

ČESKÁ TECHNICKÁ NORMA

ICS 33.060.40; 33.170 Červen 2012

**Přístup, koncová zařízení, přenos a multiplexování
(ATTM) - Přenosové systémy třetí generace pro
interaktivní služby kabelové televize - Kabelové modemy
IP -
Část 5: Bezpečnostní služby - DOCSIS 3.0**

ČSN
ETSI EN 302 878-5
V1.1.1
87 0003

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

Tato norma přejímá anglickou verzi evropské normy ETSI EN 302 878-5 V1.1.1:2011. Má stejný status jako oficiální verze.

This standard implements the English version of the European Standard ETSI EN 302 878-5 V1.1.1:2011. It has the same status as the official version.

Anotace obsahu

Tato norma je částí souboru specifikací, které definují třetí generaci vysokorychlostních systémů přenosu dat kabelem. Tento soubor byl vypracován pro kabelové odvětví a obsahuje příspěvky operátorů a dodavatelů ze Severní Ameriky, Evropy a dalších regionů. Tato norma definuje architekturu základní ochrany soukromí plus (BPI+), která pokrývá autentizaci (proces ověření) CM, výměnu klíčů a zavedení šifrovaných provozních relací mezi CM a CMTS. Počáteční autentizace a šifrování (EAE) používá BPI+ na počátku v procesu poskytování. Tato specifikace rovněž definuje bezpečnostní vlastnosti pro proces poskytování CM, který zahrnuje bezpečné stažení softwaru (SSD).

Národní předmluva

Informace o citovaných dokumentech

Cable Television Laboratories, Inc. CM-SP-OSSlv3.0-I12-100611:2010 nezavedena

ETSI EN 302 878-4 zavedena v ČSN ETSI EN 302 878-4 (87 0003) Přístup, koncová zařízení, přenos a multiplexování (ATTM) – Přenosové systémy třetí generace pro interaktivní služby kabelové televize – Kabelové modemy IP – Část 4: Protokoly MAC a horní vrstvy – DOCSIS 3.0

ETSI ES 201 488-3 V1.2.2 nezavedena

FIPS PUB 46-3:1999 nezavedena

FIPS PUB 140-2:2001 nezavedena

FIPS PUB 180-2:2002 nezavedena

FIPS PUB 197:2001 nezavedena

ISO/IEC 8859-1:1998 zavedena v ČSN ISO/IEC 8859-1:1999 (36 9111) Informační technologie – Jedním 8-bitovým bytem kódované soubory grafických znaků – Část 1: Latinská abeceda č. 1

Jednání 4. semináře o rychlém softwarovém šifrování, LNCS svazek 1267, Springer, 1997, str. 172-189
nezavedeno

NIST-800-38A:2001 nezavedena

RSA Laboratories, PKCS #7 (verze 1.5, revidovaná 1. listopad 1993) nezavedena

IETF RFC 826/STD0037:1982 nezavedena

IETF RFC 1350/STD0033:1992 nezavedena

IETF RFC 2104:1997 nezavedena

IETF RFC 2347:1998 nezavedena

IETF RFC 2348:1998 nezavedena

IETF RFC 2349:1998 nezavedena

IETF RFC 4861:2007 nezavedena

IETF RFC 2560:1999 nezavedena

IETF RFC 2616:1999 nezavedena

IETF RFC 5280:2008 nezavedena

IETF RFC 3376:2002 nezavedena

IETF RFC 4131:2005 nezavedena

RSA Laboratories, PKCS #1 (verze 1.5 – listopad 1993) nezavedena

RSA Laboratories, PKCS #1 (verze 2.0 – říjen 1999) nezavedena

ANSI/SCTE 22-2:2007 nezavedena

ANSI/SCTE 52:2008 nezavedena

Doporučení ITU-T X.509:2008 nezavedeno

Doporučení ITU-T X.690:2008 | ISO/IEC 8825-1:2002 nezavedeno

IETF RFC 4388 nezavedena

IETF RFC 5007 nezavedena

IETF RFC 4994 nezavedena

Cable Television Laboratories, Inc. CM-SP-CMClv3.0-I01-080320:2008 nezavedena

ISO 3166-1 zavedena v ČSN EN ISO 3166-1 (97 1002) Kódy pro názvy zemí a jejich částí – Část 1: Kódy zemí

IETF RFC 1750:1994 nezavedena

IETF RFC 2202:1997 nezavedena

IETF RFC 3550/STD0064:2003 nezavedena

RSA Laboratories (listopad 1993): „Některé příklady norem PKCS“, RSA Data Security, Inc., Bedford, MA nezavedeno

Kniha 2 specifikací bezpečných elektronických transakcí (SET) (verze 1.0 - květen 1997) nezavedena

Doporučení ITU-T X.680:2002 nezavedeno

ETSI EN 302 878-1 zavedena v ČSN EN 302 878-1 (87 0003) Přístup, koncová zařízení, přenos a multiplexování (ATM) - Přenosové systémy třetí generace pro interaktivní služby kabelové televize - Kabelové modemy IP - Část 1: Obecně - DOCSIS 3.0

IEEE 802.3 nezavedena

POZNÁMKY

1. Pokud jsou v originálu normy citovány nezaváděné dokumenty ETR, TBR, ES, EG, TS, TR a GSM, jsou dostupné v Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví, Informační centrum, Praha 1, Biskupský dvůr 5.
2. Doporučení ITU-T jsou dostupná v Českém metrologickém institutu, Hvoždanská 3, 148 01 Praha 4.

Vypracování normy

Zpracovatel: MAREŠKA Praha, IČ 86983555, Ing. Antonín Mareška

Technická normalizační komise: TNK 96 Telekomunikace

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Jan Křivka

Konec náhledu - text dále pokračuje v placené verzi ČSN v anglickém jazyce.