



***Society of Cable
Telecommunications
Engineers***

ENGINEERING COMMITTEE

Digital Video Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 41 2011

POD Copy Protection System

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability and ultimately the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members, whether used domestically or internationally.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the Standards. Such adopting party assumes all risks associated with adoption of these Standards, and accepts full responsibility for any damage and/or claims arising from the adoption of such Standards.

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this standard have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2011
140 Philips Road
Exton, PA 19341

CONTENTS

NOTICE	I
1. INTRODUCTION.....	1
1.1 Scope	1
1.2 References.....	1
1.2.1 Normative reference list	1
1.2.2 Informative Reference list.....	2
1.2.3 Reference acquisition	2
1.3 Acronyms, Abbreviations, and Defined Terms	4
1.4 Copy Protection System Components	6
1.5 Implementation Outline	6
1.6 Historical Perspective	7
1.7 Related Documents	7
2. SYSTEM OVERVIEW (INFORMATIVE).....	8
2.1 NRSS Copy Protection Framework	8
2.2 Device Authentication	8
2.2.1 Bi-Directional Host and Cable System	9
2.2.2 Manual Return Authentication	9
2.2.3 POD Support for Multiple Hosts.....	9
2.3 Key Exchange and Transport Stream Protection	10
2.3.1 Setup Phase	10
2.3.2 Key Derivation Phase	10
2.3.3 Interface Encryption.....	11
2.4 Data Channel Protection	12
2.4.1 Copy Control Information.....	12
2.4.2 Rules for CP-Scrambling based on EMI value and CA-Scrambling	12
2.5 Identifying Fraudulent Devices and Disabling of Services.....	12
3. HOST AUTHENTICATION MECHANISMS	13
3.1 Protocol Components	13
3.1.1 X.509 Version 3 Certificate.....	13
3.1.2 Device Parameters	13
3.1.3 System Parameters	14
3.1.4 Processing Basics	14

3.2	POD/Host Binding and Registration	18
3.2.1	ID ReportING Mechanism	19
3.2.2	Authentication Phase 1 – Certificate Verification & DH Key Exchange	20
3.2.3	Authentication Phase 2 – Authentication Key Verification	21
3.2.4	Authentication Phase 3 – Headend Report Back	21
3.2.5	Headend Report Back Methods	22
3.3	Power-up Re-Authentication	25
3.4	POD Operation with Multiple Hosts	25
3.5	Host Operation with Multiple PODs	25
4.	CRYPTOGRAPHIC FUNCTIONS	26
4.1	Authentication Key Generation	26
4.2	Copy Protection Key Generation	27
4.2.1	Basic Key Generation Protocol	27
4.2.2	POD Module Copy Protection Key	28
4.2.3	Host Copy Protection Key	29
4.3	CP-Key Refresh	29
4.3.1	Key Session Period	30
4.3.2	Key Refresh Period	30
4.3.3	CA System Key Refresh	32
4.3.4	Key Refresh Initialization	32
4.3.5	Channel Change	32
4.3.6	Two Key Synchronization Mode (Informative)	33
4.3.7	Transport Scrambling Control Field	33
4.4	Diffie-Hellman Key Exchange Algorithm	34
4.4.1	Algorithm Overview	34
4.4.2	Algorithm Implementation	35
4.5	SHA-1 Secure Hash Algorithm	36
4.6	Random Number Generation	36
4.7	DFAST Algorithm	37
4.7.1	Algorithm Overview	37
4.7.2	DFAST Characteristics	37
4.8	RSA Digital Signatures	37
5.	HOST SERVICE REVOCATION MECHANISMS	38
5.1	System Issues	38
5.2	Revocation Circumstances [Informative]	38
5.3	Fraudulent Host Identification	38
5.4	CA System Revocation & Selective Denial of Services	38

5.4.1	Definition of Revocation	38
5.4.2	Selective Service Denial.....	38
5.5	The Revocation Process	39
5.6	Implementation in the Headend	40
6.	COPY CONTROL INFORMATION (CCI).....	41
6.1	CCI Definition.....	41
6.1.1	EMI - Digital Copy Control Bits.....	41
6.1.2	APS - Analog Protection System	42
6.2	Associating CCI with a Service	42
6.3	Conveying CCI from Headend to POD.....	42
6.4	Conveying CCI from POD to Host	42
6.4.1	CCI Delivery Instances	43
6.4.2	Authenticated Tunnel Protocol	44
7.	TRANSPORT SCRAMBLING POD TO HOST	45
7.1	MPEG Scrambling	45
7.1.1	Scrambling Rules	45
7.2	Transport Processing	46
7.3	Timing of Scrambling Mode Transitions.....	46
7.4	CP-Scrambling as a function of CA-Scrambling and EMI Value	46
8.	HOST, POD, & HEADEND MESSAGING PROTOCOLS	47
8.1	Message Protocol Overview	47
8.2	POD & Host Common Messages	48
8.2.1	Opening a Session	48
8.2.2	Host Capability Evaluation	50
8.2.3	Copy Protection Key Generation	52
8.2.4	Host and POD Synchronization	55
8.3	POD-Host CP Message Protocol.....	57
8.3.1	Protocol Flow Overview	57
8.3.2	Host Authentication Messages	60
8.3.3	Host Authentication Key Verification Messages.....	63
8.4	CCI Simple Authentication Tunnel Protocol (SATP) Messages	64
APPENDIX A.	LUHN CHECK DIGIT (NORMATIVE).....	A
APPENDIX B.	APPLYING CP-KEY TO DES ENGINE (NORMATIVE)	B

Method of Application.....	B
Examples of CP encryption of MPEG DATA IN transport packets	C

List of Figures

Figure 3.1-A POD-Host CP Operation.....	17
Figure 3.1-B Headend CP Operation [informative]	18
Figure 3.2-A Example ID Reporting Screen.....	20
Figure 3.2-B Example CP System Failure Notification message	21
Figure 4.0-A Overall POD Copy Protection.....	26
Figure 4.3-A POD CP-Key Refresh Session Flow Chart	31
Figure 4.4-A Diffie-Hellman Key Agreement Protocol between POD and Host	34
Figure 6.4-A CCI Delivery Sequence	43
Figure 8.1-A Copy Protection Message Protocol Overview	47
Figure 8.3-A POD-Host CP Message Protocol Overview	57

List of Tables

Table 3.1-A Length of Device Parameters in the Host Authentication	13
Table 3.1-B Length of System Parameters	14
Table 4.2-A Length of Keys and Parameters Used in the Key Generation	29
Table 4.3-A MPEG Transport_scrambling_control values	33
Table 5.6-A CRL Based Host and POD Service Revocation	40
Table 6.1-A CCI Bit Assignments	41
Table 6.1-B EMI Values and Content	41
Table 6.1-C APS Value Definitions	42
Table 7.4-A CP-Scrambling based on CA-Scrambled State and EMI Value	46
Table 8.2-A Copy Protection Open Session Information	48
Table 8.2-B Open_Session_Request() Message Syntax	49
Table 8.2-C Copy Protection Resource Class	49
Table 8.2-D Open_Session_Response() Message Syntax	50
Table 8.2-E Host CP Support Capability Evaluation Messages	50
Table 8.2-F CP_open_req() Message Syntax	51
Table 8.2-G CP_open_cnf() Message Syntax	51
Table 8.2-H CP_system_id_bitmask Values	51
Table 8.2-I CP_data in the Transmission Key Generation Messages	52
Table 8.2-J CP_data_req() Message Syntax In the Key Generation Messages	52
Table 8.2-K Datatype_ID and Datatype_length Values	53
Table 8.2-L CP_system_id Values	54
Table 8.2-M CP_data_cnf() Message Syntax In the Key Generation Messages	54
Table 8.2-N Host and POD module Synchronization Messages	55
Table 8.2-O CP_sync_req() Message Syntax	55
Table 8.2-P CP_sync_cnf() Message Syntax	55
Table 8.2-Q Status_field Value	55
Table 8.3-A POD-Host CP Message Reference Sections	58
Table 8.3-B Host Authentication Messages	60
Table 8.3-C CP_data_req in the Host Authentication Request Message	61
Table 8.3-D CP_data_cnf in the Host Authentication Response Message	62
Table 8.3-E Host Authentication Key Verification Messages	63
Table 8.3-F CP_data_req in the Authentication Key Verification Request Message	63
Table 8.3-G CP_data_cnf in the Authentication Key Verification Response Message	64
Table 8.4-A CCI Simple Authentication Tunnel Protocol Messages	64
Table 8.4-B CP_data_req() Message Syntax in SATP Key Generation	66
Table 8.4-C CP_data_cnf() Message Syntax in CCI SATP Key Generation	66
Table 8.4-D CP_data_req() Message Syntax in CCI SATP Transmission	67
Table 8.4-E CP_data_cnf() Message Syntax in CCI SATP Transmission	67

1. INTRODUCTION

1.1 SCOPE

In digital Cable systems, high value movies and video programs (“content”) are protected by a conditional access scrambling system. A properly authorized CableCARD™ Point of Deployment (POD) security module removes the scrambling and, based on the Content Control Information from the Headend, may rescramble the content before delivering it to consumer receivers and set-top terminals (“Host devices”) across the POD-Host interface defined in ANSI/SCTE 28 2007.

This standard defines the characteristics and normative specifications for the system that prevents unrestricted copying of such high value content as it crosses the POD-Host interface.

Content that is delivered unscrambled over Cable systems is not subject to this standard. Indeed, this standard would not provide any protection against unrestricted copying of such content. Any unscrambled content output by the Host on the POD interface will not benefit by scrambling upon its subsequent output from the POD on that same interface.

This standard provides methods for authenticating Host devices, for binding POD modules to Host devices including Diffie-Hellman key exchange, for copy protection key generation, for rescrumbling high value content to protect against unauthorized copying (after the POD module employs the conditional access system to descramble it) and then descrambling by the Host, and for transmission and authentication of Copy Control Information. It also provides for revocation of Host devices that are determined to be fraudulent or non-compliant.

This standard requires the use of technology that must be licensed from CableLabs. The technology is called DFAST (U.S. Patent No. 4,860,353 and related know-how), and the license is PHILA – “POD-Host Interface License Agreement”, available from CableLabs. Please refer to section 1.2.3 under “DFAST Technology, PHILA, and PHICA” for contact information for such a license.

1.2 REFERENCES

1.2.1 NORMATIVE REFERENCE LIST

The following standards contain provisions that, through reference in this text, constitute normative provisions of this Specification. At the time of publication, the editions indicated are current. All standards are subject to revision, and parties to agreements based on this Specification are encouraged to investigate the possibility of applying for the most recent editions of the standards listed in this section.

1. ANSI/SCTE 28 2007: “Host-POD Interface Standard”
2. CEA-679-C: “National Renewable Security Standard,” Part B, (October 2005) “National Renewable Security Standard” (March 2000)
3. ITU-T Recommendation X.509, “Information Technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks”, August 2005.
4. FIPS PUB 46-3: “Data Encryption Standard (DES)” 1999 October 25
5. FIPS-PUB 81: “DES Modes of Operation” 1980 December 21

6. FIPS PUB 140-2: “Security Requirements for Cryptographic Modules”, 2001 May 25
7. FIPS PUB 180-2: “Secure Hash Standard”, 2002 August 1
8. FIPS PUB 186-2, “Digital Signature Standard” Federal Information Processing Standards Publications (FIPS PUB), 2000 January 27.
9. RSA1, “PKCS #1: RSA Encryption Standard”, Version 1.5, November 1993
10. MPEG: ISO/IEC 13818-1:2008 Information Technology - Generic coding of moving pictures and associated audio information: Systems
11. DFAST: Dynamic Feedback Arrangement Scrambling Technique; a component of the encryption algorithm specified by the PHICA. Available under license from CableLabs, see Section 1.1.

1.2.2 INFORMATIVE REFERENCE LIST

The following references contain information that is useful in understanding of this Specification. Some of these documents are drafts of standards or balloted standards with unresolved comments.

1. RSA3, “PKCS #10 V1.7: Certification Request Syntax Standard”, May 2000

1.2.3 REFERENCE ACQUISITION

DFAST Technology, PHILA, and PHICA: Cable Television Laboratories, Inc.

Cable Television Laboratories, Inc., 400 Centennial Parkway, Louisville, CO 80027; Telephone: 303-661-9100; Facsimile: 303-661-9199;
E-mail: opencable@cablelabs.com; URL: [<www.cablelabs.com>](http://www.cablelabs.com)

CEA Standards: Consumer Electronics Association

Global Engineering Documents, World Headquarters, 15 Inverness Way East, Englewood, CO USA 80112-5776; Telephone 800-854-7179; Facsimile: 303-397-2740; E-mail: global@ihs.com ; URL: [<http://global.ihs.com>](http://global.ihs.com)

IEEE Standards: Institute of Electrical and Electronic Engineers

Institute of Electrical and Electronic Engineers, 445 Hose Lane, Piscataway, NJ 08855-1331, USA; E-mail: customer.service@ieee.org ;
URL: <http://standards.ieee.org/index.html>

ISO: International Standards Organization

Global Engineering Documents, World Headquarters, 15 Inverness Way East, Englewood, CO 80112-5776, USA; Telephone: 800-854-7179; E-mail: global@ihs.com; URL: <http://global.his.com>

ITU-T: International Telecommunications Union – Telecom Standardization

International Telecommunications Union, Geneva, Switzerland.

URL: <<http://www.itu.int/publications/index.html>>

NIST Publications: National Institute of Standards and Technology

National Technical Information Service (NTIS), U. S. Department of Commerce,
5285 Port Royal Road, Springfield, VA 22161;

Telephone: 1-800-553-NTIS (6847) or 703-605-6000; FAX: 703-321-8547;

E-mail orders: orders@ntis.fedworld.gov, URL: <<http://www.itl.nist.gov/fipspubs/>>

RSA Security

RSA Security, Inc, 174 Middlesex Turnpike, Bedford, MA 01730; Telephone: 781 515 5000; FAX: 781 515 5010; URL: <<http://www.rsasecurity.com/rsalabs/pkcs>>

SCTE Standards: Society of Cable Telecommunications Engineers

Society of Cable Telecommunications Engineers, 140 Philips Road, Exton, PA 19341, USA. Telephone: 610-363-6888; Facsimile: 610-363-5898; E-mail: scte@scte.org;

URL: <<http://www.scte.org/standards/standardsavailable.html>>

1.3 ACRONYMS, ABBREVIATIONS, AND DEFINED TERMS

APDU	Application Protocol Data Unit: a command, query, and reply message exchange protocol between POD and Host
APS	Analog Protection System for copy control of analog output video
AuthKey	Authentication Key, calculated by both the POD and Host as part of the Host authentication process
Authentication	A procedure to securely confirm that a Host or POD has a genuine X.509 certificate and that the certificate has not been revoked. Also: a means to securely confirm that a message originated in a trusted source.
Authenticated	A quality resulting from the application of an Authentication procedure; securely confirmed.
CA, CA System	Conditional Access, Conditional Access System – secures delivery of Cable services to the POD from unauthorized access
CA-only	The POD mode of CA-descrambling EMI=0 content and returning it to the Host CP-unscrambled
Cable	The Cable Television industry, services, systems, or equipment
CCI	Copy Control Information
CP	Copy Protection
CP-Key	The Copy Protection Key derived between the POD and Host, and used by the POD to CP-scramble protected content sent to the Host
CP System	The Copy Protection System described in this specification
CRL	Certificate Revocation List: the means of reporting bad Host_ID's to Cable Headends
CSR	Customer Service Representative
DES	Data Encryption Standard
DES-ECB	Data Encryption Standard – Electronic Code Book
DFAST	Dynamic Feedback Arrangement Scrambling Technique, a component of the encryption algorithm
DH	Diffie-Hellman, a public key agreement protocol based on the intractability of taking discrete logarithms over the integer field
EMI	“Encryption Mode Indicator” As used in this document the meaning of this acronym is "Copy Control" Mode Indicator for digital outputs.

EMM	Entitlement Management Message
Encrypted	Data modified to prevent unauthorized access (compare with "scrambled")
FAT	Forward Application Transport, the 6 MHz digital channels from Headend to home and between POD and Host
Host Certificate	The unique X.509 certificate issued to each Host device and used for Host authentication. Parameter name: <i>Host_DevCert</i>
Host Certificate List	The pair of X.509 certificates provided by the Host to the POD for certificate verification: <i>Host_DevCert</i> and <i>Host_ManCert</i>
Host_ID	The Host device's unique identification number
LSB	Least Significant Bit, of a specified binary value
Manufacturer XCA	X.509 certificate authority authorized by PHICA to issue POD or Host Certificates. PHICA issues each Manufacturer XCA a unique manufacturer's certificate, <i>POD_ManCert</i> or <i>Host_ManCert</i> , which are used to verify POD or Host Certificates.
MMI	Man Machine Interface
MPEG	The ISO/IEC 13818 specifications and ISO/IEC 13818-1 in particular
MSB	Most Significant Bit, of a specified binary value
Nonce	A random value generated fresh for each use and included in some Host-POD exchanges to make each exchange unique
Pass-through	The POD mode of passing CA-scrambled back to the Host unchanged, leaving it unusable by the Host
PHI	POD-Host Interface as specified in ANSI/SCTE 28 2007
PHICA	POD-Host Interface Certificate Authority, root X.509 certificate administrator for X.509 certificates on the PHI. Identified under PHILA
PHILA	POD Host Interface Licensing Agreement, covers the DFAST technology and specifies the PHI Certificate Authority - PHICA
POD or POD Module	CableCARD Point of Deployment module, the removable PC-Card form factor Cable security module
POD Certificate	The unique X.509 certificate issued to each POD and used for POD authentication. Parameter name: <i>POD_DevCert</i> .
POD Certificate List	The pair of X.509 certificates provided by the POD to the Host for certificate verification: <i>POD_DevCert</i> and <i>POD_ManCert</i>

POD-CP	POD copy protection, as specified in this document
POD CPS	The POD Copy Protection System, as specified in this document
POD_ID	The POD module's unique identification number
RDC	Return Data Channel: transmitted from home to Headend
Report-back	The action or process of reporting information from the POD or Host back to the Headend
Rescramble	The POD mode of CA-descrambling and CP-scrambling content
RSA algorithm	An RSA Security defined commercial public key cryptographic algorithm
SATP	Simple Authenticated Tunnel Protocol
Scrambled	Content modified to prevent unauthorized access (compare with "encrypted")
SHA-1	Secure Hash Algorithm, a cryptographic compression function
Shall	"Shall" denotes a mandatory provision of this standard
Should, May	"Should" denotes a provision that is recommended but not mandatory. "May" denotes a feature whose presence does not preclude compliance and may or may not be present at the option of the implementer.
SPDU	Session Protocol Data Unit (SPDU)
SSK	A shared secret system parameter used by both POD (SSK_P) and Host (SSK_H) to authenticate the exchange of Diffie-Hellman public key parameters.
Validation	The process of reporting the Host_ID to the system operator, checking it against a revocation list, reporting the validated Host_ID back to the POD, and the POD confirming it matches the stored Host_ID.
X.509	The ITU-T Recommendation X.509 standard
XCA	X.509 certificate authority

1.4 COPY PROTECTION SYSTEM COMPONENTS

This copy protection system (CP System) includes:

- The Cable navigation device, or Host
- The POD module
- The Cable Headend (which revokes selected services from compromised Hosts)
- The PHICA which issues device ID's and generates X.509 manufacturer certificates.

1.5 IMPLEMENTATION OUTLINE

The POD CP System consists of the following two operational elements:

Host Authentication, based on the exchange of Host and POD certificates across the POD-Host interface. Each device verifies the other's certificate using signature verification techniques, and the Host and POD IDs are reported to the Headend. The Headend compares the IDs against a revocation list and takes appropriate revocation action against compromised devices.

Copy Protection Key Derivation, using a Diffie-Hellman shared secret key that was computed during the Host Authentication process. CP-scrambling by the POD of content marked with non-zero EMI. The POD first CA-descrambles this content and then rescrambles such High Value content using the Copy Protection Key before delivery to the Host. A companion CP-descrambling process occurs in the Host.

1.6 HISTORICAL PERSPECTIVE

This specification has its origins in EIA-679 (now CEA-679,) the National Renewable Security Standard, which was initially adopted in September 1998. Part B of that standard has the physical size, shape and connector of the computer industry PCMCIA card.

That standard did not take into account the requirements of the movie industry to protect against the unrestricted copying of digital video movies and programs.

Further extensions and modifications of EIA-679 led to the adoption of EIA-679-B in March 2000. EIA - 679-B permits the use of copy protection techniques but does not select any single approach.

Consequently, the Cable industry selected the particular approach embodied in this document, and submitted it as DVS/213 in June 1999. Extensive revisions were developed by the Cable industry, and submitted as DVS 301 (January 2000). Work on this document by the Cable industry proceeded during the first half of 2000, leading to substantial changes that were embodied in DVS 301r1, r2 and finally DVS301r3 which was successfully balloted and adopted as ANSI/SCTE 41 2001.

A subsequent update was proposed, balloted and approved as SCTE 41 2003. This document updates that work to current industry practice, notably by revising the authentication method to one based on X.509 standard certificates.

1.7 RELATED DOCUMENTS

This document is intended to supplement the functionality of the POD module interface described in ANSI/SCTE 28 2007 [1] which defines how copy protection fits into the overall POD module interface functionality.

2. SYSTEM OVERVIEW (INFORMATIVE)

2.1 NRSS COPY PROTECTION FRAMEWORK

This document is based on the copy protection framework defined in CEA-679-C, National Renewable Security Standard (NRSS), Part B, section 8.9 [2] with some substantial changes. The NRSS Copy Protection Framework includes:

- POD/Host Binding,
- DES-ECB Scrambling System (FAT Channel),
- MPEG Systems for the transport layer (FAT Channel),
- NRSS-B Interface Copy Protection Resource (Data Channel),
- NRSS-B Interface Messages (Data Channel).

But, NRSS doesn't reference any of the following operations that are described in this document:

- Device authentication,
- Host revocation via selective service denial.

Under the NRSS Copy Protection Framework, the POD module checks the ability of the Host to support POD-CP by checking availability of the Copy Protection Resource as defined in ANSI/SCTE 28 2007 and verifies the Host. If the Host is not valid, the POD module goes to "pass-through" mode, simply passing any received transport stream back to the Host unchanged.

2.2 DEVICE AUTHENTICATION

The CP System requires authentication of the Host and POD prior to the POD descrambling any of the copy-protected material. The POD requests the Host's X.509 Certificate List and the Host provides it. The Host requests the POD's X.509 Certificate List and the POD provides it. Authentication is based on:

- POD being able to verify the signature of the X.509 host device certificate that contains Host_ID and the POD being able to verify the signature of the Host Manufacturer's XCA certificate; and
- Host being able to verify the signature of the X.509 POD device certificate that contains the POD_ID and the Host being able to verify the signature of the POD Manufacturer's XCA certificate.
- POD and Host proving they each hold the private key paired with the public key embedded in the X.509 certificate by signing a DH session key and sending it to the other device for signature verification.
- POD and Host proving that they can derive the authentication key.
- The Host_ID and POD_ID extracted from the X.509 certificates are not included in the CRL, as checked in the Headend.

Additionally, the POD will validate the authenticity of the X.509 Host Certificate and the Host will validate the authenticity of the X.509 POD Certificate using the License Administrator's public verification keys that are delivered by the CA System to the POD and Host in an authenticated manner. If the *Validated_Host_ID* value is the same as the Host_ID in the authenticated X.509 Host Device Certificate and the *Validated_POD_ID* value is the same as the POD_ID in the authenticated X.509 POD Device Certificate, the Host and POD can continue with the key exchange process described in Chapter 3.

2.2.1 BI-DIRECTIONAL HOST AND CABLE SYSTEM

If both the Host and Cable system support automatic report-back, via either telco modem or an on-cable return channel, the POD sends the POD and Host information on that channel without the need for manual reporting.

2.2.2 MANUAL RETURN AUTHENTICATION

The POD and Host ID's must be reported to the service provider before the Host can access Copy Protected content. The end-user or the retailer may perform this service.

For one-way Cable systems, unidirectional Hosts, or any system without a functioning automatic report-back mechanism, reporting of the authentication ID's is accomplished manually. For example: the user making a telephone call to the service provider. The manual return authentication process is detailed in section 3.2.1.

2.2.3 POD SUPPORT FOR MULTIPLE HOSTS

Although it may be technically feasible to build a POD that is capable of binding to multiple Hosts, such that the POD can be moved from Host to Host, such operation is beyond the scope of this specification. Multiple Host capability may be added to a future extension of this specification.

2.3 KEY EXCHANGE AND TRANSPORT STREAM PROTECTION

The copy protection mechanism itself consists of three phases: Setup, Key Derivation, and Interface Encryption. PODs and Hosts contain the algorithms for Diffie-Hellman (DH) key negotiation, SHA-1 hashing, and DES. The DH system-wide constants (g and n) are chosen to be large enough to be secure for the long term (e.g., n is 1024 bits for DH based on discrete log). These constants are provided under license by the PHICA. PODs and Hosts also contain private keys (x and y , respectively) and the corresponding public keys ($g^x \bmod n$ and $g^y \bmod n$). The private keys x and y are pseudorandom integers generated each time a POD and Host are bound. The private keys must also be large enough to be secure for the long term (e.g., 1024 bits for DH based on discrete log).

2.3.1 SETUP PHASE

In case of successful mutual authentication between POD and Host, the POD and the Host negotiate and derive two long term shared secrets using Discrete Logarithm Diffie-Hellman in a protocol that is detailed later in Chapter 3 to exchange data across the interface. One of the long-term secrets is a 160-bit authentication key, and the other is a 1024-bit shared DH secret value. Finally SHA-1 and DFAST intellectual property are used to generate a Copy Protection Key (CP-Key).

2.3.1.1 AUTHENTICATION KEY SETUP

Normally an authentication key ($\text{AuthKey}_P/\text{AuthKey}_H$) is only calculated once during POD-Host binding and stored in non-volatile memory.

If AuthKey_H delivered by the Host after power-up does not match the AuthKey_P stored by the POD, then the entire Host authentication process is re-initialized.

The AuthKey generation process is detailed in section 4.1.

2.3.1.2 LONG TERM DIFFIE-HELLMAN SHARED KEY VALUE

Similar to the authentication key process, Diffie-Hellman shared key calculation is normally conducted when the Host authentication process is initiated. The derived DH shared secret (DHKey) is saved in non-volatile memory once it is calculated.

2.3.2 KEY DERIVATION PHASE

After a POD module and Host complete authentication, each device derives the Copy Protection Key (CP-Key). The CP-Key is calculated based on the long-term keys, AuthKey, DH keys, and the random numbers exchanged for key generation. This CP-Key is unique to the particular POD-Host pair, and serves to bind them together for content protection. Details are discussed in chapters 3 and 4.

2.3.3 INTERFACE ENCRYPTION

The POD uses encryption techniques to scramble copy-protected content transmitted across its interface with the Host. The POD rescrambles the content it has descrambled under the conditional access system using DES in ECB mode and the computed Copy Protection Key before sending it across the interface to the Host.

The POD passes content in one of four modes determined by CA System scrambling mode and EMI values as detailed in Table 7.4-A:

- Clear: no change of CA-uncrambled and EMI=0 content which remains 'in-the-clear'
- CA-only: descrambles CA-scrambled content marked EMI=0 for output 'in-the-clear'
- Rescramble: CA-descrambles and CP-scrambles content marked EMI>0
- Pass-through: no change of CA-scrambled content (leaving it unrecognizable to the Host)

The Copy Protection Key is applied across all rescrambled packets. Only one copy-protected MPEG program is delivered from the POD to the Host at any time.

The POD CP-scrambles only the payload portion of transport packets using DES electronic code book (DES-ECB) encryption. DES-ECB encrypts data in 8-byte blocks. The ECB DES is applied block-by-block, starting at the beginning of the transport packet payload. Any short block will therefore occur at the end of the transport packet. Partial blocks (e.g. less than 8 bytes) remaining at the end of a scrambled transport packet are not encrypted. The transport packet header and adaptation field (if any) is not scrambled. See chapter 7.

2.4 DATA CHANNEL PROTECTION

There are currently no messages defined on the data channel or extended channel POD↔Host interface that require message encryption. However, CCI information travelling from POD to Host is authenticated, as described in Chapter 6.

2.4.1 COPY CONTROL INFORMATION

Copy control information (CCI) is passed from the POD module to the Host across the data channel to inform the Host device of the level of copy protection required. The CCI is sent in the clear to the Host device, but the integrity of the information is maintained by authenticating the CCI using a simple protocol.

The one-byte CCI field contains information that the Host uses to control copying of content. Two EMI bits control copying on Host digital outputs, two APS bits control copying on analog outputs, and four bits are reserved.

2.4.2 RULES FOR CP-SCRAMBLING BASED ON EMI VALUE AND CA-SCRAMBLING

1. CP-scrambling is applied only to protected content, as indicated by EMI greater than zero.
2. All copy-protected content is delivered CA-scrambled to the POD.
3. Non-copy-protected content, with EMI = 00, may be delivered to the POD either CA-scrambled or CA-unscrambled.

2.5 IDENTIFYING FRAUDULENT DEVICES AND DISABLING OF SERVICES

The POD requests and verifies the Host Certificate. The POD then extracts the Host ID and passes it, by either manual or automated means to the service provider. The service provider confirms the Host is permitted to receive protected content by returning a Host_ID validation message back to the POD.

If the service provider determines that a fraudulent Host device should no longer receive a service or group of services, the conditional access system denies the appropriate services to the POD that is bound to the fraudulent Host. Restoration of services is also executed by the conditional access system. This CA System-based revocation is known as *Selective Service Denial* that may entail:

- Complete loss of service
- Loss of particular channels, e.g., HBO™ or Showtime™.
- Loss of individual programs on channels

The service provider may use CA mechanisms to deliver “pass/no pass” commands to the POD for each service as well as new copy protection parameters. Service provider involvement and control provides a highly flexible system for protection of content copyrights.

3. HOST AUTHENTICATION MECHANISMS

3.1 PROTOCOL COMPONENTS

Host authentication is based on:

- The POD and Host verifying the opposite device's certificate signature
- The POD and Host verifying, with the received public key, a unique message signed with the opposite device's private key.
- The CA system confirming that the POD and Host ID's extracted from the X.509 certificates are not in the CRL

3.1.1 X.509 VERSION 3 CERTIFICATE

The POD and Host each have a private key used for digital signatures and an X.509 Certificate. The certificate includes a unique ID and the public key provided to other devices to validate the digital signatures. Each device also has its Manufacturer CA's certificate that is used to sign the device certificate, and the root certificates that is used to sign the Manufacturer CA's certificate

3.1.2 DEVICE PARAMETERS

The following device parameters are used in this authentication protocol:

- DH_pubKey_H : The Host Diffie-Hellman public key, also used as a Host-generated nonce in the calculation of the Authentication Key.
- DH_pubKey_P : The POD Diffie-Hellman public key, also used as a POD-generated nonce in the calculation of the Authentication Key.
- $AuthKey_H$ (derived): The Host Authentication Key.
- $AuthKey_P$ (derived): The POD Authentication Key.

Table 3.1-A Length of Device Parameters in the Host Authentication

Key or Variables	Size (bits)
Diffie-Hellman Public Keys (DH_pubKey_H , DH_pubKey_P)	1024 each
Authentication Keys ($AuthKey_H$, $AuthKey_P$)	160 each

3.1.3 SYSTEM PARAMETERS

Table 3.1-B defines system parameter length and source:

Table 3.1-B Length of System Parameters

Key or Variable	Size (bits)	Source of Parameter
POD_ID	64 bits	PHICA and manufacturer
Host_ID	40 bits	PHICA and manufacturer
Diffie-Hellman prime (n)	1024 bits	PHICA
Diffie-Hellman base (g)	1024 bits	PHICA
RSA public signing key exponent	40 bits	PHICA

3.1.4 PROCESSING BASICS

The POD Copy Protection System (CPS) comprises the following basic steps:

1. The Host shall report copy protection as a resource during the profile inquiry process (see ref. 1). Failure to do so constitutes a failure of the copy protection system (see section 3.2.2). After the copy protection resource has been reported, the POD module shall permit CA decryption of programs with a EMI value of 00.
2. The POD module shall open a session to the copy protection resource, section 8.2.1. Failure to open a valid session constitutes a failure of the copy protection system (see section 3.2.2).
3. The POD module shall send a *CP_open_req APDU* to the Host, section 8.2.2.1.
4. The Host shall respond with *the CP_open_cnf APDU* within 5 seconds. Failure to respond to any request within 5 seconds constitutes a failure of the Host and shall cause the POD module to set the IIR flag (see ref. 1).
5. The Host shall respond with the System 2 bit set in *CP_system_id_bitmask*, section 8.2.2.2. Failure to do so constitutes a failure of the copy protection system (see section 3.2.2).
6. If the POD module contains a valid Authentication key in its non-volatile memory, it shall request the Host to send its AuthKey_H.
7. The Host shall respond with its AuthKey_H, if available. If it is not available, then it shall transmit a value of all 0's. A value of all 0's shall be recognized by the POD as an invalid AuthKey_H.
8. The POD module shall compare the received AuthKey_H with its stored AuthKey_P. If the authentication keys match, then the certificates are considered valid, the DH Key and authentication keys are preserved, only the Copy Protection Key is regenerated, and continue with step 17. If the authentication keys do not match the POD shall set Headend Validated to false in nonvolatile memory and the POD and Host shall continue with step 9.
9. The POD module shall send its POD Certificate Data (*POD_DevCert* and *POD ManCert*), the newly generated DH public key (*DH_pubKey_P*), and the Diffie-Hellman key signature. In this message, the POD also requests that the Host deliver its Host Certificate Data (*Host_DevCert* and *Host_ManCert*) and signed DH public key (*DH_pubKey_H*).

10. The Host shall reply to the POD module request with its Host Certificate Data (*Host_DevCert* and *Host_ManCert*) and newly generated and signed DH public key.
11. The POD module shall verify the *Host_DevCert*, the *Host_ManCert*, the signature on the Diffie-Hellman public key (*DH_pubKey_H*) and extract the *Host_ID* from the Host certificate. If verification fails, this constitutes a failure of the copy protection system (see section 3.2.2).
12. The Host module shall verify the *POD_DevCert*, the *POD_ManCert*, the signature on the Diffie-Hellman public key (*DH_pubKey_P*) and extract the *POD_ID* from the POD certificate. If verification fails, this constitutes a failure of the copy protection system (see section 3.2.2).
13. After these exchanges, both the POD module and the Host come up with their respective authentication key, *AuthKey_P* and *AuthKey_H*.
14. The POD module shall request *AuthKey_H* and compare it to *AuthKey_P*. If they are not equal, this constitutes a failure of the copy protection system (see section 3.2.2). If they are equal, then the POD module and Host shall complete the Diffie-Hellman operation and store the derived authentication key into non-volatile memory.
15. If headend validation of the POD and Host ID is complete, go to step 18. Otherwise, the following depends upon what path is available to report device IDs to the headend.
 - a. If possible, i.e., in a system with an active return data channel or telco return path, the POD module shall send the *POD_ID* and *Host_ID* to the cable headend via an upstream OOB private CA message or telco modem. The POD module also stores the *Host_ID* and *POD_ID*s in nonvolatile memory so they can be compared with the validated IDs received back from the headend. Status of this transmission shall be stored in non-volatile memory to prevent unnecessary retransmissions.
 - b. In systems in which no automated return path is available, the POD module sends a display message as defined in section 3.2.5.1.
16. The headend CA System records the pairing between *Host_ID* and *POD_ID*, and looks for the *Host_ID* in the revocation list. If not found, the CA System re-sends the *Host_ID* and *POD_ID* back to the POD module in a private authenticated CA System ID validation message. This message may be sent to the POD module substantially later in time than when the POD and *Host_ID*'s are reported to the headend.
17. Until the POD and Host ID headend validation is completed the POD module shall CA decrypt only those services with an EMI value of 00.

[Asynchronously and independent of this process, the CA system typically sends an EMM to the POD module to authorize appropriate services. Some of these services may have EMI values of 01, 10, or 11. The POD module shall not CA-descramble services with these EMI values until headend ID validation is complete, even if these services are otherwise authorized in an EMM.]

18. The POD module authenticates the ID validation message and compares the received *Host_ID* and *POD_ID* with the ID's extracted from the Host device certificate and the POD device certificate, respectively. If they match, the POD module shall store the Headend Validated True in nonvolatile memory and allow CA decryption of high value content with EMI values of 01, 10, or 11, if so authorized by an EMM. If they do not match, the POD module shall continue to limit its CA decryption to those services with EMI values of 00 only.
19. If the headend CA system receives a new revocation list, it shall examine all previously reported IDs and if there are any matches, it shall notify the cable operator.

20. If a POD module reports a failure of the copy protection system to the headend CA system, the headend CA system shall notify the cable operator.

The following flowcharts show an implementation of the above steps:

POD-Host CP Operation

Note: This chart is an informative illustration of a possible compliant solution. Other solutions are permissible within the requirements of this document.

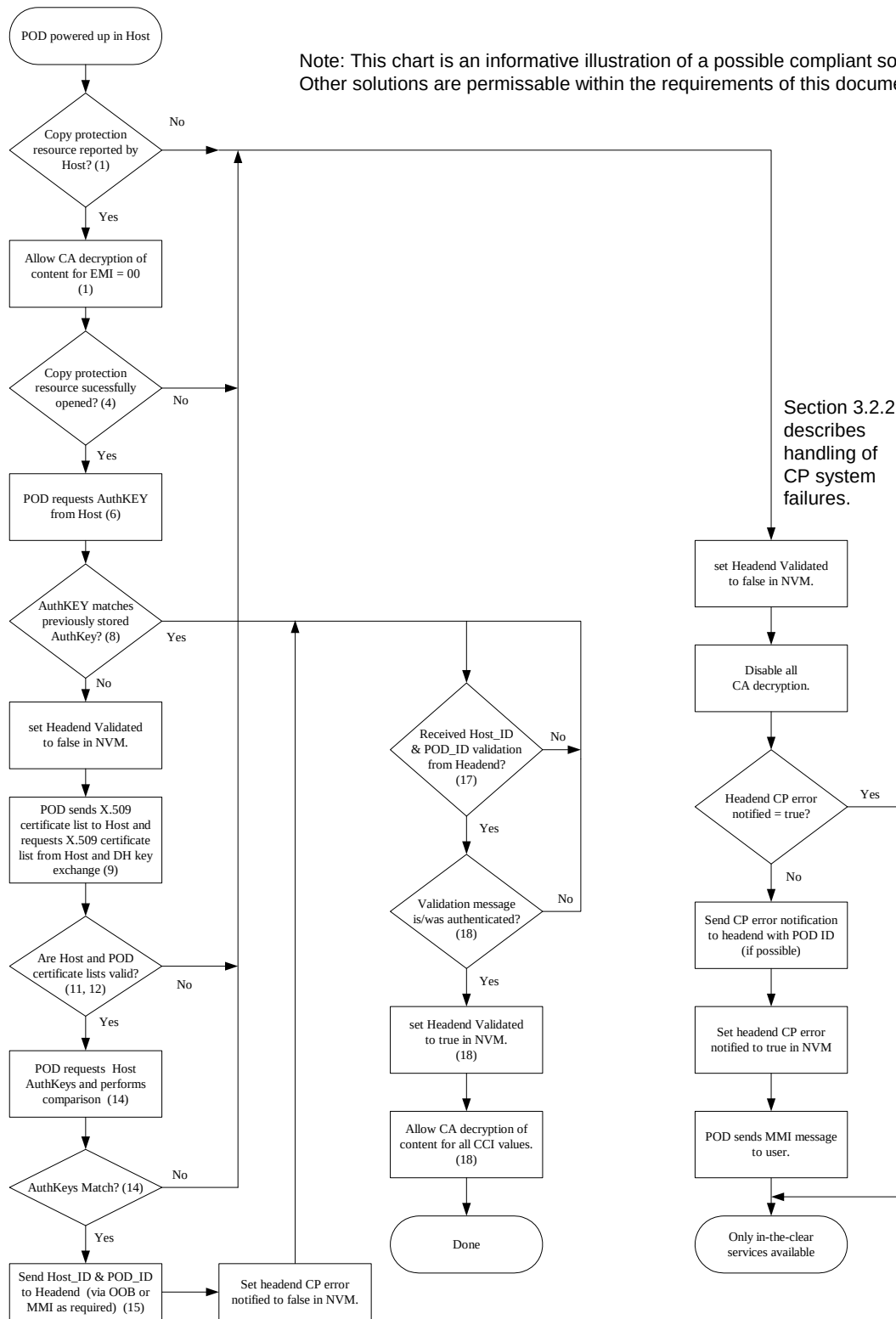


Figure 3.1-A POD-Host CP Operation