RIIGI INFOSÜSTEEMI AMET

Dokumendi versioon: 1.0
Kuupäev: 15.03.2017
Sihtgrupp: avaliku sektori avalike e-teenuste osutajad

eIDAS autentimistasemed

Dokumendi eesmärk:

- tuua välja lihtsustatud vormis eIDAS määrusega seatud nõuded autentimise tagatistasemetele;
- anda e-teenuste omanikele ja portaalide halduritele põhimõtted, millest lähtuda autentimise tagatistaseme nõuete seadmisel oma teenustele ligipääsuks.

eIDAS autentimistasemed ja nõuded

eIDAS määruse kohaselt on eID ehk autentimislahenduste tagatistasemed järgmised: **madal**, **märkimisväärne** ja **kõrge**.

Üks olulistest eIDAS määruse nõuetest seab kohustuse tagada kõigile ELi residentidele ligipääs avaliku sektori pakutavatele avalikele e-teenustele oma riigi residentidega võrdväärsetel tingimustel. See tähendab, et kui e-teenuse portaali sisselogimisel nõutakse oma kodanikult mõnda autentimislahendust, siis tuleb aktsepteerida ka teiste ELi liikmesriikide samaväärse tagatistasemega autentimislahendusi, millest liikmesriigid on ametlikult teavitanud. Praktikas tähendab see seda, et kui portaal aktsepteerib eri tagatistasemega lahendusi (näiteks paroolikaart, ID-kaart), siis peab aktsepteerima kõiki liikmesriikide lahendusi, mis on kõrgema tasemega kui see kõige madalam, mida portaal nõuab oma riigi residendilt. Seda eeldades, et vastava riigi lahendus on kirjeldatud liikmesriikide eID lahenduste nimistus.

Madala tasemega lahenduste aktsepteerimiseks jätab eIDAS määrus vabaduse. See aga ei tähenda, et kui näiteks Eesti residendilt nõutakse kas madala või kõrge tagatistasemega autentimist, siis saab ELi residendilt nõuda vaid kõrget taset. Sellisel juhul tuleb aktsepteerida ka ELi residentide märkimisväärse tagatistasemega autentimist.

Eesti riigi väljastatavate eID vahendite tasemest (skeemikirjeldus) teavitamisega tegeleb Politsei- ja Piirivalveamet. Teavitamisprotsess viiakse läbi 2017. aasta jooksul.

Piiriülese eID vahendi tunnustamise kohustus hakkab kehtima **18. septembril 2018**. Riigi Infosüsteemi Amet töötab välja keskset autentimisteenust (projekt „eINo“), mille vahendusel on võimalik ka autentida ELi kodanikke. Lahendus valmib 2017. a I kvartali lõpuks.

Allolev tabel toob välja nõuete erisuse lihtsustatud kujul. Detailsemad nõuded on usaldusväärsuse tasemete rakendusaktis.

Omadus	Tagatistase		
	Madal	**Märkimisväärne**	**Kõrge**
Väljastamine: Isikutuvastamine	Isikutuvastamisel on esitatud tõendeid, mille alusel võib eeldada, et isik on see, kes ta väidab end olevat. Ühtlasi on registritest võimalik näha, et väidetav identiteet eksisteerib.	Lisaks madala taseme nõuetele peab isikul olema ka riiklikult tunnustatud isikut tõendav dokument või teeb isikutuvastuse riigi poolt määratud pädevust omav asutus/amet. Dokumendi ehtsust on kontrollitud.	Isikutuvastuseks kasutatakse foto ja/või biomeetriliste andmetega riiklikult tunnustatud isikut tõendavat dokumenti. Nii dokumendi kui identiteedi ehtsust on kontrollitud. Alternatiivina viiakse läbi sama isikutuvastusprotseduur, mida rakendatakse foto ja/või biomeetriliste andmetega riiklikult tunnustatud dokumendi väljastamisel.
Lahenduse / vahendi haldus	Vahendi väljastamisel edastatakse see kasutajale viisil, mille puhul saab eeldada, et selle saab kätte vaid ettenähtud isik. Vahendit saab muuta kehtetuks tõhusal ja kiirel viisil. Samas on võetud kasutusele meetmeid, mis takistavad vahendi autoriseerimata tühistamist, kehtetuks tunnistamist ja taasaktiveerimist. Vahendi uuendamisel/asendamisel on arvestatud isiku tuvastamise andmete muutustega ning isik tuvastatakse samal viisil kui esmasel vahendi väljastamisel. Alternatiivina kasutatakse autentimist, mis vastab vähemalt samale tasemele kui väljastatav vahend.	Vahend väljastatakse viisil, mille puhul saab eeldada, et vahend antakse üle vaid ettenähtud isikule. Vahendit saab muuta kehtetuks tõhusal ja kiirel viisil. Samas on võetud kasutusele meetmeid, mis takistavad vahendi autoriseerimata tühistamist, kehtetuks tunnistamist ja taasaktiveerimist.	Vahendi aktiveerimise käigus veendutakse, et see anti üle vaid ettenähtud isikule. Vahendit saab muuta kehtetuks tõhusal ja kiirel viisil. Samas on võetud kasutusele meetmeid, mis takistavad vahendi autoriseerimata tühistamist, kehtetuks tunnistamist ja taasaktiveerimist.

Omadus	Tagatistase		
	Madal	**Märkimisväärne**	**Kõrge**
Tehniline lahendus	Vähemalt ühefaktorilise autentimisega lahendus. Vahendi väljastaja vastutab/kontrollib, et lahendust/vahendit kasutab vaid isik, kellele see väljastati.	Vähemalt kahefaktorilise autentimisega lahendus. Lahendus on loodud viisil, mille puhul saab eeldada, et seda saab kasutada ainult siis, kui vahend on kasutaja ainukontrolli all.	Vähemalt kahefaktorilise autentimisega lahendus, millel on dubleerimise ja manipuleerimise kaitse ning kaitse suure potentsiaaliga ründajate vastu. Autentimislahendus on kasutaja ainukontrolli all – kasutajal on võimalik kaitsta seda teiste isikute poolt kasutamise eest ning lahendust pole võimalik kasutada, kui vahend pole kasutaja kontrolli all.
Organisatoorsed protsessid	Kasutusel on tõhus infoturbe halduse süsteem. Krüptograafia kasutamisel on kontrollmehhanismidega tagatud, et krüptograafiamaterjalidele (võtmed jms) saab olla vaid autoriseeritud ja põhjendatud ligipääs ning selliseid materjale ei säilitata avateksti kujul. Korrapäraste siseauditite tagatakse, et teenuse kõik komponendid vastavad seatud nõuetele.	Kasutusel olev tõhus infoturbe halduse süsteem järgib riskide haldamisel üldtunnustatud standardeid ja meetodeid. Krüptograafia kasutamisel on kontrollmehhanismidega tagatud, et krüptograafiamaterjalidele (võtmed jms) saab olla vaid autoriseeritud ja põhjendatud ligipääs, ning et need materjalid on manipuleerimise vastu kaitstud. Korrapäraste sõltumatute sise- või välisauditite tagatakse, et teenuse kõik komponendid vastavad seatud nõuetele.	Kasutusel olev tõhus infoturbe halduse süsteem järgib riskide haldamisel üldtunnustatud standardeid ja meetodeid. Krüptograafia kasutamisel on kontrollmehhanismidega tagatud, et krüptograafiamaterjalidele (võtmed jms) saab olla vaid autoriseeritud ja põhjendatud ligipääs, ning et need materjalid on manipuleerimise vastu kaitstud. Korrapäraste sõltumatute välisauditite tagatakse, et teenuse kõik komponendid vastavad seatud nõuetele. Kui eID skeem on riigi institutsiooni hallata, siis auditeeritakse seda kooskõlas siseriikliku õigusregulatsiooniga.

Nõuanded autentimistaseme seadmiseks e-teenusele ligipääsu tagamisel avalikus sektoris

Allolevad soovitused on üldised ning kirjeldavad, millistest aspektidest lähtuda autentimise tagatistaseme nõudmisel. ISKE kohustuslastel tuleb siiski süsteemi ligipääsu planeerimisel/projekteerimisel lähtuda eeskätt ISKE nõuetest ja riskide maandamise meetmetest.

1. Kui portaalis puuduvad isikustatud teenused ning puudub ka kasu kasutajale, siis tuleb vältida autentimise nõudmist (autentimine pole teenuse administraatori / halduri / omaniku arvamuse rahuldamiseks).
2. Portaali sisselogimisel tuleb nõuda sellist autentimislahenduse tagatistaset, mida nõuab portaali pakutav kõige rangema nõudega teenus (selle teenuse miinimumtase).
3. Kui portaalis on eri teenuseid, mille minimaalne isikutuvastuse tagatistase on erinev, ning soovitakse tagada ligipääsu erinevate tasemetega lahendustele, siis tuleb iga teenuse ligipääsu andmisel kontrollida, kas nõutud tagatistase oli täidetud.
4. Kui portaalis nõutakse autentimist statistiliste andmete kogumiseks või muul põhjusel, mille tõttu ei töödelda isikuandmeid ega osutata teenust konkreetsele isikule, siis piisab ka madalast autentimistasemest.
5. Kui portaalis osutatakse teenust, milles küll osutatakse isikustatud teenust, aga teenusega ei kaasne isikustatud hüvesid, siis piisab märkimisväärse tagatistasemega autentimisest.
6. Kui portaalis on võimalik saada ligipääs kasutaja delikaatsetele isikuandmetele, siis tuleb nõuda kõrget autentimise tagatistaset.
7. Kui portaalis osutatava teenuse kaudu on võimalik saada isikustatud hüvesid, siis tuleb nõuda kõrget tagatistaset.
8. Kui portaalis osutatava teenuse kaudu on võimalik tekitada majanduslikku või maine kahju isikule endale või teenuse pakkujale, siis tuleb nõuda kõrget tagatistaset.
9. Digitaalallkiri kui omakäelise allkirjaga võrdväärne allkiri võib asendada kõrget autentimise tagatistaset, aga seda vaid ühekordsel toimingul.
10. Kolmanda osapoole autentimisteenuse kasutamise puhul kontrolli alati taset enne, kui portaali pakutav teenus avatakse isikule (usalda, aga kontrolli).

Rakendamine

Avaliku sektori osutatava elektroonse avaliku teenuse ligipääsuks:

- peavad teenuse/portaali haldurid hindama ohte ja riske, mis võivad kaasneda erinevate tagatistasemetega autentimise rakendamisest;
- peavad teenuse/portaali haldurid määrama oma teenustele ligipääsupoliitika, millega seatakse autentimise tagatistasemete tingimused teenusele ligipääsu saamiseks. ISKE kohustuslastel tuleb ligipääsu tingimuste seadmisel arvestada ka teenusele seatud ISKE taseme ja riskide maandamise meetmetega.
- Teenuste ligipääsupoliitikat tuleb kohaldada kõikidele kasutajatele – nii Eesti kui ka ELi residentidele.
- Tehnilise lahenduse, arhitektuuri koostamisel tuleb lähtuda autentimisnormatiivist (valmib 2017. aasta I kvartalis) ning, kus kohaldatav, ISKEst.
- Piiriülese autentimise võimekuseks tuleb teenuses/portaalis võtta kasutusele projektiga „eINo“ loodav SSO lahendus (valmib 2017. a I kvartalis).

- Piiriülese autentimise kohustus rakendub 2018. a 18. septembrist kõigile avaliku sektori avalikele e-teenustele.