....	68
6.2	EMM-U-Meldungen für Sende-Adressierung	68
6.2.1	Verzeichnis der möglichen Parameter bei EMM-U-Meldungen	69
6.2.2	Beschreibung der Parameter	71
6.2.3	Beschreibung von EMM-U-Meldungen anhand von Beispielen	72
6.2.3.1	Erstverbindung eines Teilnehmers mit dem Verwaltungszentrum des Programmanbieters.....	72
6.2.3.2	Individuelle Berechtigungen	72
6.2.3.3	Ungültigmachung oder Löschung von Berechtigungen	75
7	Meldungen für sämtliche Teilnehmer (EMM-G)	76
7.1	Einleitung	76
7.2	Datenformat.....	76
7.2.1	Befehlskennung CI.....	76
7.2.2	BefehlsLängenangabe CLI.....	76
7.3	EMM-G-Meldungen für Sende-Adressierung	76
7.3.1	Verzeichnis der möglichen Parameter bei EMM-G-Meldungen	77
7.3.2	Verwendung von EMM-G-Meldungen	79
7.3.2.1	Freie Erstberechtigung oder Berechtigung für sämtliche Teilnehmer	79
7.3.2.2	Gemeinschaftsberechtigung	79

7.3.3	Beschreibung der Parameter	80
7.3.3.1	Freie Erstberechtigung und Berechtigung für sämtliche Teilnehmer	80
7.3.3.2	Gemeinschaftsberechtigungen	80
7.3.4	Darstellung von EMM-G-Meldungen anhand von Beispielen	81
7.3.4.1	Freie Erstberechtigung oder Berechtigung für sämtliche Teilnehmer	81
7.3.4.2	Gemeinschaftsberechtigungen	82
8	Meldung für Gemeinschaftsteilnehmergruppen (EMM-S).....	83
8.1	Einleitung	83
8.2	Datenformat	83
8.2.1	Befehlskennung CI	83
8.2.2	BefehlsLängenangabe CLI	84
8.3	EMM-S-Meldungen für Sende-Adressierung	84
8.3.1	Verzeichnis der möglichen Parameter bei EMM-S-Meldungen	84
8.3.1.1	EMM-S mit festem Format	84
8.3.1.2	EMM-S mit variablem Format	84
8.3.2	Beschreibung der Parameter	84
8.3.2.1	EMM-S mit festem Format	84
8.3.2.2	EMM-S mit variablem Format	84
8.3.3	Darstellung von EMM-S-Meldungen anhand von Beispielen	85
9	Meldungen zur Verwaltung von Kollektivberechtigungen (EMM-C).....	87
9.1	Datenformat	87
9.1.1	Befehlskennung CI	87
9.1.2	BefehlsLängenangabe CLI	87
9.2	EMM-C-Meldungen für Sende-Adressierung	87
9.2.1	Verzeichnis der möglichen Parameter bei EMM-C-Meldungen	88
9.2.2	Verwendung von EMM-C-Meldungen	88
9.2.3	Beschreibung der Parameter	89
9.2.4	Beschreibung von EMM-C-Meldungen anhand von Beispielen	89
10	Beschreibung der Berechtigungs-Kontrollmeldungen (ECM).....	90
10.1	Format der Meldung	91
10.3	BefehlsLängenangabe CLI	92
10.4	Parameterkennung PI	92
10.4.1	Verzeichnis der möglichen Parameter bei EMC-Meldungen	93
10.4.2	Parametergruppen in ECM	94
10.4.3	Vorschriften zur Reihenfolge der Parameter in ECM	94
10.4.4	Software-Daten SOFT	95
10.4.5	Programmanbieter-Kennung PPID	95
10.4.6	Globale Gruppenadresse GGA	96
10.4.7	Kontrolle CTRL	98
10.4.8	Sendedatum CDATE + Thema/Klasse THEME/LEVEL	99
10.4.9	Sendedatum CDATE + Programmsparte LINK	100
10.4.10	Programmnummer PNUMB	100
10.4.11	Programmnummer PNUMB und Programmpreis PPV/P	101
10.4.12	Programmnummer PNUMB + Preis pro Zeiteinheit PPV/T	101
10.4.13	Geradzahliges verschlüsseltes Kontrollwort ECW	102
10.4.14	Ungeradzahliges verschlüsseltes Kontrollwort OCW	102
10.4.15	Geradzahliges und ungeradzahliges verschlüsseltes Kontrollwort ECW/OCW	103
10.4.16	HASH-Signatur	103

10.5	Beschreibung von ECM-Meldungen anhand von Beispielen	104
10.5.1	Themen- bzw. klassengebundenes Abonnement	104
10.5.2	Sparten-Abonnement bei aktiviertem Blackout	104
10.5.3	Pay-per-view pro Programm mit Impulsabbuchung	105
10.5.4	ECM-Meldung für verschiedene Zugriffsbedingungen	105
11	Nähere Ausführungen zur Implementierung der in der Spezifikation beschriebenen Zugriffskontrollmöglichkeiten	107
11.1	Teil 1	107
11.1.1	Einleitung	107
11.1.2	Abschnitt 5.3 - Statischer Datenrahmen (SDF)	107
11.1.3	Abschnitt 5.4 - Mehrfachdatenrahmen	108
11.2	Teil 2	109
11.2.1	Abschnitt 7 - Bilder mit vergrößertem Format	109
11.3	Teil 5	109
11.3.1	Einleitung	109
11.3.2	Abschnitt 2.3 - Beschreibung von Dienst-Bestandteilen	109
11.3.3	Abschnitt 3.1 - Anweisungen und Parameter	111
11.3.4	Tabelle 1	111
ANHANG 1:	BEISPIELE FÜR DIE KODIERUNG DES DIENST-IDENTIFIKATIONSKANALS MIT DER PARAMETER-GRUPPENKENNUNG PGI	112
12	Umschaltungs-Zeitdiagramme	114
12.1	Einleitung	114
12.2	Inhalt der Umschaltungs-Zeitdiagramme	114
12.3	Erzeugung eines Dienst-Bestandteils bei kontrolliertem Zugriff	115
12.4	Umschalten eines Dienst-Bestandteils auf kontrollierten Zugriff	116
12.5	Ändern der Zugriffsbedingungen für einen Dienst-Bestandteil	117
12.6	Umschalten eines Dienst-Bestandteils von kontrolliertem Zugriff auf ungescrambelten oder freien Zugriff	118
12.7	Reorganisierung von Dienst-Bestandteilen und Zugriffsbedingungen	119
12.7.1	Umstellen von zwei Dienst-Bestandteilen mit verschiedenen Zugriffsbedingungen auf die Zugriffsbedingung des ersten Dienst-Bestandteils ...	120
12.7.2	Trennung von zwei Dienst-Bestandteilen, wobei einer die ursprüngliche Zugriffsbedingung beibehält	121
12.7.3	Umstellen von zwei Dienst-Bestandteilen mit verschiedenen Zugriffsbedingungen auf eine neue Zugriffsbedingung	122
12.7.4	Trennung von zwei Dienst-Bestandteilen mit Änderung der Zugriffsbedingungen für beide Dienst-Bestandteile	123
	VERZEICHNIS DER KURZBEZEICHNUNGEN	124
	ZITIERTER LITERATUR	130
	ANHANG 1: EXTERNE SPEZIFIKATIONEN DER PC2-SMART-CARD	131
	ANHANG 2: BETRIEBSVORSCHRIFTEN ZUM SENDEN VON D2-MAC/PAKET- DIENSTEN	178
	ANHANG 3: EMPFEHLUNGEN FÜR DIE ENTWICKLUNG EINES EUROCRYPT-D2- MAC/PAKET-EMPFÄNGERS	184
	ANHANG 4: SPEZIFIKATIONEN DER PC-EUROCRYPT-KARTEN	192

1 Gegenstand

Dieses Dokument beschreibt das System EUROCRYPT, ein System der Zugriffskontrolle, das für Systeme innerhalb der MAC/Paket-Familie verwendet werden kann. Das Zugriffskontrollsystem sorgt dafür, daß Fernsehen, Hörfunkprogramme oder andere Datendienste nur für solche Teilnehmer zugriffsbereit sind, die bestimmte eindeutig festgelegte Bedingungen, meist Zahlungsbedingungen, erfüllen. Die Anwendung von EUROCRYPT auf das D2-MAC/Paket-System wird im Dokument (Lit. 1) behandelt.

Die Abschnitte 2 bis 5 in Teil 6 des Dokuments (Lit. 1) enthalten eine allgemeine Beschreibung des Zugriffskontrollsystems, allerdings ohne Beschreibung des internen Formats der Datensignale, die vom jeweiligen System bestimmt werden. Zum besseren Verständnis werden in den Abschnitten 2 bis 4 dieses Dokuments die Informationen aus Teil 6 des Dokuments (Lit. 1) erörtert, und in den Abschnitten 5 bis 10 werden diese Informationen durch nähere Beschreibungen der Teile, die speziell für die Spezifikation des Zugriffskontrollsystems EUROCRYPT von Bedeutung sind, ergänzt. Die Verwendung dieser Teile in einer Muster-Implementierung (die P2-Smart-Card) wird in der Spezifikation als Beispiel beschrieben.

Abschnitt 2 beschreibt die Grundprinzipien des Zugriffskontrollsystems; er beschreibt auch die Funktionen des Systems. Das Zugriffskontrollsystem kann grafisch in zwei Teile untergliedert werden: das **Scrambling-System** und das **Verschlüsselungssystem**. Das Scrambling-System betrifft hauptsächlich die Programmsignale, während das Verschlüsselungssystem die für den Programmzugriff erforderlichen Schlüssel und Datensignale verarbeitet.

Abschnitt 3 enthält die Spezifikationen für das Ton-, Daten- und Video-Scrambling-Verfahren. Abschnitt 4 beschreibt die Schnittstelle, über die die Sicherheitsdaten und Steuersignale zum Empfangsgerät übertragen werden, das Format und die Adressen der Berechtigungs-Verwaltungsmeldungen und die Dienst-Kennungen.

Abschnitt 5 gibt eine allgemeine Beschreibung der Berechtigungs-Verwaltungsmeldungen (EMM), und die Abschnitte 6 bis 9 beschreiben jeweils das Format der Berechtigungsmeldungen für "Einzelteilnehmer", "Gesamteilnehmer", "Gemeinschaftsteilnehmer" und "Kollektivteilnehmer". Abschnitt 10 beschreibt das Format der Berechtigungs-Kontrollmeldungen (ECM).

Abschnitt 11 befaßt sich im einzelnen mit dem Aufbau der in der Spezifikation (Lit. 1) beschriebenen Zugriffskontrollverfahren und führt eine neue Funktionsebene ein, das sogenannte "Panning".

Abschnitt 12 befaßt sich im einzelnen mit den wesentlichen Zeitdiagrammen, die bei den Schaltvorgängen auftreten.

Anhang 1 enthält, dargestellt anhand von Beispielen, die externen Spezifikationen eines Berechtigungsmediums, der PC2-Smart-Card, bei der es sich um die Muster-Implementierung eines der Spezifikation entsprechenden Berechtigungselements handelt. Alle Berechtigungsspeicherelemente für die in der Spezifikation beschriebenen Zugriffsmethoden werden grundsätzlich als PC EUROCRYPT bezeichnet.

Anhang 2 enthält die Betriebsvorschriften für das Senden von Diensten, die mit der D2-MAC/Paket-Spezifikation und dem Zugriffskontrollsystem EUROCRYPT arbeiten.

Anhang 3 beschreibt die Empfehlungen für die Entwicklung von D2-MAC/Paket-Empfängern entsprechend der im Dokument (Lit. 1) beschriebenen D2-MAC/Paket-Spezifikation für die Arbeit mit dem Zugriffskontrollsystem EUROCRYPT und den in Anhang 2 beschriebenen Betriebsvorschriften.

Anhang 4 beschreibt die Spezifikationen der PC EUROCRYPT-Karten und die Möglichkeiten ihrer Anwendung bei D2-MAC/Paket-Empfängern, wie sie in Anhang 2 beschrieben werden.

2 Allgemeine Beschreibung des Zugriffskontrollsystems

2.1 Das Scrambling- und das Verschlüsselungssystem

Bild 2.1 zeigt ein Funktionsblockdiagramm des Zugriffskontrollsystems. Einige Funktionen (z.B. das Demultiplex) sind der Einfachheit halber weggelassen worden, und Bild 2.1 **gibt nur eine globale Darstellung des Systems**. Die **Quellsignalkomponente** in Bild 2.1 kann ein Videobild, ein Ton- oder ein Datensignal sein, für das der Programmanbieter den Zugriff beschränken möchte. Ein Scrambler macht die Signalkomponente unkenntlich, und zwar mit Hilfe einer Scrambling-Sequenz, die von einem Pseudozufallsgenerator mit einer sich ständig ändernden Binärsignalfolge erzeugt wird. Im Empfangsgerät läuft der umgekehrte Vorgang ab, und zwar mit Hilfe des **Descrambling-Sequenzgenerators**, der **Descrambling-Sequenz** (die Umkehrung der Scrambling-Sequenz) und des **Descramblers**.

Der Scrambling-Sequenzgenerator ist ein Pseudozufallsgenerator mit einer Binärsignalfolge mit sehr langer Zykluszeit. In diesem Generator wird ein nicht vorherbestimmbares Ausgangssignal erzeugt, und zwar durch Verwendung eines **Kontrollwortes** und eines **zyklischen 8-Bit-Bildzählers FCNT**, der eine Zykluszeit von etwa zehn Sekunden (25 Bilder/Sekunde) hat. Das Descrambling-System muß an der Signalquelle und im Empfangsgerät synchronisiert werden. Die descrambelte Quellsignalkomponente, der Bildzähler und das Synchronisiersignal werden von Signalen abgeleitet, die auf dem gleichen Kanal übertragen werden.

Der Vermittler eines Dienstes kann entscheiden, ob das Signal ohne Scrambling-Schutz bzw. ungeschrambelt (im "Klartext") oder mit Scrambling-Schutz bzw. gescrambelt gesendet wird. Bei einer gescrambelten Sendung kann der Programmanbieter entweder mit einem lokalen Kontrollwort arbeiten, das sich nicht verändert und das im Empfangsgerät gespeichert ist, oder mit einem regenerierten Kontrollwort, das vom Verschlüsselungssystem erzeugt wird. Wird mit einem regenerierten Kontrollwort gearbeitet, kann das Empfangsgerät des Kunden intern erst dann das richtige Kontrollwort erzeugen, wenn die entsprechenden Empfangsbedingungen für den betreffenden Dienst erfüllt worden sind.

Wenn nicht mit einem lokalen Kontrollwort gearbeitet wird, kommt das Kontrollwort von einem Datenschutzesprozessor, der ein fester Bestandteil des Zugriffskontrollsystems (ACS) ist.

Dazu ist es erforderlich, daß das Kontrollwort (CW) am Übertragungspunkt erzeugt und in verschlüsselter Form an das Empfangsgerät gesendet wird, wobei die Verschlüsselung mit Betriebsschlüssel SK erfolgt (vgl. Bild 2.1). Das Kontrollwort ändert sich jeweils nach 256 TV-Bildern (d.h. etwa alle 10 Sekunden), das verschlüsselte Kontrollwort wird jedoch in Abständen von etwa 0,5 Sekunden übertragen, damit die auf den Kanal abgestimmten Empfangsgeräte eine schnelle Descramblung durchführen können. Das Kryptogramm SK (CW) wird mit einer Berechtigungs-Kontrollmeldung ECM gesendet, die auf dem gleichen Kanal wie der Dienst selbst übertragen wird. Die Meldung enthält auch Daten darüber, wie das Kontrollwort anzuwenden ist.

Neue Kontrollwörter werden in Abständen von etwa 10 Sekunden in den Descrambler geladen, vorausgesetzt, der Betriebsschlüssel ist im Empfangsgerät verfügbar und mit der Erlaubnis ausgestattet, das Kontrollwort zu erzeugen.

Die Aufgabe des Zugriffskontrollsystems (ACS), das entweder fester Bestandteil des Empfangsgerätes oder ein Zusatzteil ist, besteht darin, zu entscheiden, ob es das Kontrollwort rechnerisch ermitteln kann. Das System ist mit einem Datenschutzesprozessor ausgestattet, der sowohl einen Speicher wie auch arithmetische Fähigkeiten besitzt. Der Datenschutzesprozessor speichert die Geheimschlüssel und die dazugehörigen Berechtigungen. Aus dem Datenschutzesprozessor können nur solche Daten gelesen werden, die nicht geheim sind. Geheime Daten bleiben im Prozessor. In den Zugriffsberechtigungen sind die Parameter der Teilnehmer in verschiedener Form beschrieben: Gültigkeitsdauer, zu verbrauchende Einheiten, Empfangsgebiet usw. Der Prozessor prüft diese Parameter, bevor er ein Kontrollwort mit Hilfe eines Betriebsschlüssels berechnet.

Bei diesen Parametern handelt es sich um Verwaltungsparameter, die durch Berechtigungs-Verwaltungsmeldungen EMM in das ACS geladen werden können. Die EMM bestehen aus Daten, die im Klartext oder gescrambelt übertragen werden, sowie aus verschlüsselten Informationen. Diese

Meldungen gehören zu einem Sende-Adressierungsdienst und sind entweder für einen einzelnen Teilnehmer (spezifisch für einen bestimmten Kunden) oder gemeinschaftliche Nutzung (spezifisch für eine Gruppe von Kunden) gedacht.

Bevor der Prozessor Informationen in das ACS schreibt, prüft er die Meldung auf ihre Datenintegrität hin, ob die Meldung richtig adressiert ist, ob sie nicht schon einmal verarbeitet worden ist und ob die Quelle, die sie ausgesendet hat, zu den Einrichtungen gehört, die berechtigt sind, Daten in das ACS einzugeben. Dieser Vorgang wird kontrolliert durch einen Verwaltungsschlüssel PDK (der unter bestimmten Umständen ein Betriebsschlüssel sein kann), der dem Programmanbieter gehört.

Die Verwaltungs- und, soweit vorhanden, die Betriebsschlüssel werden unter der Kontrolle eines höherrangigen Schlüssels, des Herausgeberschlüssels, in das ACS geladen. Dieser Schlüssel kann dazu verwendet werden, die vorhandenen Dienst-Schlüssel (Verwaltungs- bzw. Betriebsschlüssel) ungültig zu machen, wenn der Dienst nicht verriegelt ist, oder bei Bedarf neue Schlüssel zu laden, damit neue Dienst-Vermittler auf das ACS eines bestimmten Kunden zugreifen können. Das System kann dazu verwendet werden, die Gruppe von Dienst-Vermittlern, die Zugriff zu einem Empfangsgerät hat, zu verändern. Bestehende Dienst-Schlüssel können mit Hilfe des Herausgeberschlüssels oder eines Verwaltungsschlüssels des Dienstes selbst modifiziert werden.

EMM-Meldungen für Gemeinschaftsteilnehmer werden verwendet, um die Sendezeit für eine Berechtigung zu verkürzen. Diese Meldungen müssen in regelmäßigen Abständen gesendet werden, damit sichergestellt ist, daß die Meldung mindestens einmal von allen Teilnehmern empfangen worden ist. Nehmen wir an, daß Gruppen aus 256 Teilnehmern bestehen, so können in weniger als einer Minute Millionen von Teilnehmern erreicht werden.

All diese einzelnen Informationen und Parameter, ob im Klartext oder geheim, sind an einen bestimmten Programmanbieter gebunden und unter der Dienst-Kennung eines Dienst-Vermittlers gespeichert. Die EMM kann unabhängig vom physischen HF-Kanal übermittelt werden, weil die Dienst-Kennung des Programmanbieters nicht an den Übertragungskanal gebunden ist.

Berechtigungs-Verwaltungsmeldungen können auch verwendet werden, um Meldungen an Einzelteilnehmer oder an Gruppen von Teilnehmern zu übermitteln. Diese gleichen Meldungen können außerdem dazu verwendet werden, Ersatzfunktionen für bestimmte Gruppen zu konfigurieren oder spezielle Berechtigungs-Verwaltungsmeldungen zu übermitteln. Eine Ersatzkonfiguration kann zum Beispiel eine spezielle Teletextseite sein, die bei einem Blackout bei einer bestimmten Gruppe von Teilnehmern das Videosignal ersetzt. Eine Ersatzseite kann auch im Zusammenhang mit der Fingerprint-Identifizierung verwendet werden. Dabei handelt es sich um die Einfügung eines Kunden-Logos auf bestimmten Bildern des Videosignals. Der Ersatz anderer Dienste (z.B. Hörfunk, Teletext usw.) ist auch möglich.

Und schließlich können Verwaltungsmeldungen zu Einzel- oder Gemeinschaftsberechtigungen auch verwendet werden, um spezielle Konfigurationsdaten zum Empfangsgerät eines Teilnehmers (Modem-Telefonnummer, Datum und Uhrzeit eines Modemrufs, Notruf durch Fernbedienung usw.) zu übertragen.

ECM =	Berechtigungs-Kontrollmeldung
EMM =	Berechtigungs-Verwaltungsmeldung
CW =	Kontrollwort
SK =	Betriebsschlüssel
FCNT =	Bildzähler (8 Bit)
CAFCNT =	256-Bild-Zähler (20 Bit)
E =	Teilnehmerberechtigung
IK =	Herausgeberschlüssel
UA =	Einzeladresse
P =	Aktueller Programmparameter
SK (P, CW) =	CW, verschlüsselt mit SK
PDK =	Dienst-Verwaltungsschlüssel
PDK (E, UA oder PPUA) =	E, verschlüsselt mit PDK
IK (SK oder PDK, UA oder PPUA) oder PDK (SK oder PDK, UA oder PPUA) =	SK oder PDK, verschlüsselt mit IK oder PDK; PDK kann nur verwendet werden zur Modifizierung von Schlüsseln, die zu dem Dienst gehören.

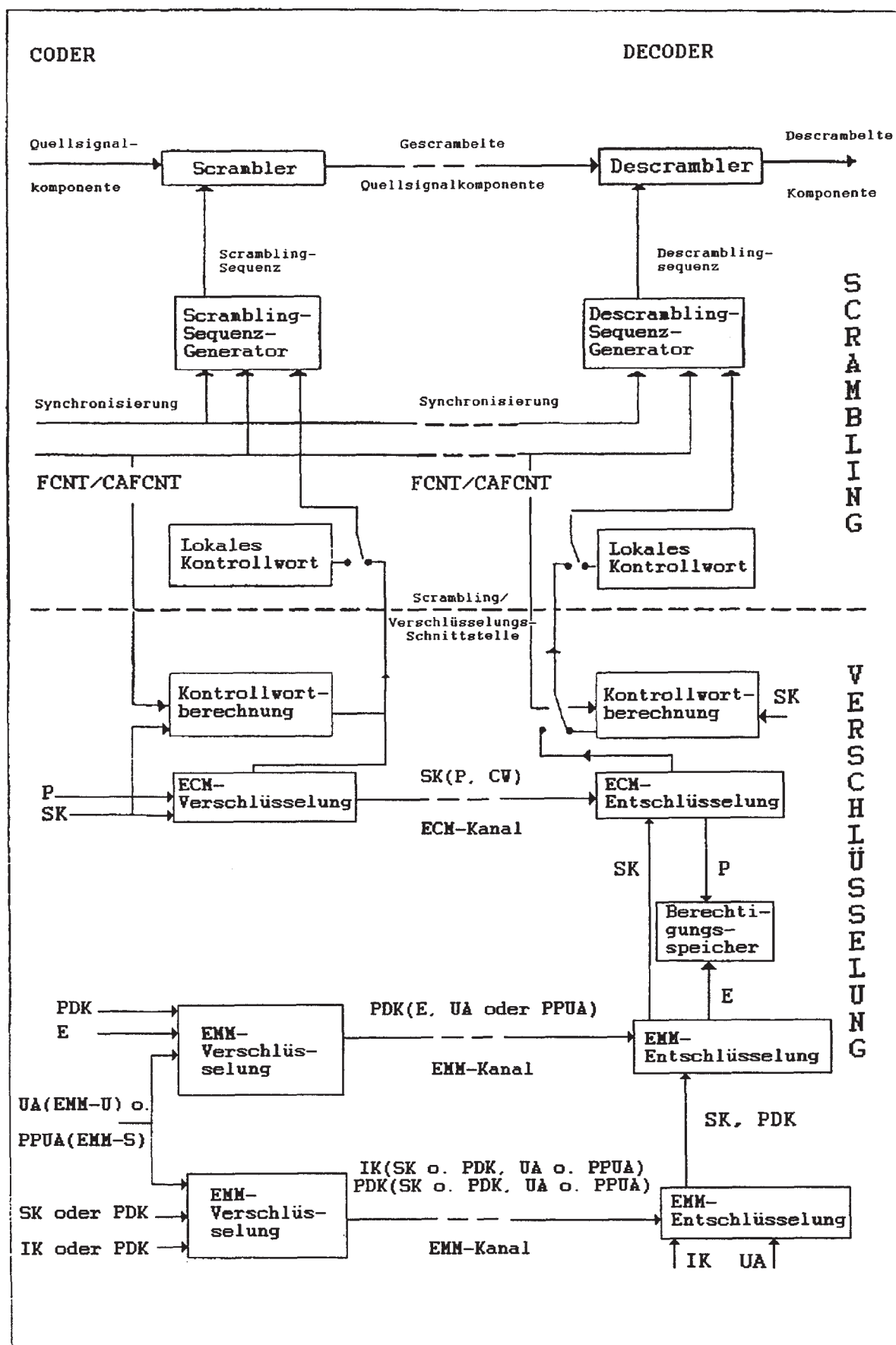


Bild 2.1: Allgemeine Beschreibung des Zugriffskontrollsystems

2.2 Initialisierung und Aktualisierung der Dienst-Schlüssel (Verwaltung oder Betrieb)

Wenn das ACS zum ersten Mal in Betrieb genommen wird, ist es nur mit einer Einzeladresse und mit einem Herausgeberschlüssel programmiert. Wie oben beschrieben, kann nur der Inhaber des Herausgeberschlüssels den ersten Verwaltungsschlüssel für einen mit einer Dienst-Kennung versehenen Dienst laden.

Ein Betriebsschlüssel kann eingegeben oder ein Betriebs- oder Verwaltungsschlüssel modifiziert werden durch einen entsprechenden Dienst-Verwaltungsschlüssel oder einen Herausgeberschlüssel. Die Möglichkeit des Eingebens oder Modifizierens von Dienst-Schlüsseln durch den Herausgeber kann jedoch durch Parameter vorgegeben werden; es kann vorkommen, daß ein Programmanbieter seinen Dienst gesperrt haben will, um die Benutzung seiner Schlüssel von seiten des Herausgebers zu verhindern, nachdem der erste Schlüssel eingegeben worden ist.

Nachdem die Schlüssel eingegeben worden sind, kann jede Quelle, die einen Dienst-Schlüssel zusammen mit der entsprechenden Dienst-Kennung empfängt, Zugriffsberechtigungen in diejenigen ACS laden, die den gleichen Schlüssel empfangen haben. Diese Quelle kann dann, wenn sie dies wünscht, eine spezielle Adresse in das ACS eingeben, die für diesen besonderen Dienst reserviert ist. Sinn und Zweck dieser Maßnahme ist es, eine maximale Ausnutzung des Systems bei der Verwendung von Gemeinschaftsmeldungen sicherzustellen.

Die Aufgabe des Herausgebers, der den Herausgeberschlüssel besitzt, ist es, die Dienst-Schlüssel an die Dienst-Vermittler zu verteilen und sie ins ACS zu laden. Der Herausgeber kann auch Dienst-Schlüssel ungültig machen. Das heißt, man kann ihn als obersten Dienst-Organisator bezeichnen, wobei seine Aufgabe auf ein Minimum beschränkt bleibt, da die meisten Aktivitäten in bezug auf das ACS von den Programmanbietern selbst durchgeführt werden, nachdem die Dienst-Verwaltungsschlüssel eingegeben worden sind.

2.3 Funktionen

Diese Spezifikation beschreibt fünf Möglichkeiten der Zugriffskontrolle:

- Abonnement nach Themen und Klassen, wobei die Teilnehmer für einen bestimmten Zeitraum, der mit einem Anfangs- und mit einem Enddatum beschrieben wird, Zugriff auf die Programme haben. Das Abonnement ist außerdem eingeteilt nach bestimmten Klassen, wobei die höchste Klasse der Programme, auf die der Teilnehmer Zugriff hat, festgelegt ist (jedes Programm hat eine Klassenbezeichnung), und nach Themen, wobei das Thema eines Programms, für das Zugriff besteht, festgelegt ist (jedes Programm hat auch eine Themenbezeichnung).
- Abonnement nach Sparten, wobei die Teilnehmer für einen bestimmten Zeitraum, der mit einem Anfangs- und mit einem Enddatum beschrieben wird, Zugriff zu den Programmen haben. Dieser Zeitraum ist außerdem eingeschränkt durch ein bestimmtes Verzeichnis von Programmsparten; das Verzeichnis legt fest, ob und für welche Sparten ein Teilnehmer Zugriff hat, wobei jedes Programm einer bestimmten Sparte zugeordnet ist.
- Pay-per-view pro Programm mit Vorbestellung, wobei die Teilnehmer Zugriff haben zu einem oder mehreren Programmen oder einer Reihe von Programmen, die durch eine Anfangs- und Endprogrammnummer definiert sind, wobei jedes Programm eine Nummer hat.
- Pay-per-view pro Programm mit Impulsabbuchung, wobei der Kunde einen Kredit eingeräumt bekommt; der Kredit wird belastet mit den entstehenden Programmkosten entsprechend den Programmzugriffen. Alle Programme sind mit einer Programmnummer und mit einem Preis versehen. Diese Methode ist besonders gut geeignet für die Bezahlung pro Programm, weil eine Rückmeldung zu den von den Teilnehmern erworbenen Programmen erfolgt.
- Pay-per-view pro Zeit mit Impulsabbuchung, wobei der Kunde einen Kredit eingeräumt bekommt. Dieser Kredit wird belastet mit den Zeitkosten (Preis des Programms pro Zeiteinheit). Alle Programme sind mit einer Programmnummer versehen. Bei dieser Methode erfolgt eine Rückmeldung zu den von den Teilnehmern erworbenen Programmen.

Es wird ein zusätzlicher Parameter eingeführt, der das Zugriffskontrollsystem ergänzen und Urheberrechtsschutz gewähren soll. Unabhängig von der Zugriffsmethode bekommt jeder Teilnehmer eine zur Dienst-Kennung gehörende Gruppenadresse. Mit diesem Parameter werden die Teilnehmer in Gruppen eingeteilt, so daß der Programmierer bei Bedarf eine oder mehrere Gruppen durch Blackout sperren oder anwählen kann, indem er die entsprechenden Signale sendet. Dieser Parameter ist mit der höchsten Priorität versehen, und sofern ein Teilnehmer zu einer der mit Blackout gesperrten Gruppe gehört, hat er keinen Zugriff zum Programm, ganz gleich, ob er eine Berechtigung hat oder nicht.

Diese Zugriffsmethoden können auch miteinander kombiniert angewendet werden, um die Bedingungen für einen Zugriff zu verschiedenen Programmkomponenten zu definieren. Eine solche Definition hat eine ständige Übertragung von Berechtigungskontrollmeldungen (ECM) im MAC/Paket-Signal zur Folge.

Eine lokale, teilnehmerorientierte Kontrolle des ACS ist ebenfalls möglich, indem Altersgruppen-grenzen programmiert werden. Jedes Programm, das innerhalb eines Dienstes gesendet wird, kann mit einer Altersgruppengrenze versehen werden, die das erforderliche Mindestalter für denjenigen definiert, der das Programm sehen kann. Sofern ein Programm eine höhere Altersangabe hat als die vom Teilnehmer programmierte, muß der Eltern-Kode, auch PIN-Kode genannt, angewendet werden. Der Teilnehmer kann auch den Zugriff zu seinem ACS für Pay-per-view mit Impulsabbuchung (pro Programm oder Zeit) sperren. Ob ein Programm erworben werden kann, hängt dann ab von der Eingabe des PIN-Kodes. Der Teilnehmer kann schließlich, wenn das ACS für Pay-per-view mit Impulsabbuchung oder für eine bestimmte Altersgruppe gesperrt ist, eine Anzahl von Programmen speichern, die, wenn sie empfangen werden, von dieser Vorschrift nicht betroffen sind. Das kann angewendet werden bei vorprogrammierten Videoaufnahmen oder beim Empfang von ausgewählten Programmen, wenn der ACS-Inhaber nicht zu Hause ist.

Für diese verschiedenen Zugriffsmethoden bekommt der Teilnehmer eine Berechtigungsspeicherkarte, die einen oder mehrere Dienst-Schlüssel enthält. Ein Dienst-Schlüssel kann für einen bestimmten Zeitraum (Abonnementverfahren) oder für eine bestimmte Anzahl von fortlaufend nummerierten Programmen (Verfahren 'Pay-per-view mit Vorbestellung') verwendet werden. Bei Pay-per-view mit Impulsabbuchung ist der Dienst-Schlüssel bis zu einem bestimmten Höchstbetrag gültig. Die Gültigkeit kann erneuert werden (für einen weiteren Zeitraum, für eine weitere Anzahl von fortlaufend nummerierten Programmen oder für ein weiteres Guthaben), indem man eine entsprechende Berechtigungs-Verwaltungsmeldung (EMM) intermittierend im MAC/Paket-Signal mit-sendet. Alle Berechtigungen werden vom ACS gespeichert, und für verschiedene Zugriffsmethoden kann der gleiche Dienst-Schlüssel verwendet werden.

Die Berechtigungsspeicherkarte wird vom Zugriffskontrollsystem (ACS) verwaltet, das über eine Empfänger-ACS-Schnittstelle (die eine virtuelle Schnittstelle sein kann, wenn das ACS in das Empfangsgerät integriert ist) mit dem Empfangsgerät verbunden ist.

Die Berechtigungs-Verwaltungs- und -Kontrollmeldungen, die für die oben beschriebenen verschiedenen Zugriffsmethoden erforderlich sind, werden in den Abschnitten 5 bis 10 ausführlich behandelt.

Über die zur Verfügung stehenden Berechtigungen kann der Teilnehmer zu Hause über sein Empfangsgerät Auskünfte einholen. Dies geschieht durch Lesen der Berechtigungen, die in den Datenschutzprozessor eingegeben worden sind. Das heißt, der Teilnehmer kann Zeiträume, Guthaben usw., die bei den einzelnen Diensten für ihn zur Verfügung stehen, prüfen. Die genaue Art und das genaue Format der angezeigten Meldungen werden in diesem Falle vom Zugriffskontrollsystem bestimmt, so daß der Dialog zwischen Mensch und Maschine so teilnehmerfreundlich wie möglich gestaltet und ganz auf das jeweilige System zugeschnitten werden kann.

3 Scrambeln von Ton, Daten und Bildern

3.1 Einleitung

Dienste, für die kein Abonnement und auch keine andere Art von Bezahlung erforderlich ist, werden als Dienste mit **freiem Zugriff** bezeichnet. Bei **kontrolliertem Zugriff** werden Ton, Daten und Bilder **immer gescrambelt**; sie können auch bei freiem Zugriff gescrambelt werden. Bei Diensten mit freiem Zugriff, die vor dem Aussenden gescrambelt werden, ist das für die Descramblung der verschiedenen Signalkomponenten erforderliche Kontrollwort (das "lokale Kontrollwort") im Empfangsgerät vorhanden (siehe Abschnitt 3.3).

Bei freiem Zugriff kann das Bildsignal je nach Entscheidung des Dienst-Vermittlers gescrambelt oder ungeschrambelt sein. Die entsprechenden Signalformen werden in Teil 2 des Dokumentes Lit. 1 beschrieben.

Die digitalen Ton- und Datensignale werden aus Gründen der Zugriffskontrolle zuerst gescrambelt und dann einer Bitverschachtelung und einem Übertragungsscrambling (zwecks Formung des Signalspektrums) unterworfen. Abschnitt 3.2 beschreibt das Scrambling-Verfahren, das aus Gründen der Zugriffskontrolle angewendet wird.

3.2 Beschreibung des Scrambling-Verfahrens für Ton und Daten

Um Ton und Daten zu scrambeln, wird den **Nutzdaten** der Ton- und Daten-Dienst-Pakete durch Modulo-2-Addition eine pseudozufällige Binärsignalfolge (PRBS) zugezählt. Dieser Vorgang kommt zu der Bitverschachtelung und dem Übertragungsscrambling hinzu, das in den Abschnitten 3.6 und 3.7 von Teil 1 im Dokument Lit. 1 beschrieben wird.

Man beachte,

- daß die Blöcke mit dem kodierten Ton gescrambelt werden, **nachdem** sie einem Fehler-schutz unterzogen wurden; das bedeutet, daß die Fehlererkennung bzw. -korrektur im Empfangsgerät nach dem Descrambeln stattfindet.
- daß die Paket-Kennung, die Paketart-Bytes (PT), die Interpretationsblöcke (BI) und die Dienst-Kennungsdaten (SI) nicht gescrambelt werden.

3.3 Erzeugung der Descramblersequenzen

Die Descramblersequenzen werden von einem nach dem Pseudozufallsprinzip arbeitenden Binärsignalsystem (PRBS) erzeugt. Das vereinfachte Blockdiagramm in Bild 3.1 zeigt die effektive Konfiguration für den wichtigsten Dienst Fernsehen (Bild und dazugehöriger Ton).

Alle Dienste können gescrambelt werden. Bei einem gescrambelten Dienst mit freiem Zugriff muß allerdings das Kontrollwort im Empfangsgerät des Teilnehmers zur Verfügung stehen.

Für das Descrambeln ist ein 60 Bit langes Kontrollwort erforderlich. Bei einem gescrambelten Dienst mit freiem Zugriff sind alle Bits des Kontrollwortes auf logisch '1' gesetzt, und das Kontrollwort ist im Empfangsgerät gespeichert. Bei kontrolliertem Zugriff werden die 60 Bit langen Kontrollwörter vom Zugriffskontrollsystem bereitgestellt.

Das vereinfachte Blockdiagramm in Bild 3.1 zeigt drei PRBS-Generatoren. Diese werden in den Bildern 3.2, 3.3 und 3.4 beschrieben.

Das PRBS-System beansprucht einen 8 Bit Bildzähler; die Spezifikation dieser Information und die Stelle, wo sich diese Information in Zeile 625 befindet, sind in Abschnitt 5.4 von Teil 1 im Dokument Lit. 1 (FCNT-Kode) beschrieben. Wie man aus Bild 3.1 entnehmen kann, werden die Wörter zur Initialisierung des PRBS-Generators durch Kombination der Kontrollwörter mit dem 8 Bit Bildzähler FCNT erzeugt. Die PRBS-Generatoren werden, wie im nächsten Abschnitt beschrieben, mit dem Bildzähler synchronisiert.

3.4 Synchronisierung der Descramblersequenzen

Nehmen wir als Beispiel zwei aufeinanderfolgende Bilder F_n und F_{n+1} . Im Verlauf der Zeile 625 trifft am Ende von F_n ein neuer Bildzählerwert FCNT mit dem Wert n ein. Dieser Wert n wird mit den Kontrollwörtern CW1 und CW2 kombiniert (Bild 3.1). Dabei entstehen zwei neue Werte IW1 und IW2 für die Initialisierungswörter, die jeweils auf die PRBS-Generatoren 1 und 2 gelegt werden. Man beachte dabei auch, daß die ersten vom PRBS-Generator 1 erzeugten 61 Bits, nachdem er das Wort empfangen hat, vom PRBS-Generator 3 benutzt werden, um das erste während des Bildes F_{n+1} empfangene Paket zu descrambeln. Gleichermaßen werden die ersten vom PRBS-Generator 2 erzeugten 16 Bits, nachdem er das Wort empfangen hat, benutzt, um Zeile 1 des Bildes F_{n+1} zu descrambeln.

Nach jeweils 256 Bildern empfängt das PRBS-System ein neues Kontrollwort, dessen Gültigkeitsdauer beginnt, wenn FCNT=0, d.h. zu Beginn von F_1 .

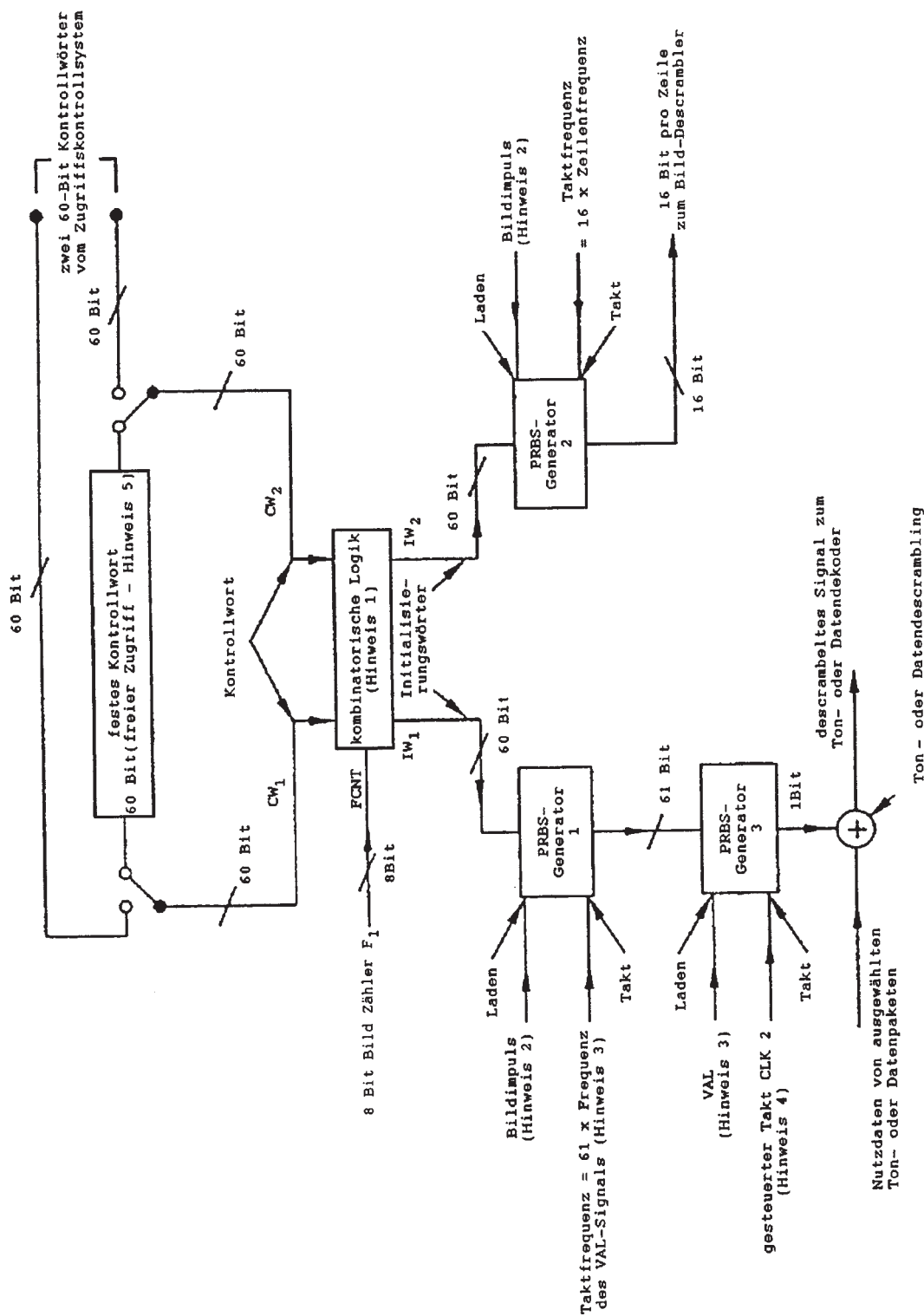


**Bild 3.1: PRBS-System für Zugriffskontrollsystem
(hier nur für das Bild und eine Tonkomponente)**

ANMERKUNG 1: Die kombinatorischen Logikfunktionen zur Verknüpfung der beiden 60 Bit langen Kontrollwörter CW_1 und CW_2 mit dem aus 8 Bit bestehenden Bildzähler FCNT zu den beiden 60 Bit langen Initialisierungswörtern IW_1 und IW_2 sind in beiden Fällen gleich und werden wie folgt definiert:

Der aus 8 Bit bestehende Bildzähler (FCNT) wird wie folgt dargestellt:

$F_0, F_1, \dots, F_7$

Das aus 60 Bit bestehende Kontrollwort (CW) wird wie folgt dargestellt:

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

Das 60 Bit lange Initialisierungswort (IW) wird dann wie folgt dargestellt:

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

IW kann wie folgt von CW und FCNT abgeleitet werden:

$IW_0 = CW_0 \oplus FCNT$ $IW_1 = CW_1 \oplus \overline{FCNT}$ $IW_2 = CW_2 \oplus FCNT$ $IW_3 = CW_3 \oplus \overline{FCNT}$
 $IW_4 = CW_4 \oplus FCNT$ $IW_5 = CW_5 \oplus \overline{FCNT}$ $IW_6 = CW_6 \oplus FCNT$ $IW_7 = CW_7 \oplus \overline{FCNT}$

Man beachte dabei,

- daß $\overline{FCNT}$ das logische Komplement von FCNT ist (d.h. $FCNT \oplus \overline{FCNT} = 11111111$).
- daß bei der Transformation von CW7 zu IW7 nur das niedrigstwertige Halbbyte von $\overline{FCNT}$ benutzt wird.

ANMERKUNG 2: Der Bildimpuls tritt einmal pro Bild auf und seine Vorderflanke (ansteigende Flanke) markiert die Grenzen des Bildes.

ANMERKUNG 3: VAL ist ein Taktsignal, das mit der gleichen Frequenz arbeitet wie die Pakete in dem betreffenden Teilbild. Der Generator PRBS 1 wird 61mal zwischen zwei Validation-Signalen VAL getaktet.

ANMERKUNG 4: CLK 2 ist ein gesteuerter Takt, wobei der Generator PRBS 3 720 Bit pro Paket überträgt und durch den Datenburst, der zu dem für die Descramblung zuständigen Modulo-2-Addierglied gelangt, synchronisiert wird.

ANMERKUNG 5: Bei einem geschrämbelten Dienst mit freiem Zugriff sind alle Bits auf logisch '1' gesetzt.

ANMERKUNGEN zu Bild 3.1

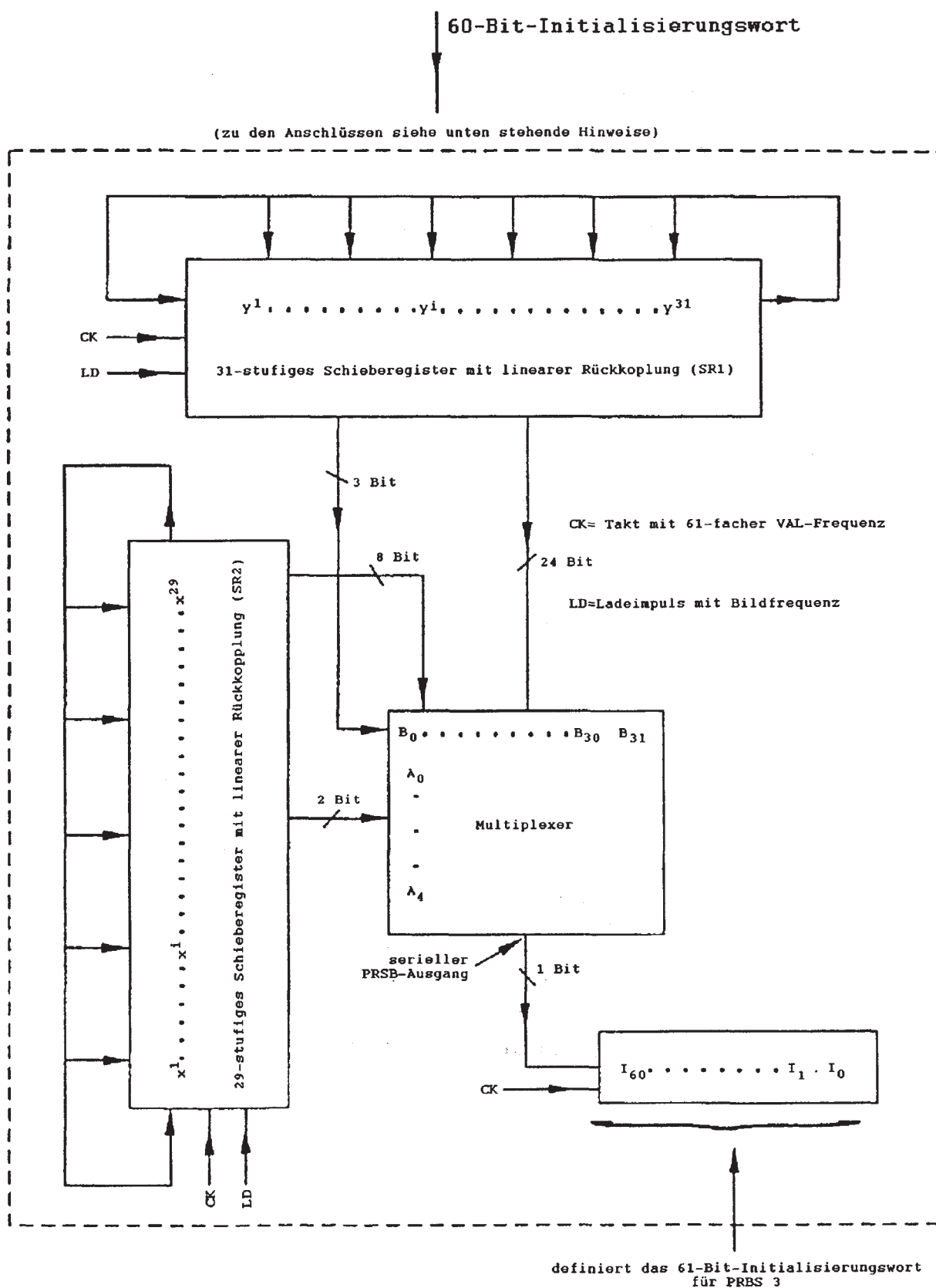


Bild 3.2: PRBS-Generator 1 aus Bild 3.1

ANMERKUNGEN:

Das Blockdiagramm in Bild 3.2 hat folgende Anschlüsse:

Der PRBS-Generator besitzt zwei mehrstufige Schieberegister mit linearer Rückkopplung SR1 und SR2. Die Polynome für die Rückkopplungskonfigurationen lauten wie folgt:

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

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

Das Initialisierungswort wird wie folgt in SR1 und SR2 geladen: das 60 Bit lange Initialisierungswort wird durch die Folge $I_{59} - I_0$ definiert, wobei I_i jeweils ein Bit darstellt und i Werte zwischen 0 und 59 annimmt.

SR1: I_i wird in $y^{(31-i)}$ geladen, wobei $i = 0$ bis 30

SR2: I_i wird in $y^{(60-i)}$ geladen, wobei $i = 31$ bis 59

Die Schieberegisterausgänge gehen zu einem Multiplexer. Die Eingänge des Multiplexers werden mit A_0 bis A_4 und B_0 bis B_{31} bezeichnet. Die Anschlüsse sind wie folgt definiert:

x^1 wird in A_0 geladen

x^2 wird in A_1 geladen

x^i wird in $B_{(i-3)}$ geladen, wobei $i = 3$ bis 10

y^1 wird in A_2 geladen

y^2 wird in A_3 geladen

y^3 wird in A_4 geladen

y^n wird in $B_{(n+4)}$ geladen, wobei $n = 4$ bis 27

Das Signal A ist ein 5 Bit Wort $A_4...A_0$, das die Adresse des Index von Signal B (Binärzahl von 0 bis 31 für $B_{31}-B_0$) definiert. Die am Ausgang anstehenden 61 aufeinanderfolgenden Werte für Signal B, die durch die Adresse A definiert werden, bilden das Initialisierungswort für den Generator PRBS 3, und zwar jeweils ein Wort pro Paket (VAL-Signalfrequenz). Das niedrigstwertige Bit im Initialisierungswort (I_0) wird zuerst ausgegeben.

Anmerkungen zu Bild 3.2

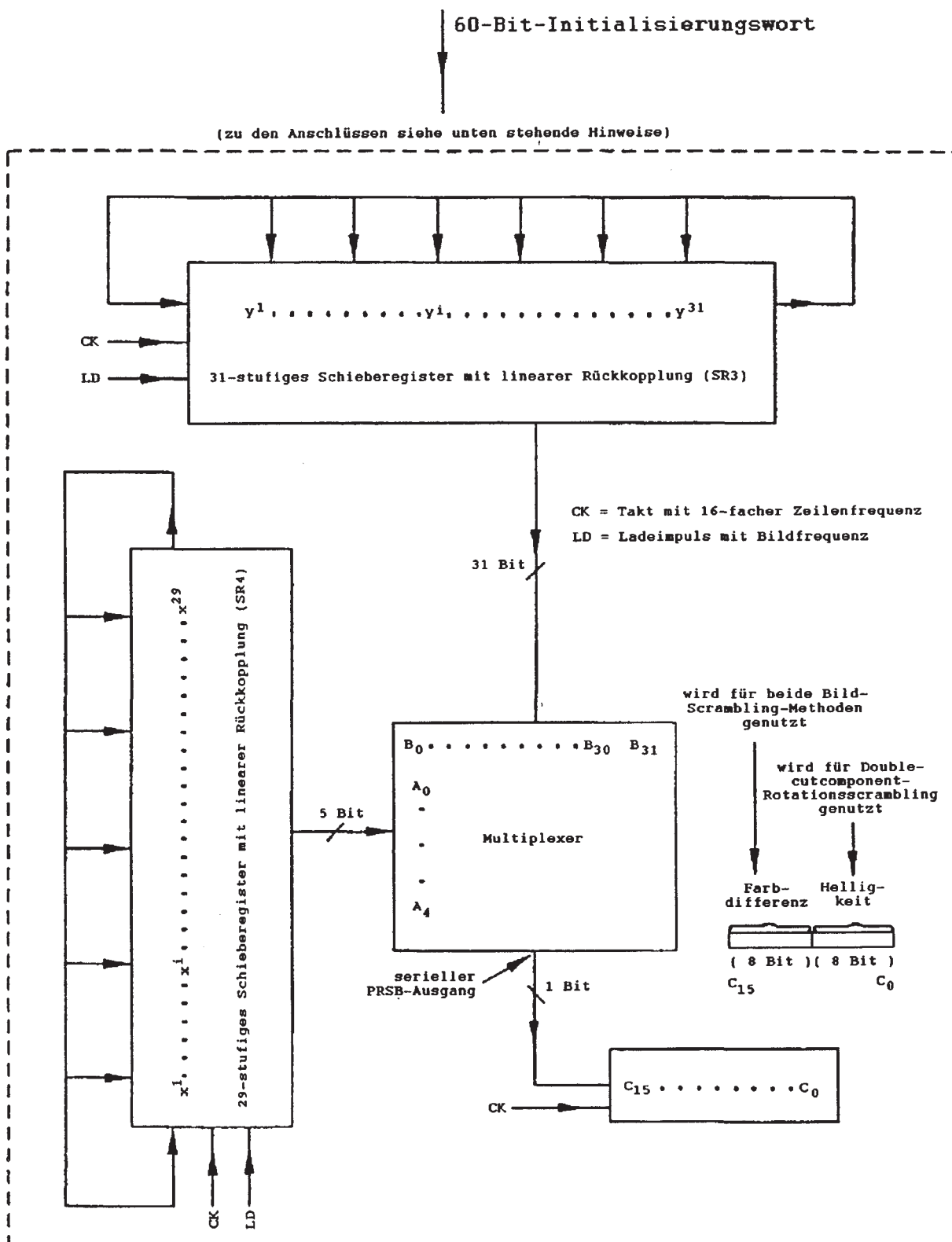


Bild 3.3: PRBS-Generator 1 aus Bild 3.1

ANMERKUNGEN:

Das Blockdiagramm in Bild 3.3 hat folgende Anschlüsse:

Der PRBS-Generator besitzt zwei mehrstufige Schieberegister mit linearer Rückkopplung SR3 und SR4. Die Polynome für die Rückkopplungskonfigurationen lauten wie folgt:

$$\begin{aligned} \text{SR3: } 1 + y + y^2 + y^3 + y^5 + y^6 + y^7 + y^9 + y^{10} + y^{11} + y^{15} + y^{19} + y^{23} + y^{27} + y^{31} \\ \text{SR4: } 1 + x^2 + x^3 + x^4 + x^5 + x^7 + x^{11} + x^{13} + x^{14} + x^{20} + x^{29} \end{aligned}$$

Das Initialisierungswort wird wie folgt in SR1 und SR2 geladen: das 60 Bit lange Initialisierungswort wird durch die Folge $I_{59} - I_0$ definiert, wobei I_i jeweils ein Bit darstellt und i Werte zwischen 0 und 59 annimmt.

SR3: I_i wird in $y^{(31-i)}$ geladen, wobei $i = 0$ bis 30

SR4: I_i wird in $y^{(60-i)}$ geladen, wobei $i = 31$ bis 59

Die Schieberegisterausgänge gehen zu einem Multiplexer. Die Eingänge des Multiplexers werden mit A_0 bis A_4 und B_0 bis B_{31} bezeichnet.

Die Anschlüsse sind wie folgt definiert:

x_i wird in $A_{(i-1)}$ geladen, wobei $i = 1$ bis 5
 y_i wird in $B_{(i-1)}$ geladen, wobei $i = 1$ bis 31

Außerdem wird B_{31} mit B_{30} gebrückt.

Das Signal A ist ein 5-Bit-Wort $A_4 \dots A_0$, das die Adresse des Index von Signal B (Binärzahl von 0 bis 31 für $B_{31}-B_0$) definiert. Die am Ausgang anstehenden 16 aufeinanderfolgenden Werte für Signal B bilden das 16 Bit lange Bild-Descramblerwort, und zwar jeweils ein Wort pro Zeile.

Beim "Double cut component"-Rotationssystem wird die Schnittpunktzahl für die Helligkeitskomponente (im Bereich 0 bis 255) durch die Binärzahl $C_7 \dots C_0$ wiedergegeben. Dabei handelt es sich um die am weitesten rechts stehenden 8 Bit im 16-Bit-Schieberegister am Ausgang des Generators PRBS 2.

Die Schnittpunktzahl der Farbdifferenzkomponente (im Bereich 0 bis 255) wird durch die Binärzahl $C_{15} \dots C_8$ wiedergegeben. Dabei handelt es sich um die am weitesten links stehenden 8 Bit im 16-Bit-Schieberegister am Ausgang des Generators PRBS 2.

Beim "Single cut line" - Rotationssystem wird nur die oben beschriebene Schnittpunktzahl der Farbdifferenz verwendet.

ANMERKUNGEN zu Bild 3.3

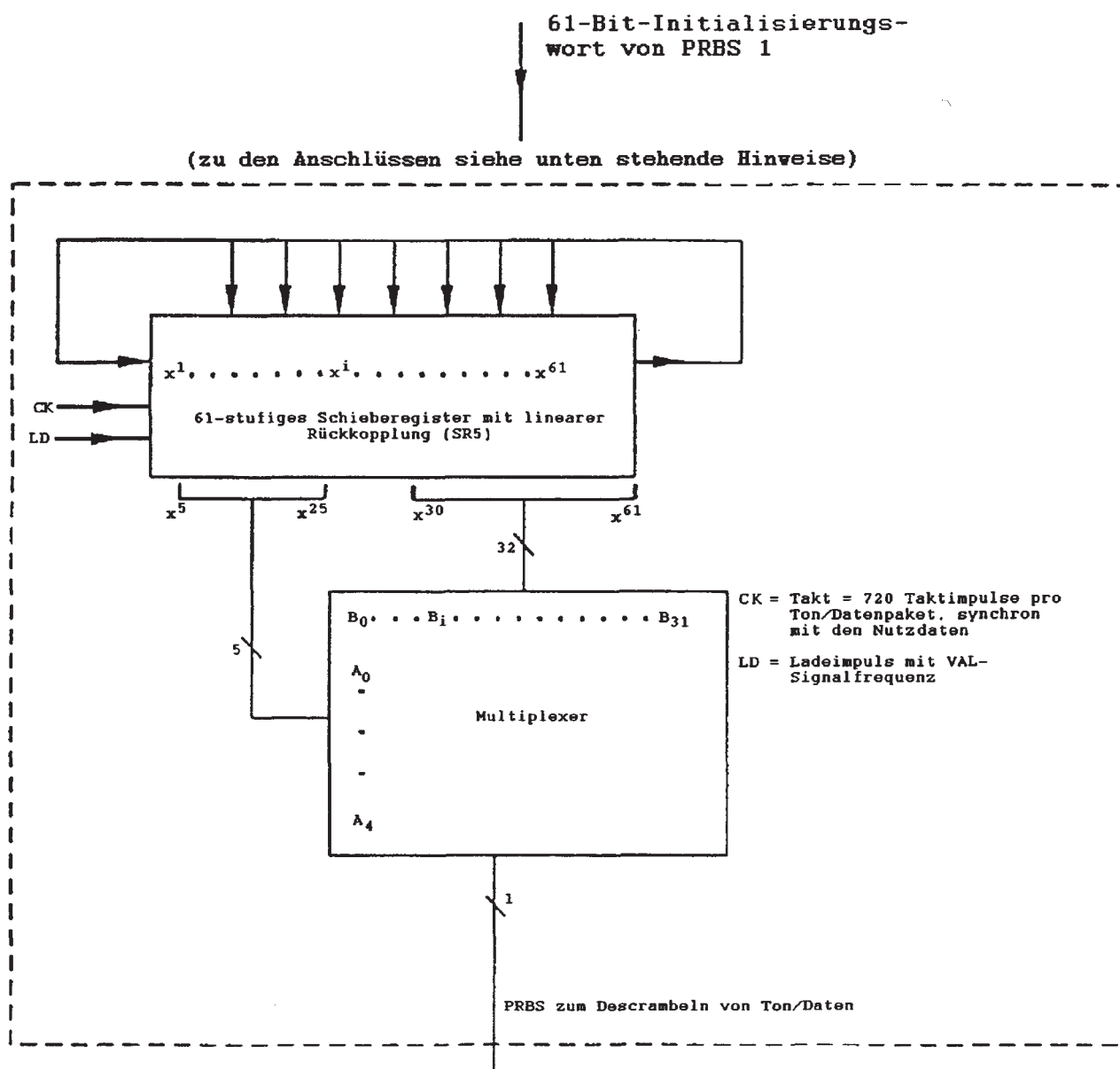


Bild 3.4: PRBS-Generator 3 aus Bild 3.1

ANMERKUNGEN:

Das Blockdiagramm in Bild 3.4 hat folgende Anschlüsse:

Der PRBS-Generator besitzt ein 61-stufiges Schieberegister mit linearer Rückkopplung SR5. Das Polynom für die Rückkopplungskonfiguration lautet wie folgt:

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

Das Initialisierungswort wird wie folgt in SR5 geladen.

Das 61 Bit lange Initialisierungswort wird durch die Folge $I_{60} - I_0$ definiert, wobei I_i jeweils ein Bit darstellt und i Werte zwischen 0 und 60 annimmt.

$$\text{SR5: } I_i \text{ wird in } x^{(60-i)} \text{ geladen, wobei } i = 0 \text{ bis } 60$$

Die Schieberegisterausgänge gehen zu einem Multiplexer. Die Eingänge des Multiplexers werden mit A_0 bis A_4 und B_0 bis B_{31} bezeichnet. Die Anschlüsse sind wie folgt definiert:

$$\begin{array}{l} x^{5(i+1)} \text{ wird in } A_{(i)} \text{ geladen, wobei } i = 0 \text{ bis } 4 \\ x^{(30+i)} \text{ wird in } B_{(i)} \text{ geladen, wobei } i = 0 \text{ bis } 31 \end{array}$$

Das Signal A ist ein 5-Bit-Wort $A_4 \dots A_0$, das die Adresse des Index von Signal B (Binärzahlen 0 - 31 für $B_{31}-B_0$) definiert. Der Wert von Signal B in der durch A definierten Adresse wird mit Taktfrequenz (CLK 2) auf den Ausgang geschaltet und bildet den seriellen Ausgangsdatenstrom, der die gleiche Frequenz hat wie die Nutzdaten.

ANMERKUNGEN zu Bild 3.4

4 Signale, an der Schnittstelle der Zugriffskontrolle

4.1 Schnittstelle zwischen Empfangsgerät und Zugriffskontrollsystem*

4.1.1 Konfigurierung der Schnittstelle zwischen Empfangsgerät und ACS

Empfangsgeräte mit Zugriffskontrolle können, wie Bild 4.1 zeigt, in Module und Systeme unterteilt werden. Das Zugriffskontrollsystem (ACS) wird über eine Empfänger-ACS-Schnittstelle an das Empfangsgerät angeschlossen.

Die Funktionen im Zusammenhang mit dem Demultiplexen der Daten, dem Selektieren der Pakete und dem Dialog zwischen Mensch und Maschine (nur bei Bildschirmausgabe-Modulverwaltung) liegen außerhalb des Zugriffskontrollsystems.

Das Zugriffskontrollsystem kann im Empfangsgerät integriert oder über eine externe Empfänger-ACS-Schnittstelle angeschlossen und abnehmbar sein. Ein Empfangsgerät kann mehr als ein ACS zur Verfügung haben. Die Entscheidung für ein bestimmtes Zugriffskontrollsystem richtet sich nach dem ACS-Typ-Informationsfeld und nach den im ACS vorhandenen Kennungen von Programmbietern.

Die ECM- und EMM-Meldungen werden im Daten-Multiplex zum Zugriffskontrollsystem gesendet. Die Berechtigungs-Verwaltungsmeldungen werden in erster Linie an Einzelteilnehmer oder an spezifische Teilnehmergruppen gesendet; diese sind mit einer Teilnehmeradresse ausgestattet, und zwar mit einer Einzeladresse, wenn es sich um eine Meldung für einen Einzelteilnehmer handelt, oder mit einer Gemeinschaftsadresse, wenn es sich um eine Meldung für eine Gruppe von Teilnehmern handelt. Dabei können nur die EMM-Pakete mit einer korrekten Teilnehmeradresse (Einzel-, Gemeinschafts- oder Kollektivadresse) die Empfänger-ACS-Schnittstelle passieren. Daraus resultiert, daß das Zugriffskontrollsystem seine Teilnehmeradressen an den EMM-Empfangsteil des Empfangsgerätes übergeben muß, bevor die Selektion durchgeführt werden kann.

Die Signale, die die Empfänger-ACS-Schnittstelle passieren, sind in Tabelle 4.1 dargestellt und werden in den Abschnitten 4.1.2 und 4.1.3 im folgenden erläutert.

4.1.2 Signale, die vom ACS empfangen werden

Berechtigungs-Verwaltungsmeldungen EMM dienen dazu, dem Teilnehmer die Möglichkeiten des Zugriffs auf die Dienste, für die er Empfangsberechtigung hat, zu vermitteln. Die EMM kann mit dem MAC/Paket-Signal über einen speziellen Sende-Adressierdienst gesendet werden, und zwar in Form des LISTX-Parameterwertes '04 im Dienst-Identifikationskanal (vgl. Abschnitt 2.1 in Teil 5 des Dokuments Lit. 1). Der ACCM-Parameter zeigt die Kanaladresse des EMM-Paketes im Datenmultiplex an (vgl. Abschnitt 11). Es werden vier verschiedene EMM-Meldungen (EMM-U, EMM-S, EMM-C und EMM-G) unterschieden; alle (außer EMM-G) enthalten eine Teilnehmeradresse, die dem Empfangsgerät (und folglich auch dem ACS) mitteilt, an wen die Meldung adressiert ist. Es passieren nur solche EMM-Pakete die Empfänger-ACS-Schnittstelle, die an das ACS adressiert sind.

EMM-U-Meldungen können auch auf anderem Wege (Post, Telefon usw.) übermittelt werden. Ebenso können Informationen, die mit EMM-S- und EMM-G-Meldungen mitgesendet werden, in Netzen übertragen werden, die keine Rundfunknetze sind; ausgenommen davon sind Meldungen mit Informationen, die mit der Programmaussendung synchronisiert sein müssen und die auf operative Entscheidungen angewiesen sind, z.B. Ersatzleistung und Fingerprint-Identifizierung (EMM-C) usw.

ECM (Berechtigungs-Kontrollmeldungen) gelten für alle Teilnehmer, sind jedoch spezifisch für einen Dienst oder eine Gruppe von Diensten. ECM können nur über Rundfunknetze übertragen werden. Der bzw. die im Dienst-Identifikationskanal beschriebene(n) ACCM-Parameter zeigt bzw. zeigen an, ob ECM und ihre entsprechende Kanaladresse(n) vorliegen (vgl. Abschnitt 2.3 in Teil 5 des Dokuments Lit. 1).

* Die Spezifikation der Eigenschaften einer elementaren, vereinfachten und systemunabhängigen Schnittstelle für ein auswechselbares Zugriffskontrollsystem ist in Beratung.

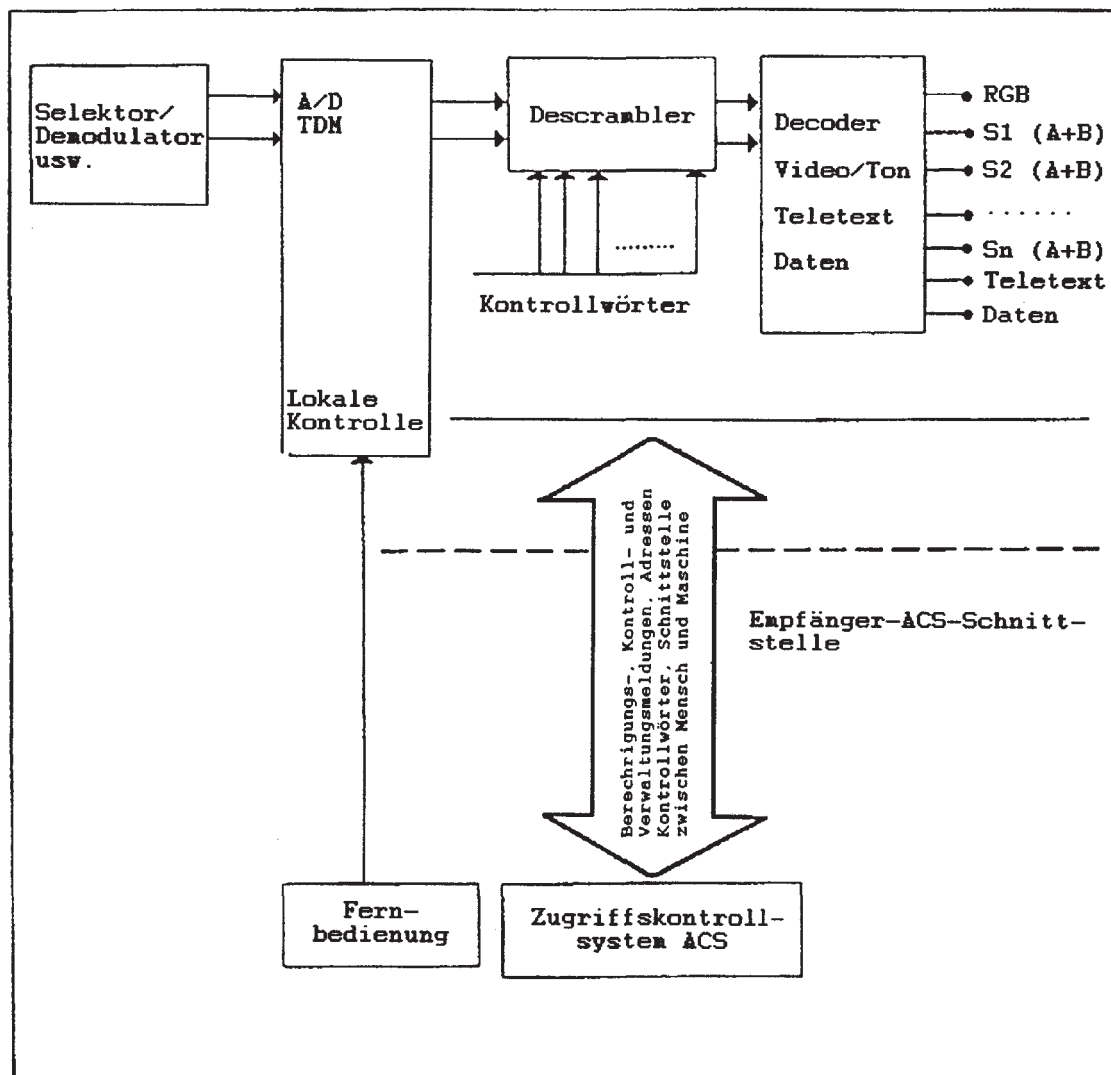


Bild 4.1: Blockdiagramm eines Empfängers und Zugriffskontrollsystems mit einer Empfänger-ACS-Schnittstelle

Das ACS wird mit dem CI-Kode, der in Abschnitt 10.1 (ECM) und Abschnitt 5.1 (EMM) beschrieben wird, angewählt. Wenn zwei ACS des gleichen Typs vorhanden sind, wird beim Anwählen ermittelt, ob Dienst-Kennungen vorhanden sind (wobei eine Dienst-Kennung nur in einem ACS vorhanden sein kann). Schlüssel und Berechtigungen innerhalb des ACS werden mit dem PPID-Parameter, der in den Abschnitten 5.5.3 und 10.4.3 beschrieben wird, angewählt. Diese Parameter sind Zeiger, die auf den gewünschten Schlüssel zeigen. Die Schlüssel-Kennung und die Erzeugung der entsprechenden Kontrollwörter werden in den Abschnitten 4.2 und 4.3 beschrieben.

Der zur Zugriffskontrolle gehörende Dialog zwischen Mensch und Maschine besteht aus zwei Teilen: Verwaltung der Bildschirmausgabe-Module, die sich außerhalb des ACS befinden, und der eigentliche Inhalt des ACS-Dialogs (ausgegebene Meldungen, Art der Tastatureingaben usw.).

Für die einzelnen Dienste bietet das ACS über ein Menü und über einen Befehl, der über die Tastatur des Empfangsgerätes (Fernbedienung) eingegeben wird, die folgenden Möglichkeiten der Bildschirmarbeit:

- Ausgabe der angebotenen Dienst-Zugriffsarten (Abonnement, Pay-per-view pro Programm mit Vorbestellung oder Impulsabbuchung, Pay-per-view pro Zeit mit Impulsabbuchung),
- Ausgabe der vom Teilnehmer gewählten Bildschirmdienst- oder Programmzugriffsart.

Tabelle 4.1: Prinzipieller Informationsaustausch über die Empfänger-ACS-Schnittstelle

Übersicht über die Meldungen, die die Empfänger-ACS-Schnittstelle passieren	Datensignale, die die Empfänger-ACS-Schnittstelle passieren
vom Empfangsgerät zum ACS	vom Empfangsgerät zum ACS
Inhalt der selektierten Pakete	EMM-U-Pakete EMM-S-Pakete EMM-C-Pakete EMM-G-Pakete ECM-Pakete
Informationen aus dem Mensch-Maschine-Dialog	Übertragung der Tastatureingaben
Initialisierung	Initialisierung
vom ACS zum Empfangsgerät	vom ACS zum Empfangsgerät
Kontrollwörter	geradzahlige und ungeradzahlige Kontrollwörter
Teilnehmeradressen	Einzeladresse Gemeinschaftsadresse Kollektivadresse Gruppenadresse
Konfigurationsdaten	Konfigurationsdaten
Daten aus EMM zur Verarbeitung für den Empfänger	Modem-Telefonnummer Datum und Uhrzeit des Aufrufs individuelle Meldungen Authentizitätsprüfungsparameter
Informationen zum Mensch-Maschine-Dialog	Bildschirmausgabedaten

- Ausgabe des gewählten Dienst-Labels (Kurzzeichen),
- Ausgabe des Preises pro Programm oder pro Zeiteinheit,
- Kauf von Programmen,
- Kauf von Zeiteinheiten (Werteinheiten),
- Ausgabe des Restguthabens,
- Ausgabe der Programme, die über Pay-per-view gekauft worden sind: Anzahl und Preise der Programme, Anzahl der verbrauchten Werteinheiten (Pay-per-view pro Zeit),
- Ausgabe der Einzelkundenadresse,
- Ausgabe der Programmanbieter-Nutzeradresse,
- Ausgabe der Gruppenteilnehmeradresse (für die einzelnen Dienste verschieden).

Eine allgemeine Beschreibung der an das ACS gesendeten Pakete finden Sie in den Abschnitten 5.1 und 10.1; die verschiedenen EMM-Formate werden in den Abschnitten 5 bis 9 beschrieben.

4.1.3 Signale vom ACS

4.1.3.1 Im ACS erzeugte Kontrollmeldungen

Das ACS liefert folgende Informationen an den übrigen Teil des Empfangsgerätes:

- die Adresse des Einzelteilnehmers (UA, siehe Abschnitt 5.2),
- die Adresse der Teilnehmergemeinschaft (PPUA, siehe Abschnitt 5.2), entsprechend der aktuellen PPID,
- die Adresse der Teilnehmergruppe (GCA, siehe Abschnitt 5.2), entsprechend der aktuellen PPID, und die Adresse des Teilnehmerkollektivs (CCA, siehe Abschnitt 5.2),
- die Befehlskennungen CI (ACS-Typ), die angeben, welche Pakete vom ACS interpretiert werden können (siehe Abschnitt 5.3), und die Art des Zugriffskontrollsystems CA (siehe Abschnitt 11.3.2),
- die Kontrollwörter, die für den bzw. die gewählten Dienst(e) oder Dienstbestandteile zur Verfügung stehen,
- die Datenkonfiguration für Ersatzleistung und Fingerprint-Identifizierung.

4.1.3.2 Im ACS erzeugte Bildschirm-Meldungen

Auf Wunsch des Teilnehmers können die folgenden Informationen zu den einzelnen Diensten ausgegeben werden:

- die möglichen Dienst-Zugriffsarten (freier Zugriff, Abonnement, vorausgegangener Kauf, Pay-per-view pro Programm oder pro Zeit usw.),
- Zugriffsart für das laufende Programm (Abonnement, Pay-per-view pro Programm oder pro Zeit usw.),
- Preis des Programms oder der Zeiteinheit,
- vorhandenes Guthaben,
- Programmnummer und die für das gekaufte Programm aufgewendeten Kosten oder Werteinheiten,
- Einzeladresse (UA) und aus der PPUA abgeleitete Gemeinschaftsadresse,
- geographischer Kode (GC) und Subjekt-Kode (SC),
- Speichermöglichkeit auf der Berechtigungsspeicherkarte (pro Dienst oder insgesamt),
- Altersgruppengrenze, Sperrzustand des Empfangsgeräts.

Es ist möglich, daß die Hersteller der Empfangsgeräte daran denken, diese Liste durch Diagnose-Informationen für den Kunden zu erweitern.

4.2 Die Dienst-Kennung und die Verbindung zu den Kontrollwörtern

Die Grundlage des Zugriffs zu den verschiedenen Diensten sind die folgenden Parameter:

PPID (24 Bit): ist die Kennung für den Dienst-Vermittler (Programmanbieter). Zeigt auf den für den Dienst oder Dienst-Bestandteil geltenden Schlüssel. Die vier niedrigstwertigen Bits (LSB) der PPID beschreiben den Index des verwendeten Schlüssels. Die 24 Bit für die Länge der PPID wurden gewählt, um die Implementierung der PC2-Karte demonstrieren zu können (siehe Bild 4.2). Außerdem kann bei diesem ACS der Index dazu verwendet werden, zwei Dienst-Schlüssel pro Dienst-Vermittler zu definieren (einen Betriebsschlüssel, der nur zur Berechnung der Kontrollwörter benutzt wird, und einen Verwaltungsschlüssel, der zur Berechnung der Kontrollwörter und zur Eingabe der Berechtigungen benutzt wird). In diesem Fall zeigt das höchstwertige Bit an, ob es sich um einen Betriebsschlüssel (Index '8 bis 'F) oder um einen Verwaltungsschlüssel (Index '0 bis '7) handelt.

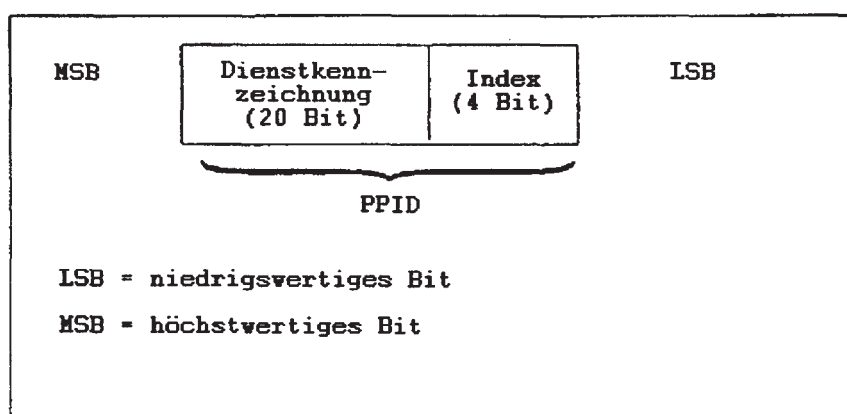


Bild 4.2: Aufbau der PPID

CDATE (16 Bit): definiert das Sendedatum des Dienstes oder Dienst-Bestandteils bei Abonnement-Zugriff.

THEME/LEVEL: (16 Bit) definiert Thema/Klasse eines Dienstes oder Dienst-Bestandteils bei Zugriff über themen- bzw. klassengebundenes Abonnement.

LINK (8 Bit): definiert die Sparte eines Dienstes oder Dienst-Bestandteils bei Zugriff über ein Spartenabonnement. Dieser Parameter zeigt auf ein Bit aus einem Verzeichnis von Sparten, die in der Berechtigungsspeicherkarte gespeichert sind (dieses Spartenverzeichnis kann 8 bis 256 Positionen haben, die sich jeweils aus dem Vielfachen von 8 Bit aufbauen).

PNUMB (24 Bit): definiert die Programmnummer, wenn der Programmanbieter Pay-per-view anbietet.

PPV/P (16 Bit): definiert den Preis des Programms. Nach Kauf besteht während der gesamten Sendezeit Zugriff zum Programm.

PPV/T (16 Bit): definiert die Zugriffskosten für ein Programm während der Gültigkeitsdauer eines Kontrollwortes.

RCI (16 Bit): definiert einen Ersatz-Dienst für ein durch Blackout unterbrochenes Programm.

CTRL (8 Bit): zeigt das Vorliegen eines Blackout an und definiert die Altersgruppengrenze für das Programm. Dieses Byte beschreibt auch, ob die Berechnung des Kontrollwortes das Prüfen bestimmter Kriterien zur Bedingung hat oder ob allein der aktuelle Betriebsschlüssel ausreicht, um die Berechnung durchzuführen.

Jeder durch Scrambling geschützte Dienst oder Dienst-Bestandteil ist mit seinem Kontrollwort über die Adresse des Kanals, der die ECM-Meldungen enthält, verbunden, wobei diese Adresse durch den ACCM-Parameter im Dienst-Identifikationskanal definiert wird (vgl. Abschnitt 4.2.1). Es wird also jeweils für einen Dienst, einen Dienst-Bestandteil oder eine Gruppe von Diensten mit verschiedenen Kontrollwörtern eine ECM-Meldung gesendet.

Die Kontrollwörter werden nicht vom ACS berechnet, bis der entsprechende Dienst-Schlüssel vorhanden ist und die Parameter, die die Programmzugriffsbedingungen definieren, in einer der Berechtigungen in der Teilnehmer-Speicherkarte enthalten sind. Angenommen, der Dienst-Schlüssel ist vorhanden, dann weisen die Ergebnisse der von der Speicherkarte durchgeführten Prüfungen je nach Programmzugriffsart geringe Unterschiede auf:

- **Bei Programmzugriff über ein themen- bzw. klassengebundenes Abonnement** muß der CDATE-Parameter innerhalb der Gültigkeitsdauer des Abonnements (Anfangsdatum - Enddatum) liegen, der LEVEL-Parameter muß kleiner oder gleich der Klasse (LE) sein und THEME muß einem der Themen (TH) entsprechen. Das Anfangsdatum (BD), Enddatum (FD), LE und TH werden unter der PPID des Dienst-Vermittlers gespeichert.
- **Bei Programmzugriff über ein Spartenabonnement** muß der CDATE-Parameter in einem durch BD und FD definierten Zeitraum enthalten sein und der LINK-Parameter muß auf eine gültige Berechtigung im Spartenverzeichnis (CUSTWD) zeigen. Das Spartenverzeichnis und die Gültigkeitsdauer werden unter der PPID des Dienst-Vermittlers gespeichert.
- **Bei Programmzugriff durch Pay-per-view pro Programm** muß der Programmnummern-Parameter PNUMB im Datenschutzprozessor gespeichert werden. Bietet der Programmanbieter die PPV/P-Methode mit Impulsabbuchung an, kann der Teilnehmer das Programm kaufen, wenn sein Restguthaben (CREDIT) höher ist als der vom PPV/P- oder PPV/T-Parameter angezeigte Preis. PNUMB und CREDIT werden unter der PPID des Dienst-Vermittlers gespeichert.

Die Dienst-Schlüssel eines Dienst-Vermittlers werden auch unter einer PPID gespeichert. Es können mehrere Dienst-Schlüssel für einen Dienst-Vermittler gespeichert werden, wobei sich dann nur der "Index"-Teil des PPID ändert, während der aus 20 Bit bestehende "Dienst-Kennungs"-Teil konstant bleibt. Diese Möglichkeit wird geboten, damit mehrere Schlüssel für einen Dienst-Vermittler (Betriebsschlüssel, Verwaltungsschlüssel, ob verschiedenartig oder nicht) nebeneinander bestehen können und damit Schlüssel erneuert werden können. Die Berechtigungen, die bei einem bestimmten Dienst-Vermittler gelten, werden in Transaktionsblöcke eingetragen, und bei diesen Blöcken wird nur der "Dienst-Kennungs"-Teil analysiert; der Index wird ignoriert.

Die Festlegung und die Verwendung der PPID kann völlig unabhängig vom HF-Übertragungskanal geschehen.

- **einer Gruppe von HF-Kanälen** kann ein und dieselbe PPID zugeordnet werden. Alle über diese Kanäle angebotenen Dienste werden mit dem gleichen Dienst-Schlüssel kontrolliert, selbst wenn die Dienste oder Dienst-Bestandteile aufgrund verschieden vereinbarter Zugriffsbedingungen für verschiedene Programmelemente (Abonnement, PPV/P usw.) mit verschiedenen Kontrollwörtern gescrambelt werden können.
- **einem HF-Kanal** kann eine PPID zugeordnet werden. Dieser Kanal wird dann mit seinem eigenen Dienst-Schlüssel kontrolliert, selbst wenn die Dienste oder Dienst-Bestandteile verschiedene Kontrollwörter haben, indem verschiedene Zugriffsbedingungen, wie oben beschrieben, festgelegt worden sind.
- **Dienst-Vermittler, ganz gleich, ob sie einen HF-Kanal gemeinsam benutzen oder mit mehreren HF-Kanälen arbeiten**, können eine eigene PPID bekommen, die dann jeweils durch deren eigenen Dienst-Schlüssel kontrolliert wird und Dienste oder Dienst-Bestandteile je nach Zugriffsbedingungen mit Kontrollwörtern scrambeln lassen kann.

4.3 Erzeugung und Zuweisung von Kontrollwörtern

4.3.1 Erzeugung von Kontrollwörtern

Geradzahlige und ungeradzahlige Kontrollwörter werden in verschlüsselter Form in den Berechtigungs-Kontrollmeldungen ECM, die zu den vom Teilnehmer gewählten Diensten oder Dienst-Bestandteilen gehören, übertragen (siehe Abschnitt 4.2).

Die Dienst-Schlüssel für die Entschlüsselung der Kontrollwörter werden unter der jeweiligen PPID gespeichert.

4.3.2 Zuweisung und Synchronisierung der Kontrollwörter

Die Kontrollwörter werden dem Descrambler bzw. den Descramblern zugewiesen, mit dem bzw. denen der Dienst arbeitet, den der Teilnehmer eingestellt hat.

Kontrollwörter müssen rechtzeitig übertragen werden, und zwar bevor sie effektiv gebraucht werden, damit sie für die gesamte ECM-Empfangszeit sowie die gesamten Prüf- und Rechenzeiten des Datenschutzprozessors zur Verfügung stehen und die Synchronisierung der Descramblersequenzen garantieren können (siehe Abschnitt 3.3).

5 Allgemeine Beschreibung der Berechtigungs-Verwaltungsmeldungen (EMM)

Berechtigungs-Verwaltungsmeldungen werden verwendet:

- für den Sende-Adressierdienst, wenn er eingesetzt wird, zur Vergabe von Berechtigungen oder zur Modifizierung von Schlüsseln,
- zur Verteilung von Ersatzkonfigurationen, wenn solche in Anspruch genommen werden.

5.1 Formate der Meldungen

Bild 5.1 zeigt die vier möglichen Formate der Berechtigungs-Verwaltungsmeldungen (EMM).

Die ersten zwei Felder, PH und PT, sind in allen Paketen vorhanden. Die Paket-Kennung (PH) besteht aus einem 10 Bit langen Adreßfeld, durch das das Paket im Daten-Multiplex von anderen unterscheidbar wird, und einem 2 Bit-Kontinuitätsindex (I). Gleichartige EMM-Pakete können über den Kontinuitätsindex (I) der Paket-Kennung miteinander verknüpft werden. Beim ersten Synchronisierungspaket einer Meldung hat der Kontinuitätsindex immer den Wert Null ($I=0$), während die folgenden Pakete Kontinuitätsindexwerte im Bereich $[1,3]$ haben, wobei der Wert von I immer dann, wenn ein Paket der gleichen Art übertragen wird, um 1 in Modulo-3-Zählung erhöht wird (siehe Bild 5.2). Das PH-Feld wird mit einem (23,12)-Golay-Kode geschützt.

Die Art der Meldung wird im Pakettypenfeld (PT) angegeben, das mit einem (8,2)-Kode geschützt wird, wie in Teil 3, Abschnitt 7.1, des Dokuments Lit. 1 beschrieben. Die vier Werte des PT-Parameters für EMM werden in Bild 5.1 definiert.

Nach dem PT-Parameterfeld haben alle Pakete ein fehlergeschütztes Datenfeld. Der Schutz wird über einen (24,12)-Golay-Kode erreicht; der Datenblock besteht dann aus 30 (24,12)-Golay-Wörtern, was einer effektiven Datenfeldlänge von 360 Bit entspricht, wenn der Schutz wieder aufgehoben ist. Die 24-Bit-Kode-Wörter werden durch den (23,12)-Kode gebildet, der durch die Paket-Kennungen bestimmt wird (vgl. Anhang zu Teil 3 des Dokuments Lit. 1), wobei das 24. Bit eine ungeradzahlige Gesamtparität festlegt.

Alle Synchronisierungspakete haben eine im Klartext vorliegende Befehlskennung (CI), die die Art der Daten in der EMM, den Typ des Verschlüsselungsalgorithmus und das Datenformat innerhalb der EMM angibt. Wenn vorhanden, beschreibt die Parameter-Kennung (PI) den Inhalt der darauffolgenden Daten (das Parameterdatenfeld).

Es werden drei mögliche Arten von EMM beschrieben, bei denen das Teilnehmeradreßfeld vor dem CI-Parameter liegt. Das vierte Format dagegen beginnt mit dem CI-Parameter (diese letzte EMM-Art kann nach dem CI-Parameter eine Gruppenadresse enthalten). Die Inhalte der Berechtigungs-Verwaltungsmeldungen werden weiter unten beschrieben und gelten für EMM-U-, EMM-G-, EMM-S- und EMM-C-Meldungen, die in den Abschnitten 6, 7, 8 und 9 beschrieben werden.

Berechtigungs-Verwaltungsmeldungen werden mit einem (24,12)-Golay-Kode geschützt. Mit der in den Abschnitten 5, 6, 7, 8 und 9 beschriebenen hexadezimalen Kodierung wird der Wert des Datenfeldes der Meldung nach aufgehobenem Golay-Kode beschrieben. Alle folgenden Angaben zu Byte-Größen beziehen sich auf Nutzdaten der Meldung.

Nur die in diesem Dokument beschriebenen CI- und PI-Werte werden von der (im Anhang 1 beschriebenen) PC2-Muster-Implementierung anerkannt.

ANMERKUNG: In den folgenden Teilen dieses Dokuments wird vor hexadezimalen Angaben das Sonderzeichen ' gesetzt (zum Beispiel: '00 und 'A8).

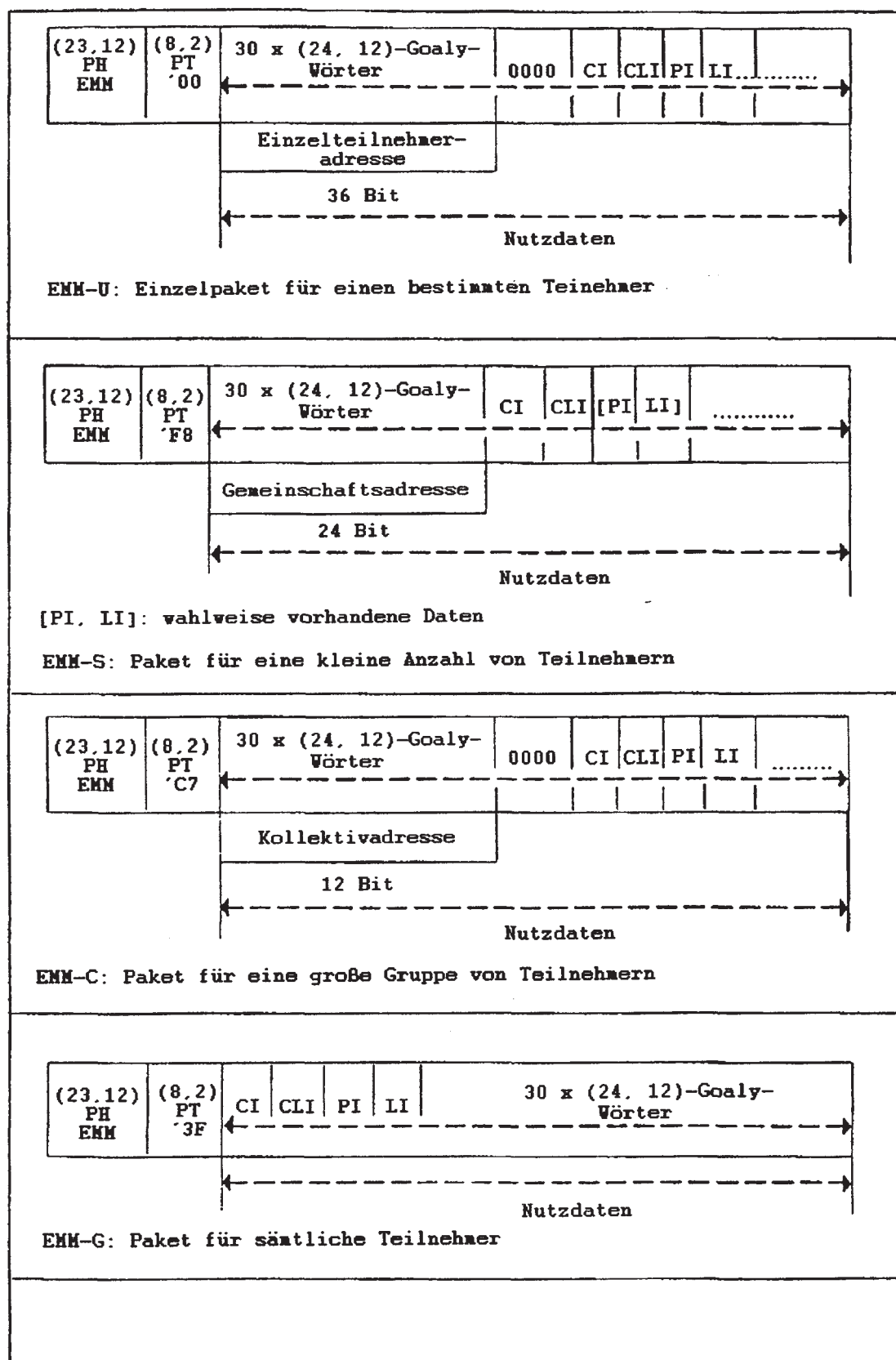


Bild 5.1: EMM-Format

Alle Meldungen mit einem nicht erkannten CI-Parameter werden ignoriert. Nicht erkannte PI-Parameter, die ein Datenfeld mit einem variablen Format einleiten (siehe Bild 5.2) werden ignoriert (ebenso das dazugehörige Datenfeld). Dies führt jedoch nicht dazu, daß die Meldung zurückgewiesen wird. Die im Dokument definierten Parameter sind für einen Anwendungszweck entsprechend ihrer Definition reserviert. Alle mit einer Parameter-Kennung (PI) beginnenden Parameter haben ein Datenfeld mit variablem Format, das mit einem Längenindikator-Flag LI versehen ist.

In den übrigen Teilen dieses Dokuments (Abschnitte 5, 6, 7, 8 und 9) entsprechen Länge und Inhalt der Datenfelder für diese Parameter der (ausführlich in Anhang 1 beschriebenen) ACS-Muster-Implementierung. Bei anderen Implementierungen kann die Länge der Datenfelder für die definierten Parameter vergrößert oder verkleinert werden, vorausgesetzt, daß der aktuell definierte Teil des Feldes benutzbar bleibt. Es können außerdem weitere Parameter eingeführt werden, und zwar unter der Bedingung, daß sie die folgenden Vorschriften, die für die EUROCRYPT-Spezifikation gelten, erfüllen:

- der PPID-Parameter muß in allen EMM mit variablem Format vorhanden sein,
- der HASH-Parameter muß in allen EMM-U, EMM-G zur Eingabe allgemeiner oder freier Erstberechtigungen und EMM-S vorhanden sein.

Die Adreßfelder, die dem CI-Kode vorausgehen, werden mit dem niedrigstwertigen Bit zuerst übertragen; darauf folgen bei Bedarf vier Null-Bits, um eine ganzzahlige Anzahl von Bytes zu bekommen.

Die Parameterdatenfelder haben eine ganzzahlige Anzahl von Bytes. Das höchstwertige Byte ist das Byte mit dem höchstwertigen Bit (MSB). Das niedrigstwertige Byte ist das Byte mit dem niedrigstwertigen Bit (LSB). Die Bytes eines Parameterdatenfeldes werden folgendermaßen übertragen: das höchstwertige Byte zuerst und das niedrigstwertige Byte zuletzt.

Alle Bytes einer Meldung (siehe Bild 5.2), ab einschließlich CI-Kode, werden folgendermaßen übertragen: das niedrigstwertige Bit zuerst und das höchstwertige Bit zuletzt.

Wenn ein Parameterfeld numerierte Bits enthält, wird das niedrigstwertige Bit (LSB) mit b0 bezeichnet.

ANMERKUNGEN zu Bild 5.2:

- PH Paket-Kennung; diese enthält den Kontinuitäts-index I (2 Bit) und die Adresse AN (10 Bit) des gewählten Datenkanals für die Berechtigungs-Verwaltungsmeldungen, wie es im Dienst-Identifikationskanal festgelegt ist.
- PT Pakettyp (2 Bit), siehe Bild 5.1 (X='00, 'F8, 'C7 oder '3F für EMM).
- CA Teilnehmeradreßfeld (0-36 Bit je nach PT-Wert, bei Bedarf bis zu einer ganzzahligen Anzahl von Bytes aufgefüllt mit Nullen), siehe Bild 5.1.
- CI Befehlskennung (8 Bit); diese beschreibt das Format des Parameterfeldes und den Typ des Verschlüsselungsalgorithmus.
- CLI Längenangabe (8 Bit) für das zur CI gehörende Parameterfeld.
- PI Parameterkennung (8 Bit), wahlweise vorhanden.
- LI Längenangabe für das zu PI (8 Bit) gehörende Parameterfeld.
- Ob es sich um die PI-LI-Struktur handelt, hängt ab vom Wert der CI. Die PI-LI-Struktur wird verwendet bei EMM-U, EMM-G, EMM-C und bei einigen EMM-S. EMM-S arbeitet an und für sich mit festem Format.
- Es gibt kein Paket-Suffix am Ende der Pakete.

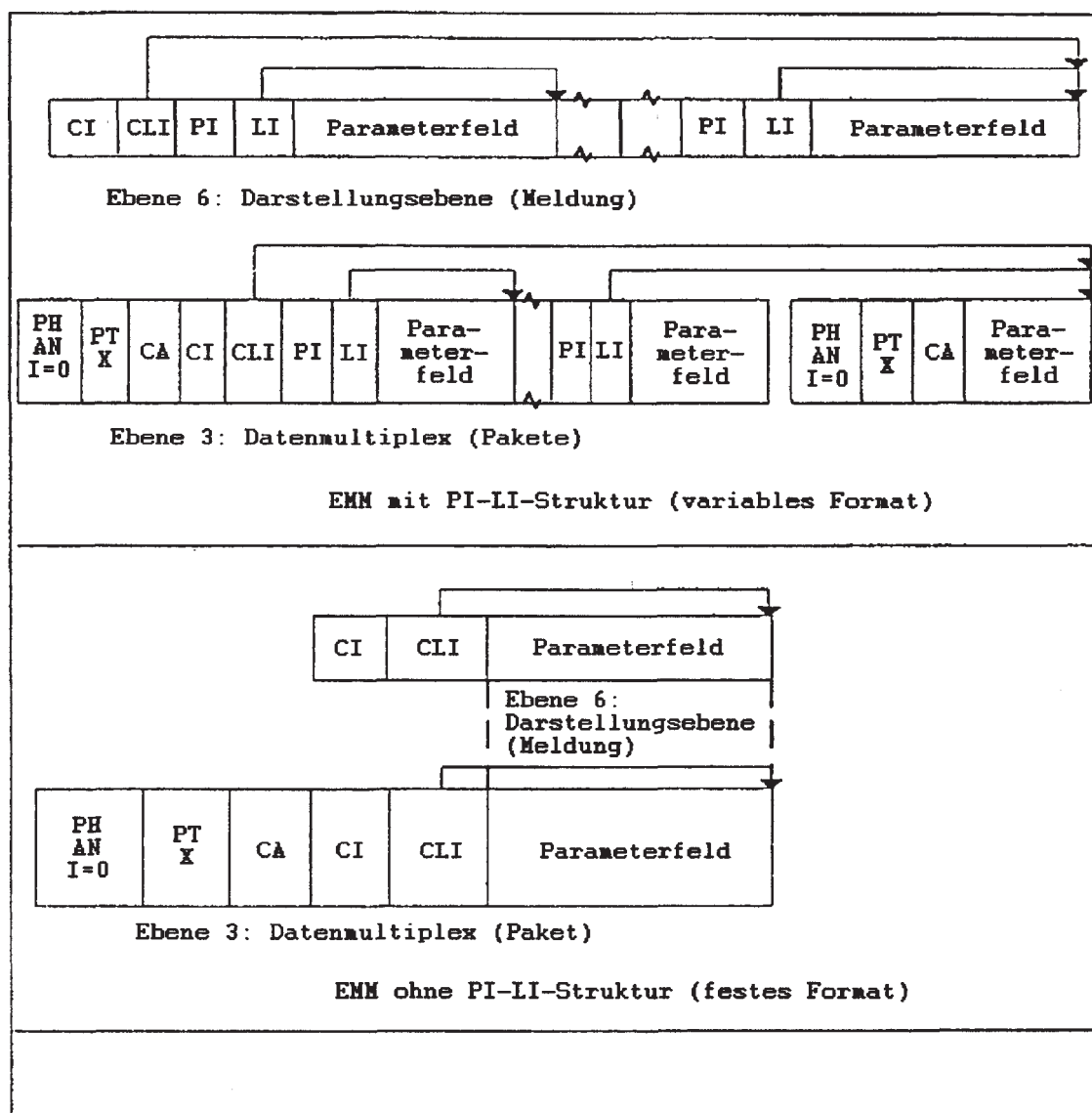


Bild 5.2: EMM-Kodierung zur Übertragung im Daten/Ton-Paketmultiplex: allgemeine Beschreibung

5.2 Teilnehmeradressen

Das ACS kann bis zu vier Arten von Adressen an das Empfangsgerät übergeben:

- eine Einzeladresse mit 36 Bit (UA)

Die UA ist für alle PPID gleich. Sie wird bei der Herstellung des Datenschutzenschalters in das ACS geladen und in einem nicht löschbaren und nicht modifizierbaren Speicher abgespeichert.

- **eine Gemeinschaftsadresse mit 24 Bit (SA) pro PPID**

Diese Adresse definiert eine Gruppe von 256 Teilnehmern zwecks Übertragung der Berechtigungen. Sie wird abgeleitet von der aus 32 Bit bestehenden Programmanbieter-Nutzeradresse (PPUA), die in den 24 höchstwertigen Bits die SA und in den acht niedrigstwertigen Bits die Position des Teilnehmers innerhalb der Gruppe (CUSTWP) enthält. Dieser letzte Parameter, CUSTWP, zeigt auf einen Teilnehmer innerhalb der Gruppe, der Mitinhaber dieser SA ist, wie in Bild 5.3 beschrieben.

Die einzelnen Gruppen werden über ihre SA angesprochen und haben jeweils 256 Teilnehmer. Die Position des Teilnehmers in der Gruppe wird durch den Zeiger CUSTWP (8 Bit) angegeben.

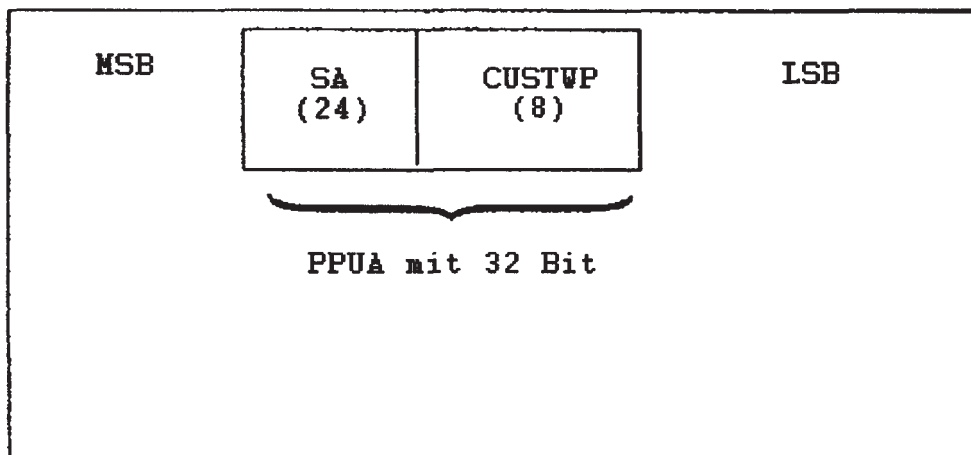


Bild 5.3: Gemeinschaftsadresse (SA) und Teilnehmerposition (CUSTWP)

- **eine Kollektivadresse mit 12 Bit (CCA)**

Die Kollektivadresse CCA wird in Bild 5.4 gezeigt.

Das EMM-C-Format ist für die Übertragung von Ersatzkonfigurationen in Gebieten, die von einem Blackout betroffen sind, reserviert. Der Wert der Kollektivadresse CCA wird auf Null gesetzt.

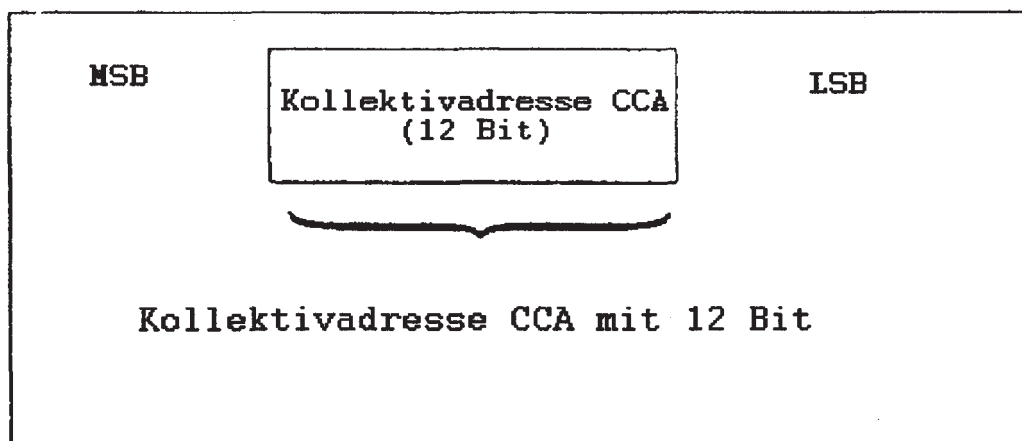


Bild 5.4: Kollektivadresse CCA

- **eine Gruppenadresse mit 32 Bit (GCA) pro PPID**

Die GCA umfaßt zwei Teile, GC und SC, und wird zur Adressierung von Gruppen verwendet, die nach ihrer geografischen Lage und nach bestimmten Kategorien (gemeinsame Interessen, Beruf usw.) unterschieden werden, siehe Bild 5.5.

Die 32 Bit des GCA-Parameters werden durch eine 8-stellige hexadezimale Nummer, abcdefg, dargestellt. Die 24 höchstwertigen Bits sind der geografische Kode (GC=abcdef), und die acht niedrigstwertigen Bits sind der Subjekt-Kode (SC=gh).

Der gespeicherte GC-Kode (abcdef) kann mit den sechs höchstwertigen Stellen der internationalen Telefonnummer des Teilnehmers oder mit der Nummer der Telefonvermittlung, an die er angeschlossen ist, gleichgesetzt werden. Weitere Angaben von nationaler Bedeutung können in dem für die Ländervorwahl bestimmten Teil der Telefonnummer festgelegt werden, und zwar dort, wo die Länder-Vorwahlnummern das betreffende Gebiet nicht eindeutig geografisch beschreiben.

Der gespeicherte SC-Kode (gh) ist einer von den 255 möglichen Subjekt-Kodes.

Der in den EMM-C-Paketen enthaltene GA-Parameter oder der in den ECM-Paketen enthaltene GGA-Parameter wird mit dem im Empfangsgerät gespeicherten GCA-Parameter verglichen. Das übertragene Paket wird erst dann analysiert, wenn die folgenden Bedingungen erfüllt sind:

- die Subjekt-Kodes stimmen überein oder der übermittelte Kategorie-Kode hat den Wert 'FF,
- und die Zeichen des übermittelten GC-Parameters stimmen überein mit den Zeichen des gespeicherten GC-Parameters oder der Wert des übermittelten Zeichens hat den Wert 'F (hexadezimal), siehe Bild 5.5.

Beispiele:

- GC = 'FFFFFF, SC = 'FF: Sammeladresse 'FF (sämtliche Teilnehmer),
- GC = 'FFFFFF, SC = 'CD: Gruppenadresse 'CD (z.B. sämtliche Bridge-Spieler),
- GC = '78FFFF, SC = 'FF: Adresse aller Empfangsgeräte in einem (durch das Telefonnetz definierten) Gebiet mit den Anfangsnummern '78,
- GC = '7883FF, SC = 'FF: Adresse aller Empfangsgeräte in einem (durch das Telefonnetz definierten) Gebiet mit den Anfangsnummern '7883,
- GC = '7883FF, SC = 'CD: Adresse einer bestimmten Gruppe von Empfängern (z.B. Bridge-Spieler) in einem (durch das Telefonnetz definierten) Gebiet mit den Anfangsnummern '7883.

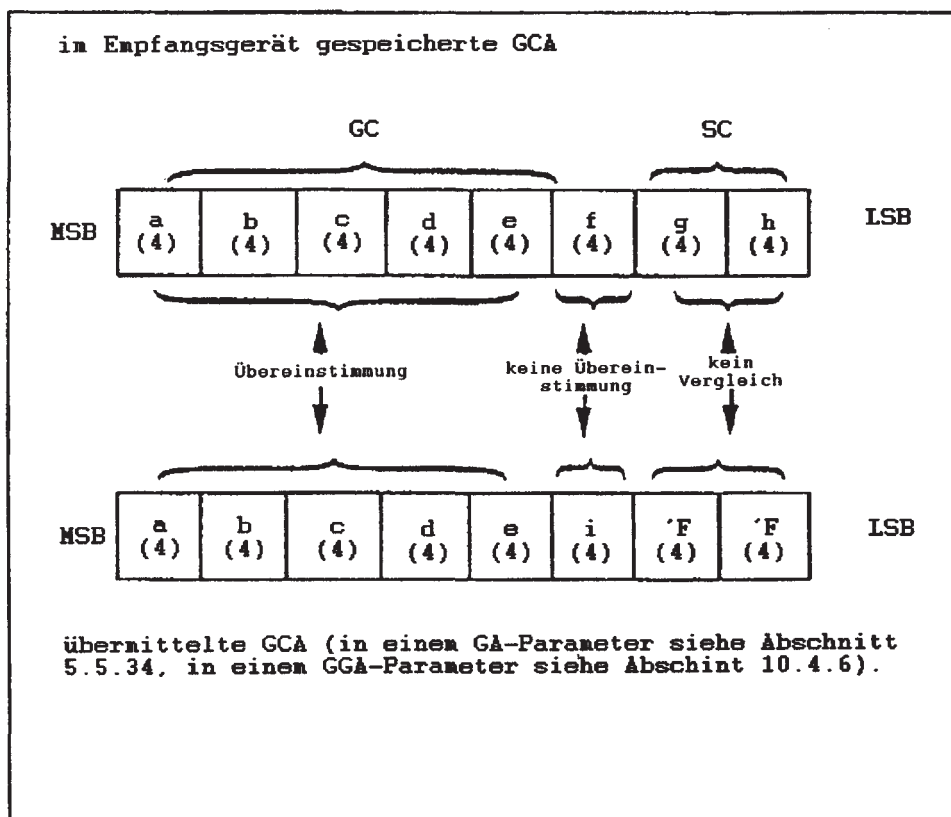


Bild 5.5: Gruppenteilnehmeradresse (GCA) mit einem geografischem Kode (GC) und einem Subjekt-Kode (SC)

Bild 5.5 zeigt ein Beispiel, bei dem die fünf höchstwertigen Halbbytes des gespeicherten GC-Kodes (abcdef), aber nicht das sechste, mit dem übertragenen GC-Kode (abcdei) übereinstimmen. Da der SC-Kode den Wert 'FF (kein Vergleich)' hat, wird dieses Feld nicht verglichen.

Alle EMM-Pakete, die beim Vergleich keine Übereinstimmung mit der Teilnehmeradresse zeigen, bleiben so lange unbeachtet, bis eine Übereinstimmung vorliegt, die besagt, daß das Paket für das ACS von Interesse ist.

UA, SA, GCA und CCA werden in einem nichtflüchtigen Speicher im Datenschutzprozessor abgespeichert.

5.3 Befehlskennung CI

Der CI-Parameter hat 8 Bit. Dieser Parameter beschreibt das für das Parameterfeld verwendete Format und den für die Entschlüsselung benötigten Verschlüsselungsalgorithmus. Er ist in allen EMM-Meldungen enthalten und befindet sich im Synchronisierungspaket der Meldung. Sein Inhalt wird im folgenden beschrieben und in Bild 5.6 dargestellt.

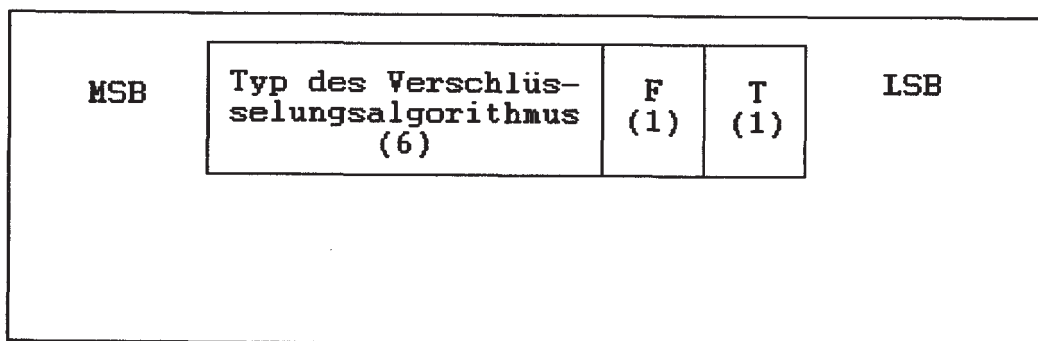


Bild 5.6: Befehlskennung CI

- T wird bei EMM-G und EMM-C verwendet, um eine Veränderung des Informationsgehaltes der Meldungen anzuzeigen (toggle bit). Er wird auch bei EMM-S-Meldungen mit festem Format verwendet, um anzuzeigen, ob das Adreßfeld ADF gescrambelt ist (T=1: ADF ist gescrambelt, T=0: ADF liegt im Klartext vor). Er hat keine Bedeutung für EMM-U. Dieses Bit wird auch als toggle bit bei ECM-Meldungen verwendet (siehe Abschnitt 10.2).
- F ist das Format-Bit, mit dem festgelegt wird, ob das nächste Parameterfeld festes Format (F=0) oder variables Format (F=1) hat, wie in Bild 5.7 dargestellt.
- Typ des Verschlüsselungsalgorithmus (6 Bit). Der aktuelle hexadezimale Wert für dieses Feld wird mit '20 definiert; er entspricht der Muster-Implementierung der im Anhang 1 beschriebenen Berechtigungsspeicherkarte (PC2).

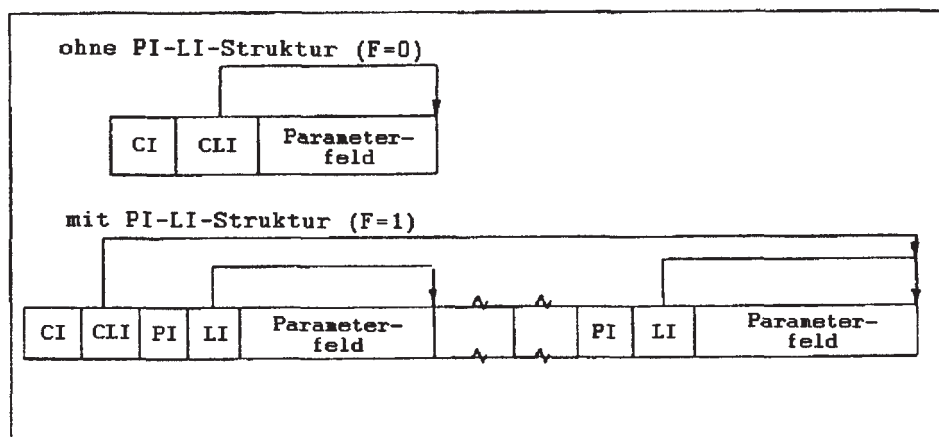


Bild 5.7: Aufbau des Parameterfeldes je nach Format-Bit (F)

5.4 Befehlslängenangabe CLI

Der CLI-Parameter hat 8 Bit. Er zeigt die Anzahl der Bytes im EMM-Datenfeld an. Dieser Parameter ist immer in einer EMM-Meldung enthalten, und zwar nach dem CI-Parameter.

5.5 Parameter-Kennung PI

Die PI-Kodes sind nur dann vorhanden, wenn der CI-Parameter ein Parameterfeld mit variablem Format (F=1) einleitet (siehe Abschnitt 5.3). Auf den PI-Kode folgt ein Byte LI, das die Länge des Parameterfeldes in Bytes angibt.

Die EMM verfügen über alle Informationen, die erforderlich sind für die Aktualisierung oder Konfigurierung des Datenschutzprozessors des Teilnehmers. Mit diesen Parametern wird folgendes beschrieben:

- die Programmanbieter-Nutzeradresse (PPUA), zu der die Gemeinschaftsadresse (SA) und die Position des Teilnehmers innerhalb der Gruppe (CUSTWP) gehören,
- die Gruppenteilnehmeradresse (GCA), zu der der geografische Kode (GC) und der Subjekt-Kode (SC) gehören,
- die Betriebsschlüssel (SK) zur Berechnung des Kontrollwortes,
- die Verwaltungsschlüssel (PDK, die auch als Betriebschlüssel verwendet werden können) für die Eingabe neuer Berechtigungen für den Teilnehmer,
- der Eltern-Kode (PIN-Kode).

Die EMM werden auch verwendet, um Berechtigungen zu erneuern und individuelle Meldungen zu übermitteln. Schließlich können in solchen Meldungen Informationen enthalten sein, die für Blackout-Konfigurierung und Fingerprinting erforderlich sind.

5.5.1 Verzeichnis der möglichen Parameter bei EMM-Meldungen

In dem folgenden Verzeichnis werden alle möglichen PI-Parameter beschrieben (Werte in hexadezimaler Kodierung). Welche Parameter im einzelnen tatsächlich in einer bestimmten EMM auftreten, hängt ab von der Art der zu übertragenden Informationen.

- PI = '70: Software-Parameter (SOFT), wird verwendet, wenn die Meldung Software enthält, die zur Bearbeitung der nachfolgenden Parameter gebraucht wird; dieser Parameter kann nur von einem ACS verarbeitet werden, das die Fähigkeit hat, Software zur Erweiterung einer residenten Anwendung nachzuladen.
- PI = '90: Programmanbieter-Kennung (PPID), bezeichnet den Dienst-Vermittler, der die EMM erzeugt.
- PI = '91: Zufallszahl (RND-ADF), dient als Grundlage der kryptografischen Berechnung zum Descrambeln des Adreßfeldes ADF.
- PI = '92: Zufallszahl (RND-CONF), dient als Grundlage der kryptografischen Berechnung zum Descrambeln der vertraulichen Daten (über den PC-Parameter eingeführte Berechtigungen, wie unten beschrieben, oder Kaufübersichten).
- PI = '93 und '94: Parameter zur Kontrolle der Authentizität des Programmanbieters, wird vor der Kaufübersicht oder der Ausgabe des Teilnehmergeuthabens benutzt.

- PI = '9E: Adreßfeld (ADF); dieser Parameter dient zur Anzeige des Status (Teilnahme erlaubt oder gesperrt) eines Teilnehmers in einer Gruppe von 256 Teilnehmern, die über eine Gemeinschaftsadresse (SA) angesprochen werden. Die einzelnen Teilnehmer werden nacheinander über ihre SA und ihre CUSTWP, die auf das entsprechende Bit der ADF zeigt, angesprochen.
- PI = 'A0: Kontrolle (CTRL); dieser Parameter wird verwendet, um Berechtigungen ungültig zu machen oder aus dem Datenschutzprozessor zu löschen. Er dient auch dazu, freie Erstberechtigungen zu übermitteln oder einen Dienst zu sperren.
- PI = 'A1: Kennung des zu aktualisierenden Datenblocks (IDUP), wird verwendet, wenn ein Schlüssel, ein Deskriptor oder ein Dienst eingegeben oder ungültig gemacht/gelöscht wird.
- PI = 'A2: Deskriptor (DESCR); dieser Parameter wird verwendet zur Eingabe der Speicherzuweisung und des Kontrolldeskriptors eines Programmanbieters. Dieser Deskriptor muß sich im Datenschutzprozessor befinden, damit ein Programmanbieter tätig werden kann; er geht allen anderen Informationen (Schlüssel usw.) voraus. Der Deskriptor bestimmt den maximalen Speicherplatz, der dem Programmanbieter zugewiesen wird, die Dienst-Sperrungsmöglichkeit und die möglichen Zugriffsmethoden wie Abonnement, Pay-per-view pro Programm usw.
- PI = 'A3: Allgemeine Daten (FAC); dieser Parameter wird verwendet zur Eingabe allgemeiner Daten, die unter einer bestimmten PPID zu laden sind. Diese Daten können vom Terminal aus für besondere Funktionen benutzt werden, wie etwa automatische Aufrufe, Eingabe eines Wertes für die Authentizitätsprüfung usw. Dieser Parameter wird auch benutzt, um eben diese Daten wieder zu löschen.
- PI = 'A4: Einzelteilnehmeradresse (UA); dieser Parameter wird verwendet zur Aktualisierung der Einzeladresse des Teilnehmers im Datenschutzprozessor. Wenn diese Adresse im Datenschutzprozessor gespeichert ist, dient sie als Filter für EMM-Meldungen.
- PI = 'A5: Programmanbieter-Nutzeradresse (PPUA); dieser Parameter wird verwendet zur Eingabe oder Aktualisierung der PPUA über EMM.
- PI = 'A6: Gruppenteilnehmeradresse (GCA); dieser Parameter bezieht sich auch auf einen Programmanbieter. Er ist dann vorhanden, wenn GCA über EMM eingegeben oder aktualisiert werden.
- PI = 'A7: Name (LABEL); dieser Parameter ist für jeden Programmanbieter (PPID) spezifisch. Er wird im Dialogbetrieb mit dem Teilnehmer als Name oder Kennung für den Programmanbieter verwendet. Er umfaßt bis zu 16 Zeichen des CCITT-Alphabetes Nr. 5 (Beispiel: CANAL+, SKY usw.).
- PI = 'A8: Datumsangaben (DATES) + Thema/Klasse (TH/LE); dieser Parameter ist vorhanden, wenn ein themen- bzw. klassengebundenes Abonnement in der EMM definiert wird.
- PI = 'A9: Datumsangaben (DATES) + Spartenverzeichnis (CUSTWD); dieser Parameter ist vorhanden, wenn ein Spartenabonnement in der EMM definiert wird.
- PI = 'AA: Anfangsnummer (INUMB) und Endnummer (FNUMB) der Programme; dieser Parameter ist vorhanden, wenn ein oder mehrere aufeinanderfolgende Programme über Pay-per-view mit Vorbestellung gekauft oder wenn bereits eingetragene Programmnummern gelöscht werden. Programme mit im Bereich INUMB-FNUMB enthaltenen Nummern werden gekauft (oder gelöscht). Dieser Parameter wird verwendet bei Pay-per-view mit Vorbestellung, um ein Programm oder eine Reihe von Programmen mit wiederkehrenden Folgen (Serie usw.) einem bestimmten Teilnehmer zuzuweisen (jeder Folge der Serie wird eine PNUMB zugewiesen, die dann jeweils um 1 erhöht wird).

- PI = 'AB: Datum (DATE) + Guthaben (CREDIT); dieser Parameter wird verwendet, wenn einem Teilnehmer ein weiterer Kredit zugewiesen wird. Dieser wird dem Restguthaben hinzugefügt, woraus sich das neue Guthaben ergibt, über das der Teilnehmer verfügen kann. Dieses Guthaben kann mit dem Bezahlungsmodus 'Pay-per-view pro Programm oder pro Zeit mit Impulsabbuchung' bearbeitet werden.
- PI = 'AC: Datum (DATE) + Gesamtguthaben (TOTAM); dieser Parameter definiert den Gesamtbetrag des Guthabens, der dem Teilnehmer zugewiesen wurde, seit er mit dem Programmanbieter verbunden ist. Dabei handelt es sich um eine weitere Form der Kreditgewährung für Teilnehmer; wenn ein Teilnehmer weiteren Kredit braucht, kann dieser in Form von CREDIT oder in Form von TOTAM gewährt werden.
- PI = 'AD: Datum (DATE) + Überziehungsbetrag (OVER); dieser Parameter beschreibt, sofern vorhanden, den Höchstbetrag, um den ein Teilnehmer seinen Kredit bei einem bestimmten Programmanbieter überziehen darf. Dieser Parameter ist vorhanden, um kleine Nachlässigkeiten auszugleichen und einem Teilnehmer das laufende Programm nicht vorzuenthalten, falls er vergessen hat, weiteren Kredit aufzunehmen, wenn sein Guthaben fast aufgebraucht ist. Der Überziehungsbetrag wird natürlich bei der nächsten Kreditgewährung abgezogen.
- PI = 'AE: Datum (DATE) + Kaufübersicht (SURVEY); dieser Parameter ist nur dann vorhanden, wenn Zugriff zu den Diensten über ein dialogfähiges Netz zwischen dem Verwaltungszentrum und dem Datenschutzprozessor des Teilnehmers möglich ist. Die Kaufübersicht ist für solche Teilnehmer erforderlich, die den Bezahlungsmodus 'Pay-per-view pro Programm oder pro Zeit mit Impulsabbuchung' benutzen und um einen Rückblick auf die fälligen Gebühren zu ermöglichen.
- PI = 'AF: Datumsangaben (DATES); dieser Parameter ist vorhanden, wenn zuvor eingetragene Abonnements gelöscht werden, und er definiert einen durch zwei Datumsangaben begrenzten Zeitraum.
- PI = 'C0, 'C2 bis 'C8 und 'CA bis 'CF: Kontrollparameter des Empfänger-Modems.
- PI = 'C1: Modem-Aktivierungskordinaten (MOD) für die Verbindung zum Verwaltungszentrum während des Ruhezustands des Empfangsgerätes.
- PI = 'C9: Die Weckruf-Koordinaten (WAK) zur Erfassung der Berechtigungs-Verwaltungsmeldungen während des Ruhezustands des Empfangsgerätes.
- PI = 'D0 bis 'D7: Kontrollparameter zur Authentizitätsprüfung des Datenschutzprozessors durch das Empfangsgerät. Diese Parameter dienen zur Rekonfigurierung oder, bei Bedarf, zur Verhinderung der Authentizitätsprüfung.
- PI = 'D8: Individuelle Meldung (INDMES), wird verwendet, wenn für den Teilnehmer Text auf dem Bildschirm ausgegeben werden soll.
- PI = 'EE: Eltern-Kode (PIN); dieser Parameter wird verwendet zur Eingabe und Aktualisierung des Eltern-Kodes (Personenkennummer).
- PI = 'EF: Geheimschlüssel (CLE); dieser Parameter wird verwendet zur Eingabe oder Aktualisierung eines Geheimschlüssels.
- PI = 'F0: Signatur (HASH); dieser Parameter sorgt für eine kryptografische Komprimierung aller in der EMM enthaltenen (verschlüsselten und unverschlüsselten) empfindlichen Daten. Die EMM wird in diesem Fall nur dann vom Datenschutzprozessor analysiert und verarbeitet, wenn er Übereinstimmung zwischen der übertragenen Signatur und dem intern erzeugten Resultat der von ihm selbst durchgeführten Komprimierung der Meldung feststellt. Das hat eine kryptografische Redundanz bei den Parametern der EMM zur Folge.
- PI = 'F1: Gruppenadresse (GA); dieser Parameter wird verwendet während der Implementierung eines Blackout oder eines Fingerprintings und stellt ein Verzeichnis der betreffenden Kundengruppen bereit. Der Parameter muß mit dem im Datenschutzprozessor gespeicherten GCA-Parameter übereinstimmen.

- PI = 'F2: Teletext-Dienst (SEI-TXT); dieser Parameter macht Angaben zum Teletext-Dienst, der für Ersatzleistung und Fingerprinting genutzt wird.
- PI = 'F3: Videosignalersatz (TTP1); dieser Parameter bestimmt die Teletext-Seite, die das Videosignal ersetzen soll.
- PI = 'F4: Ersatz des Fernseh-Tones (RCI-R1); dieser Parameter bestimmt einen Tondienst, der den Fernseh-Ton ersetzen soll.
- PI = 'F5: Zusätzlicher digitaler Hörfunk- oder Teletext-Ersatz (RCI-02, RC-R2); dieser Parameter wird verwendet, um einen digitalen Dienst zu konfigurieren, der einen weiteren Dienst ersetzen soll.
- PI = 'F6: Teletextseite für Fingerprinting (TTP2); dieser Parameter wird verwendet, wenn das Videosignal-Fingerprinting mit einer bestimmten Teletextseite aktiviert wird.
- PI = 'F7: Fingerprint-Kontrolle (FCRL); Zu diesem Parameter gehören drei getrennte Datenfelder, FMOD, LOCUA, FDUR, die in der entsprechenden Reihenfolge folgende Bedeutung haben: Fingerprint-Modus, Position der Einzeladresse und Dauer des Fingerprinting.

Ein Gruppenparameter PG, kodiert mit '80, wird eingeführt, um die oben beschriebenen PI-Parameter zu kombinieren. Die dazugehörige Längenangabe PLI zeigt auf das Ende der jeweiligen Parametergruppe. Dieser Parameter wird immer dann verwendet, wenn für eine Meldung mehr als eine Signatur erforderlich ist. Das kann beispielsweise vorkommen, wenn in der gleichen Meldung der erste Schlüssel eines Dienstes übertragen wird, auf den das Dienst-LABEL folgt (siehe Bild 5.8):

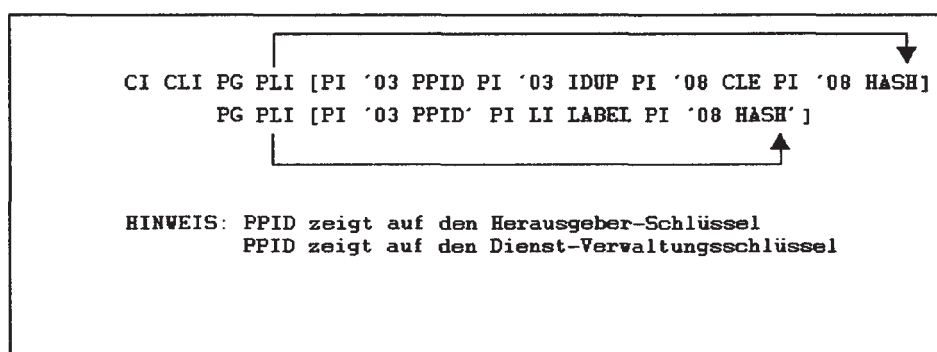


Bild 5.8: Verwendung des Gruppenparameters PG

Ein Vertraulichkeitsparameter PC, kodiert mit '81, wird eingeführt für die Übertragung gescrambelter Daten (um die gesetzlichen Regelungen zum Schutz der Privatsphäre zu erfüllen). In diesem Falle werden alle Daten in der Meldung gescrambelt (die einzelnen Parameter haben Kodierungen zwischen 'A0 und 'EF). Die Länge LC bestimmt die Länge des gescrambelten Datenfeldes (siehe Bild 5.9).

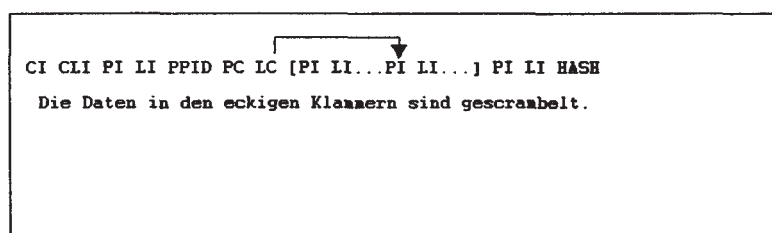


Bild 5.9: Verwendung des Vertraulichkeitsparameters PC

5.5.2 Parametergruppen bei EMM

Es werden vier Parametergruppen definiert:

- Gruppe 1:

PG-Parameter (PGI = '80)

- Gruppe 2:

Parameter, die spezifische PC-EUROCRYPT-Befehle erzeugen.

- Teilmenge 2.1: Zu dieser Gruppe gehören die folgenden Parameter:

PPID (PI = '90)

RND-ADF (PI = '91)

RND-CONF (PI = '92)

- Teilmenge 2.2: Parameter mit einem PI zwischen '93 und '9F,

- Teilmenge 2.3: PC-Parameter (PCI = '81).

- Gruppe 3:

Parameter mit einem PI von 'A0 bis einschließlich 'F0, die in diesem Dokument definiert oder undefiniert sind.

- Gruppe 4:

Weitere in diesem Dokument definierte oder undefinierte Parameter.

- Teilmenge 4.1: Parameter mit einem PI zwischen '00 und '7F

- Teilmenge 4.2: Parameter mit einem PI zwischen '82 und '8F

- Teilmenge 4.3: Parameter mit einem PI zwischen 'F8 und 'FF

Parameter zwischen 'F1 und 'F7 sind ausschließlich für EMM-C bestimmt.

5.5.3 Vorschriften zur Reihenfolge der Parameter in den EMM-U und EMM-G

- Vorschrift A:

Es werden nur Parameter der Gruppe 3 zwischen dem PC-Parameter und dem nächsten HASH-Parameter eingefügt.

- Vorschrift B:

Zwei PG-Parameter werden durch einen HASH-Parameter getrennt und umgekehrt.

- Vorschrift C:

Ist kein PG-Parameter vorhanden, so gelten zwischen zwei PG-Parametern und dem nächsten, zuletzt übertragenen PG-Parameter die Vorschriften C-1, C-2, C-3, C-4 und C-5.

- Vorschrift C-1: Parameter der Gruppe 2 werden in der Reihenfolge 2.1, 2.2, 2.3, ohne daß Parameter von anderen Gruppen eingefügt werden, vor den Parametern der Gruppe 3 und mit strenger aufsteigender Reihenfolge innerhalb jeder Teilmenge übertragen.

- Vorschrift C-2: der PPID-Parameter ist Pflicht und tritt genau einmal auf.

- Vorschrift C-3: Parameter der Gruppe 3 werden übertragen, ohne daß Parameter von anderen Gruppen eingefügt werden.

- Vorschrift C-4:

- * Für den Fall, daß EMM-U und EMM-G für sämtliche Teilnehmer gilt (ohne dazugehörige EMM-S):

- Wenn Parameter der Gruppe 3 außer HASH-Parameter übertragen werden, dann ist der HASH-Parameter Pflicht und muß unbedingt als letzter innerhalb der Parameter der Gruppe 3 stehen.

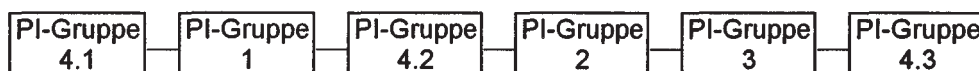
- * Für den Fall, daß EMM/G und EMM/S zusammengehören:

- Der HASH-Parameter ist in der EMM-G nicht vorhanden. Er wird durch die EMM-S übermittelt.

In der EMM-G sind die Parameter der Gruppe 3 die letzten, die übertragen werden.

- Vorschrift C-5: Parameter der Gruppe 4.1 werden vor Parametern aus anderen Gruppen übertragen, Parameter der Gruppe 4.2 werden vor Parametern aus Gruppe 2 und Parameter der Gruppe 4.3 nach Parametern aus anderen Gruppen übertragen.

Daraus ergibt sich, daß eine EMM-U oder EMM-G folgendermaßen aufgebaut sein muß:



5.5.4 Softwaredaten SOFT

PI = '70 LI = Länge der Softwaredaten Wert = Anwendungsnummern+ Software-Code Name = SOFT
--

Dieser Parameter wird angewendet, wenn für die Analyse der nachfolgenden Parameter zusätzliche Software erforderlich ist. Der zu übertragende Software-Kode aktualisiert die im Gerät eines Teilnehmers residente Software. Diese Funktion wird nur implementiert, wenn das ACS die Fähigkeit besitzt, mit nachladbarer Software zu arbeiten. Bei der in Anhang 1 beschriebenen Muster-Implementierung wird sie nicht realisiert.

- Anwendungsnummer (1 Byte): Dieser Parameter bestimmt die Nummer der Anwendung, entsprechend dem übertragenen Software-Kode. Dieser Parameter kann für eine Software-Abarbeitung in einer Anwendung im Gerät eines Teilnehmers verwendet werden.
- Software-Kode: Die auf die Anwendungsnummer folgenden Daten beschreiben den Software-Kode, der in das zur Anwendungsnummer gehörende ACS geladen werden muß.

5.5.5 Programmanbieter-Kennung PPID

PI = '90 LI = '03 Wert = Programmanbieter-Bezeichnung Name = PPID
--

Dieser Parameter bezeichnet den Programmanbieter, der die EMM erzeugt. Dieser Parameter ist Pflicht bei EMM-U, EMM-G und EMM-C.

Die Anwendung dieses Parameters zeigt geringe Unterschiede je nach der von der EMM-Meldung bestimmten Betriebsart:

- Bei der Eingabe von Berechtigungen oder bei der Aktualisierung von Teilnehmeradressen (siehe Abschnitte 6, 7 und 8) zeigt der Parameter auf den dem Programmanbieter im ACS zugewiesenen Speicherbereich.
- Der Parameter zeigt auf den aktuellen Schlüssel, mit dem die Geheimwort-Verschlüsselung oder die Integritätsprüfungsfunktionen realisiert werden.
- Der Parameter benennt den Programmanbieter, wenn es um Ersatzleistung und Fingerprint-Identifizierung geht (siehe Abschnitt 9).

5.5.6 Zufallszahl RND-ADF (zur Descramblung des Adreßfeldes)

PI = '90 LI = '08 Wert = Zufallszahl Name = RND-ADF
--

Dieser Parameter wird verwendet, um den Descramblungsvorgang im Adreßfeld ADF zu initialisieren. Dieser Parameter wird normalerweise nicht in EMM übertragen; sein (Standard-)Wert wird vom ACS auf NOT(HASH) gesetzt.

5.5.7 Zufallszahl RND-CONF (zur Descramblung von vertraulichen Daten)

PI = '92
LI = '08
Wert = Zufallszahl
Name = RND-CONF

Dieser Parameter wird verwendet, um die Descramblung der vertraulichen Daten zu initialisieren. Dabei kann es sich um die Descramblung von in EMM enthaltenen Berechtigungen oder die Descramblung von einer über das Modem laufenden Kaufübersicht handeln. Dieser Parameter wird normalerweise nicht in EMM übertragen; sein (Standard-)Wert wird vom ACS auf HASH gesetzt. Bei der Funktion 'Kaufübersicht' wird die Zufallszahl auf HASH gesetzt.

5.5.8 Authentizitätsprüfung des Programmanbieters oder des Herausgebers

Die Authentizitätsprüfung des Programmanbieters muß immer dem über das Modem erfolgenden Zugriff zur Funktion 'Übersicht über die Gesamtteilnehmer' und der Information über das Kundenguthaben vorausgehen. Der Vorgang läuft in zwei Stufen ab: Erzeugung der Zufallszahl durch den Datenschutzprozessor und Übermittlung an den Programmanbieter. Danach erfolgt die Berechnung anhand des Dienst-Schlüssels des Programmanbieters. Das Ergebnis der Berechnung wird zur Überprüfung an den Datenschutzprozessor übermittelt. Wird Übereinstimmung mit dem Ergebnis der vom Datenschutzprozessor intern durchgeführten Berechnung festgestellt, so gilt die Authentizitätsprüfungsphase als erfolgreich abgeschlossen, und das ACS akzeptiert die Ausführungsanweisung für die Funktion 'Gesamtteilnehmerübersicht' oder die Anweisung zum Lesen des Kundenguthabens. Eine genaue Definition dieser Parameter erfolgt später.

5.5.9 Adreßfeld ADF

PI = '9E
LI = '20
Wert = Adreßfeld
Name = ADF

Dieser aus 256 Bit bestehende Parameter legt für die einzelnen Teilnehmer in der Gruppe mit einer gemeinsamen SA-Adresse in der EMM-S fest, ob die betreffende EMM-S für den jeweiligen Teilnehmer bestimmt ist oder nicht. Der Datenschutzprozessor des Teilnehmers zeigt auf das entsprechende Bit im Adreßfeld mit dem Wert CUSTWP. Die Felder CUSTWP und SA werden von der PPUA des Programmanbieters, PPID, abgeleitet. Das Adreßfeld wird verwendet, wie in Bild 5.10 beschrieben.

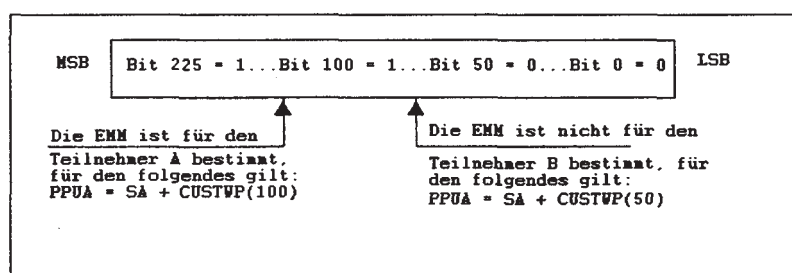


Bild 5.10: Adreßfeld ADF

Dieses Feld kann auch vor der Übertragung gescrambelt werden. Das ADF-Feld ist (ohne PI-LI-Format) in einer EMM-S mit festem Format vorhanden.

5.5.10 Kontrolle CTRL

PI = 'A0
LI = '01
Wert = Betriebsart
Name = CTRL

Der CTRL-Parameter wird verwendet, um die Betriebsart zu beschreiben, wenn spezielle Funktionen implementiert werden wie etwa Ungültigmachung (oder Löschung), Eingabe einer freien Erstberechtigung oder Sperrung eines Dienstes.

Die Kodierung dieser Parameter ist in Bild 5.11 dargestellt.

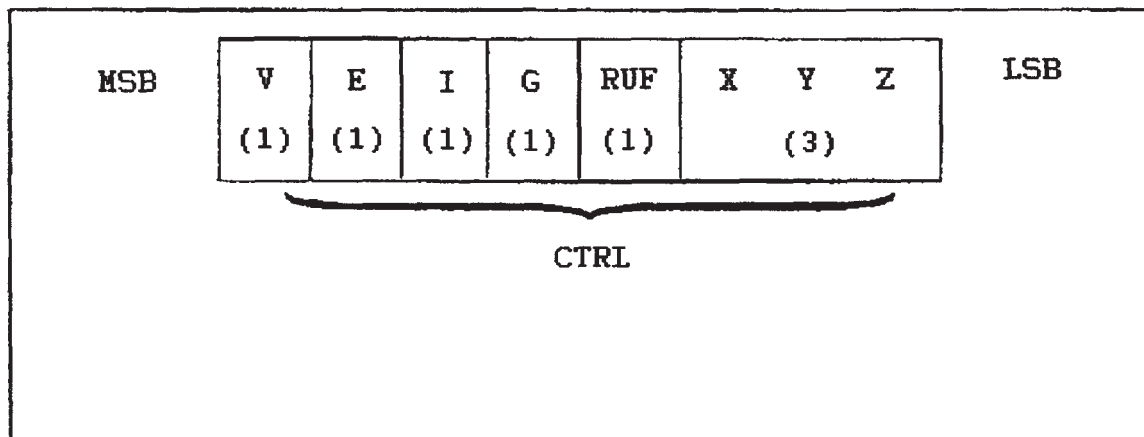


Bild 5.11: CTRL-Parameter

Die vier Flag-Bits V, E, I und G sind unabhängig voneinander. Wenn sie auf 0 gesetzt sind, wird keine spezielle Funktion ausgelöst; wenn sie auf 1 gesetzt sind, wird die jeweilige Funktion ausgelöst.

Wenn I oder E = 1, dann wird die Funktion 'Ungültigmachung oder Löschung' aktiviert. Der Wert im Feld XYZ bestimmt, um was für eine 'Ungültigmachung oder Löschung' es sich handelt.

XYZ = 000	Der mit IDUP bezeichnete Dienst wird ungültig gemacht (I=1); die unter IDUP eingegebenen Informationen sind nicht mehr nutzbar. Alle Informationen werden gelöscht, wenn E=1 ist. Wenn IDUP der Herausgeber ist, dann führt die Ungültigmachung oder Löschung zur totalen Sperrung des Datenschutzprozessors.
XYZ = 001	Der unter der Dienst-Kennung eingegebene Gesamtdatenblock IDUP (zu den Daten-Kennungen NP1 NP2 siehe Abschnitt 5.5.13) wird ungültig gemacht oder gelöscht.
XYZ = 010	Der Schlüsselblock, auf den IDUP zeigt, wird ungültig gemacht oder gelöscht.
XYZ = 011	Reserviert für eine spätere Verwendung
XYZ = 100	Die Abonnements per Thema/Klasse oder per Spartenblöcke unter PPID werden gelöscht (Ungültigmachung ist hier nicht möglich).
XYZ = 101	Die vorbestellten oder per Impuls abzubuchenden Programmblöcke unter PPID werden gelöscht (Ungültigmachung ist hier nicht möglich).
XXX = 110	Reserviert für eine spätere Verwendung
XXX = 111	Reserviert für eine spätere Verwendung

Die Löschung von Abonnements (per Thema/Klasse oder per Sparte) ist mit Hilfe des DATES-Parameters beschrieben, indem ein durch zwei Datumsangaben begrenzter Zeitraum, für den die Löschung gelten soll, bestimmt wird (alle Abonnements, bei denen das Datenfeld innerhalb des Bereiches DATES liegt).

Die Löschung von Programmen, die durch Pay-per-view mit Vorbestellung oder Impulsabbuchung erworben worden sind, wird durch die Parameter INUMB + FNUMB beschrieben. Dabei wird der Bereich von Programmnummern festgelegt, für die die Berechtigung gestrichen werden soll (alle Berechtigungen, bei denen die Programmnummern im Bereich INUMB, FNUMB enthalten sind, werden gelöscht).

Die Ungültigmachung oder Löschung von allgemeinen Daten kann durch den FAC-Parameter definiert werden, der dann festlegt, daß die Datenkennung NP1 NP2 (siehe Abschnitt 5.5.13) innerhalb eines Dienstes ungültig gemacht oder gelöscht werden soll.

ANMERKUNG: Bei der im Anhang 1 beschriebenen Muster-Implementierung der PC2-Karte in EPROM-Technologie sind nur die folgenden Möglichkeiten der Ungültigmachung erlaubt: XYZ=000, XYZ=001 und XYZ=010.

Der Datenschutzprozessor **implementiert eine Standard-Ungültigmachung**, wenn ein Parameter wie LABEL, eine Adresse, ein Schlüssel, eine Überziehung des Guthabens oder ein Deskriptor eintrifft und vorher schon ein anderer solcher Parameter gespeichert worden ist.

Wenn G = 1, dann enthält die EMM eine freie Erstberechtigung.

Das ACS läßt es zu, daß ein Programmanbieter jedem neuen Abonnenten eine freie Berechtigung erteilt. Diese Möglichkeit ist jedoch reserviert für die erste Eingabe von Berechtigungen für den betreffenden Programmanbieter. Damit kann der Programmanbieter eine Vorschau seines Dienstes anbieten, um potentielle Teilnehmer anzusprechen. Wie die freie Erstberechtigung realisiert wird, bleibt dem Programmanbieter überlassen (z.B. ein freies Abonnement für einen Tag, einen Probierkredit auf der Basis von Pay-per-view). Diese freie Erstberechtigung wird vollständig in der EMM-G beschrieben und kann eine Berechtigung aus den vom Programmanbieter angebotenen, verschiedenen Zugriffsmethoden sein.

Die EMM-G, die eine freie Erstberechtigung beschreiben, werden in regelmäßigen Zeitabständen zusammen mit dem Programm gesendet. Die Analyse der EMM-G setzt die ausdrückliche Zustimmung des Teilnehmers voraus, wenn dieser Teilnehmer* vorher keine Berechtigung für den betreffenden Programmanbieter hatte (das bedeutet, daß eine freie Erstberechtigung nicht automatisch bei Empfang der EMM-G eingegeben wird.)

Die Eingabe einer freien Erstberechtigung läuft folgendermaßen ab:

- Das ACS stellt fest, daß unter PPID keine Berechtigung vorhanden ist.
- Das ACS wartet auf eine EMM-G, die eine (in der PPID angegebene) freie Erstberechtigung genauer beschreibt.
- Das ACS teilt dem Teilnehmer mit, daß für die betreffende PPID keine Berechtigung besteht, und bittet den Teilnehmer, einer freien Erstberechtigung zuzustimmen*.
- Wenn der Teilnehmer zustimmt, verarbeitet das ACS die empfangene EMM-G.

ANMERKUNG: Die Eingabe von Berechtigungen für sämtliche Teilnehmer ist eine weitere Möglichkeit, die die EMM-G bietet. Allerdings ist diesmal der Eintrag nicht beschränkt auf die Ersteingabe; in diesem Fall ist G = 0. Von seiten des Datenschutzprozessors besteht bei dieser Möglichkeit der freien Erstberechtigung keine Beschränkung. Ein Programmanbieter kann mit dieser Methode arbeiten, um die Effizienz der Verwaltung (in bezug auf die Übertragungszeit) zu maximieren, und zwar im Hinblick auf solche Arbeitsschritte, die sämtliche Teilnehmer betreffen, einschließlich der Änderung oder Hinzufügung von Geheimschlüsseln oder der Übertragung von "Geschenk-Berechtigungen" für sämtliche Teilnehmer. Bei dieser Methode wird von seiten des Teilnehmers keine ausdrückliche Reaktion gefordert. Wenn eine solche EMM-G eintrifft, wird sie automatisch analysiert.

* Vorläufige Ergebnisse von Experimenten haben gezeigt, daß die ausdrückliche Zustimmung durch den Teilnehmer bestimmte Nachteile haben könnte. Sie könnte nämlich unterdrückt werden, und das Empfangsgerät würde dann grundsätzlich EMM mit einer freien Erstberechtigung annehmen.

Wenn $V = 1$, sperrt der Programmanbieter seinen Dienst. Nach diesem Vorgang kann der Herausgeber keine Schlüssel für diesen Dienst mehr eingeben oder aktualisieren. Es können nur noch Verwaltungsschlüssel des Programmanbieters verwendet werden, um die Schlüssel des Dienstes einzugeben oder zu aktualisieren. Diese Funktion kann nur implementiert werden, wenn sie vom Herausgeber im Programmanbieter-Deskriptor als erlaubt definiert ist (siehe Abschnitt 5.5.12).

RUF, für eine spätere Verwendung reserviertes Bit.

Wenn ein CTRL-Parameter in der EMM mit übertragen wird, dann wird er mit der HASH-Funktion auf seine Integrität überprüft. Er ist immer dann in der EMM vorhanden, wenn eine Ungültigmachung oder eine spezielle Datenschutzfunktion implementiert worden ist. Wenn der CTRL-Parameter nicht in der EMM vorhanden ist, nimmt er den Standardwert '00 an: keine spezielle Funktion implementiert.

5.5.11 Identifizierung von Aktualisierungsdaten IDUP

PI = 'A1 LI = '03 Wert = Identifizierung von Aktualisierungsdaten Name = IDUP
--

Dieser Parameter wird verwendet, um einen Dienst-Schlüssel, einen Dienst-Deskriptor oder einen Dienst einzugeben oder ungültig zu machen bzw. zu löschen. Er beschreibt die Kennung, unter der der Schlüssel, Deskriptor oder Dienst gespeichert, ungültig gemacht oder gelöscht wird.

Die Beschreibung der IDUP ist identisch mit der der PPID (vgl. Abschnitt 4.2).

5.5.12 Deskriptor DESCR

PI = 'A2 LI = '03 Wert = Programmanbieter-Deskriptor Name = DESCR
--

Dieser Parameter bestimmt die Parameter, die festlegen, wie der Programmanbieter mit dem Datenschutzprozessor arbeitet. Im einzelnen bestimmt er folgendes:

- die dem Programmanbieter zuzuweisende maximale Speicherkapazität in Bytes (2 Byte),
- die Betriebsarten (1 Byte), bei denen es die folgenden Möglichkeiten gibt:
 - themen- bzw. klassengebundenes Abonnement,
 - Sparten-Abonnement,
 - Pay-per-view pro Programm mit Vorbestellung,
 - Pay-per-view pro Programm mit Impulsabbuchung,
 - Pay-per-view pro Zeit,
 - Dienst-Sperrung.

Dieser Deskriptor muß im Datenschutzprozessor vorhanden sein, und er bereitet die Eingabe aller anderen auf den Programmanbieter bezogenen Informationen (Schlüssel, Berechtigungen usw.) vor. Er wird unter der Kontrolle des Herausgebers eingegeben.

Dieser Parameter ist in den EMM-Meldungen enthalten, wenn der Programmanbieter-Deskriptor eingegeben oder aktualisiert wird.

Das Format dieses Parameters ist in Bild 5.12 dargestellt.

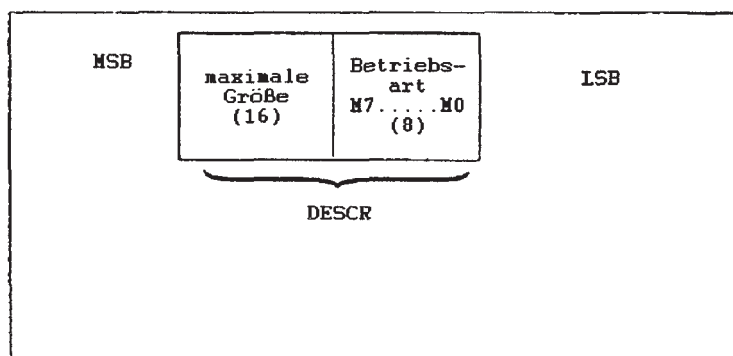


Bild 5.12: DESCR-Parameter

- M0 = themen- bzw. klassengebundenes Abonnement,
- M1 = Sparten-Abonnement,
- M2 = Pay-per-view pro Programm mit Vorbestellung,
- M3 = Pay-per-view pro Programm mit Impulsabbuchung,
- M4 = Pay-per-view pro Zeit mit Impulsabbuchung,
- M7 = Dienst-Sperrung.

Bei $M_i = 1$ wird die Funktion aktiviert. Die Funktion Dienst-Sperrung ermöglicht es dem Programm-anbieter die Verwaltung seiner Dienst-Schlüssel unabhängig vom Herausgeber zu kontrollieren. Diese Möglichkeit, die durch Aussenden einer EMM mit dem im Kontroll-Byte CTRL gesetzten V-Bit implementiert wird, setzt jedoch voraus, daß der Herausgeber dies akzeptiert, und zwar dadurch, daß er das Bit M7 im Deskriptor setzt.

5.5.13 Allgemeine Daten FAC

PI = 'A3
LI = n
Wert = NP1 NP2 (2 Byte) [+ No (1 Byte) + allgemeine Daten]
Name = FAC

Mit dem FAC-Parameter kann ein Herausgeber oder Programmanbieter seine eigenen Daten ein-führen, ohne daß diese vom Datenschutzprozessor als Teil der Datenschutzfunktionen des Systems interpretiert werden. Diese Daten können allerdings von den Datenendgeräten bzw. Emp-fangsgeräten interpretiert werden, so daß diese eine Reihe von spezifischen Arbeitsschritten wie au-tomatische Herstellung von Verbindungen, Kartenauthentizitätsprüfung usw. durchführen. Jedem FAC-Datenblock ist ein Datenkennung, NP1 NP2, zugeordnet, der die spezifische Datenart (Nummer des Aufrufs, Authentizitätswert) bestimmt. Die FAC-Datenblöcke werden durch Unterblöcke beschrieben, deren Nummer durch No wiedergegeben wird. Dieser Unterblock-Aufbau ermöglicht die Eingabe von langen variablen Blöcken.

Bild 5.13 zeigt das Format des FAC-Parameters.

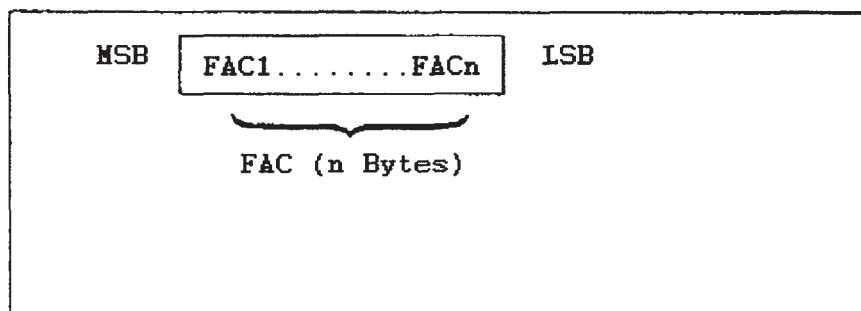


Bild 5.13: FAC-Parameter