

Koostaja: Riigi Infosüsteemi Amet

VALGE RAAMAT

2024

Identiteedihaldus ja elektrooniline identiteet

SISUKORD

Lühikokkuvõte _____	1
Sissejuhatus _____	3
Valdkonna hetkeolukord ja tulevikutrendid _____	6
eID ökosüsteem ning selle tugevused, nõrkused, väljakutsed ja võimalused _____	19
Strateegilised suunad _____	25
Rakendamine _____	35
Kasutatud allikad _____	36
Lisa 1 - Sõnaraamat _____	39

Lühikokkuvõte

Käesolev Valge Raamat (VR) kirjeldab elektroonilise identiteedi (eID) valdkonna trende lähema viie kuni kümne aasta jooksul ning annab strateegilised suunad vähemalt järgneva viieks aastaks. VR on kokku pandud koostöös avaliku sektori ning erasektori sidusrühmadega ning arvestades valdkonna ekspertide ning arvamusiidrite prognoosi eID valdkonda mõjutavate tulevikutrendide osas. Tegemist on dokumendiga, mis viib ellu digiühiskonna arengukavast tulenevaid strateegilisi eesmärke eID valdkonnas. eID Valge Raamatu keskmeks on klientidele ja kasutajatele maailma tasemel tunnustatud, usaldusväärse ja toimekindla eID pakkumine, mida on mugav ja turvaline kasutada.

Järgnevate aastate jooksul tuleb eID valdkonnas kindlasti arvestada, et e-teenuste pakkujad on eelkõige suunatud mobiilsetele platvormidele mõeldud teenuste arendamisele. Kasutajad omakorda eelistavad mugavaid, kiireid ja turvalisi lahendusi. Kindlasti on suurenemas vajadus piiriüleste teenuste tarbimise ning elektrooniliselt allkirjastatud dokumentide piiriülese edastamise järele. Euroopa Liidu tasandil on oluliseks muudatuseks Euroopa digiidentiteedikurku kasutuselevõtt suurendamiseks riikidevahelist koosvõimelisust. See omakorda toob kaasa mitmeid õiguslikke ning organisatoorseid põhimõttelisi muudatusi kogu valdkonnas. Vaatamata uute lahenduste tulekule on oluline arvestada ka asjaoluga, et senised kiipkaartidel põhinevad eID vahendid ei kao tulenevalt sõlmitud lepingutest ning välja antud eID-de kehtivuse ajast veel niipea.

Lisaks üldistele küberturvalisuse väljakutsetele tuleb eID puhul jälgida ka arenguid kvantarvutusvõimsuse valdkonnas. Oluliseks on tagada eID ökosüsteemi jätkuv turvalisus ja toimekindlus ning võimekus reageerida operatiivselt kriitilistes olukordades. Eeltoodust tulenevalt on eID valdkonna strateegilised valikud suunatud eelkõige Eesti siseriiklikule eID ökosüsteemile ning selle kooskõlale Euroopa Liidus toimivate arengutega. Peamised strateegilised märksõnad eID valdkonnas on: **turvalisus, töökindlus, privaatsuse kaitse, pidev areng, koosvõimelisus, innovatsioon ja kasutajale suunatus**. Strateegilised suunad on jagatud üldisteks põhimõteteks, millest valdkonnas lähtutakse ning valdkondlikeks suundadeks, mis hõlmavad isikutuvastuse, identiteedikandjad, eID ökosüsteemi teenused ning kompetentsikeskuse. Valdcondlike suundade puhul on omakorda eristatud avalik sektor, erasektor ning eraisikud, kes esindavad erinevaid kasutajagruppe ja vajadusi. Iga valdkonna strateegilised suunad on jagatud kolme kategooriasse vastavalt nende kriitilisuse astmele. Siinkohal on alljärgnevalt välja toodud eelnimetatud suundade kõige prioriteetsemad teemad.

Isikutuvastus

- Arendame välja kõrgele tagatistasemele vastava lahenduse isikute kaugtuvastuseks.
- Tagame turvalise tarkvara arvutis ja nutiseadmes autentimiseks ja digiallkirjastamiseks ning ID-1 formaadis dokumentide kontaktivaba kasutamise.
- Lepime kokku ühised suunad ja valdkonnad (huvid, mida Eesti soovib kaitsta), millesse panustame erilise tähelepanuga EL-i ja rahvusvahelisel tasandil.

IDENTITEEDIHALDUS JA eID

Identiteedi kandjad

- Arendame välja Euroopa digiidentiteedikukru lahenduse, mis on koosvõimeline EL raamistikuga.
- Üldjuhul lähtume põhimõttest, et riik ei telli samale tehnoloogiale dubleeritud eID lahendusi. Tagame erinevate tehnoloogiate laialdasema toe (üks tehnoloogia - üks eID).
- Võimaldame eID kandja turvakoodide edastamist elektrooniliselt, kui inimene on autentunud end teise kõrgel tasemel eID vahendiga.¹
- Võimaldame eID kandja ja/või selle sertifikaatide kehtetuks tunnistamist elektrooniliselt, kui inimene on tõsikindlalt tuvastatud.
- Võimaldame eID kandja väljastamist ilma isikliku ilmumiseta dokumendi väljaandja juurde või Eesti välisesindusse.
- Arendame välja riikliku äripõhise eID vahendi e-residentidele.
- Looime võimaluse avaliku sektori jaoks uute e-teenuste pakkumiseks läbi Euroopa digiidentiteedikukru lahenduse.
- Looime võimaluse erasektori jaoks uute e-teenuste pakkumiseks läbi Euroopa digiidentiteedikukru lahenduse.

eID ökosüsteemi teenused

- Tagame EL-i sisese veebipõhise autentimisteenuse toimimise.
- Säilitame *off-line* digitaalsete allkirjade valideerimise võimekuse.
- Võimaldame uute usaldusteenuse pakujate turule sisenemist.
- Analüüsime kahe sertifitseerimis- ja usaldusteenuse pakkuja samaaegse tegutsemise mõjusid eID ökosüsteemile.

Kompetentsikeskus

- Hindame pidevalt tehnoloogiarendide mõju olemasolevale eID ökosüsteemile.
- Identiteedihalduse ning isikut tõendavate dokumentide valdkonna hangetel oleme avatud uutele lahendustele ja tehnoloogiatele, hoiame end kursis ning kutsume ettevõtteid ja teadusasutusi neid lahendusi riigile presenteerima.
- Tutvustame eID valdkonna lahendusi ja jagame parimaid praktikaid nii siseriiklikult kui rahvusvaheliselt.

VR on elav dokument, mis ajas täieneb vastavalt muutunud keskkonnale ja asjaoludele ning seda vaadatakse üle koostöös sidusrühmadega vähemalt kord aastas. Täpsemate tegevuste ning vastutajate kokkuleppimiseks koostatakse 2024. aastal VR-i juurde ka rakenduskava.

¹ Tõsikindlalt on inimene tuvastatud kasutades teist kõrge tagatistasemega eID vahendit, nt mobiil-ID-d.

Sissejuhatus

Juurdepäas e-teenustele ning piiriüleste e-teenuste kasutamine on aasta-aastalt muutunud üha olulisemaks. Sellest tulenevalt on identiteedihaldus, elektrooniline isikutuvastamine ja sellega seotud teenused hästi toimiva e-riigi alustaladeks. Peale 2017. aasta ID-kaardi kriisi oli selge, et antud valdkond on kriitilise tähtsusega ning eeldab eraldiseisva strateegia olemasolu.² 2018. aasta lõpuks valmiski esimene valdkondlik Valge Raamat⁴, mis sisaldas elektroonilise identiteedi (edaspidi ka eID) ja selle kandja laiapõhjalisi tulevikustsenaariume ja strateegilisi valikuid järgneva viieks aastaks. Tänapäevaks on kätte jõudnud aeg valdkonna olulised strateegilised suunad uuesti üle vaadata ning kaasajastada, arvestades kasutajate ootuseid, tehnoloogia valdkonna trende ning turvalisuse vajadusi.

Eesti olemasolevat eID ökosüsteemi kirjeldab Riigi Infosüsteemi Ameti (RIA) poolt tellitud eraldi analüüsidokument. Käesoleva Valge Raamatu eesmärgiks on pakkuda vaadet identiteedihalduse ja eID valdkonna trendidest ning teha ettepanekuid valdkonna strateegiliste suundade osas vähemalt järgneva viieks aastaks. Lihtsamalt öeldes peegeldab eID Valge Raamat kogukonna kokkulepet või eriarvamusi, valdkonna trende, ohtusid, valikusuundi ja teemasid, mis vajavad tähelepanu või toovad kaasa olulise muutuse järgmise viie aasta jooksul isikutuvastuse, identiteedi kandjate, eID ökosüsteemi teenuste ning valdkondliku kompetentsikeskuse valdkonnas. Samas ei paku käesolev strateegiline dokument lahendusi kõigile identiteedihalduse ja eID valdkonnaga puutumuses olevatele väljakutsetele nagu näiteks kvantarvutusvõimsus, vaid peegeldab avaliku sektori ja erasektori huvitatud poolte ühtset valdkondlikku nägemust, mida saab kasutada sisendina teiste riiklike arengukavade koostamisel nagu Siseturvalisuse arengukava, Eesti digiühiskonna arengukava jne. Tegemist on paindliku ning ajas muutuva dokumendiga, mille kaasajastamine ja ajakohasena hoidmine on agiilne protsess. Kuna tehnoloogia valdkond on üha kiiremas muutumises ja arenemises, siis vajavad kirjapandud põhimõtted vähemalt kord aastas ülevaatamist ning vajadusel uuendamist. Valdkonnas on näha teatud trendid (näiteks tehisintellektil põhinevate lahenduste kasutamise suurenemine), aga nende täpne mõju valdkonnale ja konkreetsete lahendused on alles kujunemas. Just sellel põhjusel ei pruugi käesolevast Valgest Raamatust leida kõiki vastuseid või kokkuleppeid strateegiliste suundade osas. Samuti on välja toodud teemad, milles sidusrühmad ei ole suutnud kokkulepet saavutada.

² Key Factors in Coping with Large-Scale Security Vulnerabilities in the eID Field. Kättesaadav: https://link.springer.com/chapter/10.1007/978-3-319-98349-3_5

³ The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. Kättesaadav: <https://dl.acm.org/doi/pdf/10.1145/3133956.3133969>

⁴ Valge Raamat. Identiteedihaldus ja isikut tõendavad dokumendid 1.0. Kättesaadav: <https://www.ria.ee/media/2431/download>

IDENTITEEDIHALDUS JA eID

Identiteedihalduse ja eID Valge Raamat on strateegiadokumentide hierarhias valdkondliku digiühiskonna arengukava edasiarendus detailsemas valdkonnas. Joonisel 1 on kujutatud Euroopa Liidu ja Eesti digiühiskonna strateegiadokumente ning nende omavahelist suhestumist. Valdkonna arengukavad ja strateegiad viitavad valdkonna spetsiifilistele strateegiadokumentidele, kus omakorda on kirjeldatud valdkonna detailsem strateegiline vaade. Kuna tegemist on agiilse dokumendiga, mille põhimõtete järgimine on sätestatud kõrgema taseme strateegia dokumendis, siis puudub vajadus identiteedihalduse ja eID Valge Raamatu eraldiseisvaks jõustamiseks ministeeriumi või muul kõrgemal poliitilisel tasandil. Detailne Euroopa Liidu ja Eesti identiteedihalduse ja eID valdkonda puudutavate strateegiliste dokumentide analüüs on toodud käesoleva dokumendi lisa 2.



Joonis 1. Euroopa Liidu ja Eesti identiteedihalduse ja eID valdkonna strateegiadokumentide hierarhia

Valge Raamatu uuendamise käigus on läbi viidud mitmeid erinevaid tegevusi. Uuendamise protsess sai alguse 2022. aasta lõpus, mil toimus esimene töötuba avaliku sektori ja erasektori esindajate osalusel. Töötoa tulemusena kaardistati eID valdkonna ootused, tugevused ja nõrkused, täiendavat arutelu vajavad küsimused ning võimalikud tulevikusuunad. Töötoa detailsem tulem on esitatud käesoleva dokumendi lisa 3. Lisaks viidi läbi täiendavad intervjuud e-riigi valdkonna arvamuslimedritega, et kaardistada valdkonda üldisemalt mõjutavaid (tehnoloogia)trende, kasutajate ootusi ning Eesti suhestumist teiste riikidega. Toimused aktiivsed arutelud eID valdkonna sidusrühmadega ning Riigi Infosüsteemi Ameti (RIA) siselselt. Oma panuse Valge Raamatu valmimisse andsid avaliku sektori poolt lisaks RIA-le, Majandus- ja Kommunikatsiooniministeerium, Siseministeerium, Välisministeerium, Politsei- ja Piirivalveamet (PPA), Siseministeeriumi infotehnoloogia- ja arenduskeskus (SMIT), Tervise ja Heaolu Infosüsteemide Keskus

IDENTITEEDIHALDUS JA eID

(TEHIK), Registrate ja Infosüsteemide Keskus (RIK). Erasektori poolelt panustasid Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL), Eesti Pangaliit, SK ID Solutions AS, Cybernetica AS, eID Easy ja E-riigi Akadeemia (eGA). Teadusasutusena oli kaasatud ka Tallinna Tehnikaülikool (TalTech). Novembris 2023 viidi läbi teine töötuba, kus avaliku sektori ja erasektori sidusrühmad keskendusid juba konkreetsete arengusuundade kokkuleppimisele. Töötoa sisendi pinnalt koostas RIA dokumendi lõpliku versiooni, mis kooskõlastati avaliku sektori ja erasektori sidusrühmade esindajatega.

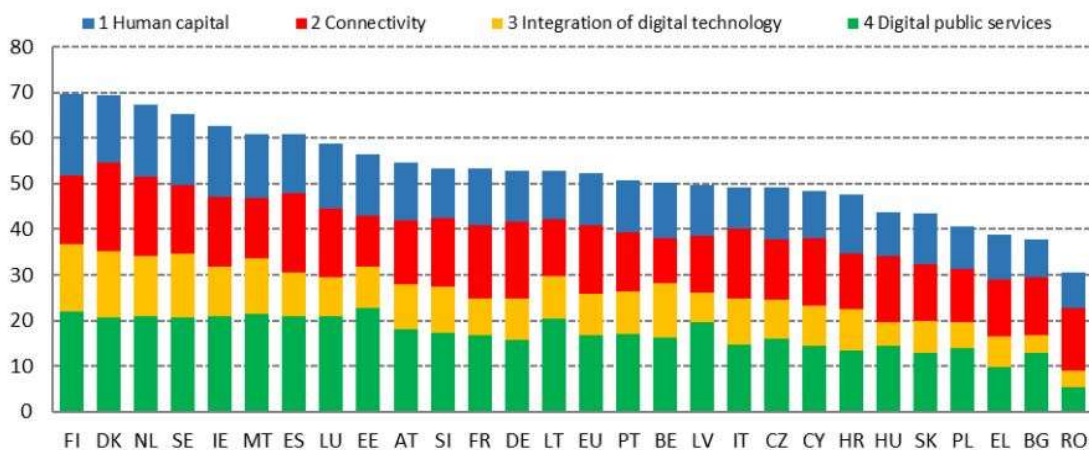
Kui sõnastada lühidalt eID valdkonna väärtuspakkumine, siis on ambitsiooniks pakkuda **kliendile ja kasutajale** usaldusväärset ja toimekindlat elektroonilist identiteeti, mis on turvaline, mugav ja maailma tasemel tunnustatud. Selleks kaitseme kasutaja identiteeti pakkudes turvalist eID lahendust, mugavaid eID toiminguid ja teenuste kasutust, aitame kasutajal säästa aega oma toimingutes, kindlustame eID ökosüsteemi koostoime, soodustame Eesti majanduse arengut ja tagame e-valitsemise sujuva toimimise. **Äriklendile** pakume turvalist, mugavat ja maailmatasemel eID lahendust ning soodustame uusi e-teenuste kasutuslugusid. Tavakasutaja osas on ambitsiooniks kaitsta tema identiteeti, teha tema elu mugavaks ning pakkuda kasutajasõbralikke lõppkasutaja rakendusi. Sarnaselt digiühiskonna arengukava mõõdikutele võtame aluseks era- ja äriklientide ning kasutajate eID valdkonna teenustega rahulolu.

Identiteedihalduse ja eID Valge Raamat koosneb neljast põhilisest osast. Esimeses osas antakse ülevaade Eesti eID valdkonna hetkeolukorrast ning teadaolevatest tulevikutrendidest, millega valdkonna arengute planeerimisel möödapääsmatult tuleb arvestada. Teine osa keskendub eID valdkonna tugevustele, nõrkustele ning võimaluste ja ohtude kaardistamisele. Kolmas peatükk keskendub identiteedihalduse ja eID valdkonna konkreetsetele strateegilistele suundadele ning tulevikuvaatele järgnevas viieks aastaks eristades üldised ning valdkondlikud strateegilised suunad. Neljandas peatükis võetakse kokku Valge Raamatu kaasaegsena hoidmise protsess ning edasise rakendamisega seonduv.

Valdkonna hetkeolukord ja tulevikutrendid

Käesolev arengusuundade ülevaade kajastab eID ja sellega tihedalt seotud valdkondades (e-teenused, tehnoloogia, õigusmaastik, standardid, kasutajad) viie kuni kümne aasta vaates aset leidvaid trende ja muudatusi laiemalt. Samuti käsitletakse muuhulgas põgusalt arenguid elektroonilise allkirjastamise valdkonnas. Tegemist ei ole arvatavate muudatustega, vaid teadaolevate protsessidega, mis on tänaseks juba osaliselt käivitunud või peagi realiseerumas ning mis mõjutavad pikemas perspektiivis valdkonda oluliselt. Lisaks on arengusuundade ülevaates välja toodud eID ja elektroonilise allkirjastamise valdkondi mõjutavad peamised väljakutsed ja ohutegurid, millega strateegilises vaates tuleb arvestada. Arengusuunad ei ole seotud ainult Eesti keskkonnaga, vaid maailmas üldiselt asetleidvate trendidega.

2018. aastal oli Eesti Euroopa Liidu digitaalrajanduse ja -ühiskonna indeksi (DESI) järgi liikmesriikide seas 9. kohal. Esimesel kohal oli Taani, teisel Rootsi ning kolmandal Soome.⁵ Hetkel kõige värskemad andmed pärinevad 2022. aastast. 2022. aastaks ei ole Eesti positsioon DESI vaates muutunud ning jätkame kokkuvõttes 9. kohal. Kuigi näiteks digitaalsete avalike teenuste vaates on Eesti esimesel kohal. Kokkuvõttes on Soome tõusnud esimeseks Taani ja Hollandi ees (vt. joonis 2).⁶ Kindlasti on positiivne see, et Eesti on suutnud nelja aasta vältel oma positsiooni säilitada. Samas ei ole varasemalt Eestist eespool olnud Ühendkuningriik enam DESI arvestuses, kuid sellest tulenevalt ei ole Eesti positsioon ka paranenud. Seega võib kokkuvõtvalt DESI indeksi põhjal öelda, et see peegeldab ühelt poolt Eesti digivaldkonna stabiilsust, kuid teisalt ka paigalseisu, mis väljendub tunnetuslikult ka identiteedihoolduse ja eID valdkonnas.



Joonis 2. Digitaalrajanduse ja -ühiskonna indeks 2022. Allikas: Euroopa Komisjon.

⁵ <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-2018-report>

⁶ <https://digital-strategy.ec.europa.eu/et/library/digital-economy-and-society-index-desi-2022>

IDENTITEEDIHALDUS JA eID

Järgnevad alapeatükid kirjeldavad eesiseisvaid muudatusi e-teenuste pakkumisel, prognoosi kasutajate käitumises, tehnoloogia arengusuundades, usaldusteenuste valdkonnas ning identiteedihalduse ja eID-ga seotud õigusruumis. Kuna valdkonnas on oluline osa standardiseerimisel, siis käsitletakse eraldi ka standardiseerimise lähiaastate perspektiivi.

ARENGUD E-TEENUSTE PAKKUMISEL

Viimastel aastatel on üha hoogustunud e-teenuste pakkumine just mobiilsete seadmete vahendusel. See trend jätkub kindlasti ka järgneva viie aasta vältel. Nii erasektori (sealhulgas finantsasutused ja pangad) kui ka avaliku sektori e-teenuse pakkujad on oma teenuste pakkumisel peamiselt suunatud nutiseadmete kasutajatele ning nendele erinevate lahenduste pakkumisele. Seega võib üsna kindlalt väita, et erinevate mobiilsetele platvormidele suunatud rakenduste (äppide) arendamine jätkub. Lisaks töötavad erinevad riigid välja enda mobiilseid lahendusi (näiteks Tšehhi, Taani, Küpros jne.). Soome on juba piloteerimas oma digiidentiteedikukru lahendust.⁷ Rakendustesse lisatakse teenuse- või platvormispetsiifilisi täiendavaid autentimisvõimekusi (näiteks finantsasutused integreerivad täiendavaid biomeetrilisi lahendusi jne.).

Kõikide e-teenuste kasutamiseks ei ole „kõrge“ tagatistasemega autentimisvahendid (nt. ID-kaart, mobiil-ID) ilmingimata vajalikud (seda eriti just erasektori poolt pakutavate e-teenuste vaates). Üha rohkem kasutatakse e-poodide puhul erasektori pakutud lahendusi, kus autentimine on juba seotud näiteks „tunne oma klienti“ (KYC) funktsioonidega. Vajadusel kasutatakse ka globaalsete suurettevõtete (nt. Google, Facebook jt.) autentimislahendusi, identiteedihalduse ja ligipääsu halduse teenuseid pakuvad aina rohkem ka Apple ja Microsoft. Erinevate sotsiaalmeedia platvormide ja nende poolt vajatavate identiteediga seotud teenuste hulk lähima viie aasta jooksul kasvab. Integreeritud identiteediplatvormide turu üldine aastane kasvumäär lähemal viiel aastal on hinnatud 24,6 protsendile⁸. Eestis pakutavatest e-teenustest on kasutajate vaates endiselt eelistatud finantssektor, tervishoiuteenused ning hariduse ja transpordiga seotud teenused⁹. Tegemist on teenustega, kus sektorid ise pakuvad mugavaid võimalusi nende e-teenuste kasutamiseks. Seega avaliku sektori e-teenused säilitavad ka järgnevatel aastatel oma populaarsuse ning määravad ka üldist turu arengut. Samas füüsiliste teeninduspunktide hulk ja nende pakutavate teenuste arv suure tõenäosusega väheneb veelgi võrreldes tänasega.

⁷ <https://dvv.fi/en/european-digital-identity-wallet>

⁸ <https://liminal.co/reports/the-rise-of-integrated-identity-platforms/>

⁹ Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. Kättesaadav: https://link.springer.com/chapter/10.1007/978-3-030-58957-8_12

IDENTITEEDIHALDUS JA eID

MUUDATUSED KASUTAJATE KÄITUMISES

Peamisteks **teguriteks, mis kasutaja käitumist mõjutavad on mugavus, kiirus ja turvalisus**¹⁰. Lisaks eelnevale mõjutab kasutajate käitumist ka teadlikkus erinevatest lahendustest ja platvormidest. Kasutaja eeldab, et ta saab kõiki teenuseid kasutada samaväärselt ja turvaliselt nii laua- ja sülearvutist kui ka mobiilse seadmega ning olenemata enda asukohast. Pigem kaldub suund sinnapoole, et kasutajad eelistavad kasutada e-teenuseid mobiilsetest seadmetest ning ainult laua- ja sülearvuti vahendusel pakutavad e-teenused kaotavad kasutajaid. Samas arvutipõhised kasutusjuhud jäävad endiselt alles ka pikemas perspektiivis.

COVID on oluliselt muutnud kasutajate töötamise harjumusi. Kodukontoris töötamine on muutunud tavapäraseks ning aina enam ei oma töötaja asukoht tähtsust¹¹. Sellega seoses **kasvab piiriülese autentimise populaarsus ning vajadus digitaalselt allkirjastatud dokumentide edastamiseks riikidevaheliselt**. See omakorda esitab väljakutse dokumentide digitaalsele allkirjastamisele ning allkirjade kehtivuse kontrollimisele. Lisaks on Euroopa Komisjon jõudnud kokkuleppele Euroopa ühtse digiidentiteedikukru õigusliku raamistiku osas, mis võimaldab piiriüleselt turvalist ligipääsu avaliku sektori ja erasektori e-teenustele (sealhulgas lõppkasutaja jaoks tasuta kvalifitseeritud e-allkirjastamisele).¹² Digiteenuste määruse kohaselt on väga suured digiplatvormid nagu Amazon, Booking.com, Meta jne. kohustatud tunnustama EL-i ühtset digiidentiteedikukrut.¹³

TEHNOLOOGIA ARENGUSUUNAD

Tulenevalt riigi poolt sõlmitud lepingute kehtivuse perioodist **ei kao kiipkaardil põhinevad riiklikud eIDd järgmise 10 aasta jooksul**. 2024. aastal jõudis Eestis lõpusirgele ID-1 formaadis dokumentide hange, millega tagatakse eID funktsionaalsusega kiipkaartide (nagu ID-kaart, elamisloakaart jt.) väljaandmine järgneva 8-10 aasta jooksul. Lisaks tuleb arvestada lepingu rakendamiseks kuluvat aega ning asjaolu, et lepingu alusel välja antud viimane eID funktsionaalsusega kiipkaart kehtib veel kuni viis aastat. See omakorda eeldab aga kogu toetava ökosüsteemi olemasolu veel vähemalt järgnevad 14-16 aastat (so. 2038-2040).

Erinevate autentimistehnoloogiate hulk suureneb veelgi ning seda eelkõige erinevate biomeetriliste lahenduste, kasutusmustrite ning krüptograafia rakenduste arvelt. Siin on suurem roll kindlasti erasektoril, kuid ka riiklikul tasandil otsitakse uusi võimalusi ja alternatiive (näiteks biomeetria kasutamiseks).

¹⁰ Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. Kättesaadav: https://link.springer.com/chapter/10.1007/978-3-030-58957-8_12

¹¹ <https://www.mkm.ee/media/9111/download>

¹² https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651

¹³ <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32022R2065>

IDENTITEEDIHALDUS JA eID

Biomeetria puhul on peamiseks väljakutseks turvalisuse tagamine ning seda nii andmete hoides, hõivekvaliteedis, andmete hoiustamises kui ka edastamises. Järgneva viie aasta jooksul vajab otsustamist ning tehnilist lahendamist, kas ja kuidas on võimalik kasutada riiklikke e-teenuseid madalama tagatistasemega (näiteks tasemel „märkimisväärne“) autentimisvahenditega (muuhulgas ka sotsiaalmeedia kontodega nagu Google, Facebook jne.). Paralleelselt püüavad Euroopa Liidu liikmesriigid leida tehnoloogilist lahendust kaugteel isikusamasuse kontrollimiseks, mis vastaks eIDAS määruse tagatistasemele „kõrge“.

Allkirjastamistehnoloogia on tugevalt standardiseeritud ning olemasoleval kujul riigisiselt hästi toimiv, väljakutseid pakub jätkuvalt erinevate tehniliste formaatide¹⁴ riskasutus ning erinevate elektrooniliste allkirjade kehtivuse kontroll. Standardiseerimise töörühmades toimub töö uute digiallkirjaformaatide (JAdES, CB-AdES) suunal, parendatakse digiallkirjades kasutatavat krüptograafiat (kvantarvuti kindlate algoritmide kasutuselevõtt) ja digiallkirjastatud dokumentide jaoks mõeldud konteinerite formaatide standardeid ning see lisab nende formaatide laiema kasutamisel täiendavat riskasutuse keerukust. Siiski ei pruugi selles valdkonnas lähima viie aasta jooksul midagi drastiliselt muutuda ja erinevate digiallkirjade koostoime lahendatakse erasektori teenusepakkujate poolt. Kindlasti lisandub valdkonda uusi krüpteerimiseks kasutatavaid algoritme ning standardeid, kus täpsustatakse nõuded jne.

Mobiilsete tehnoloogiate puhul säilib operatsioonisüsteemide mitmekesisus. See tähendab, et rahvusvahelisel tasandil ei teki ühtegi globaalset pakkujat kes naudiks domineerivat turuosa (näiteks “iPhone – 60% kasutajaid”).

Väljakutseks tehnoloogia valdkonnas saab kindlasti olema standardimise ja turvaauditite reeglite järele jõudmine paralleelselt innovaatiliste tehnoloogiate arengule ning kasutuselevõtule. Turul on küll erinevaid innovaatilisi lahendusi, aga need ei ole kooskõlas tänaste standarditega. Tehnoloogia areneb kiiremini kui valdkonna reeglid ja standardid sellele järele jõuavad. Heaks näiteks siin on juba olemasolevad tehisintellektil põhinevad näotuvastustehnoloogiad, mille kasutamise eelduseks on mitmetes eetilistes ning vastutusega seotud küsimustes sisulisele kokkuleppele jõudmine ning vastava regulatsiooni kehtestamine¹⁵. Samuti on EL seoses eIDAS 2.0, NIS2 ja CSA skeemide rakendamisega ringi korraldamas senist turvanõuete vastavushindamist. Uued lahendused pakuvad kindlasti kasutajale oluliselt paremat kogemust, kuid lahenduste turvalisuse hindamine enne nende laialdasemat kasutuselevõttu on aeganõudev protsess ning eeldab vastava reeglustiku ja hindamisraamistiku olemasolu. Tootjatele ja eriti usaldusteenuse osutajatele

¹⁴ https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html#_specificities_of_signature_creation_in_different_signature_formats

¹⁵ The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. Kättesaadav: <https://link.springer.com/article/10.1007/s43681-021-00077-w>

IDENTITEEDIHALDUS JA eID

lisandub oluliselt auditeerimise kohustust ja sellega kaasnevalt oma toodete ja teenuste uute õigusaktide ja nendest tulenevate standardite ja skeemidele vastavusse viimist. Kvalifitseeritud usaldusteenuste pakkujate kontekstis suurendab see kindlasti uute teenuste osutajatele turule sisenemise maksumust. Suureneb ENISA roll ja EU spetsiifilised nõuded võivad lähiaastatel oluliselt hakata piirama kasutatavate toodete valikut.

Eestis on küll tehnilisel tasandil eelistatud hajusa arhitektuuri suund, kuid selle komponendid peavad olema koosvõimelised. Allkirjastamis- ja autentimisteenuste laienevad õigusaktidest ja standarditest tulenevad kõrgendatud nõuded ning regulaarne auditeerimiskohustus, mis mõjutavad vahetult konkurentsivõimekust antud turul. Tehnilisest vaatest on allkirjastamis- ja autentimisteenuste puhul tegemist spetsiifiliste teenustega, millega seotud komponentide hajus haldamine on keerukas ning kõrge riskiga. Eeltoodust tulenevalt on **allkirjastamis- ja autentimisteenuste vaates eelistatud keskne lähenemine hajutatud arhitektuuriga tehnoloogiate kasutamise ees.**

Küberturvalisuse seisukohast mõjutavad eID valdkonda arengud kvantarvutusvõimsuse valdkonnas, kus käesoleval ajal puudub Eestil ajakava või juhiseid kvantarvuti kindlatele krüptoalgoritmidele üleminekuks. Cybernetica AS poolt 2023. aastal koostatud uuringu „Krüptoalgoritmid ning nende tugi teekides ja infosüsteemides“ kohaselt on tegemist ohtliku olukorraga, seda eriti just elutähtsate teenuste puhul, kus keskseks on avaliku võtmega signeerimise funktsionaalsus, mille jaoks kasutatavad algoritmid muutuvad kvantarvutite kasutuselevõtul ebaturvaliseks. Samas hinnatakse eelnimetatud uuringu kohaselt järgmise viie aasta perspektiivis näiteks RSA-2048 krüptoalgoritmi murdmise riski vähem kui 24 tunni jooksul pigem madalaks.¹⁶

USALDUSTEENUSTE VALDKOND, MÕJU JA eID ÖKOSÜSTEEMIGA SEOTUD ARENGUD

Lähima viie aasta perspektiivis jääb EL-is kasutusse traditsiooniline nimekirjapõhine usaldusahela skeem (LOTL-TL-(q)TSP).¹⁷ Käesoleval ajal on näiteks Prantsusmaal ja Saksamaal üle kümne kvalifitseeritud usaldusteenuse pakkuja. Samas kui Eesti turul osutab usaldusteenuseid praktikas hetkel veel ainult üks ettevõtte. Sisuliselt puudub turul arvestatav konkurents ning alternatiiv teenust osta Eesti turult mõne teise teenusepakkuja käest. Kindlasti tuleb järgneva viie kuni kümne aasta jooksul otsustada ning leida lahendus, kas riigil peab olema endal usaldusteenuse osutamiseks vajalik kompetents või piisab koostöö jätkamisest erasektori ettevõtetega läbi hankemenetluse reeglite kohandamise. 2023. aastal läbiviidud uue sertifitseerimis- ja usaldusteenuste hankel esitas pakumuse samuti vaid üks ettevõtte (Zetes).¹⁸ Käesolevaks ajaks on leping sõlmitud ning ees seisab väljakutse, kus Eesti eID ökosüsteem peab esmakordselt paralleelselt toime tulema kahe sertifitseerimis- ja usaldusteenuste pakkujaga. Lisaks suureneb vajadus

¹⁶ Krüptoalgoritmid ning nende tugi teekides ja infosüsteemides. Kättesaadav: <https://www.ria.ee/media/3041/download>

¹⁷ EU/EEA Trusted List Browser. Kättesaadav: <https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home>

¹⁸ <https://tsp.zetes.com/>

IDENTITEEDIHALDUS JA eID

Euroopa Liidu väliste poolte usaldusahelate tunnustamise ning sellega seotud õigussuhete reguleerimise järele.

Euroopa tasandil liigutakse järgneva viie aasta jooksul e-teenuste kasutamise ning koosvõime võimekuse väljaarendamise suunas läbi Euroopa digiidentiteedi raamistiku kehtestamise ning **Euroopa digiidentiteedikukru (digikukru) rakendamise**¹⁹. Muutused toimuvad eri valdkondade paralleelsetel suundadel:

- Esiteks Euroopa digiidentiteedi raamistiku eIDAS uuendamine, mis paneb paika regulatsiooni ning võimaldab eID skeeme sertifitseerida.
- Samal ajal arendatakse nii liikmesriikides eraldi kui EL komisjoni poolt keskselt digikukru referentsarhitektuuri raamistikku ja tarkvaralahendusi.²⁰
- Kasutuslugude pilootprojektid (juhiloast ravikindlustuskaardi, digiretsepti ja reisidokumendini) kestavad 2025 aasta keskpaigani.²¹
- Eraldi töögrupid tegelevad küberturvalisuse ja sertifitseerimisnõuetega.

Seda kõike kokku võttes on digikukru kasutusvõimalus 2026. aasta lõpus reaalne ja 2030 eesmärk saavutatav. Samas, arvestades liikmesriikide senist praktikat uute tehnoloogiate kasutuselevõtmisel, siis võtavad reaalsed muudatused ning toimiva koosvõime väljaarendamine pigem rohkem aega. Seega saab üheks väljakutseks kindlasti olema digikukru juurutamine Euroopa üleselt. Lisaks tuleb arvestada, et digikukru kasutuselevõtt eeldab Eesti keskkonnalt kohanemist, kuna see toob endaga kaasa erineva lähenemise isikuga seotud andmete jagamisel – kasutaja saab ise valida, milliseid andmeid ta jagab (nt ainult vanust, aga mitte nime ega isikoodi). Digikukru kasutuselevõtu eelduseks on eIDAS määrusele vastava eID skeemi koostamine, siseriiklik rollide, vastutuse ja töökorralduse kokku leppimine ning vajalike siseriiklike õiguslike muudatuste analüüs ja rakendamine.

Koos EL seadusandluse arenguga lisandub erinevaid usaldusteenuseid (näiteks atribuutide elektrooniline tõendamine ja elektrooniline arhiveerimine). Samas jääb usaldusteenuste ülepiiriline osutamine tagasihoidlikuks. Valdonna turg on killustatud erinevaid tehnoloogiaid (kiipkaardid, *wallet*-id, biomeetria jne.) kasutatavate lahenduste pakkujate vahel. Seda peamiselt elektroonilist autentimist võimaldavate

¹⁹ Euroopa Parlamendi ja nõukogu määrus, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega. Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52021PC0281>

²⁰ <https://github.com/eu-digital-identity-wallet>

²¹ <https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet>

IDENTITEEDIHALDUS JA eID

lahenduste vallas. eID valdkonnas eeldatakse senisest suuremat privaatsuse kaitset ning sellega arvestamist eID vahendite disainis.

Suure tõenäosusega lisandub valdkonnas nn lisaväärtusteenuste osutajate hulk. Siinkohal on eelkõige mõeldud dokumentide digitaalset allkirjastamist ja nende töövoogusid ning allkirjade kehtivuse kontrollimise lahenduse pakkujate hulga suurenemist. Seda trendi toetab ka Eestis viimastel aastatel valdkonnas tegutsevate uute teenusepakkujate lisandumine (Dokobit²², eIDEasy²³ jt.). Kasutatakse erinevaid usaldusteenuseid (rQSCD, autentimisteenused, KYC, digikukru tõendite valideerimine). Tunne oma klienti (KYC) teenuste osutajad võivad laiendada teenuste pakkumist ka eID valdkonnas, eelkõige elektroonilise autentimise võimaldamisel. Ehk sisuliselt võib tekkida turule uusi usaldusteenuse pakkujaid. Digiidentiteedikukru kontekstis on oluline riiklike tõendite väljastamine kui eraldi usaldusteenus ning sellekohase strateegilise plaani olemasolu.

ÕIGUSVALDKONNA ARENGUSUUNAD

Euroopa Liidu regulatsioonid mõjutavad oluliselt eID ning elektroonilise allkirjastamise valdkondi. Euroopa Liit jõuab tehnoloogia reguleerimise vallas järgi või isegi läheb ette liikmesriikide tasandil kehtestatud regulatsioonidest. Ühe näitena võib siinkohal tuua eIDAS 2.0 määruse ning selle rakendusaktid, mis kehtestavad Euroopa digiidentiteedi raamistiku ning kohustuvad kasutusele võtma Euroopa digiidentiteedikukru, kahandavad siseriiklike regulatsioonide vajadust veelgi. Siseriiklikul tasandil kehtestatud reeglid omavad üha väiksemat rolli infoturbe ja andmekaitse korraldamises (ISKE/EITS²⁴ vs. CSA EL skeemid) ning tehisintellektil põhinevate süsteemide kasutamise vaates²⁵. Sellest tulenevalt lähtume EL-i õigusruumist ning vajadusel viime siseriiklikud õigusaktid kooskõlla EL-i õigusruumiga.

Lisaks eID valdkonnaga otseses puutumuses olevatele õigusaktidele mõjutavad EL-i tasandil valdkonnaga kaudes puutumuses olevad õigusaktid. Näidetena võib siinkohal tuua Küberturvalisuse direktiivi (NIS 2)²⁶,

²² <https://www.dokobit.com/et/>

²³ <https://eideasy.com/>

²⁴ <https://eits.ria.ee/>

²⁵ Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte. Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52021PC0206>

²⁶ Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv). Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32022L2555&qid=1693222236585>

IDENTITEEDIHALDUS JA eID

tehisintellekti käsitleva õigusakti²⁷ jne. Sellised paralleelselt väljatöötamisel ja muutmisel olevad õigusaktid tekitavad palju segadust, kuna sageli puudub õigusaktide vaheline põhimõtete harmoniseerimine.

Avaliku võtme infrastruktuuril (PKI) põhinev digitaalallkirja regulatsioon on eIDAS-e üks osa ning õigusaktide ja standardite tasandil küllaltki põhjalikult reguleeritud. PKI-l põhinevad lahendused on selles valdkonnas laialdaselt kasutusel. Seetõttu ei ole reaalne, et järgneva viie aasta jooksul kaovad olemasolevad nõuded digitaalselt allkirjastatud dokumentidele. Pigem täpsustatakse olemasolevaid nõudeid või lisatakse üht-teist juurde. Põhiline muutus toimub vastavushindamise valdkonnas seoses *Subcarrier Spacing (SCS) 5G*, pilveteenuste ja infoturbe toodete skeemide rakendamisega ja nende ülemuslikkusega analoogsete rahvuslike skeemide ees.

Isikutuvastust puudutav üldine õiguslik regulatsioon jääb elektroonilist autentimist võimaldavate vahendite vastastikuse tunnustamise ja väljastamisprotsessi keskseks. Täpsustatakse oluliselt eID skeemide vastastikuse tunnustamise protsessi ja isikutuvastuse reegleid Euroopa Liidu tasandil ning väljastamisprotsessis otsitakse tehnilisi ja õiguslikke lahendusi kõrgel tasemel tunnustatud eID vahendi väljaandmiseks kaugtuvastuse teel. Lisaks luuakse täiesti uue eID skeemide sertifitseerimise võimalus. Samas ollakse jätkuvalt elektroonilist isikusamasuse kontrolli võimaldavate tehnoloogiate osas neutraalsemad ning õiguslikult vähem reguleeritud võrreldes digitaalset allkirjastamist võimaldavate tehnoloogiatega. Usaldusteenuste regulatsioon Euroopa Liidus jääb ja täieneb uute teenuste ja reeglitega.

Koostalitlusvõime ning piiriüleste teenuste pakkumise seisukohalt ei ole oluliseks Euroopa unikaalse identifikaatori osas konsensuse saavutamine, vaid ühise arusaama saavutamine atribuutide osas, mida saab kasutada vastendamise (i.k. *identity matching*) protsessis. Selle protsessi osas võib näitena tuua 22.09.2023 Põhja- ja Baltimaade ministrite poolt allkirjastatud deklaratsiooni piiriülese *identity matching*-u alase koostöö osas.²⁸

TRENDID STANDARDISEERIMISES

Standardiseerimine on tehnoloogia valdkonnas olulise tähtsusega, tagades kasutatavate tehnoloogiate ühetaolisuse, ühilduvuse, koostalitlusvõime ning kvaliteedi. Kindlasti lisandub järgnevatel aastatel eID ja e-allkirjastamise valdkonda uusi standardeid. Seda kindlasti juba Euroopa digiidentiteedikukru kasutuselevõtuga, kuid ka näiteks elektroonilise allkirjastamise valdkonnas, kus Euroopa

²⁷ Euroopa Parlamendi ja Nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte. Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52021PC0206>

²⁸ <https://www.norden.org/en/declaration/declaration-nordic-and-baltic-ministers-digitalisation-cross-border-identity-matching>

IDENTITEEDIHALDUS JA eID

Telekommunikatsiooni Standardiinstituut (ETSI)²⁹ on töötanud välja uue tehnilise spetsifikatsiooni JADES allkirjade osas³⁰ jne. Euroopa Liidu Küberturvalisuse Ameti (ENISA) on alustanud juba ka analüüsi digikukruga seotud standardite valdkonnas.³¹ Eeltoodust tulenevalt on prognoositav järgneva viie aasta jooksul digikukruga seotud standardite raamistiku väljaarendamine.

Standardiseerimise valdkonnas tegeletakse kindlasti aktiivselt ka kvantkindlate algoritmidega ning olemasolevate standardite harmoniseerimisega. Riiklikul tasandil väljatöötatud standardid omavad aina vähem tähtsust ning Euroopa Liidu üleselt väljatöötatud standardid võetakse liikmesriikides kasutusele vahetult täiendava harmoniseerimise vajaduseta. Seda näitab asjaolu, et üha vähem kasutatakse EL tasandil direktiivi formaati ning konkreetsete standardite kasutamine tuuakse välja määruse või selle rakendusakti tasandil. Lisaks jätkub trend, kus Euroopa Liidu kandidaatriigid ning kolmandad riigid tuginevad oma lahenduste puhul just Euroopa Liidu standarditele.

VALDKONNA ARVAMUSLIIDRITE VAADE

Lisaks juba eelpool kirjeldatud trendidele, mis on lähima viie aasta jooksul juba ära määratletud või kindlalt ette näha, on oluline aru saada eID valdkonda mõjutavatest üldistest tehnoloogilistest suundadest ja arengutest. Selleks sai läbi viidud üheksa intervjuud Eesti digivaldkonna eestkõnelejate ja arvamussliidritega. Sealhulgas näiteks ka president Toomas Hendrik Ilves-e ja president Kersti Kaljulaid-iga, kes on teadlikult panustanud ning jätkuvalt panustavad Eesti digiriigi arengusse. Täpsem nimekiri läbiviidud intervjuudest ning esitatud küsimustest on toodud käesoleva dokumendi lisa 4. Alljärgnevalt on lühidalt kokku võetud intervjuudes välja toodud suunad ja põhimõtted. Taustal on oluline arvestada, et käesoleval ajal sisuliselt puuduvad uuringud, kuidas digitaliseerimine on meie ühiskonda ja käitumist laiemalt mõjutanud. Samas ei ole kahtlust, mis juhtub siis kui e-teenused pole kättesaadavad või eID pole kasutatav e-teenuste puhul (ID-kaardi ROCCA kriis³², vaegnägijate kaebused jne).

eID valdkond on kiires arenemises ning järgneva viie aasta jooksul on kindlasti oodata hulgaliselt muudatusi. See omakorda seab surve alla kõik olemasolevad eID ökosüsteemid. Muudatused on eelkõige seotud tehnoloogiate valitsemisega, kus riikide osatähtsus otsuste tegemisel suureneb. Samas võimekus selliseid otsuseid langetada on jätkuvalt madal. Valdkonnas tuleb enim arvestada arengutega USA-s, Hiinas ning

²⁹ <https://www.etsi.org/>

³⁰ Electronic Signatures and Infrastructures (ESI). JAdES digital signatures. Kättesaadav: https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.01.01_60/ts_11918201v010101p.pdf

³¹ Digital Identity Standards. Kättesaadav: <https://www.enisa.europa.eu/publications/digital-identity-standards>

³² https://doi.org/10.1007/978-3-319-98349-3_5

IDENTITEEDIHALDUS JA eID

Euroopa Liidus. Aina rohkem tuleb pildile ka ainult masinatevaheline suhtlus, tehisintellekti kasutamine ja suurandmete töötlemine. Rõhk on rohkem tarkvaralistel lahendustel ning riistvaraliste komponentide osatähtsus (sh. eID füüsilised kandjad) väheneb. Riigi rolliks on eelkõige tagada tuvastamist võimaldavate usaldusväärsete atribuutide pakkumine.

Kui püüda selles kontekstis positsioneerida Eesti eID-d Euroopa/maailma kontekstis järgneval viiel aastal, siis jäi intervjuudest läbivalt kõlama kaks märksõna – siseriiklik eID ökosüsteem ja selle koosvõimelisus. Eesti peaks eelkõige keskenduma oma siseriiklikule ökosüsteemile ning selle arendamisele, kuid samas on oluline tagada koosvõimelisus teiste ümbritsevate lahendustega. Koosvõimelisuse puhul ei peetud silmas vaid teisi riike või Euroopa Liitu, vaid teisi eID lahendusi üldisemalt. eID valdkonna liidripositsioon maailmas ei ole eesmärk omaette. Pigem tuleb tagada parimate seas olek läbi mugavalt kasutatava ja koosvõimelise lahenduse ning kõrge kasutatavuse. Uute lahenduste osas ei tohi olla ignorantne, vaid pigem saada nende olemusest aru ning innovatsiooniga kaasa minna. Lisaks on oluline ka volitamine ja delegeerimise teema, kuna hetkel on eID vahend isikupõhine ning ei ole võimalik lihtsasti eristada, millistes volitustes isik konkreetsel hetkel tegutseb. Näiteks kas tegemist on füüsilise isikuga, kes tegutseb enda nimel, või hoopis juriidilise või teise füüsilise isiku esindajana.

Eesti eID ökosüsteemi peamiste tugevustena töid intervjueeritavad välja:

- eID kui keskse teenuste ligipääsu võimaldaja;
- tugeva ja keskselt hallatud riikliku identiteedi;
- usaldusväärse ja läbipaistvuse;
- toimiva digiriigi ja digiühiskonna;
- võimu vertikaalide väiksuse Eestis;
- eID kui alusarhitektuuri osa, mida tuleb hoida;
- eID kõrge kasutatavuse;
- eID kõrge turvalisuse;
- ID-kaardi olemasolu *back-up* lahendusena;
- Selge ja ühetaoline lähenemine tagatistasemete osas.

Samas on Eesti eID valdkonnas ka mitmeid nõrku kohti. Alates puudujääkidest missioonis, visioonis ja innovatsiooni valdkonnas, lõpetades valdkonna ekspertide nappuse ning ebapiisava rahastusega.

Valdkondi, mis järgneva viie aasta jooksul ka eID valdkonda mõjutavad, on mitmeid. Intervjueeritavad töid välja järgmised valdkonnad:

- **Tehisintellekt**il saab olema suur mõju ning vajalik on kujundada positsioon selles osas. Eelkõige, millises ulatuses ja viisil seda saaks valdkonnas ära kasutada.

IDENTITEEDIHALDUS JA eID

- **Biomeetria** osatähtsuse suurenemine autentimislahendustes.
- **Kvantarvutuse** arenguid tuleb jälgida ning riigil peab olema kvantarvuti kindel krüptograafia lahendus.
- **Roheteemad** ja keskkonnasäästlikud lahendused üldisemalt.
- **Virtuaalreaalsus** kindlasti mõjutab, kuid selle ulatust on hetkel keeruline hinnata.
- **Turvalisus** ning turbe olulisus üldisemalt, kuna rünnete rohkus ja keerukus kasvab.

Eristada saab lähemas ning pikemas vaates mõjutavaid valdkondi. Lühiajalises plaanis mõjutab eID valdkonda kindlasti Euroopa Liidus hetkel arendatav digikukru lahendus ning sellega paralleelselt arendatavad erinevad *wallet-i* põhised lahendused. Siinkohal mõjutavad eID valdkonda kindlasti ka GAMAM³³ poolsed identiteedihaldusega seotud tegevused. Pikemaajaliselt võib täheldada eID füüsiliste kandjate asendumist erinevate tarkvaraliste lahendustega. Ühe ohuna toodi intervjuu käigus välja, et näiteks EL-i digikukru projekti edukuse korral võidakse Eesti enda seniste kasutatavate ja hästitoimivate lahenduste kasutamist piirata.

Osa eID valdkonda mõjutavatest arengutest esitavad valdkonnale ka tõsiseid väljakutseid. Identiteedi tõsikindel tuvastamine ning selle eristamine teistest (sh. masinatest) muutub üha olulisemaks. Piirid inimeste ja masinate vahel elektroonilises keskkonnas ning võime neid omavahel eristada hägustuvad. Samas soovivad kasutajad maksimaalset privaatsuse kaitset. Siinkohal on kindlasti eID valdkonna üheks peamiseks väljakutseks küberturvalisuse tagamine ning tasakaalu leidmine turvalisuse ja kasutusmugavuse vahel. Väljakutseks saab kindlasti olema ka juba eelnevalt nimetatud kvantarvutus. Selleks, et erinevate väljakutsetega toime tulla, peaks õigusruum ning senine õigusloome loogika olema märksa paindlikum.

Kasutajad üldjuhul ei mõtle eraldi, mida nad konkreetset eID valdkonnalt soovivad, vaid tahavad ajada oma asju toimivas ökosüsteemis. Peamisteks märksõnadeks on mugavus, lihtsus, kiirus ja turvalisus. See tähendab, et eID vahendit on võimalik saada lihtsalt ning see on universaalselt kasutatav. Samuti tuleb arvestada, et kasutaja on täna selgelt mobiilsetele lahendustele suunatud. See toob omakorda kaasa ohu, mis on seotud konkreetsest seadmest sõltuvusega ehk mobiilne seade kui *single point of failure*.

Tulenevalt tugevast digiriigi kuvandist on Eesti ka teiste riikide huvialas. Teised riigid huvituvad eelkõige kasutuslugudest, poliitikast ja innovatsioonist ning kuidas seda oleks võimalik üle võtta. Eeltoodust tulenevalt küsiti intervjuude käigus ka teiste riikide ootuste kohta Eesti suunas ning kuidas hoida selles valdkonnas head mainet. Eesti muudab eriliseks eelkõige see, et meil on tegelikult toimiv eID ökosüsteem, mis on igapäevaselt aktiivses kasutuses. Seega on teiste riikide ootused eelkõige seotud Eesti tehnoloogia valitsemismudeliga ning selle tundmaõppimisega. Siinkohal on arukas seda küpsust ära kasutada ning ka

³³ Google, Amazon, Meta (varasemalt Facebook Inc), Apple ja Microsoft.

IDENTITEEDIHALDUS JA eID

rohkem turundada. Kui suudame hoida oma lahenduste kasutatavust ja kvaliteeti, siis tagame jätkuva huvi ka maailma tasandil.

Strateegilist otsustamist vajavad küsimused:

- Kuidas EUDIW ehk EU digiidentiteedikukkur sobitub Eesti eID ökosüsteemi?
- Kas Eestis võiks tunnustada ka madalama tagatistasemega (näiteks „märkimisväärne“) eID vahendeid?
- Milline saab olema mobiil-ID lahenduse tulevik?
- Kas ja kuidas kavatseme kasutada biomeetriat?
- Kas krüpteerimise funktsionaalsuse säilitamine on otstarbekas?
- Millised on e-residentide soovid, vajadused ning kuidas nendega parimal viisil arvestada?
- Kuidas tegeleda senise *legacy*-ga?

Intervjuude käigus tehti ka mitmeid soovitusi, mida eID valdkonnas tuleks kaaluda. Siinkohal on välja toodud loetelu tehtud ettepanekutest:

- Kindlasti peaks turvalisuse kaalutlustel olema kasutusel paralleelselt mitu üksteisest sõltumatu ja erineva tehnilise arhitektuuriga eID vahendit.
- EL digiidentiteedikukru puhul on oluliseks võtta suund just kahe eraisiku vahelistele kasutusjuhtudele (näiteks ühistranspordis soodustuse saamise tõendamiseks avaldamata seejuures konkreetse soodustuse saamise alust).
- Lahendamist vajab tehisintellektil põhinevate süsteemide volitamise teema.
- Standardiseerida häälkäsklusele põhinev digiallkiri ning selle andmine.
- Tähelepanu tuleb pöörata brauserite koosvõimekusele.
- Mitmed intervjuueeritavad rõhutasid, et GAMAM ettevõtetega peaks olema sõlmitud koostöölepingud ning Eesti eID võiks nende ettevõtete poolt olla tunnustatud.
- Eesti võiks olla EL-is pilootriik identiteedi valdkonnas. See tähendab, et Eesti töötab EL rahastuse baasil välja referentslahenduse ning teised riigid saavad selle kasutusele võtta.
- Leida eID valdkonnas lahendus kvantarvutusvõimsusega toimetulekuks.
- eID valdkonnas peaks olema riskiplaan kvantarvutusest tulenevate riskidega toimetulekuks.
- Valdonna strateegiliste eesmärkide puhul tuleks defineerida prioriteedid ning eristada, mida tuleb kindlasti teha ning mida oleks hea täiendavalt teha.
- Madalamate tagatistasemete aktsepteerimisel on vajalik teostada äriprotsesside riskianalüüs.

VALIDEERIMINE

Valdkonna ekspertide ning eestkõnelejate ja arvamuslimidrite väljaõeldu kõrval sai käesoleva dokumendi lisa 4 toodud intervjuu läbi viidud ka tehisintellektil põhineva juturoboti ChatGPT versioon 3.5-ga. Intervjuu

IDENTITEEDIHALDUS JA eID

tulemus on toodud käesoleva dokumendi lisa 5. Lühidalt võib öelda, et juturobot tõi välja üldisemad olulised suundumused (küberturvalisuse, biomeetria, tehisintellekt) ning soovitused, mis on heaks esmaseks sisendiks. Siiski ei suuda juturobot pakkuda veel konkurentsi ekspertide ja praktikute tasemel ning käsitleda eID valdkonna arenguid süvitsi.

eID ökosüsteem ning selle tugevused, nõrkused, väljakutsed ja võimalused

Eesti eID ökosüsteemil on üle kahekümne aastane ajalugu ning see valdkond on pidevas muutumises ja arenemises. Seetõttu on RIA tellimusel AS Cybernetica poolt koostatud eraldiseisvalt detailne eID ökosüsteemi ülevaade „Eesti e-identiteedi ökosüsteemi kirjeldus“. Eeltoodust tulenevalt ei keskendu käesolev peatükk niivõrd eID ökosüsteemist üldise ülevaate andmisele, vaid toob välja ökosüsteemiga seotud avaliku sektori ja erasektori sidusrühmad, kasutusstatistika ning hetkeseisu tugevustest, nõrkustest ja väljakutsetest, võimalustest.

Eesti identiteedihalduse ja isikut tõendavate dokumentide valdkond põhineb avaliku ja erasektori tihedal koostööl. Allpool on välja toodud eID ökosüsteemiga seotud peamised sidusrühmad ning nende rollid.

Avaliku sektori poolelt on eID ökosüsteemiga seotud:

- **Politsei- ja Piirivalveamet (PPA)** vastutab isikute tuvastamise ja identiteedihalduse eest, hangib isikut tõendavaid dokumente ja tagab nende väljaandmise. Lisaks vastutab PPA käesoleval ajal ID-1 formaadis Eesti riikliku eID skeemi kirjeldamise eest.³⁴
- **Riigi Infosüsteemi Amet (RIA)** vastutab eID tarkvara ning usaldusteenuste infrastruktuuri arendamise ja haldamise korraldamise eest. Samuti vastutab RIA küberturvalisuse tagamise eest ning teostab järelevalvet usaldusteenuste valdkonnas vastavalt eIDAS määrusele ning e-identimise ja e-tehingute usaldusteenuste seadusele.^{35 36}
- **Siseministeeriumi Infotehnoloogia ja arenduskeskus (SMIT)** arendab, hangib ja haldab Siseministeeriumi valitsemisala ülesannete täitmiseks vajalikke info- ja kommunikatsiooniteenuseid (IKT), sealhulgas identiteedihalduse ja isikut tõendavate dokumentide valdkonnaga seotud IKT teenused.³⁷
- **Majandus ja Kommunikatsiooniministeerium** kujundab ja koordineerib Eesti infoühiskonna poliitikat strateegilisel tasandil ning vastutab valdkondliku õigusloome eest.³⁸

³⁴ <https://www.riigiteataja.ee/akt/112112022004>

³⁵ <https://www.riigiteataja.ee/akt/103102023003>

³⁶ <https://www.riigiteataja.ee/akt/125102016001>

³⁷ <https://www.riigiteataja.ee/akt/126112022002>

³⁸ <https://www.mkm.ee/ministeerium-uudised-ja-kontakt/ministeerium-ja-ministrid/ministeeriumi-tutvustus-ja-struktuur>

IDENTITEEDIHALDUS JA eID

- **Siseministeerium** töötab välja identiteedihalduse ning Eesti kodaniku ja välismaalase isikut tõendava dokumendi väljaandmise poliitika.³⁹
- **Välisministeerium** tagab Eesti riigi ja isikute huvide kaitse välisriikides, sealhulgas võtab vastu isikut tõendavate dokumentide taotlusi ning väljastab isikut tõendavaid dokumente.⁴⁰
- **EASi ja KredExi ühisasutus** e-residendi programmi eest vastutajana loob tingimusi teenuste arenguks ja korraldab infovahetust e-residentidega.⁴¹

Erasektori poolelt on eID ökosüsteemi kaasatud:

- **Usaldusteenuse pakkuja**, kes on riigi partner usaldusteenuste valdkonnas isikut tõendavate dokumentide sertifikaatide väljastamisel ning sertifikaatidega seotud toimingutes.
- **Mobiilsideoperaatorid**, kes väljastavad mobiil-ID võimekusega SIM kaarte oma klientidele.
- **Finantsteenuste pakkujad**, kes on eID ökosüsteemi suurimad kasutajad.
- **Isikut tõendavate dokumentide tootja**, kes on riigi partner ID-1 vormis isikut tõendavate dokumentide kandjate tootmisel ning isikut tõendavate dokumentide isikustamisel.
- **Turvalise teenuse osutaja** dokumentide väljastamisel.

Valdkonnaga seotud e-teenuse pakkujad võivad olla nii avaliku kui ka erasektori asutused.

Eesti eID ökosüsteem on hästi toimiv ning intensiivselt kasutatav. Vahemikus 2018-2023 väljastati kokku üle 1,9 miljoni ID-kaardi ja üle 380 000 mobiil-ID (vt tabel 1). Viimase nelja aasta jooksul on püsivalt riiklike eID vahenditega antud keskmiselt 7 miljonit digitaalset allkirja kalendriaastas (vt tabel 2). Riigi allkirjastamisteenuse (SiGA) vahendusel kahe viimase aasta jooksul riiklike allkirjastamisvahenditega antud digitaalsete allkirjade arv ületab 3,5 miljonit digitaalset allkirja (vt tabel 4). Need numbrid näitavad, et Eesti eID ökosüsteemi kasutatakse aktiivselt ning on oluline panustada valdkonna arendamisse ning turvalisuse tagamisse. Samas tuleb arvestada asjaolu, et kui 2020. aastal moodustasid ID-kaardi ning mobiil-ID-ga antud allkirjad 94,8% antud digitaalsete allkirjade koguarvust, siis 2021. aastal oli see protsent 84,7% ning 2022. aastal 76%. Antud statistikat mõjutab Smart-ID-ga digitaalse allkirjastamise võimaldamine läbi DigiDoc tarkvara. ID-kaardi ja mobiil-ID-ga autentimiste arv läbi riikliku autentimisteenuse TARA jäi aastatel 2021 ja 2022 ligikaudu 19 miljoni autentimise piirimaile kalendriaastas (vt tabel 4), moodustades ligikaudu poole autentimiste kogumahust ning on aastaks 2023 tõusnud juba üle 22 miljoni autentimiseni. Lisaks sellele moodustab suure osa autentimiste koguarvust erasektori poolt väljaantava Smart-ID-ga läbi riikliku autentimisteenuse TARA teostatud autentimiste arv, moodustades 2023. aastal 57% autentimiste koguarvust (so. 27 094 512 autentimist).

³⁹ Isikut tõendavad dokumendid ja identiteedihaldus. Kättesaadav:

<https://www.siseministeerium.ee/tegevusvaldkonnad/tohus-rahvastikuhaldus/isikut-toendavad-dokumendid-ja-identiteedihaldus>

⁴⁰ <https://www.riigiteataja.ee/akt/114072023002>

⁴¹ <https://eas.ee/e-residentsus/>

IDENTITEEDIHALDUS JA eID

eID vahend	2018	2019	2020	2021	2022	2023
ID-kaardid	379 242	356 567	255 025	277 778	370 744	283 439
Aktiveeritud mobiil-ID	66 087	59 466	62 649	86 973	36 402	73 376
Kokku	445 329	416 033	317 674	364 751	407 146	356 815

Tabel 1. Vahemikus 2018-2023 väljastatud/aktiveeritud eID vahendid. Allikas: PPA (ID-kaardid)/SK ID Solutions AS (mobiil-ID).

eID vahend	2020	2021	2022	2023
ID-kaardid	5 697 151	5 427 878	4 748 964	4 229 407
Mobiil-ID	2 031 651	3 173 243	2 918 590	2 657 628
Kokku	7 728 802	8 601 121	7 667 554	6 887 035

Tabel 2. Vahemikus 2020-2023 läbi DigiDoc4 tarkvara ja DigiDoc mobiilirakenduse antud digitaalsed allkirjad. Allikas: RIA.

eID vahend	2022	2023
ID-kaardid	555 945	1 518 753
Mobiil-ID	632 356	801 900
Kokku	1 188 301	2 320 653

Tabel 3. 2022 ja 2023 Riigi allkirjastamisteenuse (SiGA) statistika. Allikas: RIA.

IDENTITEEDIHALDUS JA eID

eID vahend	2020	2021	2022	2023
ID-kaardid	5 169 199	11 091 501	10 998 229	13 283 898
Mobiil-ID	3 264 029	8 091 019	7 941 924	9 067 384
Kokku	8 433 228	19 182 520	18 940 153	22 351 282

Tabel 4. Vahemikus 2020-2023 riigi autentimisteenuse TARA kaudu tehtud autentimiste arv. Allikas: RIA.

Kuigi Eesti eID ökosüsteem on küllaltki lihtsalt kasutatav, siis tuleb strateegiliste suundade seadmisel arvestada ka kasutajate probleemidega, mis on tekkinud eID ökosüsteemi kasutamisel. Kui vaadata kasutajatoe pöördumiste statistikat perioodil aprill 2023 kuni oktoober 2023, siis vastavalt pöördumiste arvule on viis enim levinud pöördumise põhjust:

- 1) e-teenuste autentimine (autentimine ebaõnnestub), 2024 pöördumist.
- 2) Windows – tarkvara paigaldamine/uuendamise juhendamine, 1299 pöördumist.
- 3) Windows – mittetoetatud operatsiooni süsteemid, 1054 pöördumist.
- 4) e-teenustes allkirjastamine – allkirjastamine ebaõnnestub, 901 pöördumist.
- 5) DigiDoc4 klient – Minu eID – PIN koodid lukus/muutmine, 831 pöördumist.

09.12.2022 toimunud avaliku sektori ja erasektori sidusrühmade töötoa ning 22.08.2023 toimunud RIA eID osakonna väliseminari tulemusel sai kokku pandud eID ökosüsteemi SWOT analüüs, mis kaardistab Eesti eID ökosüsteemi tugevused, nõrkused, ohud ja võimalused (vt. joonis 3). Kokkuvõtvalt võib öelda, et Eesti eID ökosüsteemi tugevuseks on selle pikaajalisus, suur kasutajate hulk, lihtsus ja turvalisus, usaldusväärsus. Samas on olemasoleval ökosüsteemil ka hulgaliselt nõrkusi alates selle liigsest unikaalsusest lõpetades erinevate puuduvate võimekustega, mis vajavad väljaarendamist. Ohtudena toodi välja eriteadmistega inimressursi vähesus, üldise arhitektuurilise vaate puudumine, liigne sõltuvus konkreetsetest teenusepakujatest, kriisiolukordadeks valmisoleku puudumine ning erinevatest tehnoloogiatest tulenevad ohud. Võimalustena nähti eelkõige EL digiidentiteedikukrut, mobiilsetele platvormidele liikumist, teenuste pakkumise laiendamist erasektorile, edasi liikumist *identity matching*-u vallas ning võimalike uute isikusamasuse kontrollimiseks kasutatavate vahendite (sh biomeetrilised andmed) laialdasemat kasutuselevõttu.

IDENTITEEDIHALDUS JA eID



Joonis 3. eID ökosüsteemi tugevused, nõrkused, võimalused ja ohud.

Lisaks juba ülalkirjeldatule on valdkonna väljakutsed ja ohud kindlasti seotud ka Ukraina sõja ning sellel suunal toimivate arengutega. Juba 2022. aastal registreeriti näiteks rekordiline kogus teenustökestusründeid⁴². Lisaks suurenevad ründed kriitiliste infrastruktuuri, nagu seda on ka elektrooniline isikutuvastamine ja digitaalne allkirjastamise⁴³, vastu.

Füüsilised riskid muutuvad ohuhinnangutes reaalseteks. Rohkem tuleb arvestada ka tegelike füüsiliste rünnete võimalusega serveriruumidele. Suurenevad kesksete teenuste käideldavusnõuded. Järk-järgult suurenevad ka õngitsuste ja tarneahelaga seotud riskid.

Seoses uute ning väheküpsete tehnoloogiate kasutuselevõtuga kasvab oluliselt uute ning tundmatute nõrkuste hulk, mille mõju on raske hinnata. Seega muutub turvaanalüüside ja rahvusvaheliste turvameetodite rakendamine riiklikes lahendustes üha olulisemaks (CC, CSA skeemid jne.). Paraku on tegemist aeganõudva protsessiga ning EL on omalt poolt asunud ümber kujundama seniste struktuuride

⁴² Küberturvalisuse aastaraamat 2023. Kättesaadav: <https://www.ria.ee/media/2653/download>

⁴³ Hädaolukorra seadus. Kättesaadav: <https://www.riigiteataja.ee/akt/130062023022>

IDENTITEEDIHALDUS JA eID

nagu SOG-IS MRA tegevust (CC sertifikaatide vastastikku tunnustamise lepingu alusel loodud töörühmade tööd on oluliselt vähendanud jmt.). Paralleelselt lisanduvate nõrkustega ei kao ka vanad väljakutsed, vaid oluliseks saab nendele kiire reageerimine. **eID valdkonna vaates on näiteks kriitiliseks tagada valmisolek kõikide riiklike eID- kandjate kiireks väljavahetamiseks selle vajaduse ilmnemisel.**

Biomeetria kasutamine isikutuvastuslahendustes esitab väljakutse lahenduste turvalisusele ning toimekindlusele. Sellest tulenevalt tuleb hakkama saada uute väärkasutusjuhtudega identiteedihalduse valdkonnas ning ründeohuga, mis on suunatud just biomeetriliste isikutuvastuslahenduste vastu. Väljakutseks on kindlasti ka ühtsustatud turvalisuse hindamisreeglite, meetodite ja hindamisstruktuuride puudumine sellisel tasemel nagu näiteks on tänaseks välja kujunenud kiipkaartidega seotud lahenduste vastavushindamisel.

Jätkub intensiivne töö kvantarvuti kindla krüptograafia kasutuselevõtmiseks enne pädeva kvantarvuti tekkimist. Antud valdkonnas tegutsetakse Eestis nii siseriiklikult kui ka Euroopa Liidu üleselt, eelkõige Euroopa Liidu Küberturvalisuse Ameti (ENISA)⁴⁴ eestvedamisel. Turvaline kvantkommunikatsioon ja selle väljaarendamine on ka üheks Euroopa Liidu 2030. aasta digitaalsetest eesmärkidest.⁴⁵

Lisaks tuleb arvestada juba eID valdkonnas kasutusel olevate algoritmide ja võtmepikkuste aegumisega ning juba loodud digitaalselt allkirjastatud dokumentide pikaajalise säilitamise ning nende allkirjade tõestusväärtuse tagamisega. Eelkõige puudutab probleem neid digitaalselt allkirjastatud dokumente, mis on säilitustähtajaga 75 aastat ja enam.

⁴⁴ <https://www.enisa.europa.eu/>

⁴⁵ https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

Strateegilised suunad

Identiteedihalduse ja eID valdkonna keskmeks on kasutaja, kelleks võib olla eraisik, erasektori asutus või avaliku sektori kasutaja. Olenemata konkreetsest kasutajagrupist on üldiseks ootuseks, et eID ökosüsteem pakub usaldusväärse, töökindla, turvalise ning mugava lahenduse, mis toetab kasutajate igapäevaseid toiminguid olenemata kasutaja füüsilisest asukohast.⁴⁶ **Ideaalis peab ökosüsteem toimima taustal nähtamatult.**

Käesolev peatükk keskendubki konkreetsetele **strateegilistele suundadele ja valikutele** identiteedihalduse ja eID valdkonnas. Strateegilised suunad keskenduvad eelkõige Eesti eID ökosüsteemile hõlmates ka Euroopa Liidu konteksti. Eraldi on välja toodud üldised

põhimõtted ning seejärel valdkondlikud suunad identiteedihalduses, eID kandjate halduses, eID-ga seotud teenuste valdkonnas ning kompetentsikeskuse vaates erinevatest kasutajagruppidest lähtuvalt.

09.12.2022 toimunud töötoa tulemusena toodi välja järgmised olulised eID valdkonnad, mis kindlasti vajavad strateegia kontekstis lahtimõtestamist:

- Eesti olemasoleva eID ökosüsteemi jätkusuutlikkus Euroopa kontekstis.
- Volituste ja pääsuhalduste teema.
- Biomeetria ning biomeetrilised lahendused isikutuvastuses ning nende reguleerimine.
- Erivajadustega kasutajatele suunatud lahendused.
- Toimepidevuse tagamine ning riskihaldus.
- Kvantkrüptograafia ning kvantarvuti kindlad lahendused.
- eID sõltumatus kandjast.

⁴⁶ Ettevõtja Tanel on siinkohal vaid üks persoona.

“Eesti eID ökosüsteem on töökindel, turvaline, koosvõimeline ja mugav kasutada.”

“Tanel (45) on ettevõtja, abikaasa ja kahe tütre (7 ja 13 aastased) isa, kes peale koroonapandeemiat veedab ligikaudu 4-6 kuud aastast (novembrist aprillini) Hispaanias. Tanel ajab kõiki oma äriasju digitaalselt ning kasutab nii Eesti kui ka Hispaania poolt pakutavaid avalikke e-teenuseid talle Eesti poolt väljastatud eID vahendit kasutades. Ta sõlmib äripartneritega digitaalselt allkirjastades lepinguid ja korraldab ettevõtte rahaasju ning aruandlust digitaalselt. Taneli lapsed on distantsõppel ning saavad kogu vajaliku info e-kooli süsteemi vahendusel. Kohapeal on Taneli perel ka perearst, kellele on võimaldatud juurdepääs pere terviseandmetele juhuks, kui keegi pereliikmetest peaks arstiabi vajama. Üldiselt reisib pere sihtkohta lennukiga, kuid mõnikord võetakse ette ka reis autoga. Tanel ei mäleta, millal ta viimati juhiluba või isikut tõendavat dokumenti füüsiliselt kaasas kandis. Tanel on eluga rahul.”

- Konkurentsi võimalused usaldusteenuste valdkonnas.
- Kõrgel tasemel tunnustatud kaugtuvastuse lahendused.
- Keskkonnasõbralikud lahendused identiteedihalduse valdkonnas.

ÜLDISED PÕHIMÕTTED

Selles peatükis on välja toodud identiteedihalduse ja eID valdkonna olulisimad üldised strateegilised valikud ja põhimõtted, millest valdkonna arendamisel lähtutakse. Läbi üldiste põhimõtete sõnastamise on eesmärgiks luua üldine raamistik, tagades seeläbi valdkonna ühetaoline, jätkusuutlik ning stabiilne areng. Põhimõtete sõnastamisel on üle vaadatud 2018. aastal kokkulepitu ning täiendatud seda 09.12.2022 ning 14.11.2023 toimunud sidusrühmade kohtumistel arutatud suundadest lähtuvalt.

1 Üldised põhimõtted

- 1.1 Eesti eID ökosüsteem on kergesti kättesaadav, hästi toimiv, lõppkasutaja jaoks tasuta ning koosvõimeline teiste ökosüsteemidega. Aluspõhimõtted, millest lähtume on: turvalisus, töökindlus, privaatsuse kaitse, pidev areng, koosvõimelisus, innovatsioon ja kasutajale suunatus.
- 1.2 Toetame innovatsiooni ja uuenduslikkust ning julgeme piloteerida erinevaid lahendusi ja tehnoloogiaid hoides Eesti tugeva ja turvalise e-riigi mainet.
- 1.3 eID valdkonna lahenduste hankimisel tagame konkurentsi ning hangime lahendused turu parimatelt ja professionaalseimatelt pakkujatelt sh. vajaduste kaardistamisel kaasame ja kasutame ka erasektori kompetentsi ja teadmisi.
- 1.4 Kindlustame valdkonnas valmisoleku eID ökosüsteemi toimekindluse tagamiseks ning töötame avaliku sektori ja erasektori koostöös välja toimekindluse plaani koos maandamistegevustega. Samuti planeerime eelarve toimekindluse plaanist tulenevate tegevuste elluviimiseks.
- 1.5 Vaatame üle pädevused identiteedihalduse ja eID valdkonnas, et tagada selge rollijaotus. Vajadusel teeme vastavad muudatused õigusruumis seoses eIDAS 2.0 rakendamisega.
- 1.6 Rakendame rahvusvaheliselt kasutatavaid ja standardiseeritud komponente, et vähendada kasutatavate komponentide unikaalsust ja ühilduvusprobleeme.
- 1.7 Analüüsime identiteedihalduse ja eID valdkonna komponente, mida riik peab ja ei pea ise haldama ning mida on võimalik senisest enam rakendada erasektori toel.

2 Isikute tuvastamine

Isiku tuvastamisel ja isikusamasuse kontrollimisel lähtume lisaks Euroopa Liidu ja Eesti siseriiklikele regulatsioonidele Siseministeeriumi identiteedihalduse ja isikut tõendavate dokumentide poliitika põhialustest⁴⁷:

- isiku identiteedi määratleb riik;
- ühel isikul on üks identiteet;
- teise isiku identiteedi või isikut tõendava dokumendi kasutamine on keelatud;
- identiteedihaldus toimub riigi poolt ja tsentraliseeritult;
- nii füüsilise kui ka digitaalne isikut tõendav dokument on lahutamatu ja üheselt seotud dokumendi kasutaja identiteediga;
- digitaalse isikut tõendava dokumendi digitaalset tuvastamist ja digitaalset allkirjastamist võimaldavad sertifikaadid on üheselt seotud dokumendi kasutaja isikuandmetega;
- nii füüsilise kui digitaalse dokumendi andmed, sealhulgas digitaalset tuvastamist ja digitaalset allkirjastamist võimaldavad sertifikaadid, on avalikult kontrollitavad.

Lisaks eeltoodud põhialustele on identiteedihalduse ja eID valdkonnas oluliseks:

- 2.1 Isikukood on identiteedi alustalaks. Otsime alternatiive isikukoodi struktuuri muutmiseks, et selles esitatud andmed ei oleks otseselt seostatavad kasutaja isikuandmetega.
- 2.2 Jätkame suunda, kus riigi poolt tellitavate/väljastatavate eID-de tasemed on autentimisvahendi puhul „kõrge“ ja e-allkirja andmise vahend vastab QSCD tasemele.
- 2.3 Toetame ka madalama tagatistasemega (s.o. „märkimisväärne“) eID skeemide tunnustamist riigi siseselt ning ei sea piiranguid selle kasutamisel.
- 2.4 Võtame suuna, et riigist saab tõsikindla identiteedi osas teenusepakkuja ja partner erasektorile, et võimaldada erasektoril veelgi tõhusamalt kasutada riigi käes olevaid ning õiguslikul alusel väljastatavaid isikuandmeid.

3. Identiteedi kandjad ja teenused

- 3.1 Riik tagab kasutajatele vähemalt kahe teineteisest sõltumatu tehnilise lahendusega kõrge tagatistasemega eID vahendi olemasolu.
- 3.2 Tagame kasutajatele isiklikul otstarbel tasuta digitaalse allkirjastamise võimaluse ja sellega seotud riigipoolse digitaalse allkirjastamise tarkvara olemasolu.
- 3.3 Tagame krüpteerimisvõimekuse riigi poolt väljaantavate eID vahenditega.
- 3.4 Tagame riigi poolt tellitud eID ökosüsteemi arenduskomponentide tasuta olemasolu e-teenuste pakkujatele avatud lähtekoodi mudeli alusel.

⁴⁷ <https://www.siseministeerium.ee/tegevusvaldkonnad/tohus-rahvastikuhaldus/isikut-toendavad-dokumendid-ja-identiteedihaldus>

4. Turberiskide haldamine

- 4.1 Panustame infoturbe valdkonna (sh krüptograafia) ja eID tarkvara arenduse kompetentsi ja ekspertide järelkasvu kasvatamisse ja säilitamisse riigis.
- 4.2 Teeme kindlaks, millised kvantarvuti kindlad krüptograafia lahendused sobivad eID valdkonnas kasutamiseks ning tagame turul saadaoleva parima lahenduse rakendamise.
- 4.3 Hindame pidevalt küberturvalisuse olukorda ning selle võimalikku mõju eID valdkonnale ja võtame turvalisuse tagamiseks kasutusele asjakohased meetmed.
- 4.4 Korraldame regulaarselt ja erinevaid sidusrühmi hõlmavaid kriisiõppuseid eID valdkonnas.
- 4.5 Kõikide olemasolevate ja kasutusele võetavate tehnoloogiliste lahenduste puhul eID ökosüsteemis koostame riskianalüüsi ning pakume välja maandamisemeetmed.

5. Siseriiklik ja rahvusvaheline koostöö

- 5.1 Arendame koostöö järjepidevuse tagamiseks välja toimiva valdkondliku partnervõrgustiku.
- 5.2 Jätkame piiriülest koostööd naaberriikidega, et oleks tagatud vastastikune teenuste toimepidevus.
- 5.3 Osaleme ja panustame aktiivselt rahvusvahelistesse arendus- ning koostööprojektidesse ja võrgustikesse.
- 5.4 Osaleme eIDAS 2.0 regulatsiooni ning selle rakendusaktide väljatöötamise protsessis ning tagame Eesti huvide parima kaitse.
- 5.5 Tõhustame koostööd nii siseriiklikul kui ka rahvusvahelisel tasandil, muuhulgas:
 - 5.5.1 kaasame erasektorit valdkonnapõhistesse arendus- ja uurimistegevustesse;
 - 5.5.2 suurendame oma teadmist biomeetria ja kaugtuvastuse lahenduste valdkonnas (sh. õpime teiste riikide kogemusest);
 - 5.5.3 panustame koostöös erasektoriga valdkondlike standardite väljatöötamisse ning tagame riigi esindatuse eID valdkonna rahvusvahelistes töögruppides;
 - 5.5.4 parendame infovahetust avaliku sektori ja erasektori sidusrühmade vahel, mis on seotud rahvusvahelise suhtlusega (sh uute teadmiste jagamine).
 - 5.5.5 Juurutame avaliku sektori ja erasektori sidusrühmade infovahetuse tagamiseks regulaarse koostööformaadi (eID koordinatsioonikogu).

VALDKONDLIKUD SUUNAD

Valdkondlikud suunad keskenduvad neljale põhilisele suunale, milleks on isikutuvastus, identiteedi kandjad, eID ökosüsteemiga seotud teenused ning valdkonna kompetentsikeskus. Varasemalt on valdkonna strateegilise planeerimise lähtekohaks olnud erinevad väljakutsed ja nende võimalikud lahendussuunad. Käesolev dokument lähtub kliendikesksusest ning keskendub eID ökosüsteemi erinevatele kliendisegmentide väärtuspakkumisele. Siinkohal on oluline välja tuua kolm põhilist eID ökosüsteemi kasutajagrupperi:

- eraisikud

IDENTITEEDIHALDUS JA eID

- avaliku sektori asutused
- erasektor

Eelnimetatud kasutajagruppide ootused eID ökosüsteemi osas ning väljakutsed võivad osaliselt kattuda, kuid kindlasti on ka valdkondi, mis omavad tähtsust ainult konkreetse kasutajate rühma jaoks. Lisaks on Majandus- ja Kommunikatsiooniministeerium koostöös RIA-ga valdkondlikud suunad üle vaadanud ning jaganud need vastavalt prioriteetsuse astmele kolme gruppi (madal, keskmine ja kõrge). Tabelites on prioriteedid märgitud erineva taustavärviga järgmiselt:

- madal – roheline;
- keskmine – kollane;
- kõrge – punane.

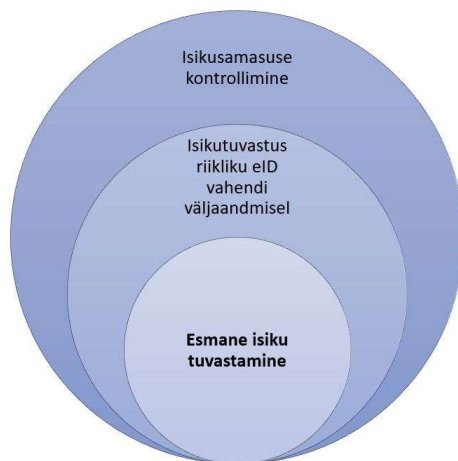
Isikutuvastus

Nagu juba eelnevalt mainitud, siis riiklik identiteedihalduspoliitika baseerub tsentraliseeritud ja tõsikindlal isikutuvastusel. Riigi poolt määratletud identiteet peab olema ajas muutumatu (va erandjuhud seaduslikul alusel) ja avalikult kontrollitav. Identiteedihaldusega seotud teenused peavad olema tõhusad, vähekoormavad nii riigile kui ka selle kasutajale. Samuti on oluline, et tuvastusprotsess on taaskasutatav, kvaliteetne, kindel ja efektiivne ning tagatud on teenuse paindlikkus kriiside lahendamisel.

Isikute tuvastamine hõlmab endas kolme peamist kihti (vt joonis 4):

- 1) **Esmane isiku tuvastamine** – protsess, mille käigus toimub esialgne andmehõive (biomeetria, nimi, isikukood, teise riigi ID) ja esmase identiteedi loomine;
- 2) **Isikutuvastus (riikliku) eID vahendi väljaandmisel** - isiku tuvastamine kas riikliku (ID-kaart, Mobiil-ID) või erasektori (näiteks Smart-ID) tuvastusvahendi välja andmisel;
- 3) **Isikusamasuse kontrollimine** – isiku tõendamine kolmandate osapooltega suhtluses.

IDENTITEEDIHALDUS JA eID



Joonis 4. Isikutuvastamise kolmeastmeline mudel.

Isikutuvastuse puhul lähtume alljärgnevatest strateegilistest suundadest.

Kasutajad	Suunad
Kõik kasutajad (eraisikud, avalik sektor, erasektor)	Kirjeldame ja reguleerime biomeetria ja biomeetriliste andmete turvalise kasutamise identiteedihalduse valdkonnas.
	<ul style="list-style-type: none"> • Arendame välja kõrgele tagatistasemele vastava lahenduse isikute kaugtuvastuseks.
	<ul style="list-style-type: none"> • Lepime kokku kas ja kuidas toimub eraskeemide teavitamine piiriüleseks kasutamiseks. • Toetame vastendamise (<i>identity matching</i>) võimekuse väljaarendamist Balti- ja Põhjamaade tasandil.
Eraisikud	Tagame turvalise tarkvara arvutis ja nutiseadmes autentimiseks ja digiallkirjastamiseks ning ID-1 formaadis dokumentide kontaktivaba kasutamise.
	<ul style="list-style-type: none"> • Arvestame erinevate kasutajagruppide vajaduste ja ootustega.
Avalik Sektor	Vajadusel vaatame üle ja muudame identiteedihalduse valdkonna tervikliku vastutusmudeli.
	<ul style="list-style-type: none"> • Koostame identiteedihalduse ja eID valdkonna tervikliku rahastamise vaate, et tagada valdkonna arenduste ja turvalisuse jätkusuutlikkus ning toimekindlus.

IDENTITEEDIHALDUS JA eID

	<ul style="list-style-type: none"> Lepime kokku ühised suunad ja valdkonnad (huvid, mida Eesti soovib kaitsta), millesse panustame erilise tähelepanuga EL-i ja rahvusvahelisel tasandil.
Erasektor	<ul style="list-style-type: none"> Teeme koostööd rahvusvaheliste isikutuvastust pakkuvate partneritega ning oleme avatud vahendamaks EL-i välise riikide eID-sid Eesti e-teenuste pakkujatele.

Identiteedi kandjad

Identiteedi kandjate puhul on hõlmatud nii digitaalset tuvastamist kui ka digitaalset allkirjastamist võimaldavad vahendid. Tulenevalt olemasolevatest ning sõlmimisel olevatest lepingutest jäävad ID-1 formaadis eID kandjad kindlasti vähemalt järgnevas kümneks aastaks kasutusele. Samas tuleb uute hangete ettevalmistamisel võtta suund füüsilistest kandjatest sõltumatute eID lahendustele.

Kasutajad	Suunad
Kõik kasutajad (eraisikud, avalik sektor, erasektor)	Arendame välja Euroopa digiidentiteedikukru lahenduse, mis on koosvõimeline EL raamistikuga.
	<ul style="list-style-type: none"> Hindame ühe seadme liigsest sõltuvusest tingitud riske ja pakume välja võimalikud maandamismeetmed.
	<ul style="list-style-type: none"> Võtame suuna saavutamaks eID sõltumatuse konkreetsetest identiteedi füüsilistest kandjatest (nn. vahendivabadus).
	<ul style="list-style-type: none"> Üldjuhul lähtume põhimõttest, et riik ei telli samale tehnoloogiale dubleeritud eID lahendusi. Tagame erinevate tehnoloogiate laialdasema toe (üks tehnoloogia - üks eID).
	<ul style="list-style-type: none"> Tagame tehnilise lahenduse eID kandja sertifikaatide/kiibirakenduse uuendamiseks üle avaliku interneti (nt turvanõrkuste lahendamine, paikamine).
Eraisikud	<ul style="list-style-type: none"> Arvestame erinevate kasutajagruppide vajaduste ja ootustega.
	<ul style="list-style-type: none"> Võimaldame eID kandja turvakoodide edastamist elektrooniliselt, kui inimene on autentunud end teise kõrgel tasemel eID vahendiga.⁴⁸
	<ul style="list-style-type: none"> Võimaldame eID kandja ja/või selle sertifikaatide tühistamist elektrooniliselt, kui inimene on tõsikindlalt tuvastatud.

⁴⁸ Tõsikindlalt on inimene tuvastatud kasutades teist kõrget eID vahendit, nt mobiil-ID-d.

IDENTITEEDIHALDUS JA eID

	<ul style="list-style-type: none"> Võimaldame eID kandja väljastamist ilma isikliku ilmumiseta dokumendi väljaandja juurde või Eesti välisesindusse. Arendame välja riikliku äpipõhise eID vahendi e-residentidele.
Avalik Sektor	<ul style="list-style-type: none"> Loome võimaluse avaliku sektori jaoks uute e-teenuste pakkumiseks läbi Euroopa digiidentiteedikukru lahenduse. Enne identiteedihalduse ja eID valdkonna hangete väljakuulutamist teostame võimalusel ja vajadusel igakordselt eelanalüüsi, milles on kajastatud hinnang asjade ja teenuste koos ning eraldi hankimise otstarbekusele (sh autentimist ning digitaalset allkirjastamist võimaldavate lahenduste koos/eraldi hankimisele).
Erasektor	<ul style="list-style-type: none"> Loome võimaluse erasektori jaoks uute e-teenuste pakkumiseks läbi Euroopa digiidentiteedikukru lahenduse.

eID ökosüsteemi teenused

eID ökosüsteemi teenused hõlmasid Valge Raamatu eelmises redaktsioonis tahteavalduse kinnituse, infoteenuse ning rahvastikusündmuste käsitlemise ja kasutuse. Tahteavalduse kinnitus hõlmab oma sisult nii autentimise kui ka digitaalse allkirjastamise. Iseäranis autentimine – kui kõige laialdasema kasutusega teenus – peab üha enam arvestama kliendi ootustega. Kasutajad ootavad mugavust, kiirust, privaatsust ja usaldusväärsust.

Tahteavalduse kinnituse puhul on oluliseks alljärgnevad strateegilised suunad.

Kasutajad	Suunad
Kõik kasutajad (eraisikud, avalik sektor, erasektor)	<ul style="list-style-type: none"> Analüüsime volituste teemat ning proovime leida lahenduse volituste küsimuse piiriüleseks lahendamiseks.
	<ul style="list-style-type: none"> Tagame turuküpsuse ning pakume valmis lahendusi (DSS, eID draiverid jne.) sidusrühmadele kasutamiseks.⁴⁹
	<ul style="list-style-type: none"> Tagame EL-i sisese veebipõhise autentimisteenuse toimimise.
	<ul style="list-style-type: none"> Analüüsime kas ja millises ulatuses oleme valmis võimaldama kasutada Eesti eID kasutajatel oma

⁴⁹ Õigusaktidest tulenevad kohustused ning kriitilised vead on siiski kõrge prioriteediga ehk punased.

IDENTITEEDIHALDUS JA eID

	riiklikku eID-d suurte rahvusvaheliste teenusepakkujate juures (Facebook, eBay, Google jne).
	<ul style="list-style-type: none"> Täiustame elektrooniliste allkirjade valideerimise võimekust ning viime selle vastavusse kasutajate vajadustega.
	<ul style="list-style-type: none"> Säilitame Eestis enamlevinud digitaalsete allkirjade valideerimise võimekuse <i>off-line</i>-s.
Eraisikud	<ul style="list-style-type: none"> Soodustame tasuliste teenuste väljaarendamist üksikisikule.
Avalik Sektor	<ul style="list-style-type: none"> Teeme endast oleneva, et võimaldada uute usaldusteenuse pakkujate turule sisenemist. Analüüsime riikliku julgeoleku tagamise eesmärgil alternatiivsete kvalifitseeritud usaldusteenuse pakkujate kaasamist ja kasutamist. Analüüsime kahe sertifitseerimis- ja usaldusteenuse pakkuja samaaegse tegutsemise mõjusid eID ökosüsteemile.
Erasektor	<ul style="list-style-type: none"> Tagame riigi poolt tasuta baasteenused ja komponendid, et erasektor saaks neid oma teenuste osutamisel kasutada. Arendame välja kesksete teenuse (näiteks riigi keskne autentimisteenus TARA) pakkumise võimekuse erasektorile. Jätkame praktikat, kus riik võimaldab erasektoril tasuliste teenuste väljaarendamist.

Infoteenusteks loetakse need teenused, mille läbi tagatakse riikliku identiteedi aktiivne kasutus. Infoteenusteks loetakse e-posti aadress (eesti.ee) ning rahvastiku/perekonna sündmuste kohta käivad andmed. Rahvastikusündmuste käsitlemise ja kasutuse puhul on tegemist füüsilise isiku atribuutide ja nende muutuste (automaatne või nõusolekupõhine) levitamise. Kuna käesolev identiteedihalduse ja eID valge raamat keskendub rohkem eID-ga seonduvale, siis rahvastikusündmuste käsitlemise ja kasutuse strateegilisi suundi kujundab Siseministerium ning seetõttu käesolevas dokumendis seda eraldiseisvalt ei käsitleta, vaid teiste valdkondade või teemade (näiteks *identity matching*) raames.

Infoteenuste osaks oleva eesti.ee e-posti teenuse vaates on oluline silmas pidada, et alates 01.11.2023 suleti eesnimi.perenimi@eesti.ee e-posti teenus. Selle tulemusel ei ole eelnimetatud kujul võimalik eesti.ee e-posti

IDENTITEEDIHALDUS JA eID

aadressi kasutada. Kasutusele jäid isikukood@eesti.ee e-posti aadressid, mille kaudu avaliku sektori asutused saavad eraisikutega ametlikku kirjavahetust pidada.⁵⁰

Ametlik e-post on andmevahetusteenus. Teenuse tarbijateks on kõik kolm kliendi gruppi (füüsilised isikud, erasektor, avalik sektor). Erasektori puhul on teenuse tarbimise eelduseks füüsilise isiku nõusolek. Teenust iseloomustavad järgmised märksõnad:

- tegemist on isiku ametliku kontaktpunktiga (digi)maailmas;
- hõlmab nii elektroonilise kui ka füüsilise kasutuse;
- avalik ja mõeldud ametlikuks infoedastuseks;
- avatud lisateenustele.

Kompetentsikeskus

RIA vastutab e-teenuste arendajatele ja pakkujatele suunatud eID tarkvaraliste komponentide eest ning tagab toe arendajatele. Lisaks tagab RIA eID tarkvara kasutajatoe teenuse kasutajale. RIA on ka eID valdkonna eestkõneleja ja seisukohtade kujundaja konsulteerides teisi (riigi)asutusi Eestis eID kasutusele võtmisel nii siseriiklikuks kui ka piiriüleseks kasutamiseks ning vastutab koostöös sidusrühmadega rahvusvaheliste eID koosvõime ehk riikide ülese tarkvaralise lahenduse toimimise, arengu ja halduse eest. Eeltoodust tulenevalt on oluliseks ka kompetentsikeskuse funktsioon, mis toetab olemasoleva eID ökosüsteemi parimal viisil toimimist ning parimate valikute tegemist selle arendamisel.

Kasutajad	Suunad
Kõik kasutajad (eraisikud, avalik sektor, erasektor)	<ul style="list-style-type: none">• Analüüsime seadmete identiteedi seost eID ökosüsteemiga ning sellega seotud edasiste tegevuste vajadust.
	<ul style="list-style-type: none">• Hindame pidevalt tehnoloogiatrendide mõju olemasolevale eID ökosüsteemile.
Avalik Sektor	<ul style="list-style-type: none">• Identiteedihalduse ning isikut tõendavate dokumentide valdkonna hangetel oleme avatud uutele lahendustele ja tehnoloogiatele, hoiame end kursis ning kutsume ettevõtteid ja teadusasutusi neid lahendusi riigile presenteerima.

⁵⁰ <https://www.eesti.ee/et/aliaste-sulgemine/aliaste-sulgemine>

Rakendamine

Identiteedihalduse ja eID valdkonna strateegilised suunad täpsustavad Eesti digiühiskonna arengukavas sätestatud ning kirjeldavad eID valdkonna visiooni vähemalt järgneva viieks aastaks. Seega saavad kõik eID ökosüsteemi sidusrühmad toetuda oma planeerimisprotsessis identiteedihalduse ja eID valdkonna Valge Raamatule ning selles toodud põhimõtetele.

2024. aasta jooksul tuleb välja töötada ka identiteedihalduse ja eID valdkonna Valge Raamatu rakenduskava, kus kirjeldatakse ära strateegilise suunaga seotud detailsemad tegevused, lepitakse kokku vastutajad ning indikatiivsed tähtajad. Rakenduskava on identiteedihalduse ja eID valdkonna Valge Raamatu lisaks, mida nii avaliku sektori kui ka erasektori sidusrühmad saavad oma tööplaanide koostamisel aluseks võtta.

Selleks, et identiteedihalduse ja eID valdkonna Valge Raamat ei jääks ainult mõteteks paberil, on vajalik selles kirjeldatud põhimõtete järjepidev ülevaatamine ning vajadusel uuendamine. Selleks peab toimuma vähemalt kord aastas sidusrühmadega sisuline strateegiline arutelu, mille eestvedajaks on RIA. Täpne kohtumise formaat ei ole piiritletud ning see võib toimuda ka mõne juba olemasoleva koostööformaadi raames (näiteks eID koordinatsioonikogu). Oluline on see, et valdkonna strateegiliste suundadega tegeletaks teadlikult ning regulaarselt.

Kasutatud allikad

KASUTATUD ÕIGUSAKTID

- 1) Euroopa Parlamendi ja nõukogu määrus, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega. Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52021PC0281>
- 2) Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte. Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52021PC0206>
- 3) Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv). Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32022L2555&qid=1693222236585>
- 4) Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2065, mis käsitleb digiteenuste ühtset turgu ja millega muudetakse direktiivi 2000/31/EÜ (digiteenuste määrus). Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32022R2065>
- 5) Politsei- ja Piirivalveameti põhimäärus.
Kättesaadav: <https://www.riigiteataja.ee/akt/112112022004>
- 6) Riigi Infosüsteemi Ameti põhimäärus.
Kättesaadav: <https://www.riigiteataja.ee/akt/103102023003>
- 7) Siseministeriumi infotehnoloogia- ja arenduskeskuse põhimäärus. Kättesaadav: <https://www.riigiteataja.ee/akt/126112022002>
- 8) Välisministeriumi põhimäärus. Kättesaadav: <https://www.riigiteataja.ee/akt/114072023002>
- 9) E-identimise ja e-tehingute usaldusteenuste seadus.
Kättesaadav: <https://www.riigiteataja.ee/akt/125102016001>
- 10) Hädaolukorra seadus. Kättesaadav: <https://www.riigiteataja.ee/akt/130062023022>
- 11) Isikut tõendavate dokumentide seadus. Kättesaadav: <https://www.riigiteataja.ee/akt/120062022057>

MUUD ALLIKAD

- 12) Valge Raamat. Identiteedihaldus ja isikut tõendavad dokumendid 1.0. Kättesaadav: <https://www.ria.ee/media/2431/download>
- 13) Digital Economy and Society Index 2018 Report. Kättesaadav: <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-2018-report>
- 14) Digitaalmajanduse ja -ühiskonna indeks (DESI) 2022. Kättesaadav: <https://digital-strategy.ec.europa.eu/et/library/digital-economy-and-society-index-desi-2022>
- 15) mRiik. Kättesaadav: <https://www.ria.ee/riigi-infosusteem/masinoppe-ja-keeletehnoloogia-lahendused/mriik>

IDENTITEEDIHALDUS JA eID

- 16) The Rise of Integrated Identity Platforms. Insight Report. Kättesaadav: <https://liminal.co/reports/the-rise-of-integrated-identity-platforms/>
- 17) Tsap, V., Lips, S., Draheim, D. (2020). Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. In: Kõ, A., Francesconi, E., Kotsis, G., Tjoa, A., Khalil, I. (eds) Electronic Government and the Information Systems Perspective. EGOVIS 2020. Lecture Notes in Computer Science(), vol 12394. Springer, Cham. https://doi.org/10.1007/978-3-030-58957-8_12
- 18) Kaugtöö analüüs 2022. Kättesaadav: <https://www.mkm.ee/media/9111/download>
- 19) Digital Signature Service.
Kättesaadav: <https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html#specificities-of-signature-creation-in-different-signature-formats>
- 20) The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. Kättesaadav: <https://link.springer.com/article/10.1007/s43681-021-00077-w>
- 21) Krüptoalgoritmid ning nende tugi teekides ja infosüsteemides. Kättesaadav: <https://www.ria.ee/media/3041/download>
- 22) EU/EEA Trusted List Browser. Kättesaadav: <https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home>
- 23) The EU Digital Identity Wallet. The Architecture and Reference Framework. Kättesaadav: <https://github.com/eu-digital-identity-wallet>
- 24) EU Digital Identity: 4 projects launched to test EUDI Wallet. Kättesaadav: <https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet>
- 25) Eesti infoturbestandard. Kättesaadav: <https://eits.ria.ee/>
- 26) Declaration from the Nordic and Baltic ministers of digitalisation on cross-border identity matching in the region. Kättesaadav: <https://www.norden.org/en/declaration/declaration-nordic-and-baltic-ministers-digitalisation-cross-border-identity-matching>
- 27) Electronic Signatures and Infrastructures (ESI). JAdES digital signatures. Kättesaadav: https://www.etsi.org/deliver/etsi_ts/119100_119199/11918201/01.01.01_60/ts_11918201v010_101p.pdf
- 28) Digital Identity Standards. Kättesaadav: <https://www.enisa.europa.eu/publications/digital-identity-standards>
- 29) Isikut tõendavad dokumendid ja identiteedihaldus. Kättesaadav: <https://www.siseministeerium.ee/tegevusvaldkonnad/tohus-rahvastikuhaldus/isikut-toendavad-dokumendid-ja-identiteedihaldus>
- 30) E-residentsus. Kättesaadav: <https://eas.ee/e-residentsus/>
- 31) Küberturvalisuse aastaraamat 2023. Kättesaadav: <https://www.ria.ee/media/2653/download>
- 32) Europe's Digital Decade: digital targets for 2030. Kättesaadav: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en
- 33) Lips, S., Pappel, I., Tsap, V., Draheim, D. (2018). Key Factors in Coping with Large-Scale Security Vulnerabilities in the eID Field. In: Kõ, A., Francesconi, E. (eds) Electronic Government and the

- Information Systems Perspective. EGOVIS 2018. Lecture Notes in Computer Science(), vol 11032. Springer, Cham. https://doi.org/10.1007/978-3-319-98349-3_5
- 34) Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017, October). The return of coppersmith's attack: Practical factorization of widely used rsa moduli. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1631-1648).

Lisa 1 - Sõnaraamat

Kuna eID valdkond hõlmab erinevaid sidusrühmi nii avalikust sektorist kui ka erasektorist, siis on äärmiselt oluline, et strateegiliste suundade kokkuleppimine toimuks ühetaolistel semantilistel alustel. Juba varasemalt on elavat diskussiooni tekitanud teenustega seotud mitmed mõisted, mida valdkonnas kasutatakse, kuid mille sisu ei ole täpselt piiritletud ega üheselt arusaadav. Valge Raamat on ka dokumendiks, mis fikseerib ja sisustab valdkonnas enimkasutatavad terminid ning vajadusel mõtestab need ümber.

- **eID** – elektrooniline identiteet, elektrooniline vahend isiku või organisatsiooni eristamiseks teistest ning identiteedi tõendamiseks.
- **eIDAS määrus**- Euroopa Parlamendi ja EL Nõukogu määrus (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul.
- **eIDAS 2.0** - Euroopa Parlamendi ja EL Nõukogu määrus, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega.
- **EUDIW/EL digiidentiteedikukkur** – eIDAS 2.0 sätestatud eID vahend, mis võimaldab kasutajal turvaliselt salvestada, hallata ja kinnitada oma identiteedi andmeid ja elektrooniliste atribuutide tõendeid, esitada neid taotluse korral seotud isikutele ja teistele EL digiidentiteedikukkrutele ja luua kvalifitseeritud e-allkirju ja e-templeid.
- **ID-1 formaadis dokument** - ISO/IEC 7810 standardile vastavas formaadis ning isikut tõendavate dokumentide seaduse (ITDS) § 2 lõike 2 punktides 1, 1¹, 1² nimetatud isikut tõendav dokument.
- **Isikut tõendav dokument** – ITDS § 2 lõikes 2 nimetatud dokument.
- **Identiteedi kandja** – isiku või organisatsiooni identiteedi eristamise ja tõendamise abivahend teenuste kasutamiseks. Nii füüsiline kui ka digitaalne (eID kandja), sealhulgas isik ise. Kandjate puhul eristatakse nii füüsilisi kui ka elektroonilisi kandjaid ning riiklikult tunnustatud ja/või väljastatud kandjaid ning kolmandate isikute poolt väljastatud kandjad (sh Google, FB).
- **Infoteenus** – teenus, mille läbi tagatakse riikliku identiteedi aktiivne kasutus ja laialdane teadlikkus.
- **Identiteedi kandjate haldus** – identiteedi kandja väljastamine, kehtivuse tõendamine, elutsükli haldus.
- **Kliendid** – identiteedihalduse ja isikut tõendavate dokumentide valdkonna teenuste tarbijad ja teenuse pakujad, mis jagunevad kolmeks: füüsilised isikud kui teenuste tarbijad; avalik sektor ja ametnikud – siinkohal on mõeldud kõiki avaliku sektori asutusi, kes pakuvad ja/või tarbivad identiteedihaldusega seotud teenuseid; erasektor – erasektori ettevõtted, kes pakuvad ja/või tarbivad identiteedihaldusega seotud teenuseid.
- **NFC (Near Field Communication)** – Lähivälja kontaktivaba tehnoloogia.
- **PKI (Public Key Infrastructure)** – avaliku võtme taristu.
- **Reisidokument** – ITDS § 2 lõikes 2 punktides 2-8 nimetatud dokument.
- **QSCD (Qualified Signature Creation Device)** – Kvalifitseeritud allkirja andmise vahend, mis vastab EL määruse 910/2014 (eIDAS) kõrgeimale võimalikule tasemele.
- **Vastendamine (i.k. identity matching)** – protsess, mille käigus isiku isikusamasust kontrollitakse piiriülel digitaalsete teenuste kasutamisel selles riigis varasemalt registreeritud andmete kaudu.