

Pealkiri:	Zetes Estonia OÜ – Zetes Estonia OÜ poolt Eesti Vabariigi ID-1 formaadis isikut tõendavate dokumentide jaoks väljaantud sertifikaatide kasutustingimused
Märgistus:	[ZE TC-ID1-SUB]
Dokumendi OI:	[1.3.6.1.4.1.47718.3.14].01
Kategooria:	Kasutustingimused
Versioon:	1.3
Staatust:	Kinnitatud
Kehtiv alates:	20.10.2025
Organisatsioon:	Zetes Estonia OÜ
Klassifikatsioon	AVALIK
Autoriõigus: © 2025 Zetes Estonia OÜ – Kõik õigused kaitstud. Selle dokumendi või selle sisu mis tahes osa ei tohi reprodutseerida, kopeerida, muuta ega kohandada ilma autori eelneva kirjaliku nõusolekuta, kui eraldi materjalide puhul ei ole märgitud teisiti. Dokumendi sisu kommertskasutus ja levitamine on keelatud ilma autori sõnaselge ja eelneva kirjaliku nõusolekuta.	

Sisukord

1	SERTIFIKAAT JA ID1-DOKUMENT	3
1.2	Sertifikaadid, dokumendi kasutajad, subjektid ja tellijad	3
1.3	Mis on dokumendi ja sertifikaatide vaheline seos?	3
1.4	Milline on Zetes Estonia OÜ roll?	3
1.5	Kasutustingimused.....	4
1.6	Avaliku võtme taristu avalikustamise avaldusest	4
2	KASUTUSTINGIMUSED	5
2.1	Üldtingimused.....	5
2.2	Kohaldatavad õigusaktid.....	5
2.2.1	Eesti õigusaktid.....	5
2.2.2	ELi õigusaktid.....	6
2.3	Sertifikaadi aktsepteerimine	6
2.3.1	Sertifikaadi aktsepteerimine osana tavapärasest dokumendi aktsepteerimise protseduurist	6
2.3.2	Sertifikaadi aktsepteerimine osana olemasolevate dokumentide võtmete asendamise protsessist	6
2.3.3	Uue dokumendi sertifikaadi kehtetuks tunnistamine	7
2.4	Sertifikaadi kehtetuks tunnistamine	7
2.5	Sertifikaadi kasutamine	7
2.5.1	Võtme ja sertifikaadi lubatud kasutamine.....	7
2.5.2	Võtme ja sertifikaadi keelatud kasutamine	8
2.6	Sertifikaatide tasud tellijale	8
2.7	Hüvitamine	8
2.8	Tuginemise piirangud.....	8
2.9	Muud tellija õigused ja kohustused.....	9
2.10	Muud ZE õigused ja kohustused.....	9
2.11	Sertifikaadi staatuse kontrollimise kohustused tellijatele ja tuginevatele pooltele.....	10
2.12	Sertifikaadi staatuse teenused	10
	CRL.....	10
	OCSP	10
2.13	Piiratud garantii ja vastutuse välistamine	11
2.14	Väärramatu jõud	11
2.15	Kohaldatav õigus.....	11
2.16	Kontaktandmed	11
2.17	Kaebused ja vaidluste lahendamine	11
2.18	Kohaldatavad lepingud, sertifitseerimispõhimõtted ja sertifitseerimispoliitika	12
2.19	Isikuandmete privaatsus	12
2.19.1	Privaatsuseeskiri.....	12
2.19.2	Privaatsena käsitletav teave.....	13
2.19.3	Teave, mida ei käsitleta privaatsena	13
2.19.4	Teatis ja nõusolek isikuandmete kasutamiseks	13
2.19.5	Säilitamisaeg.....	13
2.19.6	Avalikustamine kohtu- või haldusmenetluse raames.....	14
2.19.7	Muud teabe avalikustamise asjaolud	14
3	SERTIFIKAATE SISALDAVATE DOKUMENTIDE LOETELU	15

Dokumendi ajalugu

Versioon	Muudatused
1.3	Dokumendi sisu pole võrreldes versiooniga 1.2 muutunud. Tegemist on esimese tootmisotstarbel kasutatava versiooniga, mis jõustub sertifikaatide avaliku väljastamisega. Versioon on PMA poolt heaks kiidetud ja märgistatud sildiga „AVALIK“.
1.2	Ainult asutusesiseseks kasutamiseks eeltootmise kontekstis. Asutusesisese läbivaatamise versioon. Muudatused viiakse dokumenti sisse pärast täiendavat kontrolli. Kontaktides uuendatud e-posti aadressi. Lisatud piirang, et ühe OCSP-päringu kohta võib kasutada ainult ühte sertifikaadi seerianumbrit.
1.1	Ainult asutusesiseseks kasutamiseks eeltootmise kontekstis. Asutusesisese läbivaatamise versioon. Vaadata läbi pärast 2025. aasta juuni auditeerimist. Lisatud peatükk 2.19.5, mis sisaldab teavet andmete säilitamise tähtaegade kohta.
1.0	Ainult asutusesiseseks kasutamiseks eeltootmise kontekstis. Asutusesisese läbivaatamise versioon. Esialgse auditi jaoks heakskiidetud versioon.

1 SERTIFIKAAT JA ID1-DOKUMENT

1.1 Mis on minu isiklik „dokument“?

ID-1 formaadis isikut tõendavad dokumendid (edaspidi „dokumendid“) on Eesti Vabariigi poolt väljaantud isikut tõendavad dokumendid (nt ID-kaart, elamisloakaart, e-residendi digi-ID või diplomaatiline isikutunnistus).

Dokument sisaldab turvakiipi, mida saab kasutada arvutirakendustes, nagu enamik veebibrausereid, DigiDoc, Adobe Reader jt. Kiipi saab kasutada brauseriga, et sisse logida sellistesse veebiteenustesse nagu eesti.ee, pankade veebisaitidele jne, samuti elektrooniliste dokumentide krüpteerimiseks ja/või allkirjastamiseks. DigiDociga saab allkirjastada ja krüpteerida erinevaid failivorminguid.

1.2 Sertifikaadid, dokumendi kasutajad, subjektid ja tellijad

Dokumendi kasutaja on isik (teie), kes on dokumendi Eesti Vabariigilt saanud.

Sertifikaadid seovad dokumendi kasutaja unikaalse identiteedi krüptograafiliste võtmetega, mida dokumendis olev kiip kasutab dokumendi kasutaja nimel isiku tuvastamisel, krüpteerimisel või allkirjastamisel.

Kuna dokumendi kasutaja saab need sertifikaadid oma dokumendi kiibile, loetakse dokumendi kasutaja sertifikaadi väljaandmise ja elutsükli haldamise teenuste kasutajaks. Sel põhjusel nimetatakse dokumendi kasutajat sertifikaatide kontekstis tavaliselt subjektiks või tellijaks, samas kui terminit „dokumendi kasutaja“ kasutatakse dokumentide kontekstis.

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

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

Sertifikaat seob subjekti identiteedi (nimi, isikukood jne) unikaalse krüptograafilise võtmega, mis on loodud Politsei- ja Piirivalveameti (PPA) või Välisministeeriumi (VM) väljaantud dokumendi kiibis. Mõlemad valitsusasutused mängivad olulist rolli subjekti isiku tuvastamisel ning subjektile sertifikaatidega dokumendi väljaandmise otsuse tegemisel. Need valitsusasutused ja nende alltöövõtjad vastutavad täielikult dokumentide väljaandmise ja elutsükli haldamise eest.

1.3 Mis on dokumendi ja sertifikaatide vaheline seos?

Dokumentide ja sertifikaatide elutsüklid on tihedalt seotud.

- Sertifikaat kehtib sama kaua kui sertifikaadiga seotud dokument.
- Kui dokumendi kasutaja vajab mingil põhjusel uut dokumenti, luuakse uue dokumendi jaoks uued sertifikaadid.
- Kui dokumendi kasutaja sureb, tunnistatakse sertifikaadid dokumendi kuritarvitamise vältimiseks kehtetuks.
- Kui dokumendi kasutaja isikuandmed muutuvad, tunnistatakse kehtivad sertifikaadid kehtetuks ja isik saab uue dokumendi uute sertifikaatidega, mis kajastavad tema uusi isikuandmeid.

1.4 Milline on Zetes Estonia OÜ roll?

Kuigi dokumente annavad välja PPA ning VM, loob isiklikud sertifikaadid nendel dokumentidel eraettevõtte Zetes Estonia OÜ (ZE), kes täidab kvalifitseeritud usaldusteenuse osutaja rolli. ZE registreeris kvalifitseeritud usaldusteenuse osutajana Riigi Infosüsteemi Amet (RIA), kes täidab Eesti Vabariigi järelevalveasutuse rolli. Kvalifitseeritud usaldusteenuse osutaja vastutab sertifikaatide loomise ja sertifikaatide elutsükli staatuse (peatatud, aktiivne või kehtetuks tunnistatud) haldamise eest.

ZE kui kvalifitseeritud usaldusteenuse osutaja tegutseb Eesti Vabariigi ja Euroopa Liidu õigusaktide alusel, eelkõige usaldusteenuste osutajaid reguleeriva eIDAS määruse alusel. Dokumendi lõpus on esitatud

kohaldatavate õigusaktide loetelu. ZE on PPA-ga sõlminud lepingu dokumentidele sertifikaatide väljaandmiseks. Kuna sertifikaadid on mõeldud kasutamiseks ainult Eesti Vabariigi poolt väljaantud dokumentidega, järgib kvalifitseeritud usaldusteenuse osutaja PPA sertifitseerimispoliitikat.

ZE kui kvalifitseeritud usaldusteenuse osutaja pakub avalikke teenuseid, mida saate kasutada:

- CRL ja OCSP, et kontrollida enda ja teiste sertifikaatide sertifikaadi staatuse teavet,
- veebileht sertifikaatide kehtetuks tunnistamise taotlemiseks,
- LDAP-kataloogiteenus teiste sertifikaatide leidmiseks.

1.5 Kasutustingimused

Dokumendi „**Kasutustingimused**“ viide on [ZE TC-ID1-SUB]. See on kättesaadav tellijatele ZE poolt Eesti Vabariigis väljaantud dokumentide sertifikaatide kontekstis.

1.6 Avaliku võtme taristu avalikustamise avaldusest

Tellijal soovitatakse lugeda dokumenti „**Avaliku võtme taristu avalikustamisavaldus**“ [ZE PDS-ID1]. See sisaldab lihtsustatud kokkuvõtet sertifitseerimispõhimõtetest, mis on põhjalik avalik dokument, milles kirjeldatakse üksikasjalikult kvalifitseeritud usaldusteenuse osutaja ja teiste poolte poolt sertifikaatide väljaandmisel rakendatavaid tavasid dokumentide väljaandmise osana ning esitatakse ka üksikasjalikum teave tellijate ja tuginevate poolte õiguste ja kohustuste kohta.

2 KASUTUSTINGIMUSED

Dokumendi asjakohane versioon on viimane versioon, mis on kättesaadav veebiaadressil www.id.ee/kasutustingimused dokumendi taotlemise kuupäeval. Teenindustes võivad asuda dokumendi trükitud versioonid, kuid need ei asenda, tühistata ega tunnista muul viisil kehtetuks veebis avaldatud versiooni.

2.1 Üldtingimused

Tellijal nõustub, et ZE peab järgima Eesti õigusakte, eelkõige peatükis 2.2 loetletut.

Tellijal nõustub, et sertifikaadid on Eesti Vabariigi poolt väljaantud dokumentide lahutamatu osa ning nõustub sertifikaate sisaldava dokumendi eeskirjade ja tingimustega.

Tellijal nõustub, et dokumendi väljaandja (PPA või VM) reguleerib kõiki isikute tuvastamise, sertifikaate sisaldava dokumendi taotlemise ning nimetatud dokumendi ja sertifikaatide väljaandmise menetlustega seotud aspekte olenevalt dokumendi liigist.

Tellijal nõustub, et sertifikaatide kasutamine reguleeritakse siinses dokumendis ja ZE sertifitseerimisprotsessides [ZE CPS-ID1-EID-CA] sätestatud kasutustingimustega.

ZE-l on õigus muuta teenuste seaduslikkuse, turvalisuse, järjepidevuse, kvaliteedi ja terviklikkuse tagamise tingimusi.

2.2 Kohaldatavad õigusaktid

2.2.1 Eesti õigusaktid

EST DITM	Diplomaatilise isikutunnistuse väljaandmise ja kehtetuks tunnistamise kord, vorm, tehniline kirjeldus ja diplomaatilisele isikutunnistusele kantavate andmete loetelu ning tulumaksust vabastatud mitteresidentide registreerimise kord Saadaval aadressil: https://www.riigiteataja.ee/akt/101022022008?leiaKehtiv
EST EUTS	E-identimise ja e-tehingute usaldusteenuste seadus, RT I, 25.10.2016, 1 Saadaval aadressil: https://www.riigiteataja.ee/akt/130122024006?leiaKehtiv
EST HOS	Hädaolukorra seadus, RT I, 03.03.2017, 1. Saadaval aadressil: https://www.riigiteataja.ee/akt/128122017049?leiaKehtiv
EST RLS	Riigilõivuseadus. Saadaval aadressil: https://www.riigiteataja.ee/akt/131122015037?leiaKehtiv
EST ITDS	Isikut tõendavate dokumentide seadus, RT I, 03.03.2017, 365. Saadaval aadressil: https://www.riigiteataja.ee/akt/126062025003?leiaKehtiv
EST IKS	Isikuandmete kaitse seadus, RT I, 03.03.2017, 11. Saadaval aadressil: https://www.riigiteataja.ee/akt/104012019011?leiaKehtiv
EST TISKM	Dokumendi taotleja isiku tuvastamise ja isikusamasuse kontrollimise kord Saadaval aadressil: https://www.riigiteataja.ee/akt/102072025013?leiaKehtiv
EST IDLM	Isikutunnistuse, elamisloakaardi, digitaalse isikutunnistuse, Eesti kodaniku passi, meremehe teenistusraamatu, välismaalase passi, ajutise reisidokumendi, pagulase reisidokumendi või meresõidutunnistuse väljaandmise taotlemisel esitatavate tõendite ja andmete loetelu, väljastamise kord ning väljaandmise tähtsajad Saadaval aadressil: https://www.riigiteataja.ee/akt/129072025002?leiaKehtiv

2.2.2 Eli õigusaktid

**Määrus (EL) nr
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

Saadaval aadressil: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32014R0910>

**Määrus (EL) 2016/679
(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)

Saadaval aadressil: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32016R0679>

**Rakendusmäärus (EL)
2015/1502**

Komisjoni rakendusmäärus (EL) 2015/1502, 8. september 2015, millega kehtestatakse e-identimise vahendite usaldusvärsuse 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

Saadaval aadressil: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32015R1502>

2.3 Sertifikaadi aktsepteerimine

2.3.1 Sertifikaadi aktsepteerimine osana tavapärasest dokumendi aktsepteerimise protseduurist

Sertifikaadi aktsepteerimise protsess on dokumentide aktsepteerimise protsessi lahutamatu osa.

Tellijal loetakse sertifikaatide loomisega nõustunuks, kui ta on sõnaselgelt taotlenud sertifikaate sisaldavat dokumenti.

Sertifikaadid luuakse peatatud olekus ning muudetakse aktiivseks osana dokumendi ja sertifikaadi aktsepteerimise protseduurist.

Tellijal peab enne dokumendi ja sertifikaatide vastuvõtmist kontrollima, kas dokumendis olevad nimed ja isikukood on õiged.

Tellijal kinnitab sertifikaatide sisu aktsepteerimist ja õigsust, allkirjastades aktsepteerimisklausli dokumendi kandjal või muul viisil aktsepteerimist väljendades ja sertifikaate sisaldava dokumendi omandades.

2.3.2 Sertifikaadi aktsepteerimine osana olemasolevate dokumentide võtmete asendamise protsessist

Sertifikaadi aktsepteerimise protsess on uute võtmete loomise protsessi lahutamatu osa. Võtme asendamine on erakorraline protseduur, mille käigus asendatakse olemasolevate dokumentide võtmed ja sertifikaadid.

Olemasolevate dokumentide võtmete asendamise raames väljaantud sertifikaatidel on sama tellija teave kui originaalsertifikaatidel ja need antakse välja aktiivses olekus.

Tellijal peab enne võtmete asendamise protsessi alustamist ja sertifikaatide vastuvõtmist kontrollima, kas dokumendis olevad nimed ja isikukood on õiged.

Kui võtme asendamine toimub kaarditootja veebiportaalis, kinnitab tellija sertifikaadi õigsust ja kasutustingimustega [ZE TC-ID1-SUB] nõustumist

- vastava linnukese tegemisega
- dokumendi kiipkaardilugejasse sisestamisega võtme asendamise protsessi ajal.

Kui võtme asendamine toimub teeninduses, kinnitab tellija sertifikaadi õigsust ja kasutustingimustega [ZE TC-

ID1-SUB] nõustumist

- taotluse vormi allkirjastamisega ja
- dokumendi kiipkaardilugejasse sisestamisega võtme asendamise protsessi ajal või dokumendi andmisega teeninduse ametnikule.

2.3.3 Uue dokumendi sertifikaadi kehtetuks tunnistamine

Tellijal võib dokumendi kättesaamisel taotleda sertifikaatide kohest kehtetuks tunnistamist.

2.4 Sertifikaadi kehtetuks tunnistamine

Sertifikaatide kehtetuks tunnistamine ei mõjuta dokumendi kehtivust (välja arvatud e-residendi digi-ID). E-residendi digi-ID puhul kaotab dokument sertifikaatide kehtetuks tunnistamisel kehtivuse.

Pärast sertifikaatide kehtetuks tunnistamist ei saa dokumenti enam kasutada veebipõhiseks tuvastamiseks, krüpteerimiseks ega allkirjastamiseks.

Sertifikaadi kehtetuks tunnistamine on pöördumatu protsess.

Tellijal nõustub, et sertifikaatide kehtetuks tunnistamine võib muuta varem krüpteeritud andmete dekrüpteerimise keeruliseks või võimatuks.

Tellijal nõustub mitte kasutama kehtetuks tunnistatud sertifikaate muul eesmärgil kui varem krüpteeritud andmete dekrüpteerimiseks.

Sertifikaadi kehtetuks tunnistamine ei anna õigust tagasimaksele ega muule hüvitisele või soodustusele. Tellijal võib sertifikaatide kehtetuks tunnistamist taotleda igal ajal.

Tellijal saab taotleda sertifikaatide kehtetuks tunnistamist

- sertifikaatide kehtetuks tunnistamise portaali kaudu aadressil <https://revocation.eidpki.ee>. Tellijal peab end tuvastama ühe meetodi abil järgmistest: dokument, Smart-ID, mobiil-ID või ühekordne parool. ZE ei vastuta tellijal põhjustatud tuvastamise ebaõnnestumise eest ega tellijal võimetuse või soovimatuse eest kasutada mõnda aktsepteeritud tuvastamise vahendit.
- PPA teeninduses või diplomaatilise isikutunnistuse puhul VM-i esinduses.

ZE-l on õigus kehtetuks tunnistada tellijal sertifikaat, kui ta on kohustatud seda tegema PPA või VM-iga sõlmitud lepingulise kohustuse alusel, PPA või VM-i juhisel, seaduse ja konkreetselt määruse (EL) nr 910/2014 alusel või vastavalt sertifitseerimisjuhenditele [ZE CPS-ID1-EID-CA].

Tellijal nõustub, et uute sertifikaatide saamiseks pärast nende kehtetuks tunnistamist on vaja taotleda uus dokument.

Tellijal saab sertifikaatide kehtetuks tunnistamise kohta teate oma ametlikule Eesti e-posti aadressile (isikukood@eesti.ee).

Kõik sellele aadressile saadetud kirjad on võimalik automaatselt edastada isiklikule e-posti kontole.

Tellijal ei ole sertifikaatide õiguspärase kehtetuks tunnistamise puhul õigust tagasimaksetele, kahjuhüvitistele ega muudele hüvitistele.

2.5 Sertifikaadi kasutamine

2.5.1 Võtme ja sertifikaadi lubatud kasutamine

Tellijal peab privaativõtit ja sertifikaate kasutama seaduslikult ning kooskõlas kasutustingimustega [ZE TC-ID1-SUB].

Sertifikaate on keelatud kasutada muul eesmärgil kui järgmised:

- tuvastamise ja krüpteerimise sertifikaat on mõeldud tuvastamiseks ja krüpteerimiseks.

- allkirjastamise sertifikaat on mõeldud kvalifitseeritud digiallkirjade andmiseks.

Dokumentide või tehingute allkirjastamisel allkirjavõtmeiga soovitatakse tellijatel kasutada allkirjastamise lahendust, mis lisab sertifikaadi staatuse allkirja andmestruktuuri, ning kasutada kvalifitseeritud ajatemplit.

Tellijatel soovitatakse kasutada tarkvara DigiDoc allkirjastamise funktsiooni.

2.5.2 Võtme ja sertifikaadi keelatud kasutamine

Aegunud või kehtetuks tunnistatud sertifikaate on keelatud kasutada muul eesmärgil kui krüpteeritud andmete (failid, sõnumid, tehingud jne) dekrüpteerimiseks.

Dokumendi ja selle sertifikaatide kasutamise kontrolli delegeerimine või loovutamine teisele isikule või automatiseeritud süsteemile on keelatud.

Sertifikaati on keelatud kasutada automaatseks allkirjastamiseks.

Allkirjastamise sertifikaati on keelatud kasutada muul eesmärgil kui allkirja andmiseks.

Sertifikaati on keelatud kasutada dokumentide allkirjastamiseks, mis võivad kaasa tuua soovimatuid tagajärgi, või dokumentide allkirjastamiseks testimise eesmärgil.

Sertifikaate on keelatud kasutada mis tahes eesmärgil, mis ei ole sõnaselgelt lubatud, sealhulgas ebaseaduslikuks tegevuseks (sh küberrünnakud ja sertifikaadi või dokumendi rikkumise katsed), teiste sertifikaatide väljaandmiseks jne.

Tuvastamise ja krüpteerimise sertifikaati on keelatud kasutada digiallkirja andmiseks.

Tuvastamise ja krüpteerimise sertifikaati on keelatud kasutada ebaseadusliku tegevusega seotud andmete krüpteerimiseks.

2.5.3 Kohustus kasutada usaldusnimekirja sertifikaadi ja sertifikaadiga antud digiallkirja kehtivuse kontrollimiseks

Tellija peab kasutama vahendeid, mis kinnitavad, et sertifikaadi on välja andnud kvalifitseeritud usaldusteenuse osutaja, kes on loetletud Eesti Vabariigi usaldusnimekirjas või ELi usaldusnimekirjas.

Järgmised URL-id on esitatud ainult mugavuse huvides ja võivad muutuda ilma ette teatamata:

Eesti Vabariigi usaldusnimekiri: <https://sr.riik.ee/en/trusted-list/>

Euroopa Liidu usaldusnimekiri: <https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls>

2.6 Sertifikaatide tasud tellijale

Sertifikaatide tasu on arvestatud dokumendi tasu sisse kooskõlas riigilõivuseadusega (EST RLS) ning diplomaatiliste isikutunnistuste puhul kooskõlas VM-i ja PPA vahelise kokkuleppega.

2.7 Hüvitamine

ZE ei maksa hüvitisi tellijatele väljaantud sertifikaatide eest.

Kõik võimalikud hüvitamise alused tulenevad tellija õigustest, mis on sätestatud riigilõivuseaduses (EST RLS), ja on seotud sertifikaate sisaldava dokumendi hüvitamise eeskirjaga.

Hüvitise taotlused tuleb esitada dokumendi väljaandjale, kas PPA -le või VM-ile, olenevalt dokumendi liigist.

2.8 Tuginemise piirangud

Sertifikaatidel on kehtivusaeg, mis on märgitud sertifikaadis (mitte varasem, mitte hilisem).

Sertifikaat kehtib sama kaua kui dokument, millega sertifikaat on seotud. Sertifikaatidel on staatus, mis võib olla üks järgmistest: aktiivne, peatatud ja kehtetuks tunnistatud.

See, kas sertifikaat kehtib, oleneb nii kehtivusajast kui ka sertifikaadi staatusest.

2.9 Muud tellija õigused ja kohustused

Tellijal soovitatakse dokumendi kättesaamisel valida uus, raskesti äraarvatav PIN-kood, mis asendab algse PIN-koodi. Tellija võib sertifikaatide kehtetuks tunnistamist taotleda igal ajal.

Tellijal on õigus taotleda sertifikaatide kehtetuks tunnistamist põhjust täpsustamata, tingimusel et dokument ja turvakoodid (PIN ja PUK) on endiselt tellija valduses (st pole kadunud, varastatud, kompromiteeritud, kahjustatud jne).

Tellija peab kaitsma dokumenti ja sellega seotud PIN-koode kadumise, varguse, avalikustamise või kompromiteerituse eest.

Tellija peab esitama PPA-le või VM-ile tõese ja täieliku teabe kõigi dokumendi ja sertifikaatidega seotud aspektide kohta.

Tellija peab kooskõlas Eesti õigusaktidega teavitama PPA-d või VM-i ühe kuu jooksul kõikidest muudatustest, mis puudutavad subjekti isikuandmeid ja ametlikku staatust, sealhulgas kodakondsust, elamisõigust, diplomaatilist staatust jne.

Tellija peab viivitamatult teavitama PPA-d või VM-i dokumendi kaotamisest, vargusest, kahjustumisest või hävimisest ning esitama taotluse sertifikaatide kehtetuks tunnistamiseks.

Tellija peab teavitama PPA-d või VM-i dokumendi ja selle sertifikaatide üle kontrolli kaotamise või selle kahtluse korral, sealhulgas turvakoodide teatavaks saamisest kolmandatele isikutele, ning esitama taotluse sertifikaatide kehtetuks tunnistamiseks.

Tellija peab sertifikaatide kasutamise lõpetama, kui talle antakse otse või avalikult teada, et sertifikaate ei tohi enam kasutada.

Tellijal soovitatakse dokumendi kehtivusaja lõppemisel või uue dokumendi väljastamisel eelmise dokumendi kontaktkiip füüsiliselt hävitada, näiteks läbi torgates või lõigates, välja arvatud juhul, kui seadusega on ette nähtud dokumendi tagastamine PPA-le või VM-ile.

Hoiatus: kontaktkiibi hävitamine muudab varem krüpteeritud failide dekrüpteerimise võimatuks.

Tellija ei tohi kasutada aegunud või kehtetuks tunnistatud sertifikaatide võtmeid muul eesmärgil kui krüpteeritud andmete (failid, sõnumid, tehingud jne) dekrüpteerimiseks.

Tellija peab tagama, et kõik tema krüpteeritud andmed dekrüpteeritakse võimalikult kiiresti ja enne dokumendi sertifikaatide aegumist või kehtetuks tunnistamist või enne dokumendi tagastamist PPA-le või VM-ile või muul viisil hävitamist.

2.10 Muud ZE õigused ja kohustused

ZE-l on õigus võtta mis tahes meetmeid, mis on ZE-le kohustuslikud Eesti või ELi õigusaktide või PPA-ga sõlmitud lepingu alusel.

ZE-l on õigus sertifikaadi staatuse teenused lõpetada, kui kõik sertifikaadid on aegunud või kehtetuks tunnistatud. Lõpuks sertifikaadi staatuse teenused lõpetatakse.

ZE-l on õigus avaldada autentimise ja krüpteerimise sertifikaat avalikult kättesaadavas veebipõhises hoidlas (LDAP). ZE on kohustatud osutama tellijatele ja tuginevatele pooltele järgmisi ööpäevaringseid teenuseid:

- sertifikaadi staatuse teenus (CRL ja OCSP)
- sertifikaatide hoidla teenus (LDAP)
- sertifikaatide kehtetuks tunnistamise portaal tellijatele
- dokumentatsiooni ja sertifitseerija sertifikaadi digihoidla teenus

ZE peab täitma kõiki kvalifitseeritud usaldusteenuse osutaja kohustusi kooskõlas Eesti ja ELi õigusaktidega. ZE

peab täitma kõiki PPA-ga sõlmitud lepingus sätestatud kohustusi.

2.11 Sertifikaadi staatuse kontrollimise kohustused tellijatele ja tuginevatele pooltele

Märkus. Loetavuse huvides nimetatakse selles peatükis tellijat ja tuginevat poolt ühiselt tuginevaks pooleks.

Tuginev pool peab olema teadlik sertifikaadile tuginemise ja selle aktsepteerimisega seotud riskidest ja kohustustest.

Tuginev pool peab keelduma sertifikaadile tugimisest, kui sertifikaat on selle kasutamise ajal peatatud, kehtetuks tunnistatud või aegunud.

Kui tuginev pool kasutab sertifikaati selle ettenähtud otstarbel, peavad kasutatavad süsteemid ja tarkvara suutma sertifikaadi staatust valideerida, kasutades vähemalt ühte kahest sertifikaadi staatuse teenusest (CRL ja OCSP), mis on märgitud sertifikaadis, või suutma valideerida õigesti dateeritud ja kontrollitavat sertifikaadi staatuse teavet, mis on lisatud faili või tehingusse või nendega seotud.

Tuginev pool peab sertifikaati kontrollima vähemalt ühe sertifikaadi staatuse teenuse abil.

Tuginev pool tohib sertifikaadile tugineda ainult juhul, kui see ei ole asjaomase perioodi jooksul peatatud ega ole enne asjaomast perioodi kehtetuks tunnistatud.

Tuginev pool ei tohi sertifikaadile tugineda, kui sertifikaadi staatust ei ole võimalik kindlaks teha või kui seda ei ole võimalik nõuetekohaselt seostada sertifikaadi kasutamise kuupäeva ja kellaajaga.

Tuginev pool tugineb sertifikaatidele ainult siinses dokumendis, dokumentides [ZE CPS-ID1- EID-CA] ja [PPA CP-ID1-EID-CA] ning sertifikaadis endas kodeeritud võtme kasutamise teabes sätestatud eesmärgil.

Tuginev pool vastutab täielikult kuupäeva ja kellaaja asjakohasuse ja tõlgendamise eest seoses sertifikaadi staatuse kehtivuse kontrollimisega ning selle kohaldamise eest sertifikaadi staatuse tõlgendamisel konkreetsel ajahetkel.

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.

2.12 Sertifikaadi staatuse teenused

Tellijad ja tuginevad pooled saavad kasutada tasuta kahte standardse sertifikaadi staatuse teenust (CRL ja OCSP).

CRL

Maksimaalse koostalitlusvõime tagamiseks kolmanda poole tarkvaraga

- vastab CRL standardile RFC 5280
- sisaldab kontrollitav sertifikaat CRL-i URI-d
- allkirjastab CRL-i sertifitseerija ise
- ei kasuta kvalifitseeritud usaldusteenuse osutaja CRL-i allkirjastamiseks mõnda teist usaldusväärset asutust
- saab CRL-faile alla laadida HTTP ja HTTPS-i kaudu

Tuginev pool vastutab ainuisikuliselt CRL-i perioodilisuse arvesse võtmise eest.

OCSP

Maksimaalse koostalitlusvõime tagamiseks kolmanda poole tarkvaraga

- vastab OCSP standardile RFC 6960
- sisaldab kontrollitav sertifikaat OCSP URI-d

- toetavad OCSP-d nonsi kasutamist requestExtensionis
- ei tohi OCSP-päringud sisaldada rohkem kui 1 (ühte) sertifikaadi seerianumbrit

Tuginevad pooled, kes soovivad OCSP-vastused kiirema töötlemise ja võrguliikluse vähendamise eesmärgil vahemällu salvestada, ei saa OCSP-päringus nonsse kasutada.

Kvalifitseeritud sertifikaatide kehtivusaja lõppemise järel sertifikaadi staatuse teabe säilitamise periood

Sertifikaadi staatuse teenustes tuleb sertifikaadi staatuse teavet ajakohastada vähemalt seni, kuni kõik väljastatud sertifikaadid on aegunud või kehtetuks tunnistatud.

Sertifikaadi staatuse teenuste lõpetamine

Tellijatel ja tuginevatel pooltel soovitatakse kasutada süsteeme ja tarkvara, mis sisaldab sertifikaadi staatuse teavet kasutamise ajal failis või tehingus, eriti kui fail või tehing on pikaajaline ja võib tulevikus vajada kontrollimist.

2.13 Piiratud garantii ja vastutuse välistamine

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

- sertifikaati ei kasutatud õigesti,
- 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,
- turvalisuse ja usalduse aluseks olevad kontseptsioonid või põhimõtted ei ole teaduse või tehnoloogia murrangulise arengu tõttu enam asjakohased.

Kvalifitseeritud usaldusteenuse osutaja välistab oma vastutuse, sealhulgas tellijate ja kõigi tuginevate poolte suhtes. Välistused ja piirangud on korratud muu hulgas dokumendi [ZE CPS-ID1-EID-CA] peatükkides 9.7 ja 9.8.

2.14 Vääramatu jõud

ZE kui kvalifitseeritud usaldusteenuse osutaja ei vastuta garantii rikkumise, viivituse või täitmise ebaõnnestumise eest, mis tuleneb tema kontrolli alt väljas olevatest sündmustest, nagu loodusõnnetused, sõjategevus, terrorismiaktid, epideemiad, elektri- või telekommunikatsiooniteenuste rikked, tulekahjud ja muud loodusõnnetused. Vaata ka dokumendi [ZE CPS-ID1-EID-CA] peatükki 9.8 välistatud vastutuse kohta.

2.15 Kohaldatav õigus

Eesti Vabariigis kvalifitseeritud usaldusteenuse osutajana registreeritud ZE tegevust reguleerivad Euroopa Liidu ja Eesti Vabariigi õigusaktid.

2.16 Kontaktandmed

Dokumentide sertifikaatidega seotud küsimuste korral võite ZE-ga ühendust võtta järgmiste kanalite kaudu:

E-post: info_eidpki AT ee.zetes.com

Veebisait: <https://repository.eidpki.ee>

2.17 Kaebused ja vaidluste lahendamine

Dokumentide menetlemisega seotud kaebused (tasud, taotlemine, kättetoimetamine või üleandmine, võtmete asendamine jne) tuleb esitada dokumendi väljaandjale.

Tarkvaraga DigiDoc seotud kaebused tuleb esitada Riigi Infosüsteemi Ametile (RIA) aadressil <https://www.ria.ee>.

Kaebused sertifikaatide sisu või ZE osutatavate avalike teenuste, näiteks sertifikaatide staatuse teenuste (CRL ja OCSP), LDAP-hoidla teenuste ning sertifikaatide kehtetuks tunnistamise portaali kohta tuleb esitada ZE-le. Kaebused ZE-le tuleb esitada e-posti teel (vt peatükk 2.17).

Kõik vaidlused lahendatakse kooskõlas Eesti õigusaktidega.

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

2.18 Kohaldatavad lepingud, sertifitseerimispõhimõtted ja sertifitseerimispoliitika

Allpool loetletud dokumendid on avaldatud järgmistel veebisaitidel:

- Inglise ja eesti keeles: <https://repository.eidpki.ee>
- Inglise keeles: <https://www.id.ee/en/rubriik/certificates/>
- Eesti keeles: <https://www.id.ee/rubriik/sertifikaadid/>

Dokumentide nimekiri:

[ZE CPS-ID1-ROOT-CA]	Zetes Estonia OÜ – Certificate Practice Statement for the Root CA for ID-1 Documents of the Republic of Estonia
[ZE CPS-ID1-EID-CA]	Zetes Estonia OÜ – Certificate Practice Statement for the Intermediate CA for ID-1 documents of the Republic of Estonia
[ZE PDS-ID1]	Zetes Estonia OÜ – avaliku võtme taristu avalikustamise avaldus Eesti Vabariigi ID-1 formaadis dokumentide tellija sertifikaatide kohta
[ZE PROFILES]	Zetes Estonia OÜ Technical profile of Certificates, OCSP responses and CRLs
[ZE TSPS-ID1]	Zetes Estonia OÜ – Trust Services Practice Statement for the CA-hierarchy for ID-1 Documents of the Republic of Estonia
[ZE TC-ID1-SUB]	Zetes Estonia OÜ – Zetes Estonia OÜ poolt Eesti Vabariigi ID-1 formaadis isikut tõendavate dokumentide jaoks väljaantud sertifikaatide kasutustingimused
[ZE TC-ID1]	Zetes Estonia OÜ – Eesti Vabariigi ID-1 formaadis isikut tõendavate dokumentide jaoks väljaantud sertifikaatidega seotud CRL-, OCSP-,LDAP- ja muude teenuste kasutajaleping ning tingimused
[PPA CP-ID1-EID-CA]	Politsei- ja Piirivalveamet – Certificate Policy for the ID-1 format identity documents of the Republic of Estonia, https://www.id.ee
[PPA CP-ID1-ROOT-CA]	Politsei- ja Piirivalveamet – Certificate Policy of for the root Certification Authority of the Republic of Estonia, https://www.id.ee

2.19 Isikuandmete privaatsus

2.19.1 Privaatsuseeskiri

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

Kvalifitseeritud usaldusteenuse osutaja kohustused:

- isikuandmete töötlemisel järgida IKÜMi (määrus (EL) 2016/679) ning e-identimise ja e-tehingute usaldusteenuste seaduse (EST EUTS) nõudeid;
- kohelda kõiki isikuandmeid konfidentsiaalsena, kui tellija ei otsusta teisiti;
- rakendada piisavaid tehnilisi ja organisatsioonilisi meetmeid, mis tagavad isikuandmete töötlemise turvalisuse kooskõlas IKÜMi (määrus (EL) 2016/679) ning e-identimise ja e-tehingute usaldusteenuste

seaduse (EST EUTS) nõuetega.

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 isikuandmete kaitse seadusega (EST IKS) kohaldatavatest kohustustest ja nende siinsetest kohustustest.

2.19.2 Privaatsena käsitletav teave

Sertifikaadis kodeeritud isikuandmed loetakse privaatseks teabeks, kui neid töötlevad kvalifitseeritud usaldusteenuse osutaja, registreerijad ja nende 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 kasutamise teave, nagu taotleja IP-aadress ning OCSP-päringu kuupäev ja kellaaeg, loetakse privaatseks teabeks, kuid säilitatakse Eesti õiguse kohaselt volitatud õiguskaitseasutuste võimalike tulevaste kohtuekspertiisi uurimiste jaoks.

2.19.3 Teave, mida ei käsitleta privaatse

LDAP-teenuses avaldatud sertifikaadid ei ole privaatseid.

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

2.19.4 Teatis ja nõusolek isikuandmete kasutamiseks

Sertifikaadi taotlemise protsessi käigus tutvustatakse tellijale kasutustingimusi [ZE TC-ID1-SUB] ning tellija annab nõusoleku oma isikuandmete kasutamiseks kooskõlas isikut tõendavate dokumentide seaduse (EST ITDS) ning e-identimise ja e-tehingute usaldusteenuste seadusega (EST EUTS). Tellija võib sertifikaatide kehtetuks tunnistamist taotleda igal ajal.

2.19.5 Säilitamisaeg

ZE säilitab auditeerimislogisid ja tellija sertifikaatide koopiaid viis aastat alates sertifikaadi kehtivusaja lõppemisest.

PPA ja VM säilitavad tellija sertifikaatide väljaandmise ja elutsükli haldamisega seonduvat teavet vähemalt 10 aastat pärast sertifikaadi kehtivuse lõppemist.

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

VM-i paberandjal kirjed arhiveerib VM. 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 elektroonilised kirjed säilitatakse andmebaasi eeskirjade alusel, mis ületavad eIDASi nõudeid ning on sätestatud õigusaktis EST VEISM.

PPA tagab, et dokumentide ja sertifikaatide väljaandmise ning väljastamisjärgse ajakohastamisega seonduvat teavet säilitatakse vähemalt 10 aastat pärast sertifikaadi kehtivuse lõppemist.

2.19.6 Avalikustamine kohtu- või haldusmenetluse raames

Teavet võib avalikustada kohtu- või haldusmenetluse käigus.

2.19.7 Muud teabe avalikustamise asjaolud

Kvalifitseeritud usaldusteenuse osutajal ei ole kohustust avaldada muud teavet peale selle, mis on sätestatud õiguspärases ja seaduslikus kohtumääruses.

3 SERTIFIKAATE SISALDAVATE DOKUMENTIDE LOETELU

Järgmises tabelis on loetletud kõik dokumendid, mis sisaldavad sertifikaate ja igäihe suhtes kohaldatav sertifitseerimispoliitika [PPA CP-ID1-EID-CA].

Sertifikaadi eeskirja OID	Väljaandja	Dokumendi liik	Kasutus
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

----- Dokumendi viimane lehekülg -----