SLOVENSKI STANDARD
SIST EN 302 878-5 V1.1.1:2012

01-februar-2012

Dostop, priključki, prenos in multipleksiranje (ATTM) - Tretja generacija prenosnih sistemov za storitve interaktivne kabelske televizije - IP-kabelski modemi - 5. del: Varnostne storitve - DOCSIS 3.0

Access, Terminals, Transmission and Multiplexing (ATTM) - Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems - Part 5: Security Services - DOCSIS 3.0

Ta slovenski standard je istoveten z: **EN 302 878-5 Version 1.1.1**

ICS:

35.180	Terminalska in druga periferna oprema IT	IT Terminal and other peripheral equipment

SIST EN 302 878-5 V1.1.1:2012 **en**

ETSI EN 302 878-5 V1.1.1 (2011-11)

Access, Terminals, Transmission and Multiplexing (ATTM); Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems; Part 5: Security Services; DOCSIS 3.0

Reference
DEN/ATTM-003006-5

Keywords
access, broadband, cable, data, IP, IPCable, 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://ipr.etsi.org).

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 European Standard (EN) has been produced by ETSI Technical Committee Access, Terminals, Transmission and Multiplexing (ATTM).

The present document is part 5 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.9].

National transposition dates	
Date of adoption of this EN:	14 November 2011
Date of latest announcement of this EN (doa):	29 February 2012
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 August 2012
Date of withdrawal of any conflicting National Standard (dow):	31 August 2012

1 Scope

1.1 Introduction and Purpose

The present document is part of a series of specifications that define the third generation of high-speed data-over-cable systems. This series was developed for the benefit of the cable industry, and includes contributions by operators and vendors from North America, Europe, and other regions.

The present document defines the Base Line Privacy Plus (BPI+) architecture which covers CM authentication, key exchange, and establishing encrypted traffic sessions between the CM and CMTS. Early Authentication and Encryption (EAE) applies BPI+, earlier in the provisioning process (see clause 8). This specification also defines security features for the CM provisioning process, which includes Secure Software Download (SSD).

1.2 Requirements

Throughout the present document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

The present document defines many features and parameters and a valid range for each parameter is usually specified. Equipment (CM and CMTS) requirements are always explicitly stated. Equipment must comply with all mandatory (MUST and MUST NOT) requirements to be considered compliant with the present document. Support of non-mandatory features and parameter values is optional.

1.3 Conventions

In this specification the following convention applies any time a bit field is displayed in a figure. The bit field should be interpreted by reading the figure from left to right, then from top to bottom, with the MSB being the first bit so read and the LSB being the last bit so read.

```
MIB syntax and XML Schema syntax is represented by this code sample font.
```

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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 necessary for the application of the present document.

[1] Cable Television Laboratories, Inc. CM-SP-OSSIv3.0-I12-100611 (June 2010): "Data-Over-Cable Service Interface Specifications - DOCSIS 3.0 - Operations Support System Interface Specification".

[2] ETSI EN 302 878-4: "Access, Terminals, Transmission and Multiplexing (ATTM); Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems; Part 4: MAC and Upper Layer Protocols; DOCSIS 3.0".

[3] ETSI ES 201 488-3 (V1.2.2): "Access and Terminals (AT); Data Over Cable Systems; Part 3: Baseline Privacy Plus Interface Specification".

[4] FIPS PUB 46-3 (October 1999): "Data Encryption Standard (DES)".

[5] FIPS PUB 140-2 (May 2001): "Security Requirements for Cryptographic Modules".

[6] FIPS PUB 180-2 (August 2002): "Secure Hash Standard".

[7] FIPS PUB 197 (November 2001): "Advanced Encryption Standard (AES)".

[8] ISO/IEC 8859-1:1998: "Information technology -- 8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No. 1".

[9] Proceedings of the 4th Workshop on Fast Software Encryption, LNCS vol. 1267, Springer, 1997. Pages 172-189: "MMH: Software Message Authentication in the Gbit/second Rates", S. Halevi and H. Krawczyk.

[10] NIST-800-38A (2001): "Recommendation for Block Cipher Modes of Operation, Methods and Techniques", Morris Dworkin.

[11] RSA Laboratories, PKCS #7 (Version 1.5, Revised November 1, 1993): "Cryptographic Message Syntax Standard", an RSA Laboratories Technical Note.

[12] IETF RFC 826/STD0037 (1982): "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware".

[13] IETF RFC 1350/STD0033 (1992): "The TFTP Protocol (Revision 2)".

[14] IETF RFC 2104 (1997): "HMAC: Keyed-Hashing for Message Authentication".

[15] IETF RFC 2347 (1998): "TFTP Option Extension".

[16] IETF RFC 2348 (1998): "TFTP Blocksize Option".

[17] IETF RFC 2349 (1998): "TFTP Timeout Interval and Transfer Size Options".

[18] IETF RFC 4861 (2007): "Neighbor Discovery for IP version 6 (IPv6)".

[19] IETF RFC 2560 (1999): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[20] IETF RFC 2616 (1999): "Hypertext Transfer Protocol -- HTTP/1.1".

[21] IETF RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[22] IETF RFC 3376 (2002): "Internet Group Management Protocol, Version 3".

[23] IETF RFC 4131 (2005): "Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus".

[24] RSA Laboratories PKCS #1 (Version 1.5 - November 1993): "RSA Encryption Standard".

[25] RSA Laboratories PKCS #1 (Version 2.0 - October 1999): "RSA Cryptography Standard".

[26] ANSI/SCTE 22-2 (2007): "Data-Over-Cable Service Interface SpecificationDOCSIS 1.0 Baseline Privacy Interface (BPI)".

[27] ANSI/SCTE 52 (2008): "Data Encryption Standard - Cipher Block Chaining Packet Encryption Specification".

[28] ITU-T Recommendation X.509 (2008): "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks".

[29] ITU-T Recommendation X.690 (2008) | 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)".

[30] IETF RFC 4388: "Dynamic Host Configuration Protocol (DHCP) Leasequery".

[31] IETF RFC 5007: "DHCPv6 Leasequery".

[32] IETF RFC 4994: "DHCPv6 Relay Agent Echo Request Option".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Cable Television Laboratories, Inc. CM-SP-CMCIv3.0-I01-080320 (March 2008): "Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment, Interface Specification".

[i.2] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".

[i.3] IETF RFC 1750 (December 1994): "Randomness Recommendations for Security", D. Eastlake 3rd, S. Crocker, J. Schiller.

[i.4] IETF RFC 2202 (September 1997): "Test Cases for HMAC-MD5 and HMAC-SHA-1", P. Cheng, R. Glenn.

[i.5] IETF RFC 3550/STD0064 (July 2003): "RTP: A Transport Protocol for Real-Time Applications", H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson.

[i.6] RSA Laboratories (November 1993): "Some Examples of the PKCS Standards", RSA Data Security, Inc., Bedford, MA.

[i.7] Secure Electronic Transaction (SET) Specification Book 2 (Version 1.0 - May 1997): "Programmer's Guide".

[i.8] ITU-T Recommendation X.680 (July 2002): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[i.9] ETSI EN 302 878-1: "Access, Terminals, Transmission and Multiplexing (ATTM); Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems; Part 1: General; DOCSIS 3.0".

[i.10] IEEE 802.3: "Ethernet Working Group".