Riigi Infosüsteemi Amet

EESTI VABARIIGI INFOSÜSTEEMIS AUTENTIMISLAHENDUSTELE KEHTIVAD NÕUDED

(autentimisnormatiiv)

ver. 1.0

Tallinn 2017

Sisukord

1. Kehtivusala

Dokument kehtestab Eesti Vabariigi infosüsteemi kuuluvates rakendusinfosüsteemides kasutatavatele autentimislahendustele avaliku interneti vahendusel, avalikku teenust saavate kasutajate autentimiseks:

1. arhitektuurilised nõuded,
2. tehnilised piirangud,
3. mittefunktsionaalsed nõuded,
4. soovitused eIDAS tagatistasemete rakendamiseks,
5. eIDAS tagatistasemetele ISKE kohaldamise piirid.

Autentijad on füüsilised ja juriidilised isikud:

1. Eesti Vabariigi residendid
2. teiste Euroopa Liidu liikmesriikide residendid, kelle autentimisel on kohaldatavad Euroopa Liidu eIDAS määruses 910/2014 kehtestatud reeglid.

Käesolevas dokumendis kehtestatud nõudeid, piiranguid ja soovitusi peab arvestama kõigi selliste rakendusinfosüsteemide autentimislahenduste loomisel:

1. millele on kohaldatavad ISKE nõuded;
2. mille hanke-, loomise, kirjeldamise ja haldamise dokumentides või seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus on seda nõutud.

Käesolev dokument ei reguleeri autentimisi, millele ei ole kohaldatavad Euroopa Liidu eIDAS määruses 910/2014 kehtestatud reeglid:

1. selliste füüsiliste isikute autentimisi, kes kasutavad infosüsteemi oma ametialaste toimingute tegemiseks,
2. infosüsteem-infosüsteem (masin-masin) liidese kaudu tehtavaid autentimisi.

2. Rahvusvahelised piirangud – eIDAS tagatistasemed

Euroopa Liidu eIDAS määrus 910/2014 kehtestab autentimisele kolm tagatistaset: „kõrge“ (*high*), „märkimisväärne“ (*substantial*) ja „madal“ (*low*). Väljapoole seda gradatsiooni jäävad „määratlemata“ (*un-notified*) tasemega autentimisvahendid:

Tagatisase	**Vahendid**	**Isiku tuvastamise tase**	**eIDAS tunnustamise nõue**
Kõrge	Isik omab ja teab midagi (nt ID-kaart, mID või ELi liikmesriigi eID ja PIN-kood vms).	Isik on pädevalt, füüsiliselt tuvastatud (isiklik kontakt).	Kohustus tunnustada ELi teise liikmesriigi autentimisvahendit sama või madalama tagatistasemega autentimisprotsessis.
Märkimisväärne	Isikul on mõni enamasti turvaline identimise vahend (nt *soft sertificate* ja PIN-kood, kasutajanimi ja kordumatud paroolid või koodikalkulaator jms).	Isik on tuvastatud tasemel, mis võimaldab kinnitada, et tegemist on just selle isikuga ja mitte kellegi teisega.	Kohustus tunnustada ELi teise liikmesriigi autentimisvahendit sama või madalama tagatistasemega autentimisprotsessis.
Madal	Isikul on nõrk identimisvahend (nt kasutajanimi ja püsiparooli või korduvate paroolidega paroolikaart; kasutajanimi ja e-kirja või SMSiga saadetav parool vms).	Isik ei ole tuvastatud, kuid ta on esitanud ja kinnitanud usutavana tunduvaid andmeid; võimaldab maksimaalselt tuvastada ainult seda, et igal autentimisel on tegemist sama	Õigus tunnustada ELi teise liikmesriigi autentimisvahendit sama tagatistasemega autentimisprotsessis.

		isikuga. Isikuandmete muutmise või väärkasutamise oht ei ole märkimisväärselt tagatud.	
Määratlemata	Määratlemata (nt e-kirjaga saadetav parool, Facebook Connect, Twitter Login vms).	Määratlemata	Määratlemata

Tabel 1. Autentimise tagatistasemed

Selle gradatsiooni kolme esimesse tagatistasemesse kuuluvad ainult riigi poolt välja antud, riigi volitusel välja antud või riigi poolt tunnustatud autentimisvahendid. Kõik ülejäänud autentimisvahendid kuuluvad määratlemata tasemesse.

ELi liikmesriik, mis kasutab oma residentide autentimiseks avalikus võrgus oma rakendustes kõrgema ja/või märkimisväärse tagatistasemega autentimisvahendeid, peab lubama alates 29.09.2018 ELi teiste liikmesriikide residentidel autentida oma rakendusinfosüsteemides nende riikide sama või kõrgema tagatistaseme autentimisvahenditega vastavalt sellele, millist autentimise tagatistaset nõuab see rakendusinfosüsteem, kuhu autenditakse.

Teiste ELi liikmesriikide madala tagatistasemega autentimisvahendite tunnustamine on jäetud liikmesriikidele vabatahtlikuks. Nende tunnustamisel lubatakse neid kasutades autentida ainult sellistesse rakendusinfosüsteemidesse, mis nõuavad just seda taset.

Määratlemata tagatistasemega autentimisvahendite kasutamist määrus ei reglementeeri ja nende kasutamise otsustamine on jäetud iga liikmesriigi pädevusse.

vt ka eIDAS 910/2014 määrus:
http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32014R0910

3. Autentimise tagatistasemete autentimisvahendid

Tagatistase	Vahendid
Kõrge	Eesti Vabariigi ID-kaart Eesti Vabariigi Digi-ID (sh e-Residendi eID) Mobiil-ID ELi teiste liikmeriikide poolt hinnatud kõrge tasemega vahendid (teised sama taseme instrumendid)
Märkimisväärne	Softsert ja PIN-kood Kasutajanimi ja OTP kalkulaator/PIN-kood Kasutajanimi ja kordumatud paroolid ELi teiste liikmeriikide poolt hinnatud märkimisväärse tasemega vahendid
Madal	Kasutajanimi ja paroolikaart Kasutajanimi ja parool
Määratlemata	e-kirjaga/SMSiga saadetud parool Facebook Connect Twitter login jt riigi poolt määratlemata tasemega kolmandate osapoolte autentimislahendused

Tabel 2. Autentimise tasemete rakendamise tehnoloogiline kaart

Autentimistoimingute läbi viimisel tuleb tagada autentimiskanali turvalisus. Piisav turvalisus on tagatud, kui kasutatakse näiteks järgmisi protokolle: SAML (v.2 või hilisem), TLS kliendisertifikaat (Challenge response), OpenID Connect, OAuth2 jms.

Piisava turvalisusega autentimiseks loetakse ka eIDAS infrastruktuuril ja pangalingil baseeruvad autentimised.

Sama autentimislahendus võib autentimiseks pakkuda erineva tagatistasemega autentimismeetodeid. Kui samast autentimiskanalist võib teostada autentimist, kasutades selleks erinevaid vahendeid, ja nende erinevate vahendite kasutamine tingib erineva tagatistasemega

autentimise, siis peab autentimise järgselt kontrollima autentimiseks kasutatud vahendit ja selle vastavust soovitud tagatistasemele.

4. Tagatistasemetele kehtivad piirangud

Väliste kasutajate autentimiseks kasutatava autentimislahenduse tagatistasemena peab üldjuhul kasutama eIDAS määruses 910/2014 kirjeldatud tagatistasemeid: „kõrge“ ja „märkimisväärne“. Põhjendatud vajaduse olemasolul võib autentimisel kasutada ka "madala" ja "määratlemata" tagatistasemega autentimislahendusi.

Kuna autentimise "nõrga" ja "määratlemata" tagatistaseme puhul on isik nõrgalt (kontrollimatult) määratletud, siis tuleb nende tagatistasemetega autentimise asemel kaaluda autentimata ligipääsu rakendusinfosüsteemidele.

5. Autentimislahendusele esitatavad nõuded

Kõigi autentimislahenduste korral peab kohaldama järgmisi nõudeid:

1. Infosüsteemide kasutajate autentimine peab olema lahendatud lahus rakendusinfosüsteemist.
2. Sama vastutava töötleja kõik eraldi seisvad rakendusinfosüsteemid peavad autentimiseks kasutama sama autentimislahendust. Eraldiseisva, uue autentimislahenduse loomine ei ole keelatud, kuid selle vajadus peab olema selgelt põhjendatud.
3. Tagatistasemete "kõrge", "märkimisväärne" ja "madal" implementeerimisel autentimislahenduses peab kasutama käesoleva dokumendi jaotises 3 kirjeldatud vahendeid.
4. Autentimise järgselt peab autentimislahendus rakendusinfosüsteemile minimaalselt üle andma autentinud isiku identiteedi ja teostatud autentimise tagatistaseme („kõrge“, „märkimisväärne“, „madal“ või "määratlemata") või veateate autentimise ebaõnnestumise kohta.
5. Autentimislahenduse turvalisuse peab määrama vastavalt toetatavate rakendusinfosüsteemide käideldavusele, terviklusele ja konfidentsiaalsusele kehtestatud nõuetele. Kui rakendusele, mille kaudu pöördutakse infosüsteemi poole, esitatavad turvalisuse nõuded erinevad infosüsteemile esitatavatest turvalisuse nõuetest, siis peab autentimislahenduse turvalisuse määramisel lähtuma sellele rakendusele kehtestatud turvalisuse nõuetest. Autentimislahenduse käideldavuse, tervikluse ja konfidentsiaalsuse nõue ei saa olla madalam kui kõige kõrgemate kehtestatud nõuetega infosüsteemi või infosüsteemi poole pöördumise rakenduse oma.
6. Autentimistoimingute kohta peab pidama turvalogi, mis võimaldab tuvastada teostatud toimingu iseloomu ja selle osapooled. Kui logis sisalduvad isikuandmed, siis tuleb logi andmeid töödelda vastavalt isikuandmete kaitset reguleerivatele õigusaktidele.
7. eIDAS autentimisnormatiivil põhinevaks ELi residentide autentimiseks peab autentimislahendus kasutama eIDAS konnektorsõlme (eIDAS Connector Node).

Konnektorsõlmena võib kasutada kas RIA-s paigaldatud keskset eIDAS konnektorsõlme või lokaalselt autentimislahenduse juurde paigaldatud eIDAS konnektorsõlme.

8. Uue autentimislahenduse kasutusele võtmisel või olemasoleva autentimislahenduse muutmisel tuleb läbi viia turvaanalüüs ja testimine.

6. ISKE kohaldamine autentimise tagatistasemetele

Kui infosüsteemile või andmete edastuskanalile on kohaldatavad ISKE nõuded, siis tuleb autentimislahenduse tagatistaseme valimisel lähtuda infosüsteemile või andmete edastuskanalile kehtestatud turvaklassist.

ISKE metoodikas on eristatavad kolm turbeastet: "L" – madal, "M" – keskmine, "H" – kõrge:

		K0	K1	K2	K3
T0	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T1	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T2	S0	M	M	M	H
	S1	M	M	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T3	S0	H	H	H	H
	S1	H	H	H	H
	S2	H	H	H	H
	S3	H	H	H	H

Tabel 3. ISKE turvaklasside vastavused turbetasemetele.

Lõplik ISKE tase määratakse ISKE valdkonna spetsialistide läbi viidud analüüsi alusel.

Autentimislahenduse tagatistaseme valikul peab lähtuma järgmistest vastavustest:

1. ISKE turbeaste "kõrge" – autentimislahenduse tagatistase "kõrge";
2. ISKE turbeaste "keskmine" – autentimislahenduse tagatistase "märkimisväärne" või "kõrge";
3. ISKE turbeaste "madal" – autentimislahenduse tagatistase "madal", "märkimisväärne", "kõrge" või autentimiseta ligipääs.

Lõplik autentimislahenduse tagatistase määratakse infoturbe spetsialistide läbi viidud analüüsi alusel.

vt ka Infosüsteemide kolmeastmeline etalonturbe süsteem, rakendusjuhend:
https://iske.ria.ee/8_00

7. Täiendavad materjalid

DRAFT NIST (National Institute of Standards and Technology) Special Publication 800-63B, Digital Authentication Guideline. Authentication and Lifecycle Management (section: 5. Authenticator and Verifier Requirements) https://pages.nist.gov/800-63-3/sp800-63b.html#sec5