Avaldatud eesti keeles: oktoober 2014
Jõustunud Eesti standardina: oktoober 2014

INFOTEHNOLOOGIA
Turbemeetodid
Võrguturve
Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkudega (VPN)

Information technology
Security techniques
Network security
Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
(ISO/IEC 27033-5:2013)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27033-5:2013 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina sellekohase teate avaldamisega EVS Teataja 2014. aasta oktoobrikuu numbris.

Standardi on tõlkinud AS Cybernetica, standardi tõlke on heaks kiitnud EVS/TK 4 „Infotehnoloogia“.

Standardi tõlkimise ettepaneku on esitanud EVS/TK 4, standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

See standard on rahvusvahelise standardi ISO/IEC 27033-5:2013 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardikeskus ja sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the International Standard ISO/IEC 27033-5:2013. It has been translated by the Estonian Centre for Standardisation. It has the same status as the official versions.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.040 Märgistikud ja informatsiooni kodeerimine

SISUKORD

EESSÕNA IV
1 KÄSITLUSALA 1
2 NORMIVIITED 1
3 TERMINID JA MÄÄRATLUSED 1
4 LÜHENDID 1
5 DOKUMENDI STRUKTUUR 2
6 ÜLEVAADE 2
6.1 Sissejuhatus 2
6.2 Virtuaalsete privaatvõrkude tüübid 3
7 TURVAOHUD 4
8 TURVANÕUDED 4
8.1 Ülevaade 4
8.2 Konfidentsiaalsus 5
8.3 Terviklus 5
8.4 Autentsus 6
8.5 Volitamine 6
8.6 Käideldavus 6
8.7 Tunneli otspunktide turvalisus 6
9 TURVAMEETMED 6
9.1 Turvaaspektid 6
9.2 Virtuaalkanalid 6
10 KAVANDAMISMEETODID 7
10.1 Ülevaade 7
10.2 Regulatiivsed ja õiguslikud aspektid 7
10.3 Virtuaalsete privaatvõrkude haldusaspektid 8
10.4 Virtuaalsete privaatvõrkude arhitektuuriaspektid 8
10.5 Virtuaalsete privaatvõrkude tehnilisi küsimusi 11
11 JUHISED TOODETE VALIMISEKS 12
11.1 Kandeprotokolli valimine 12
11.2 VPN-eriseadmed 12
Kirjandus 13

EESSÕNA

ISO (Rahvusvaheline Standardimisorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmesorganisatsioonid osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendes organisatsioonides rajatud käsitlema tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvi pakkuvatel aladel. Selles töös osalevad käsikäes ISO ja IEC-ga ka rahvusvahelised, riiklikud ja valitsusvälised organisatsioonid. Infotehnoloogia valdkonnas on ISO ja IEC rajanud ühendatud tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse ISO/IEC direktiivide 2. osas esitatud reeglite kohaselt.

Ühendatud tehnilise komitee põhiülesanne on rahvusvaheliste standardite koostamine. Ühendatud tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse hääletamiseks liikmesorganisatsioonidele. Avaldamine rahvusvahelise standardina nõuab, et hääletanud liikmesorganisatsioonidest kiidaks selle heaks vähemalt 75 %.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse subjekt. ISO-t ega IEC-d ei saa pidada vastutavaks sellis(t)e patendiõigus(t)e väljaselgitamise eest.

Standardi ISO/IEC 27033 on koostanud ühendatud tehnilise komitee ISO/IEC JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Infoturbemeetodid“

See, esimene redaktsioon tühistab ja asendab standardi ISO/IEC 18028-5:2006, olles selle tehniline uustöötlus.

ISO/IEC 27033 üldpealkirjaga „Information technology – Security techniques – Network security“ („Infotehnoloogia. Turbemeetodid. Võrguturve“ koosneb järgmistest osadest:

— Part 1: Overview and concepts (Osa 1: Ülevaade ja mõisted)

— Part 2: Guidelines for the design and implementation of network security (Osa 2: Võrguturbe kavandamise ja teostamise juhised)

— Part 3: Reference networking scenarios — Threats, design techniques and control issues (Osa 3: Tüüpsed võrgustsenaariumid. Riskid, kavandamismeetodid ja reguleerimisküsimused)

— Part 4: Securing communications between networks using security gateways (Osa 4: Võrkudevahelise side turve turvalüüside abil)

— Part 5: Securing communications across networks using Virtual Private Networks (VPNs) (Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkudega (VPN))

— Part 6: Securing wireless IP network access (Osa 6: Traadita IP-võrku pääsu turve)

(Tuleb silmas pidada, et võib järgneda veel muid osi. Nende osadega kaetavate võimalike teemade hulka kuuluvad näiteks kohtvõrgud, laivõrgud, lairibavõrgud, veebimajutus, Interneti e-post, marsruuditav juurdepääs kolmandatele organisatsioonidele. Kõigi niisuguste osade põhijaotised peaksid olema riskid, kavandamismeetodid ja reguleerimisküsimused.)

1 KÄSITLUSALA

ISO/IEC 27033 see osa annab juhiseid võrguturbe tagamiseks vajalike tehniliste turvameetmete valimise, rakendamise ja seire kohta VPN-ühenduste kasutamisel võrkude kokkuühendamiseks või kaugkasutajate ühendamiseks võrkudega.

2 NORMIVIITED

Alljärgnevalt nimetatud dokumendid, mille kohta on standardis esitatud normiviited, on kas tervenisti või osaliselt vajalikud selle standardi rakendamiseks. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27002:2005. Information technology — Security techniques — Code of practice for information security management

ISO/IEC 27005:2011. Information technology — Security techniques — Information security risk management

ISO/IEC 27033-1:2009. Information technology — Security techniques — Network security — Part 1: Overview and concepts

3 TERMINID JA MÄÄRATLUSED

Dokumendi rakendamisel kasutatakse standardis ISO/IEC 7498 (kõik osad), ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 ja ISO/IEC 27033-1 esitatud termineid ja määratlusi.

4 LÜHENDID

Selle dokumendi rakendamisel kasutatakse standardis ISO/IEC 27033-1 ja alljärgnevalt esitatud lühend-termineid.

AH	autentimispäis
ESP	protokoll ESP („kapseldav turvalast“)
IKE	võtmevahetusprotokoll IKE
IPsec	turvaprotokoll IPsec
ISAKMP	autentimise ja võtmehalduse protokoll ISAKMP
L2F	kihi 2 edastusprotokoll L2F
LDP	sildijaotusprotokoll LDP
MPPE	krüpteerimisprotokoll MPPE („Microsofti kakspunktkrüpteerimine“)
MPLS	marsruutimisstandard MPLS („multiprotokoll-siltkommutatsioon“)
NAS	võrkusalvestus
OSI	OSI mudel („avatud süsteemide kokkuühendamine“)