INFOTEHNOLOOGIA
Turbemeetodid
Infotehnoloogiavõrkude turve
Osa 4: Kaugpöörduse turve
(ISO/IEC 18028-4:2005)

Information technology
Security techniques
IT network security
Part 4: Securing remote access
(ISO/IEC 18028-4:2005)

EESTI STANDARDIKESKUS

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard on 2005. aastal ilmunud rahvusvahelise standardi ISO/IEC 18028-4 “Information technology – Security techniques – IT network security – Part 4: Securing remote access” tõlge eesti keelde.

Standard EVS-ISO/IEC 18028-4 on koostatud Majandus- ja Kommunikatsiooni-ministeeriumi tellimusel. Standardi tõlkis Cybernetica AS ja tõlke kiitis heaks EVS/TK 4 “Infotehnoloogia”.

Rahvusvahelise standardi ISO/IEC 18028-4:2005 tekst on avaldatud Eesti standardina EVS-ISO/IEC 18028-4:2007, mis on kinnitatud Eesti Standardikeskuse 07.12.2007 käskkirjaga nr 202 ning jõustub selle kohta EVS Teataja 2008. aasta jaanuarikuu numbris teate avaldamisega.

This standard is the Estonian [et] version of the International standard ISO/IEC 18028-4:2005 “Information technology – Security techniques – IT network security – Part 4: Securing remote access”. It has the same status as the official version.

In case of interpretation disputes the English text applies.

SISUKORD

EESSÕNA

ISO (Rahvusvaheline Standardiorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmeskogud 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 IECga ka muud rahvusvahelised riiklikud ja mitteriiklikud organisatsioonid. Infotehnoloogia alal on ISO ja IEC loonud ühise tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse vastavalt ISO/IEC direktiivide 2. osas esitatud reeglitele.

Ühise tehnilise komitee peamine ülesanne on koostada rahvusvahelisi standardeid. Ühises tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse rahvuslikele kogudele hääletamiseks. Avaldamine rahvusvahelise standardina nõuab heakskiitu vähemalt 75 protsendilt hääletanud rahvuslikelt kogudelt.

Tuleb pöörata tähelepanu võimalusele, et mõned selle rahvusvahelise standardi elemendid võivad olla patendiõiguse objektiks. ISO ega IEC ei ole kohustatud mingeid või kõiki selliseid patendiõigusi välja selgitama.

ISO/IEC 18028-4 koostas ISO/IEC ühendatud tehniline komitee JTC 1 "Infotehnoloogia" alamkomitee SC 27, "Infoturbemeetodid".

ISO/IEC 18028, üldpealkirjaga "Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve", koosneb järgmistest osadest.

– Osa 1: Võrguturbe haldus
– Osa 2: Võrguturbe arhitektuur
– Osa 3: Võrkudevahelise side turve turvalüüside abil
– Osa 4: Kaugpöörduse turve
– Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkude abil.

Tulevase 1. osa teema on võrguturbe haldus ja tulevase 5. osa teema on võrkudevahelise side turve virtuaalsete privaatvõrkude abil.

SISSEJUHATUS

Infotehnoloogias kasvab pidevalt vajadus kasutada organisatsioonides ja organisatsioonide vahel võrke. Võrkude turvaliseks kasutamiseks tuleb täita teatavaid nõudeid.

Infoturbe vajaduse korral vajab kaug-võrkupääsu valdkond spetsiifilisi meetmeid. ISO/IEC 18028 käesolev osa annab juhiseid kaugpöördumiseks võrkudesse meili kasutamiseks, failiedastuseks või lihtsalt kaugtööks.

INFOTEHNOLOOGIA
Turbemeetodid. Infotehnoloogiavõrkude turve
Osa 4: Kaugpöörduse turve

Information technology
Security techniques. IT network security
Part 4: Securing remote access

1 KÄSITLUSALA

ISO/IEC 18028 see osa annab juhiseid kaugpöörduse turvalise kasutamise kohta; kaugpöördus on meetod arvuti kaugühendamiseks avalike võrkude abil teise arvuti või võrguga ja ta mõjutab infotehnoloogia turvalisust. Ta tutvustab seejuures mitmesuguseid kaugpöörduse tüüpe, hõlmates ka kasutatavaid protokolle, käsitleb kaugpöördusega seotud autentimisküsimusi ning aitab kaugpöördust turvaliselt korraldada. Ta on mõeldud abistama võrguadministraatoreid ja tehnilist personali, kes plaanivad sedalaadi ühenduse kasutamist või kellel see on juba kasutusel, kuid kes vajavad nõu selle kohta, kuidas seda turvaliselt korraldada ja turvaliselt käitada.

2 TERMINID, MÄÄRATLUSED JA LÜHENDID

Selle dokumendi otstarbeks kehtivad järgmised terminid, määratlused ja lühendid.

2.1
pääsupunkt
AP
süsteem, mis annab pääsu traadita võrgust maapealsesse võrku

2.2
AES
standardis FIPS 197 spetsifitseeritud sümmeetrilise krüpteerimise mehhanism, mis kasutab muutuva pikkusega võtit ja mida saab tõhusalt teostada

2.3
autentimine
kinnituse andmine olemi väidetavale identiteedile. Kasutaja autentimise korral identifitseerib kasutajat talle teadaolev (nt parool), tema valduses olev (nt pääsmik) või ta isiku tunnusomadus (biomeetrik). Tugev autentimine põhineb tugevatel mehhanismidel (nt biomeetrial) või kasutab nimetatud vahenditest vähemalt kaht (nn mitmefaktoriline autentimine).

2.4
tagasihelistus
mehhanism helistamiseks ettemääratud või pakutavasse kohta (ja aadressile) pärast kehtivate identifitseerimisparameetrite vastuvõtmist