Pealkiri:	**Zetes Estonia OÜ – Zetes Estonia OÜ poolt Eesti Vabariigi ID-1 formaadis isikut tõendavate dokumentide jaoks väljaantud sertifikaatide avaliku võtme taristu avalikustamise avaldus**
Märgistus:	**[ZE PDS-ID1]**
Dokumendi OI:	**[1.3.6.1.4.1.47718.3.13].01**
Kategooria:	**Sertifitseerimispõhimõtted ja poliitikad**
Versioon:	**1.3**
Olek:	**Kinnitatud**
Kuupäev:	**12.11.2025**
Organisatsioon:	**Zetes Estonia OÜ**
Salastatuse tase	**AVALIK**

Sisukord

Dokumendi ajalugu

Versioon	Kuupäev	Muudatused
1.3	12.11.2025	Versiooni number on kooskõlas sertifitseerimispõhimõtete [ZE CPS-ID1-EID-CA] versiooni numbriga.

1 AVALIKU VÕTME TARISTU AVALIKUSTAMISE AVALDUSEST

1.1 Sissejuhatus

See dokument on **avaliku võtme taristu avalikustamise avaldus (PDS).** Dokumendis ja sellega seotud muudes dokumentides viidatakse sellele tähisega [ZE PDS-ID1]. Dokument on kokkuvõte olulisest infost, mis on saadud sertifitseerimispõhimõtetest (edaspidi CPS), millele viidatakse tähisega [ZE CPS-ID1-EID-CA], ja kasutustingimustest tellijatele ja tugipooltele, millele viidatakse tähistega [ZE TC-ID1] ja [ZE TC-ID1-SUB].

[ZE CPS-ID1-EID-CA] on avalik dokument, milles kirjeldatakse põhimõtteid, mida Zetes Estonia OÜ (edaspidi ZE) kui kvalifitseeritud usaldusteenuse osutaja ja teised pooled, nagu Politsei- ja Piirivalveamet (edaspidi PPA) ja Välisministeerium (edaspidi VM), kohaldavad ID-1 formaadis isikut tõendavate dokumentide (edaspidi dokumendid) väljaandmiseks.

See dokument on mõeldud füüsilisele isikule, kellel on Eesti Vabariigi poolt välja antud dokument, millele on kantud ZE väljaantud sertifikaadid. Neid isikuid nimetatakse tellijateks. See on mõeldud ka kõigile füüsilistele või juriidilistele isikutele, kes tuginevad tellija sertifikaatidele, näiteks digiallkirja kinnitamiseks või tellija autentimiseks veebitehingus. Neid isikuid nimetatakse tuginevaks pooleks.

Dokument on esitatud üksnes teavitamise eesmärgil ja sellel ei ole õiguslikku jõudu. Dokumendi sisu ei asenda ega muuda PPA sertifitseerimispoliitikas (CP) sisalduvaid sätteid ega ZE välja antud sertifitseerimispõhimõtteid (CPS) või kasutustingimusi (TC). Mis tahes vastuolu korral on ülimuslikud ametlikud sertifitseerimispoliitikad, sertifitseerimispõhimõtted ning kasutustingimused.

Sellel dokumendil ei ole oma jõustumiskuupäeva. See on kooskõlas kehtivate dokumentidega [ZE CPS-ID1-EID-CA], [ZE TC-ID1] ja [ZE TC-ID1-SUB].

1.2 Mõisted ja lühendid

1.2.1 Mõisted

Aktiveerimisandmed	Andmeväärtused, mis ei hõlma täielikke privaatvõtmeid, kuid on vajalikud privaatvõtmete või privaatvõtmeid sisaldavate krüptomoodulite kasutamiseks, näiteks PIN-kood, paroolifraas või privaatvõtme osad, mida kasutatakse võtmejagamise skeemis. Aktiveerimisandmete kaitse takistab privaatvõtme volitamata kasutamist.
Sertifikaat	Sertifitseerija poolt digitaalselt allkirjastatud failis sisalduv teabeühik. See sisaldab vähemalt väljaandjat, avalikku võtit ja teavet, millega on võimalik tuvastada avalikule võtmele vastava privaatvõtme omanik.
Sertifitseerimispoliitika	Reeglite kogum, mis näitab sertifikaadi kohaldatavust konkreetsele kogukonnale ja/või rakenduste klassile, millel on ühised turvanõuded.
Sertifikaatide tühistusnimekiri	Kehtetuks tunnistatud ja peatatud sertifikaatide loend. Lühendatud nimetus CRL (*Certificate Revocation List*). Sertifitseerija teeb selle (perioodiliselt) kättesaadavaks tellijatele ja tuginevatele pooltele.
Sertifitseerija	Olenevalt kontekstist võib see termin viidata 1) tark- ja riistvarasüsteemile, mis moodustab sertifikaadi väljaandmise taristu, või 2) organisatsioonile, mis haldab sertifitseerija võtmeid, annab välja sertifikaate ja ajakohastab sertifikaadi staatust kogu sertifikaadi elutsükli jooksul.
Sertifitseerimispõhimõtted	Sertifitseerija poolt sertifikaatide väljaandmisel, haldamisel, kehtetuks tunnistamisel ja uuendamisel või uute võtmete loomisel kasutatavad põhimõtted.
Kvalifitseeritud allkirja andmise vahend	Dokumendis olev avaliku võtme taristu toega kiip. Kvalifitseeritud digiallkirja puhul, millel on eeskirjale [QCP-n-qscd] vastav sertifikaat, vastab kiip eIDAS-määruses [EL 910/2014 EIDAS] sätestatud kvalifitseeritud allkirja andmise vahendi nõuetele.
Registreerija	Olenevalt kontekstist võib see mõiste viidata 1) tarkvara- ja riistvarasüsteemile, mis moodustab taristu subjektide ja/või tellijate kasutuselevõtuks, registreerimiseks ja tuvastamiseks, või 2) organisatsioonile, mis vastutab kasutuselevõtu, registreerimise ja tuvastamise eest.
Tuginev pool	Iga füüsiline või juriidiline isik, kes ei ole tellija või subjekt ise, kuid kes peab kasutama ja tuginema selle sertifikaadi kaudu välja antud tellija/subjekti avaliku võtme ja sertifikaadis sisalduva tellija/subjekti identiteedi ja/või muude atribuutide vahelise seose täpsusele.
Subjekt	Juriidiline või füüsiline isik, kellele sertifikaat on välja antud ja kellel on sertifikaadi kasutusõigus. Sertifikaadi nime väljad määravad subjekti. See on üksikasjalikumalt määratletud igas konkreetses CPSis, et viia see vastavusse CPSi kontekstiga.
Tellija	Usaldusteenust telliv juriidiline või füüsiline isik. Tellija ja subjekt võivad olla samad või erinevad isikud. See on üksikasjalikumalt määratletud igas konkreetses CPSis, et viia see vastavusse CPSi kontekstiga.
Tellija sertifikaadid	Tellijale välja antud sertifikaat. See on üksikasjalikumalt määratletud igas konkreetses CPSis, et viia see vastavusse CPSi kontekstiga.

1.2.2 Lühendid

Lühend	Täisnimetus
CPS	Sertifitseerimispõhimõtted
CRL	Sertifikaatide tühistusnimekiri (*Certificate Revocation List*)
VM	Eesti Vabariigi Välisministeerium
OCSP	Võrgusertifikaadi staatuse protokoll (*Online Certificate Status Protocol*)
OID	Objekti identifikaator
PPA	Politsei- ja Piirivalveamet
PDS	Avaliku võtme taristu avalikustamise avaldus
PKI	Avaliku võtme taristu (*Public Key Infrastructure*)
QSCD	Kvalifitseeritud allkirja andmise vahend (*Qualified Signature Creation Device*)
QTSP	Kvalifitseeritud usaldusteenuse osutaja (*Qualified Trust Service Provider*)
QES	Kvalifitseeritud elektrooniline allkiri (*Qualified Electronic Signature*), digiallkiri
RIA	Riigi Infosüsteemi Amet
LDAP	Kataloogipöörduse kergprotokoll (*Lightweight Directory Access Protocol*)
ZE	Zetes Estonia OÜ

1.2.3 Viited

Viited muudele dokumentidele või muudele allikatele on märgitud nurksulgudes, nt **[EST ITDS].**

Viidete loetelu on esitatud lisas A.

2 AVALIKU VÕTME TARISTU AVALIKUSTAMISE AVALDUS

2.1 Kontaktandmed

Sertifikaate puudutava teabe saamiseks võtke ühendust Zetes Estoniaga. Zetes Estonia on Tallinnas asutatud osaühing, mille registrikood on 17066049 ja mis on kantud Eesti usaldusnimekirja kui QTSP.

Sertifikaatidega seotud küsimuste korral võite Zetes Estoniaga ühendust võtta järgmiste kanalite kaudu:

E-post: info_eidpki AT ee.zetes.com

Veebileht: https://repository.eidpki.ee

Dokumendi taotlemise ja väljaandmise protsessi, sertifikaatide kasutamise, Digidoci tarkvara kasutamise, dokumendi kadumisest või vargusest teatamise või sertifikaatide kehtetuks tunnistamise taotlemisega seonduvates küsimustes pöörduge dokumendi väljaandja veebilehtede või teeninduste poole.

Veebileht: https://www.politsei.ee

Veebileht: https://www.id.ee

Veebileht: https://vm.ee

2.2 Sertifikaadi tüüp, valideerimine ja kasutamine

2.2.1 Sertifikaatide liigid

Iga dokument sisaldab kaht tüüpi tellija sertifikaate:

- sertifikaat autentimiseks/krüpteerimiseks;
- sertifikaat kvalifitseeritud elektrooniliste allkirjade (digiallkirjade) andmiseks.

Eesti isikut tõendavate dokumentide seaduse [EST ITDS] kohaselt väljaantavad kahte tüüpi tellija sertifikaadid on Euroopa standardites määratletud sertifikaadi tüübid:

- NCP+ nõuetele vastavad autentimise ja krüpteerimise tellija sertifikaadid
- QCP-n-qscd nõuetele vastavad kvalifitseeritud elektrooniliste allkirjade tellija sertifikaadid

NCP+ tellija sertifikaadid autentimiseks ja krüpteerimiseks peavad sisaldama järgmisi OID-sid:

- 0.4.0.2042.1.2 kooskõlas [ETSI EN 319 411-1] punktiga 5.3 b),
- eID CP OID, mis on määratletud [PPA CP-ID1-EID-CA].

QCP-n-qscd QES-i tellija sertifikaadid peavad sisaldama järgmisi OID-sid:

- 0.4.0.194112.1.2 kooskõlas [ETSI EN 319 411-2] punktiga 5.3 c),
- eID CP OID, mis on määratletud [PPA CP-ID1-EID-CA].

Alljärgnevas tabelis on loetletud kõik dokumendid, mis sisaldavad OID numbritega sertifikaate, ning neile kohaldatavat sertifitseerimispoliitikat [PPA CP-ID1-EID-CA].

Sertifitseerimispoliitika OID	Väljaandja	Dokumendi liik	Kasutamine
1.3.6.1.4.1.51361.2.1.1 0.4.0.2042.1.2	PPA	Eesti kodaniku ID-kaart	Tuvastamise sertifikaat tuvastamiseks, krüpteerimiseks ja turvaliseks e-kirjavahetuseks
1.3.6.1.4.1.51361.2.1.1 0.4.0.194112.1.2	PPA	Eesti kodaniku ID-kaart	Kvalifitseeritud digiallkirja sertifikaat eIDAS määrusele vastavate kvalifitseeritud digiallkirjade andmiseks

1.3.6.1.4.1.51361.2.1.2 0.4.0.2042.1.2	PPA	Euroopa Liidu kodaniku ID-kaart	Tuvastamise sertifikaat tuvastamiseks, krüpteerimiseks ja turvaliseks e-kirjavahetuseks
1.3.6.1.4.1.51361.2.1.2 0.4.0.194112.1.2	PPA	Euroopa Liidu kodaniku ID-kaart	Kvalifitseeritud digiallkirja sertifikaat eIDAS määrusele vastavate kvalifitseeritud digiallkirjade andmiseks
1.3.6.1.4.1.51361.2.1.3 0.4.0.2042.1.2	PPA	Pikaajalise elaniku elamisloakaart	Tuvastamise sertifikaat tuvastamiseks, krüpteerimiseks ja turvaliseks e-kirjavahetuseks
1.3.6.1.4.1.51361.2.1.3 0.4.0.194112.1.2	PPA	Pikaajalise elaniku elamisloakaart	Kvalifitseeritud digiallkirja sertifikaat eIDAS määrusele vastavate kvalifitseeritud digiallkirjade andmiseks
1.3.6.1.4.1.51361.2.1.4 0.4.0.2042.1.2	PPA	Tähtajaline elamisloakaart	Tuvastamise sertifikaat tuvastamiseks, krüpteerimiseks ja turvaliseks e-kirjavahetuseks
1.3.6.1.4.1.51361.2.1.4 0.4.0.194112.1.2	PPA	Tähtajaline elamisloakaart	Kvalifitseeritud digiallkirja sertifikaat eIDAS määrusele vastavate kvalifitseeritud digiallkirjade andmiseks
1.3.6.1.4.1.51361.2.1.5 0.4.0.2042.1.2	PPA	ELi ja Ühendkuningriigi kodanike pereliikmete elamisloakaart	Tuvastamise sertifikaat tuvastamiseks, krüpteerimiseks ja turvaliseks e-kirjavahetuseks
1.3.6.1.4.1.51361.2.1.5 0.4.0.194112.1.2	PPA	ELi ja Ühendkuningriigi kodanike pereliikmete elamisloakaart	Kvalifitseeritud digiallkirja sertifikaat eIDAS määrusele vastavate kvalifitseeritud digiallkirjade andmiseks
1.3.6.1.4.1.51361.2.1.6 0.4.0.2042.1.2	PPA	E-residendi digi-ID	Tuvastamise sertifikaat tuvastamiseks, krüpteerimiseks ja turvaliseks e-kirjavahetuseks
1.3.6.1.4.1.51361.2.1.6 0.4.0.194112.1.2	PPA	E-residendi digi-ID	Kvalifitseeritud digiallkirja sertifikaat eIDAS määrusele vastavate kvalifitseeritud digiallkirjade andmiseks
1.3.6.1.4.1.51455.2.1.1 0.4.0.2042.1.2	VM	Diplomaatiline isikutunnistus	Tuvastamise sertifikaat tuvastamiseks, krüpteerimiseks ja turvaliseks e-kirjavahetuseks
1.3.6.1.4.1.51455.2.1.1 0.4.0.194112.1.2	VM	Diplomaatiline isikutunnistus	Kvalifitseeritud digiallkirja sertifikaat eIDAS määrusele vastavate kvalifitseeritud digiallkirjade andmiseks

2.2.2 Sertifikaadi valideerimiskord

Sertifikaati kasutades peab tuginev pool alati esmalt kontrollima sertifikaadi staatust, kasutades vähemalt ühte avalikku sertifikaadi staatuse teenust. CRL-idele tugineva taotluse esitanud pooled peavad arvesse võtma CRL-ide perioodilisust. Tuginevad pooled peavad hindama, kas see perioodilisus on nende jaoks oluline või mitte.

Sertifikaati saab kasutada:

- sertifikaadi kehtivuse, peatamise või kehtetuks tunnistamise kontrollimiseks, kasutades jooksvat teavet kehtetuks tunnistamise staatuse kohta, nagu on märgitud;
- kõigi sertifikaadi kasutamise piirangute arvesse võtmiseks, mis on sertifikaadil märgitud tuginevale poolele, ja;
- muude ettevaatusabinõude võtmiseks, mis on ette nähtud dokumentides [ZE TC-ID1], [ZE TC-ID1-SUB], [ZE CPS-ID1-EID-CA], [ZE CPS-ID1-ROOT-CA], [PPA CP-ID1-EID-CA], [PPA CP-ID1-ROOT-CA].

2.3 Tellijad ja subjektid

Järgnev on väljavõte [ZE CPS-ID1-EID-CA] punktist 1.3.3 „Subjektid ja tellijad“.

Termin **subjekt** viitab isikule, kellele sertifikaat on välja antud ja kellel on sertifikaadi kasutusõigus. Subjekt on füüsiline isik, kelle identiteet on kodeeritud sertifikaadi subjekti nime väljale.

Termin **tellija** viitab isikule, kes on tellinud sertifikaadiga seotud usaldusteenuse.

Subjekt ja tellija võivad olla üksnes füüsilised isikud, kellel on selleks õigus [EST ITDS] alusel (mis viitab tellijale kui „dokumendi kasutajale“). Ühel isikul võib igal ajahetkel olla ainult üks kehtiv samaliigiline dokument.

Iga subjekt ei ole ka tellija. Näiteks alaealisele lapsele välja antud sertifikaatide puhul on laps subjekt ja lapse vanem või seaduslik eestkostja on tellija. Täiskasvanud ja teovõimelisele isikule välja antud sertifikaatide puhul on isik nii subjekt kui ka tellija. Juhul, kui subjekti ei peeta õigusvõimeliseks, on tellija volitatud isik, kellel on seadusjärgne volitus subjekti esindamiseks.

Kohaldatakse järgmist:

- alla 15-aastased alaealised on subjektid, mitte tellijad;
- 15–17-aastased alaealised on subjektid, kuid [EST ITDS] võimaldab neil iseseisvalt teha selles seaduses ette nähtud menetlustoiminguid, st neid alaealisi käsitatakse tellijatena. Nad võivad iseseisvalt taotleda dokumente ja sertifikaate, iseseisvalt nõustuda [ZE TC-ID1-SUB]-iga ning iseseisvalt taotleda oma sertifikaatide kehtetuks tunnistamist;
- lapsevanemad ja seaduslikud eestkostjad võivad tegutseda [EST PKS] määratletud alaealise nimel tellijana;
- täielikult teovõimelised täisealised isikud on alati nii tellijad kui ka subjektid;
- passiivse õigusvõimega või piiratud õigusvõimega isikud, nagu on määratletud [EST HMS] ja [EST TsÜS], võivad olla ainult subjektid.

Selles dokumendis tuleb kõiki viiteid terminile „subjekt“ tõlgendada kui isikut, kelle identiteediandmed on talletatud tellija sertifikaatides. Kõiki viiteid terminile „tellija“ tuleb tõlgendada kui isikut, kellel on õigus ja kellelt eeldatakse tegutsemist subjekti nimel (iseenda või teise isiku nimel) tellija sertifikaatidega seotud taotlemise, kehtetuks tunnistamise ja muude kohustuste haldamise eesmärgil.

2.4 Tuginemise piirangud

Järgnev on väljavõte [ZE CPS-ID1-EID-CA] punktist 4.5.1 „Subjekti privaatvõtme ja sertifikaadi kasutamine“.

Tellija peab tagama, et sertifikaate kasutatakse ainult [ZE CPS-ID1-EID-CA] punktis 6.7.1 kirjeldatud eesmärkidel.

Tellija, kes vastutab oma hoole all oleva subjekti eest, st vanemad või seaduslikud eestkostjad, vastutab ka tema hoole all olevale subjektile välja antud QSCD nõuetekohase kasutamise eest.

Väljastatakse kahte tüüpi sertifikaate, mõlemal on oma kindel kasutusotstarve. Tuvastamise ja krüpteerimise sertifikaat on ette nähtud võrguteenustes autentimiseks ja failide või sõnumite krüpteerimiseks ning seda ei tohiks kasutada digiallkirjade loomiseks. Kvalifitseeritud elektroonilise allkirja sertifikaat on mõeldud digiallkirjade andmiseks.

Pärast QSCD üleandmist vastutab tellija võtmete ja sertifikaatide nõuetekohase kasutamise eest, st tellija peab tagama, et QSCD-d ja PIN-koode kasutatakse sertifikaatides kodeeritud kasutusotstarbel.

Võtmed genereeritakse ja salvestatakse QSCD-s, millest ei saa privaatvõtit välja võtta ja mis tagab ainukontrolli privaatvõtme üle.

Tellija peab tagama, et QSCD ja sellega seotud PIN-kood on kaitstud kaotsimineku, varguse, avalikustamise või ohustamise eest.

Tellijal on järgmised kohustused:

- hoiustada QSCD-d turvaliselt ja kontrollitult
- mitte jagada QSCD-d teise isikuga
- hoida PIN-koode ja PUK-i teiste isikute eest saladuses
- valida PIN-kood, mis ei ole ilmne

- QSCD kaotuse või varguse korral viivitamatult teavitada dokumendi väljaandjat või esitada sertifikaatide kehtetuks tunnistamise portaali kaudu avaldus
- hoiduda sellise QSCD kasutamisest, mille sertifikaadid on aegunud või kehtetuks tunnistatud.

Järgnev on väljavõte [ZE CPS-ID1-EID-CA] punktist „4.5.2 Tugineva poole avalik võti ja sertifikaadi kasutamine“:

Tuginev pool peab sertifikaati kontrollima vähemalt ühe sertifikaadi staatuse teenuse abil. Tuginev pool usaldab sertifikaati ainult siis, kui see ei ole peatatud või kehtetuks tunnistatud, ning ei tohi tugineda sertifikaadile, kui sertifikaadi staatust ei ole võimalik kindlaks teha.

Tuginev pool tugineb sertifikaatidele ainult siinses CPSis ning sertifikaadis endas kodeeritud poliitikateabes ja võtmekasutusteabes sätestatud eesmärgil.

Tuginev pool vastutab täielikult allkirjaga seotud kuupäeva ja kellaaja asjakohasuse tõlgendamise eest seoses sertifikaadi staatusega allkirja andmise kuupäeval ja kellaajal ning allkirja iga kinnitamise kuupäeval ja kellaajal.

Tuginev pool vastutab täielikult allkirjaga seotud kuupäeva ja kellaaja asjakohasuse tõlgendamise eest seoses sertifikaadi kehtivusaja lõppemise kuupäeva ja kellaajaga võrrelduna allkirja andmise kuupäeva ja kellaajaga ning allkirja iga kinnitamise kuupäeva ja kellaajaga.

Kui sertifikaadi kehtivusaeg on lõppenud, see on peatatud või kehtetuks tunnistatud, siis ei usalda tuginev pool sertifikaati ega kasuta seda autentimiseks või krüpteerimiseks.

Järgnev on väljavõte [ZE CPS-ID1-EID-CA] punktist „4.5.2 Arhiivi säilitamisperiood“:

Sertifitseerija säilitab auditeerimislogisid sertifitseerija ja OCSP võtmete genereerimise sündmuste, sertifitseerija ja OCSP sertifikaatide väljaandmise sündmuste ning sertifitseerija ja OCSP sertifikaatide elutsükli sündmuste kohta vähemalt 10 aastat pärast vastavat sündmust.

Sertifitseerija säilitab auditeerimislogisid tellija sertifikaatide väljaandmise sündmuste ja tellija sertifikaatide elutsükli sündmuste kohta vähemalt 10 aastat pärast vastavat sündmust.

Sertifitseerija säilitab auditeerimislogisid sertifikaadi oleku valideerimise teenuste (CRL ja OCSP) sündmuste kohta vähemalt 10 aastat pärast vastavat sündmust.

Sertifitseerija säilitab kõigi genereeritud sertifitseerija sertifikaatide, OCSP sertifikaatide ja tellija sertifikaatide kirjeid (koopiaid) vähemalt 10 aastat alates sertifikaadi kehtivuse alguskuupäevast.

Registreerija ja kaarditootja säilitavad auditeerimislogisid registreerimissündmuste, võtmete genereerimise sündmuste, sertifikaaditaotluste sündmuste ja sertifikaadi elutsükli sündmuste kohta vähemalt 10 aastat pärast vastavat sündmust.

Registreerija säilitab tellija sertifikaatide väljaandmist ja elutsükli haldamist toetavat teavet vähemalt 10 aastat pärast seda, kui sertifikaadi kehtivus on lõppenud.

PPA paberkandjal kirjeid arhiveeritakse keskselt PPA-s (see hõlmab registreerija lepingupartnerite ja saatkondade hallatavate teeninduste paberkandjal kirjeid nagu väljastamisteatised ja saatkondades esitatud taotlused). Sertifikaadiga seotud tõendeid säilitatakse e-identimise ja e-tehingute usaldusteenuste seaduse (EST EUTS) ja eIDAS-määruse (määrus (EL) nr 910/2014) nõuete kohaselt ettenähtud ajavahemiku jooksul.

PPA elektroonilised kirjeid säilitatakse andmebaasi eeskirjade alusel, mis ületavad eIDASi nõudeid ning on sätestatud õigusaktides tähistega EST ITDAM, EST ABISM ja EST ARHS. Registreerija lepingupartnerite valduses olevaid elektroonilisi kirjeid hoitakse lepingupartnerite juures ja seejärel edastatakse PPA-le.

VM-i paberkandjal kirjeid arhiveeritakse VM-is. Sertifikaadiga seotud tõendeid säilitatakse e-identimise ja e-tehingute usaldusteenuste seaduse (EST EUTS) ja eIDAS-määruse (määrus (EL) nr 910/2014) nõuete kohaselt ettenähtud ajavahemiku jooksul.

VM-i elektroonilisi kirjeid säilitatakse andmebaasireeglite alusel, mis ületavad eIDAS-i nõuded ning on sätestatud dokumendis [EST VEISDB REG].

Kaarditootja säilitab dokumentide ja sertifikaatide väljaandmist ja väljaandmise järgset uuendamist tõendavat teavet vähemalt 10 aastat pärast sertifikaadi kehtivuse lõppemist.

2.5 Tellijate kohustused

Tellijad on seotud CPSis [ZE CPS-ID1-EID-CA] ja kasutustingimustes [ZE TC-ID1-SUB] nimetatud kohustustega. Vt ka väljavõte [ZE CPS-ID1-EID-CA] punktist „4.5.1 Subjekti privaatvõti ja sertifikaadi kasutamine“ peatükis 2.4.

Tellija tuvastamissertifikaati ei saa kasutada eIDAS-määrusele [EL 910/2014 EIDAS] vastavate kvalifitseeritud digiallkirjade loomiseks.

Järgnev on väljavõte [ZE CPS-ID1-EID-CA] punktist „4.5.1 Subjekti privaatvõtme ja sertifikaadi kasutamine“.

Tellija peab tagama, et QSCD ja sellega seotud PIN-kood on kaitstud kaotsimineku, varguse, avalikustamise või ohustamise eest.

Tellijal on järgmised kohustused:

- hoiustada QSCD-d turvaliselt ja kontrollitult
- mitte jagada QSCD-d teise isikuga
- hoida PIN-koode ja PUK-i teiste isikute eest saladuses
- valida PIN-kood, mis ei ole ilmne
- QSCD kaotuse või varguse korral viivitamatult teavitada dokumendi väljaandjat või esitada sertifikaatide kehtetuks tunnistamise portaali kaudu avaldus
- hoiduda sellise QSCD kasutamisest, mille sertifikaadid on aegunud või kehtetuks tunnistatud.

Järgnevalt on esitatud väljavõte [ZE CPS-ID1-EID-CA] punktist 9.6.3 „Tellija kinnitused ja garantiid“.

Vastavalt [ZE CPS-ID1-EID-CA] punktile 9.6.3 hõlmavad tellijate kohustused seoses kinnituste ja garantiidega järgmist:

- tellija järgib ZE poolt käesolevas CPSis, tellija lepingus, sealhulgas kasutustingimustes sätestatud nõudeid;
- tellija esitab registreerijale dokumendi taotlemisel tõesed ja õiged andmed;
- kui subjekti nimi ja/või isikukood muutub, peab tellija ühe kuu jooksul teatama registreerijale õiged andmed vastavalt kehtestatud õigusaktidele;
- subjekt kasutab privaatvõtmeid ainult selleks otstarbeks, mis on märgitud tellija sertifikaatides;
- subjekt kasutab privaatvõtmeid ja vastavaid tellija sertifikaate ainult dokumenti integreeritud turvalises krüptoseadmes ZE poolt ettenähtud viisil;
- subjekt kasutab privaatvõtit vastavalt käesolevale dokumendile;
- subjekt teavitab registreerijat viivitamatult kõigist kahtlustest või võimalusest, et privaatvõtit on omavoliliselt kasutatud, ja taotleb tellija sertifikaatide kehtetuks tunnistamist;
- tellija taotleb viivitamata tellija sertifikaatide kehtetuks tunnistamist, kui dokument on varastatud, kahjustatud, kadunud või muul moel ei ole enam tellija kontrolli all;
- subjekt ei kasuta privaatvõtmeid pärast tellija sertifikaatide kehtivusaja lõppemist või pärast tellija sertifikaatide kehtetuks tunnistamist või pärast tipmise sertifitseerija sertifikaadi ja/või alamsertifitseerija sertifikaadi kehtetuks tunnistamist;
- tellija on teadlik, et aegunud, kehtetuks tunnistatud või peatatud sertifikaatide alusel antud kvalifitseeritud elektroonilised allkirjad on kehtetud;
- tellija on teadlik, et on äärmiselt soovitatav kasutada kvalifitseeritud elektroonilise allkirja tellija sertifikaati ainult koos kvalifitseeritud ajatempliga.

Tellija ei vastuta dokumendiga tehtud toimingute eest, kui tellija sertifikaadid olid enne dokumendi üleandmist peatatud staatuses.

Tellija on teadlik, et ZE avaldab kehtiva tellija sertifikaadi tuvastamiseks kehtivusaja jooksul LDAP kataloogiteenuse kaudu.

2.6 Sertifikaadi staatuse kontrollimise kohustused tuginevatele pooltele

Tuginevad pooled on seotud CPSis [ZE CPS-ID1-EID-CA] ja kasutustingimustes [ZE TC-ID1] nimetatud kohustustega. Vt ka väljavõte [ZE CPS-ID1-EID-CA] punktist „4.5.2 Tugineva poole avalik võti ja sertifikaadi kasutamine“ peatükis 2.4 .

2.7 Piiratud garantii ja vastutuse välistamine

Järgmine on väljavõte [ZE CPS-ID1-EID-CA] punktist 9.7 Garantiist loobumine.

QTSP loobub sõnaselgelt igasugusest vastutusest tuginevate poolte ja tellijate ees kõikidel juhtudel, kui

- sertifikaati kasutati ebaõigesti,
- sertifikaati kasutati muul eesmärgil kui sertifikaadi ettenähtud kasutusotstarve,
- sertifikaadi kehtivust ei kontrollitud asjakohasel ajal nõuetekohaselt,
- tuvastamise sertifikaati kasutati eraõiguslike isikute vahelises eraõiguslikus kontekstis, mis ületab riikliku õiguse või haldustava kohaselt avaliku sektori asutuse poolt osutatava teenuse kasutamiseks nõutava tuvastamise ulatuse.

2.8 Vastutuse piiramine

QTSP vastutuse piirangut kohaldatakse erinevalt sõltuvalt sellest, kas (i) kahju võis olla põhjustatud QTSP poolt seetõttu, et QTSP ei täitnud oma kohustusi eIDAS-määruse [EU 910/2014 EIDAS] alusel, või (ii) kahju on põhjustatud veast või rikkest, mis ei tulene eIDAS-määruse [EU 910/2014 EIDAS] alusel kehtestatud kohustuste rikkumisest.

Järgmine on väljavõte [ZE CPS-ID1-EID-CA] punktist 9.8.1 EIDAS määruse kohaste kohustuste täitmata jätmise tõttu tekitatud kahju eest .

QTSP vastutab kahju eest, mis on tahtlikult või hooletusest põhjustatud füüsilisele või juriidilisele isikule eIDAS-määrusest [EL 910/2014 EIDAS] tulenevate kohustuste täitmata jätmise tõttu. Igal füüsilisel või juriidilisel isikul, kes on kannatanud eIDASi määruse [EL 910/2014 EIDAS] rikkumise tõttu QTSP poolt materiaalset või mittevaralist kahju, on õigus nõuda hüvitist vastavalt liidu ja siseriiklikule õigusele.

Kvalifitseeritud usaldusteenuse osutaja tahtlust või hooletust eeldatakse, välja arvatud juhul, kui kõnealune kvalifitseeritud usaldusteenuse osutaja tõendab, et esimeses lõikes osutatud kahju tekkis ilma kvalifitseeritud usaldusteenuse osutaja tahtluseta või hooletusest.

Ilma et see piiraks eelmiste lõigete kohaldamist, kohaldatakse järgmisi piiranguid:

- QTSP välistab igasuguse vastutuse QSCD rikke eest, kuna QSCD on kaarditootja poolt pakutav.
- Eeldusel, et QTSP on täitnud oma eIDASi määrusest [EL 910/2014 EIDAS] tulenevaid kohustusi, ei vastuta ta tellijate või tuginevate poolte ees teiste PKI osalejate tegude või tegevusetuse eest.
- Käesoleva CPSi eelmises punktis 9.7 kirjeldatud välistused ja piirangud kehtivad eIDASi määruse [EL 910/2014 EIDAS] artikli 13 lõike 2 kohase teenuste kasutamise piiranguna.

Teatavate kahju hüvitamise elementide välistamine

Eesti seadustega kehtestatud piirides ja mitte piirates rohkem kui eIDAS määruse [EL 910/2014 EIDAS] artikli 13 kohaselt lubatud, nagu eespool kirjeldatud, ei vastuta QTSP:

- igasuguse saamata jäänud kasumi eest;
- mis tahes kaudse või kaudselt tekkinud kahju eest, mis on põhjustatud andmete kaotamisest;
- mis tahes kaudsete, tulenevate või karistuslike kahjude eest, mis tulenevad sertifikaatide või digiallkirjade kasutamisest, tarnimisest, litsentsist, täitmisest või mittetäitmisest või sellega seoses;
- kaarditootja mis tahes mittevastavuse või lepingurikkumise eest; või
- mis tahes muu kahju eest, mis ületab tõestatud otsest kahju.

Kui Eesti kohus tunnistab mis tahes vastutuse piiramise või garantii välistamise sätte kehtetuks, ebaseaduslikuks või jõustamatuks vastavalt kohaldatavale õigusele, jäävad ülejäänud sätted täielikult kehtima.

Järgnev on väljavõte [ZE CPS-ID1-EID-CA] punktist 9.8.2 Kahju, mis on põhjustatud veast või puudusest, mida ei loeta eIDAS määruse kohaste kohustuste täitmata jätmiseks.

Mis tahes kahju suhtes, mis on põhjustatud QTSP veast või puudusest, mis ei ole tahtlikult või hooletusest põhjustatud kahju, mis tuleneb eIDAS määruse [EL 910/2014 EIDAS] kohaste kohustuste täitmata jätmisest, kohaldatakse järgmisi vastutuse piiranguid.

- Kõik punktis 9.8.1. kohaldatavad piirangud ja välistused [ZE CPS-ID1-EID-CA][ZE CPS-ID1-EID-CA].
- Lisaks sellele on QTSP vastutuse korral tellija või tugineva poole ees tõendatud otseste kahjude eest QTSP vastutus mis tahes nõude esitaja ees igal juhul piiratud kahjude maksmisega kuni avaldatud kindlustusteabes märgitud ülempiiri ulatuses. Sellist ülempiiri kohaldatakse iga sertifikaadi kohta, mis on nõude aluseks, ja selle sertifikaadi kogu kehtivusaja jooksul ning iga nõude esitaja kohta.
- Järgnevalt on välja toodud erandid.

Vastutuse välistamine

Kui QTSP ei ole tahtlikult või hooletusest rikkunud oma kohustusi vastavalt eIDAS määrusele [EL 910/2014 EIDAS], ei vastuta QTSP absoluutselt mitte mingi kahju eest, mis on seotud või tuleneb ühest (või mitmest) järgmistest asjaoludest või põhjustest.

- Kui sertifikaat, mis on nõude esitajal või muul viisil nõude esitamisega seotud tellijal, on kahjustatud sertifikaadi või sellele juurdepääsu kontrollimiseks kasutatud salasõna või aktiveerimisandmete loata avaldamise või loata kasutamise tõttu.
- Kui sertifikaat, mis on nõude esitaja või muul viisil nõudega seotud tellija valduses, on välja antud asjaomase (kavandatud) tellija valeandmete esitamise, faktivea, identiteedipettuse või tegevusetuse tõttu.
- Kui sertifikaat, mis on nõude esitaja või muul viisil nõude tellija valduses, on aegunud või kehtetuks tunnistatud enne nõude aluseks olevate asjaolude tekkimise kuupäeva.
- Kui sertifikaati, mis on nõude esitaja või muul viisil nõudega seotud tellija valduses, on muudetud mis tahes viisil või seda on kasutatud muul viisil kui [ZE TSPS-ID1], käesoleva CPSi ja/või asjaomase tellija lepingu ja kasutustingimuste [ZE TC-ID1-SUB] või mis tahes kohaldatava seaduse või määruse kohaselt lubatud.
- Kui sertifikaadiga seotud privaatvõti, mis on nõude esitajal või muul viisil nõude esitamisega seotud tellijal, on kahjustatud.
- Kui sertifikaat, mis on nõude esitaja valduses, või allkiri, millele tuginev pool on tuginenud, on pärast selle kasutamist kehtetuks tunnistatud, ilma et see oleks olnud QTSP süü või kavatsus.
- Kui taotluse esitanud pool tugineb sertifikaadile, mis ületab sertifikaadi kehtivusaega, või kui taotluse esitanud pool tugineb sertifikaadil põhinevale elektroonilisele allkirjale, mis on antud väljaspool sertifikaadi kehtivusaega, ilma et oleks olemas oluline ajaline tõend, et elektrooniline allkiri on antud sertifikaadi kehtivusaja jooksul.
- Arvutiriistvara või -tarkvara või matemaatilised algoritmid on arendatud viisil, mis muudab avaliku võtme krüptograafia või asümmeetrilised krüptosüsteemid ebaturvaliseks, eeldusel et QTSP on võtnud kõik vajalikud meetmed teenuste ja tarneahela kvaliteedi ja turvalisuse taseme tõstmiseks selliselt, et säiliks kõrge kvaliteedi- ja turvatasemega samaväärsete teenuste ja toodete kasutamine muutunud asjaoludes ning tagataks teenuste ja toodete jätkuv kasutamine nende ettenähtud otstarbel ning kõrgel turvalisuse tasemel.
- Elektrikatkestus, vooluhäire või muud elektrivarustuse häired, eeldusel et QTSP on võtnud kõik vajalikud meetmed teenuste ja tarneahela kvaliteedi ja turvalisuse taseme tõstmiseks selliselt, et säiliks kõrge kvaliteedi- ja turvatasemega samaväärsete teenuste ja toodete kasutamine muutunud asjaoludes ning tagataks teenuste ja toodete jätkuv kasutamine nende ettenähtud otstarbel ning kõrgel turvalisuse tasemel.
- Ühe või mitme arvutisüsteemi, sideinfrastruktuuri, töötlemis- või salvestusmeediumi või -mehhanismi või nende mis tahes alamkomponendi rike, mis ei ole QTSP ja/või selle alltöövõtjate või teenusepakkujate ainukontrolli all.
- Üks või mitu järgmistest sündmustest: loodusõnnetus (sealhulgas, kuid mitte ainult, üleujutus, maavärin või muu loodus- või ilmastikuga seotud põhjus); töörahutused; sõda, ülestõus või varjatud või avalik sõjaline või geopoliitiline sekkumine ja/või vaenulikkus; varasemad tundmatud krüptoalgoritmid, nullpäeva küberrünnak või sabotaaž, ebasoodsad või tagasiulatuvad õigusaktid või valitsuse meetmed, keelustamine, embargo või

boikott; mässud või rahvarahutused; tulekahju või plahvatus; katastroofiline epideemia; kaubandusembargo; piirangud või takistused (sealhulgas, kuid mitte ainult, ekspordikontroll); telekommunikatsiooni kättesaadavuse või terviklikkuse puudumine; juriidiline sund, sealhulgas pädeva kohtu otsused, mille suhtes QTSP on või võib olla allutatud; ja mis tahes sündmus või sündmus või asjaolu või asjaolude kogum, mis ei ole QTSP kontrolli all.

Kui mõni vastutuse piiramise või garantii välistamise säte tunnistatakse kohaldatava õiguse alusel kehtetuks, ebaseaduslikuks või jõustamatuks, jäävad ülejäänud sätted täielikult kehtima.

2.9 Kohaldatavad lepingud (sertifitseerimispoliitikad/CPS/kasutustingimused)

[ZE CPS-ID1-ROOT-CA]	Certification Practice Statement for the Root CA for ID-1 Documents of the Republic of Estonia Avaldatud: https://repository.eidpki.ee/repository/
[ZE CPS-ID1-EID-CA]	Certification Practice Statement for the Intermediate CAs for ID-1 Documents of the Republic of Estonia Avaldatud: https://repository.eidpki.ee/repository/
[ZE PDS-ID1]	Zetes Estonia OÜ – PKI Disclosure Statement for Subscriber Certificates for ID-1 documents of the Republic of Estonia Avaldatud: https://repository.eidpki.ee/repository/
[ZE PROFILES]	Technical profile of certificates, OCSP responses and CRLs Avaldatud: https://repository.eidpki.ee/repository/
[ZE TSPS-ID1]	Trust Services Practice Statement for the ID-1 Documents of the Republic of Estonia Avaldatud: https://repository.eidpki.ee/repository/
[ZE TC-ID1-SUB]	Zetes Estonia OÜ poolt Eesti Vabariigi ID-1 formaadis isikut tõendavate dokumentide jaoks väljaantud sertifikaatide kasutustingimused. Avaldatud: https://repository.eidpki.ee/repository/
[ZE TC-ID1]	Eesti Vabariigi ID-1 formaadis isikut tõendavate dokumentide jaoks väljaantud sertifikaatidega seotud CRL-, OCSP-, LDAP- ja muude teenuste kasutajaleping ning tingimused Avaldatud: https://repository.eidpki.ee/repository/
[PPA CP-ID1-EID-CA]	Certificate Policy for ID-1 format identity documents of the Republic of Estonia (eID CP) (eID CP), OI: 1.3.6.1.4.1.51361.2 (PPA) ja OI: 1.3.6.1.4.1.51455.2 (VM) Avaldatud: https://www.id.ee
[PPA CP-ID1-ROOT-CA]	Certificate Policy for the root Certification Authority of the Republic of Estonia (Root CP) OI: 1.3.6.1.4.1.51361.3 Avaldatud: https://www.id.ee

2.10 Privaatsuseeskiri

QTSP on andmetöötleja. Andmete omanik on PPA või VM olenevalt dokumendiliigist.

Järgnev on väljavõte [ZE CPS-ID1-EID-CA] punktist 9.4 „Isikuandmete kaitse“.

Kvalifitseeritud usaldusteenuse osutaja ei avalda ega ole kohustatud avaldama konfidentsiaalset teavet ilma autentse ja põhjendatud taotluseta.

Kvalifitseeritud usaldusteenuse osutaja kohustused:

- isikuandmete töötlemisel järgida [EL 2016/679 IKÜM] ning [EST EUTS] nõudeid, kuna need viitavad andmetöötlejale;
- kohelda kõiki isikuandmeid konfidentsiaalsena, kui tellija ei otsusta teisiti;
- rakendama piisavaid tehnilisi ja korralduslikke meetmeid, mis tagavad isikuandmete töötlemise turvalisuse kooskõlas [EL 679/2016 IKÜM] ja [EST EUTS].

Kvalifitseeritud usaldusteenuse osutaja tagab, et:

- tehnilised ja organisatsioonilised meetmed pakuvad asjakohast kaitset, mis on proportsionaalne riskidega, mis on seotud isikuandmete juhusliku või volitamata hävitamise, kaotamise, muutmise või juurdepääsuga või mis tahes muu isikuandmete volitamata töötlemisega;
- töötajatel on juurdepääs isikuandmetele ainult niivõrd, kuivõrd see on vajalik nende ülesannete täitmiseks;
- isikuandmete töötlemisega tegelev personal on nõuetekohaselt teavitatud [EST IKS] kohaldatavatest kohustustest ja nende siinsetest kohustustest.

Sertifikaadi taotlemise protsessi käigus esitatakse tellijale teatisena tellija leping ja tingimused [ZE TC-ID1-SUB] ning tellija väljendab nõusolekut oma isikuandmete kasutamise kohta, valides sertifikaatide lisamise dokumendile vastavalt [EL 679/2016 IKÜM], [EST ITDS] ja [EST EUTS].

QTSP rakendab andmetöötlejana piisavad tehnilised ja korralduslikud meetmed, mis tagavad isikuandmete töötlemise turvalisuse kooskõlas [EL 679/2016 IKÜM] ja [EST EUTS].

Sertifikaati kodeeritud isikuandmed loetakse privaatseks teabeks, kui neid töötlevad kvalifitseeritud usaldusteenuse osutaja, registreerijad ja registreerija rollis tegutsevad alltöövõtjad ning kaarditootja. Sertifikaadid on siiski mõeldud avalikuks kasutamiseks kas allkirja andmestruktuuri osana, tuvastamise andmestruktuuri osana või krüpteerimise eesmärgil avalikustatud LDAP-hoidlas. OCSP kasutusteavet, mis on seotud tellija sertifikaadiga, peetakse privaatseks teabeks.

LDAP-teenuses avaldatud sertifikaate ja nende nähtavat sisu ei peeta privaatseks.

CRL-teenuse ja OCSP-teenuse kaudu avaldatud sertifikaadi staatuse teave ei ole konfidentsiaalne.

2.11 Hüvitamine

Sertifikaadid antakse tellijatele kaudselt Eesti Vabariigi poolt välja antud dokumentide lahutamatu osana. QTSP ei anna tellijatele sertifikaatide eest tagasimakseid. Tellija võib taotleda PPA-lt või VM-ilt oma dokumendi eest tagasimakset.

Järgnevalt on esitatud väljavõte [ZE CPS-ID1-EID-CA] punktist 9.1 Tasud.

- Tellija sertifikaatide väljaandmise tasu sisaldub dokumendi taotluse läbivaatamise tasus kooskõlas [EST RLS]-iga. Diplomaatilise isikutunnistuse tellija sertifikaatide väljaandmise tasu katab VM vastavalt VM-i ja PPA vahelisele vastastikusele kokkuleppele. Tellija sertifikaatide ja sertifitseerija hierarhia sertifikaatide kasutamine on tasuta.
- Kasutaja saab avalikku LDAP-teenust kasutada tasuta.
- Tellija sertifikaatide kehtetuks tunnistamine on tasuta.
- CRL- ja OCSP-teenus on tasuta.
- Avalike dokumentide digihoidla teenus on tasuta.

Järgnev on väljavõte dokumendi [ZE CPS-ID1-EID-CA] punktist 9.1.5 „Tagasimaksete tingimused“.

Tellijal on õigus taotleda riigilõivu tagastamist või dokumendi taotluse läbivaatamist vastavalt [EST RLS].

2.12 Kohaldatav õigus

QTSP on reguleeritud Euroopa Liidu ja Eesti Vabariigi õigusaktidega.

Euroopa Liidu õigusaktid:

[EL 910/2014 EIDAS] 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 – muudetud määrusega (EL) 2024/1183
Avaldatud https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018

[EL 679/2016 IKÜM] 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)
Avaldatud: http://data.europa.eu/eli/reg/2016/679/oj

[EL 765/2008 ACC] Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 765/2008, 9. juuli 2008 , millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 Saadaval aadressil:
http://data.europa.eu/eli/reg/2008/765/2021-07-16

[EL 1025/2012 STND] Euroopa Parlamendi ja nõukogu määrus (EL) nr 1025/2012, 25. oktoober 2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ
Avaldatud: http://data.europa.eu/eli/reg/2012/1025/oj

[EL 1502/2015] Komisjoni rakendusmäärus (EL) 2015/1502, 8. september 2015, millega kehtestatakse e-identimise vahendite usaldusväärsuse 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
Avaldatud: http://data.europa.eu/eli/reg_impl/2015/1502/oj

[EL 650/2016 QSCD] Komisjoni 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:
http://data.europa.eu/eli/dec_impl/2016/650/oj

Eesti Vabariigi õigusaktid:

EST ABISM Automaatse biomeetrilise isikutuvastuse süsteemi andmekogu põhimäärus:
Avaldatud: https://www.riigiteataja.ee/akt/103102023017?leiaKehtiv

EST ARHS Arhiiviseadus.
Avaldatud: https://www.riigiteataja.ee/akt/113032019033?leiaKehtiv

EST KONS Konsulaarseadus, RT I 2009, 29, 175.
Avaldatud: https://www.riigiteataja.ee/akt/126062025011?leiaKehtiv

EST KÜTS Küberturvalisuse seadus.
Avaldatud: https://www.riigiteataja.ee/akt/130122025015?leiaKehtiv

EST DITM Diplomaatilise isikutunnistuse väljaandmise ja kehtetuks tunnistamise kord, vorm, tehniline kirjeldus ja diplomaatilisele isikutunnistusele kantavate andmete loetelu ning tulumaksust vabastatud mitteresidentide registreerimise kord
Avaldatud: https://www.riigiteataja.ee/akt/101022022008?leiaKehtiv

EST EUTS E-identimise ja e-tehingute usaldusteenuste seadus, RT I, 25.10.2016, 1:
https://www.riigiteataja.ee/akt/130122025016?leiaKehtiv

EST E-ITS Eesti infoturbestandard
Saadaval aadressil: https://eits.ria.ee

EST HOS Hädaolukorra seadus, RT I, 03.03.2017, 1.
Avaldatud: https://www.riigiteataja.ee/akt/130122025019?leiaKehtiv

EST RLS Riigilõivuseadus.
Avaldatud: https://www.riigiteataja.ee/akt/130122014001?leiaKehtiv

EST ITDS Isikut tõendavate dokumentide seadus, RT I, 03.03.2017, 365.
Avaldatud: https://www.riigiteataja.ee/akt/126062025006?leiaKehtiv

EST ITDAM Isikut tõendavate dokumentide andmekogu pidamise põhimäärus:
Avaldatud: https://riigiteataja.ee/akt/122122015045?leiaKehtiv

EST IKS	Isikuandmete kaitse seadus, RT I, 03.03.2017, 11.: Avaldatud: https://www.riigiteataja.ee/akt/106032026010?leiaKehtiv
EST TISKM	Dokumendi taotleja isiku tuvastamise ja isikusamasuse kontrollimise kord. Avaldatud: https://www.riigiteataja.ee/akt/126082022002?leiaKehtiv
EST VEISM	Välisriikide ja rahvusvaheliste organisatsioonide esinduste, rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonide ning nende isikkoosseisu andmekogu põhimäärus: https://www.riigiteataja.ee/akt/118082017002?leiaKehtiv
EST TsÜS	Tsiviilseadustiku üldosa seadus. Avaldatud: https://www.riigiteataja.ee/akt/131122024048?leiaKehtiv

2.13 Kaebused

Kõik kaebused, mis on seotud kasutaja sertifikaatide ja nendega seotud teenustega, nagu sertifikaadi valideerimine (OCSP või CRL) ning LDAP-sertifikaatide hoidlas, võib saata e-posti aadressil <tc_cps_tsps@ee.zetes.com>. Kõik kaebused lahendatakse kooskõlas Eesti õigusega.

Dokumendi taotlemise protsessi või dokumendi endaga seotud kaebused tuleb esitada PPA-le või VM-ile. E-post ppa@politsei.ee või vminfo@mfa.ee

Digidoci tarkvara puudutavad kaebused tuleb saata Riigi Infosüsteemi Ametile (RIA). E-post: help@ria.ee

2.14 Vaidluste lahendamine

Kõik vaidlused lahendatakse kooskõlas Eesti õigusaktidega.

Kui pooled ei ole teisiti kokku leppinud, toimub vahekohtumenetlus Eesti Vabariigis.

2.15 Hoidla kasutuslitsentsid, usaldusmärgised ja auditeerimine

2.15.1 Auditid

Järgnevalt on esitatud väljavõte [ZE CPS-ID1-EID-CA] punktist 8. Vastavusaudit ja muud hindamised.

Üldiselt kohaldab QTSP Euroopa tehnilistes standardites ETSI EN 319 401, ETSI EN 319 411-1 ja ETSI EN 319411-2 sätestatud poliitika- ja turvanõudeid sertifikaate väljastavatele usaldusteenuse pakkujatele. Sertifikaadid, CRL ja OCSP teenused järgivad IETF RFC 6818, RFC 5280 ja RFC 8399.

QTSP tegutseb vastavalt eIDASi määruse [EL 910/2014 EIDAS] tingimustele, mis sätestab usaldusteenuste õigusraamistiku Euroopa Liidus. QTSP kavandab vastavusauditeid ja muid hindamisi, et tagada vastavus õiguslikele ja tehnilistele nõuetele, tavadele ja teenustasanditele vastavalt kohaldatavale tegevusjuhendile.

PKI osalejad, kes täidavad sertifitseerija, registreerija ja kaarditootja rolli, osalevad kõik eIDASi auditites oma vastavate rollide osas.

Akrediteeritud vastavushindamisasutus auditeerib eIDASi määruse [EL 910/2014 EIDAS] järgimist vähemalt kord iga kahe aasta tagant või iga kord, kui usaldusteenuse toimingutes tehakse olulisi muudatusi.

Eriolukorras (nt turvarikkumine) võib järelevalveasutuse, vastavushindamisasutuse, PPA või poliitikahaldusasutuse taotlusel läbi viia ka plaaniväliseid auditeid ja hindamisi.

QTSP vastavust eIDAS-määrusele [EL 910/2014 EIDAS] auditeerib akrediteeritud vastavushindamisasutus, nagu on määratletud määruse (EÜ) nr 2008/765 artikli 2 punktis 13 ja ETSI EN 319 304 "Elektroonilised allkirjad ja infrastruktuurid (ESI) - usaldusteenuse pakkujate hindamine - Nõuded usaldusteenuse pakkujaid hindavatele vastavushindamisasutustele".

Akrediteeritud vastavushindamisasutus on:

Vastavushindamisasutuse nimi:	LSTI
Vastavushindamisasutuse veebisait:	https://www.lsti-certification.fr/

2.15.2 ELi usaldusnimekiri

Euroopa Komisjon avaldab kõigi ELi riikide usaldusnimekirja eIDASi veebisaidil.

QTSP on loetletud Eesti all sellel URL-il: https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls/tl/EE.

2.15.3 Eesti Vabariigi usaldusnimekiri

RIA on Eesti Vabariigi eIDASi järelevalveasutus ja avaldab Eesti usaldusnimekirja aadressil: https://sr.riik.ee/en/trusted-list.

APPENDIX A - VIITED

Järgnevalt on esitatud väljavõte [ZE TSPS-ID1] lisast A:

A.1 EUROOPA ÕIGUSAKTID

[EL 910/2014 EIDAS] 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 - muudetud määrusega (EL) 2024/1183.
Avaldatud https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018

[EL 679/2016 IKÜM] 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)
Avaldatud: http://data.europa.eu/eli/reg/2016/679/oj

[EL 765/2008 ACC] Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 765/2008, 9. juuli 2008 , millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93. Avaldatud:
http://data.europa.eu/eli/reg/2008/765/2021-07-16

[EL 1025/2012 STND] Euroopa Parlamendi ja nõukogu määrus (EL) nr 1025/2012, 25. oktoober 2012 , mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ EMPs kohaldatav tekst.
Avaldatud: http://data.europa.eu/eli/reg/2012/1025/oj

[EL 1502/2015] Komisjoni rakendusmäärus (EL) 2015/1502, 8. september 2015, millega kehtestatakse e-identimise vahendite usaldusväärsuse 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.
Avaldatud: http://data.europa.eu/eli/reg_impl/2015/1502/oj

[EL 650/2016 QSCD] Komisjoni 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:
http://data.europa.eu/eli/dec_impl/2016/650/oj

A.2 EESTI VABARIIGI ÕIGUSAKTID

EST ABISM Automaatse biomeetrilise isikutuvastuse süsteemi andmekogu põhimäärus:
Avaldatud: https://www.riigiteataja.ee/akt/103102023017?leiaKehtiv

EST ARHS Arhiiviseadus.
Avaldatud: https://www.riigiteataja.ee/akt/113032019033?leiaKehtiv

EST KONS Konsulaarseadus, RT I 2009, 29, 175.
Avaldatud: https://www.riigiteataja.ee/akt/126062025011?leiaKehtiv

EST KÜTS Küberturvalisuse seadus.
Avaldatud: https://www.riigiteataja.ee/akt/130122025015?leiaKehtiv

EST DITM Diplomaatilise isikutunnistuse väljaandmise ja kehtetuks tunnistamise kord, vorm, tehniline kirjeldus ja diplomaatilisele isikutunnistusele kantavate andmete loetelu ning tulumaksust vabastatud mitteresidentide registreerimise kord
Avaldatud: https://www.riigiteataja.ee/akt/101022022008?leiaKehtiv

EST EUTS	E-identimise ja e-tehingute usaldusteenuste seadus, RT I, 25.10.2016, 1: https://www.riigiteataja.ee/akt/130122025016?leiaKehtiv
EST E-ITS	Eesti infoturbestandard Saadaval aadressil: https://eits.ria.ee
EST HOS	Hädaolukorra seadus, RT I, 03.03.2017, 1. Avaldatud: https://www.riigiteataja.ee/akt/130122025019?leiaKehtiv
EST RLS	Riigilõivuseadus. Avaldatud: https://www.riigiteataja.ee/akt/130122014001?leiaKehtiv
EST ITDS	Isikut tõendavate dokumentide seadus, RT I, 03.03.2017, 365. Avaldatud: https://www.riigiteataja.ee/akt/126062025006?leiaKehtiv
EST ITDAM	Isikut tõendavate dokumentide andmekogu pidamise põhimäärus: Avaldatud: https://riigiteataja.ee/akt/122122015045?leiaKehtiv
EST IKS	Isikuandmete kaitse seadus, RT I, 03.03.2017, 11.: Avaldatud: https://www.riigiteataja.ee/akt/106032026010?leiaKehtiv
EST TISKM	Dokumendi taotleja isiku tuvastamise ja isikusamasuse kontrollimise kord. Avaldatud: https://www.riigiteataja.ee/akt/126082022002?leiaKehtiv
EST VEISM	Välisriikide ja rahvusvaheliste organisatsioonide esinduste, rahvusvaheliste organisatsioonide ja rahvusvahelise kokkuleppega loodud institutsioonide ning nende isikkoosseisu andmekogu põhimäärus: https://www.riigiteataja.ee/akt/118082017002?leiaKehtiv
EST TsÜS	Tsiviilseadustiku üldosa seadus. Avaldatud: https://www.riigiteataja.ee/akt/131122024048?leiaKehtiv

A.3 ZETES ESTONIA OÜ DOKUMENDID

[ZE CPS-ID1-ROOT-CA]	Certification Practice Statement for the Root CA for ID-1 Documents of the Republic of Estonia Avaldatud: https://repository.eidpki.ee/repository/
[ZE CPS-ID1-EID-CA]	Certification Practice Statement for the Intermediate CAs for ID-1 Documents of the Republic of Estonia Avaldatud: https://repository.eidpki.ee/repository/
[ZE PDS-ID1]	Zetes Estonia OÜ – PKI Disclosure Statement for Subscriber Certificates for ID-1 documents of the Republic of Estonia Avaldatud: https://repository.eidpki.ee/repository/
[ZE PROFILES]	Technical profile of certificates, OCSP responses and CRLs Avaldatud: https://repository.eidpki.ee/repository/
[ZE TSPS-ID1]	Trust Services Practice Statement for the ID-1 Documents of the Republic of Estonia Avaldatud: https://repository.eidpki.ee/repository/
[ZE TC-ID1-SUB]	Zetes Estonia OÜ poolt Eesti Vabariigi ID-1 formaadis isikut tõendavate dokumentide jaoks väljaantud sertifikaatide kasutustingimused. Avaldatud: https://repository.eidpki.ee/repository/
[ZE TC-ID1]	Eesti Vabariigi ID-1 formaadis isikut tõendavate dokumentide jaoks väljaantud sertifikaatidega seotud CRL-, OCSP-, LDAP- ja muude teenuste kasutajaleping ning tingimused Avaldatud: https://repository.eidpki.ee/repository/

A.4 PPA DOKUMENDID

[PPA CP-ID1-EID-CA]	Certificate Policy for ID-1 format identity documents of the Republic of Estonia (eID CP) (eID CP), OI: 1.3.6.1.4.1.51361.2 (PPA) ja OI: 1.3.6.1.4.1.51455.2 (VM) Avaldatud: https://www.id.ee

[PPA CP-ID1-ROOT-CA] Certificate Policy for the root Certification Authority of the Republic of Estonia (Root CP)
OI: 1.3.6.1.4.1.51361.3
Avaldatud: https://www.id.ee

A.5 ETSI/CEN/CENELEC STANDARDID

[ETSI TS 119 615] ETSI TS 119 615 "Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists"

[ETSI TS 119 172-4] ETSI TS 119 119 172-4: "Signature policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists"

[ETSI EN 319 401] ETSI EN 319 401 "General Policy Requirements for Trust Service Providers"

[ETSI EN 319 403] ETSI EN 319 403 "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers."
Published: https://www.etsi.org/

[ETSI EN 319 411-1] ETSI EN 319 411-1 "Policy and Security Requirements for Trust Service Providers issuing Certificates; Part 1: General requirements"

[ETSI EN 319 411-2] ETSI 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"

Published: https://www.etsi.org/

[ETSI EN 319 412-1] ETSI EN 319 412-1 "Certificate Profiles; Part 1: Overview and common data structures"

Published: https://www.etsi.org/

[ETSI EN 319 412-2] ETSI EN 319 412-2 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for Certificates issued to natural persons. "
Published: https://www.etsi.org/

[CEN EN 419 211] CEN EN 419 211 Protection profiles for secure signature creation device.
Published: https://www.cencenelec.eu/

[CENELEC EN 50600] 50600-1:2019 Information technology - Data centre facilities and infrastructures

Published: https://www.cencenelec.eu/

A.6 ISO/IEC AND NATO STANDARDID

[ISO 9001] ISO/IEC 9001 Quality management systems– Requirements
Published: https://www.iso.org

[ISO 14001] ISO/IEC 14001 Environmental management systems
Published: https://www.iso.org

[ISO 20000] ISO/IEC 20000 Information technology — Service management
Published: https://www.iso.org

[ISO 27001] ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements
Published: https://www.iso.org

[ISO 17065] ISO/IEC 17065 Conformity assessment — Requirements for bodies certifying products, processes and services
Published: https://www.iso.org

[AQAP 2110] NATO AQAP 2110 NATO Quality Assurance Requirements for design, development and production
Published: https://nso.nato.int

A.7 IETF - RFC

[IETF RFC 3647] Internet Engineering Task Force RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”
Published: https://www.rfc-editor.org/rfc/rfc3647.html

[IETC RFC 5280] Internet Engineering Task Force RFC 5280 “X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile” https://www.rfc-editor.org/rfc/rfc5280.html

[IETF RFC 6960] Internet Engineering Task Force RFC 6960 “X.509 Public Key Infrastructure - Online Certificate Status Protocol – OCSP”
Published: https://www.rfc-editor.org/rfc/rfc6960.html

[IETF RFC 5480] Internet Engineering Task Force RFC 5480 “Elliptic Curve Cryptography Subject Public Key Information”
Published: https://www.rfc-editor.org/rfc/rfc5480.html

[IETF RFC 5639] Internet Engineering Task Force RFC 5639 “Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation”
Published: https://www.rfc-editor.org/rfc/rfc5639.html

---------- Käesoleva dokumendi viimane lehekülg ----------