Avaldatud eesti keeles: veebruar 2016
Jõustunud Eesti standardina: veebruar 2016

INFOTEHNOLOOGIA
Turbemeetodid
Olemi autentimiskindluse karkass

Information technology
Security techniques
Entity authentication assurance framework
(ISO/IEC 29115:2013)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 29115:2013 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina sellekohase teate avaldamisega EVS Teataja 2016. aasta veebruarikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 4 „Infotehnoloogia“, standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud Cybernetica AS, standardi on heaks kiitnud tehniline komitee EVS/TK 4.

See standard on rahvusvahelise standardi ISO/IEC 29115:2013 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 29115:2013. It was 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

SISUKORD

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 muud rahvusvahelised, riiklikud ja valitsusvälised organisatsioonid. Infotehnoloogia alal on ISO ja IEC loonud ühise tehnilise komitee ISO/IEC JTC 1.

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

Ühise tehnilise komitee peamine ülesanne on rahvusvaheliste standardite koostamine. Ühises tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse hääletamiseks rahvuslikele liikmesorganisatsioonidele. Avaldamine rahvusvahelise standardina nõuab, et hääletusel osalenud rahvuslikest liikmesorganisatsioonidest kiidaks selle heaks vähemalt 75 %.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse subjekt. ISO ja IEC ei vastuta sellis(t)e patendiõigus(t) väljaselgitamise eest.

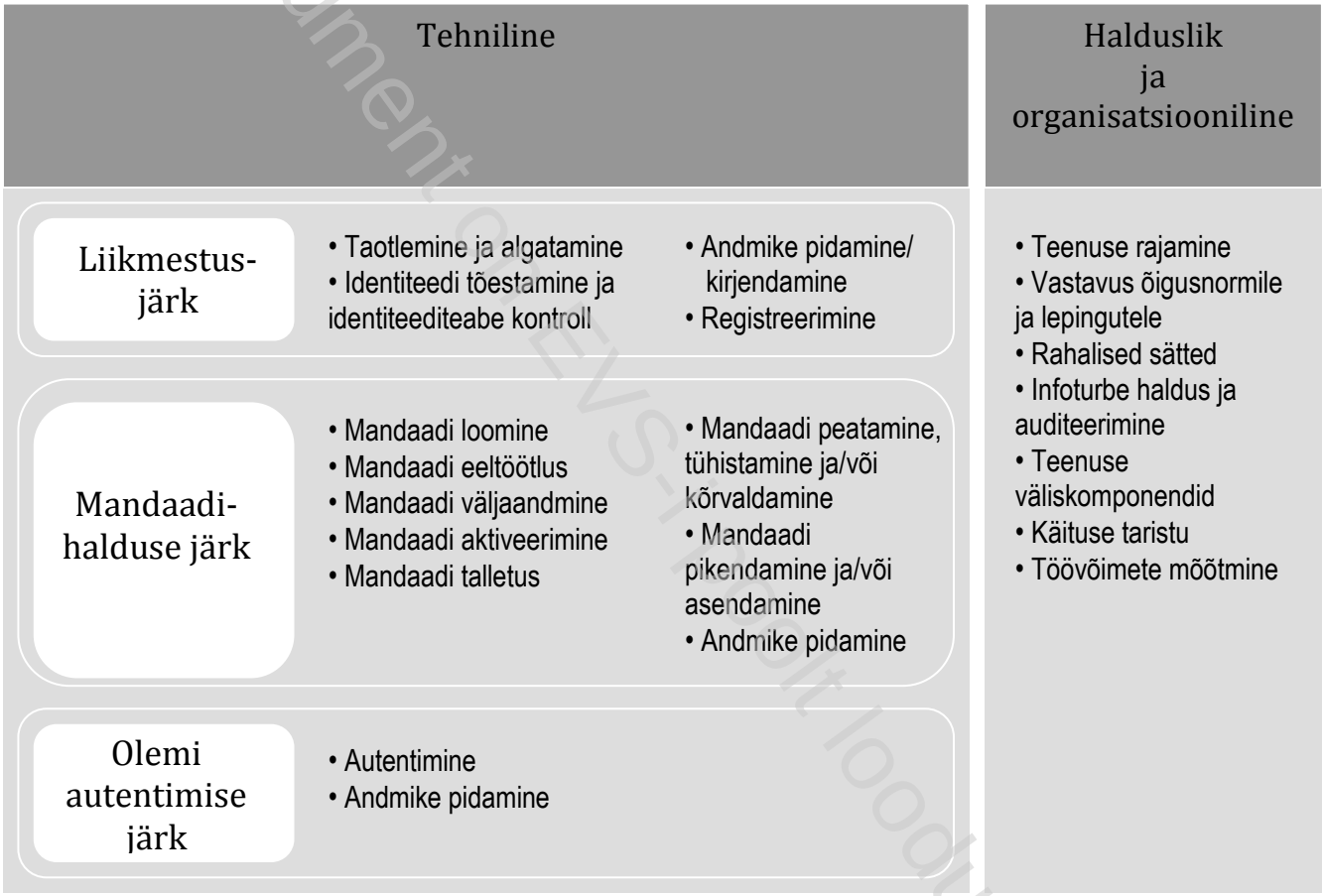
Standardi ISO/IEC 29115 koostas ühise tehnilise komitee ISO/IEC JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Infoturbemeetodid“.

Sarnane tekst on avaldatud ITU-T soovitusena X.1254 ning erineb sellest kolmes kohas: 1) 3.8: ISO/IEC määratlus sisaldab ütluslikke identiteete; 2) tabel 10-1: ISO/IEC lisab teesklusnäite, mis sisaldab olematu olemi identiteedi kasutamist; 3) 10.2.2.1: ISO/IEC nimetab kaitstud kanali näitena protokolli SSL.

SISSEJUHATUS

Paljudel info- ja sidesüsteemides või nende vahel toimuvatel elektroonilistel tehingutel on turvanõuded, mis sõltuvad mingist eeldatavast või spetsifitseeritud veendumustasemest tehingus osalevate olemite identiteetide suhtes. Niisugused nõuded võivad hõlmata varade ja ressursside kaitset volitamata juurdepääsu eest (selleks võidakse kasutada mingit pääsu reguleerimise mehhanismi) ja/või jälitatavuse kehtestust asjasse puutuvate sündmuste revisjonilogide pidamise teel, samuti arvestuse ja tasustamise otstarbeks.

See standard annab olemi autentimiskindluse karkassi. Kindlus tähendab selles standardis veendumust, mis põhineb kõikidel tehingute autentimise otstarbel olemi identiteedi kehtestuseks ja halduseks kasutatavatel protsessidel, haldustegevustel ja tehnoloogiatel.



Joonis 1 — Olemi autentimiskindluse karkassi ülevaade

Nelja spetsifitseeritud kindlustaset kasutades annab see standard juhiseid reguleerimise tehnoloogiate, protsesside ja haldustegevuste ning kindluskriteeriumide kohta, mida tuleks kasutada autentimise ohtude vähendamiseks nelja kindlustaseme teostamisel. Ta annab juhiseid ka muude autentimiskindluse skeemide vastavusse seadmiseks nende nelja spetsifitseeritud tasemega, samuti juhiseid autentimistehingu tulemite vahetuseks. Ja lõpuks annab see standard teabelisi juhiseid autentimisprotsessiga seotud isikutuvastusteabe (PII) kaitse kohta.

See standard on mõeldud kasutamiseks peamiselt mandaatoritele ja teistele, kes on nende teenustest huvitatud (nt nende teenuste sõltlastele, hindajatele ja audiitoritele). See olemi autentimiskindluse karkass (EAAF) spetsifitseerib eri mandaatorite väljaantud mandaatide vahelise ekvivalentsi tagamiseks minimaalsed tehnilised, halduslikud ja protsessinõuded neljale kindlustasemele. Ta esitab ka mõned halduslikud ja organisatsioonilised lisakaalutlused, mis mõjutavad olemi autentimiskindlust, kuid ei püstita nende kaalutluste kohta erikriteeriume. Sõltlastele ja teistele võib see standard osutuda abistavaks iga kindlustaseme pakutava mõistmisel. Peale selle võib seda kasutada mingis usalduskarkassis kindlustasemete tehniliste nõuete määratlemiseks. EAAF on muuhulgas mõeldud mitmesuguseid autentimise tehnoloogiaid kasutavateks seansipõhisteks ja dokumendikeskseteks kasutusmallideks. Võimalikud on otsese ja vahendatud usaldusega stsenaariumid nii kahepoolsetes kui ka ühenduslikes õiguslikes moodustistes.

Taotluslikult tühjaks jäetud

1 KÄSITLUSALA

See standard annab ühe karkassi, millega hallata olemi autentimiskindlust mingis konkreetses kontekstis. Sealhulgas ta

— spetsifitseerib olemi autentimiskindluse nelja taset;

— spetsifitseerib kriteeriumid ja juhised olemi autentimiskindluse iga taseme saavutamiseks nende nelja hulgast;

— annab juhiseid muude autentimiskindluse skeemide vastavusse seadmiseks nende nelja kindlustasemega;

— annab juhiseid nendel neljal kindlustasemel põhineva autentimise tulemite vahetuseks;

— annab juhiseid meetmete kohta, mis tuleks rakendada autentimise ohtude vähendamiseks.

2 NORMIVIITED

Alljärgnevalt loetletud 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.

2.1 Identsed soovitused/standardid

Puuduvad.

2.2 Paralleelsed soovitused/standardid

Puuduvad.

2.3 Lisaviited

Puuduvad.

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse alljärgnevalt esitatud termineid ja määratlusi.

3.1
ütlus (*assertion*)
olemi lausung kaasneva kehtivustõenduseta

[ITU-T X.1252]

MÄRKUS Terminite „väide“ ja „ütlus“ tähendused loetakse üldiselt mõnevõrra sarnasteks, kuid väikeste erinevustega. Selle standardi otstarbeks loetakse ütlust tugevamaks lausungiks kui väidet.

statement made by an entity without accompanying evidence of its validity

[ITU-T X.1252]

NOTE The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. For the purposes of this International Standard, an assertion is considered to be a stronger statement than a claim.