ETSI TS 102 639-5 V1.1.1 (2009-04)

Technical Specification

Access and Terminals, Transmission and Multiplexing (ATTM); Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems; Part 5: Security Services

[ITU-T Recommendation J.222.3 (07/2007), modified]

Reference
DTS/ATTM-02006-5

Keywords
aceess, broadband, cable, endorsement, MAC, modem

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Access, Terminals, Transmission and Multiplexing (ATTM).

The present document is part 5 of a multi-part deliverable covering Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable modems. Full details of the entire series can be found in part 1 [i.1].

Introduction

This European Standard (Cable DOCSIS 3.0 Network series) has been produced by ETSI Access, Terminals, Transmission and Multiplexing Technical Committee (ATTM), Cable Access Network sub-group.

1 Scope

The present document defines the security requirements as part of a series of specifications for the third generation of high-speed Data-Over-Cable Systems Interface Specifications (DOCSIS®).

They were developed for the benefit of the cable industry, including contributions by operators and vendors from, Europe, North America and other regions.

The source material for this specification was provided by the ITU-T Recommendation J.222.3 [3] for which the most recent version can be found at http://www.itu.int/ITU-T/.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 102 639-4: "Access and Terminals, Transmission and Multiplexing (ATTM); Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems; Part 4: MAC and Upper Layer Protocols ITU-T Recommendation J.222.2 (07/2007), modified]".

[2] ETSI TS 101 909-11 "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security".

[3] ITU-T Recommendation J.222.3" Third-generation transmission systems for interactive cable television services - IP cable modems: Security services".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.2] ETSI TS 102 639-3: "Access and Terminals, Transmission and Multiplexing (ATTM); Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems; Part 3: Downstream Interface [ITU-T Recommendation J.210 (11/2006), modified]".

[i.3] ETSI TS 102 639-1: "Access and Terminals, Transmission and Multiplexing (ATTM); Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems; Part 1: General".

[i.4] ETSI ES 201 488: "Access and Terminals (AT); Data Over Cable Systems; Part 1: General".

[i.5] ITU-T Recommendation J.222.1: "Third-generation transmission systems for interactive cable television services - IP cable modems: Physical layer specification".

[i.6] ITU-T Recommendation J.210: "Downstream RF Interface for Cable Modem Termination Systems".

[i.7] ITU-T Recommendation J.222.2: "MAC and Upper Layer protocols for third-generation transmission systems for interactive cable television services - IP cable modems".

[i.8] ITU-T Recommendation J.112: "Transmission systems for interactive cable television services".

[i.9] ITU-T Recommendation J.170: "IPCablecom security specification".

[i.10] ITU-T Recommendation X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

DER Encoded: Refers to a value which is encoded using the ASN.1 Distinguished Encoding Rules (see ITU-T Recommendation X.690 [i.11]).

downstream: flow of signals from the cable system control center through the distribution network to the customer

NOTE: For communication purposes, associated with transmission (down) to the end-user.

dynamically-joined multicast sessions: multicast sessions joined after cable modem registration

key transition period: time period in which an Authentication Key that is near its expiration is replaced by a new Authentication Key through a negotiated update process between the CMTS and the CM

MAC domain: logical link layer network consisting of a common address scheme (such as IEEE 802.3 Ethernet) in which elements may send and receive OSI layer 2 messages between and among one another

NOTE: MAC domain boundaries may be established through both physical and logical means; separate channels or subchannels utilizing differing frequency and/or encoding methods, or assigning separate bundles/bridge groups or subinterfaces to common frequency-domain channels or subchannels.

static multicast sessions: multicast sessions joined during cable modem registration

upstream: term used to describe traffic and paths that go from the subscriber to the headend

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASN.1	Abstract Syntax Notation 1
CM	Cable Modem
CMCI	Cable Modem to Customer Premises Equipment Interface
CMTS	Cable Modem Termination System
CRL	Certificate Revocation List

DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DOCSIS	Data-Over-Cable Service Interface Specifications
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPR	Intellectual Property Rights
IPv6	Version 6 of the Internet Protocol
ISO	International Organization for Standards
MAC	Media Access Control
MMH	Multilinear Modular Hash
OCSP	Online Certificate Status Protocol
RFC	Request For Comments
RSA	Rivest, Shamir, Adleman (a public key cryptographic algorithm)
RTP	Real-time Transport Protocol
SA	Security Association
SET	Secure Electronic Transaction
SHA-1	Secure Hash Algorithm 1
TFTP	Trivial File Transfer Protocol

Endorsement notice

Modifications to ITU-T Recommendation J.222.3

The elements of ITU-T Recommendation J.222.3 [3] (07/2007) apply, with the following modifications:

NOTE: Underlining and/or strike-out are used to highlight detailed modifications where necessary.

Replace references given in J.222.3 as shown in table 1.

Table 1

	Reference(s) in J.222.3 [3]	Replaced reference(s)
1	ITU-T Recommendation J.222.1	ETSI TS 102 639-2
2	ITU-T Recommendation J.210	ETSI TS 102 639-3
3	ITU-T Recommendation J.222.2	ETSI TS 102 639-4
4	ITU-T Recommendation J.222.3	ETSI TS 102 639-5
5	ITU-T Recommendation J.112	ETSI ES 201 488
6	ITU-T Recommendation J.122	ETSI ES 202 488-2
7	ITU-T Recommendation J.170	ETSI TS 101 909-11

Annex A (informative): Bibliography

ITU-T Recommendation J.125: "Link privacy for cable modem implementations".

Proposed Draft SCTE Standard, DOCSIS Operations Support System Interface Specification version 3.0.

ETSI ES 202 488-2: "Access and Terminals (AT); Second Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems; Part 2: Radio frequency interface specification".

Federal Information Processing Standards Publication (FIPS PUB) 46-3: "Data Encryption Standard", October 1999.

Federal Information Processing Standards Publication (FIPS PUB) 140-2: "Security Requirements for Cryptographic Modules", June 2001.

Federal Information Processing Standards Publication (FIPS PUB) 180-2: "Secure Hash Standard", February 2003.

Federal Information Processing Standards Publication (FIPS PUB) 197: "Advanced Encryption Standard", November, 2001.

ISO 8859-1: "8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No.1".

NIST-800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Morris Dworkin, 2001 Edition.

IETF RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.

IETF RFC 826: "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", D.C. Plummer.

IETF RFC 1350: "The TFTP Protocol, Revision 2", K. Sollins.

IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1", R. Fielding, et al.

IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication", H. Krawczyk et al.

IETF RFC 3376: "Internet Group Management Protocol, Version 3", B. Cain, et al.

IETF RFC 2347: "TFTP Option Extension", G. Malkin, A. Harkin.

IETF RFC 2348:" TFTP Blocksize Option", G. Malkin, A. Harkin.

IETF RFC 2349: "TFTP Timeout Interval and Transfer Size Options", G. Malkin, A. Harkin.

IETF RFC 2461: "Neighbor Discovery for IP Version 6 (IPv6)", T. Narten, E. Nordmark, W. Simpson.

IETF RFC 2560: "X.509 Internet Public Key Infrastructure Certificate Status Protocol - OCSP", M. Myers et al.

IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", R. Housley, W. Ford, W. Polk, D. Solo.

IETF RFC 4131: "Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modems and Cable Modem Termination Systems for Baseline", S. Green et al.

IETF RFC 2437: "PKCS #1: RSA Cryptography Specifications Version 2.0".

ITU-T Recommendation X.509 (1997): "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework".

ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002, Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

Data-Over-Cable Service Interface Specifications Cable Modem to Customer Premise Equipment Interface Specification SP-CMCI-I10-050408, April 8, 2005, Cable Television Laboratories, Inc.

ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".

S. Halevi and H. Krawczyk, "MMH: Software Message Authentication in Gbit/sec Rates," Proceedings of the 4th Workshop on Fast Software Encryption, (1997) vol. 1267 Springer-Verlag, pp. 172-189.

IETF RFC 1750: "Randomness Recommendations for Security", D. Eastlake, et al.

IETF RFC 2202: "Test cases for HMAC-MD5 and HMAC-SHA-1", P. Cheng, R. Glenn.

IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications", H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson.

IETF RFC 3447: "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1".

RSA Laboratories, "Some Examples of the PKCS Standards," RSA Data Security, Inc., Bedford, MA, November 1, 1993.

ANSI/SCTE 22-2: "DOCSIS 1.0 Baseline Privacy Interface".

ANSI/SCTE 52 2003: "Data Encryption Standard Cipher Block Chaining Pocket Encryption".

SET, Secure Electronic Transaction Specification Book 2: Programmer"s Guide, Version 1.0, May 31, 1997.

ITU-T Recommendation X.680, (July, 2002): "Abstract Syntax Notation One (ASN.1): Specification of basic notation".