FAILI NUMBER: 2022-0941
KLASSIFIKATSIOONI ID: 3.2.3

Usaldusraamistik

Rootsi e-identimiseks

Versioon 2022-10-04

1. Taust ja eesmärk

Rootsi e-identimise usaldusraamistiku eesmärk on kehtestada ühtsed nõuded Rootsi digivalitsuse ameti (DIGG) poolt läbi vaadatud ja heaks kiidetud elektrooniliste isikutunnistuste väljastajatele. Nõuded on jagatud erinevateks kaitsetasemeteks – usaldusväärsuse tasemeteks –, mis vastavad väljastaja erinevale tehnilise ja tegevusturvalisuse tasemele ning erinevale kontrollitasemele selle kohta, et isik, kellele e-identimise dokument väljastatakse, on tõepoolest see, kes ta väidab end olevat.

Selle usaldusraamistiku nõudeid kohaldatakse 2.–4. usaldusväärsuse taseme suhtes, kusjuures 4. tase vastab kõrgeimale kaitsetasemele.

Vastavust tõlgendatakse järgmiselt:

(a) kui usaldusväärsuse taset ei ole kindlaks määratud, peab nõue olema täidetud kõigil tasanditel; ja

(b) kui usaldusväärsuse tase on kindlaks määratud, tagatakse vastavus vähemalt asjakohasel tasemel.

Asjakohasest tasemest madalamale tasemele seatud nõudeid ei võeta arvesse.

2. Korraldus ja juhtimine

Üldised tegevusnõuded

K2.1 Rootsi eID-de väljastajad, kes ei ole avalik-õiguslikud asutused, peavad tegutsema registreeritud juriidiliste isikutena ning sõlmima ja säilitama äritegevuseks vajaliku kindlustuse.

K2.2 Rootsi eID-de väljastajatel peab olema asutatud ettevõte, nad peavad olema täielikult toimivad kõigis käesolevas dokumendis nimetatud osades ning nad peavad olema hästi kursis neile kui Rootsi eID-de väljastajatele kehtivate õiguslike nõuetega.

K2.3 Rootsi eID-de väljastajad peavad olema suutelised kandma kahjude eest vastutamise riski ja neil peavad olema piisavad rahalised vahendid oma tegevuse läbiviimiseks vähemalt ühe aasta jooksul.

Infoturve

K2.4 Rootsi eID-de väljastajad peavad olema loonud usaldusraamistikust mõjutatud tegevusvaldkondade jaoks infoturbe halduse süsteemi (ISMS), mis põhineb vajaduse korral standardil ISO/IEC 27001 või samaväärsetel infoturbealase töö juhtimise ja kontrollimise põhimõtetel, sealhulgas järgmisel.

(a) Kõik ohutuse seisukohast olulised haldus- ja tehnilised protsessid peavad olema dokumenteeritud ja põhinema ametlikul alusel, kus rollid, kohustused ja volitused on selgelt määratletud.

(b) Rootsi eID-de väljastajad tagavad, et neil on igal ajal piisavalt inimressursse oma kohustuste täitmiseks.

(c) Rootsi eID-de väljastajad kehtestavad riskijuhtimisprotsessi, millega asjakohasel viisil, pidevalt või vähemalt iga 12 kuu järel analüüsitakse ettevõttes esinevaid ohte ja nõrku kohti ning mis turvameetmete kehtestamise kaudu tasakaalustab riskid vastuvõetava tasemeni.

(d) Rootsi eID-de väljastajad kehtestavad intsidentide haldamise protsessi, mis süstemaatiliselt tagab teenuse kvaliteedi, edasise teatamise vormid ning asjakohaste reageerivate ja ennetavate meetmete võtmise sellistest sündmustest tuleneva kahju leevendamiseks või ennetamiseks.

(e) Rootsi eID-de väljastajad koostavad ja testivad korrapäraselt talitluspidevuse kava, mis vastab ettevõtte ligipääsetavusnõuetele, võimaldades kriisi või tõsiste intsidentide korral taastada kriitiliste protsesside toimivuse.

(f) Rootsi eID-de väljastajad hindavad korrapäraselt infoturbealast tööd ja võtavad juhtimissüsteemis kasutusele parandusmeetmeid.

K2.5 Juhtimissüsteemi ulatus ja küpsus.

Tase 4 Infoturbe haldussüsteem peab vastama standardile SS-ISO/IEC 27001:2017 või samaväärsele hilisemale või rahvusvahelisele versioonile ning selle kohaldamisala peab hõlmama kõiki Rootsi eID-de väljastajatele kehtestatud nõudeid.

Alltöövõtu tingimused

K2.6 Rootsi eID-de väljastaja, kes on ühe või mitme turvalisuse seisukohast olulise protsessi täitmise edasi andnud teisele poolele, määrab lepinguga kindlaks, milliste kriitiliste protsesside eest alltöövõtja vastutab ja milliseid nõudeid nende suhtes kohaldatakse, ning selgitab lepingulist suhet väljastaja deklaratsioonis.

Dokumentide jälgitavus, kustutamine ja säilitamine

K2.7 Rootsi eID-de väljastajad peavad säilitama:

(a) taotlusdokumendid ning e-identimise väljastamise, vastuvõtmise või blokeerimisega seotud dokumendid;

(b) lepingud, poliitikadokumendid ja väljastaja deklaratsioonid; ja

(c) töötlemisajaloo ja muud dokumendid, mis on vajalikud Rootsi eID-de väljastajatele kehtestatud nõuete täitmise tõendamiseks ja mis võimaldavad võtta järelmeetmeid, mis näitavad, et turvalisuse seisukohast olulised protsessid ja kontrollid on kehtestatud ja tõhusad.

K2.8 Säilitamisaeg ei tohi olla lühem kui viis aastat ja materjali peab olema võimalik esitada loetavalt kogu selle aja jooksul, välja arvatud juhul, kui kustutamise nõue on vajalik eraelu puutumatuse seisukohast ja seda toetab seadus või muu määrus.

Läbivaatamine ja järelmeetmed

K2.9 Rootsi eID-de väljastajad peavad looma siseauditi funktsiooni, mis vaatab väljastamistegevuse korrapäraselt läbi. Siseaudiitor on oma ülesannete täitmisel sõltumatu viisil, mis tagab objektiivse ja erapooletu kontrolli, ning tal on oma ülesannete täitmiseks vajalik pädevus ja kogemused. Siseaudiitor kavandab iseseisvalt auditi läbiviimise ja dokumenteerib selle kolmeaastast perioodi hõlmavas auditikavas. Auditielemendid valitakse riski- ja olulisuse analüüsi alusel ning nende aluseks on tegevuste kirjeldused, mille väljastaja on esitanud Digivalitsuse Ametile.

Tasemed 3 ja 4. Siseaudit viiakse läbi tunnustatud auditeerimisstandardite alusel.

3. Füüsiline, administratiivne ja isikukeskne julgeolek

K3.1 Toimingu kesksed osad peavad olema füüsiliselt kaitstud keskkonnasündmuste, loata juurdepääsu või muudest välistest häiringutest tulenevate kahjustuste eest. Juurdepääsukontrolli kohaldatakse nii, et juurdepääs tundlikele aladele on piiratud volitatud töötajatega, teabekandjaid säilitatakse ja kõrvaldatakse turvaliselt ning juurdepääsu kõnealustele kaitstud aladele jälgitakse pidevalt.

K3.2 Enne kui isik asub täitma mõnda K2.4(a) kohaselt kindlaks määratud rolli, mis on turvalisuse seisukohast eriti oluline, peab Rootsi eID-de väljastaja olema teinud taustakontrolli tagamaks, et isikut saab pidada usaldusväärseks ning et isikul on kvalifikatsioon ja väljaõpe, mis on vajalik rollist tulenevate ülesannete ohutuks ja turvaliseks täitmiseks.

K3.3 Väljastajad kehtestavad korra, millega tagatakse, et ainult eriloaga töötajatel on juurdepääs K2.7 kohaselt kogutud ja säilitatud andmetele.

K3.4 **Tasemed 3 ja 4.** Väljastajad tagavad kogu väljastamisprotsessi vältel, et ülesannete lahusust kohaldatakse nii, et ükski isik ei saa teise isiku nimel eID-d.

4. Tehniline turvalisus

K4.1 Rootsi eID-de väljastajad tagavad, et kehtestatud tehnilised kontrollid on piisavad, et saavutada äritegevuse laadi, ulatust ja muid asjaolusid silmas pidades vajalikuks peetav kaitsetase, ning et need kontrollid toimivad ja on tõhusad.

K4.2 Tundlike andmete edastamisel kasutatavaid elektroonilisi sidevahendeid kaitstakse pealtkuulamise, manipuleerimise ja taasesitamise eest.

K4.3 Tundlikku krüptograafilist võtmematerjali, mida kasutatakse eID-de väljaandmiseks, omanike tuvastamiseks ja identiteedisertifikaatide väljaandmiseks, kaitstakse nii, et:

(a) juurdepääs on loogiliselt ja füüsiliselt piiratud rangelt vajalike rollide ja rakendustega;

(b) võtmematerjali ei salvestata kunagi püsivale andmekandjale lihttekstina;

(c) võtmematerjal on kaitstud krüptograafilise riistvaramooduliga, millel on aktiivsed turbemehhanismid, mis takistavad nii füüsilisi kui ka loogilisi katseid võtmematerjali ohtu seada;

(d) võtmematerjali kaitse turvamehhanismid on läbipaistvad ning põhinevad tunnustatud ja väljakujunenud standarditel; ja

(e) **Tasemed 3 ja 4:** võtmematerjali kaitse aktiveerimisandmeid hallatakse mitme isiku kontrolli kaudu.

K4.4 Väljastajatel peavad olema kasutusel dokumenteeritud menetlused, et tagada asjakohases IT-keskkonnas nõutava kaitsetaseme säilitamine aja jooksul ja seoses muudatustega, sealhulgas korrapärased haavatavuse hindamised, ning asjakohane valmisolek reageerida muutuvatele riskitasemetele ja aset leidvatele intsidentidele.

5. Taotlemine, identifitseerimine ja registreerimine

Teave tingimuste kohta

K5.1 Rootsi eID-de väljastajad peavad andma teavet lepingute, tingimuste, seonduva teabe ja teenuse kasutamise piirangute kohta ühendatud kasutajatele, e-teenuste osutajatele ja teistele, kes võivad väljastaja teenusest sõltuda.

K5.2 Rootsi eID-de väljastaja viitab selgelt tingimustele ja kavandab menetlused nii, et tingimused esitatakse taotlejale väljastamisprotsessi käigus.

K5.3 Rootsi eID-de väljastajad esitavad väljastaja deklaratsiooni, mis sisaldab järgmist:

(a) väljastaja identiteet ja kontaktandmed;

(b) väljastaja pakutavate teenuste ja lahenduste lühikirjeldus, sealhulgas kohaldatavad rakendamis-, väljastamis- ja blokeerimismeetodid;

(c) osutatava teenusega seotud tingimused, sealhulgas kasutaja kohustus kaitsta oma elektroonilist ID-d, väljastaja kohustused ja vastutus, antud garantiid ja lubatud kättesaadavus;

(d) teave isikuandmete töötlemise ja selle teostamise viisi kohta; ja

(e) osutatava teenuse tingimuste või muude tingimuste muutmise kord, sealhulgas meetmed, mida tuleb võtta teenuse kontrollitud lõpetamiseks.

K5.4 **Tasemed 3 ja 4.** Rootsi eID-de väljastajad esitavad Digivalitsuse Ameti (DIGG) või muu väljastaja osutatavatele teenustele tugineva lepinguosalise taotluse korral teabe selle kohta, kuidas ettevõtet omatakse ja juhitakse.

K5.5 Rootsi eID-de väljastaja, kes lõpetab oma tegevuse, peab järgima eelnevalt kehtestatud plaani teenuse osutamise lõpetamiseks. Kava hõlmab kõigi teenuse kasutajate ja DIGGi teavitamist. Väljastaja peab säilitama arhiveeritud materjali ka pärast lõpetamist kättesaadavana vastavalt K2.7 ja K2.8 nõuetele.

Rakendamine

K5.6 Rootsi eID võib väljastada üksnes taotleja taotlusel või muu samaväärse aktsepteerimismenetluse kaudu ning alles pärast seda, kui taotlejat on teavitatud eID väljastamise tingimustest ja talle määratavast vastutusest.

Samas võib sellise eID väljaandmine, mis asendab või täiendab sama väljastaja poolt varem välja antud kehtivat või hiljuti blokeeritud eID-dokumenti, toimuda ilma eelneva taotlusmenetluseta.

K5.7 Rootsi eID taotlus seotakse isikukoodi või koordineerimisnumbriga, samuti teabega, mis on väljastajale muul moel vajalik sellise eID väljastamiseks.

Taotleja isiku kindlakstegemine

K5.8 Rootsi eID-de väljastajad peavad kontrollima, kas taotlusega seotud teave on täielik ja vastab ametlikus registris registreeritud teabele.

K5.9 Kui ametlikus registris kontrollitav teave on märgitud konfidentsiaalseks („kaitstud identiteet"), võib vajalikud kontrollid teha muude samaväärsete vahendite abil.

K5.10 Taotleja isikusamasuse tuvastamine näost näkku kohtumise ajal:

Rootsi eID-de väljastajad võivad kontrollida taotleja isikusamasust näost näkku tehtava kontrollkäigu ajal samamoodi nagu standardse isikut tõendava dokumendi väljastamisel.

K5.11 Taotleja kaugidentimine olemasolevas suhtes:

Tase 3 Rootsi eID-de väljastajad, kes on taotleja juba tuvastanud seoses majanduslikult või õiguslikult oluliste tehingutega ja kelle puhul saab taotlejat eemalt tuvastada muude usaldusväärsete vahendite abil, mis on samaväärsed Rootsi eID kvaliteedimärgi 3. taseme nõuetega, võivad kasutada seda meetodit taotleja isiku kindlakstegemiseks.

Tase 4 Ei kohaldata.

K5.12 Identifitseerimine Rootsi eID kaudu:

Rootsi eID-de väljastaja võib taotleja eemalt tuvastada olemasoleva kehtiva Rootsi eID abil, mille usaldusväärsuse tase on vähemalt sama kui väljastataval eID-l, kui ta saab ilma lepinguliste takistusteta kasutada sellist tuvastamist uue eID väljastamise alusena.

Tase 4 Uue eID kehtivusaeg ei tohi ületada olemasoleva eID kehtivusaega.

K5.13 Taotleja kaugidentimine:

Tase 2 Rootsi eID-de väljastajad võivad kasutada kehtiva standardse isikut tõendava dokumendi usaldusväärseid salvestisi ja taotleja näokujutist taotleja isiku kaugtuvastamise alusena, kui võrdlus ei tekita kahtlusi taotleja tegelikus isikusamasuses.

Tase 3 Rootsi eID-de väljastajad võivad elektrooniliselt säilitatavaid biomeetrilisi andmeid sisaldava kehtiva standardse isikut tõendava dokumendi turvalise lugemise teel teha nende andmete alusel kaugelt kindlaks taotleja isiku, kui tuvastatava isiku vastavaid biomeetrilisi andmeid on võimalik koguda piisavalt turvalisel viisil, nii et võrdlus on sama usaldusväärne kui näost näkku külastuse puhul, ja kui võrdlus ei tekita kahtlust taotleja tegelikus isikusamasuses.

Tase 4 Ei kohaldata.

Registreerimine

K5.14 Võttes arvesse kohaldatavaid isikuandmete kaitse norme, peavad Rootsi eID-de väljastajad pidama ühendatud kasutajate ja määratud elektrooniliste identifitseerimisdokumentide registrit ning tagama selle ajakohasuse.

6. eID väljastamine ja blokeerimine

Tehniliste vahendite projekteerimine

K6.1 Tehnilised vahendid:

Tasemed 2 ja 3. Rootsi eID kvaliteedimärgiga eID tehnilised vahendid kavandatakse kahe teguri põhimõttel, kusjuures üks osa koosneb elektrooniliselt salvestatud teabest, mida kasutaja hoiab, ja teine osa koosneb sellest, mida kasutaja kasutab eID aktiveerimiseks.

Tase 4 Rootsi eID kvaliteedimärgiga eID tehnilised vahendid projekteeritakse vastavalt kahe teguri põhimõttele, mille kohaselt üks osa koosneb isiklikust turvamoodulist, mis peab kasutajal olema, ja teine osa koosneb sellest, mida kasutaja kasutab turvamooduli aktiveerimiseks.

K6.2 Aktiveerimismehhanism ja isikustatud kood peavad olema kavandatud nii, et on ebatõenäoline, et kolmandad isikud rikuvad kaitset isegi mehaaniliste vahendite abil.

Tasemed 3 ja 4. Kaitse hõlmab mehhanisme elektroonilise identifitseerimisdokumendi kopeerimise ja manipuleerimise vältimiseks.

K6.3 Rootsi eID kvaliteedimärgiga eID kasutajad saavad omal algatusel eID kehtivusaja jooksul tasuta ja ilma märkimisväärsete ebamugavusteta vahetada või taotleda uut isikukoodi ning juhendamise või automaatse tootmise kaudu aidata täita K6.2 nõudeid.

Kui eID on kujundatud nii, et isikustatud koodi ei ole võimalik vahetada, peaks kasutajal selle asemel olema samadel tingimustel võimalik saada kiiresti uus eID uue isikustatud koodiga, mis blokeerimise teel asendab eelmist.

K6.4 Rootsi eID-de väljastajad peavad tagama, et omanike elektrooniliseks identifitseerimiseks registreeritud andmed esindavad taotlejat kordumatult ja need omistatakse kõnealusele isikule eID dokumendi väljastamisel.

K6.5 Väljastatud eID-de kehtivusaega piiratakse, võttes arvesse eID dokumendi turvaelemente ja väärkasutamise ohtu. eID maksimaalne kehtivusaeg on viis aastat.

eID dokumendi väljastamine

K6.6 Kaugteenuse säte:

Tase 2 Rootsi eID-de väljastaja esitab e-ID dokumendi viisil, mis kinnitab ametlikus registris hoitavaid kontaktandmeid või sellist teavet, mis on registreeritud seoses elektroonilise menetlusega vastavalt K5.13 2. tasemele.

Tase 3 Rootsi eID-de väljastaja, kes väljastab eID elektroonilise menetluse kaudu, mis vastab K5.11 3. tasemele, K5.12 3. tasemele või K5.13 3. tasemele, tagab uue väljastamise korral eraldi ja sõltumatult turvalisuse sättest, et kasutajat teavitatakse sellest, et selline e-ID dokument on üle antud, või tagab muude meetmetega samaväärse kontrolli selle üle, et isikut teavitatakse identiteedivarguse ohust seoses väljastamisega.

Tase 4 Rootsi eID-de väljastaja, kes annab eID välja K5.12 4. tasemele vastava elektroonilise menetluse kaudu, peab uue väljastamise korral eraldi ja turvalisuse seisukohast sättest sõltumatult tagama, et kasutajat teavitatakse sellise eID dokumendi üleandmisest.

K6.7 Näost näkku visiidi ajal pakutavad teenused.

Rootsi eID-de väljastaja esitab näost näkku külastuse ajal ja pärast isikusamasuse kontrollimist vastavalt K5.10 nõuetele e-identimise dokumendi allkirjastatud kviitungi vastu ning lisaks turvalisuse tagamiseks eID aktiveerimiseks vajamineva osa eID dokumendist eraldi ja sõltumatult, tuginedes ametlikus registris hoitavatele kontaktandmetele või muule samaväärse usaldusväärsusega teabele.

Blokeerimisteenus

K6.8 Rootsi eID-de väljastajad peavad pakkuma kasutajale hea juurdepääsuga blokeerimisteenust, et tal oleks võimalik oma eID blokeerida.

K6.9 Rootsi eID-de väljastajad töötlevad ja täidavad blokeerimistaotlusi kiiresti ja turvaliselt ning võtavad meetmeid, et vältida blokeerimisteenuse süstemaatilist väärkasutamist või muid tahtlikke tegevusi, mis toovad kaasa e-identimise dokumentide laialdase blokeerimise, tagades, et kasutajate eID-d on vajaduse korral kättesaadavad

7. Omanike elektrooniliste identiteetide kontrollimine

K7.1 Rootsi eID-de väljastajad tagavad, et omaniku isikusamasuse kontrollimisel tehakse usaldusväärsed kontrollid eID dokumendi autentsuse ja kehtivuse üle.

K7.2 Rootsi eID-de väljastajad tagavad, et omanike elektroonilise identiteedi kontrollimisel on rakendatud tehnilisi turvameetmeid, nii et on ebatõenäoline, et kolmandad isikud võivad protsessi äraarvamise, pealtkuulamise, taasesitamise või manipuleerimise kaudu rikkuda kaitsemehhanisme.

8. Isikutunnistuste väljaandmine

Rootsi eID-de väljastajad, kes osutavad isikusamasuse sertifikaatide väljastamise teenust sellele tuginevatele e-teenustele, peavad samuti järgima käesoleva jao sätteid.

K8.1 Rootsi eID-de väljastajad tagavad, et identiteedisertifikaatide väljastamise teenusele on hea juurdepääs ja et identiteedisertifikaatide väljastamisele eelneb usaldusväärne tuvastamine vastavalt 7. jao sätetele.

Tase 4 Sertifikaadid sisaldavad viidet krüptograafilisele võtmematerjalile, mille väljastaja on kinnitanud olevat omaniku ainuomandis.

K8.2 Esitatud isikut tõendavad dokumendid kehtivad ainult nii kaua, kui on vajalik kasutaja juurdepääsu võimaldamiseks taotletud e-teenusele, ning peavad olema kaitstud nii, et teavet saab lugeda ainult ettenähtud saaja ja et sertifikaatide saajad saavad kontrollida sertifikaatide autentsust.

K8.3 Võttes arvesse sertifitseerimisteenuse väärkasutamise ohtu, piiravad Rootsi eID-de väljastajad ajavahemikku, mille jooksul võib konkreetsele omanikule väljastada mitu järjestikust identiteedisertifikaati enne omaniku uuesti tuvastamist vastavalt jao 7 sätetele.