Doc. PS/70A
10 June 2004

Proposed Standard: Conditional Access System for Terrestrial Broadcast, Revision A

Advanced Television Systems Committee
1750 K Street, N.W.
Suite 1200
Washington, D.C. 20006
www.atsc.org

The Advanced Television Systems Committee, Inc., is an international, non-profit organization developing voluntary standards for digital television. The ATSC member organizations represent the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries.

Specifically, ATSC is working to coordinate television standards among different communications media focusing on digital television, interactive systems, and broadband multimedia communications. ATSC is also developing digital television implementation strategies and presenting educational seminars on the ATSC standards.

ATSC was formed in 1982 by the member organizations of the Joint Committee on InterSociety Coordination (JCIC): the Electronic Industries Association (EIA), the Institute of Electrical and Electronic Engineers (IEEE), the National Association of Broadcasters (NAB), the National Cable Television Association (NCTA), and the Society of Motion Picture and Television Engineers (SMPTE). Currently, there are approximately 140 members representing the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries.

ATSC Digital TV Standards include digital high definition television (HDTV), standard definition television (SDTV), data broadcasting, multichannel surround-sound audio, and satellite direct-to-home broadcasting.

Table of Contents

1. SCOPE 6

1.1 Purpose 6

1.2 Application 6

1.3 Organization 6

2. REFERENCES 7

3. DEFINITIONS 7

3.1 Compliance Notation 7

3.2 Acronyms and Abbreviations 8

3.3 Definition of Terms 9

3.4 Reserved Fields 9

3.5 Section and Data Structure Syntax Notation 9

4. ATSC CONDITIONAL ACCESS ARCHITECTURE 9

4.1 ATSC CA Simulcrypt Standards 9

4.1.1 Scrambling Standard 9

4.1.2 Multiplexer and Scrambler Interfaces 9

4.1.3 Transport Stream Extensions and Constraints 10

4.2 ATSC CA Scrambling 12

4.2.1 Replaceable Scrambling Algorithm 12

4.2.2 Scrambling Algorithm 12

4.2.3 Modes of Operation 12

4.2.4 Scrambling Method 12

4.2.5 Scrambling Control Field 12

4.2.6 Scrambling Identification 13

4.3 ATSC CA Return Channel 13

4.4 Renewable Security Interface 13

4.4.1 Interface Chosen 13

4.4.2 Number of Sockets 13

4.4.3 NRSS-B Man Machine Interface 13

4.4.4 NRSS Homing 14

4.4.5 NRSS Chaining 14

4.4.6 NRSS Copy Protection Framework 14

ANNEX A. MAPPING OF MPEG PAYLOAD BYTES INTO THE DES BLOCK (NORMATIVE)...................15

ANNEX B. TRIPLE-DES SCRAMBLING MODES (INFORMATIVE) 17

B1. 56-Bit Single DES 17

B2. 168-Bit Triple DES 17

B3. 112-Bit Mode of 168-Bit TDES 18

B4. 56-Bit Mode of 168-Bit TDES 18

B5. ABC EDE TDES Cipher Block Chaining 19

ANNEX C. BROADCAST HEADEND SECURITY (INFORMATIVE) 21

ANNEX D. AN OVERVIEW OF THE CONDITIONAL ACCESS STANDARD FOR TERRESTRIAL BROADCAST (INFORMATIVE)....22

D1. Introduction 22

D2. System Elements 22

D3. Common Scrambling Algorithm 26

D4. Transport Stream Messages for CA 28

D5. Signaling the Existence of Conditional Access Services 30

Index of Tables and Figures

Table 4.1 Table ID Values 10

Table 4.2 ATSC Conditional Access Descriptor 11

Table 4.3 CA Descriptor Usage 11

Table 4.4 Transport Scrambling Control Values 12

Table A.1 Transport Stream Packet Payload and DES Bits 16

Figure B.1 FIPS 46-2 56-bit single DES. 17

Figure B.2 168-bit EDE processing. 17

Figure B.3 Alternate symbology for ATSC TDES. 18

Figure B.4 112-bit mode of 168-bit TDES. 18

Figure B.5 56-bit mode of 168-bit TDES. 19

Figure B.6 Basic ABC EDE TDES Cipher Block Chaining. 20

Figure D.1 Main elements of a Conditional Access system. 25

Figure D.2 Scrambling algorithm and Terminating Short Block. 27

Figure D.3 Scrambling of a Solitary Short Block. 28

Figure D.4 Triple DES as a cascade of three DES encryption/decryption engines. 28

Figure D.5 Contents of the Conditional Access Table. 30

Figure D.6 Conditional Access Content of a Program Map Table. 31

Proposed Standard: Conditional Access System for Terrestrial Broadcast, Revision A

1. SCOPE

1.1 Purpose

This document defines the Conditional Access system for ATSC Terrestrial Broadcasting. Prepared by the Specialist Group on Service Multiplex and Transport Systems (T3/S8), the necessary building blocks are called out that will enable broadcasters to fully exploit the capabilities of digital broadcasting using ATSC. This standard is based, whenever possible, on existing open standards.

No presumption of a business model is made by this standard: in fact, the likelihood is great that multiple business models will exist. This standard instead defines only building blocks necessary to ensure interoperability (that is, any ATSC CA module can operate with any ATSC compatible hosts designed to support ATSC CA). As the ATSC CA module is replaceable, ATSC hosts are protected against obsolescence as security is upgraded and this standard can be expected to last as long as the ATSC standard itself does.

For an informative description of the concepts and elements defined in this protocol, first time readers are encouraged to start with Annex D.

1.2 Application

This document describes an architecture that shall be applicable to terrestrial (over-the-air) broadcast systems. Applicability of this document to cable and satellite broadcast systems is outside the scope of this document.

This standard applies to the broadcasters of ATSC signals and services and to the ATSC receiver manufacturers for the purpose of allowing the broadcaster to field pay services using a conditional access system. This standard applies to all CA vendors that supply CA service on behalf of an ATSC service provider.

1.3 Organization

The sections of this document are organized as follows:

- **Section 1 –** Provides a general introduction.
- **Section 2 –** Lists references and applicable documents.
- **Section 3 –** Provides a definition of terms and a list of acronyms and abbreviations used in this document.
- **Section 4 –** Describes the ATSC Conditional Access elements.
- **Annex A –** Mapping of MPEG payload bytes into the DES block
- **Annex B –** Triple-DES scrambling modes
- **Annex C –** Broadcast headend security
- **Annex D –** An overview of the CA Standard for Terrestrial Broadcast

2. REFERENCES

The following documents are applicable to this Standard:

[1] ATSC Standard A/53C (2004), "ATSC Digital Television Standard," Advanced Television Systems Committee. (*Normative*). Available from the ATSC at www.atsc.org.

[2] ATSC Standard A/65B (2003), "Program and System Information Protocol for Terrestrial Broadcast and Cable (PSIP)." (*Normative*). Available from the ATSC at www.atsc.org.

[3] CEA 679-B (1999), "National Renewable Security Standard (NRSS)," Consumer Electronics Association (*Normative*). Available from Global Engineering Documents at www.global.ihs.com.

[4] ETSI TS 101 197 V1.2.1 (2002-02), "Technical Specification of DVB Simulcrypt," February 2002, European Telecommunications Standards Institute. (*Informative*). Available from ETSI at www.etsi.org.

[5] ISO/IEC 13818-1:2000, Information Technology — Generic coding of moving pictures and associated audio — Part 1: Systems. (*Normative*). Available from the International Telecommunications Union at www.itu.org (as ITU-T Rec. H.222.0), and Global Engineering Documents at www.global.ihs.com.

[6] FIPS PUB 46-3 (1999), "Specification for the Data Encryption Standard," National Institute of Standards and Technology. (*Normative*). Available from the U.S. Department of Commerce, National Technical Information Service at www.itl.nist.gov/fipspubs/.

[7] FIPS PUB 74 (1981), "Guidelines for Implementing and Using NBS DES," National Institute of Standards and Technology. (*Informative*). Available from the U.S. Department of Commerce, National Technical Information Service at www.itl.nist.gov/fipspubs/.

[8] FIPS PUB 81 (1980), "DES Modes of Operation," National Institute of Standards and Technology. (*Normative*). Available from the U.S. Department of Commerce, National Technical Information Service at www.itl.nist.gov/fipspubs/.

[9] "Data Encryption Standard – Cipher Block Chaining Packet Encryption Specification," ANSI/SCTE 52 2003, Society of Cable and Telecommunications Engineers, 1 July 2003 (*Normative*). Available from the SCTE at www.scte.org.

[10] ETR 289 ed.1 (1996-10), "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcast systems," European Telecommunications Standards Institute (*Informative*). Available from ETSI at www.esti.org.

[11] BS EN 50221, "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications," August 1997. (Certain sections *Normative*). Available from Global Engineering Documents at www.global.ihs.com.

3. DEFINITIONS

3.1 Compliance Notation

As used in this document, "shall" denotes a mandatory provision of the standard. "Should" denotes a provision that is recommended but not mandatory. "May" denotes a feature whose presence does not preclude compliance that may or may not be present at the option of the implementer.

3.2 Acronyms and Abbreviations

The following acronyms and abbreviations are used within this Standard:

ABA TDES	112-bit Triple DES used in “encrypt-decrypt-encrypt” mode
ABC TDES	168-bit Triple DES used in “encrypt-decrypt-encrypt” mode
ATSC	Advanced Television Systems Committee
bslbf	bit serial, leftmost bit first
CA	Conditional Access
CAM	Conditional Access Module
CAT	Conditional Access Table
CBC	Cipher Block Chaining
CW	Control Word. The key used for MPEG Transport Scrambling.
DES	Data Encryption Standard
DTV	Digital Television
DVB	Digital Video Broadcasting
ECB	Electronic Codebook (DES Cipher Mode)
ECM	Entitlement Control Message
EDE	Encrypt-Decrypt-Encrypt
EIT	Event Information Table
EMM	Entitlement Management Message
HTML	Hypertext markup language
IV	Initialization Vector, also referred to as the Whitener
MGT	Master Guide Table
MMI	Man-Machine Interface
MPEG	Moving Picture Experts Group
NRSS	National Renewable Security Standard (see [3])
PCR	Program Clock Reference
PES	Packetized Elementary Stream
PID	Packet Identifier
PMT	Program Map Table
PSI	Program Specific Information
PSIP	Program and System Information Protocol
SCTE	Society of Cable Telecommunications Engineers
TDES	Triple DES
TS	Transport Stream
uimsbf	unsigned integer, most significant bit first

VCT	Virtual Channel Table
unicode	Unicode™

3.3 Definition of Terms

The following terms are used throughout this document:

encryption – The method of protecting EMM and ECM messages by cryptographic methods.

host – A device where module(s) can be connected. For example, a television, an integrated receiver-decoder, or a PC.

module – A small device, not working by itself, designed to run specialized conditional access processing in association with a host. For example, a conditional access subsystem.

scrambling – The method of obscuring digital streams by cryptographic methods.

3.4 Reserved Fields

reserved – Fields in this Standard marked "reserved" shall not be assigned by the user, but shall be available for future use. Decoders are expected to disregard reserved fields for which no definition exists that is known to that unit. Each bit in the fields marked "reserved" shall be set to one until such time as they are defined and supported.

user_private – Indicates that the bit or bit field is not defined within the scope of this Standard. The owner of the bit, and hence the entity defining its meaning, is derived via its context within a message.

zero – Indicates that the bit or bit field shall have the value zero.

3.5 Section and Data Structure Syntax Notation

This document contains symbolic references to syntactic elements. These references are typographically distinguished by the use of a different font (e.g., restricted), may contain the underscore character (e.g., sequence_end_code) and may consist of character strings that are not English words (e.g., dynrng).

The formats of sections and data structures in this document are described using a C-like notational method employed in ISO/IEC 13818-1 [5].

4. ATSC CONDITIONAL ACCESS ARCHITECTURE

This section describes the building blocks that comprise the ATSC Conditional Access system: Simulcrypt, Common scrambling, Host CA Software, Return Channel, and CA Module Interface.

4.1 ATSC CA Simulcrypt Standards

4.1.1 Scrambling Standard

A common scrambling standard is necessary for Simulcrypt. The initial ATSC CA common scrambling shall be as described in Section 4.2.

4.1.2 Multiplexer and Scrambler Interfaces

This Standard does not specify or define multiplexer or scrambler interfaces. However, to maximize interoperability and to support multiple CA vendors, it is recommended that these interfaces comply with the principles outlined in Part 1 and Part 2 of the DVB Simulcrypt Technical Specification referenced in Section 2.

4.1.3 Transport Stream Extensions and Constraints

4.1.3.1 Conditional Access Table

There shall be a Conditional Access Table (CAT), as defined in ISO/IEC 13818-1 [5]. The CAT shall contain one or more CA_descriptor, as defined in ISO/IEC 13818-1 [5]. Each CA_descriptor provides the PID for EMMs for a particular conditional access system.

A list of CA_system_id values shall be managed by ATSC. A set of CA_system_id values shall be given to each CA provider.

NRSS-B CA modules shall filter the CAT table. NRSS-A CA modules may filter the CAT table.

4.1.3.2 Table ID Values for CA Support

Transport Stream PSI sections shall be as defined in ISO/IEC 13818-1 [5]. Table 4.1 defines the table_id values reserved for CA support, this is an extension on ISO/IEC 13818-1 [5].

Table 4.1 Table ID Values

table_id Value	Description
0x80	CA message section, ECM
0x81	CA message section, ECM
0x82 – 0x8F	CA message section, EMM and CA System private

4.1.3.3 CA Controlled Service

As required in A/65, any program which has one or more streams controlled by conditional access shall have the access_controlled bit in the VCT set to be '1'. The access_controlled bit does not indicate how many streams are controlled by conditional access.

4.1.3.4 PMT Usage Description

The PMT as described in ISO/IEC 13818-1 [5] is mandatory. For each program with conditional access, the PMT shall contain one or more CA descriptors. The CA descriptors shall provide the PIDs for ECMs for each scrambled PID that comprises a virtual channel or program.

The changes of the PMT version number should be minimized.

4.1.3.5 ATSC CA Descriptor

4.1.3.5.1 Definition of ATSC CA Descriptor

The ATSC_CA_descriptor contains CA related information. Its content is CA provider dependent. Its content shall be provided to the CA dependent hardware and software when event inquiry or impulse purchase is performed. The ATSC_CA_descriptor is defined by Table 4.2.

Table 4.2 ATSC Conditional Access Descriptor

Syntax	No. of Bits	Format
ATSC_CA_descriptor() {		
descriptor_tag	8	0x88
descriptor_length	8	uimsbf
CA_System_ID	16	uimsbf
for (i = 0 ; i < descriptor_length - 2 ; i++) {		
private_data_byte	8	bslbf
}		
}		

descriptor_tag – This 8-bit unsigned integer shall have the value 0x88, identifying this descriptor as the ATSC_CA_descriptor.

descriptor_length – This 8-bit unsigned integer specifies the length (in bytes) immediately following this field up to the end of this descriptor.

CA_System_ID – This 16-bit unsigned integer indicates the type of CA system applicable for the information conveyed in this descriptor. The coding of the information conveyed in this descriptor is privately defined and it is not specified in this document.

4.1.3.6 Usage of CA Descriptors

Conditional access descriptors may exist in several different tables, as shown in Table 4.3.

Table 4.3 CA Descriptor Usage

Descriptor Name	Descriptor Tag	CAT	PMT	MGT	VCT	EIT
ATSC_CA_descriptor	0x88				O	O
CA_descriptor	0x09	M	M			

Table 4.3 shall be interpreted as described in [2] Section 6.9. When present, the ATSC_CA_descriptor may be present in any location shown with an “O”. When present, the CA_descriptor shall be in each location shown with an “M”.

For the ATSC_CA_descriptor, if the same CA related information applies to all events on a channel, then that information may appear in the VCT only. If specific CA related information is needed for an event, an ATSC_CA_descriptor may be added to the EIT for this event. If an ATSC_CA_descriptor exists in both the VCT and EIT, the ATSC_CA_descriptor in the VCT shall override the ATSC_CA_descriptor in the EIT.

For each program with conditional access, the CAT and PMT shall contain one or more CA descriptors.

4.1.3.7 PID Assignment for CA

The CAT and the PMT contain CA descriptors which identify PID values for CA data. Two CA systems shall not have common CA PID values in the same Transport Stream. Packets labeled with CA PID values shall be used to carry only CA information.

4.2 ATSC CA Scrambling

4.2.1 Replaceable Scrambling Algorithm

The descrambling function shall be performed by the replaceable CA module. This section specifies the initial ATSC common scrambling/descrambling algorithm.

4.2.2 Scrambling Algorithm

The ATSC scrambling algorithm shall use FIPS 46-2 DES in “ABC EDE Triple DES” mode, with key size of 168 bits.

4.2.3 Modes of Operation

ATSC CA shall use Cipher Block Chaining (CBC) mode with ABC EDE TDES, as specified in references [6], [7], and [8].

4.2.3.1 Initialization Vectors

The Initialization Vectors (IVs) shall be set to zero. Note that the term Whitener is used in ANSI/SCTE 52 [9] instead of the term Initialization Vector. These two terms are equivalent.

4.2.3.2 Basic Cipher Block Chaining

ABC EDE TDES packet scrambling shall be performed using Cipher Block Chaining (CBC). TDES scrambles data in blocks that are 8 bytes long, however there may be a short block (e.g., less than 8 bytes) remaining at the end of a Transport Stream packet. The CBC shall be block-by-block starting at the beginning of the Transport Stream packet body. The Transport Stream packet header and adaptation field (if any) shall not be scrambled. Any short block will therefore occur at the end of the Transport Stream packet.

4.2.3.3 Solitary and Terminating Short-Block Processing

Terminating short blocks are short blocks that have one or more complete blocks preceding. Solitary short blocks are short blocks that do not have one or more complete blocks preceding. Terminating short blocks (residual termination blocks) and solitary short blocks (solitary termination blocks) shall be treated as described in ANSI/SCTE 52 [9].

4.2.4 Scrambling Method

Only transport-level scrambling shall be used. PES-level scrambling shall not be used.

4.2.5 Scrambling Control Field

The following values from Table 4.4 shall be used in the transport_scrambling_control field of the ISO/IEC 13818-1 [5] Transport Stream packet (§ 2.4.3.2) (see [10]):

Table 4.4 Transport Scrambling Control Values

Bit Values	Description
00	No scrambling of TS packet payload
01	Reserved
10	Transport packet scrambled with Even key
11	Transport packet scrambled with Odd key

4.2.6 Scrambling Identification

A descrambling identifier is required in order to allow a transition from one descrambling algorithm to another or to support more than one descrambling algorithm at a time. This identification method is not described in this Standard; the conditional access system and the replaceable module should communicate this information privately (for example, in ECMs).

4.3 ATSC CA Return Channel

The ATSC return channel is optional for hosts supporting ATSC CA. When a return channel is available, the host shall establish a connection at the request of the CA module. The CA module shall be responsible for the management of any communication protocols (e.g., PPP, etc.) necessary for setting up a return channel. Host support for this functionality shall be consistent with the communications resources interface specification of NRSS.

4.4 Renewable Security Interface

4.4.1 Interface Chosen

The NRSS interface shall be used. The host shall support either NRSS Part A (smart card) or NRSS Part B (PCMCIA) form factors or both. No CA system specific information (hardware or software) shall be required in the host device. The host shall completely implement the appropriate NRSS interface.

4.4.2 Number of Sockets

The host shall provide at least one NRSS interface to enable use of modules for CA. Hosts may support additional NRSS connections to support Multicrypt CA and/or other functionality such as e-commerce, memory or return path extensions.

4.4.3 NRSS-B Man Machine Interface

The NRSS part B interface specifies an HTML engine in the host for display of CA-originated text. The host shall not be required to implement the HTML MMI features. If HTML MMI features are implemented, the host shall implement the HTML MMI as described in NRSS part B.

A host that implements NRSS part B shall implement DVB Common Interface High Level MMI, as specified in [11] §8.6 with the following changes:

- Where [11] states “Text delivered by display objects in high level mode is coded according to [4].” change to “Text delivered by display object in high-level mode shall be coded according to the multiple string structure in [2] Section 6.10”.
- Where [11] states “In [4] character table selection for text fields (if different from the default) is indicated by the initial byte (or bytes) of the text field. The character table bytes are a non-ordered list of the character table selection bytes defined by [4].” change to “character_table_byte shall be coded according to the multiple string structure in A/65 [2] Section 6.10”.
- Where [11] states “All hosts must support input and output using the default (table 0) Latin Alphabet as defined by [4].” change to “All hosts shall support input and output using Unicode™ page 0 (ISO Latin-1), as defined in A/65 [2].”

- Where [11] states "Text information is coded using the character sets and methods described in [4]." change to "Text information shall be coded using the multiple string structure in A/65 [2] Section 6.10".

4.4.4 NRSS Homing

The NRSS interface specifies optional homing resources for the host. The host shall implement NRSS homing resources.

4.4.5 NRSS Chaining

The NRSS interface specifies optional chaining for the host. The host shall implement NRSS chaining.

4.4.6 NRSS Copy Protection Framework

The NRSS interface specifies a copy protection framework for protection of data transmitted across the NRSS interface. An ATSC compliant host which implements copy protection across the NRSS interface shall comply with the copy protection framework defined by NRSS.

It should be noted that copy protection may be required for certain transmissions.

ANNEX A. Mapping of MPEG Payload Bytes into the DES Block (Normative)

This Annex illustrates the mapping of MPEG payload bytes into the DES (64 bit) block. A MPEG transport packet consists of the following elements:

MPEG Transport Stream Packet

H0	H1	H2	H3	A0	A1	…	An	D0	D1	…	Dn
MPEG Transport Stream Packet Header				MPEG Transport Stream Adaptation Field (if present)				MPEG Transport Stream Packet Payload			

Where “H0 H1 H2 H3” represent the 4 byte MPEG Transport Stream packet header and “A0, A1, A2...An” represent the MPEG Transport Stream adaptation field (if present) in the packet. These bytes are not scrambled (see Section 4.2.3.2). “D0, D1...Dn” represent the MPEG Transport Stream packet payload.

For scrambling and descrambling, the Transport Stream packet payload is divided into 8-byte blocks and possibly one block of from 1 to 7 bytes. This last block is called a ‘solitary short block’ if it is the only block or else a ‘terminating short block’. The first 8 bytes of the Transport Stream packet payload in transmit order (denoted D[0..7], above) form the first block. Subsequent groups of 8 bytes form subsequent blocks. Any short block will therefore consist of the last 1 to 7 bytes in the Transport Stream packet payload (in transmit order).

Using the above convention, D[2](7) is the most-significant bit in the 3rd data byte, and D[2](0) is the least-significant bit in the 3rd data byte.

Each contiguous block of 8 payload data bytes is descrambled via the TDES process. Note that the TDES references use a different bit ordering convention (little-endian). This payload data is grouped into 64-bit blocks for DES and TDES processing by concatenating the 8 bytes of contiguous data such that the MSB of the first MPEG payload byte is the MSB of the 64-bit DES block, and the LSB of the eighth MPEG payload byte is the LSB of the 64-bit DES block. This is done by serializing the 8 MPEG payload bytes (D0…D7) and left shifting them to form one 64-bit block.

This bit mapping is shown below. Note that MPEG payload bytes use engineering notation (i.e., MSb=7, LSb=0) while TDES uses FIPS notation (i.e., MSb=1 LSb=64).

To avoid confusion between the DES references and this document, the following table can be used to correlate DES bits with Transport Stream packet payload bits, for each 8-byte block of Transport Stream packet payload bytes (using the above notation, D[0..7]), and each 64-bit block for DES processing (using the DES notation, DES(1..64)).

Table A.1 Transport Stream Packet Payload and DES Bits

Transport Stream Packet Payload Bits	DES Bits
D[0](7..0)	DES(1..8)
D[1](7..0)	DES(9..16)
D[2](7..0)	DES(17..24)
D[3](7..0)	DES(25..32)
D[4](7..0)	DES(33..40)
D[5](7..0)	DES(41..48)
D[6](7..0)	DES(49..56)
D[7](7..0)	DES(57..64)

Using the above table, the bit D[4](4) is the bit DES(36).

ANNEX B. Triple-DES Scrambling Modes (Informative)

B1. 56-BIT SINGLE DES

56-bit FIPS 46-2 DES is shown in Figure B.1 to define symbology and terms only.

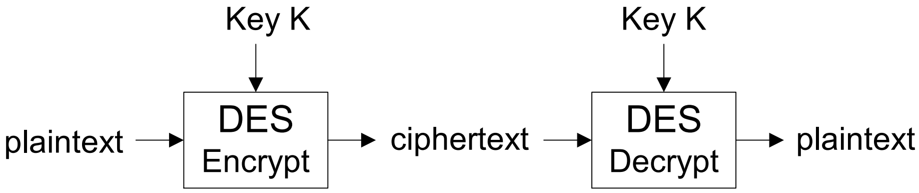


Figure B.1 FIPS 46-2 56-bit single DES.

B2. 168-BIT TRIPLE DES

The 168-bit ABC EDE Triple DES mode of FIPS 46-2 DES is shown in Figure B.2. This algorithm uses three independent single DES operations, each with its own 56-bit key labeled A, B, and C. To encrypt via ABC EDE Triple DES, the first (key A) and third (key C) single DES operations are encryption, and the second (key B) operation is decryption. To decrypt via ABC EDE Triple DES, the first and third single DES operations are decryption, and the second operation is encryption. This 168-bit mode is referred to as “maximum level MPEG security”.

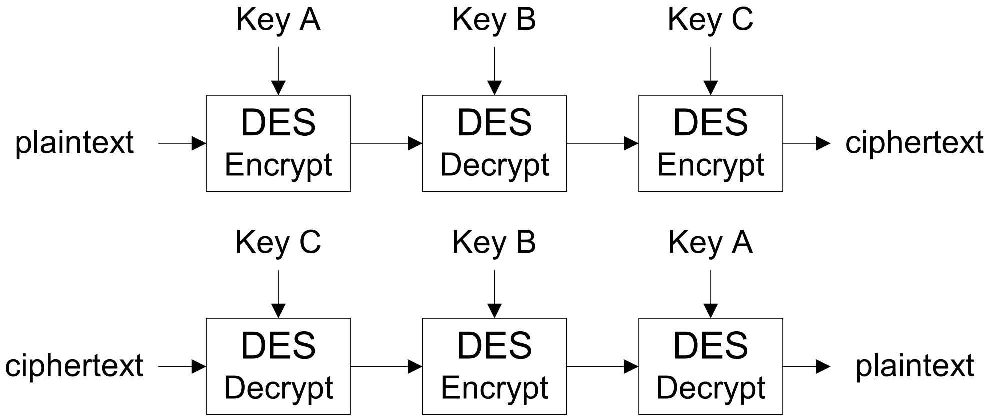


Figure B.2 168-bit EDE processing.

The figures in Figure B.3 show simple symbols useful in depicting the ATSC ABC EDE Triple DES scrambling algorithm.

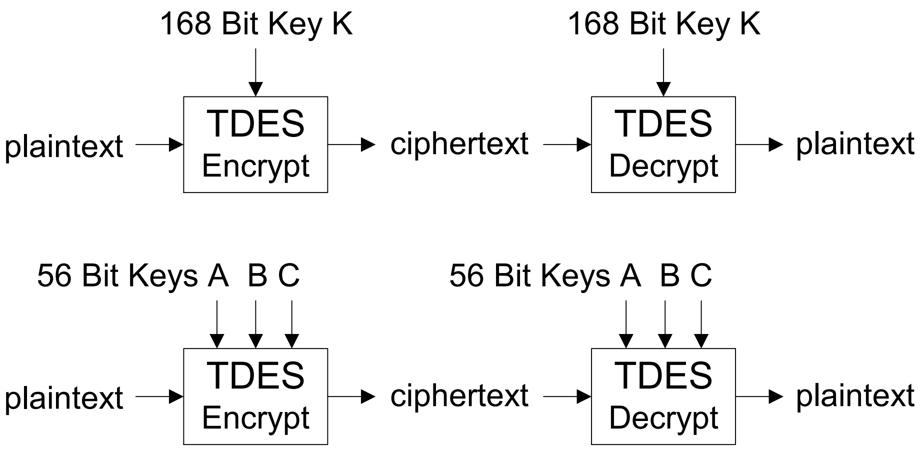


Figure B.3 Alternate symbology for ATSC TDES.

B3. 112-BIT MODE OF 168-BIT TDES

It is possible for the 168 TDES mode to be backward compatible with a 112-bit DES mode. This is achieved by setting the value of the "C" key to be equal to the "A" key. The 112-bit "ABA EDE Triple DES" mode of "ABC EDE TDES" is shown in Figure B.4. This 112-bit mode is referred to as "high level MPEG security".

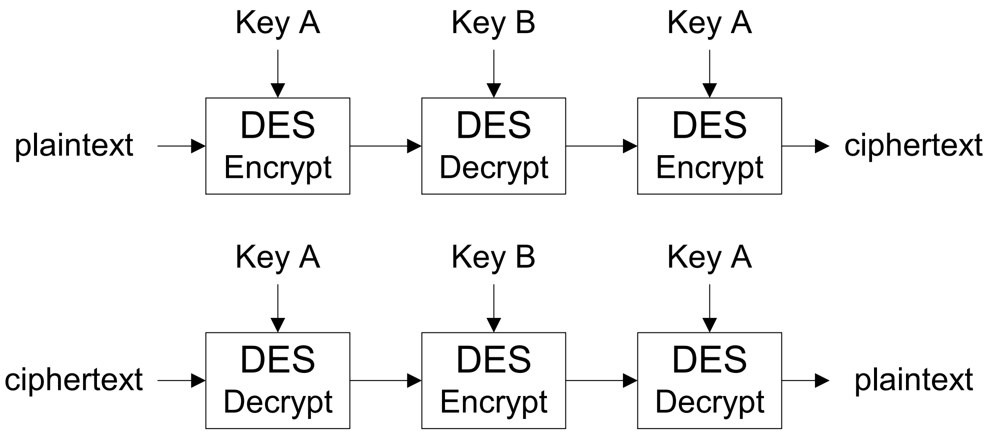


Figure B.4 112-bit mode of 168-bit TDES.

B4. 56-BIT MODE OF 168-BIT TDES

It is possible for the 168 TDES mode to be backward compatible with the 56-bit single DES mode. This is achieved by setting the value of the "A", "B", and "C" keys to be equal as shown in Figure B.5. This arrangement allows the second and third DES operations to cancel, leaving in effect a single DES operation. The 56-bit single DES mode of ABC EDE TDES is shown in Figure B.5. This 56-bit mode is referred to as "base level MPEG security".

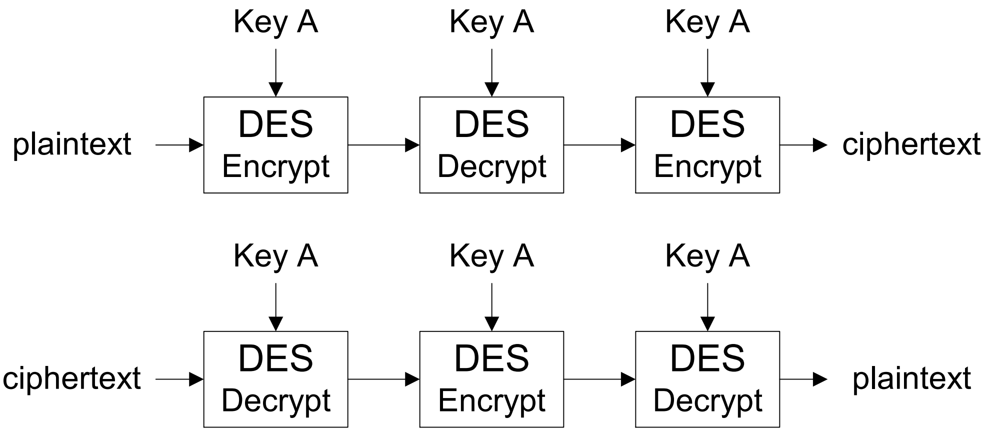


Figure B.5 56-bit mode of 168-bit TDES.

Modes with less than 56 bits of effective key are referred to as “low level MPEG security” modes.

B5. ABC EDE TDES CIPHER BLOCK CHAINING

Figure B.6 shows where initialization vectors are inserted, and cipher block chaining.

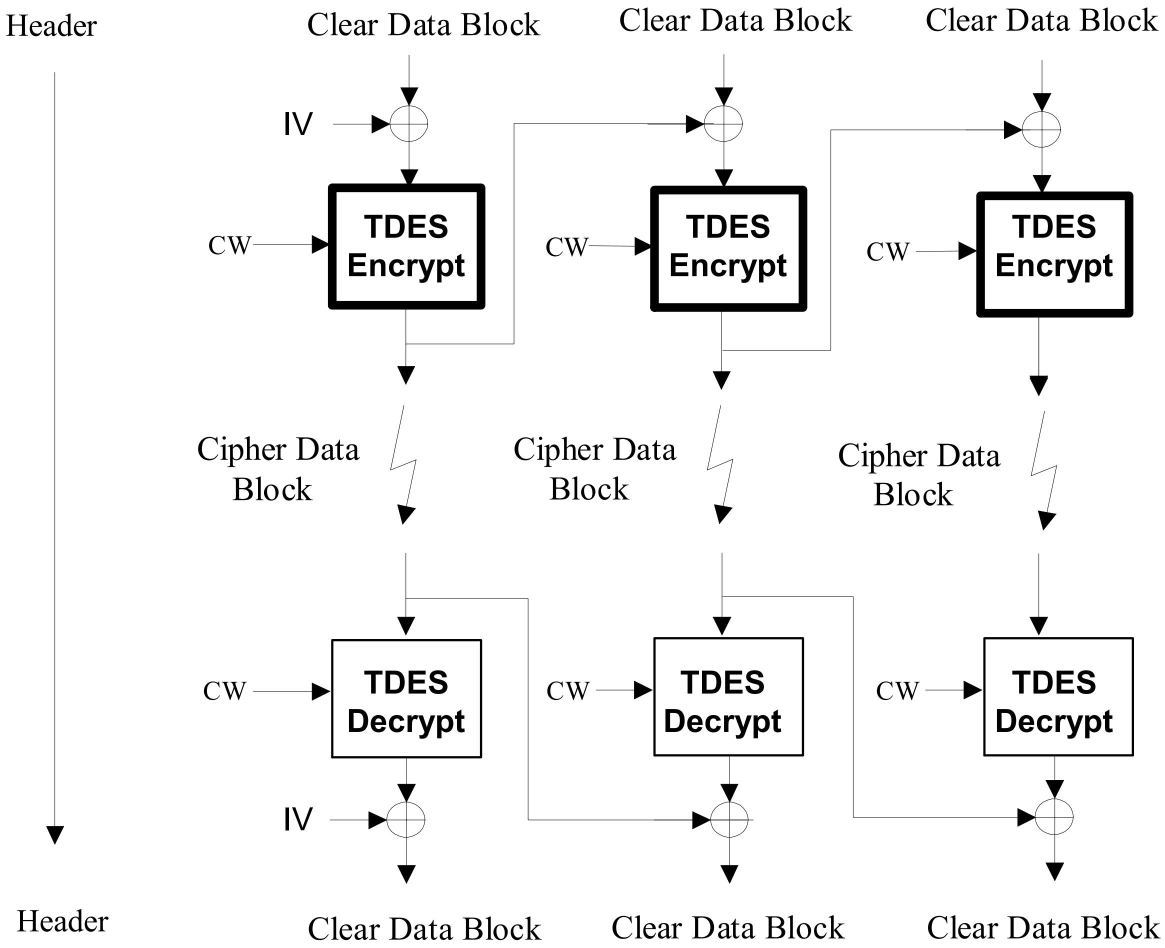


Figure B.6 Basic ABC EDE TDES Cipher Block Chaining.

ANNEX C. Broadcast Headend Security (Informative)

MPEG content is protected by the MPEG transport scrambling algorithm and CW. The CW is protected by each CA system that redistributes that key, as are other valuable keys used by each CA system. ATSC broadcast headend security has the objective of protecting CW creation and sharing when the CW is not within the security mechanisms of a CA system.

ATSC broadcast headend security can be the "weak link" that obviates the protection of both the MPEG transport scrambling algorithm and all CA systems operating on that Transport Stream. This vulnerability defines a minimum level of protection that ATSC broadcast headend security must provide.

ATSC broadcast headend security should protect the movement of all CWs with a protection level no less than that applied to the MPEG Transport Stream, as exemplified in the following:

- Maximum security MPEG scrambling (i.e., 168-bit TDES) has its key protected by 168-bit TDES.
- High MPEG security scrambling (i.e., 112-bit TDES) has its key protected by 112-bit or 168-bit TDES.
- Base MPEG security scrambling (i.e., 56-bit TDES) has its key protected by 56-bit, 112-bit or 168-bit TDES.
- Low Security MPEG scrambling (i.e., less than 56-bit TDES) has its key protected by a like-sized key or 56-bit, 112-bit or 168-bit TDES.

One way to satisfy this requirement is to match the protection level applied to MPEG transport scrambling with that deployed in the ATSC broadcast headend. This allows embodiments such as fixed key or clear mode systems, where MPEG transport scrambling uses only a single key or is disabled, and no broadcast headend security is required.

Alternatively, a single maximum-security level approach can be employed at the broadcast headend, and the security level of MPEG transport scrambling could vary based on broadcaster, content provider, or export requirements.

Regardless, the security levels and techniques employed in ATSC CW key sharing must be capable of a range of security strengths. This range must cover the same levels of cryptographic strength available in the ATSC MPEG transport scrambling algorithm (i.e., from zero to 168 bits of strength).

ANNEX D. An Overview of the Conditional Access Standard for Terrestrial Broadcast (Informative)

D1. INTRODUCTION

With the deployment of terrestrial digital television, each of the 6-MHz channels that used to carry analog TV signals becomes a digital stream with a throughput of 19.39 Mbps. According to MPEG terminology, each of these digital streams is called a Multiplex or a Transport Stream able to support one or more simultaneous television programs as well as non-traditional services such as data broadcasting. Some of the services conveyed in a Transport Stream may be targeted to a restricted audience. This is the case, for example, of pay-TV where only subscribers in good standing are allowed to have access to pay-TV events or packages. Hence, access is said to be offered conditionally.

This Annex uses application examples to describe the set of rules that comprise the ATSC Conditional Access standard. Compared to other ATSC standards, this one has a very unique feature. This Standard does not describe precisely all the techniques and methods to provide conditional access. Instead, it provides only data envelopes and transport functions that will allow several conditional access systems of different types to operate simultaneously and perhaps to compete with each other. In simple words, a broadcaster may offer pay-TV services by means of one or more CA systems, each of which may have different transaction mechanisms, different security strategies, and more importantly, different business models.

The overview begins in Section D2 with a description of the elements that compose a typical CA system. In Section D3, we review the common scrambling algorithm that is necessary to standardize in an environment where multiple CA systems control access to scrambled programs. In Section D4, we describe data envelopes and transport messages that broadcasters use to make evident the existence of CA services. Section D5 describes how receivers detect the existence of CA controlled services.

It is important to note that besides the standards described in this Annex, three other companion standards are necessary to provide an end-to-end solution to conditional access. These other standards describe Simulcrypt, host-module communications, and copy protection of the host-module interface.

D2. SYSTEM ELEMENTS

The basic elements of a conditional access system for terrestrial DTV are the headend broadcast equipment, the conditional access resources, a DTV host and the security module(s). Figure D.1 illustrates these basic elements and some possible interactions among them. The headend broadcast equipment generates the scrambled programs for over-the-air transmission to the constellation of receivers. The DTV host demodulates the transmitted signals and passes the resulting Transport Stream to the security module for possible descrambling.

Security modules are distributed by CA providers in any of a number of ways: for example, either directly, through CE manufacturers, through broadcasters or through their agents. Security modules typically contain information describing the status of the subscriber. Every time the security module receives from the host a Transport Stream with some of its program components scrambled, the security module will decide, based on its own information and information in the

Transport Stream, if the subscriber is allowed access to one or more of those scrambled programs. When the subscriber is allowed access then the security module starts its most intensive task, the descrambling of the selected program.

The packets of the selected program are descrambled one by one in real time by the security module, and the resulting Transport Stream is passed back to the DTV host for decoding and display. According to this Standard, two types of security module technologies are acceptable: NRSS-A and NRSS-B. A DTV host with conditional access support needs to include hardware/software to process either A or B or both. This Standard does not define a communication protocol between the host and the security module. Instead, this Standard mandates the use of NRSS. Similarly, for copy protection of the interface between the host and the security module, this Standard relies on NRSS specifications.

Besides the scrambled programs, the digital Multiplex carries streams dedicated to the transport of ECMs and EMMs. ECMs are data units that mainly carry the key for descrambling the signals. EMMs provide general information to subscribers and most likely contain information about the status of the subscription itself. Broadcasters interested in providing conditionally accessed services through one or more CA providers need to transmit ECMs and EMMs for each of those CA providers. This standard defines only the envelope for carrying ECMs and EMMs. A security module is capable of understanding the content of EMMs and ECMs privately defined by one (or more) CA provider.

The digital Multiplex for terrestrial broadcast carries a program guide according to the specifications defined in A/65. The program guide contains detailed information about present and future events that may be useful for the implementation of a CA system. For this reason, this Standard defines a descriptor called the ATSC_CA_descriptor() which can be placed in either the channel or event tables of A/65. Similar to the definitions of ECMs and EMMs, only the generic descriptor structure is defined while its content is private. The host is required to parse the program guide tables in search of this descriptor and pass it to the security module. Due to its private content, it is the security module that ultimately processes the information. Note that although A/65 PSIP does not require use of conditional access, this conditional access standard requires the use of A/65 PSIP.

Most of the communications between the CA network and a subscriber receiver can be performed automatically through broadcast streams using EMMs. EMMs are likely to be addressed to a specific security module (or receiver, possibly groups of security modules or receivers). Security modules will receive their EMMs by monitoring the stream of EMMs in the Multiplex, or by searching for addressed EMMs by homing. Homing is the method for searching EMM streams while the receiver is in stand-by mode. Homing is initiated by the host according to schedules and directives as defined in NRSS specifications for the security module. As Figure D.1 shows, the security module may communicate with the CA network using a telephone modem integrated into the host. This return channel is optional according to this Standard, but if it exists, the host and the security module will adhere to the communication resource specifications of NRSS. A combination of homing and return channel EMM delivery may be used at the discretion of the CA provider.

Figure D.1 shows that the interconnection between CA networks and the broadcast headend equipment requires Simulcrypt. Simulcrypt is a DVB protocol defining equipment and methods for adequate information exchange and synchronization. The most important information elements that get exchanged are the scrambling keys. According to Simulcrypt procedures, a new key can be generated by the headend equipment after a certain time interval that ranges from a fraction of a second to almost two hours. Before the encoder activates the new key, it is transferred to each CA system for encapsulation using their own protocols. Encapsulated keys in the form of ECMs are transferred back to the transmission equipment and are broadcast to all receivers. Shortly after the encoder has transmitted the new ECMs, the encoder uses the new key to scramble the content.

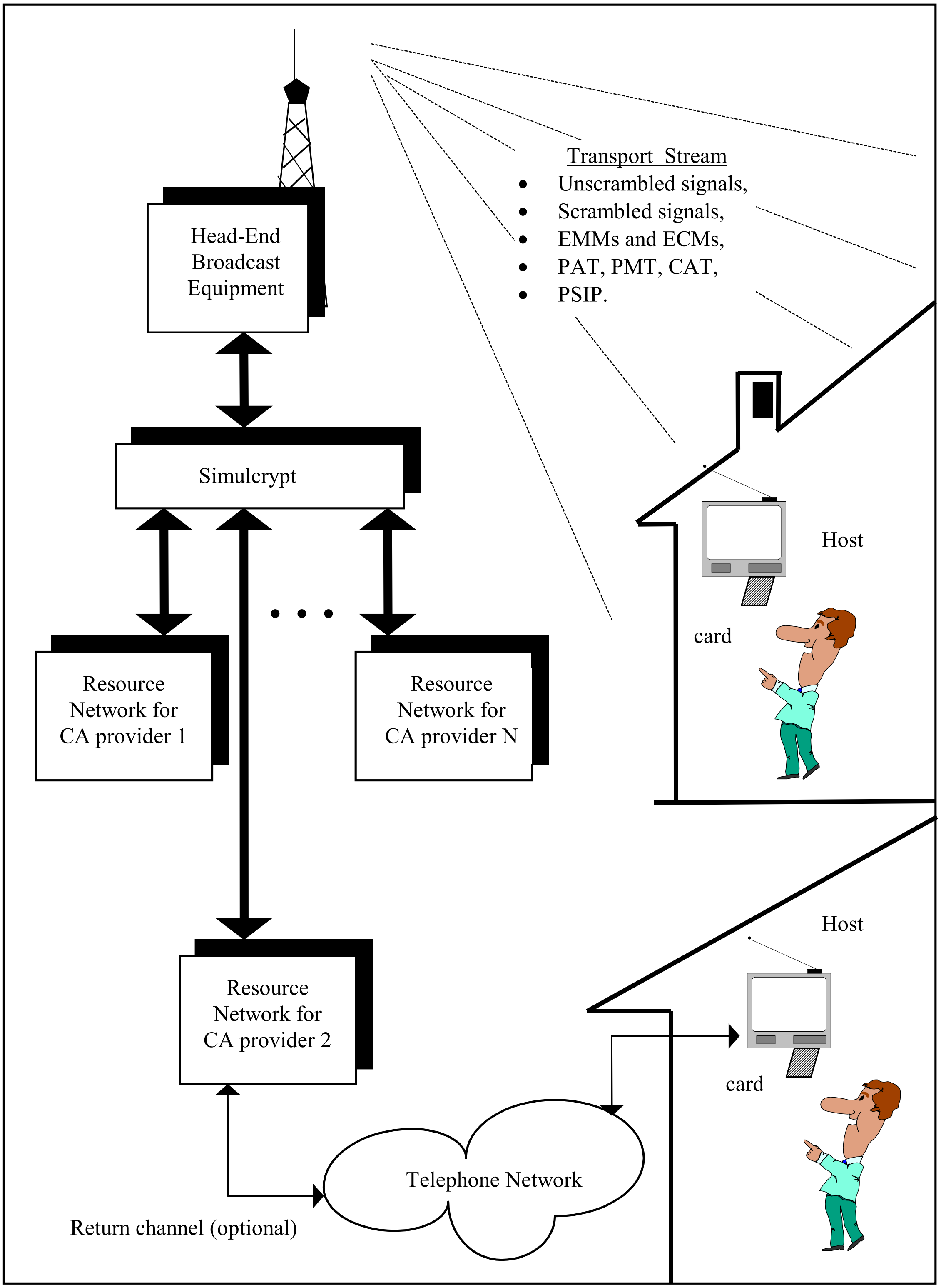

Transport Stream
• Unscrambled signals,
• Scrambled signals,
• EMMs and ECMs,
• PAT, PMT, CAT,
• PSIP.
Head-End Broadcast Equipment
Simulcrypt
Resource Network for CA provider 1
. . .
Resource Network for CA provider N
Host
card
Resource Network for CA provider 2
Host
card
Telephone Network
Return channel (optional)

Figure D.1 Main elements of a Conditional Access system.

D3. COMMON SCRAMBLING ALGORITHM

This Standard defines Triple-DES in Cipher-Block-Chaining mode as the algorithm to use for scrambling Transport Stream packets. The algorithm takes a block of 8 bytes and generates an output of 8 encrypted bytes. Figure D.2 illustrates the process of scrambling a Transport Stream packet. As the figure shows, headers and adaptation fields are never scrambled. The remaining data-payload bits are segmented in 8-byte blocks and passed through the TDES scrambling engine.

If $\boldsymbol{b}(n)$ represents the nth block in the sequence, then its scrambled version, denoted as $\boldsymbol{s}(n)$, is obtained from

$$\boldsymbol{s}(n) = E\,[\ \boldsymbol{b}(n) \oplus \boldsymbol{s}(n\text{-}1)\ ]$$

where $E[\ ]$ is the encryption or scrambling function performed by the TDES algorithm, the symbol "⊕" is the bitwise exclusive-or (xor) operation, and $\boldsymbol{s}(n\text{-}1)$ is the output of the previously-scrambled block.

Notice that for the first block $\boldsymbol{b}(1)$, the data for $\boldsymbol{s}(0)$ does not exist. It is therefore necessary to define an Initialization Vector, denoted as $\boldsymbol{IV}$, which is used to compute the first scrambled block as follows

$$\boldsymbol{s}(1) = E\,[\ \boldsymbol{b}(1) \oplus \boldsymbol{IV}\ ]$$

This Standard mandates that the data for $\boldsymbol{IV}$ is a bit sequence of 64 zeros.

There are two special cases that need to be identified: *terminating short blocks* and *solitary short blocks*. The first case occurs when the total number of blocks is at least two ($N \geq 2$) and the last block has less than eight bytes. In this case, the last block $\boldsymbol{b}(N)$ is encrypted by computing

$$\mathbf{s}(\mathrm{N}) = \mathbf{b}(\mathrm{N}) \oplus \mathrm{E}\,[\ \mathbf{s}(\mathrm{N}\text{-}1)\ ]$$

Figure D.2 illustrates an example of this case. If M represents the length of $\boldsymbol{b}(N)$ in bits, then only the first M bits of $E[\boldsymbol{s}(N\text{-}1)]$ are used for the xor operation. The second case, solitary short blocks, occurs when the total number of blocks is one ($N = 1$) and the bytes in this block are less than eight. In this case, the scrambling of the unique block $\boldsymbol{b}(1)$ is computed as

$$\mathbf{s}(1) = \mathbf{b}(1) \oplus \mathrm{E}\,[\ \mathbf{IV}\ ]$$

where, as before, the Initialization Vector is a bit sequence of 64 zeros. Similarly to the previous case, the M bits of $\boldsymbol{b}(1)$ are aligned with the first M bits of $E[\boldsymbol{IV}]$ for the xor operation. Figure D.3 illustrates this second case.

The triple DES algorithm, which so far has been represented as a single block in Figure D.2 and Figure D.3, is actually a sequence of three cascaded DES algorithms (See Figure D.4). The first and last algorithms perform DES encryption while the second one performs decryption. Since each DES block uses a 56-bit key, the resulting key for a TDES engine has 168 bits.

Mainly for reasons of improved security, the ATSC may in the future decide to change or modify the common scrambling algorithm. CA providers are encouraged to use some form of algorithm identifier in their messaging protocols (ECMs and/or EMMs) to facilitate this eventual transition.

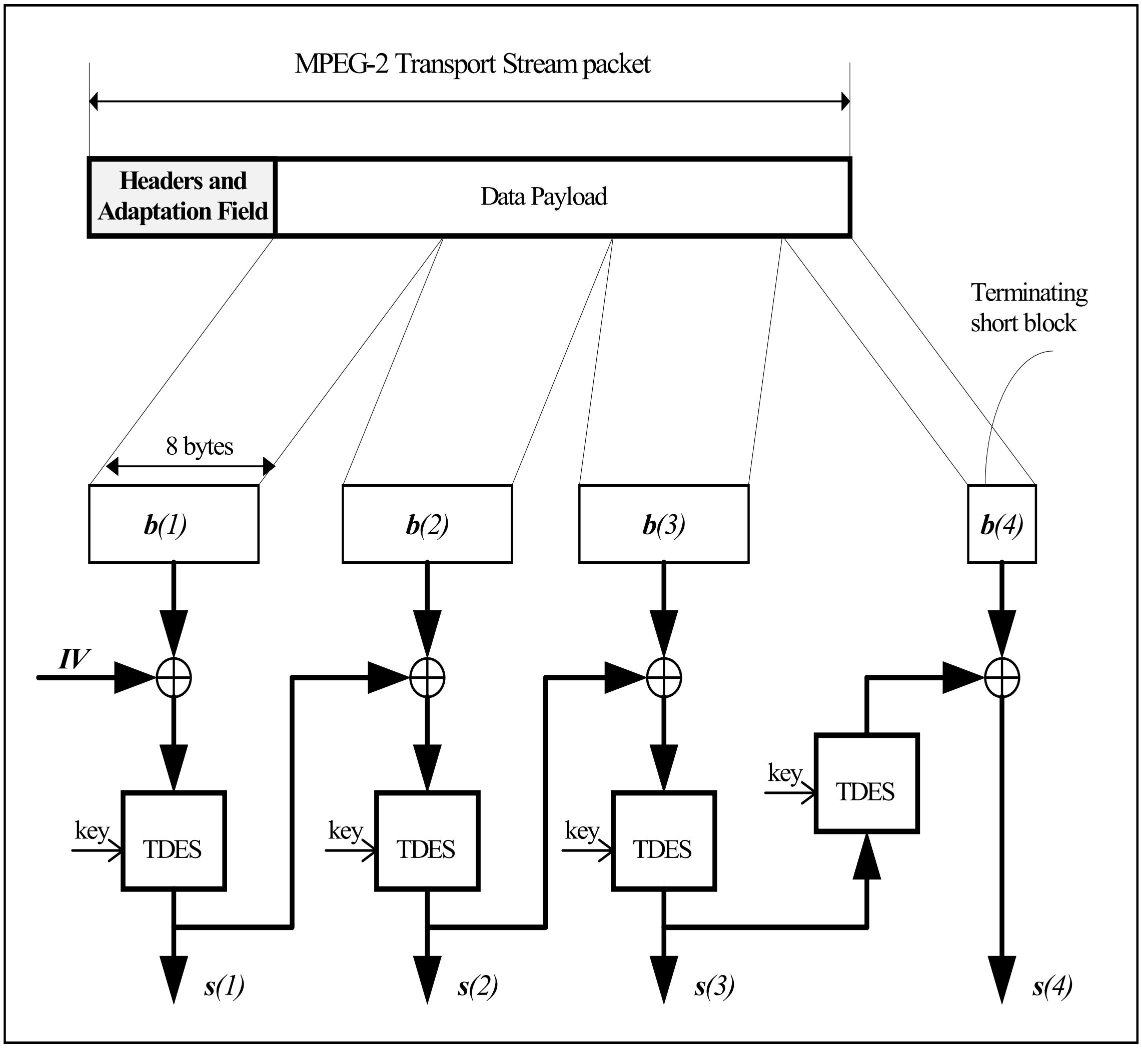


Figure D.2 Scrambling algorithm and Terminating Short Block.

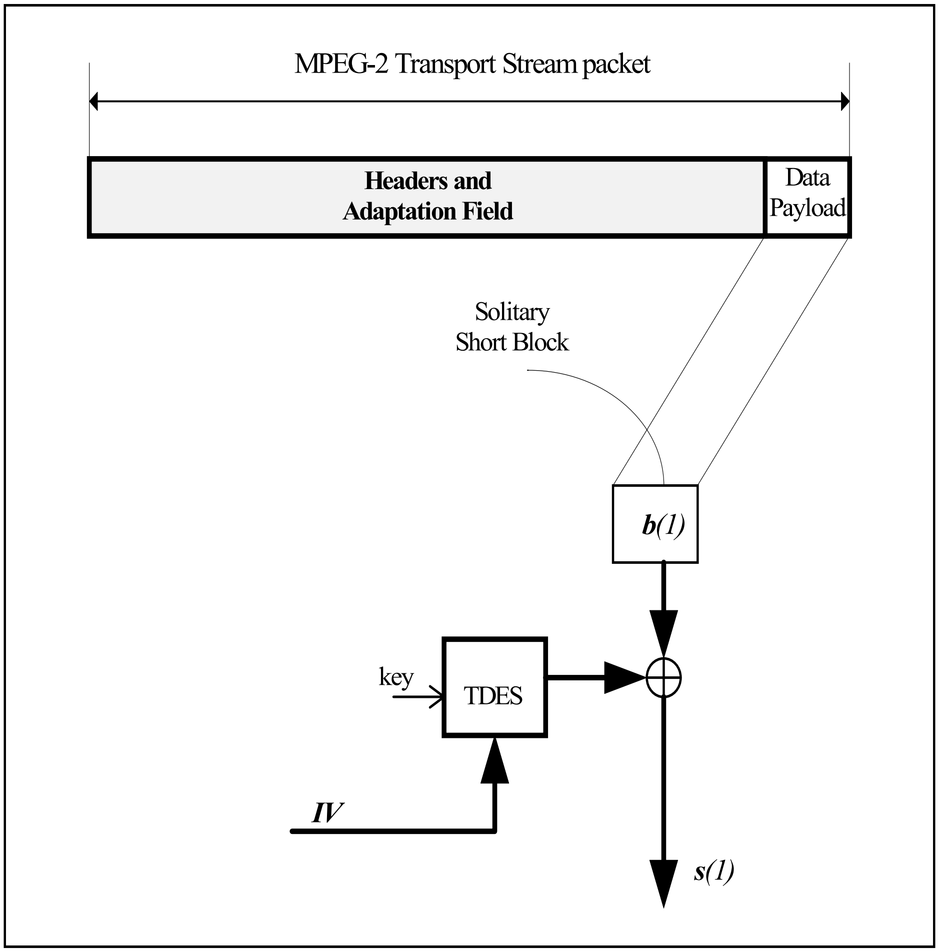


Figure D.3 Scrambling of a Solitary Short Block.

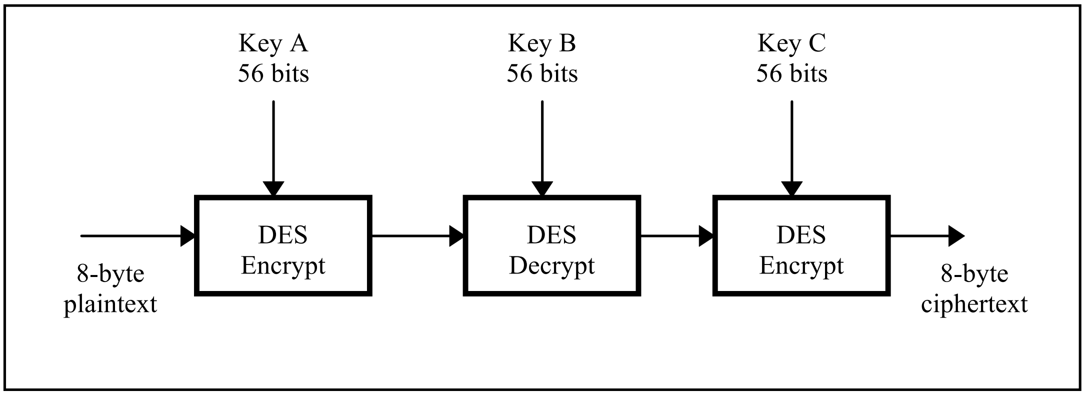


Figure D.4 Triple DES as a cascade of three DES encryption/decryption engines.

D4. TRANSPORT STREAM MESSAGES FOR CA

Besides carrying the scrambled signal, the Transport Stream carries messages to identify properties and parameters of the scrambled signals. The messages are ECMs, EMMs, and two CA descriptors. As mentioned before, the syntax of the message content is, in general, privately defined and only data envelopes are specified. This section describes how to set up the messaging system that is based on using the Conditional Access Table (CAT), the Program Map Table (PMT), and the channel and event tables of the program guide (carried via PSIP).

For the purpose of this section, assume that a certain broadcaster is offering pay-TV services in partnership with two CA providers here called “Cardex” and “Tarhex”. Both providers have obtained from ATSC valid identification numbers that, in the Standard, are the CA_system_id values. The actual procedures for obtaining valid identification numbers are exclusively defined by the ATSC and the reader is encouraged to contact this organization for further information. Assume that in this case, the CA system ID values for Cardex and Tarhex are 15 and 37 respectively.

The first step for this broadcaster is to set up a CAT that provides a list of CA providers and defines the stream PIDs for their EMMs. Figure D.5 shows the CAT for the example given here. The CAT is a table that always uses PID 0x0001 and a table_id of 0x01. The content of this table is a list of MPEG-2 CA descriptors which contain 3 pieces of information: (1) the CA system id, (2) a PID, (3) private information.

As shown in Figure D.5, the CAT for our example contains two MPEG-2 CA descriptors, one for each of the CA providers. The PID values of these descriptors indicate the PIDs where the EMMs are located.

Assuming that at a certain time, a scrambled program with program_number of 712 is available on channel 7-3, then the PMT for this program will resemble that of Figure D.6. The normal function of the PMT is to list program parameters for the program and for each of its elementary streams. When the program is scrambled, the PMT also contains one or more MPEG-2 CA descriptors that indicate the location of the ECMs for each CA provider. ECMs carry the keys required for descrambling.

Notice that the descriptor used in the CAT and the PMT is actually the same MPEG-2 descriptor with a tag of 0x09. This descriptor identifies the EMM PIDs and ECM PIDs when placed in the CAT and PMT respectively. Notice also from Figure D.6 that it is possible to define an ECM stream for the entire program as Cardex uses in the example, or instead, it is also possible to define ECM streams per elementary stream as Tarhex does. Notice that Tarhex uses the same ECM PID for video and Spanish audio, and a different ECM PID for English audio.

The program guide for ATSC is defined in A/65 [2], Program and System Information for Terrestrial Broadcast and Cable (PSIP). It defines a collection of tables to describe the structure and organization of channels and programs in a Transport Stream. The Virtual Channel Table (VCT) in PSIP lists all the existing virtual channels. Following with our example, the entry for channel 7-3 will contain the identifying major and minor numbers (7 and 3 respectively), and will list the program_number field as 712 for linkage with its PMT. Every virtual channel entry in the VCT allows the insertion of descriptors with information about this particular virtual channel. As an option to CA providers, one of these descriptors may be the so called ATSC_CA_descriptor() which is defined in this standard.

The Event Information Table (EIT) in PSIP contains a list of those events scheduled over a 3-hour interval for a certain virtual channel. For every event entry in the EIT, a set of descriptors can be included expanding the information for a particular event. As an option to CA providers, the ATSC_CA_descriptor() can also be placed within an event entry in the EIT.

The payload of this descriptor starts with the CA system ID. The remaining information is privately defined. When this descriptor is found either in the VCT or EIT, it has to be transferred to the security module for further processing. The transference of this information follows NRSS specifications. If the ATSC_CA_descriptor() is found simultaneously in the VCT and an EIT, it is defined that the VCT descriptor takes precedence over the EIT descriptor.

It is recommended that CA providers avoid changing information in an ATSC_CA_descriptor() in the VCT or the PMT unless the information is different from that previously included in that descriptor in the EIT for the current event. It is assumed that any event related information will be obtained from the EITs and retained by the CA provider's system. The descriptor may be used in the VCT to correct the previous information if necessary. Every change made to PMT and VCT parameters requires some processing time at the receiver that may lead to tuning delays. For this reason, it is good practice to maintain the PMT information as constant as possible.

D5. SIGNALING THE EXISTENCE OF CONDITIONAL ACCESS SERVICES

Normal operation of a receiver requires the detection of channels and signals subjected to conditional access. For channels, each virtual channel entry in the VCT carries a flag called access_controlled which, when set to ‘1’, indicates that channel access is restricted. This flag gives no information about which elementary streams are scrambled. Using this flag for example, a displayed program guide could announce the scrambled virtual channel with a different color.

For scrambled elementary streams, there are two steps for recognition of CA services. First, the PMT for the program will carry either MPEG-2 CA descriptors for each of the scrambled elementary streams, or at least a single CA descriptor valid for all the streams in the program. Second, the header of the Transport Stream packets will have its transport_scrambling_control field equal to either ‘10’ or ‘11’, corresponding to even and odd key scrambling respectively.

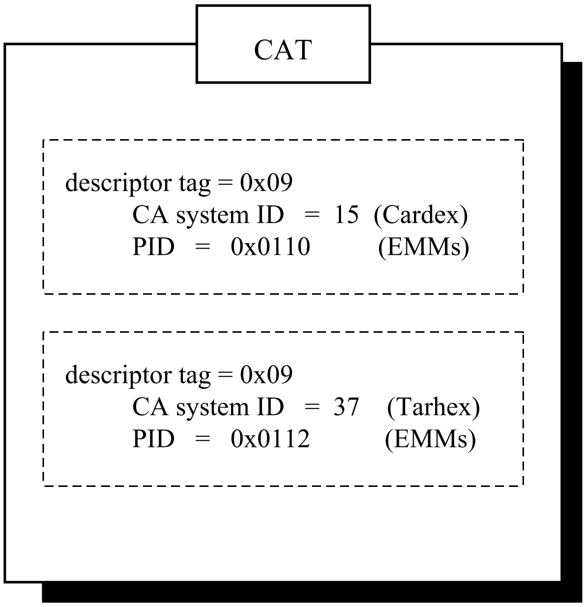
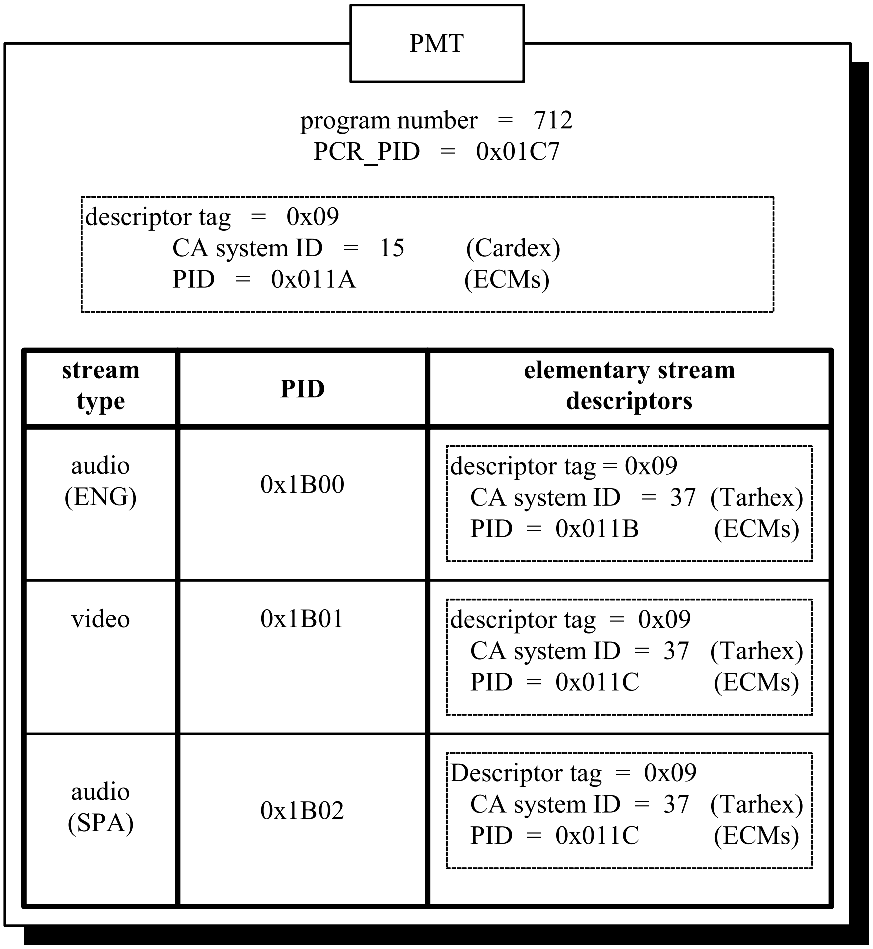


Figure D.5 Contents of the Conditional Access Table.



PMT

program number = 712
PCR_PID = 0x01C7

descriptor tag = 0x09
CA system ID = 15 (Cardex)
PID = 0x011A (ECMs)

stream type	PID	elementary stream descriptors
audio (ENG)	0x1B00	descriptor tag = 0x09 CA system ID = 37 (Tarhex) PID = 0x011B (ECMs)
video	0x1B01	descriptor tag = 0x09 CA system ID = 37 (Tarhex) PID = 0x011C (ECMs)
audio (SPA)	0x1B02	Descriptor tag = 0x09 CA system ID = 37 (Tarhex) PID = 0x011C (ECMs)

Figure D.6 Conditional Access Content of a Program Map Table.