

Eesti e-identiteedi ökosüsteem

Ülevaade

Version 1.4

D-16-388

Sisukord

1 Sissejuhatus.....	5
1.1 Eesmärk	5
1.2 Mõisted ja lühendid	5
1.2.1 Kasutatud mõisted ja terminid.....	5
1.2.2 Kasutatud lühendid	7
1.3 Ülevaate struktuur	9
1.4 Eesti eID ökosüsteemi erilisus ja erinevused.....	9
1.4.1 Ajalooline taust	9
1.4.2 Eriline kasutuskeskkond	10
1.4.3 Tavad ja piirangud	11
2 Identiteedi mõiste ja e-identiteedi ökosüsteemi olemus	14
2.1 eID ökosüsteemi käsitluse üldpõhimõtted	15
2.2 Identiteet ja selle kasutamise vahendid	15
2.2.1 Alusidentiteet.....	15
2.2.2 Isikukood	15
2.2.3 Isikukoodi omadused	16
2.2.4 Isikukoodi päritolu.....	16
2.2.5 Isikukoodi privaatsus.....	17
2.3 eID-vahendid.....	17
2.3.1 ID-kaart.....	17
2.3.2 Mobiil-ID.....	17
2.3.3 Smart-ID	18
2.4 eID-vahendi sisu.....	18
2.5 eID-vahendite omavaheline suhe.....	18
2.6 Sertifikaadid	19
3 Valdkonnad ja vastutajad.....	20
3.1 Siseministeerium	20
3.2 Justiits- ja Digiministeerium	20
3.3 Välisministeerium.....	20
3.4 Erasektori eID-vahendite pakkujad	21
3.5 Riigi Infosüsteemi Amet.....	21
3.5.1 Küberturvalisuse keskus.....	21
3.6 Politsei- ja Piirivalveamet.....	22

3.7	Siseministeriumi infotehnoloogia- ja arenduskeskus (SMIT)	22
3.8	Usaldusteenuse osutajad	22
3.8.1	SK ID Solutions AS.....	23
3.8.2	Zetes Estonia OÜ	23
3.9	Ökosüsteemi muud osalised	23
3.9.1	Vahendite tootjad ja personaliseerijad	23
3.9.2	Vahendite väljastajad	23
3.9.3	Kasutaja	24
3.9.4	E-teenuste osutajad	24
4	Eesti eID ökosüsteemi teenused.....	25
4.1	Põhiteenused	25
4.1.1	Lõppkasutajateenus	25
4.1.2	Liidestatud ja tootestatud universaalteenus	26
4.1.3	Koosvõimeteenus.....	27
4.2	Tugiteenused	27
4.3	Abitoimingud	28
5	E-identiteedi kasutusjuhud ja integratsioon	29
5.1	Autentimine	29
5.2	Digiallkirja andmine.....	30
5.2.1	Digiallkirja loomine.....	32
5.2.2	Digiallkirja valideerimine.....	34
5.3	Krüpteerimine.....	36
Lisa A.	E-identiteedi ökosüsteemi normatiivsed raamid.....	38
A.1.	Isikut tõendavate dokumentide seadus	38
A.2.	E-identimise ja usaldusteenuste määrus (eIDAS).....	39
A.2.1.	E-identimise ja e-tehingute usaldusteenuste seadus	41
A.3.	Teenuste turve.....	41
A.3.1.	Hädaolukorra seadus	41
A.3.2.	NIS direktiiv	42
A.3.3.	Küberturvalisuse seadus	42
A.3.4.	Eesti infoturbestandard E-ITS ja E-ITSi määrus.....	42
Lisa B	E-identiteedi ökosüsteemi tehnilised raamid	44
B.1	eID-vahendid ja nende võimalused.....	44
B.1.1	Standardid ja tootjad	46
B.2	Digiallkirja andmise tehnilised vahendid	46

B.3	Tehnilised normid.....	48
B.3.1	eIDASi rakendusaktid	48
B.3.2	Tehnilised ja korralduslikud standardid	49
Lisa C.	Eesti eID ökosüsteemi põhinõuded (vastavustabel)	53

Viited	58
---------------	-----------

1 Sissejuhatus

1.1 Eesmärk

See ülevaade on kirjutatud Riigi Infosüsteemi Ameti (edaspidi RIA) tellimusel ning selgitab Eestis toimiva e-identiteedi (edaspidi eID) ökosüsteemi ülesehitust, korraldust ja kasutust. Ülevaade on mõeldud lugemiseks kõigile, kes soovivad mõista, millest koosneb Eesti eID ökosüsteem, millised on selle toimimispõhimõtted ja piirangud, kuidas ta praktikas toimib ning missugused riigiasutused ja erafirmad on selles koosluses tegevad.

Ülevaade on valminud 2025. aasta suvel ning selle aluseks on tol hetkel eID-teenuste turul valitsenud olukord ja kehtinud õigusaktid. Teenusepakkujate, vahendite jms lisandumisega võib see osalt minetada oma ajakohasuse.

Ülevaate mõned osad (Lisa C) on suunatud avaliku sektori asutustele, kes peavad tagama oma IT-süsteemide ühtesobivuse ja ühilduvuse senise Eesti eID ökosüsteemiga (vt 2017. a autentimismormatiiv [1], jaotis 5) ning selgitama oma IT-partneritele, milles täpselt ühilduvus seisneb või kuidas seda realiseerida.

1.2 Mõisted ja lühendid

E-identiteedi ökosüsteemi ülevaates esinevaid mõisteid ja termineid tarvitatakse üldjuhul vastavuses andmekaitse ja infoturbe leksikoniga **AKIT** [2], mida haldab Cybernetica AS. Leksikoni algne eesmärk oli aidata tõlgendada erialaseid ingliskeelseid rahvusvahelisi standardeid ja muid juhendmaterjale, mistõttu on märksõnade allikaks põhiosas ISO, IEC, IEEE jm standardid. Lisaks eriterminitele sisaldab leksikon ka standardite ja juhendmaterjalide tekstides sagedasi mitmetähenduslikke sõnu, mille õige tõlgendamine on sisu mõtestamiseks oluline.

Ülevaates kasutatavad terminid on esitatud järgmisel kujul: mõiste, selle ingliskeelne vaste, mõiste selgitus ja kommentaarid tava- ja oskuskeeles kasutusel olevate alternatiivsete terminite ning võimalike tõlgendusprobleemide kohta.

1.2.1 Kasutatud mõisted ja terminid

Ajatempel (*timestamp*) – andmeüksus, mis näitab sündmuse toimumise aega, näiteks templijäljendina või logielemendina, ning kinnitab sellega digitaalse objekti eksisteerimist teatud ajahetkel

Autentimine (*authentication*) – identiteediväite kontrollimise protsess: üks kasutaja, süsteem või muu olem¹ kontrollib teise olemitõendava identiteedi tõesust, aluseks tavaliselt mingi spetsiifiline esitatud teave (parool), ese (kiipkaart või muu turvatõend), eristav püsitunnus (biomeetrik) või eristav asukoht (aadress)

Digitaalallkiri – ka **digiallkiri**, tehnilises mõistes **digitaalsignatuur** (*digital signature*): andmete võltsimatu matemaatiline teisend, mis võimaldab tõestada andmeallika autentsust, kontrollida

¹ ISO/IEC 2382-36: igasugune konkreetne või abstraktne miski, mis eksisteerib, eksisteeris või võiks eksisteerida, koos nende millegite vaheliste seostega. Näiteid: inimene, objekt, sündmus, idee, protsess vm.

andmete terviklust, tagada sõnumi saatmise salgamatust. Levinud meetodites luuakse digiallkiri räsifunktsioonidega² ja avaliku võtmega krüptograafiaga³; võib täita allkirja funktsiooni.

Eesti keel eristab signeerimist (kui tehnilist toimingut) digiallkirja andmisest – toimingust, millel on juriidiline tähendus. Digiallkirja andmine on omakäelisega võrdsustatud e-allkirja andmine. „Digiallkirja“ mõiste Eestis on EUTSi kaudu võrdsustatud eIDASis kirjeldatud kvalifitseeritud taseme elektroonilise allkirjaga (QES).

E-identiteet (*e-identity, electronic identity*) – kitsamas kontekstis digitaalandmed, mis üheselt kirjeldavad isikut või muud olemit. Selle sünonüümina kasutatakse eriti võõrkeelsete allikate tõlgetes ka „digitaalidentiteeti“, mis avaramas tähenduses kirjeldab igasugust võrgus olevat teavet isiku ja ta seoste kohta: autentimisteave, isikuteave, identifikaatorid, digijäljed.

eIDAS – Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul. eIDASi määruse eesmärk on lihtsustada rahvusvahelist digiteenuste kasutamist: kui kõikidele teenusepakkujatele ning avalikele asutustele kehtivad ühesugused nõuded, toimimisalused ja põhimõtted, on võimalik tagada usaldusteenuste võrreldavus.

E-identimine (*e-identification*) – isiku või muu olemi identiteedi ühetähenduslik määramine elektrooniliste vahenditega. Mitmed ELi liikmesmaad võimaldavad oma kodanikele elektroonilist identimist kiipkaartide, mobiiltelefonide või muu tehnoloogiaga.

ID-kaart (*ID-card*) – ID-kaardi terminit kasutatakse Eestis erinevat moodi. Ühel juhul kasutatakse terminit kitsamalt, tähistamaks vaid isikutunnistust. Teise variandina kasutatakse terminit laiendatud tähenduses, ID-kaarti kui platvormi, hõlmates erinevaid digitaalset kasutust võimaldavaid dokumente, milleks on:

- isikutunnistus,
- elamisloakaart,
- diplomaatiline isikutunnistus,
- e-residendi digitaalne isikutunnistus,
- digitaalne isikutunnistus ehk digi-id (väljaandmine lõpetatud alates 01.05.2025, kuid väljaantud dokumente saab kasutada kehtivusaja lõpuni).

Terminid ID-kaart kasutatakse siin laiendatud tähenduses, välja arvatud juhtudel, kus on märgitud teisiti (kirjutatud dokumendi tüüp eraldi välja või lisatud täpsustus, et on mõeldud ID-kaarti kui isikutunnistust).

Identiteet (*identity*) – ISO/IEC 24713 kohaselt isiku identiteet tavalises tähenduses - atribuudid, mille abil identiteeti määratleda võivad olla nimi, isiksuse või välimuse aspektid, rakenduse ja lõppkasutaja vaheline tehingulugu, rahvus, haridusandmed, töandaja, teabeload, rahalised ja krediidiandmed.

Kohati nimetatakse identiteedikaks ka **identifikaatorit**, st olemit kontekstis üheselt tähistavat ja esindavat atribuuti, nagu kasutajanimi, isikukood, inventarinumber.

² Üldises tähenduses funktsioon, mis seab suurema andmekogumiga vastavusse väiksema, ettemääratud suurusega andmekogumi ehk räsi.

³ Krüptograafia, kus krüpteerimiseks ja dekrüpteerimiseks kasutatakse avalikku võtit ja vastavat privaativõtit; kui krüpteerimiseks kasutatakse avalikku võtit, tuleb dekrüpteerimiseks kasutada vastavat privaativõtit, ja vastupidi.

Eestis määratleb isikut tõendavate dokumentide seadus (ITDS) identiteediandmed isiku biomeetriliste ja biograafiliste andmetena, mille järgi on võimalik isik tuvastada või isikusamasust kontrollida.

Krüptovõti (*cryptographic key*) – matemaatiline väärtus, mida kasutatakse algoritmis, mis teisendab krüpteerimata ehk avateksti krüptogrammiks või vastupidi. Eesti e-identiteedi ökosüsteem põhineb avaliku võtmega krüptograafial, kus krüpteerimiseks ja dekrüpteerimiseks kasutatakse avalikku võtit ja vastavat privaatvõtit (mis üheskoos moodustavad **võtmepaari**).

Sertifikaat (*certificate*) – teatav autentsustõend. Digitaalsertifikaadi tähenduses elektrooniline dokument (fail), mis seob kasutaja avaliku võtme teda identivate andmetega, näiteks isiku või organisatsiooni nime ja/või aadressiga. Sertifikaadi enda autentsust kinnitatakse väljaandja digitaalsignatuuriga (tüüpilises PKI süsteemis sertifitseerimiskeskuse omaga). Kasutaja võtmepaari ja sertifikaadi saab korraldada kasutaja autentimist ning sõnumite terviklust ja salgamatust.

Usaldusteenus (*trust service*) – elektrooniline teenus, mis aitab erinevatel osapooltel siduvaid otsuseid teha. Euroopa Liidus on usaldusteenusteks näiteks isikusertifikaatide väljastamine ja elutsükli haldus, ajatempliteenuse osutamine, e-allkirjade loomine, e-allkirjade kontrollimine, e-allkirjade säilitamine, e-andmevahetusteenus ja veebiserverite sertifikaatide väljastamine. Täpsed nõuded ja tingimused igale usaldusteenusele ja allkirja andmise ning tembeldamise aspektidele määratleb eIDAS. eIDAS määratleb ka usaldusteenuste tasemed - kvalifitseeritud ja mitte kvalifitseeritud. Kvalifitseeritud usaldusteenuseid saavad osutada vaid kvalifitseeritud usaldusteenuste osutajad. Euroopa Komisjon peab ja avaldab kõigi ELi riikide usaldusteenuse osutajate ja nende pakutavate usaldusteenuste üldnimekirja *List of Trusted Lists* (LOTL).

1.2.2 Kasutatud lühendid

Allpool on lahti kirjutatud ülevaates kasutatavad lühendid. Eesti IT-keeles omakeelseid infotehnoloogia lühendeid peaaegu ei kasutata, enamik lühendeid on ingliskeelsed ja sisuliselt talitlevad terminina. See omakorda tähendab, et eestikeelne lahti kirjutatud versioon terminist võib kasutusest üldse puududa. Keelte märkimisväärse erinevuse tingimustes kindlustab selline kasutusviis mõistete koherentsuse keelte vahel.

AdES – *Advanced Electronic Signature* – eIDASi määramises määratletud e-allkirjade kolm ülemist taset

ASiC-E – *Associated Signature Container (Extended)* – konteineri vorming, mis sisaldab signeeritud andmeid koos allkirja või ajatempliga mingis konkreetsetes vormingus (XaDES/CADES)

ASiC-S – *Associated Signature Container (Simple)* – konteineri lihtsustatud vorming, mis sisaldab signeeritud andmeid koos allkirja või ajatempliga mingis konkreetsetes vormingus (XaDES/CADES)

BDOC – digiallkirja pärandvorming Eestis, digiallkirja ja konteineri kombinatsioon

CA – *certificate authority* – sertifitseerimiskeskus (SK)

CDOC – krüpteeritud failikonteiner sideturbeks, kuhu lisatud faile saab dekrüpteerida eID-vahenditega.

CERT-EE – intsidentide käsitlemise osakond RIA küberturvalisuse keskus

CP – *Certification Policy* – sertifitseerimispoliitika

CRL – *Certificate Revocation List* – sertifikaatide tühistusnimekirja

eeid – värske ristautentimisteenus Interneti Sihtasutuselt

eID – elektrooniline identiteet

eIDAS – *regulation on electronic identification and trust services* – e-identimise ja e-tehingute jaoks vajalike usaldusteenuste määramine

EUTS – e-identimise ja e-tehingute usaldusteenuste seadus

EITS – Eesti infoturbestandard, ISKE järglane, *BSI IT Grundschutz* edasiarendus

ENISA – *EU Agency for Cybersecurity* – ELi Küberturvalisuse Amet

GDPR – *General Data Protection Regulation* – isikuandmete kaitse üldmäärus

GovSSO – riigi SSO teenus

HSM – *Hardware Security Module* – riistvaraline turvamoodul

KÜTS – küberturvalisuse seadus

LDAP – *Lightweight Directory Access Protocol* – kataloogipöörduse kergprotokoll

LoA – *Level of Assurance* – kindlustase

LoTL – *List of The Lists* – Euroopa Komisjoni ametlik usaldusnimekiri

mobiil-ID – elektrooniline teenus, mis võimaldab mobiiltelefoni abil isikut tuvastada ja dokumente digiallkirjastada.

NFC – *Near Field Communication* – lähiväljaside, traadita side kokkupuutes või lähedaste seadmete vahel (vahemaa alla 10 cm)

NIS – *Network and Information Systems Regulations 2018* – Võrgu- ja infoturbe direktiiv

NIST – National Institute of Standards and Technology – riiklik standardi- ja tehnikainstituut, USA kaubandusministeeriumi allasutus

OCSP – *Online Certificate Status Protocol* – võrgusertifikaadi staatuse protokoll

PKI – *Public Key Infrastructure* – avaliku võtme taristu

PPA – Politsei- ja Piirivalveamet

QC – *Qualified Certificate* – kvalifitseeritud sertifikaat

QES – *Qualified Electronic Signature* – kvalifitseeritud elektrooniline allkiri, käsitsi kirjutatud allkirjaga samaväärse õigusliku toimega

QSCD – *Qualified Signature Creation Device* – sertifitseeritud seade kvalifitseeritud e-allkirja loomiseks

QTSP – *Qualified Trust Services Provider*, kvalifitseeritud usaldusteenuse osutaja

REST – Representational State Transfer – esitusoleku siire

RIA – Riigi Infosüsteemi Amet

SEPA – *Single European Payment Area* – ühtne euromaksete piirkond

SIM – Subscriber Identification Module – abonendi identimise moodul

SSCD – *secure signature creation device*, turvaline allkirja andmise seade, vt ka QSCD

SSL – *Secure Sockets Layer*, nüüd TLS

SSO – *Single Sign-On* – ainulogimisega pöördus

TARA – riigi autentimisteenus, mõeldud valitsussektori asutustele kasutajate autentimiseks.

TLS-CCA – *TLS with Client Certificate Authentication* – vastastikku autentiv turvaprotokoll, koos serveri ja isiku sertifikaatidega

TSL – *Trust-service Status List* – usaldusnimekiri

XAdES – *XML Advanced Electronic Signature(s)* – üle-euroopaline e-allkirjade standard, kooskõlas eIDASi määrusega

1.3 Ülevaate struktuur

Ülevaate praegune versioon keskendub eelkõige füüsiliste isikute e-identiteedile ja toimingutele ökosüsteemis ning jätab seetõttu vaatluse alt välja juriidilistele isikutele mõeldud e-templi (*E-Seal*).

Dokumendi **jaotised 2 ja 3** on mõeldud viima lugejat kurssi eID ökosüsteemi põhialustega. **2. jaotis** mõtestab lahti mõisted „identiteet“, „e-identiteet“ ning „e-identiteedi ökosüsteem“, kirjeldab, kuidas toimub identiteetide arvestus ja milline on nende seos eID-vahenditega. Samuti annab see ülevaate Eestis kasutusel olevatest eID-vahenditest ja nendes sisalduvast teabest. **3. jaotis** käsitleb Eesti eID ökosüsteemiga seotud valdkondi ja neid kureerivaid asutusi.

Jaotised 4 ja 5 on suunatud isikutele, kes peavad oma töö raamides langetama eID teenustega seotud otsuseid. **4. jaotis** käsitleb Eesti eID ökosüsteemi teenuseid. **5. jaotis** kirjeldab praktilist integratsiooni lõppkasutaja toimingute (kasutusjuhtude) ning Eesti eID ökosüsteemi universaalteenuste vahel. Kõige mahukamad jaotises vaadeldavad näited käsitlevad digiallkirja andmist ja loodud allkirjade valideerimist, kuivõrd esitatud nõuete ja täidetavate tehniliste normide vaatepunktist on see keerulisim kasutusjuht.

Dokumendi **lisad** on mõeldud ennekõike eID teenuste elluvijatele. **Lisa A** avab Eesti eID ökosüsteemi normatiivset tausta, mis moodustub õigusaktidest (seadustest, määrustest, rakendusaktidest, direktiividest) ning koosvõimet tagavatest tehnilistest standarditest. **Lisa B** kirjeldab selle tehnilisi raame: eID-vahendite üksikasju, digiallkirja andmise tehnilisi vahendeid ja neile rakenduvaid tehnilisi norme. **Lisa C** koondab nõuded, millega peab tutvuma iga Eesti eID ökosüsteemiga kokku puutuv tootja, väljastaja, teenuse osutaja ja integraator.

1.4 Eesti eID ökosüsteemi erilisus ja erinevused

1.4.1 Ajalooline taust

Eesti eID ökosüsteemi avalik-õiguslik osa eeldab toetumist selle toimimist reguleerivale õiguslikule baasile. ID-kaardi⁴ loomisel reguleeriti selle väljaandmine:

- isikut tõendavate dokumentide seaduses (ITDS) [3] (15. 02.1999);
- digitaalallkirja seaduses (DAS) [4] (08.03.2000).

ITDS käsitles muuhulgas ID-kaardi⁴ füüsilist osa ja selle väljaandmist ning DAS ID-kaardi elektroonilist osa, kusjuures seadused üksteisele ei viidanud.

Eesti eID ökosüsteemi loomise ajal oli oluliseks dokumendiks Euroopa Parlamendi ja nõukogu direktiiv 1999/93/EÜ 13. detsembrist 1999 ühenduse elektroonilisi allkirju käsitleva raamistiku kohta. Kuivõrd Eesti ei olnud tollal veel ELi liige, siis puudus vajadus Eesti eID ökosüsteemi loomisel selle direktiiviga arvestada. Euroopa Liiduga liitumisel suuri sisulisi muudatusi ei tehtud; seega võib siiski eeldada, et Eesti eID ökosüsteemi loojad olid taustauuringu raames ELi direktiividega tutvunud.

⁴ Siin ID-kaart isikutunnistuse tähenduses, kuna esialgu teisi ID-kaardi tüüpe ei eksisteerinud.

Seoses otsekohalduva eIDASi määrusega (hakkas kehtima 01.07.2016) tuli Eesti õigusaktid viia selle määrusega [5] vastavusse. Selleks tunnustati DAS kehtetuks ning eIDASi määruse mõningate sätete pehmeks ülekandmiseks Eesti õigusruumi dubleeriti need e-identimise ja e-tehingute usaldusteenuste seadusse (EUTS, jõustus 26.10.2016) [6]. Et tagada eestikeelse termini „digitaalallkiri“ jätkuv sisu uute juriidiliste väljendite kontekstis, seostas EUTS selle termini eIDASi määruse QES-taseme allkirjaga. See tähendab erinevust e-allkirja ja digiallkirja vahel: viimane hõlmab Eestis üksnes QES-taseme allkirju.

Suur roll digitaalsete autentimisvahendite totaalsel kasutuselevõtul (vähemasti Eestis) oli ühtse euromaksete piirkonna SEPA (*Single European Payment Area*) sisseseadmisel alates 2008. aastast. Selle käigus, 2018. aastal, seadis EL paroolidega ja koodikaartidega autentimisele sedavõrd väikesed tehingulimiidid, et nende autentimisviisidega jätkamine ei osutunud enam praktiliseks. Vastav otsus oli tingitud küberturvalisuse olukorrast Euroopas.

1.4.2 Eriline kasutuskeskkond

Eesti eID ökosüsteemil kui keskkonnal on kolm sotsiaalse dimensiooniga omadust. See on **kõikjalolev**, **universaalne** ja **totaalse kasutusega**.

Eestit külastavad isikud mainivad kõigepealt ära siinse eID kasutuskeskkonna kõikjaleulatuvuse. Isikutunnistus on Eestis elavale Eesti kodanikule alates 15. eluaastast kohustuslik ja seda saab kasutada autentimiseks ja digiallkirja andmiseks kiipkaardilugejaga varustatud arvuti vahendusel. Kiipkaardilugejad on levinud nii koduarvutitel, avaliku sektori töökohtadel kui erafirmade arvutitel, seda hoolimata viimase aja mobiilsetest suundumustest. Muudes riikides leidub kiipkaardilugejaid ennekõike väga spetsiifilistes valdkondades nagu sõjandus ja valitsussektor. Lisaks saab ID-kaarti kasutada digiallkirja andmiseks ka RIA DigiDoc mobiilirakenduses, kasutades selleks eraldiseisvat kiipkaardilugejat või lähiväljasidet (NFC). Veel on võimalik e-identimiseks ja digiallkirja andmiseks kasutada mobiil-ID ja Smart-ID lahendusi, mis ei nõua kiipkaardilugejat. Samuti on oluliseks kõikjaleulatuvuse faktoriks laialt levinud lokaalse digiallkirja loomise lõppkasutajatarkvara DigiDoc4 ja RIA DigiDoc. Riik on ühtlasi vabalt kättesaadavaks teinud arendusvahendid nii autentimise kui digiallkirja andmise integreerimiseks e-teenustesse.

Eesti eID ökosüsteemi funktsioonistik on universaalne. See tähendab, et kasutusel olevad eID-vahendid (ID-kaart, mobiil-ID, Smart-ID) pakuvad kõik samu autentimise ja digiallkirja andmise funktsioone, sealjuures samal turvasemel ja sarnase kasutajakogemusega, ning neid saab enamjaolt kasutada võrdselt kõigis e-teenustes. Samuti on nii kodanike kui residentide eID-vahendid ühesuguse funktsioonistikuga. Teistes riikides on vahendid sageli jaotunud segmenditi, näiteks panganduse ja e-tervise valdkonnad võivad vajada erinevaid juurdepääsuvahendeid.

Eesti eID ökosüsteemi kasutus nii kodanike, residentide kui ka e-residentide hulgas on massiline ja totaalne. Kasutus hõlmab elu kõiki aspekte, alates lepingute sõlmimisest ja maksude deklareerimisest, haridusest ja tervishoiust ning lõpetades arvukate riiklike ja kommertsportaalidega. Kui välja arvata ostlemine globaalsetes e-poodides, siis kõik muud eluks vajalikud toimingud on võimalik sooritada kaugrežiimis ning standardsete eID-vahenditega. Sellist läbistustaset e-teenustega pole veel üheski teises riigis õnnestunud saavutada.

Need kolm olulist omadust on välja toodud selleks, et osutada uute lahenduste sobivusele Eesti eID senise ökosüsteemiga. Riigi kodanikkonna elustiili säilitamiseks tuleb tagada, et potentsiaalsed uued süsteemid haakuksid olemasolevatega.

1.4.3 Tavad ja piirangud

Eesti eID ökosüsteem allub teatud tavadele ja piirangutele. Tavasid on kirjeldatud allpool, piirangud esitab lisa C.

Ökosüsteemi alustalad ja olulised iseärasused on järgmised.

1. Isiku identiteedi määrab riik ning identiteedihaldust sooritab riik keskselt. Isikul on vaid üks identiteet (alusidentiteet). Tuleb eristada kaht erinevat protsessi – üks alusidentiteedi loomiseks vajalik isiku tuvastamine ning vajalike andmete registrisse kandmine, teine eID-vahendi väljastamiseks vajalik isikusamasuse kontrollimine. Teise isiku identiteedi kasutamine on kuritegu. (Vt järgmisi seotud nõudeid, lisa C: R-L-06, R-L-07, R-G-01, R-S-08)
2. Isiku nii füüsilised kui digitaalsed dokumendid on unikaalselt ja lahutamatult seotud dokumendi kasutaja unikaalse identiteediga. (Vt nõuded R-L-06 ja R-G-01)
3. Autentimist ja digiallkirja andmist võimaldavad eID vahendid ja neid toetav tarkvara on piisavalt turvalised (tagatakse lööktestimise (*red-teaming*) ja komponentide sertifitseerimisega). (Vt ka nõue R-L-05)
4. Autentimist ja digiallkirja andmist võimaldavad krüptosertifikaadid on unikaalselt ja lahutamatult seotud eID-vahendi kasutaja alusidentiteediga. (Vt nõuded R-L-6 ja R-G-01)
5. Inimese identimiseks erasektoris kasutatakse isikukoodi sarnaselt inimese identimisel avalikus sektoris. (Vt nõue R-L-06)
6. Füüsiliste isikut tõendavate dokumentide ning digitaalsete eID-vahendite kehtivus on avalikult verifitseeritavad.
7. eID-vahendi autentimise ja digiallkirja andmise funktsioone käsitletakse peaaegu alati ühtse komplektina ning Eesti ei ole iseseisvaid vahendeid autentimiseks ja digiallkirja andmiseks. (Vt ka nõue R-G-06)
 - Eesti eID ökosüsteemi kaks põhiteenust (elementaartoimingut, väärtusteenust) on vastavalt autentimine ja digiallkirja andmine.
 - On Eesti tava, et lõppkasutajad üldjuhul saavad autentimise ja digiallkirja andmise funktsiooni toetava vahendi kätte ühe komplektina. Mõlemad funktsioonid on realiseeritud samal tehnoloogilisel baasil, kuigi autentimiseks kasutatakse ühte võtmepaari ja sertifikaati ning digiallkirja andmiseks teist võtmepaari ja sertifikaati. Ka nende funktsioonide haldus on seotud – tühistada/kehtetuks tunnistada saab vaid mõlemat krüptosertifikaati koos. Et eristada kasutaja jaoks selgemalt autentimist ja digiallkirja andmist on tavaks kasutada nende jaoks erinevaid PIN-koode. Nõuded ja protsessid on autentimisele ja digiallkirja andmisele siiski erinevad. (Vt nõue R-G-07).

8. ID-kaartidel⁵ on autentimise ja digiallkirja andmise funktsioonid realiseeritud spetsiaalse kiipkaardile laetud programmiga (aplett). Kiipkaartide arvutis kasutamiseks on loodud (lisaks üldistele PKI teenustele) täiendav lõppkasutaja tarkvara (draiverid, DigiDoc4, RIA DigiDoc, Web eID). Mitmeid ID-kaarte (isikutunnistust, elamisloakaarte, diplomaatilist isikutunnistust) saab kasutada ka isikut tõendavad dokumendina füüsilises keskkonnas (isikut tõendavate dokumentide seaduse alusel). Lisaks on võimalus neid ID-kaarte kasutada CDOC-vormingus krüptokonteinerite dekrüpteerimiseks. Veel on ID-kaartide puhul võimalus NFC vahendusel nii dokumendi info lugemiseks kui ka RIA DigiDoc'i rakenduses andmete digiallkirjastamiseks.
9. Mobiil-ID puhul kasutatakse täiustatud SIM-kaarte, kuhu on lisatud ID-kaardile sarnane programm (aplett). SIM-kaardil paikneva apletiga suhtlemine toimub üle mobiilivõrgu ning tuginevate isikute tagasüsteemid saavad kasutada vastava API kaudu apleti funktsioone.
10. Smart-ID puhul on eID-vahend komplekt nutiseadmest ja kesksest teenusest. Kasutajakeskkond on nutiseade. Samalaadselt mobiil-ID API teenusele on olemas Smart-ID API teenus, mille abil saab kasutaja arvutis töötav tarkvara või e-teenuse osutaja serverid Smart-ID autentimise ja digiallkirja andmise funktsiooni algatada.
11. Kõik laia kasutusega eID-vahendid on PKI-põhised (avaliku võtme taristu, *public key infrastructure*). Vahendite väljaandmiseks ja kasutamiseks on vajalik sertifitseerimisteenus (koos selle tehniliste alamteenustega nagu OCSP (sertifikaadi staatuse protokoll, *online certificate status protocol*), CRL (sertifikaatide tühistusnimekiri, *certificate revocation list*). Digiallkirja andmiseks vajatakse ka ajatempliteenust. Digiallkirja andmiseks on loodud tasuta kättesaadav avatud lähtekoodiga tarkvara. (Vt nõue R-S-01)
12. Infosüsteemid Eesti avalikus sektoris ning sageli ka erasektoris kasutavad isikute autentimiseks eID-vahendeid. See tähendab, et organisatsioonid ja infosüsteemid saavad loobuda kasutajate füüsilise isikutuvastusest, registreerimisest, identifitseerimisvahendite loomisest ja väljaandmisest jms tugitegevustest. See lihtsustab süsteeme ning vähendab kulusid, kuna need tegevused tehakse juba riigi poolt. Sellist praktikat on kirjeldatud „autentimismormatiivis“ [1]. Autentimismormatiiv sätestab, et autentimismoodulit ei tohi ise ehitada ning et see peab olema süsteemi muust talitlusest eraldatud.
13. Ideaaljuhul on vahendid dubleeritud ja vastastikku asendatavad. Sel põhjusel põhinevad kõik avalikkusele suunatud liidesed avalikel standarditel ja *vendor lock-in* on raskendatud. (Vt nõuded R-S-04 ja R-U-01)
14. Eesti eID ökosüsteemi komponentide puhul eelistatakse avatud lähtekoodi.
15. Eesti elektrooniline hääletamine Euroopa Parlamendi, Riigikogu ja KOV valimistel toetub samale Eesti eID ökosüsteemile.

⁵ ID-kaarti on siin mõeldud laiemas tähenduses (kui platvormi): riiklikult väljastatud ID-1 formaadis dokument, millel on autentimise ja digiallkirjastamise funktsionaalsus (ID-kaart, elamisloakaart, digitaalne isikutunnistus (digi-ID), e-residendi digitaalne isikutunnistus ning diplomaatiline isikutunnistus). Vt ka mõiste selgitust peatükis 1.2.1.

16. Mistahes muude osiste lisandumisel Eesti eID ökosüsteemi peab RIA ID-tarkvara (draiverid, DigiDoc4, RIA DigiDoc, Web eID) tööle jääma.
17. Autentimise ja digiallkirjade leviku seisukohast on oluline tasuta ja kõigile kättesaadavaks tehtud RIA ID-tarkvara.
18. Lõppkasutajale pakutav riiklik ID-tarkvara tugi on olemas kolmele peamisele platvormile: Windows, Linux ja Mac. Nutiseadmete tugi elementaartoimingutele on olemas Apple'i ja Androidi platvormidele.
19. Mistahes integratsioon Eesti eID ökosüsteemiga toob väga tõenäoliselt kaasa vajaduse liidestuda X-teega, mis on turvaline andmete liigutamise keskkond institutsionaalse kasutaja ja andmekogude vahel (vt nõue R-L-05). Vt ka X-tee üldinfo [7] ning X-tee dokumentatsioon [8].

2 Identiteedi mõiste ja e-identiteedi ökosüsteemi olemus

Selles jaotises mõtestame lahti mõisted **identiteet**, **e-identiteet** ning **e-identiteedi ökosüsteem**. Üheselt aktsepteeritud definitsiooni mõistetele „e-identiteet“ ja „eID ökosüsteem“ pole tänaseni leitud. E-identiteeti on erinevad autorid selgitanud järgmiste lausetega:

1. andmete kogum, mis seob elektroonilises keskkonnas isiku tema füüsilise identiteediga/isikuga;
2. elektrooniline tõend sellest, et inimene on see, kelle ta väidab end olevat;
3. elektroonilises keskkonnas kasutusel olev isikutuvastusvahend;
4. elektrooniliseks kasutamiseks mõeldud isikut tõendav dokument, üks osa riigi kriitilisest taristust;
5. Eestis on isikutel füüsilises ja digimaailmas täpselt sama identiteet. Leidub mitu eID-vahendit kuid isiku identiteet neis jääb alati samaks [9].

Ka eID ökosüsteemi on defineeritud erinevalt:

1. põhineb turvalisel avaliku võtme infrastruktuuril;
2. hõlmab eID-vahendeid, kasutajatarkvara ning ühtlasi ka erafirmade või riigipoolseid teenuseid. Teemavaldkonda kuulub veel eID-vahendite valmistamine ja väljastamine;
3. eID ökosüsteem moodustub isikut tõendavast digivõimega dokumendist, veebisaitidesse integreeritavast sobitustarkvarast ning tagaplaanil tüviteenuseid andvatest asutustest ja firmadest;
4. eID ökosüsteemi oluliseks osaks tuleb lugeda ka valdkonna regulaatorite tehtav töö ning usaldusteenuste järelevalve.

Need erinevad vaatenurgad koos illustreerivad e-identiteedi tahke. Arvame, et eID ökosüsteemi üks parimaid definitsioone on esitatud Maailma Majandusfoorumi materjalides [10] – „eID ökosüsteem on võrgustik koostööd tegevatest avaliku ja erasektori osapooltest, kes määratlevad, loovad ja rakendavad kasutajakeskseid vahendeid, mille kaudu üksikisikud saavad oma identiteeti organisatsioonidele tõestada“ (lk 12).

Sama dokument defineerib eID ökosüsteemi **viis põhiprintsiipi**, nendeks on

- kasutajakesksus
- usaldatavus
- koostalitlus(võime)
- avaliku ja erasektori koostöö
- kestlikkus

eID ökosüsteemi juures saab eristada järgmisi aspekte, mida tuleb vaadelda ühtse koostoimiva tervikuna:

- **õiguslik** (seadused, määrused, direktiivid)
- **organisatoorne** (koostöö, asutuste ja eraettevõtete vaheline andmevahetus)
- **tehniline** (protokollid, standardid, seadmed)
- **turvalisuse** aspekt (intsidentidest raporteerimine, vastutustundlik teavitamine nõrkustest)

- järelevalve

2.1 eID ökosüsteemi käsitluse üldpõhimõtted

eID ökosüsteemi tegelik keerukus on väga suur, mistõttu seda ökosüsteemi on mõtet käsitleda üksnes süsteemselt ja eri vaadete kaupa. Varem on kirjeldatud Eesti eID ökosüsteemi valitud tehnilisi aspekte [11]. ENISA avaldas 2023. a juulis kokkuvõtliku analüüsi (edaspidi ENISA DIS) ELis ja maailmas eID valdkonda reguleerivatest standarditest [12]. Siinne käsitlus toetub teatud osas ENISA DIS esitatud liigitustele ja süstemaatikale ning lisaks kasutakse ülevaates osaliselt mõistelise alusena sõnastusi, mida kasutab ENISA.

2.2 Identiteet ja selle kasutamise vahendid

Selles jaotises selgitame, milles digi-identiteet seisneb, kuidas toimub identiteetide arvestus ja milline on nende seos eID-vahenditega. Ühtlasi anname kiire ülevaate Eestis kasutusel olevatest eID-vahenditest ning vaatleme, missugust teavet need sisaldavad.

Standardi EN 319 412-1 [52] jaotis 5.1.3 osutab, et identiteedi tähisena saab kasutada isikukoodi, maksukohuslase numbrit või muud mõnest usaldusväärsest allikast pärit identifikaatorit. Selles kontekstis saab öelda, et identiteet Eestis on absoluutne, põhineb alusidentiteedil ning väljendub isikukoodis.

2.2.1 Alusidentiteet

Et isikule oleks võimalik väljastada eID-vahendeid, peab tal olema rahvastikuregistris korrakohaselt registreeritud alusidentiteet. Selleks tuvastab PPA isiku ning kannab registrisse identiteedi andmed ning isiku tuvastamise andmed. Alusidentiteedi põhilandmestik on nimi ja isikukood. Läbi isikukoodi seotakse konkreetsed eID-vahendid alusidentiteediga.

Kuivõrd rahvastikuregistri põhists alusidentiteeti paljudes riikides ei eksisteeri, siis sageli nimetatakse elektrooniliseks identiteediks konkreetset krüptosertifikaati konkreetsetes eID-vahendis. Seejuures ei selgu ELi õigusest ilmutatult, kas e-identiteedi alla mahub nii autentimine kui ka allkirja andmine või siiski vaid esimene. Eesti mõistes on tegu kahe olulisima, kuid samas siiski eraldi väärtusteenusega (vt jaotis 4.1.1), mida aga teenindab üks ja sama eID-vahend/seade/tööriist (näiteks ID-kaart).

2.2.2 Isikukood

Eesti alusidentiteet väljendub isikukoodis. Isikukoodi moodustamise ja andmise kord on rahvastikuregistri seaduse § 40 (6) alusel sätestatud siseministri määruses [62]. Isikukood on üleriigiline. Kohaliku (regionaalse, näiteks maakonna) identiteedi mõiste puudub. Võrdlusena näiteks Saksamaal on identiteedi identifikaatoreid traditsiooniliselt väljastatud liidumaa tasemel.

Isikukoodil kui mõistel ei ole ühest ingliskeelset vastet. Kasutatud on näiteks termineid PIC – *personal identification code* ja terminit *personal identification number*, mis paraku ei eristu pangakaardi PIN-koodist. Vikipeedia koondab eri riikide isikukoode käsitleva teabe võtmesõna *national identification number* alla [64].

Helen Raamat on uurinud oma magistritöös [9] ELi andmete ristkasutust (lk 55) ning püstitab kvaliteetse ristkasutuse põhieeldusena Eestiga sarnase isikukoodi olemasolu. EuroSmart [63] on oma piiriülest ristkasutust käsitlevas analüüsis väitnud, et paljudes ELi riikides püsiv identifikaator kas puudub või siis ei kuulu see identiteedi kohustuslike atribuutide hulka.

Isikul võib eID-vahendeid olla mitu, igapähele neist eraldi sertifikaadipaar. Isikukood on aga isiku kõigis sertifikaatides sama ning see isiku eluea jooksul ei muutu. Eksisteerib siiski mehhanism, millega erivajadusel isikukoodi muuta (soovahetus, vigade parandus).

2.2.3 Isikukoodi omadused

Eesti isikukoodi eripärana on see loodud avalikuna. MKMi IT-valdkonna kunagine asekanstler Taavi Kotka on seetõttu öelnud, et isikukood on inimese digitaalne nimi.

Pelgalt isikukoodi teades ei ole võimalik hankida teise inimese kohta kuigivõrd rohkem teavet kui isikukoodita. Võrdluseks nt USA SSN (*Social Security Number*) ja mitme teise riigi isikukoodid on loodud paroolina – numbrit kasutades leiab sisuliselt aset autentimine ning küsijal on võimalik saada juurdepääs andmetele, millele see varem puudus. Mainitud asjaolu teeb säärase „isikukoodid“ küllaltki haavatavaks andmeleketele.

Isikukoodile kui identifikaatorile esitavad nõuded on järgmised:

- globaalsus – kõikjal kasutatakse isiku kohta sama identifikaatorit;
- unikaalsus – ühelgi kahel isikul ei tohi olla sama isikukoodi;
- persistentus – püsivus ajas.

2.2.4 Isikukoodi päritolu

Eesti isikukoodi tähenduse ja semantika mõistmiseks on oluline teada selle kujunemislugu. Isikukood juurutati Eestis 1989. aastal ning kontrollnumbri arvutusvalem on teadaolevalt seotud Ungari isikukoodi arvutusvalemiga [65]. Eesti isikukoodi päritolu on kirjeldatud Vikipeedia artiklis [65].

Isikukoodi kontrollsummat defineerivas Ungari päritolu arvutusvalemis on metoodiline matemaatiline viga, mille tõttu kontrollnumber ei võimalda parandada paljusid ühenumbriisi sisestusvigu [66]. Teistes keeltes on avaldatud teave sarnase Jugoslaavia päritolu vea kohta [67], kuid infot selle kohta, et ka Eesti isikukoodil leidub sarnane viga, on võimalik leida vaid eesti keeles [65].

Paljud ELi riigid ei kasuta isikukode ajaloolis-kultuurilistel põhjustel. Selles mõttes tüüpiline näide on Ungari [68], kus „Konstitutsioonikohus aastal 1991 otsustas: üldine, ühetaoline kasutuspiiranguteta isikutuvastuskood, mida ühesugusel printsiibil antakse riigi igale kodanikule ja residendile, on vastuolus põhiseadusega“ [69]. Peamine tõlgendus, mis säärase järelduseni viis, oli asjaolu, et isikukoodi olemasolul on kodaniku andmeid potentsiaalselt võimalik eri andmekogude vahel tõhusalt agregeerida, ilma et kodanik ise sellest kunagi teada ei saaks.

Sellist otsust saab 33 aastat hiljem vastustada kolmes vaates:

- enamik riike kasutab käibemaksukohuslase koodi, SSNi või mõnda teist identifikaatorit, mille mõju agregeerimisele on sarnane;
- globaalne turvaolukord on muutunud ja vajadus inimeste täpseks identimiseks on tõusnud;

- tehnilist lahendust, millega andmete agregeerimist seirata ja tõkestada, 1991. aastal ei eksisteerinud, ent tänases Eestis on see X-teel kasutatava Andmejälgija teenusena olemas [70] ja privaatsusriiskid seetõttu ka tegelikult ja tõhusalt leevendatavad. Eestis on olnud kohtuasju, kus kaebaja vastustab oma andmete vaatamist riiklikus registris.

2.2.5 Isikukoodi privaatsus

Isikukoodi privaatsuse nõue on võrdeline andmetöötlusvajadusega. Toimiva e-riigi eelduseks on, et tehingute ja transaktsioonide osapooled oleksid unikaalselt tuvastatavad, vastasel juhul avatakse võimaluste aken kelmustele, pettustele ja varavastastele kuritegudele.

GDPRi [31] artikkel 4 vaatepunktist on isikukood käsitletav isikuandmetena ja artiklis 87 sisaldub „isikukood“ ilmutatult. Isikuandmed mahuvad GDPRi artikkel 6 punkti 1.e alla, mis lubab isikuandmeid töödelda „avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks“ või eraõiguslike suhete korral punkti 1.f alla.

Isikukood puudub GDPRi artikkel 9 lõike 1 loetelust, mis tähendab, et isikukood ei kuulu isikuandmete eriliigi hulka. See tähendab muuhulgas näiteks, et kui isikukoodi töötleb riiklike registrite toel eraõiguslik teenuse osutaja, tuleb tal lähtuda GDPR üldistest sätetest ja töötlemiseks peab olema seaduslik alus.

2.3 eID-vahendid

eID-vahendis hoitakse e-identiteedi kasutamiseks vajalikke krüptograafilisi võtmeid ning mille abil saab neid praktiliselt kasutada. Järgnevalt on kirjeldatud Eesti eID ökosüsteemis toimivaid eID-vahendeid, üksikasjaliku ülevaate annab lisa B.1 tabel B.1.

2.3.1 ID-kaart⁶

ID-kaardil on privaativõtmed kaardil olemas kiibis ning autentimise ja digiallkirja andmise funktsioonid on realiseeritud spetsiaalse kaardile laaditud programmina (apletina). ID-kaardi kasutamiseks arvutis on vajalik kiipkaardilugeja olemasolu. ID-kaarti saab kasutada digiallkirja andmiseks ka RIA DigiDoc mobiilirakenduses kasutades selleks eraldiseisvat kiipkaardilugejat või lähiväljasidet (NFC). Lisaks autentimisele ja digiallkirja andmisele on ID-kaarti võimalik kasutada ka CDOC-krüptokonteineritesse lisatud failide dekrüpteerimiseks.

2.3.2 Mobiil-ID

Mobiil-ID toetab autentimise ja digiallkirja andmise funktsioone. Mobiil-ID puhul on privaativõtmed paigutatud mobiiltelefoni SIM-kaardile. Mobiil-ID kasutamiseks pole vaja kasutada lisaseadet nagu kiipkaardilugeja. Samuti pole mobiil-ID kasutamiseks ilmtingimata vaja nutitelefoni, ka tavalise nuputelefoni saab autentida ja allkirjastada.

⁶ ID-kaarti on siin mõistetud laiemas tähenduses (kui platvormi): riiklikult väljastatud ID-1 formaadis dokument, millel on autentimise ja digiallkirjastamise funktsionaalsus (ID-kaart, elamisloakaart, digitaalne isikutunnistus (digi-ID), e-residendi digitaalne isikutunnistus ning diplomaatiline isikutunnistus). Vt ka mõiste selgitust peatükis 1.2.1.

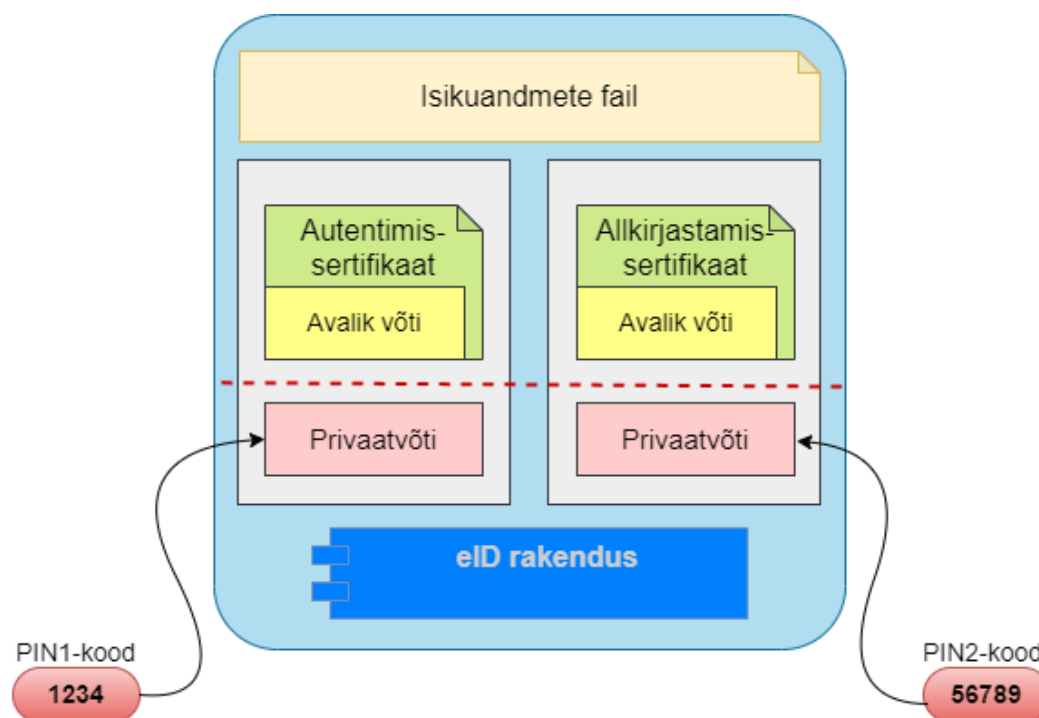
Mobiil-ID turvaaspektidest rääkides tuleb arvestada, et mobiil-ID loodi eesmärgil, et (tollal veel mitte-nuti) mobiiltelefon saaks talitleda koostöös tava-arvutist algatatud turvalise veebiseansiga. Alles hiljem, nutitelefonide levides, tekkis võimalus algatada seans samast seadmest, kus kasutaja kinnitab ka tehingu kontrollnumbri õigsust.

2.3.3 Smart-ID

Smart-ID on komplekt nutiseadmest ja keskest teenusest, mis üheskoos pakub autentimise ja digiallkirja andmise funktsioone. Tähelepanuväärne erinevus võrreldes ID-kaardi või mobiil-IDga on see, et privaatvõtmeid ei hoita ühes kohas vaid on jagatud kahe osapoole (nutiseade ja server) vahel ning neid ei liideta kunagi kokku ühes kohas, mis tõstab turvalisust. Smart-ID kasutamiseks pole sarnaselt mobiil-IDga vajalik kasutada lisaseadet nagu näiteks kiipkaardilugejat. Smart-ID tehnilist arhitektuuri on lähemalt selgitatud smart-id.com blogis [74].

2.4 eID-vahendi sisu

Joonis 1 illustreerib eID-vahendi olulisemaid sisuelemente ID-kaardi näitel. Tegelikus vahendis võib elemente olla rohkem, sh eelmised võtmed, platvormi teenindavad võtmed, vahendi omaniku tehnilised võtmed isikusertifikaatide lisamiseks jne. Elemente võib olla ka vähem.



Joonis 1. eID-vahendi olulisimad elemendid ID-kaardi näitel

2.5 eID-vahendite omavaheline suhe

Turvameetmena on soovitatud, et ühel isikul oleks samaaegselt mitu erinevat tüüpi eID-vahendit. See võimaldab isikul oma normaalset elektroonilist elu jätkata ka oludes, kus ühe vahendi kehtivus on

lõppenud, vahend ei ole tehniliselt töökorras või selle vahendi turvalisus on ajutiselt mõjutatud (nagu näiteks ROCA 2017 juhtumis⁷).

Teatud juhtudel saab eID-vahendi registreerimisprotsessi e-keskkonnas teha teise kehtiva vahendi alusel. See lihtsustab registreerimist, kuna kasutaja ei pea minema teeninduspunkti kohale. Näiteks üks võimalus Smart-ID konto registreerimiseks e-keskkonnas on näiteks seda teha ID-kaardi alusel.

2.6 Sertifikaadid

Eesti eID ökosüsteemis on sertifikaate seni alati käsitletud paarina. See tähendab, et igal eID-vahendil on alati kaks paarset sertifikaati – üks **autentimiseks** ja teine **digiallkirja andmiseks**. Paarina toimub ka nende sertifikaatide haldus, mis tähendab, et vahendil pole võimalik uuendada või kehtetuks tunnistada vaid üht sertifikaati kahest: need toimingud sooritatakse alati mõlema sertifikaadiga korraga. Alates 2007. aastast kehtivad ID-kaardid dokumentidena viis aastat ning nende sertifikaadid samuti viis aastat [71].

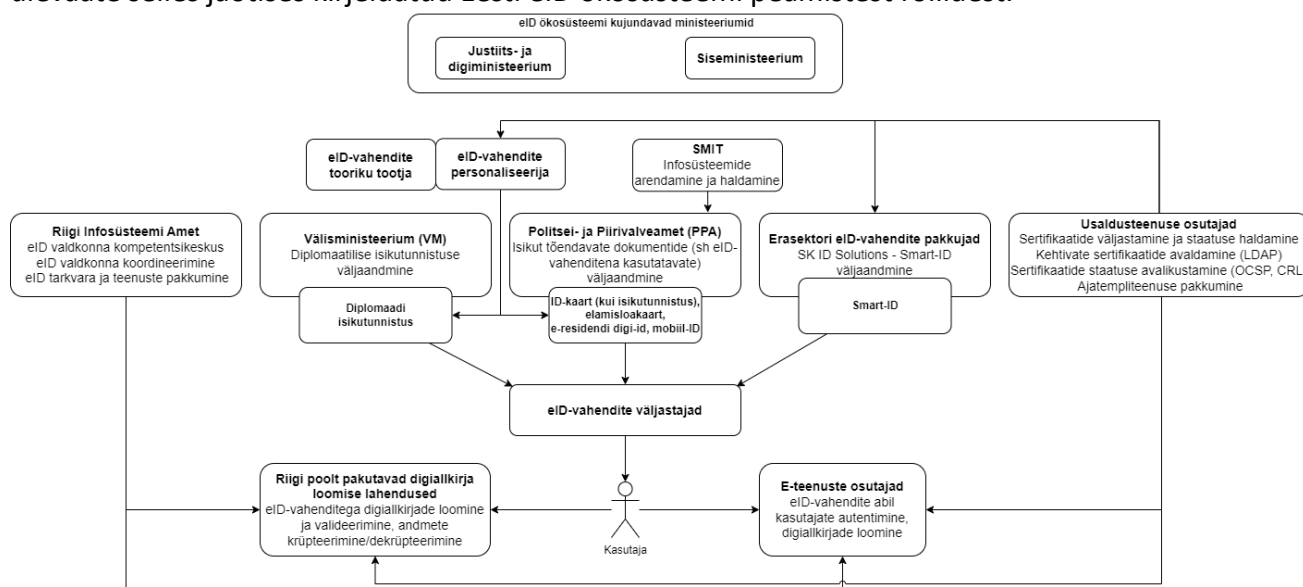
Mõnes Euroopa riigis võib juhtuda, et autentimine toimub mingi ühe vahendi ühe sertifikaadiga, kuid digiallkirja andmine hoopis teise vahendi teise sertifikaadiga. Eestis ei ole see täna praktikas võimalik, kuivõrd pea kõigi e-teenuste töövoog piirab digitaalse allkirja andmise sama eID-vahendi teise sertifikaadiga. Tegemist on arhitektuursete valikutega, mis on igas riigis unikaalsed.

Rohkem kui üks sertifikaat on kasulik ka pettuste vähendamiseks. Kui kasutaja jaoks selgelt eristada sisselogimist ja dokumendi digitaalallkirja andmist, siis kahe eri tüüpi PIN-koodi püüdmine ning kasutajale võltsitud toimingute esitamine vahendusründe abil on algoritmiliselt keerukam ning kasutajale vähem usutavam kui ühe universaalse (mõlemaks otstarbeks sobiva) võtmepaari ning PIN-koodi puhul.

⁷ ROCA (*Return of Coppersmith's Attack*) turvanõrkus on krüptograafiline nõrkus, mis võimaldab tuletada turvanõrkusega seadme genereeritud võtmepaari privaatvõtme selle avalikust võtmest. ROCA nõrkuse avalikustas 2017. aastal Masaryki Ülikooli juures tegutsev rahvusvaheline uurimisrühm. 30. augustil 2017 teavitas uurimisrühma liige Eestit ID-kaardi kiipide haavatavusest ROCA ründele. ID-kaartide turvalisuse tagamiseks otsustas RIA asendada senised RSA krüptosüsteemil põhinevad sertifikaadid elliptikrüptograafia (ECC) põhistelega. Uue sertifikaadiga ID-kaartide väljastamine algas 25. oktoobril 2017, samal päeval alustati ka sertifikaatide kauguuendamise testimist. 30. oktoobril avalikustas rahvusvaheline uurimisrühm avastatud nõrkuse. 3. novembril blokeeriti nõrkusega ID-kaartide sertifikaadid; kaardi edaspidiseks elektrooniliseks kasutamiseks tuli blokeeritud sertifikaat internetis või PPA teenindusbüroos uuendada. Blokeeritud sertifikaadid kaotasid lõplikult kehtivuse 2018. aasta 1. aprillil [83].

3 Valdkonnad ja vastutajad

Selles jaotises käsitletakse peamised Eesti eID ökosüsteemiga seotud valdkondi ja neid kureerivaid asutusi. Rollide jaotus võib ajas muutuda. Kahe ministeeriumi – Siseministeeriumi ning Justiits- ja Digiministeeriumi – ning kahe võtmeasutuse – Politsei- ja Piirivalveameti (PPA) ning Riigi Infosüsteemi Ameti (RIA) – koostöös vaadatakse rollide jaotus regulaarselt üle ning seda võidakse korrigeerida seaduses toodud volituste piires ja vastavalt vajadusele. Joonis 2 (kohandatud allikast [30]) annab ülevaate selles jaotises kirjeldatud Eesti eID ökosüsteemi peamistest rollidest.



Joonis 2. Eesti eID ökosüsteemi peamised rollid (kohandatud allikast [30])

3.1 Siseministeerium

eID valdkonnas on Siseministeeriumi roll töötada välja isiku identiteedi haldus, Eesti kodanike ja välismaalaste isikut tõendavate dokumentide väljaandmise poliitika ning suunata ja koordineerida asjaomaste valitsusasutuste tegevust.

3.2 Justiits- ja Digiministeerium

Justiits- ja Digiministeeriumil juhib, korraldab, edendab ja koordineerib avaliku sektori digiarengut, koordineerib avalike teenuste ja infosüsteemide arendust ning korraldab üleriigiliste digilahenduste arendamist ning jagatud infotehnoloogiasteenuste osutamist.

3.3 Välisministeerium

eID ökosüsteemi kontekstis on Välisministeeriumi roll anda välja, väljastada ja kuulutada kehtetuks diplomaatilist isikutunnistust. Samuti saab teatud teisi riiklike eID-vahendeid välisesinduste kaudu taotleda ja väljastada.

3.4 Erasektori eID-vahendite pakkujad

Eestis on kasutusel üks erasektori pakutav eID lahendus Smart-ID, mida pakub ja haldab SK ID Solutions. Ka mobiil-ID teenust osutab SK ID Solutions, kuid teenust tellib riik ning teenuse omanik PPA.

3.5 Riigi Infosüsteemi Amet

Riigi Infosüsteemi Amet (RIA) tegutseb põhimääruse [60] alusel. RIA on valitsusasutus, selle erinevad osakonnad tegelevad erinevate teemavaldkondadega. eID ökosüsteemis on RIA eID kompetentsikeskus, kes kujundab eID valdkonna arengu visiooni ja strateegia ning on eID valdkonna eestkõneleja ja seisukohtade kujundaja Eestis. RIA täidab eID ökosüsteemis järgmisi ülesandeid:

Riigi infosüsteemi valdkonnas

- korraldab autentimist, digitaalallkirjade andmist ja krüpteerimist võimaldava tarkvara ja internetipõhise autentimise ja allkirjade andmise süsteemi, sh:
 - kogu eID valdkonna pikaajalise arengu koordineerimine asutuste vahel;
 - portaali id.ee ülalhoid;
 - eID ökosüsteemis kasutatava tarkvarakomponentide arendamine, näiteks
 - lauaarvutile mõeldud DigiDoc4 rakenduse arendus;
 - nutiseadmetele mõeldud RIA DigiDoc rakenduse arendus;
 - veebis autentimise ja allkirja andmise lahenduse Web eID arendus;
 - teekide arendus, näiteks digidoc4j ja libdigidocpp;
 - jms
 - mitmesuguste Eesti eID ökosüsteemi seisukohast kriitiliste avalikes sektori asutustele pakutavate teenuste ja neid majutavate serverite ülalhoid, sh:
 - autentimisteenused (TARA, riigi SSO teenus);
 - digiallkirja moodustamise teenus SiGa;
 - digiallkirja valideerimisteenus SiVa;
 - ajatempliteenus vahendusteenus;
 - Web eID lahendus (autentimine ja allkirja andmine veebis);
 - kasutajatugi (sh telefonitsi);
- korraldab hankeid.

Küberturvalisuse valdkonnas

- korraldab kriitilise informatsiooni infrastruktuuri (CIIP) kaitset;
- tegeleb õigusaktide alusel haldusliku ja riikliku järelevalvega (sh Eesti eID ökosüsteemi üle). Rakendab haldussundi ja menetleb väärtegusid.

Samuti korraldab RIA mitmesuguseid teadlikkuse tõstmise kampaaniaid ja koolitusi erinevates valdkondades, mh Eesti eID ökosüsteemi huvides.

3.5.1 Küberturvalisuse keskus

RIA küberturvalisuse keskuse vastutusalaks on üks RIA kahest tegevussuunast – küberturve. Kokkupuude Eesti eID ökosüsteemiga on küberturvalisuse keskuse järgmistel osakondadel:

- **intsidentide käsitlemise osakond** (sh CERT-EE), mille pädevusse kuulub turvaprobleemide ja küberrünnete avastamine ja lahendamine muuhulgas ka Eesti eID ökosüsteemis;
- **riigi infoturbemeetmete osakond**, mis muuhulgas valmistab ette Eesti infoturbestandardi (E-ITS), sh selle eID aspekte käsitlevad moodulid (avaldatud on X-teen puudutavad moodulid SYS.EE.1 ja APP.EE.1, ettevalmistamisel e-identiteeti puudutav SYS.EE.2);
- **järelevalve osakond**, mis muuhulgas kontrollib teenuste vastavust standarditele ja seaduste ning määruste nõuetele, eID osas vastavust KÜTSi, EUTSi, E-ITSiga jne. Osakonnal on väärtegade menetlemise õigus. Sealhulgas tegeleb osakond järgmisega:
 - peab usaldusnimekirja;
 - sh haldab sellega seotud TSL (*Trust Service Status List*) e-teenust;
 - publitseerib usaldusteenuseid usaldusnimekirjas;
 - eemaldab usaldusteenuseid usaldusnimekirjast;
 - täidab muid eIDASi määrusest tulenevaid kohustusi;
- **analüüsi- ja ennetusosakond** – muuhulgas kogub ja süstematiseerib ohukirjelduste vooge ja tehnouudiseid, sh krüptograafia valdkonnas.

3.6 Politsei- ja Piirivalveamet

Ajalooliselt tegeles identiteediküsimustega Kodakondsus- ja Migratsiooniamet, mis muudeti 2010. aastal PPA osakonnaks.

PPA roll ja vastutus Eesti eID ökosüsteemis on järgmine:

- isikut tõendavate dokumentide (sh eID-vahenditena kasutatavate) väljaandmine;
- isikut tõendavate dokumentide arendamine, lepingute sõlmimine teenuse osutajatega;
- hangete korraldamine (koos RIAGA).

3.7 Siseministeriumi infotehnoloogia- ja arenduskeskus (SMIT)

Siseministeriumi infotehnoloogia- ja arenduskeskus (SMIT, www.smit.ee) tegeleb PPA ülesannete täitmiseks vajaliku tehnoloogia (sh tarkvara) arendamisega ning süsteemide haldamisega, sealhulgas ka identiteedi halduseks ja isikut tõendavate dokumentide väljaandmiseks ja haldamiseks vajalike süsteemide arenduse ja haldamisega..

3.8 Usaldusteenuse osutajad

Usaldusteenuse osutaja ehk usaldusteenuse tarnija (ingl k *trust service provider* – TSP) on (Eesti eID ökosüsteemis) eelkõige organisatsioon, mis haldab ja talletab eID ökosüsteemiga seotud isikusertifikaate. Samuti loetakse usaldusteenuseks näiteks ajatempliteenust. Eestis on mitmed teenused jagatud vastutava töötleja (enamasti PPA) ja volitatud töötleja vahel. Vahetu teenuse tarnija neil juhtudel on volitatud töötleja. Järgmised kaks alajaotist käsitlevad Eesti usaldusnimekirjas olevaid (SK ID Solutions AS) ja sinna lähitulevikus lisanduvaid (Zetes Estonia OÜ) eID ökosüsteemi kontekstis olulisi usaldusteenuste osutajaid.

3.8.1 SK ID Solutions AS

Eestis on pikka aega olnud vaid üks ettevõtte, mille põhitegevus on usaldusteenused – **SK ID Solutions AS** (varasema nimega AS Sertifitseerimiskeskus). Kõigi käibivate eID-vahendite (ID-kaardi, mobiil-ID ja Smart-ID) sertifikaate teenindab sama firma.

AS Sertifitseerimiskeskus asutati pankade ja telekomifirmade poolt 12.14.2001, kui siseminister ja ASI Sertifitseerimiskeskus juhataja allkirjastasid lepingu, mille kohaselt hakkas Sertifitseerimiskeskus osutama siseministeriumile digitaalallkirja seadusega kooskõlalist sertifitseerimisteenust.

SK ID Solutions osutab Eesti eID ökosüsteemile järgmisi teenuseid:

- kvalifitseeritud allkirja andmise sertifikaatide väljastusteenus;
- autentimissertifikaatide väljastusteenus;
- elektrooniline ajatempliteenus;
- teeb ID-kaardiga seotud sertifikaatide registri kättesaadavaks LDAP-teenuse kaudu;
- vastab elektroonilistele päringutele sertifikaatide kehtivuse osas (OCSP / CRL);
- vajaduse korral peatab sertifikaadid või tunnistab need kehtetuks.

Lisaks on SK ID Solutions eID-vahendi Smart-ID omanik, arendaja, väljaandja ja teenuse osutaja. SK ID Solutions väljastab ka e-templi sertifikaate firmadele ja asutustele. Samuti haldab SK ID Solutions mobiil-ID skeemi. SK ID Solutions liigitub elutähtsa teenuse osutajaks (HoS § 36 lg (1) p 8).

3.8.2 Zetes Estonia OÜ

Zetes Estonia OÜ lisandub Eesti usaldusnimekirja kvalifitseeritud usaldusteenuse osutajana ning tagab alates 2025. aasta lõpust välja antavate uute ID-kaartide (kui isikutunnistuste), elamisloakaartide, e-residendi digitaalse isikutunnistuse ja diplomaatilise isikutunnistuse puhul kvalifitseeritud sertifitseerimisteenuse, hõlmates ka kvalifitseeritud sertifikaatide väljastamist.

3.9 Ökosüsteemi muud osalised

3.9.1 Vahendite tootjad ja personaliseerijad

Vahendite tootjad valmistavad vahendite toorikud (näiteks, ID-kaardi, SIM-kaardi), mis hiljem personaliseeritakse. ID-kaardi dokumendi personaliseerimises osalevad Eestis hetkel järgmised ettevõtted: IDEMIA, Thales, Hansab ja HID. ID-kaart tüüpi dokumentide esimeste versioonide valmistajaks ja personaliseerijaks oli TRÜB (hiljem Gemalto), mis tegutses Eesti eID turul kuni aastani 2020. Mobiil-ID SIM-kaarte personaliseerib väljastaja (konkreetne sideettevõtte). Smart-ID kui virtuaalne vahend spetsiaalset valmendamist ega personaliseerimist ei vaja, see toimub Smart-ID konto registreerimise käigus.

3.9.2 Vahendite väljastajad

eID-vahendi väljastamine tähendab vahendi kätteandmist kasutajale. ID-kaartide väljastamine toimub PPA teenindustes või Eesti välisesindustes. PPA on viimastel aastatel püüdnud vähendada oma teeninduspunktide koormust, mistõttu on sõlmitud haldusleping ID-kaardi (kui isikutunnistuse) ja elamisloakaardi väljastamiseks kolmanda osapoole ehk välise teenuseosutaja vahendusel. Hetkel on väljastamiseks sõlmitud haldusleping Hansabiga, mida tehakse poekett Selveri teenindustest kaudu [61]. Ajalooliselt on teatud eID-vahendeid väljastatud ka suuremate pankade teenindusletist.

Mobiil-ID väljastajaks on sideettevõtted. Kuivõrd SIM-kaart on seotud konkreetse mobiilsideoperaatoriga, siis väljastab iga firma vaid omaenda SIM-kaarte. Hetkel on Eestis kolm sidefirmat, mis väljastavad digitaalset isikutunnistust mobiil-ID:

- Telia Eesti AS
- Elisa Eesti AS
- Tele2 Eesti AS

Smart-ID puhul kasutajale midagi spetsiaalselt (füüsilist) üle ei anta (nagu nt ID-kaarti või SIM kaarti). Väljastamine on osa Smart-ID konto registreerimisest. Konto registreerimist saab teha SK ID Solutions pakutavate digitaalsete kanalite kaudu või kohapeal partnerite juures (valitud pankade kontorid).

3.9.3 Kasutaja

Eesti eID ökosüsteemi turvaline toimimine on võimalik üksnes turvateadliku kasutaja puhul kes:

- ei anna oma eID-vahendit kellelegi edasi ega jäta seda järelevalveta;
- eID-vahendi varguse või kadumise korral helistab SK ID Solutions abitelefoni ja peatab sertifikaadid;
- vastavalt vahendi sertifikaatide kasutustingimustele hoiab vahendi PIN-koodid salajas;
- vastutab oma arvuti või nutiseadme jätkuva turvalisuse eest ning paigaldab sinna saadaolevad turvapaigad;
- väldib riskikäitumist küberruumis;
- on teadlik petuskeemidest ega allu neile;
- küberintsidendi toimumisel annab sellest kohe teada vahendi väljaandjale, RIA intsidentide käsitlemise osakonnale CERT-EE ning kahju tekkides ka politseile.

Tabel C.1 nimetab kolm kasutajale esitatavat nõuet: R-U-01, R-U-02 ja R-U-03.

Kasutajat abistavaid abitekstid on leitavad veebisaidil id.ee või eID-vahendi omaniku veebisaidil. RIA analüüsi- ja ennetusosakond organiseerib pidevalt elanikkonna teavituskampaaniaid küberohtude suhtes.

3.9.4 E-teenuste osutajad

Ökosüsteemi osalised on ka need riigiasutused ja eraettevõtted, kes kasutavad eID-vahendite võimalusi oma infosüsteemide kasutajate autentimiseks ja digiallkirjade loomiseks. Neid nimetatakse ka tuginevateks isikutest (ingl *relying party* (RP)). On tähelepanuväärne, et Eestis on selliseid e-teenuste osutajaid palju ning nad toetavad tavapäraselt kõiki ökosüsteemis leiduvaid eID-vahendeid. See tähendab, et e-teenuste osutajate vajadusi on ökosüsteemi arendamisel ja kujundamisel hästi arvesse võetud ning seda tuleb teha ka tulevikus.

4 Eesti eID ökosüsteemi teenused

Selles jaotises käsitleme Eesti eID ökosüsteemi teenuseid. On oluline mõista, et järgnevalt käsitleme üksnes e-identiteeti ennast puudutavaid teenuseid ning jätame täielikult vaatluse alt välja e-ühiskonna teenused (pangandus, e-tervis, e-haridus, e-valitsemine jne), mille turvalist kasutamist eID võimaldab.

Eestis puudub igasugune vajadus loetleda sisuteenuseid, mida eID võimaldab; ka puudub Eestis säärase loetelu või register. Selline lähenemine on unikaalne võrreldes teiste riikidega, kus e-teenuse sisseadmiseks kohati vajatakse mingit luba või kusagile registrisse kandmist. Eestis on lävendiks tehniliste normide täitmine ja korrektne liidestumine.

Jaotis selgitab, millised on lõppkasutaja toimingud (tinglikult -teenused) eID ökosüsteemis ning kuidas need suhestuvad eID tehniliste ning normikohaselt korraldatud universaalteenustega. Sellisena konstrueerib jaotis piisavalt detailse pinna ja mõistesüsteemi integratsiooni käsitlemiseks jaotises 5.

ENISA avaldatud eID standardite analüüs [12] esitab eID ökosüsteemi teenuste liigituse, mida siin võimaluste piires järgime. Eesti traditsioonist erineva käsitluse tõttu ENISA DIS dokumendis on mõningaid teenuseid võimalik liigitada mitmeti.

Eesti eID ökosüsteemi võimaldatavad teenused jagunevad kaheks:

- **põhiteenused** (jaotis 4.1), mis hõlmavad:
 - (4.1.1) lõppkasutaja elementaartoiminguid (autentimine, digiallkirja andmine jne);
 - (4.1.2) liidestatud ja tootestatud universaalteenuseid (TSL, PKI/LDAP, sertifikaadi kehtivusinfo teenus), millega lõppkasutaja tarkvara suhtleb;
 - (4.1.3) koosvõimeteenuseid (TARA, SSO, eeid, jne);
- **tugiteenused** (4.2) – näiteks ajatempliteenus.

Täiendame terminoloogiat veel liigitusega „abitoimingud“ (28).

4.1 Põhiteenused

Eesti eID ökosüsteemi **põhiteenused** on liigiti järgmised:

- lõppkasutaja elementaartoimingud (autentimine ja digiallkirja andmine);
- liidestatud ja tootestatud universaalteenused (TSL, PKI/LDAP, sertifikaadi kehtivusinfo teenus);
- koosvõimeteenus (identiteedimaaklerlus, eIDAS Node, TARA, eeid, SSO);

4.1.1 Lõppkasutajateenus

Lõppkasutaja elementaartoiminguid (kasutusjuhud), mida ühtlasi saab käsitleda väärtusteenustena, on järgmised.

1. **Autentimine** (*authenticate*) – tüüpiliselt toimub sisselogimine mingisse e-teenusesse.
2. **Digiallkirja andmine** (*sign*) – toimub põhiliselt kas kasutaja arvutis või kasutaja mobiiliseadmes. Samuti võib digiallkirja andmine toimuda näiteks

dokumendihalduskeskkonnas või teenusepakkuja keskkonnas, kes valmistab ette allkirjastatava konteineri ning lisab sinna kasutaja eID-vahendi poolt tagastatud allkirja.

3. **Allkirja valideerimine (kehtivuse kontrollimine)** – ENISA DIS käsitleb seda toimingut tagavat tugiteenust, kuid ei osuta kasutusjuhule. Lisaks digiallkirja tehnilistele aspektidele on digiallkirja puhul veel juriidilised aspektid, et mida allkirja olemasolu konkreetses situatsioonis üldse tähendab.
4. **Allkirja ületembeldamine** – ENISA DIS käsitleb seda tagava tugiteenuse **säilitusteenusena**. Eestis see teenus puudub, kuid ületembeldamist sooritas näiteks vallasrakendus TERA⁸.
5. **Krüpteerimine/dekrüpteerimine (encrypt/decrypt)** – toimub lauaarvuti tarkvaraga **DigiDoc4** või mobiilirakendusega **RIA DigiDoc** ning kasutades ID-kaarti (varsti lisandub ka mobiil-ID ja Smart-ID tugi). Nende rakendustega saab luua ning avada CDOC-krüptokonteinereid ning sedaviisi edastada konfidentsiaalseid faile saatjalt vastuvõtjale. Vastuvõtja identiteet määratakse näiteks ID-kaardil oleva autentimise võtmepaari avaliku võtmega või vastuvõtja isikukoodiga. Eestis on eID-vahenditega seotud krüptokonteinerite kasutamine tavapärane ning levinud, kuid mujal maailmas on eID ökosüsteemi krüpteerimise ja dekrüpteerimise teenuse lisamine haruldasem ning ENISA DIS sellist teenust ei kirjelda.
6. **Sertifikaatide peatamine ja kehtetuks tunnistamine** (näiteks seadme varguse või valdusest väljumise puhuks) – Eestis on hetkel tehniliselt võimalik teatud vahenditega (näiteks ID-kaart) seotud sertifikaatide peatamine ja seejärel taasaktiveerimine, kuid turvakaalutlustel võidakse võtta ka suund, et pärast kasutuselevõetud kehtivate sertifikaatide peatamist neid enam uuesti aktiveerida ei saa.
7. Käsitleme teenuse/toiminguna ka mõne seadme/vahendi puhul kohustuslikku **aktiveerimist**.
8. **Tehniline tugi** – pakutakse eelistatult telefonitsi ja e-maili kaudu.
9. Kasutus **kliendikaardina** on äärmiselt Eesti-spetsiifiline kasutus [75]. Sel otstarbel loetakse kaardilt mitte sertifikaate, vaid isikufaili.
10. Kasutus **elektroonilisel hääletamisel**. On paradigma küsimus, kas käsitleda sellist kasutusviisi eraldi, eemal tavalisest autentimisest ja digiallkirja andmisest. Soovitame seda teha, kuivõrd elektrooniline hääletamine toimub täiesti teistsuguse klienditarkvaraga ning toimingul on demokraatia seisukohast fundamentaalsem tähendus kui igapäevasel kasutusel.
11. Ökosüsteemi teenindava **tarkvara uuendamine** (kaardilugeja draiverid, DigiDoc, brauseripluginad)

4.1.2 Liidestatud ja tootestatud universaalteenus

Universaalteenused on väga kitsad, ühtainukest funktsiooni pakkuvad teenused, millele tuginevad kasutajatoimingud. Universaalteenustega ühendumine toimub konkreetses tarkvaras ning need on eelduseks kasutajatoimingute läbiviimisele.

Universaalteenused on järgmised:

- **TSL**ide ehk usaldusnimekirjade haldamine ja avaldamine. Näiteks on olemas Eesti usaldusteenuste nimekiri (<https://sr.riik.ee/et/usaldusteenus/>) ning ELi usaldusnimekirjad (<https://eid.ec.europa.eu/efda/trust-services/browse/eidas/tls/>);
- **LDAP**-teenus sertifikaatide otsinguks. Seda teenust kasutatakse näiteks CDOC-konteinerite loomisel, et kuvada kasutajale inimeste nimed, kes saavad oma eID-vahenditega konteinereid lahti krüpteerida;

⁸ TeRa ei uuendanud konteineris olevat allkirja, vaid allkirjastas kogu konteineri uuesti.

- **Sertifikaadi kehtivuse kontrolli** teenus, mis esineb kahel kujul:
 - **OCSP**-päringutele vastamine;
 - (teatud vahendite puhul) tühistusnimekirja (**CRL**) serverimine.

4.1.3 Koosvõimeteenus

Koosvõimeteenuseid reguleerib ELi ühtse digivärava määrus (*Single Digital Gateway Regulation, SDGR*) [76]. Selle artikkel 14 ütleb, et andmeid peaks koguma vaid üks kord – põhimõte, mis Eestis X-tee puhul realiseeriti juba 2004. aastal. E-identimise ja usaldusteenuste määrus eIDAS näeb ette kohustuse riikidevaheliseks ristautentimiseks ning kohustab iga riiki sisse seadma nn eIDAS-Node'i, mille kaudu sisselogimisel toimub automaatne infovahetus.

Eestis on saadaval järgmised ristautentimiskeskonnad:

- **eIDAS-Node:**
 - Eesti residendist autentija tuvastamiseks ELi portaalidele;
 - ELi riigi (üksikutel juhtudel ka ELi-välise riigi) residendist autentija tuvastamine Eesti portaalides;
 - kaks eelnevat loetletud funktsiooni on realiseeritud TARA vahendusel;
- **TARA/GovSSO** – sisselogimiskiht vahendite ja teenuste vahel. Teenused saavad TARA ja GovSSO teenust kasutada vastavalt protokollile OpenID Connect [77];
- **erasektori lahendused** – teised erasektori poolt arendatud lahendused, nagu eeid, eID Easy, Dokobit, jms.

4.2 Tugiteenused

ENISA DISi (vt jaotis 2.1) mõistes tugiteenusteks loetakse järgnevaid teenuseid.

- **Ajatempliteenus.** Ajatempel kinnitab, et miski (tõend, digiallkiri) oli loodud enne teatud ajahetke.
- **Digiallkirja valideerimise teenus.** Eestis täidab allkirjade tehnilise valideerimise ülesannet RIA pakutav valideerimisteenus SiVa. eIDASi määruse keskse e-allkirja valideerimisteenuse mõiste on siiski laiem ning SiVa pole EU usaldusnimekirjas kajastatud kvalifitseeritud (ega ka kvalifitseerimata) e-allkirja valideerimisteenus.
- **Säilitusteenus.** Võimaldab tagada allkirja kehtivust (näiteks pika kehtivusajaga laenulepingul) ka siis, kui mõne krüptograafilise primitiivi (lõplik krüptograafiliste algoritmide kogum mingiks otstarbeks, nagu räsialgoritm või signeerimisfunktsioon) turvalisus on vähenenud või signeerimisel kasutatud võtmepaari kunagist kehtivust ei ole praegu võimalik enam selgelt tuvastada. Eestis säilitusteenus seni puudub. Eestis kasutusel olnud allkirjade ületembeldamislahendust (TeRa) tuleb käsitleda kas rakenduse või ühekordse toiminguga võtmes, kuna see toimis ilma keskse teenuse olemasoluta.
- **Digiallkirja loomise teenus.** Digiallkirja loomiseks on mitmeid variante, kuid juhtudel, kus digiallkirja andmist pakutakse internetis, on otstarbekas konteiner vormindada otse serveris. Võimalikud on erinevad manipulatsioonid konteineriga – atribuutide lisamine ja vormindamine – enne kui kasutaja dokumendi lõplikult allkirjastab (vt joonis 6).

4.3 Abitoimingud

Kasutusel on ka mitmed abitoimingud, mida ei saa pidada otseselt kasutaja tahtlikeks/teadlikeks tegevusteks, kuid mis on kvaliteetse tulemuse saamiseks vajalikud.

Nendeks abitoiminguteks on:

- LoTLi ja TSLi hankimine DigiDoci tarkvara käivitamisel,
- sertifikaadiahela kontroll,
- tarkvarakonfiguratsiooni haldus – juhul kui kasutajatarkvara on vananenud, sunnitakse kasutajat seda uuendama,
- allalaadimiskoormuse ajaline hajutamine standardtarkvara järgmise versiooni hankimisel.

Neis kontekstides suhtleb DigiDoci rakendus kasutaja eest universaalteenuste ja toetavate serveritega.

5 E-identiteedi kasutusjuhud ja integratsioon

Elektroonilise identiteedi kaks olulisimat väärtusteenust on **autentimine** ja **digiallkirja andmine**. Selles jaotises tutvustame olulisemate kasutusjuhtude sisulist külge ning vaatleme, kuidas on korraldatud nende integratsioon Eesti eID ökosüsteemi toimimist tagavate tagateenustega. Jaotis kirjeldab lõppkasutaja toimingute (kasutusjuhtude) praktilist integratsiooni Eesti eID ökosüsteemiga. Kõige mahukamad näited käsitlevad digiallkirjade andmist ja loodud allkirjade valideerimist, kuivõrd esitatud nõuete ja täidetavate tehniliste normide vaatepunktist on see keerulisim kasutusjuht.

eID-teenuste realiseerimiseks on RIA koos partneritega loonud eID-tarkvara standardkomplekti nii serveri poolele kui ka kasutaja poolele. eID-tarkvara üldist arhitektuuri kirjeldab allikas [78].

5.1 Autentimine

Autentimine tähendab kasutaja isikusamasuse (väidetava identiteedi) tõestamist kas süsteemis endas või mõne välise süsteemi kaasabil.

Eestis on infosüsteemide puhul tavaks kasutada mõnele eID-vahendile tuginevat lahendust. e-identimise skeeme on Eestis hetkel kolm: ID-kaart, mobiil-ID ja Smart-ID. ID-kaart ja mobiil-ID kuuluvad kategooriasse „teavitatud“ (*notified*)⁹. Smart-ID pole „teavitatud“, aga on siseriiklikuks kasutamiseks „hinnatud“, mis tähendab, et on RIA poolt kokku kutsutud ekspertrühm leidis, et eIDAS määruses kirjeldatud meetodika põhjal vastab Eesti isikukoodiga isikutele väljastatud Smart-ID elektroonilise isikutuvastuse tasemele „kõrge“ [84].

Isikusamasuse tehniline kontroll veebitehnoloogiate raames seisneb toimingus, kus kasutajal tuleb eID-vahendis asuva privaativõtme allkirjastada serveri poolt edastatud seansiga seotud andmed (sealhulgas ka juhuslikult genereeritud nonss¹⁰) ning tagastada signatuur ning autentimissertifikaat. Seejärel kontrollib server näiteks OCSP-teenuse kaudu, kas sertifikaat on kehtiv ning kas selle on väljastanud usaldatud sertifitseerimisasutus. Seejärel kasutab server sertifikaadis olevat avalikku võtit ja kontrollib, kas talle esitatud krüptograafiline signatuur on kehtiv ning kas see loodi serveri poolt edastatud andmetele. Kui kõik kontrollid on edukad, siis saab järeldada, et seansis osaleval kasutajal on kontroll oma eID-vahendi üle ning sertifikaadis esitatud kasutaja identiteet on tuvastatud. Sellise autentimislahenduse puhul võib ka öelda, et tegemist on infosüsteemi suhtes **välise autentimisvektoriga**.

Autentimisnormatiiv ([1], jaotis 5 p 1) esitab avaliku sektori infosüsteemidele kaks põhilist nõuet. Kõigepealt ei tohiks autentimismoodulit iseseisvalt ehitada, vaid sel otstarbel tuleks kasutada RIA teeke. Lisaks peaks autentimismoodul olema infosüsteemist eraldatud. See on suur erinevus võrreldes süsteemidega, mis eID võimalusi ei kasuta, kuivõrd neil jääb üle pidada lokaalselt arvet isikute, nende identiteetide ja eID-vahendite või kasutajanimede ja paroolide (mandaadid, ingl *credentials*) üle, mis tõstab süsteemi keerukust.

⁹ Tegemist on eIDASi terminitega – nimetatud skeemid on teavitatud Euroopa Komisjonile. e-identimise skeemide ja teavitamise nõuete kohta saab lähemalt lugeda eIDAS määruse jaost 2.

¹⁰ Üksainus kord kasutatav arv, enamasti juhuslik või pseudojuhuslik.

Autentimine saab toimuda kas otse e-teenust pakkuvasse infosüsteemi või muude vahendavate süsteemide toetusel, nagu autentimisteenused (TARA, GovSSO). E-teenuse osutaja nimetamiseks kasutatakse tihti lühendit RP (*relying party*) ehk tuginev isik.

Põhjalikult käsitletakse autentimistoimingute detaile analüüsi „SPOF2.1. Autentimis-protokollistikud“ [77] jaotises 3.

5.2 Digiallkirja andmine

Eestis on enamjaolt kasutusel eIDASis defineeritud kvalifitseeritud e-allkiri, mis on Eestis võrdsustatud EUTSi kaudu terminiga „digiallkiri“. Samas üldisemalt, e-allkirja andmine, tähendab eIDASi kohaselt ükskõik missugusel eIDASis loetletud tasemel elektroonilise allkirja andmist.

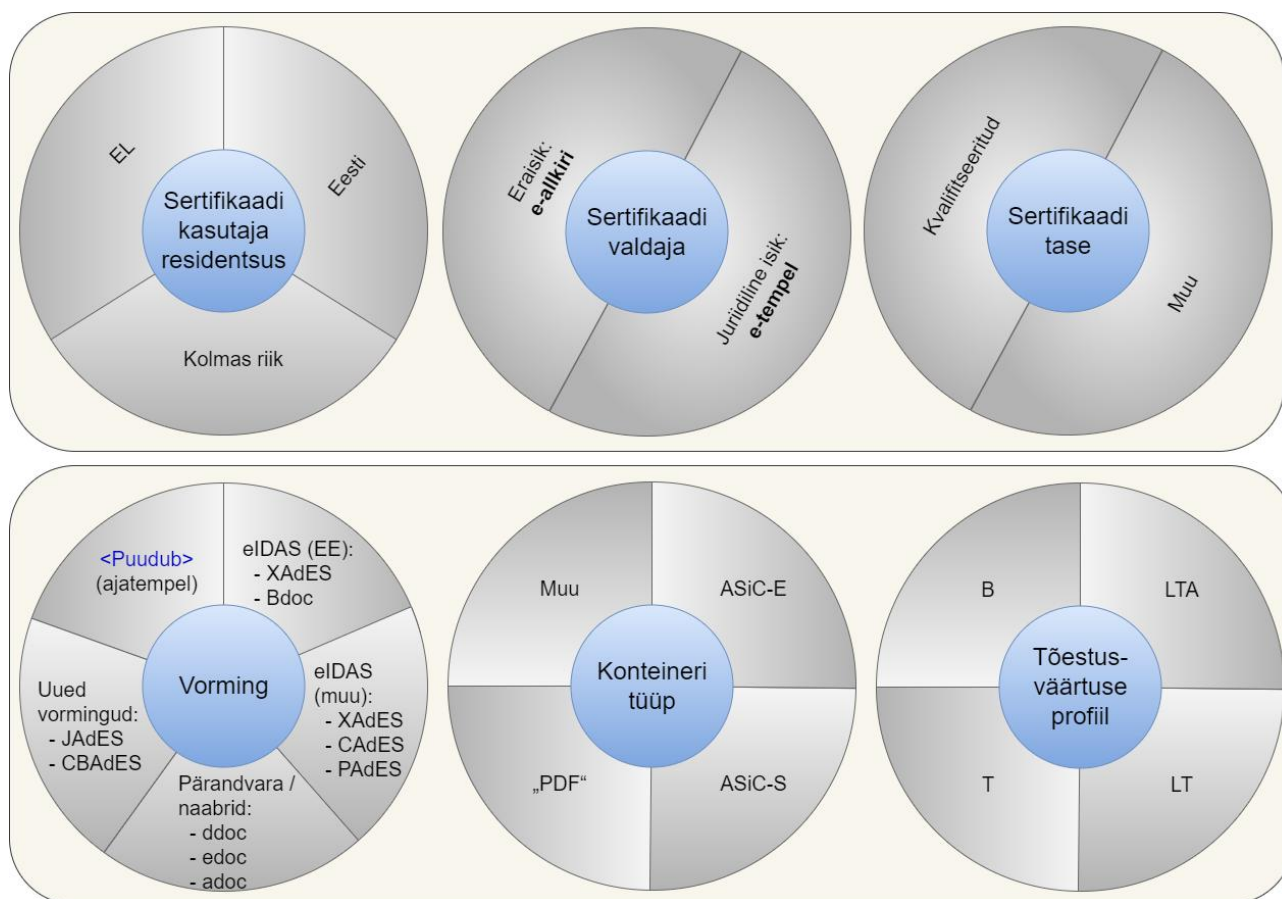
E-allkirja andmine kui tegevus on autentimisest keerukam, see on tingitud teostusdetailide ja näiteks andmeformaate rohkusest. Kõigepealt määratleb eIDAS e-allkirjade usaldustasemed (QES, AdES/QC, AdES, muu, vt lisa A.2) ning tehnilised standardid kirjeldavad e-allkirjade erinevad parameetreid. Arvestada tuleb järgmiste elementidega:

- **allkirjavormingud** (XAdES, CAAdES, PAdES, vt lisa B.3)
- **allkirjastamisel kasutatava sertifikaadi tase** (kvalifitseeritud, muu)
- **konteineri tüübid** (ASiC-S, ASiC-E, PDF, ilma konteinerita)
- **tõestusväärtuse profiilid** (*Basic, Timestamped, Long-Term, Long-Term Archival*)

Lisaks rahvusvaheliselt kasutatavatele standarditele võivad riigis leiduda ka kohalikud lahendused. Eesti puhul on olnud nendeks eelkõige allkirjavormingud **ddoc** ja **bdoc**. Nüüdseks saab nendes vormingutes allkirju vaid valideerida, juurde luua nendes vormingutes allkirju enam ei saa, vt [79].

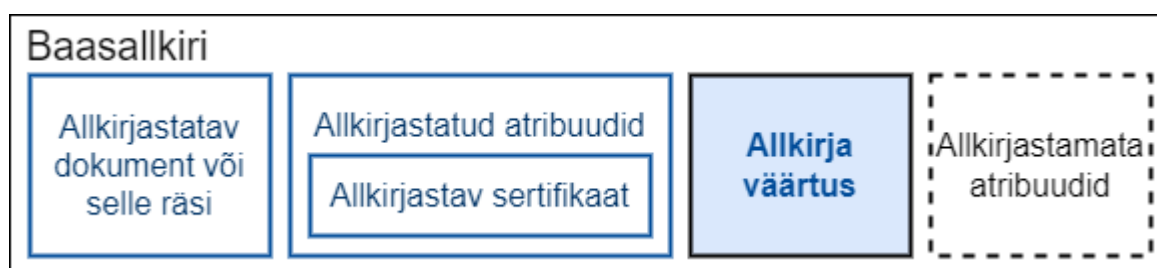
Õiguslikel põhjustel eristatakse füüsilistele ja juriidilistele isikutele väljastatud sertifikaate. Kuigi need võivad tehniliselt olla väga sarnased, nimetatakse juriidilise isiku antud e-allkirja ELis „e-templiks“ (*e-Seal*).

Joonis 3 koondab e-allkirjadesse puutuvad erinevad elemendid graafiliselt, osutades, missugused valikud võivad igas kategoorias ette tulla.



Joonis 3. E-allkirjade olulisimad elemendid

Veel üks oluline kategooria on allkirja tõestusväärtuse profiil. Joonis 4 kujutab baasallkirja (*Basic Signature*), mille eeliseks on lihtsus ja puuduseks on ajatempli kaitsmatus (ehk ei ole võimalik kindlaks teha allkirja andmise aega).

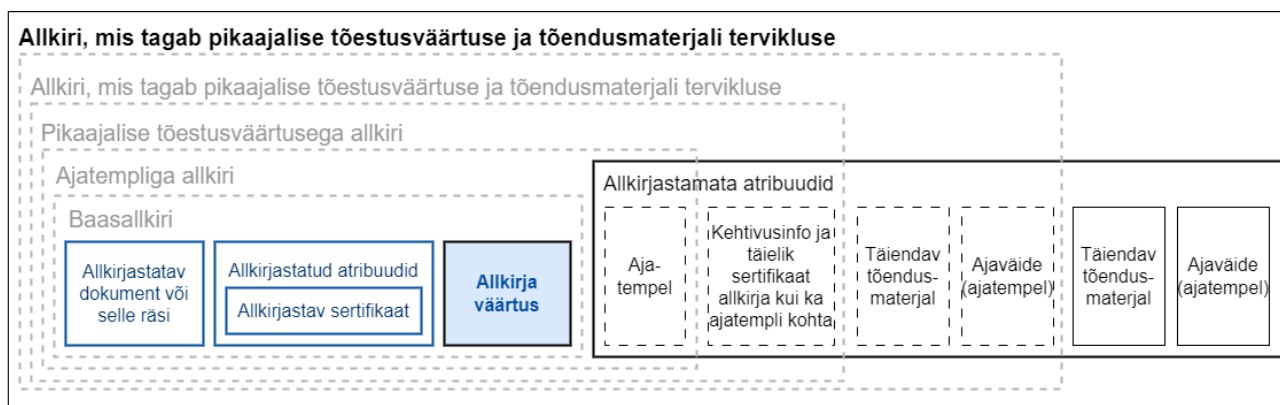


Joonis 4. Baasallkiri¹¹

Joonis 5 kujutab pikaajalise tõestusväärtusega allkirja. Esimene ajatempel on signatuuriajatempel. Üksteisele järgnevad punktiirjoontega tähistatud alad märgivad allkirja keerukuse tõusu (tasemed: *Basic (B)*, *timestamped (T)*, *long time (LT)*, *long time archival (LTA)*). Täisulatuses kujutab joonis endast LTA allkirja, mis on tasemel LTA veel kord üle tembeldatud – vajadus selleks võib tekkida näiteks krüptoprimitiivi turvalisuse vähenemise tõttu. Ületembeldamise vajadus võib allkirja pikaajalise

¹¹ Standardist ETSI EN 319 102-1 [35].

säilitamise vältel tekkida korduvalt. Ületembeldamise praktilist külge me ei vaatle, kuivõrd see pole Eesti eID ökosüsteemi teenusena korraldatud.

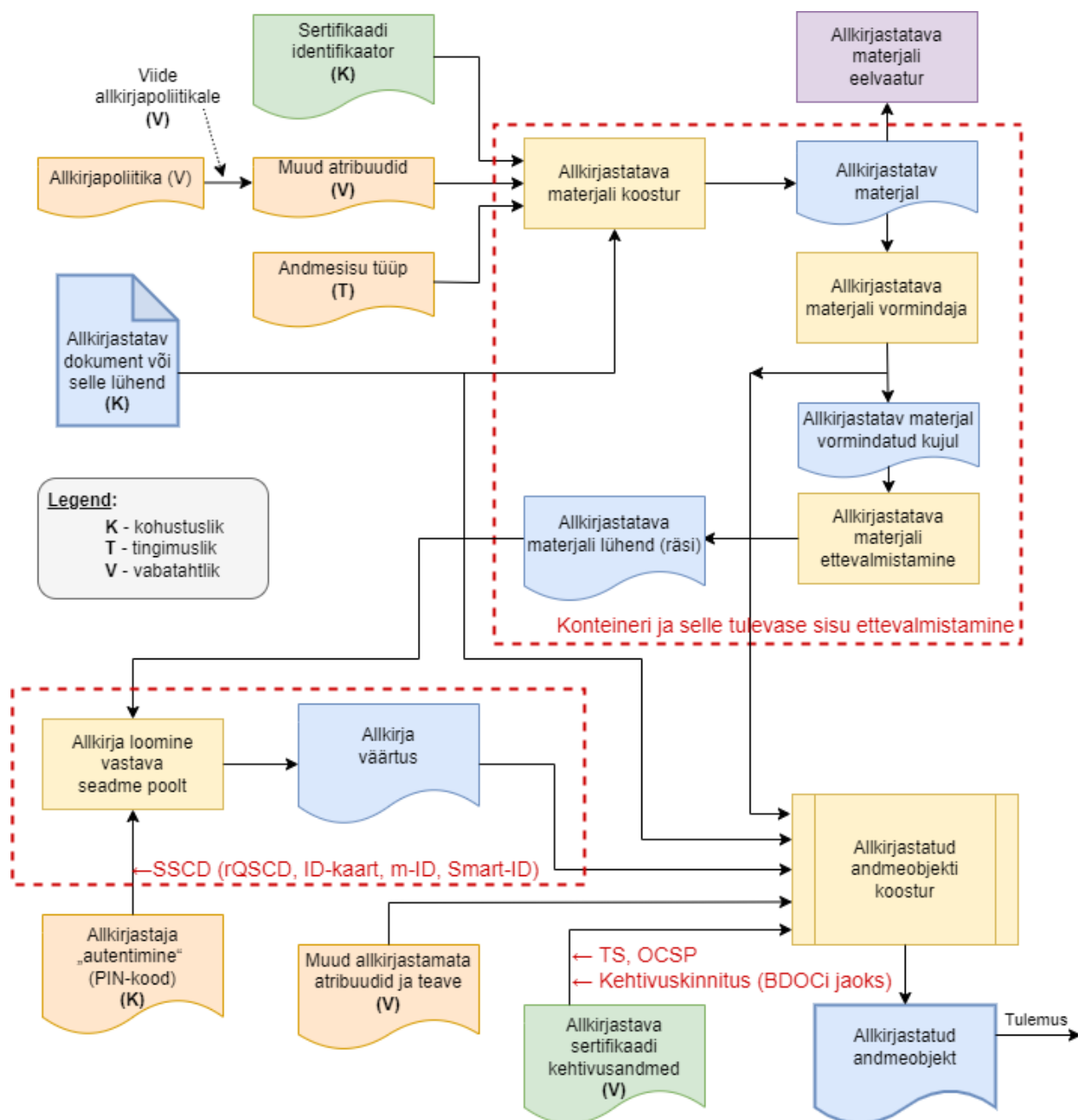


Joonis 5. Allkirja keerukuse ja tõestusväärtuse järkjärguline tõus¹²

5.2.1 Digiallkirja loomine

Standardist EN 319 102-1 [35] pärit joonis 6 kirjeldab allkirja loomise protseduuri. Jooniselt nähtub, et vahendi valdaja sekkumist vajatakse alles allkirja loomise viimases järgus. See annab võimaluse allkirjakonteineri eelnevaks ettevalmistamiseks. Juhul kui allkirjastatakse teenuses (näiteks transaktsiooni), siis on loomulik, et konteiner valmistatakse ette serveris.

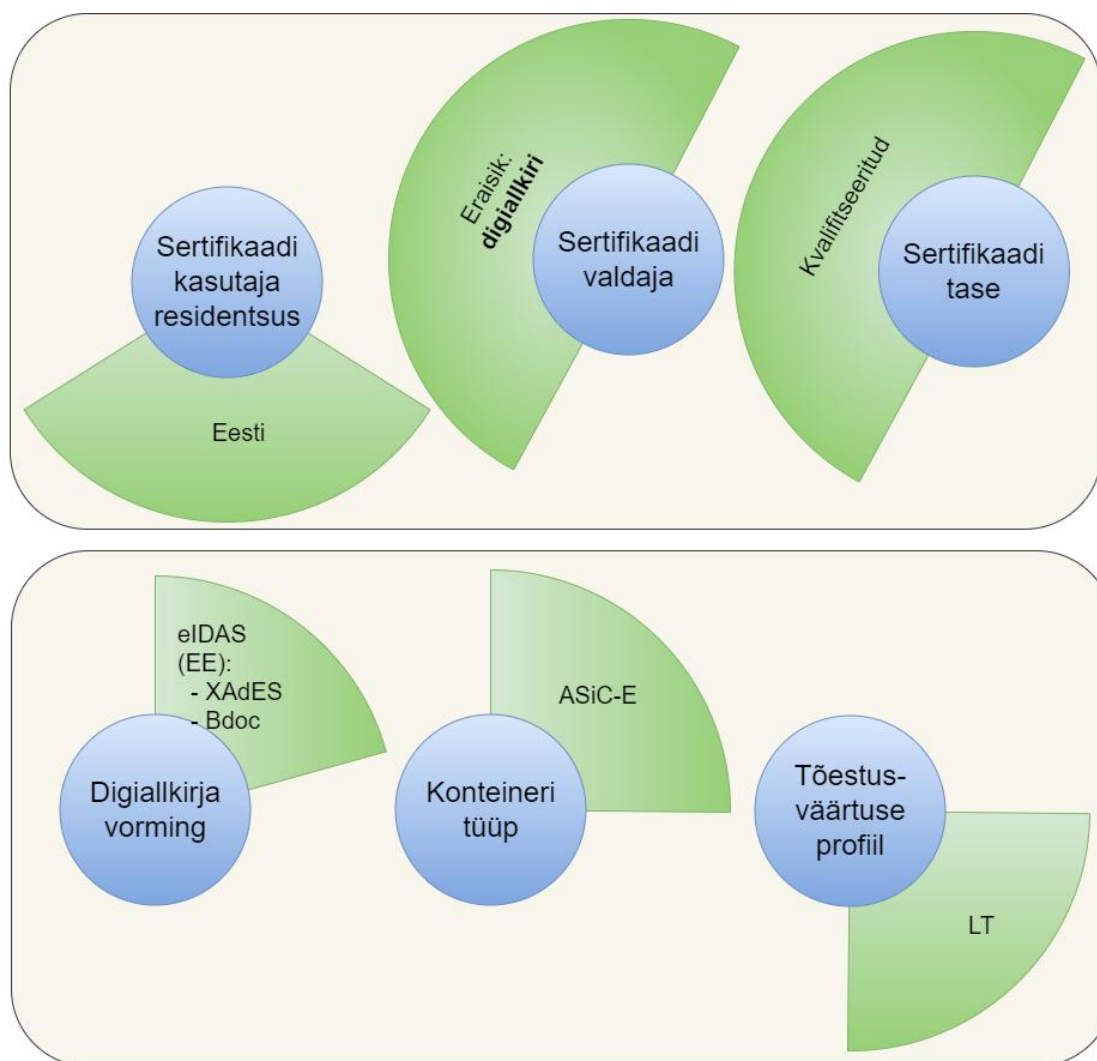
¹² Standardist ETSI EN 319 102-1.



Joonis 6. Allkirja moodustamine¹³

Eesti riiklikud allkirjade loomise tööriistad (DigiDoc4, RIA DigiDoc'i mobiilirakendus, teegid **digidoc4j** ja **libdigidocpp** ning teenus SiGa) loovad täna sellise struktuuriga digiallkirju (digiallkirju, ehk eIDAS tähenduses kvalifitseeritud tasemega e-allkirju), nagu kujutab joonis 7. Rohelise värviga on tähistatud parameetrite väärtused, mis on loodud digiallkirjal. Vajaduse korral on võimalik valideerida vanemas vormingus (nt BDOC) allkirju, mida vajatakse pärandvara süsteemide käiguhoidmiseks, kuid juurde luua selles vormingus allkirju enam ei saa.

¹³ Ümber töötatud standardist EN 319 102-1.



Joonis 7. Eestis loodavate digiallkirjade vaikeparameetrid

Digiallkirjade loomise üksikasju Eesti eID ökosüsteemis kirjeldab lisa B.2.

5.2.2 Digiallkirja valideerimine

E-allkirja valideerimise nõuded tulevad eIDASi määrusest [5]. Digiallkirja (ehk kvalifitseeritud e-allkirja) valideerimise nõuded on kehtestatud eIDASi määruse artiklis 32. Täiustatud e-allkiri peab vastama määruse artiklis 26 toodud tingimustele. E-allkirja (QES või AdES/QC tase) andmisel kasutatud kvalifitseeritud sertifikaat peab vastama eIDASi määruse I lisa tingimustele. See teeb valideerimisteenuse reeglistiku suhteliselt keerukaks.

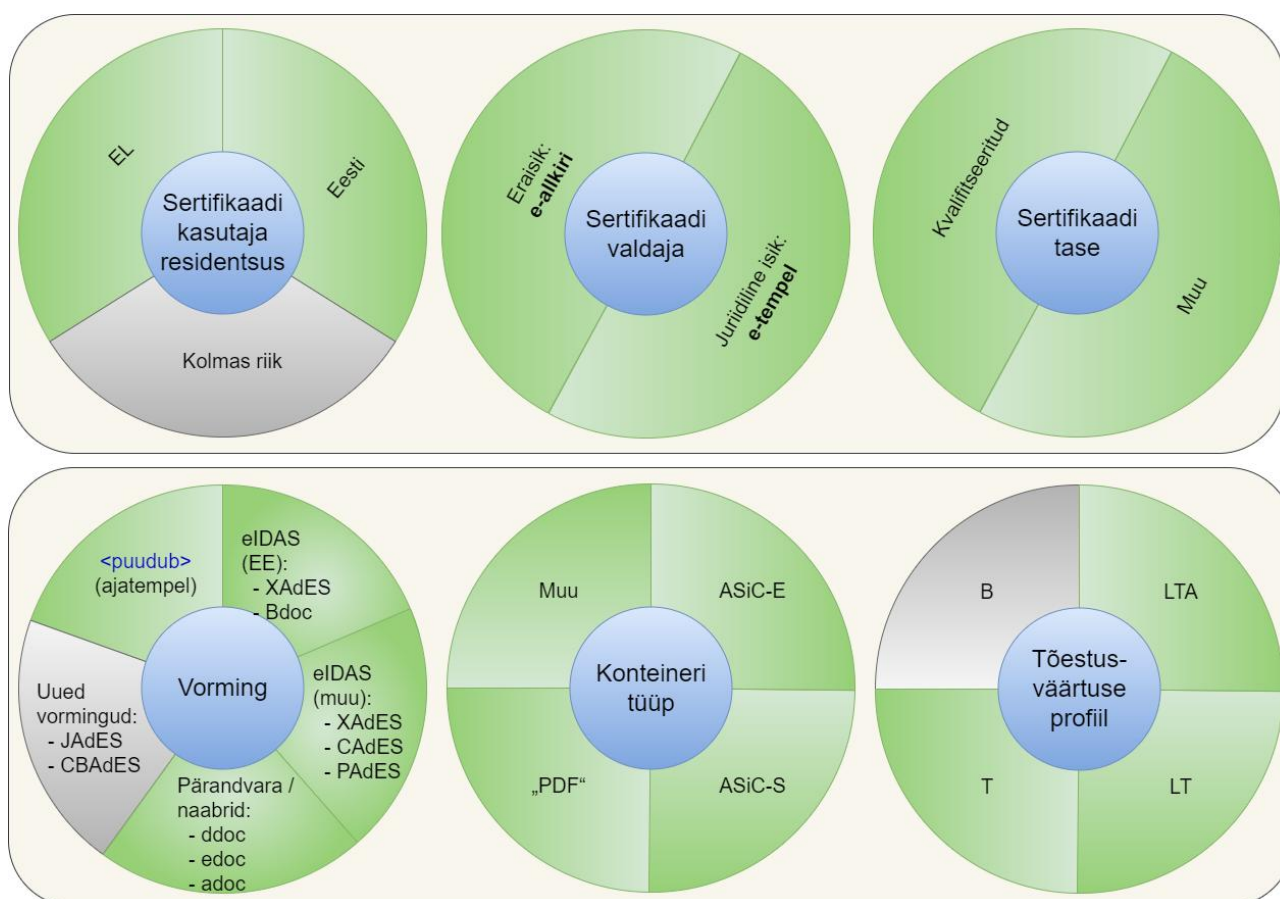
E-allkirjade (või kitsamalt digiallkirjade) valideerimiseks võib kasutada nii kasutaja arvutis töötavat tarkvara kui ka serveris töötavaid lahendusi. Raskusi võib tekitada erinevate signatuuriformaatide ja usaldustasemetete rohkus.

Idealmaailmas annavad allkirjade valideerimise kõik viisid sama tulemuse, kuid praktika võib erineda. Nii näiteks võivad kommertsiaalsed lahendused keskenduda mingile konkreetsele

segmendile ning eirata kõike sellest väljapoole jäävat. Teise näitena võib Eesti päritolu teenusel tekkida soov eirata Eestis vähepopulaarseid PDF-failidele lisatud allkirju, mis on väga levinud ülejäänud maailmas ning mis võivad sisaldada nii madalama taseme e-allkirju kui ka kvalifitseeritud e-allkirju.

Eesti olulisimateks valideerimislahendusteks on keskne teenus SiVa ning rakendustega DigiDoc4 ja RIA DigiDoc kaasnevad võimalused. Lahknevuste tekkimisel tuleb eelkõige lähtuda SiVa tulemustest, kuivõrd SiVa käsitusala on laiem (hõlmates näiteks ka X-tee allkirju), äratuntavate allkirjavormingute hulk suurem. Muuhulgas kasutavad DigiDoc4 ja RIA DigiDoc osade allkirjavormingute valideerimiseks SiVa teenust.

Joonis 8 koondab teabe selle kohta, missuguseid allkirjade aspekte on valideerimisteenus SiVa võimeline ära tundma.



Joonis 8. SiVa valideerimisvõimalused

Rohelise värviga on märgitud aspektid, mida SiVa on võimeline e-allkirjades tuvastama ja valideerima. Halli värviga on märgitud aspektid, mille tuvastamisega SiVa nõudluse puudumisel täna ei tegele. AdES/QC taseme allkirjad, mis kehtivad ka Eestis, kuid kuna Eesti ise kasutab enamjaolt QES taseme allkirju, võib juhtuda, et AdES/QC usaldustasemega allkirja valideerimine ei toimi (mis aga on juriidiline, mitte tehniline sobimatus).

DigiDoc4 ja RIA DigiDoc rakenduste võimalused allkirjade eri aspektide tuvastamisel on SiVa omast veidi piiratumad.

5.3 Krüpteerimine

CDOC [80] on nimetus Eesti-spetsiifilisele **transpordikrüptograafia ja säilituskrüptograafia** lahendusele, mis võimaldab mitmele vastuvõtjatele edastada saatja poolt krüpteeritud konteinerisse lisatud faile. Lahendus kasutab ära juba toimivat eID ökosüsteemi ning asjaolu, et vastuvõtjate identiteedihaldus on juba korraldatud, kõigil vastuvõtjatel on olemas vastavad eID-vahendid ning eID-vahenditel asuvaid asümmeetrilisi krüptovõtmeid saab ära kasutada ka andmete dekrüpteerimiseks.

Krüpteerimise ja dekrüpteerimise funktsioonid on integreeritud lauaarvutis töötavasse rakendusse DigiDoc4 või mobiiliseadmes töötavasse rakendusse RIA DigiDoc. Sedaviisi on krüpteerimise ja dekrüpteerimise funktsioon kõigile eID ökosüsteemi kasutajatele kohe kättesaadav ning nad ei pea endale lisatarkvara hankima. Konteinerite vastuvõtja ei pea selleks midagi spetsiaalset tegema, et saatja temale konfidentsiaalseid faile edastama saaks hakata.

Krüptokonteineri failinime laiendiks on *.cdoc või *.cdoc2. Lisaks avatud lähtekoodiga rakendustele DigiDoc4 ja RIA DigiDoc on CDOC-konteineritega töötamiseks loodud Java ja C++ programmeerimiskeelte jaoks avatud lähtekoodiga teegid cdoc2-lib (<https://github.com/open-eid/cdoc2-java-ref-impl>) ja libcdoc (<https://github.com/open-eid/libcdoc>)

Lisaks failide edastamisele ühelt kasutajalt teisele (transpordikrüptograafia) lisatakse CDOC-lahendusele järgmises versioonis ka failide säilitamise võimalus (säilituskrüptograafia), kasutades tavalist parooli või sümmeetrilist krüptovõtit. Transpordikrüptograafia vahenditega kaitstud konteinereid ei saa pikaajaliselt säilitada, kuna ID-kaardi vahetamisel või võtmete uuendamisel ei saa enam vanale ID-kaardile krüpteeritud konteinereid avada.

Tehniliselt krüpteeritakse konteineris olevad failid uue sümmeetrilise võtmega, mis omakorda kaitstakse sedaviisi, et seda saab lahti krüpteerida ainult vastuvõtja eID-vahendil oleva privaatvõtmega. Mitme vastuvõtja puhul või mitme eID-vahendi puhul krüpteeritakse sümmeetriline võti igale vastuvõtjale või igale eID-vahendile eraldi.

Hetkel töötab CDOC-lahendus ID-kaardi ning krüptopulkadega. CDOC-lahendust arendatakse praegu edasi, et võimaldada ka mobiil-ID ja Smart-ID vahendite kasutamist. Kuna mobiil-ID ja Smart-ID ei võimalda krüptograafiliste võtmekehtestusalgoritmide kasutamist, siis täpselt samasugust krüptoskeemi, nagu ID-kaardi puhul, ei ole võimalik kasutada. Mobiil-ID ja Smart-ID kasutamisel toimub krüptokonteineri krüptovõtme (võtmekapsli) edastamine läbi spetsiaalsete vahendusserverite. Krüptokonteiner ise edastatakse saatjalt vastuvõtjatele kas e-maili või muu transpordi vahendusel.

Vahendusservereid saab olema rohkem kui üks ning neid hakkavad haldama erinevad organisatsioonid. Edastatud konteineri dekrüpteerimiseks vajalik võtmekapsel jagatakse matemaatiliselt sõltumatuteks osakuteks ning saatja laadib osakud erinevatesse vahendusserveritesse. Sellisel juhul ei saa ründaja kontrolli alla sattunud üksik vahendusserver iseseisvalt konteinerit avada, kuna tal ei ole kõiki võtmekapsli osakuid. Konteineri vastuvõtja peab võtmekapsli kõik osakud vahendusserveritest alla laadima ning kogu kapsli osakutest kombineerima.

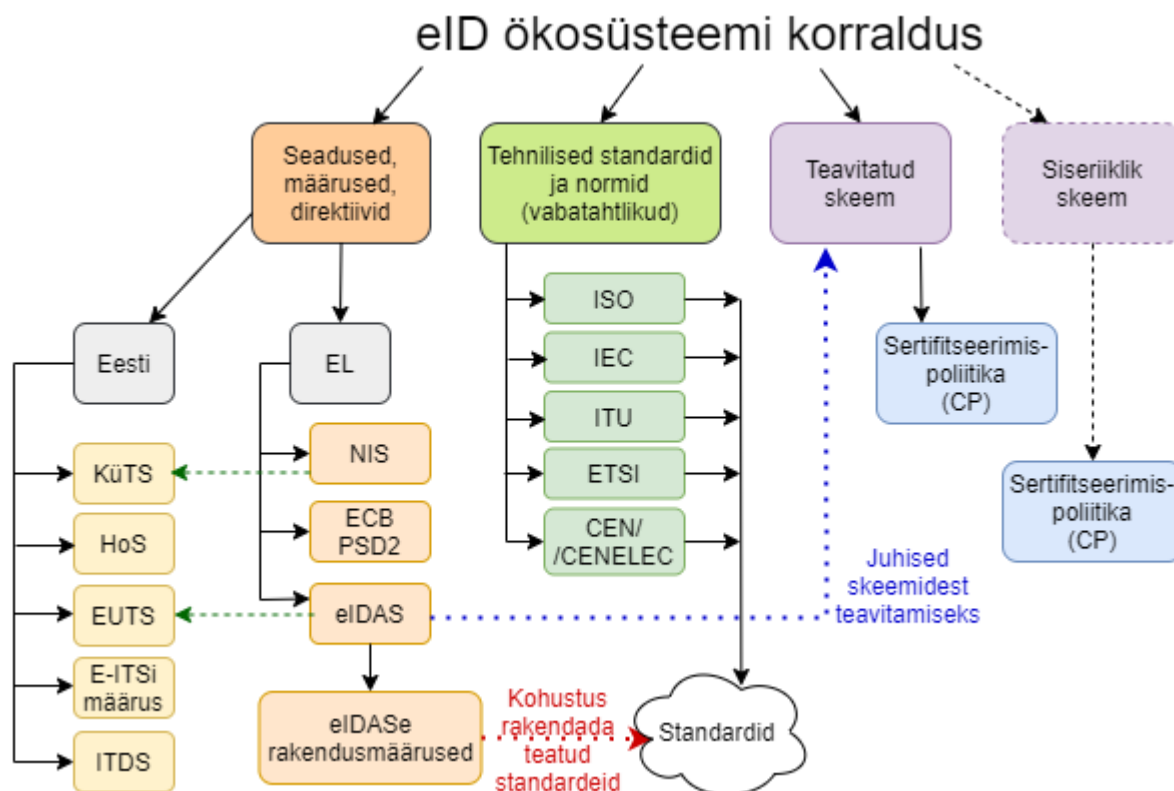
Allalaadimiseks kasutatakse vastuvõtja autentimist kas ID-kaardi, mobiil-ID või Smart-ID vahenditega. Seejärel saab vastuvõtja krüptokonteineri lahti krüpteerida ning saab juurdepääsu edastatud failidele.

CDOCi funktsioonistikku on lähemalt kirjeldatud allikates [81] ja [82].

Lisa A. E-identiteedi ökosüsteemi normatiivsed raamid

Eesti eID ökosüsteemi korralduslik taust moodustub õigusaktidest (seadustest, määrustest, rakendusaktidest, direktiividest) ning koostalitlusvõimet tagavatest tehnilistest standarditest. Oluline on mõista, et tehniline standard ei pruugi olla kohustuslik seni, kuni seadus vastavat kohustust ei sätesta. Standardid on kohustuslikud üksnes ulatuses ja kontekstis, mis on määratletud mõnes konkreetses õigusaktis. Kohati on vastavus teatud standarditega siiski ka vaike-eelduseks.

Joonis A.1 illustreerib Eesti eID ökosüsteemi korralduslikku tausta. Põhinõuded nii autentimisele ja digiallkirjastamisele on sätestatud eIDASi määruses [5]. Ühtlasi kohustavad eIDASi rakendusaktid (vt lisa B) juhinduma ökosüsteemi ülesehituses ja tehniliste vahendite valimisel teatud standarditest.



Joonis A.1. Eesti eID ökosüsteemi korraldus

A.1. Isikut tõendavate dokumentide seadus

Isikut tõendavate dokumentide seadus (ITDS) [3] esitab loetelu isikut tõendavate dokumentide seaduse alusel väljaantavatest dokumentidest. Tabel A.1 kajastab vastavust nimetatud loetelus olevate isikut tõendavat dokumentide, nende füüsiliste kandjate ja võimaliku elektroonilise sisu vahel. Kuigi Smart-ID ei ole isikut tõendavate dokumentide seaduses loetletud dokument, on Smart-ID võrdluse eesmärgil tabelisse siiski lisatud. Tabelist nähtub, et kolmest Eesti autentimis- ja digiallkirjade andmise vahendist kaks ei ole füüsiliste dokumentidega üldse seotud. Pass sisaldab küll kiipi, kuid ei ole eID-vahend.

Tabel A.1. ITDS loetletud isikut tõendavate dokumentid ja nende füüsilise ja digitaalse (eID-vahendina) kasutuse võimalused

		eID vahend							
		ID-kaardid			Muu				
Isikut tõendav dokument (ITDS § 2)	Kasutav eID vahendina	ID-kaart (kui isikutunnistus)	Elamisloakaart	Digitaalne isikutunnistus ehk Digi-ID	E-residendi digitaalne isikutunnistus	Diplomaatiline isikutunnistus	Mobiil-ID	Smart-ID	
		1) Isikutunnistus (ID-kaart)	Jah	Füüsiline ja digitaalne kasutus			Üksnes digikasutus		
1 ²) Elamisloakaart	Jah		Füüsiline ja digitaalne kasutus						
1 ¹) Digitaalne isikutunnistus (digi-ID)	Jah			Üksnes digikasutus					
2) Eesti kodaniku pass	Ei - kiip ei sobi eID jaoks								
3) Diplomaatiline pass	Ei - kiip ei sobi eID jaoks								
5) Välismaalase pass	Ei - kiip ei sobi eID jaoks								
6) Ajutine reisidokument	Ei - kiipi pole								
7) Pagulase reisidokument	Ei - kiipi pole								
4) Meremehe teenistusraamat	Ei - kiipi pole								
8) Meresõidutunnistus	Ei - kiipi pole								
9), 10), 11), 12)	-								

A.2. E-identimise ja usaldusteenuste määrus (eIDAS)

eIDAS (inglise keeles **electronic IDentification, Authentication and Trust Services**)¹⁴ on Euroopa Liidu e-identimise ja e-tehingute määrus [5], mis võeti vastu 23.07.2014. Määrus loodi, kuivõrd liikmesriigid ei järginud 1999. aasta direktiivi sätteid ega edendanud elektrooniliste allkirjade andmist ja kaugtuvastamist eeldatud määral. Kasutati otsekohalduva määruse vormi, et võtta riikidelt suuniste eiramise võimalus. 11. aprillil 2024 võeti vastu oluliselt uuendatud ja täiustatud eIDASi määrus (nn eIDAS 2.0).

eIDAS defineerib elektroonilise allkirja neli taset:

- muud elektroonilised allkirjad (nt sellised, mida mõned erafirmad¹⁵ kasutavad lepingutele elektrooniliste allkirjade lisamiseks tahvelarvutite ekraanil)
- täiustatud elektrooniline allkiri (AdES)

¹⁴ Kohati esineb lühend ka punktiga: eID.AS: electronic IDentification, Authentication and trust Services.

¹⁵ Telia, kullerifirmad (nt DPD).

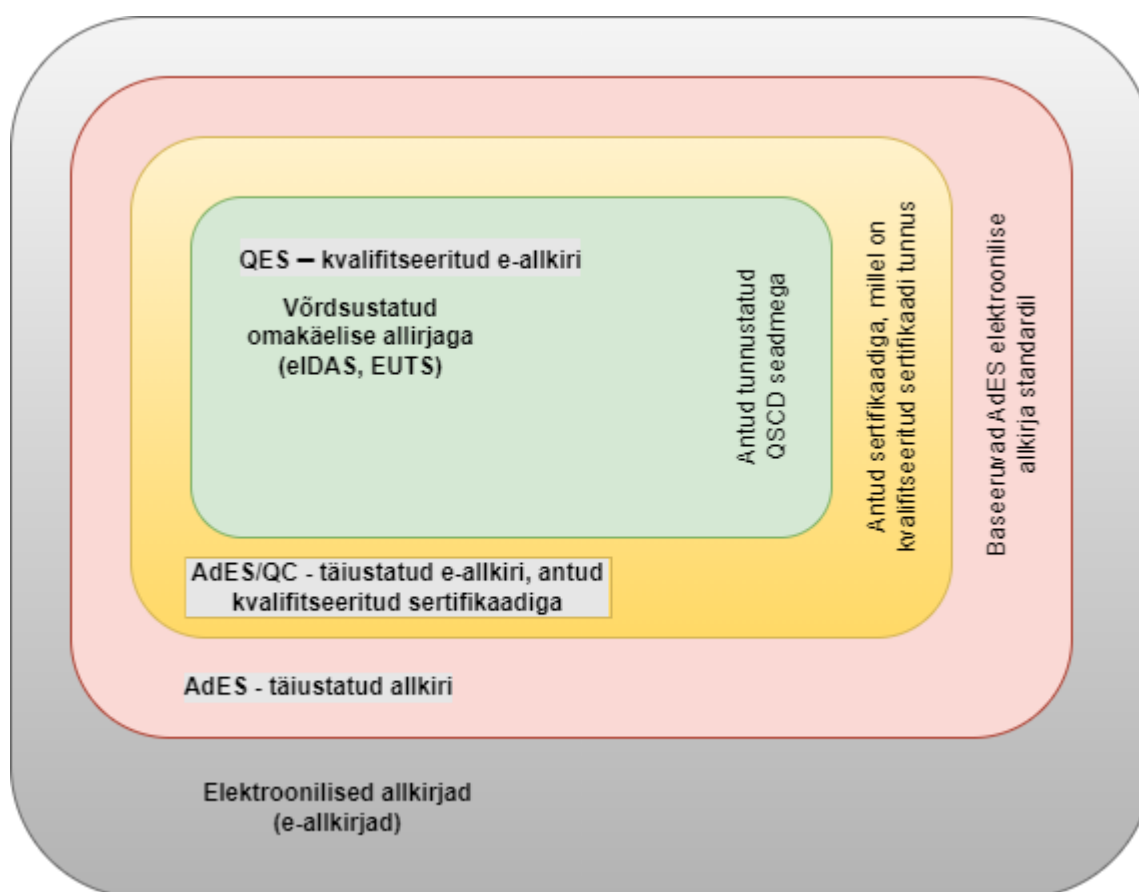
- elektroonilise allkirja kvalifitseeritud sertifikaadil põhinev täiustatud elektrooniline allkiri (AdES/QC)
- kvalifitseeritud elektrooniline allkiri (QES) – kõrgeim tase

Joonis A.2 esitab e-allkirja tasemete kihtmudeli. Nii eIDAS [5] kui EUTS [6] võrdsustavad QES-taseme allkirja omakäelise allkirjaga. Digiallkirjaks tohib nimetada vaid kõige ülemist, QES-taset, muul juhul on tegemist elektroonilise allkirjaga.

Autentimise kontekstis defineerib eIDAS kolm **kindlustaset**¹⁶ (LoA – *level of assurance*¹⁷):

- madal (ISO/IEC 29115 LoA 2),
- märkimisväärne¹⁸ (ISO/IEC 29115 LoA 3) ja
- kõrge (ISO/IEC 29115 LoA 4).

Lahenduste osas, mis ühelegi neist kolmest tasemest ei vasta, kasutatakse nimetust „määratlemata“ (sh ISO 29115 LoA 1). Ühe 2022. aasta uurimuse kohaselt [15] on Euroopas kokku teavitatud 40 skeemist: 25 skeemi toetasid taset *LoA High*, 20 skeemi taset *LoA Substantial* ning 12 skeemi taset *LoA Low*. ENISA DIS [12] suhtestab autentimisalased nõuded standardiga ISO/IEC 29115.



Joonis A.2. e-allkirjade usaldustasemete kihtmudel

¹⁶ Tõlgitud ka sõnasõnaliselt kui „usaldustase“, „usaldusväärtuse tase“ ja „usalduse tagatistase“.

¹⁷ Tuleb arvestada, et eri allikad ja koolkonnad kasutavad seda määratlust eri kontekstides. Siinkohal on mõeldud eIDASi / ISO 29115 konteksti.

¹⁸ „Märkimisväärne“ (tagasitõlge inglise keelde pigem „*remarkable*“ kui „*substantial*“) on ebaõnnestunud terminivaste, kuivõrd eesti keeleloogikas näib see paiknevat kõrgest tasemest kõrgemal ning selline vaste eirab termini iseseletuvuse nõuet.

eIDAS paneb olulist rõhku e-allkirja andmisele ning käsitleb autentimist piiratumas matus. eIDAS sätestas, et riigid võivad hakata vastastikku ja piiriüleselt üksteise e-allkirja andmise vahendeid tunnustama alates 01.07.2016. Samuti sätestas eIDAS, et riigid peavad hakkama alates 18.09.2018 [16] vastastikku ja piiriüleselt tunnustama üksteise autentimisvahendeid.

Üleminekuperioodil tuli riikidel, sh Eestil [14], seni käibivad autentimiskeemid sõltumatult hinnata ja teavitada (*to notify*) Euroopa Liidule. Näite skeemi kirjeldusest leiab allikast [14]. Elektroonilisele allkirjastamisele läheneb eIDAS teisiti – läbi arvukate nõuete ja tehniliste standardite.

Euroopa Liit publitseerib usaldusteenustega seoses nimekirja LoTL – (*list of trusted lists*) [17], mis omakorda riigiti viitab usaldusteenuste ja nende staatuste nimekirjale TSL (*Trust-service Status List*). Allkirjasertifikaatide puhul veendutakse, et nende väljaandja on selles nimekirjas olemas ja olekus „kehtiv“. Samad tingimused kehtivad ka ajatempliteenuse osutajale ehk see peab olema nimekirjas ja olekuga „kehtiv“. Lisaks saab nimekirja alusel teada, kas usaldusteenus on tunnustatud kvalifitseeritud usaldusteenuseks.

Üheksa eIDASi rakendusakti määratlevad e-allkirja standardid ning usaldusteenuste korralduse. Ülevaate neist rakendusaktidest leiab lisast B.

A.2.1. E-identimise ja e-tehingute usaldusteenuste seadus

eIDASi määruse sätete sujuvamaks inkorporeerimiseks Eesti seadusruumi võeti 2016. a oktoobris vastu E-identimise ja e-tehingute usaldusteenuste seadus (EUTS) [6]. Seadus kordab eIDASi määruse sätteid, kuid teatud juhtudel ka täpsustab neid. Nii näiteks annab seaduse § 25 õigusliku kaitse varasematele digiallkirjadele ning § 24 samastab senise eestikeelse mõiste „digiallkiri“ eIDASi määruse kvalifitseeritud e-allkirjaga (QES).

A.3. Teenuste turve

Teenuste turvalisust ja jätkusuutlikkust Eestis sätestavad hädaolukorra seadus (HoS), küberturvalisuse seadus (KÜTS) ja lisaks veel ka E-ITSi määrus. HoS defineerib **elutähtsad** teenused, KÜTS defineerib **olulised** teenused. Praktikas võib osutada, et täiendavaks kontekstiks on mingite väliste infosüsteemide sõltuvus usaldusteenusest (e-teenused võivad vajada katkematut autentimisteenust) ning X-tee (Eesti avaliku sektori andmevahetuskiht), mille kasutamine riiklike andmekogudega (nt dokumendiregister, rahvastikuregister) ühendumiseks on usaldusteenuse osutajal vältimatu.

Järgnevad alajaotised selgitavad, millised õigusaktid ning kuidas tagavad (e-)teenuste turvalisuse taseme Eestis.

A.3.1. Hädaolukorra seadus

Hädaolukorra seadus [26] eksisteeris Eestis ka varem, kuid 2017. aastal korrastati seda oluliselt. Seaduse § 36 esitab elutähtsate teenuste loetelu, mille hulka kuulub ka „elektrooniline isikutuvastamine ja digitaalne allkirjastamine“ (lg 1 p 8). HoS § 2 (5) toob terminoloogiliselt sisse

„elutähtsa teenuse osutaja“¹⁹ mõiste ning esitab sellistele ettevõtetele regulatiivseid nõudeid. Sealhulgas tuleb elutähtsa teenuse osutajal koostada teenuse „toimepidevuse“ riskianalüüs ja plaan. Ühtlasi tuleb teenus korraldada viisil, mis tagaks selle sõltumatuse välisriigis asuvatest infosüsteemidest.

Ettevõtetus- ja tehnoloogiainistri määrus „Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektroonilise isikutuvastamise ja digitaalse allkirjastamise tagamisel“ (2019) [59] seob elutähtsa teenuse mõiste otseselt isikutuvastamise ja digitaalallkirjade andmisega.

A.3.2. NIS direktiiv

Euroopa Nõukogu ja Parlamendi direktiiv 2016/1148 [27] (nn NIS direktiiv) ärgitas Eestit mõnevõrra modifitseerima senist elutähtsate teenusepakujate korraldust, mistõttu lisaks HoSile võib teenuseandjatele olulisi sätteid nüüd leida veel ka KÜTSis.

Hetkel on käimas protsess NIS direktiivi täiustamiseks, nn NIS2. Tõenäoliselt tuuakse NIS2 direktiivist tulenevad uuendused Eesti õigusruumi läbi KÜTSi (vt lisa A.3.3). Hetkel pole veel teada, kuidas tuuakse Eesti õigusruumi uuendused küsimustes, kus NIS2 täpsustab eIDASi määruse sätteid või arendab neid edasi.

A.3.3. Küberturvalisuse seadus

NISi nõuete sujuvaks sisetoomiseks Eesti õigusruumi võeti 09.05.2018 vastu küberturvalisuse seadus [28]. Seega on Eestis hetkel kaks teenuseosutajaid reguleerivat seadust – KÜTS ja HoS. KÜTS defineerib olulise „teenuse osutaja“ ning esitab talle regulatiivseid nõudeid. Digitaalse teenuse osutaja peab muuhulgas koostama süsteemi riskianalüüsi ning haldama ettetulevaid küberintsidente kehtestatud korras. KÜTS § 7 lg 5 p 1 viitab infoturbe halduse nõudeid sisaldavale Eesti infoturbestandardile.

A.3.4. Eesti infoturbestandard E-ITS ja E-ITSi määrus

E-ITSi aluseks on Saksa päritolu BSI IT-Grundschutz etaloniturbemeetod. E-ITSi koostamisel on arvestatud vajadusega saavutada vastavus standardi EVS-EN ISO/IEC 27001 nõuetega. E-ITS on kohustuslik Eesti avalikus sektoris tegutsejatele, teatud juhtudel ka avalikke teenuseid andvatele, vahendavatele või majutavatele erafirmadele.

Standardi E-ITS 2023. aasta versiooni on lisatud moodul SYS.EE.2: eID komponendid, mis on riigi- ja avalikus sektoris täitmiseks kohustuslik. See tähendab, et vastava vajadusega puutub kokku enamik integraatoreid.

Ülevaate E-ITSi nõuetest saab portaalist eits.ria.ee, portaalis on saadaval ka verifitseerimata tõlge inglise keelde.

Niinimetatud E-ITSi määrus on kehtestatud Valitsuse määrusega nr 101 [28] 16. detsembril 2022 viitega KÜTSi § 7 lg 5-le ning Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ [29] § 3 lg 1-le.

¹⁹ Eesti seadustes (HoS, KÜTS) kasutatav termin „osutaja“ ei ole keeleliselt kõige täpsem.

Lisa B. E-identiteedi ökosüsteemi tehnilised raamid

Sertifikaadid Eesti eID ökosüsteemis vastavad eIDASi määruse nõuetele (vt lisa B.3.2) ning on kooskõlas standarditega ISO/IEC 9594-8, ETSI EN 319 411 ning ITU-T X.509.

Sertifikaat sisaldab identiteediomaniku võtmepaari avalikku võtit, mis on varustatud teatud kokkulepitud **lisaatribuutidega** ning allkirjastatud sertifitseerimisteenuse osutaja salajase võtmega.

B.1. eID-vahendid ja nende võimalused

Tabel B.1 loetleb ja kirjeldab Eesti eID ökosüsteemis toimivad eID-vahendid. Elementaarteenuseid käsitleme ENISA DIS (vt jaotis 2.1) ontoloogiale tuginedes.

Tabel B.1. Eesti eID ökosüsteemi eID-vahendid ja nende võimalused

Kategooria	Omadus	ID-kaart (kui isikutunnistus)	Elamisloa-kaart	Digitaalne isikutunnistus (digi-ID) ²⁰	E-residendi digitaalne isikutunnistus	Diplomaatiline isikutunnistus	Mobiil-ID	Smart-ID	
Ökosüsteemi osalised	Teenuse omanik ehk dokumendi väljaandja	PPA	PPA	PPA	PPA	VM	PPA	SK	
	Vahendi väljastaja	PPA, välisesindused, välised teenuseosutajad	PPA, välisesindused, välised teenuseosutajad	-	PPA, välisesindused	Välisministeerium (VM)	Sideettevõtte	SK elektrooniliselt; füüsiliselt partnerite juures	
	Sertifikaadid	SK	SK	SK	SK	SK	SK	SK	
	Tugi	SK	SK	SK	SK	VM	SK	SK	
Võimalused, omadused, tingimused, funktsioonid	Kasutus kliendi-kaardina	JAH	JAH	EI	EI	EI	NA	NA	
	Eksemplaride arv liigi kohta	1	1	1	1	1	M (1 enne 2022)	M	
	Väljastamise eeldused	Alus-identiteet, kodanik, EL kodanik	Alusidentiteet, elamisloaba	Alusidentiteet	Taotlus, tausta-kontroll	Akrediteeritud diplomaat	Alusidentiteet	1. Alusidentiteet, 2. Muu	
	QSCD	ISO-7816 GP Javacard	ISO-7816 GP Javacard	ISO-7816 GP Javacard	ISO-7816 GP Javacard	ISO-7816 GP Javacard	SIM-kaart koos apletiga	Virtuaalne, SplitKey	
	Autentimise kindlustase digiallkirja usaldustase	high/QES	high/QES	high/QES	high/QES	high/QES	high/QES	high/QES	
	Isiku foto dokumendil	JAH	JAH	EI	EI	JAH	EI	EI	
	Valimisõiguse olemasolul saab e-hääletada	JAH	JAH	JAH	EI	EI	JAH ²¹	JAH ²²	
	Jätkusuutlik 10 a perspektiivis	JAH	JAH	EI	EI	JAH	EI	JAH	
Lõpp-kasutaja toimingud (teenused, elementaar-toimingud)	Aktiveerimine	EI	EI	EI	EI	EI	JAH	JAH	
	Autentimine	JAH	JAH	JAH	JAH	JAH	JAH	JAH	
	Digiallkirjade andmine	JAH	JAH	JAH	JAH	JAH	JAH	JAH	
	Allkirja valideerimine	Ei eelda ökosüsteemis osalemist. DigiDoc tarkvara, omanduslik teenus Docobit, SiVa jne							
	Krüpteerimine (CDOC)	JAH	JAH	JAH	JAH	JAH	JAH	järgmises DigiDoc4 versioonis	järgmises DigiDoc4 versioonis
	Sertifikaatide tühistamine	PPA	PPA	PPA	PPA	VM	PPA	SK	
	Tarkvara uuendamine	JAH*	JAH*	JAH*	JAH*	JAH*	EI	JAH*	

* ID-kaardi (kui isikutunnistuse), elamisloakaardi, digi-ID, e-residendi digitaalse isikutunnistuse puhul mõeldakse tarkvara uuendamise all kaardil oleva rakenduse uuendamist (seda tehakse PPA

²⁰ Alates 01.05.2025 on digi-ID väljaandmine lõpetatud, kuid väljastatud digitaalsed isikutunnistusi saab kasutada kehtivuse lõppemiseni.

²¹ E-valimistel on mobiil-ID kasutatav üksnes kontekstis, kui valimisrakendus käivitatakse arvutist.

²² E-valimistel on Smart-ID kasutatav üksnes kontekstis, kui valimisrakendus käivitatakse arvutist.

teeninduspunktis või hädaolukorras ka kaugmeetodil). Smart-ID puhul mõeldakse tarkvara uuendamise all nutiäpi versiooni uuendamist.

** Koondtabel ei nimeta teenuseosutaja poolset tuge. Koondtabel ei maini ENISA DIS-teenuste hulgas loetletud **säilitusteenust**, kuivõrd Eestis säärane teenus puudub (teatud ajaperioodil oli kasutusel digiallkirjade ületembeldamise vallasrakendus TeRa).

Märkus: Smart-ID iga isend (*instance*) on seotud seadmega, mitte isikuga. See langeb kokku eIDAS 2.0 ja ENISA DIS käsitlusega.

B.1.1. Standardid ja tootjad

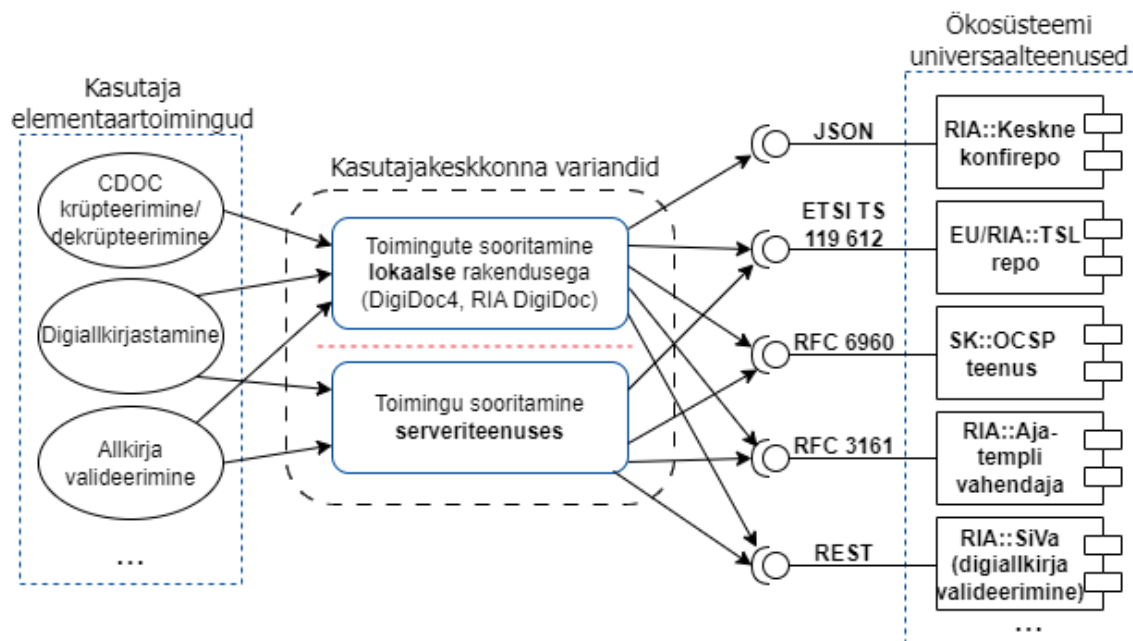
ID-kaardi aluseks on standardne Global Platform [72] tüüpi Java kiipkaart [73], mille elektriline osa on määratud standardiga ISO/IEC 7810. Standardi viimane teadaolev redaktsioon on 2019. aastast. Huvitavat taustamaterjali sisaldab standardiseeria ISO 7816.

ICAO ja ELi määruse nõudel sisaldab isikut tõendava dokumendina kasutatav elektrooniline isikutunnistus (nt ID-kaart kui isikutunnistus, elamisloakaart) selle kandja biomeetrilisi andmeid (foto, alates 13.08.2021 ka sõrmejäljed).

B.2. Digiallkirja andmise tehnilised vahendid

Standardsetesse veebiserveritesse ja veebibrauseritesse on transpordikihi turvaprotokolli TLS tugi juba sisse ehitatud. Huvitava lisavõimalusena saab ID-kaartide puhul kasutada TLS-CCA laiendust, mille puhul TLS-ühenduse loomisel kasutatakse kliendi autentimiseks konkreetsel kaardil olevat autentimisvõtit. Sel juhul on TLS-kiht otseselt seotud kasutaja identiteediga. Lähemalt vt autentimisprotokollistike analüüsi [77] jaotises 3.2.1. Lisaks saab ID-kaardi puhul kasutada veebis autentimiseks ja allkirja andmiseks Web eID lahendust.

Kasutaja saab elementaartoiminguid sooritada mitmel erineval viisil, olenevalt sellest, kas ta pruugib kohalikus rakenduses (DigiDoc4, RIA DigiDoc) või mõnes serveriteenuses paiknevat äri loogikat. Valiku olemasolul saab kasutaja talitada oma äranägemise järgi, millist olukorda illustreerib joonis B.1.

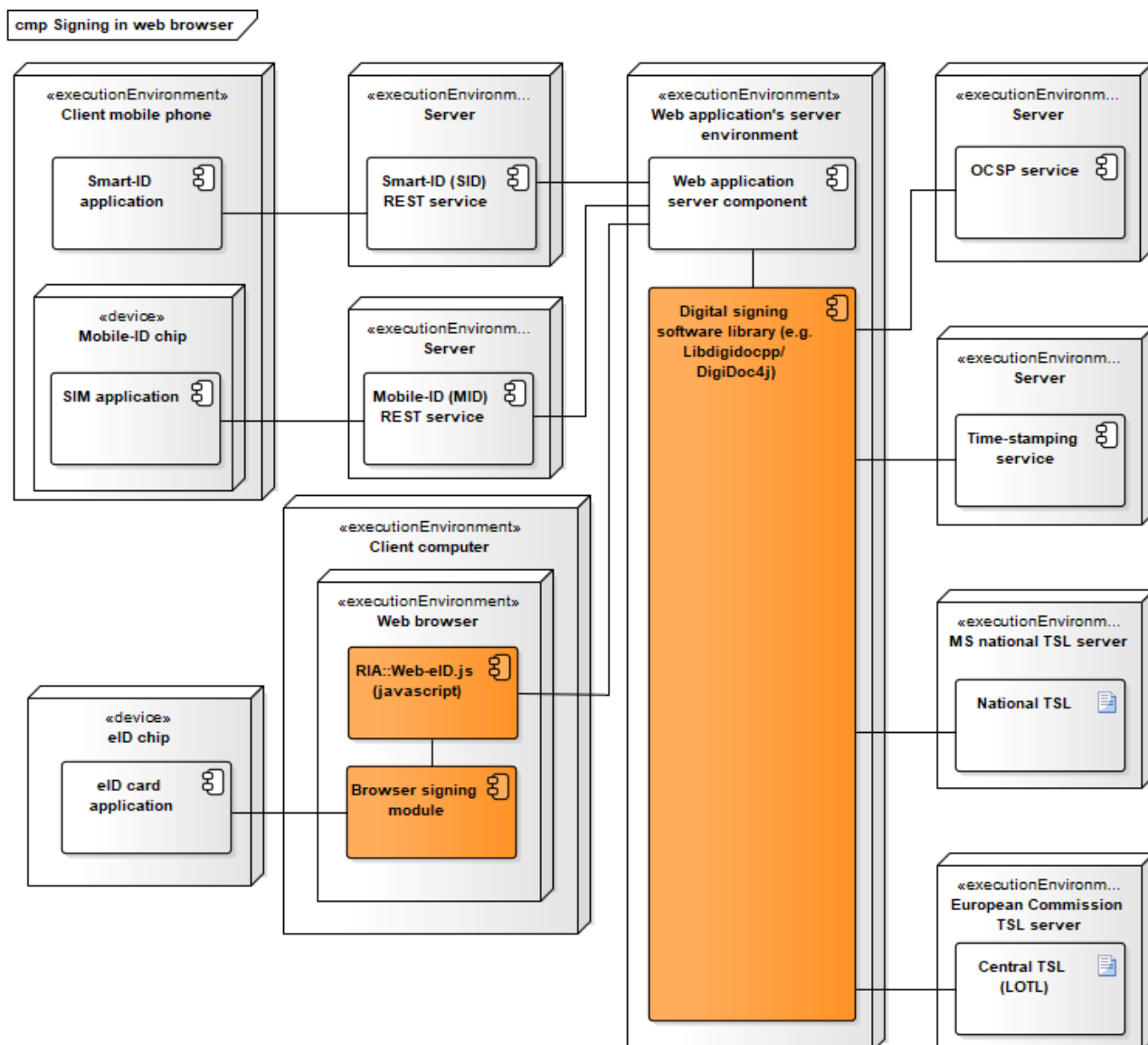


Joonis B.1. Kasutaja elementaartoimingute seos ökosüsteemi universaalteenustega

Joonis B.2 esitab evituskeemi, mis illustreerib erinevate vahenditega digiallkirja andmist veebiteenustes. Veebiteenus võimaldab kasutajal valida, millise vahendiga kolmest (ID-kaart, mobiil-ID, Smart-ID) ta soovib dokumenti või transaktsiooni digiallkirjastada. Juhul kui kasutaja valib ID-kaardi, rakendub ID-kaardi draiver ning dokumendi räsi digiallkirjastamise viimane järk toimub lokaalselt, kasutaja arvutis.

Juhtudel, kui kasutaja valib digiallkirja andmise teises seadmes paikneva vahendiga, toimub digiallkirja andmise viimane järk vastavalt kas Smart-ID rakenduses või mobiiltelefoni SIM-kaardi abil. Veebiteenuse server valib suhtlemiseks õige kanali ja protseduuri. Allikas [78] esitab teisegi sarnase, kuid juba DigiDoc4 keskse evituskeemi. Ökosüsteemi tagateenustega ühendutakse kõigi kasutuskeemide puhul.

Normaalseks praktikaks tuleb lugeda, et iga digiallkirja valideeritaks kohe pärast loomist (mõne usaldusväärse tarkvara või teenusega). Sellega tagatakse, et potentsiaalselt vigased digiallkirjad ei pääse käibesse.



Joonis B.2. Digiallkirjastamine veebis erinevate vahenditega

B.3. Tehnilised normid

B.3.1. eIDASi rakendusaktid

Üheksa eIDASi määruse [5] rakendusakti määratlevad e-allkirja standardid ning usaldusteenuste korralduse. Nii keskendub näiteks määrus 2015/1502 [24] „e-identimise“ vahendite usaldusväärsuse kirjeldamisele (tasemeil **madal**, **märkimisväärne** ja **kõrge**). Tabel B.2 esitab nimekirja eIDASi määruse [5] rakendusaktidest.

Tabel B.2. Ülevaade eIDASi määruse rakendusaktidest

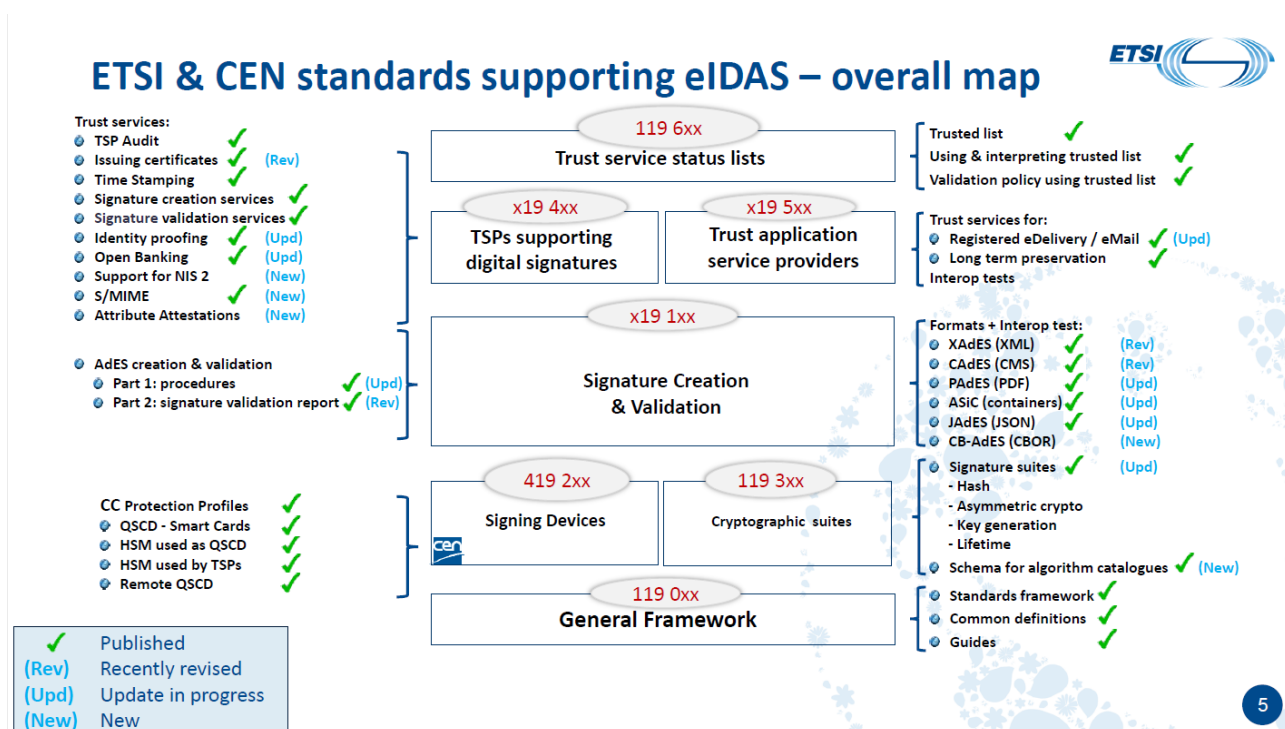
Rakendusakt	Sisu	Viide
2015/296	Menetluskord liikmesriikidevaheliseks koostööks e-identimise valdkonnas vastavalt eIDASi määruse [5] artikli 12 lõikele 7	[18]

2015/806	Eli kvalifitseeritud usaldusteenuse usaldusmärgi vormingu kirjeldus (pilt ja lubatud kasutusviis)	[19]
2015/1501	Koostalitlusvõime raamistik vastavalt eIDASi määruse [5] artikli 12 lõikele 8	[20]
2015/1502²³	e-identimise vahendite usaldusväarsuse tasemete minimaalsed tehnilised kirjeldused ja menetlused vastavalt eIDASi määruse [5] artikli 8 lõikele 3	[21]
2015/1505	Usaldusnimekirjade (TSL – <i>Trust-service Status List</i>) tehnilised kirjeldused ja vormingud vastavalt eIDASi määruse [5] artikli 22 lõikele 5, viide standardile ETSI TS 119 612 v2.1.1	[22]
2015/1506	Täiustatud e-allkirja ja täiustatud e-templi vormingu kirjeldus vastavalt eIDASi määruse [5] artikli 27 lõikele 5 ja artikli 37 lõikele 5	[23]
2015/1984	eIDASi määruse [5] artikli 9 lõike 5 kohase teavitamise asjaolud, vormingud ja kord	[24]
2016/650	QSCD seadmete turvastandarditest	[25]

B.3.2. Tehnilised ja korralduslikud standardid

ENISA DIS [12] käsitleb põhjalikult standardeid ja nende rolli eID ökosüsteemis. Joonis B.3 annab ülevaate peamistest standarditest ja nende uuendustest seisuga okt/nov 2023.

²³ Määrus 2022/960 on tabelist välja jäetud, sest puudub üksnes määruse 2015/1502 tšehhikeelset teksti.



5

Joonis B.3. eIDASi määruse tugistandardid

Standardeid on võimalik grupeerida vastavalt sellele, mida nad reguleerivad:

- usaldusteenuste korraldust
- e-allkirjade vorminguid, moodustamist ja valideerimist
- e-allkirjade moodustamise vahendeid

Tabel B.3 annab ülevaate eIDASi määrusega [5] kooskõlalise eID ökosüsteemi tehnilistest standarditest. Tuleb arvestada, et juriidiliste protseduuride keerukuse tõttu viitab eIDASi määruse tekst endiselt kehtestamise aegsetele standardiversioonidele, kuigi teatud standardeid on vahepeal uuendatud ja neist on saadaval uuemad versioonid.

Tabel B.3. Autentimisse, e-allkirja andmisse ja usaldusteenustesse puutuvad tehnilised ja korralduslikud standardid

Standard	Sisu	Seosed rakendus-aktidega	Viide
ISO/IEC 15408	Evaluation Criteria for IT security, osad 1-3: ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008 (vt ka 2023.a versioonid)	2016/650	[32]
ISO/IEC 18045:2008	Information technology – Security techniques – Methodology for IT security evaluation (vt ka 2023.a. versioonid)	2016/650	[32]
EN 419 211	Protection profiles for secure signature creation device, osad 1–6	2016/650	[32]
ISO/IEC 29115:2013	Infotehnoloogia. Turbemeetodid. Olemi autentimis-kindluse karkass (annab aluse	2015/1502	[32]

	rakendusaktile)		
BSI TR-03110	eIDAS Token Specification	-	[33]
ITU-T X.520	Recommendation regarding certificates: ISO/IEC 9594-6 standard, using ASN.1 syntax	ENISA DIS 4.3.3.3	[34]
EN 319 102-1	Procedures for Creation and Validation of AdES Digital Signatures (Part 1: Creation and Validation)	-	[35]
TS 119 102-2	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report		[36]
ETSI TS 102 853	Signature validation procedures and policies	-	[37]
ETSI TS 119 612	Trusted Lists	2015/1505	[38]
EN 319 122-1	CAdES digital signatures (Part 1: Building blocks and CAdES baseline signatures)	2015/1506	[39]
ETSI TS 103 173²⁴	CAdES Baseline Profile (vanem versioon)	2015/1506	[40]
EN 319 132-1	XAdES digital signatures (Part 1: Building blocks and XAdES baseline signatures)	2015/1506	[41]
ETSI TS 103 171	(XAdES Baseline Profile) (vanem versioon)	2015/1506	[42]
EN 319 142-1	PAdES digital signatures (Part 1: Building blocks and PAdES baseline signatures)	2015/1506	[43]
ETSI TS 103 172	PAdES Baseline Profile (vanem versioon)	2015/1506	[44]
EN 319 162-1	Associated Signature Containers (ASiC) (Part 1: Building blocks and ASiC baseline containers)	2015/1506	[45]
ETSI TS 103 174	ASiC Baseline Profile (vanem versioon)	2015/1506	[46]
EN 319 401	General Policy Requirements for Trust Service Providers	eIDAS §5(1), §13(2), §15	[47]
EN 319 403	Trust Service Provider Conformity Assessment (Requirements for conformity assessment bodies assessing Trust Service Providers)	-	[48]
EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates (Part 1: General requirements)	eIDAS §24	[49]
EN 319 411-2	Policy and security requirements for Trust Service Providers issuing certificates (Part 2: Requirements for trust service providers issuing EU qualified certificates)	eIDAS §24	[50]
EN 319 411-3	Policy and security requirements for Trust Service Providers issuing certificates (Part 3: Policy requirements for Certification Authorities issuing public key certificates)	–	[51]
EN 319 412-1	Certificate Profiles (Part 1: Overview and common data structures)	–	[52]

²⁴ Kollase värviga on tähistatud standardite eelmised versioonid, millele eIDAS viitab.

EN 319 412-2	Certificate Profiles (Part 2: Certificate profile for certificates issued to natural persons)	–	[53]
EN 319 412-3	Certificate Profiles (Part 3: Certificate profile for certificates issued to legal persons)	–	[54]
EN 319 412-4	Certificate Profiles (Part 4: Certificate profile for web site certificates)	–	[55]
EN 319 412-5	Certificate Profiles (Part 5: QCStatements)	–	[56]
EN 319 421	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps	eIDAS §24, §42(2)	[57]
EN 319 422	Time-stamping protocol and time-stamp token profiles	eIDAS §42(2)	[58]

Lisa C. Eesti eID ökosüsteemi põhinõuded (vastavustabel)

Tabel C.1 koondab põhilised nõuded, millega peab tutvuma iga Eesti eID ökosüsteemiga puutumusse sattuv tootja, väljastaja, teenuse osutaja ja integraator. Lisanduda võivad spetsiifilised nõuded konkreetsetest tootetingimustest ja lepingutest.

Legend: nõude kategooria nimetus:

- G – generic – Eestis geneeriline
- L – *legal* – juriidiline
- M – *manufacturer* – tootja
- S – *service* – teenus
- U – *user* – kasutaja (keda turvaküsimustes juhendavad vahendi väljastaja ja RIA)
- (R – *requirement* – nõue)

Tabel C.1. Eesti eID ökosüsteemi põhinõuded

Nõue	Päritolu või kohustuslikkus	Nõude lühikokkuvõte	Nõude selgitus ja kommentaarid
R-L-01	eIDAS	eIDAS 1.0 [5] nõuded on täidetud	Vt ka lisad A.2 ja B.3
R-L-02	provisoorne	On valmisolek eIDAS 2.0 [13] nõuete täitmiseks	Oluline juhul, kui teenuse periood jätkub kava kohaselt ka eIDAS 2.0 [13] kehtivusajal
R-L-03	Eesti õigusruum	EUTS nõuded on täidetud	EUTS täpsustab eIDASi määruse mõningaid aspekte, sh annab „digiallkirja“ definitsiooni (§ 24 lg 1)
R-L-04	Eesti õigusruum	Elutähtsa teenuse osutaja allub HoS nõuetele (vt § 36 lg 2, § 41), olulise teenuse osutaja KüTS nõuetele.	Teenuste jätkuvuse tagamiseks peavad elutähtsate ja oluliste teenuste osutajad täitma teatud kohustusi (audit, talitluspidevuse riskiplaan, turvameetmed, intsidendist raporteerimine jne). Usaldusteenus võib osutada mõne muu teenuse sõltuvuseks
R-L-05	Eesti õigusruum	Vajadus teatud juhtudel alluda „E-ITS määrusega“ kehtestatud Eesti Infoturbestandardile (E-ITS)	Kehtestatud KüTS § 7 lg 5 ja määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 3 lg 1 alusel. Viimase § 12 kohaselt võib usaldusteenus osutada „avalike ülesannete täitmist oluliselt mõjutavate süsteemide“ sõltuvuseks. E-ITSi aluseks on Saksa päritolu BSI IT-Grundschutz etalonurbe meetod. „Teatud juhud“ hõlmavad X-tee

			kasutamist
R-L-06	Eesti õigusruum	Igal isikul on unikaalne number – digitaalne nimi. (Vt isikukoodide moodustamise ja andmise kord [62]). Olemuselt: riiklik alusidentiteet	Üks olulisemaid aksioome. Nõutav on globaalne, püsiv, unikaalne ning avalik (GUPI/QP) isikukood. Probleeme tekib eIDASist lähtuval riskasutusel välisriikide kodanikega, kel säärane isikukood puudub
R-L-07	Eesti õigusruum	Isikukoodi valem on kirjeldatud standardis EVS 585:2007 ja dubleeritud õigusaktis „Isikukoodide moodustamise ja andmise kord“	
R-G-01	Eesti õigusruum	Alusidentiteeti haldab riik Rahvastikuregistris, mitte erafirmad. Alusidentiteet pole kommertsiaalne	Erafirmad võivad teenindada protsessi üksikuid elemente, kuid nad põhimõtteliselt ei saa kanda vastutust alusidentiteedi eest. Tegemist on fundamentaalse filosoofilise ning usaldusküsimusega. Nt USAs on olukord vastupidine
R-G-02		Väljastatavate vahendite kogus isiku kohta erineb liigiti. On eID-vahendeid, mille kehtivaid instantsse tohib isikul olla vaid üks, kuid on vahendeid, mille samaaegne kogus isiku kohta pole piiratud. Ühe eID vahendi või vahendi liigi lubatud instantside arv isiku kohta võib ajas muutuda	Näiteks Smart-ID vahendeid (seadmeid) võib igal isikul olla mitu. Väljastajal tuleb provisoorselt jälgida muutusi riiklikes poliitikates.
R-G-03	Oluline taustainfo	Samal isikul ei saa olla kehtivaid eID-vahendi teatavaid alamliike (ID-kaart (kui isikutunnistus) vs. elamisloakaart) korraga	Seotud õigusliku staatusega. ID-kaart (kui isikutunnistus) on kodaniku ja EL kodaniku, elamisloakaart välismaalase isikut tõendav dokument
R-G-04	Oluline taustainfo	Praktikas kasutab Eesti üksnes eIDASi määruse autentimistaset LoA=High	Madalama taseme eIDAS riskasutuse kohustus seetõttu puudub.
R-G-05	Oluline taustainfo	Digiallkirjad Eestis vastavad enamjaolt eIDAS QES-tasemele [QC+QSCD] (üksnes see tase on Eestis võrdsustatud omakäelise allkirjaga)	Kuivõrd Eesti realiseeris QES-sarnase nõude juba 2001. aastal, siis AdES/QC tasemele alanemisel puudub mõte, v.a. riskasutuseks teiste riikidega. Madalama taseme eIDAS riskasutuse kohustus seetõttu puudub.
R-G-06	Oluline	Kõigil senistel eID-	Teoreetiliselt pole tulevikus välistatud

	taustainfo	vahenditel Eestis käivad sertifikaadid [Auth + Sign] paaris. Neid ei genereerita, uuendata ega tühistata lahus (paariväliselt). ²⁵	järjestikune autentimine ühe vahendiga ning digiallkirja andmine teisega, kuid tuleb arvestada, et ei tootjate, väljastajate ega teenuseosutajate (sh pangateenuste) praegune töövoog säärast lähenemist ei toeta.
R-G-07	Oluline taustainfo	Privaatvõtme kasutamist võimaldav PIN-kood on võtme atribuut.	PIN-kood ei ole vahendi, vahendi liidese (NFC) ega kasutaja vahendiülene atribuut. Eksisteerib pörandaalune väärdõpetus, mille kohaselt PIN-kood on isiku atribuut, see langetab oluliselt iga vahendi turvalisust. Selgitus: teenuseosutaja kohustus on tagada kasutajale minimaalsed turvaoskused
R-M-01	Ajalooline	Võtmematerjal genereeritakse eID-vahendis ega välju seadmest kunagi avatekstina	Algselt püstitati see nõue ID-kaardile, kuid kehtib ka SIM-kaardi ja Smart-ID puhul
R-M-02	Ajalooline	Nõuded võtmekasutust võimaldava(te)le PIN-koodidele	Autentimist avava PIN-koodi pikkus on vähemalt 4 märki. Digiallkirja andmist avava PIN-koodi pikkus on vähemalt 5 märki. PUK koodide pikkus on vähemalt 8 märki. Lubatud on üksnes numbrid. PIN-kood lukustub pärast kolme järjestikust ebaõnnestunud katset
R-S-01	Protseduurid	Sertifikaadi kehtivust tuleb kontrollida teenuse igal kasutuskorral	Meetodid on kas OCSP või CRL
R-S-02	Protseduurid	Sertifikaadi kontrollimisel tuleb üle kontrollida ka selle usaldusahel	Autentimissertifikaati kontrollitakse konkreetse sertifikaadiahela (nt EstEID-2018) juureni. Allkirjastamissertifikaadi kontrolliks laaditakse LoTL, sealt vastava riigi TSL ning kontrollitakse nende vastu
R-S-03	Ajaloolis-kultuuriline	Enne teenusesse autentimise õnnestumist ei tohi teenus väljastada isikuandmeid	2011. aastal mõned mobiil-ID teenused teatasid telefoninumbri või isikukoodi esitamise peale autentiva isiku nime, mis võimaldas kurjategijal kasutajabaasi enumereerimist.

²⁵ Ainus olukord, kus võtmepaare käsitletakse lahus, on Smart-ID ajutine „ajalukk“. Näiteks, kui kasutaja sisestab PIN1 koodi kolm korda valesti, ei ole tema sertifikaadid veel tühistatud, vaid ta saab tunni aja pärast uuesti proovida. Peale üheksandat valesti sisestamist lukustatakse võtmepaarid lõplikult, kasutaja mõlemad sertifikaadid tühistatakse ning konto suletakse.

			eBay.com tervitab kasutajat eesnime pidi ka siis, kui ta pole sisse loginud
R-S-04	Riskihaldus, kaudselt KÜTS ja HoS	Autentimine ja digiallkirja andmine igas e-teenuses peaksid olema võimalikud vähemalt kahe erineva eID-vahendiga.	Riskihaldus ROCA-2017 ²⁶ ja DigiNotar 2011 ²⁷ taoliste juhtumite puhuks
R-S-05	Hea tava	Vastuvõtjale edastatud konfidentsiaalsete failide dekrüpteerimiseks taaskasutatakse vastuvõtja autentimise võtmepaari ning selleks ei ole ette nähtud eraldi spetsiaalset võtmepaari/sertifikaati	Eesti eID ökosüsteemi lõppkasutajatarkvaras DigiDoc4 ja RIA DigiDoc on realiseeritud vastavad krüpteerimise ja dekrüpteerimise funktsioonid
R-S-06	Hea tava	Igale digiallkirja andmisele mistahes keskkonnas järgneva kohe ka selle allkirja valideerimine	Allkirja valideerimine on võimalik nt teenuse SiVa kaudu
R-S-07	CP, CSP	Teenus või tarkvara peab järgima võtme sertifikaadis määratletud kasutusotstarvet	Ametlik tarkvara piirab väärkasutust. Vigade vältimiseks ei tohiks teenused ega utiliidid võimaldada autentimis- ja digiallkirjasertifikaatide kasutamist sertifikaadis nimetamata otstarbel
R-S-08	Riskihaldus	On kategooriliselt keelatud luua teenust, mis kasutab isikukoodi paroolina	Selgitus: isikukood on vaid unikaalne identifikaator. Oma õigust andmetele juurde pääseda tuleb tõestada muul moel (sh autentimisega)
R-S-09	Riskihaldus (MitM oht)	TLS-CCA vastastikust autentimist tuleks kasutada alati kui see on võimalik	Võimalik vaid ID-kaartidega. Ühtlasi parandab ärivõimalusi, kuivõrd isiku identiteet on teada ka ilma eelneva lepinguta
R-S-10	Integratsioon	Võtmete aktiveerimise tingimused. Kombi-natsioon kaardiäpist ja kaardi draiveritest peab tagama, et PIN2-kood mitte kunagi ei puhverdataks ning et kaardi digiallkirjaga varustamise funktsioon	Ajalooliselt on teada juhus, kui PIN1-kood elas IE6 vahemälu säilimise tõttu üle arvuti külma restardi

²⁶ Vt allmärkust jaotises 2.5.

²⁷ DigiNotar oli Hollandi sertifitseerimisasutus, mida teiste hulgas kasutas sertifikaatide väljastajana Hollandi valitsus. DigiNotari juursertifikaati tunnistas usaldatavaks ka enamik veebibrausereid. 2011. aasta juulis õnnestus Iraani päritolu häkkeril tungida DigiNotari süsteemi ning väljastada sadu võltsitud sertifikaate, sh võltsitud Google'i sertifikaadi, mida kasutati vahendusründeks iraanlastest Gmaili kasutajate vastu. Ründe ulatuslikkuse tõttu sattusid kõik DigiNotari väljastatud sertifikaadid musta nimekirja ning firma oli usalduse kaotuse tõttu kuulutama välja pankroti. Lähemalt loe nt <https://slate.com/technology/2016/12/how-the-2011-hack-of-diginotar-changed-the-internets-infrastructure.html>.

		avaneks vaid üheks krüptograafiliseks operatsiooniks	
R-U-01	Riskihaldus	Igal lõppkasutajal peaks olema vähemalt kaks eID-vahendit usaldusteenuste kasutamiseks, soovitavalt erinevat	
R-U-02	Kuritegevuse oht	Kui autentimisvahend küsib nõusolekut toimingule, mida kasutaja ei algatanud, siis kasutaja 1) ei sisesta PIN-koodi, 2) teavitab teenuseosutajat	Selgitus: teenuseosutaja kohustus on tagada kasutaja miinimumoskused
R-U-03	Kuritegevuse oht	Kui toimingule saabub vale kontrollkood, siis kasutaja 1) ei sisesta PIN-koodi, 2) teavitab teenuseosutajat ja/või usaldusteenuse andjat	Selgitus: teenuseosutaja kohustus on tagada kasutaja miinimumoskused. (Ei puuduta ID-kaarte, sest need kontrollkoode ei kasuta)

Viited

- [1] Riigi Infosüsteemi Amet. Eesti Vabariigi infosüsteemis autentimislahendustele kehtivad nõuded (autentimismormatiiv), 2017. URL: <https://ria.ee/media/1971/download> (vaadatud 15.07.2024).
- [2] Cybernetica AS. Andmekaitse ja infoturbe portaal AKIT. URL: <https://akit.cyber.ee/> (vaadatud 11.07.2024).
- [3] Isikut tõendavate dokumentide seadus (26.04.2024). URL: <https://www.riigiteataja.ee/akt/120062022057?leiaKehtiv> (vaadatud 15.07.2024).
- [4] Digitaalalkirja seadus (kehtivuse kaotanud). URL: <https://www.riigiteataja.ee/akt/71878> (vaadatud 15.07.2024).
- [5] Euroopa Liit. Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. URL: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32014R0910> (vaadatud 11.07.2024).
- [6] E-identimise ja e-tehingute usaldusteenuste seadus (03.03.2023). URL: <https://www.riigiteataja.ee/akt/125102016001?leiaKehtiv> (vaadatud 15.07.2024).
- [7] Riigi Infosüsteemi Amet. Andmevahetuskiht X-tee. URL: <https://www.ria.ee/riigi-infosusteem/andmevahetuse-platvormid/andmevahetuskiht-x-tee> (vaadatud 15.07.2024).
- [8] Riigi Infosüsteemi Amet. X-tee: Eesti keskkonna dokumentatsioon. URL: <https://www.x-tee.ee/docs/live/xroad/> (vaadatud 15.07.2024).
- [9] Helen Raamat. Estonian Digital Public Service Improvement Analysis in Cross-Border Use Cases. MSc Thesis. TalTech, 2021. URL: <https://digikogu.taltech.ee/et/Item/df2c6ccd-3ba6-42c3-afe0-6d61c50b8e99> (vaadatud 15.07.2024).
- [10] World Economic Forum. Digital Identity Ecosystems: Unlocking New Value. An interactive guide for executives, 2021. URL: https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf (vaadatud 15.07.2024).
- [11] Riigi Infosüsteemi Amet. ID-kaardi dokumentatsioon. URL: <https://www.id.ee/artikkel/id-kaardi-dokumentatsioon/> (vaadatud 15.07.2024).
- [12] European Union Agency for Cybersecurity. Digital Identity Standards. Analysis of standardisation requirements in support of cybersecurity policy, 2023. URL: <https://www.enisa.europa.eu/publications/digital-identity-standards> (vaadatud 15.07.2024).
- [13] Euroopa Liit. Euroopa Parlamendi ja nõukogu määrus (EL) 2024/1183, 11. aprill 2024, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega (eIDAS 2.0). URL: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=OJ:L_202401183 (vaadatud 15.07.2024).
- [14] Police and Border Guard Board. Estonian eID scheme: Digi-ID. Technical specifications and procedures for assurance level high for electronic identification, 2018. URL: <https://web.archive.org/web/20220206011154/https://ec.europa.eu/cefdigital/wiki/download/attachments/62885749/EE%20eID%20LoA%20mapping%20-%20Digi-ID.pdf?version=1&modificationDate=1531759815275&api=v2> (vaadatud 15.07.2024).
- [15] Amir Sharif, Matteo Ranzi jt. „The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes“. Appl. Sci. 12 (24) (2022), 12679. DOI: [10.3390/app122412679](https://doi.org/10.3390/app122412679).
- [16] Riigi Infosüsteemi Amet. eIDAS autentimistasemed, 2017. URL: <https://www.ria.ee/media/1975/download> (vaadatud 15.07.2024).
-

- [17] European Commission. EU/EEA Trusted List Browser. URL: <https://eid.ec.europa.eu/efda/tl-browser/#/screen/home> (vaadatud 15.07.2024).
- [18] Euroopa Komisjon. Rakendusotsus (EL) 2015/296, 24. veebruar 2015, millega kehtestatakse menetluskord liikmesriikidevaheliseks koostööks e-identimise valdkonnas vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 12 lõikele 7. URL: <http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32015D0296> (vaadatud 15.07.2024).
- [19] Euroopa Komisjon. Rakendusmäärus (EL) 2015/806, 22. mai 2015, millega kehtestatakse ELi kvalifitseeritud usaldusteenuse usaldusmärgi vormingu kirjeldus. URL: <http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32015R0806> (vaadatud 15.07.2024).
- [20] Euroopa Komisjon. Rakendusmäärus (EL) 2015/1501, 8. september 2015, koostalitlusvõime raamistiku kohta vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 12 lõikele 8. URL: <http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32015R1501> (vaadatud 15.07.2024).
- [21] Euroopa Komisjon. Rakendusmäärus (EL) 2015/1502, 8. september 2015, millega kehtestatakse e-identimise vahendite usaldusväarsuse tasemete minimaalsed tehnilised kirjeldused ja menetlused vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 8 lõikele 3. URL: <http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32015R1502> (vaadatud 15.07.2024).
- [22] Euroopa Komisjon. Rakendusotsus (EL) 2015/1505, 8. september 2015, millega kehtestatakse usaldusnimekirjade tehnilised kirjeldused ja vormingud vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 22 lõikele 5. URL: <http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32015D1505> (vaadatud 15.07.2024).
- [23] Euroopa Komisjon. Rakendusotsus (EL) 2015/1506, 8. september 2015, millega kehtestatakse täiustatud e-allkirja ja täiustatud e-templi vormingu kirjeldus vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 27 lõikele 5 ja artikli 37 lõikele 5. URL: <http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32015D1506> (vaadatud 15.07.2024).
- [24] Euroopa Komisjon. Rakendusotsus (EL) 2015/1984, 3. november 2015, millega määratakse kindlaks Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 9 lõike 5 kohase teavitamise asjaolud, vormingud ja kord (teatavaks tehtud numbri C(2015) 7369 all). URL: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32015D1984> (vaadatud 15.07.2024).
- [25] Euroopa Komisjon. Rakendusotsus (EL) 2016/650, 25. aprill 2016, millega kehtestatakse kvalifitseeritud allkirja andmise ja templi loomise vahendi turvalisuse hindamise standardid vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 30 lõikele 3 ja artikli 39 lõikele 2. URL: <https://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1462798608178&uri=CELEX:32016D0650> (vaadatud 15.07.2024).
- [26] Hädaolukorra seadus (06.07.2023). URL: <https://www.riigiteataja.ee/akt/130062023022?leiaKehtiv> (vaadatud 15.07.2024).
- [27] Euroopa Liit. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (NIS direktiiv). URL: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016L1148> (vaadatud 15.07.2024).
- [28] Küberturvalisuse seadus (21.06.2024). URL: <https://www.riigiteataja.ee/akt/122052018001?leiaKehtiv> (vaadatud 15.07.2024).

- [29] Vabariigi Valitsuse 16. detsembri 2022 määrus nr 101 „Eesti infoturbestandard“. URL: <https://www.riigiteataja.ee/akt/121122022034> (vaadatud 15.07.2024).
- [30] Silvia Lips, Valentyna Tsap, Nitesh Bharosa, Robert Krimmer, Tanel Tammet, Dirk Draheim. Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership: Learning from the Case of Estonia. Information Systems Frontiers, 25, 2439–2456 (2023). <https://doi.org/10.1007/s10796-022-10363-5>.
- [31] Euroopa Liit. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). URL: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679> (vaadatud 15.07.2024).
- [32] Eesti standardimis- ja akrediteerimiskeskus. URL: <https://www.evs.ee/et/> (vaadatud 15.07.2024).
- [33] Federal Office for Information Security. BSI TR-03110 (eIDAS Token Specification). URL: <https://www.bsi.bund.de/dok/TR-03110-en> (vaadatud 15.07.2024).
- [34] ITU X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types, 2019. URL: <https://www.itu.int/rec/T-REC-X.520-201910-I/en> (vaadatud 15.07.2024).
- [35] ETSI EN 319 102-1. Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation. URL: https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/ (vaadatud 15.07.2024).
- [36] ETSI TS 119 102-2. Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report. URL: https://www.etsi.org/deliver/etsi_ts/119100_119199/11910202/ (vaadatud 15.07.2024).
- [37] ETSI TS 102 853. Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies. URL: https://www.etsi.org/deliver/etsi_ts/102800_102899/102853/ (vaadatud 15.07.2024).
- [38] ETSI TS 119 612. Electronic Signatures and Infrastructures (ESI); Trusted Lists. URL: http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/ (vaadatud 15.07.2024).
- [39] ETSI EN 319 122-1. Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 1: Building blocks and CAAdES baseline signatures. URL: https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/ (vaadatud 15.07.2024).
- [40] ETSI TS 103 173. Electronic Signatures and Infrastructures (ESI); CAAdES Baseline Profile. URL: https://www.etsi.org/deliver/etsi_ts/103100_103199/103173/ (vaadatud 15.07.2024).
- [41] ETSI EN 319 132-1. Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures. URL: https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/ (vaadatud 15.07.2024).
- [42] ETSI TS 103 171. Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile. URL: http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/ (vaadatud 15.07.2024).
- [43] ETSI EN 319 142-1. Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures. URL: http://www.etsi.org/deliver/etsi_en/319100_319199/31914201/
- [44] ETSI TS 103 172. Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile. URL: https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/ (vaadatud 15.07.2024).
- [45] ETSI EN 319 162-1. Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers. URL: http://www.etsi.org/deliver/etsi_en/319100_319199/31916201/ (vaadatud 15.07.2024).
- [46] ETSI TS 103 174. Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile. URL: https://www.etsi.org/deliver/etsi_ts/103100_103199/103174/ (vaadatud 15.07.2024).

- [47] ETSI EN 319 401. Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/319401/ (vaadatud 15.07.2024).
- [48] ETSI EN 319 403. Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/319403/ (vaadatud 15.07.2024).
- [49] ETSI EN 319 411-1. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/ (vaadatud 15.07.2024).
- [50] ETSI EN 319 411-2. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/ (vaadatud 15.07.2024).
- [51] ETSI EN 319 411-3. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/31941103/ (vaadatud 16.07.2024).
- [52] ETSI EN 319 412-1. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/ (vaadatud 16.07.2024).
- [53] ETSI EN 319 412-2. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/31941202/ (vaadatud 16.07.2024).
- [54] ETSI EN 319 412-3. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/ (vaadatud 16.07.2024).
- [55] ETSI EN 319 412-4. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/ (vaadatud 16.07.2024).
- [56] ETSI EN 319 412-5. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements. URL: http://www.etsi.org/deliver/etsi_en/319400_319499/31941205/ (vaadatud 16.07.2024).
- [57] ETSI EN 319 421. Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. URL: https://www.etsi.org/deliver/etsi_en/319400_319499/319421/ (vaadatud 16.07.2024).
- [58] ETSI EN 319 422. Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles. URL: https://www.etsi.org/deliver/etsi_en/319400_319499/319422/ (vaadatud 16.07.2024).
- [59] Vabariigi Valitsuse 11. jaanuari 2019 määrus nr 4 „Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektroonilise isikutuvastamise ja digitaalse allkirjastamise tagamisel“. URL: <https://www.riigiteataja.ee/akt/115012019011> (vaadatud 16.07.2024).
- [60] Majandus- ja Kommunikatsiooniministeerium. Riigi Infosüsteemi Ameti põhimäärus. URL: <https://www.riigiteataja.ee/akt/128042011001?leiaKehtiv> (vaadatud 16.07.2024).
- [61] Politsei- ja Piirivalveamet. Dokumendi kättesaamine kaupluses. <https://www.politsei.ee/et/dokumendi-kaettesaamine-kaupluses> (vaadatud 16.07.2024).

- [62] Siseministerium. Isikukoodide moodustamise ja andmise kord. URL: <https://www.riigiteataja.ee/akt/120092023008?leiaKehtiv> (vaadatud 16.07.2024).
- [63] Eurosmart. Implementation of the eIDAS nodes: State of play, 03.09.2020. URL: <https://www.eurosmart.com/implementation-of-the-eidas-nodes-state-of-play/> (vaadatud 16.07.2024).
- [64] Wikipedia. National identification number. URL: https://en.wikipedia.org/wiki/National_identification_number (vaadatud 16.07.2024).
- [65] Vikipeedia. Isikukood. URL: <https://et.wikipedia.org/wiki/Isikukood> (vaadatud 16.07.2024).
- [66] Vikipeedia. Isikukood. Kontrollnumbri metoodiline viga. URL: https://et.wikipedia.org/wiki/Isikukood#Kontrollnumbri_metoodiline_viga (vaadatud 16.07.2024).
- [67] Wikipedia. Unique Master Citizen Number (JMBG). Checksum Calculation. URL: https://en.wikipedia.org/wiki/Unique_Master_Citizen_Number#Checksum_calculation (vaadatud 16.07.2024).
- [68] Wikipedia. National identification number. Hungary. URL: https://en.wikipedia.org/wiki/National_identification_number#Hungary (vaadatud 16.07.2024).
- [69] Privacy International. Hungarian Constitutional Court Decides on Identity Numbers"Stream: Blog". Privacy International, 1996. URL: <https://web.archive.org/web/20110120075253/http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-64762> (vaadatud 16.07.2024).
- [70] Riigi Infosüsteemi Ameti blogi. Andmejälgija, 2.03.2017. URL: <https://blog.ria.ee/aj/> (vaadatud 16.07.2024).
- [71] Vikipeedia. ID-kaart. URL: <https://et.wikipedia.org/wiki/ID-kaart> (vaadatud 13.08.2024).
- [72] <https://github.com/martinpaljak/GlobalPlatformPro> (vaadatud 16.07.2024).
- [73] Oracle. Oracle Java Card technology. URL: <https://www.oracle.com/technetwork/java/embedded/javacard/overview/index.html> (vaadatud 16.07.2024).
- [74] Smart-ID. Smart-ID Technical overview, 2017. URL: <https://www.smart-id.com/wordpress/wp-content/uploads/2017/01/smart-id-technical-overview-v0.6.html> (vaadatud 16.07.2024).
- [75] Riigi Infosüsteemi Amet. Isikuandmete faili lugemine ID-kaardilt. <https://www.id.ee/artikkel/isikuandmete-faili-lugemine-id-kaardilt/> (vaadatud 16.07.2024).
- [76] Euroopa Liit. Euroopa Parlamendi ja nõukogu määrus (EL) 2018/1724, 2. oktoober 2018, millega luuakse ühtne digivärv teabele ja menetlustele ning abi- ja probleemilahendamisteenustele juurdepääsu pakkumiseks ning millega muudetakse määrust (EL) nr 1024/2012 (ühtse digivärava määrus). URL: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32018R1724> (vaadatud 16.07.2024).
- [77] Riigi Infosüsteemi Amet. SPOF 2.1 – autentimisprotokollistikud, 2022. URL: <https://www.ria.ee/media/2614/download> (vaadatud 16.07.2024).
- [78] Estonian Information System Authority. Architecture of ID-software, v. 2.7, 2024. URL: <https://open-id.github.io/> (vaadatud 16.07.2024).
- [79] Riigi Infosüsteemi Amet. DigiDoc konteineri formaatide elutsüklid. URL: <https://www.id.ee/artikkel/digidoc-konteineri-formaatide-elutsykkel/> (vaadatud 16.07.2024).
- [80] Riigi Infosüsteemi Amet. Failide krüpteerimine ja dekrüpteerimine DigiDoc4 kliendiga. URL: <https://www.id.ee/artikkel/dokumentide-krüpteerimine-ja-dekrüpteerimine/> (vaadatud 16.07.2024).
- [81] AS Sertifitseerimiskeskus. Encrypted Digidoc Format Specification, 2012. URL: https://www.id.ee/wp-content/uploads/2020/06/sk-cdoc-1.0-20120625_en.pdf (vaadatud 16.07.2024).

[82] Estonian Information System Authority. CDOC2 System documentation. URL: <https://open-eid.github.io/CDOC2/1.1/> (vaadatud 21.05.2025)

[83] Information System Authority. ROCA Vulnerability and eID: Lessons Learned. URL: <https://www.ria.ee/sites/default/files/documents/2022-11/Roca-vulnerability-and-eID-lessons-learned-2018.pdf> (vaadatud 13.08.2024).

[84] <https://www.ria.ee/riigi-infosusteeim/elektrooniline-identiteet-ja-usaldusteenused/eid-integratsioonivahendid>