



DIGI- JA
VÄESTÖTIETO-
VIRASTO

VARMENNEPOLITIIKKA KANSALAI- VARMENNE

Digi- ja väestötietoviraston kansalaisvarmennetta varten

OID: 1.2.246.517.1.10.302

OID: 1.2.246.517.1.10.352

13.3.2023



Dokumentinhallinta

Omistaja	
Laatinut	Ville Aarnio
Tarkastanut	
Hyväksynyt	Mikko Pitkänen

Version hallinta

versionro	mitä tehty	pvm/henkilö
1.0	Versio 1.0	1.6.2021/VA
1.1.	Lisätty kuvaus lokidatasta	1.10.2021/VA
1.2	Päivitetty versio ja linkit varmennepolitiikkasivulle	29.9.2022/SK
1.3	Korvattu termi "PUK-koodi" termillä "aktivointitunnusluku". Lisätty aktivointitunnusluvun määritelmään, että sillä voi vapauttaa lukkiutuneen PIN-tunnusluvun. Tarkennettu kohtaan 5.2, mikä on ISO IEC 27001. Poistettu kohdasta 5.2 SSCD a lisätty QSCD. Korjattu kohtaan 9.2.8 RSA-avaimen bittimäärä. Päivitetty linkkejä.	8.3.2023/AG



Sisällysluettelo

1	Esipuhe.....	5
2	Johdanto	5
3	Soveltamisala.....	6
4	Viiteluettelo	6
5	Määritelmät ja lyhenteet	8
5.1	Määritelmät.....	8
5.2	Lyhenteet.....	13
6	Yleiskäsitteet.....	14
6.1	Varmentaja	14
6.2	Varmennepalvelut.....	16
6.2.1	Varmenteeseen luottava osapuoli.....	18
6.3	Varmennepolitiikka ja varmennuskäytäntö	18
6.3.1	Tarkoitus.....	18
6.3.2	Yksityiskohtaisuus	19
6.3.3	Lähestymistapa.....	19
6.3.4	Muut varmentajan julkaisemat asiakirjat	19
6.4	Varmenteen hakija.....	20
7	Johdanto varmennepolitiikkoihin	20
7.1	Yleistä.....	20
7.2	Yksilöintitunnukset	22
7.3	Käyttäjyhteisö ja sovellettavuus	22
7.3.1	QCP:n QSCD -varmennepolitiikka	22
7.4	Vaatimustenmukaisuus.....	22
8	Velvollisuudet ja vastuu sekä vastuunrajoitukset	22
8.1	Varmentajan velvollisuudet	23
8.1.1	Varmentajan velvollisuudet	23
8.1.2	Rekisteröijää koskevat velvollisuudet.....	24
8.2	Varmenteen hakijan velvollisuudet.....	24
8.3	Tiedottaminen varmenteeseen luottaville osapuolille	25
8.4	Vastuu	26
8.4.1	Varmentajan vastuut	26
8.4.2	Rekisteröijän vastuut	26
8.4.3	Kansalaisvarmenteen haltijan vastuut.....	27
8.4.4	Kansalaisvarmenteeseen luottavan osapuolen vastuut.....	27



8.4.5	Vastuiden rajoitukset	27
8.4.6	Muut osapuolet	28
9	Varmentajan toimintaa koskevat vaatimukset	28
9.1	Varmennuskäytäntö	29
9.2	Julkisen avaimen järjestelmässä käytettävien avainten elinkaaren hallinta	29
9.2.1	Varmentajan avaimen luominen.....	29
9.2.2	Varmentajan avaimen tallennus, varmuuskopiointi, ja palauttaminen.....	29
9.2.3	Varmentajan julkisen avaimen jakelu	30
9.2.4	Vara-avainjärjestelmä	30
9.2.5	Varmentajan avaimen käyttö.....	30
9.2.6	Varmentajan avaimen elinkaaren päättyminen	30
9.2.7	Varmenteiden allekirjoittamisessa käytettävän salauslaitteiston elinkaaren hallinta ..	31
9.2.8	Varmentajan tarjoamat allekirjoittajan avaimen hallintapalvelut.....	31
9.2.9	Turvallisen allekirjoituksen luomisvälineen valmistaminen	31
9.3	Julkisen avaimen järjestelmässä käytettävien varmenteiden elinkaaren hallinta	32
9.3.1	Allekirjoittajan rekisteröinti	32
9.3.2	Varmenteen uusiminen, sen avainparin vaihtaminen ja varmenteen päivittäminen ..	33
9.3.3	Varmenteiden luominen	33
9.3.4	Käyttöehtojen jakelu	34
9.3.5	Varmenteiden jakelu	35
9.3.6	Varmenteen peruuttaminen ja asettaminen keskeytystilaan.....	35
9.3.7	Sulkulistan julkaisu tiheys	37
9.4	Avainparin uusiminen varmenteen sulkulistalle asettamisen jälkeen.....	37
9.5	Varmentajan johtamis- ja toimintakäytännöt.....	38
9.5.1	Turvallisuuden hallinta	38
9.5.2	Varantojen luokittelu ja hallinta	38
9.5.3	Henkilöstö ja tietoturva.....	39
9.5.4	Fyysinen ja ympäristön turvallisuus.....	40
9.5.5	Toiminnan hallinta.....	41
9.5.6	Järjestelmiin pääsyn hallinta	42
9.5.7	Luotettavien järjestelmien käyttöönotto ja ylläpito	42
9.5.8	Liiketoiminnan jatkuvuuden hallinta ja häiriötilojen käsittely	42
9.5.9	Varmentajan toiminnan lakkauttaminen	42
9.5.10	Lainsäädäntöön perustuvien vaatimusten noudattaminen.....	43
9.5.11	Allekirjoitusvarmenteita koskevan tiedon säilyttäminen	44
9.6	Organisaatioon liittyvät vaatimukset.....	44
10	Määrittelypuitteet muita varmennepolitiikkoja varten.....	45



10.1	Varmennepolitiikan hallinta	45
10.2	Poikkeukset varmennepolitiikkoihin, jotka koskevat muille kuin yleisölle myönnettäviä allekirjoitusvarmenteita	46
10.3	Lisävaatimukset	46
10.4	Vaatimustenmukaisuus	46



VARMENNEPOLITIIKKA KANSALAI SVARMENNE

1 Esipuhe

Tämä asiakirja perustuu tekniseen määritykseen, jonka on laatinut sähköisiä allekirjoituksia ja järjestelmiä käsittelevä ETSIn tekninen komitea (ETSI Technical Committee Electronic Signatures and Infrastructures (ESI)).

Varmennepalveluita tarjoavan viraston nimenmuutoksesta on säädetty laissa Digi- ja väestötietovirastosta (304/2019). Väestörekisterikeskuksen nimi muuttuu 1.1.2020 Digi- ja väestötietovirastoksi.

2 Johdanto

Sähköinen asiointi edellyttää sähköisen tiedon lähteen tunnistamista asiakirjoihin käsin tehtyyn allekirjoitukseen verrattavalla tavalla. Tämä voidaan yleensä toteuttaa käyttämällä sähköisiä allekirjoituksia. Varmennepalveluiden tarjoajat, joita yleisesti kutsutaan varmentajiksi, tuottavat sähköisten allekirjoitusten tekemiseen tarkoitettuja varmenteita.

Sähköisten allekirjoitusten käyttäjät voivat luottaa sähköisten allekirjoitusten aitouteen, jos varmentajalla on käytössään asianmukaiset menettelyt ja suojautumiskeinot, joilla minimoidaan julkisiin salausavainten järjestelmiin liittyvät toiminnalliset ja taloudelliset riskit.

Tämä asiakirja perustuu seuraavan asetuksen mukaisesti määriteltyyn sähköisen allekirjoituksen luotettavuuden erityisiin vaatimuksiin:

Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (Asetus). Tässä asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat asetuksen mukaisesti allekirjoitusvarmenteita myöntävien varmentajien toimintaa ja hallintokäytäntöjä.

Varmennepolitiikka on varmentajan laatima kuvaus menettelytavoista ja toimintaperiaatteista, joita varmenteita myönnettäessä noudatetaan. Varmennuskäytäntö on varmennepolitiikkaa yksityiskohtaisempi kuvaus varmentajan toiminnasta.

Tätä varmennepolitiikkaa sovelletaan Digi- ja väestötietoviraston kansalaisvarmenteeseen, jo-ka myönnetään väestötietojärjestelmään rekisteröidyille Suomen kansalaisille ja Suomessa pysyvästi asuville ulkomaalaisille.

Kansalaisvarmenne koostuu kolmesta eri varmenteesta, joilla on kaksi eri käyttötarkoitusta: todentaminen- ja salaus sekä sähköiset allekirjoitukset. Todentamisvarmenne on mainitun lain mukainen vahvan sähköisen tunnistamisen väline. Allekirjoitusvarmenteet ovat vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaisia sähköisiä allekirjoitusvälineitä. Toinen saman vaatimustason täyttävistä allekirjoitusvarmenteista on toteutettu RSA-algoritmiin ja toinen ECC-algoritmiin perustuen. Varmenteen haltija voi käyttää kumpaa tahansa näistä varmenteista sähköisiin allekirjoituksiin.



3 Soveltamisala

Tässä asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat tunnistus- ja allekirjoitusvarmenteita myöntäviä varmentajia sekä vahvan sähköisen tunnistamisvälineen tarjoajana olevaa Digi- ja väestötietovirastoa. Menettelytapavaatimuksia asetetaan varmenteita myöntävien varmentajien toiminnalle ja hallintakäytännölle, jotta varmenteen hakijat, varmentajan varmentamat allekirjoittajat sekä varmenteeseen luottavat osapuolet voisivat luottaa siihen, että varmenteella voidaan vahvistaa sähköisiä allekirjoituksia.

Digi- ja väestötietoviraston tarjoaman vahvan sähköisen tunnistamisen välineen tarjoaminen tapahtuu samassa tuotantoympäristössä, samanlaisin teknisin ja toiminnallisin ratkaisuin ja siihen sovelletaan samoja menettelytapoja noudattaen kuin Digi- ja väestötietoviraston myöntämän allekirjoitusvarmenteen tarjoamiseen.

Varmentajaa koskevat menettelytapavaatimukset sisältävät vaatimuksia rekisteröintipalvelujen tarjoamisesta, varmenteiden luomisesta, varmenteiden jakelusta, varmenteiden peruuttamisen hallinnasta, sulkutilasta ja tarvittaessa allekirjoituksen luomisvälineen tarjoamisesta. Muut varmennepalvelujen tarjoajan toiminnot, kuten aikaleimat, attribuuttivarmenteet ja luottamuksellisuutta tukevat palvelut, eivät kuulu tämän asiakirjan soveltamisalaan. Tässä asiakirjassa ei esitetä vaatimuksia varmentajan varmenteille, ei myöskään varmennehierarkioille tai ristiinvarmentamiselle. Nämä menettelytapavaatimukset on rajattu koskemaan sähköisten allekirjoitusten yhteydessä käytettävien avainten varmentamista.

Nämä menettelytapavaatimukset on erityisesti kohdistettu yleisölle myönnettäviin allekirjoitusvarmenteisiin, joita käytetään tukemaan sähköisiä allekirjoituksia Asetuksen mukaisia allekirjoitusvarmenteita myöntäviä varmentajia. Näiden menettelytapavaatimusten mukaisesti myönnettyjä varmenteita voidaan käyttää henkilön todentamisessa, kun henkilö toimii omasta puolestaan tai edustamansa luonnollisen henkilön, oikeushenkilön tai yhteisön puolesta.

Nämä menettelytapavaatimukset koskevat julkisen avaimen salauksen käyttöä sähköisten allekirjoitusten vahvistamisessa.

Asiantuntevat riippumattomat elimet voivat käyttää tätä asiakirjaa perustana arvioi-
dessaan, täyttääkö varmentaja allekirjoitusvarmenteiden myöntämistä koskevat vaatimukset.

Varmenteenhaltijoita ja varmenteeseen luottavia osapuolia suositellaan lukemaan varmentajan varmennuskäytännöstä tarkempia lisätietoja siitä, kuinka kyseinen varmentaja toteuttaa tiettyä varmennepolitiikkaansa.

Tässä asiakirjassa ei kuitenkaan tarkenneta, kuinka riippumattomat osapuolet voivat arvioida tässä yksilöityjä vaatimuksia, esimerkiksi ei määritetä vaatimuksia riippumattomien arvioijien saataville annettavan tiedon tai riippumattomien arvioijien suhteen.

4 Viiteluettelo

Tässä asiakirjassa viitataan seuraavissa asiakirjoissa esitettyihin säännöksiin ja määrittelyihin, jotka ovat sitovia tässä asiakirjassa kuvattuihin toimintoihin liittyen.





Käytetyt viittaukset liittyen julkaisupäivään ja laitoksen tai version numeroihin ovat täsmällisiä tai yleisluontoisia.

Täsmällisten viittausten osalta lähteen myöhempiä tarkistuksia ei sovelleta.

Yleisluontoisten viittausten osalta sovelletaan lähteen viimeisintä versiota.

Tähän asiakirjaan liittyvää aineistoa on saatavilla muun muassa osoitteessa <http://docbox.etsi.org/Reference>. ETSI ei takaa linkin toimivuutta pitkällä aikavälillä.

Määräävät viittaukset:

[1] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[2] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security

requirements for trust service providers issuing certificates; Part 1: General requirements".

[3] Guidelines for The Issuance and Management of Extended Validation Certificates v1.5.5 CA/Browser Forum.

[4] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

Ohjeelliset viittaukset:

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) N 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".



[i.3] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum.

[i.4] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.6] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

Terminologiset kuvaukset:

For the purposes of the present document, the terms and definitions given in ETSI EN 319 401 [1], ETSI

EN 319 411-1 [2], the Regulation (EU) N° 910/2014 [i.1] and the following apply:

EU Qualified Certificate: qualified certificate as specified in Regulation (EU) No 910/2014 [i.1]

Qualified Electronic Signature/Seal Creation Device: As specified in Regulation (EU) No 910/2014 [i.1].

5 Määritelmät ja lyhenteet

5.1 Määritelmät

Tässä asiakirjassa käytetään seuraavia käsitteitä ja määritelmiä:

Aktivointitieto: Sellainen luottamuksellinen tieto (PIN-tunnus), jota tarvitaan mikro-sirulla olevien yksityisten avainten aktivointiin ja niiden käyttöön julkisen avaimen menetelmissä (esim. sähköinen allekirjoitus).

Aktivointitunnusluku: Kansalaisvarmenteen käyttäjä saa kortin käyttämistä varten haltuunsa henkilökohtaisen aktivointitunnusluvun, jonka jälkeen käyttäjä voi aktivoida ja määritellä omat, henkilökohtaiset PIN-tunnuslukunsa. Aktivointiprosessin jälkeen käyttäjä pystyy käyttämään henkilökorttiaan sähköisessä asiointissa. Aktivointitunnuslukua voi lisäksi käyttää lukkiutuneen PIN-tunnusluvun vapauttamiseen.

Allekirjoittaja: taho, joka on varmenteessa merkitty varmenteessa annettuun julkiseen avaimeen liittyvän yksityisen avaimen haltijaksi

Allekirjoituksen luomiseen käytettävät tiedot: ainutlaatuinen tietokokonaisuus, esimerkiksi koodit tai yksityiset salausavaimet, joita allekirjoittaja käyttää luodakseen sähköisen allekirjoituksen.



Kun kyseessä ovat julkisen avaimen salaukseen perustuvat allekirjoitusvarmenteet, kuten tämän asiakirjan soveltamisalassa, allekirjoituksen luomiseen käytettävät tiedot sisältävät yksityiset avaimet. Tässä asiakirjassa allekirjoituksen luomiseen käytettävistä tiedoista käytetäänkin käsitettä yksityinen avain.

Allekirjoituksen luomisväline: tarkoituksenmukaisesti määritetty ohjelmisto tai laiteisto, jolla allekirjoituksen luomiseen käytettävät tiedot käsitellään.

Allekirjoituksen todentamiseen käytettävät tiedot: tietokokonaisuus, esimerkiksi koodit tai julkiset salausavaimet, joita käytetään sähköisen allekirjoituksen todentamiseen.

Kun kyseessä ovat julkisen avaimen salaukseen perustuvat allekirjoitusvarmenteet, kuten tämän asiakirjan soveltamisalassa, allekirjoituksen todentamiseen käytettävät tiedot sisältävät julkiset avaimet. Tässä asiakirjassa allekirjoituksen todentamiseen käytettävistä tiedoista käytetäänkin käsitettä julkinen avain.

Allekirjoitusvarmenne: Varmenne, jonka käyttötarkoitus on kiistämätön sähköinen allekirjoitus.

Attribuutti: tahoon liitetty tieto, joka määrittelee tahon ominaisuuden, kuten ryhmän jäsenyyden tai roolin, tai muu kyseiseen tahoon liittyvä tieto

Avainpari: Julkisen avaimen menetelmissä käytettävät, toisiinsa liittyvät avaimet, joista toinen on julkinen ja toinen yksityinen. Avainten käyttötarkoitus on määritelty varmenteessa (ks. varmenteen haltijan allekirjoitusvarmenne sekä todentamis- ja salausvarmenne).

ECC-algoritmi ja ECC-avain: ECC-algoritmi kattaa erilaiset elliptisten käyrien salausmenetelmiin liittyvät algoritmit, jotka toteuttavat julkisen avaimen salausjärjestelmän. ECC-avaimella on RSA-avainparin tapaan julkinen ja yksityinen avain.

Epäsymmetrinen salaus: Epäsymmetrisessä salauksessa käytetään avainparia, joista toinen on julkinen ja toinen yksityinen. Julkisella avaimella salattu viesti voidaan avata vain kyseisen avainparin yksityisellä avaimella.

Henkilökortti: Poliisin myöntämä henkilöllisyystodistus, jonka tekniseen osaan on talletettu kortinhaltijan kansalaisvarmenne.

Julkinen avain: Julkisen avaimen menetelmässä epäsymmetrisessä salauksessa käytettävän avainparin julkinen osa. Varmentaja varmentaa sähköisellä allekirjoituksellaan julkisen avaimen kuulumisen varmenteen haltijalle. Julkinen avain on osa varmenteen tietosisältöä.

Julkisen avaimen järjestelmä: Tietoturvainfrastruktuuri, jossa tietoturvapalveluita tuotetaan julkisen avaimen menetelmillä.

Julkisen avaimen menetelmä: Tietoturvapalvelu, esimerkiksi henkilön sähköinen tunnistaminen, joka tuotetaan käyttämällä julkisia ja yksityisiä avaimia, varmenteita ja epäsymmetristä salausta.

Kansalaisvarmenne: Digi- ja väestötietoviraston luonnolliselle henkilölle myöntämä tässä asiakirjassa tarkemmin määritelty varmennepari, joka allekirjoitusvarmenne,



jonka tietosisältö on määritelty laissa Digi- ja väestötietoviraston varmennepalveluista (661/2009).

Kehittynyt sähköinen allekirjoitus: sähköinen allekirjoitus, joka täyttää seuraavat vaatimukset: se liittyy yksiselitteisesti

- a) sen allekirjoittajaan
- b) sillä voidaan yksilöidä allekirjoittaja
- c) se on luotu keinoilla, jotka allekirjoittaja voi pitää yksinomaisessa valvonnassaan,
- d) se on liitetty sen kohteena olevaan tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita

Kortinlukijaohjelmisto: Kortinlukijaohjelmistoa käytetään työasemassa ns. loppukäyttäjän sovelluksena. Sen avulla käyttäjä voi hyödyntää henkilökorttiaan ja sillä olevia varmenteita erilaisissa käyttö- ja sovellusympäristöissä, esimerkiksi sähköisessä asioinnissa, turvapostissa ja työasemaan kirjautumisessa.

Luottava osapuoli: Taho, joka luottaa varmenteen tietoihin ja käyttää varmennetta erilaisiin tietoturvapalveluihin, kuten varmenteen haltijan sähköiseen tunnistamiseen ja sähköisen allekirjoituksen todentamiseen.

Maksukortti: Luotto-, yhdistelmä-, raha- ja maksuaikakortin yleisnimitys.

Mikrosiru: Tekninen alusta, jolla varmenne ja yksityiset avaimet sijaitsevat ja joka on sijoitettu henkilökortille, maksukortille tai mobiilipäätelaitteen kortille.

Mobiilipäätelaite: Matkapuhelin tai muu mobiililaitte, jonka avulla voidaan käyttää varmennetta ja mikrosirulla olevia yksityisiä avaimia.

PIN-tunnus: Aktivointitieto, jolla mikrosirulla oleva yksityinen avain aktivoidaan käytettäväksi. PIN 1: perustunnusluku todentamista ja salausta varten. PIN 2: allekirjoitustunnusluku sähköistä allekirjoitusta varten.

Rekisteröijä: Rekisteröijä tunnistaa varmenteen hakijan henkilöllisyyden varmennepolitiikan ja varmennuskäytännön mukaisesti varmentajan lukuun ja vastuulla.

RSA-algoritmi ja RSA-avain: RSA-algoritmi on eräs yleisesti käytetty julkisen avaimen algoritmi. Osa kansalaisvarmenteeseen liittyvistä avainpareista on RSA-avaimia.

Sulkulista: Varmentajan sähköisesti allekirjoittama ja julkaisema luettelo kesken voimassaoloajan suljetuista varmenteista ja niiden sulkuajankohdista. Sulkulistasta ilmenee sen ja sitä seuraavan sulkulistan julkaisuajankohta. Suljetut varmenteet viedään sulkulistalle.

Sulkupalvelu: Tekninen toimittaja, joka ottaa vastaan ja välittää varmenteiden sulkupyynnöt varmennejärjestelmään varmentajan lukuun.

sähköinen allekirjoitus: sähköisessä muodossa oleva tieto, joka on liitetty tai loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään kyseisen muun tiedon todentamismenetelmänä.



Sähköinen asiointitunnus: Numeroista ja tarkistusmerkistä muodostettu tunniste, jonka avulla voidaan yksilöidä Suomen kansalaiset ja kotikuntalaiset mukaisesti Suomessa vakinaisesti asuvat ulkomaalaiset, jotka on merkitty Väestötietojärjestelmään.

Sähköinen allekirjoitus: kehittynyt sähköinen allekirjoitus, joka perustuu allekirjoitusvarmenteeseen ja joka on tehty turvallisella allekirjoituksen luomisvälineellä

Turvallinen allekirjoituksen luomisväline: allekirjoituksen luomisväline, joka täyttää Asetuksessa säädetyt vaatimukset

Varmenne: sisältää käyttäjän julkisen avaimen sekä muita tietoja, joiden väärentäminen on estetty salakirjoittamalla ne varmenteen myöntäneen varmentajan yksityisellä avaimella. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.

Varmenne: Sähköinen todistus, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa allekirjoittajan. Varmenne sisältää siihen liittyvän varmennuskäytännön yksilöivän tunnuksen.

Varmennejärjestelmä: Tietotekninen järjestelmä, jonka avulla luodaan varmenteet ja allekirjoitetaan sulkulistat.

Varmennekuvaus: Asiakirja sisältää varmennepolitiikan ja varmennuskäytännön keskeiset kohdat.

Varmennepalvelujen tarjoaja: yhteisö, oikeushenkilö tai luonnollinen henkilö, joka myöntää varmenteita tai tarjoaa muita sähköisiin allekirjoituksiin liittyviä palveluja

Tässä asiakirjassa käsitellään varmennepalvelujen tarjoajia, jotka myöntävät allekirjoitusvarmenteita (tai tarjoavat allekirjoitusvarmenteiden myöntämisen osapalveluja – katso kohta 4.1). Tässä asiakirjassa ei käsitellä varmennepalvelujen tarjoajan muuntotyypisiä toimintoja, kuten aikaleimausta ja vara-avainjärjestelmiä.

Varmennepolitiikka: nimetty säännöstö, joissa osoitetaan tietyn varmenteen soveltuvuus tietyille yhteisölle ja/tai sovellusluokka, jota koskee yhteiset turvallisuusvaatimukset. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.

Varmennerekisteri: Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukainen rekisteri, jota allekirjoitusvarmenteita yleisölle tarjoavan varmentajan on velvollisuus pitää. Tiedot on säilytettävä vähintään viiden vuoden ajan varmenteen voimassaolon päättymisestä.

Varmennetietojärjestelmä: Tietotekninen järjestelmä, joka koostuu varmennejärjestelmistä, tietoliikenteestä, varmennehakemistosta ja sulkulistapalvelusta, neuvonta- ja sulkupalvelusta sekä varmenteiden ja korttien hallinnoinnista.

Varmennuskäytännön yksilöivä tunnus on osa varmenteen tietosisältöä.

Varmennuskäytäntö: lausunto toimintatavoista, joita varmentaja noudattaa varmenteiden myöntämisessä, hallinnoimisessa, peruuttamisessa ja uusimisessa sekä varmenteiden avainparin vaihtamisessa. Jokaisella varmennuskäytännöllä on oma yksilöivä tunnuksensa.



Varmentaja: Varmenteita myöntävä organisaatio, joka vastaa varmenteiden tuottamisesta sekä laatii toimintaansa kuvaavan varmennepolitiikan sekä varmennuskäytännön. Varmentajan toimintaan luottaa yksi tai useampi taho. Varmentaja on varmenteita myöntävä varmennepalvelujen tarjoaja. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509. Varmentajan käsitettä selvennetään lisää kohdassa 4.2.

Varmentajan varmenne: Sisältää varmentajan nimen, sijaintimaan ja julkisen avaimen.

Varmentajan yksityinen avain: Varmentajan myöntämien varmenteiden ja sen julkaisemien sulkulistojen allekirjoittamiseen käytettävä yksityinen avain.

Varmenteen hakija: Henkilö, joka hakee kansalaisvarmennetta ja joka tunnustetaan hakemisen yhteydessä luotettavasti.

Varmenteen haltija: Henkilö, jonka henkilöllisyys ja julkinen avain on varmennettu varmentajan sähköisellä allekirjoituksella, ja jonka hallussa varmenteeseen liittyvät yksityiset avaimet ovat.

Varmenteenhakija/haltija: Varmennetta hakeva luonnollinen henkilö, joka tunnustetaan henkilökohtaisella tavalla ja joka vastaanottaessaan varmenteen on varmenteen haltija.

Varmenteen haltijan allekirjoitusvarmenne: Varmenteella olevalla julkisella avaimella todennetaan sitä vastaavalla yksityisellä avaimella eli allekirjoitusavaimella varmenteen haltijan tekemä sähköinen allekirjoitus. Allekirjoituksen tekemiseen tarvitaan allekirjoitustunnusluku (PIN 2).

Varmenteen haltijan todentamis- ja salausvarmenne: Varmennetta käytetään henkilön sähköiseen tunnistamiseen ja tiedon salaukseen. Varmenteen haltija käyttää yksityistä todentamis- ja salausavaintaan sähköiseen tunnistautumiseen ja salatun tiedon tai viestin salauksen purkuun. Avaimen käyttämiseen tarvitaan perustunnusluku (PIN 1).

Varmenteen käyttö ja käyttötarkoitus: Tässä dokumentissa varmenteen käyttö on nimitys sekä itse varmenteen että siihen liittyvien avainten käytölle. Esimerkiksi varmenteen käytöllä sähköisessä allekirjoituksessa tarkoitetaan sekä yksityisen avaimen käyttöä allekirjoituksessa että julkisen avaimen ja varmenteen käyttöä allekirjoituksen todentamisessa.

Varmenteeseen luottava osapuoli: varmenteen vastaanottaja, joka toimii luottaen kyseiseen varmenteeseen ja/tai digitaalisiin allekirjoituksiin, jotka on todennettu kyseisellä varmenteella. Tarkempi kuvaus perustuu RFC 3647-määritykseen.

Varmenteiden sulkulista: allekirjoitettu varmenneluettelo, jonka sisältämiä varmenteita niiden myöntäjät eivät enää katso voimassa oleviksi. Tarkempi kuvaus perustuu ITU-T:n suositukseen X.509.

Yksityinen avain: Julkisen avaimen menetelmässä epäsymmetrisessä salauksessa käytettävän avainparin yksityinen osa. Varmenteen haltijan yksityiset avaimet on tallennettu mikrosirulle niiden suojaamiseksi oikeudettomalta käytöltä.



5.2 Lyhenteet

ISO 27001	ISO IEC 27001 Kansainvälinen standardi tietoturvan hallinnalle
CA	Certification Authority, varmentaja
CSP	Certification Service Provider: varmennepalvelujen tarjoaja
CP	Certificate Policy, varmennepolitiikka
CPS	Certification Practise Statement, varmennuskäytäntö
CRL	Certificate Revocation List, varmenteiden sulkulista
ECC	Elliptic Curve Cryptography
FINEID	Finnish Electronic Identification
HSM	Hardware Security Module, turvamoduuli
HST	Henkilön sähköinen tunnistaminen
HTTP	Hypertext Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, suorakäyttöinen varmenteen tilan palauttava palvelu
OID	Object Identifier, yksilöivä tunnus
PDS	PKI Disclosure Statement, varmennekuvaus
PIN	Personal Identification Number, PIN-tunnus
PKI	Public Key Infrastructure, julkisen avaimen järjestelmä
RSA	Rivest, Shamir, Adleman, RSA-tunniste, eräs julkisen avaimen algoritmi, epäsymmetrinen algoritmi
SATU	Sähköinen asiointitunnus
SIM	Subscriber Identity Module
DVV	Digi- ja väestötietovirasto
QSCD	Qualified Signature Creation Device: hyväksytty allekirjoituksen luomisväline



6 Yleiskäsitteet

6.1 Varmentaja

Varmentaja luo ja myöntää varmenteita, jonka toimintaan varmennepalvelujen käyttäjät, eli varmenteen hakijat ja varmenteeseen luottavat osapuolet luottavat. Varmentaja on kokonaisvastuussa kohdassa 4.2 määriteltyjen varmennepalvelujen tarjoamisesta. Varmentaja on yksilöity varmenteessa varmenteen myöntäjäksi. Allekirjoitusvarmenteet allekirjoitetaan sen yksityisellä avaimella.

Varmentaja voi käyttää varmennepalvelussaan muita osapuolia, jotka tarjoavat palvelun osia. Varmentaja vastaa kuitenkin aina koko tuottamansa palvelun osalta ja varmistaa sen, että tässä asiakirjassa määritellyt menettelytapavaatimukset täyttyvät. Varmentaja voi esimerkiksi hankkia alihankintana kaikki osapalvelut, myös varmenteiden luomispalvelun. Varmenteiden allekirjoittamiseen käytettävä avain kuitenkin määritellään kuitenkin varmentajalle kuuluvaksi, ja varmentajalla säilyy kokonaisvastuu tässä asiakirjassa määriteltyjen vaatimusten täyttämistä sekä vastuu yleisölle myönnettävien varmenteiden myöntämisestä Asetuksen mukaisesti.

Digi- ja väestötietovirasto voi myöntää varmenteen myös omiin tarkoituksiinsa. Tällöin se noudattaa samoja vaatimuksia kuin muut organisaatiot.

Varmentaja on Asetuksen mukainen varmennepalvelujen tarjoaja, joka myöntää varmenteita.

Tässä asiakirjassa määritellään menettelytapavaatimukset, jotka koskevat allekirjoitusvarmenteita myöntäviä varmentajia sekä vahvan sähköisen tunnistamisvälineen tarjoajana olevaa Digi- ja väestötietovirastoa. Menettelytapavaatimuksia asetetaan varmenteita myöntävien varmentajien toiminnalle ja hallintakäytännölle, jotta tilaajat, varmentajan varmentamat allekirjoittajat sekä varmenteeseen luottavat osapuolet voisivat luottaa siihen, että varmenteella voidaan vahvistaa sähköisiä allekirjoituksia.

Digi- ja väestötietoviraston tarjoaman vahvan sähköisen tunnistamisen välineen tarjoaminen tapahtuu samassa tuotantoympäristössä, samanlaisin teknisin ja toiminnallisoin ratkaisuin ja siihen sovelletaan samoja menettelytapoja noudattaen kuin Digi- ja väestötietoviraston myöntämän allekirjoitusvarmenteen tarjoamiseen.

Digi- ja väestötietovirasto (DVV) toimii valtiovarainministeriön hallinnonalalla. DVV on henkilörekisteriä ylläpitävä viranomainen, jonka Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) mukainen tehtävä on tuottaa varmennettuja sähköisen asiointin palveluita. Digi- ja väestötietovirasto toimii myös terveydenhuollon lakisääteisenä varmentajana 1.12.2010 alkaen (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) ja laki sähköisestä lääkemääräyksestä (61/2007)). Digi- ja väestötietoviraston varmennepalvelut -toiminto vastaa viraston varmennetoiminnasta. DVV on tarjonnut varmennepohjaisia allekirjoitus- ja tunnistusvälineitä vuodesta 1999 lähtien ja toiminut allekirjoitusvarmentajana 31.3.2003 lukien.

DVV:n varmennetietojärjestelmä ja varmennepalvelut perustuvat julkisen avaimen järjestelmään (Public Key Infrastructure eli PKI). DVV:n varmenneinfrastruktuuri muodostuu varmennejärjestelmästä, varmennekortteihin sisältyvien varmennetietojen



toimittajasta, sulkulistasta, neuvontapalvelusta ja hakemistopalvelusta. DVV:n toimintoja varmentajana ovat varmenne-, hakemisto- ja sulkupalveluiden tuottaminen, rekisteröinti sekä varmenteen sisältävän kortin valmistus ja yksilöinti. DVV vastaa koko varmennejärjestelmän toimivuudesta, myös käyttämiensä rekisteröijien ja teknisten toimittajien osalta. DVV:n Varmennepalvelut -toiminto ylläpitää varmenteitaan koskevia varmennepolitiikka-, varmennuskäytäntö- ja varmennekuvausasiakirjoja, jotka ovat saatavilla sähköisesti osoitteessa www.dvv.fi/cps.

Euroopan parlamentin ja neuvoston asetusta (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta sovelletaan luottamuspalveluihin 1.7.2016 alkaen. Asetuksen velvoitteet on eräiltä osin saatettu myös lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) 1.7.2016 voimaan tulevaan muutokseen. Lailla säädetään vahvan sähköisen tunnistamisen palvelujen tarjoamisesta sekä sähköisestä allekirjoituksesta ja niiden oikeusvaikutuksista. Henkilökortista on säädetty henkilökorttilaissa (663/2016).

DVV tuottaa tietoturvallisuuden tasoltaan korkealaatuisia sähköisen allekirjoituksen ja tunnistamisen varmenteita ja niihin liittyviä palveluja. Varmenteen avulla varmentaan varmenteen haltijan henkilöllisyys sekä varmenteeseen sisältyvien tietojen oikeellisuus, eheys ja alkuperäisyys. Allekirjoitusvarmenteella tehty sähköinen allekirjoitus sekä vahvan sähköisten tunnistamisen välineen avulla tehty henkilön vahva sähköinen tunnistaminen antavat kansalaisille mahdollisuuden turvalliseen, ajasta ja paikasta riippumattomaan ja joustavaan verkkoasiointiin. Allekirjoitusvarmenteen ja vahvan sähköisen tunnistuspalvelun tarjoajia valvoo Suomessa Traficom.

Tämän kansalaisvarmenteen myöntämistä kuvaavan varmennepolitiikan on rekisteröinyt Digi- ja väestötietovirasto.

Tämä varmennepolitiikka kuvaa Asetukseen perustuvan, vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaisen sähköisen allekirjoituksen allekirjoitusvarmenteen myöntämiseen, tuottamiseen ja vastuun jakoon liittyviä yksityiskohtaisia vaatimuksia. Tämän varmennepolitiikan mukaisesti myönnettäviä allekirjoitusvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka vastaavat hyväksytyiltä sähköisten allekirjoitusten varmenteilta ja luontivälineiltä edellytettäviä vaatimuksia kuten Asetuksen 28 artiklassa säädetään. Tunnistusvarmenteen taso täyttää Asetuksen ja sen nojalla annetun varmuustasoasetuksen mukaisesti vaatimustason ”korkea”.

Tämä asiakirja kuvaa myös kansalaisvarmenteeseen sisältyvän, vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaisen vahvan sähköisen tunnistamisen välineenä tarjottavan tunnistusvarmenteen myöntämiseen, tuottamiseen ja tietojen tallentamiseen liittyviä ratkaisuja ja menettelytapoja allekirjoitusvarmenteen tuotantoympäristön vaatimuksia noudattaen.

Kansalaisvarmenne koostuu varmenneparista, jolla on kaksi toisistaan poikkeavaa käyttötarkoitusta. Todentamis- ja salausvarmenne täyttää vahvan sähköisen tunnistamisvälineen vaatimukset. Yksinomaan allekirjoituksen toteuttamiseen tarkoitettu allekirjoitusvarmenne täyttää allekirjoitusvarmenteen vaatimukset. Varmenteen hakijan henkilöllisyyden oikeellisuuden takaa Digi- ja väestötietovirasto.



Varmenteiden myöntämiseen sekä peruuttamiseen liittyvää lokidataa säilytetään vähintään seitsemän (7) vuotta varmenteen voimassaoloajan jälkeen.

6.2 Varmennepalvelut

Varmenne on sähköinen todistus, joka liittää allekirjoituksen todentamistiedot allekirjoittajaan ja vahvistaa varmenteen haltijan henkilöllisyyden. Varmenteen tiedot on sähköisesti allekirjoitettu varmentajan yksityisellä avaimella. Tämän varmennepolitiikan mukainen varmenne perustuu julkisen avaimen järjestelmään ja menetelmiin. Tämän varmennepolitiikan mukaisten varmenteiden tietosisältö on määritelty Digi- ja väestötietoviraston varmennepalveluista annetussa laissa (661/2009).

Tämän varmennepolitiikan mukainen kansalaisvarmenne voidaan myöntää Suomen kansalaiselle tai kotikuntalain (201/1994) mukaisesti Suomessa vakinaisesti asuvalle ulkomaalaiselle, jonka henkilötiedot on talletettu väestötietojärjestelmään.

Varmentajana toimiva Digi- ja väestötietovirasto yksilöi varmenteen haltijan sähköisen asiointitunnuksen (SATU) avulla, joka on myös osa varmenteen tietosisältöä. Sähköinen asiointitunnus on sähköistä asiointia varten erikseen luotu Digi- ja väestötietoviraston varmennepalveluista annetussa laissa (661/2009) määritelty tekninen tunnistetieto, joka ei sisällä henkilöön liittyviä tunnistetietoja.

Kansalaisvarmenne voidaan myöntää ja tallettaa erilaisille viranomaisen myöntämille teknisille alustoille eli mikrosiruille kuten henkilökortille. Tämä varmennepolitiikka on yhteinen kuvaus näillä eri teknisillä alustoilla oleville kansalaisvarmenteille.

Digi- ja väestötietoviraston varmennepolitiikalla ja varmennuskäytännöllä on molemmilla yksilöivä tunnuksensa (OID).

Digi- ja väestötietoviraston allekirjoitusvarmenteiden myöntäminen on tässä asiakirjassa jaoteltu vaatimusten luokittelusyistä seuraaviin osapalveluihin:

Rekisteröintipalvelu: Rekisteröintipalvelussa todennetaan allekirjoittajan henkilöllisyys ja mahdolliset häneen liittyvät erityiset attribuutit, jotka välitetään varmenteiden luomispalveluun.

Rekisteröintipalvelu sisältää toimintana myös asiakkaan itsensä tai jonkin muun kuin varmentajan generoiman avaimen toimittamisen. Digi- ja väestötietoviraston rekisteröintipalvelussa ei käsitellä muita kuin sen itsensä tuottamat avainparit.

Kansalaisvarmenteen rekisteröinti tapahtuu noudattaen lain väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista mukaista menettelytapaa. Tarkempi menettelytapa kuvataan kyseessä olevaa teknistä alustaa kuvaavassa varmennuskäytännössä.

Varmenteiden luomispalvelu: Varmenteiden luomispalvelussa luodaan ja allekirjoitetaan varmenteet, jotka perustuvat rekisteröintipalvelussa todennettuun henkilöllisyyteen ja muihin attribuutteihin.

Jakelupalvelu: Jakelupalvelun kautta varmenteet jaetaan allekirjoittajille sekä asetetaan varmenteeseen luottavien osapuolten saataville, jos allekirjoittajalta saadaan



siihen lupa. Lisäksi palvelussa asetetaan varmentajan käyttöehdot sekä kaikki julkaistut varmennepolitiikkoja ja varmennuskäytäntöä koskevat tiedot tilaajien ja varmenteeseen luottavien osapuolten saataville. Digi- ja väestötietovirasto toimittaa tiedot saataville. Hakemistopalvelu on julkinen Internet-palvelu, josta on saatavilla kaikki varmentajan myöntämät tunnistusvarmenteet sekä varmentajan varmenteet sekä sulkulista. Hakemistopalvelu on saatavissa osoitteesta <ldap://ldap.fineid.fi>.

Peruutustenhallintapalvelu: Peruutustenhallintapalvelu sulkee varmenteet, jotka varmenteen haltija haluaa suljettavaksi ennen varmenteen voimassaoloajan päättymistä.

Peruutusten hallintapalvelussa käsitellään peruuttamispyynnöt ja -ilmoitukset, ja määritetään tarvittavat toimet käsittelyn perusteella. Palvelun tulokset jaetaan sulkulistan välityksellä.

Sulkutilasta tiedottava palvelu:

Sulkutilasta tiedottavan palvelun kautta annetaan varmenteiden sulkutilatietoja varmenteeseen luottaville osapuolille. Palvelussa voidaan käyttää varmenteiden sulkulistoja tai reaaliaikaista yksittäisten tilatietojen välittämistä. Digi- ja väestötietovirasto ilmoittaa tiedot sulkupalveluun varmenteeseen luottavien osapuolten saataville. Tilatietoja päivitetään tietyin väliajoin, joka on yksityiskohtaisesti kuvattu varmennuskäytäntöasiakirjassa.



Allekirjoituksen luomisvälineen tarjoaminen allekirjoittajalle:

Allekirjoituksen luomisväline valmistetaan ja toimitetaan allekirjoittajille. Toimikortin tai mikrosirun valmistaja ja yksilöijä toimii varmenteen, siihen liittyvien avainparien ja aktivointitietojen osalta varmentajan toimeksiannosta ja vastuulla ja yhteistyösopimuksen mukaisesti. Toimikortit ja mikrosirut yksilöidään rekisteröijän toimittamien tietojen mukaisesti.

Käytetyn palvelujaottelun ainoa tarkoitus on selventää menettelytapavaatimuksia. Tässä kuvauksessa ei rajoiteta varmentajan palvelutoteutuksen jaottelua.

6.2.1 Varmenteeseen luottava osapuoli

Varmenteeseen luottava osapuoli on henkilö tai organisaatio, joka luottaa varmenteen tietoihin ja joka käyttää varmennetta todentamiseen, tiedon salaukseen ja sähköiseen allekirjoitukseen. Varmenteeseen luottavan osapuolen on tarkastettava, että käytettävä varmenne on voimassa.

6.3 Varmennepolitiikka ja varmennuskäytäntö

Tässä kohdassa kuvataan varmennepolitiikan ja varmennuskäytännön välistä suhdetta. Varmennepolitiikan muotoa tai varmennuskäytännön erittelyjä koskevia rajoituksia ei sovelleta tässä luvussa.

6.3.1 Tarkoitus

Varmennepolitiikka, jonka tunnus ilmoitetaan varmenteessa, kertoo yleisellä tasolla varmennustoiminnan pääperiaatteet. Varmennuskäytännössä kerrotaan varmennetoiminnan, erityisesti luomisen ja ylläpitämisen osalta vaadittavat yksityiskohtaiset toteuttamiseen liittyvät käytännöt ja menetelmät sen osalta, kuinka varmennepolitiikassa esitetyt vaatimukset täytetään.

Tässä asiakirjassa määritetään varmennepolitiikka, joilla täytetään allekirjoitusvarmenteita koskevat Asetuksessa säädetyt vaatimukset. Tässä asiakirjassa kuvataan myös, kuinka vahvan sähköisen tunnistamisvälineen myöntäjä toimii laskiessaan liikkeelle vahvan sähköisen tunnistuksen välineitä. Varmentajana toimiva Digi- ja väestötietovirasto määrittää varmennuskäytännöissään, kuinka nämä vaatimukset täytetään.

Digi- ja väestötietovirasto noudattaa tätä varmennepolitiikkaa myöntäessään kansalaisvarmenteen. Varmenteen haltijoiden ja varmenteeseen luottavien osapuolien tulee toimia tämän varmennepolitiikan mukaisesti.

Tämän varmennepolitiikan mukaista kansalaisvarmennetta voidaan käyttää henkilön vahvaan sähköiseen tunnistamiseen, tiedon salaukseen ja sähköiseen allekirjoitukseen. Kansalaisvarmennetta voidaan käyttää käyttötarkoituksensa mukaisesti rajoituksitta sekä hallinnollisissa että yksityisten organisaatioiden tarjoamissa sovelluksissa ja palveluissa.

Varmennepolitiikka ja varmennuskäytäntö sisältävät vaatimuksia, jotka koskevat varmentajan, rekisteröijän, varmenteen haltijan ja varmenteeseen luottavan osapuolen



velvoitteita sekä lainsäädäntöön ja mahdollisten erimielisyyksien ratkaisuun liittyviä kysymyksiä.

Varmentajana toimiva Digi- ja väestötietovirasto vaihtaa varmennepolitiikkaa koskevan yksilöivän tunnuksen, jos se muuttaa varmennepolitiikkaansa sovellettavuuden osalta.

6.3.2 Yksityiskohtaisuus

Varmennepolitiikka kuvaa varmentajan toiminnan yleiset vaatimukset. Varmennuskäytännössä kuvataan varmennepolitiikkaa yksityiskohtaisemmin menettelytavat, joita varmentaja toteuttaa varmenteiden myöntämisessä ja muussa hallinnoinnissa. Varmennuskäytännössä määritellään, kuinka varmentaja täyttää varmennepolitiikassa määritetyt tekniset sekä organisaatioon ja menettelyihin liittyvät vaatimukset.

Varmentajana toimiva Digi- ja väestötietovirasto on laatinut sisäisten toimintojensa sekä ulkoistettujen toimintojensa ohjaamista varten asiakirjoja, jotka eivät ole julkisia.

Tämän varmennepolitiikan on rekisteröinyt Digi- ja väestötietovirasto. Digi- ja väestötietovirasto on julkista luottamusta nauttivaa valtakunnallista henkilörekisteriä ylläpitävä viranomaislain (661/2009) mukainen tehtävä on tuottaa varmennettuja sähköisen asioinnin palveluita.

6.3.3 Lähestymistapa

Varmennepolitiikka- ja varmennuskäytäntöasiakirjat on laadittu erilaisia käyttötarkoituksia varten. Varmennepolitiikka on yleiskuvaus varmentajan toiminnasta. Varmennuskäytäntö kuvaa varmentajan toiminnan yksityiskohdat organisaatorakenteen, toimintatapojen, toimitilojen ja tietoteknisen ympäristön mukaisesti.

6.3.4 Muut varmentajan julkaisemat asiakirjat

Varmennepolitiikan ja varmennuskäytännön lisäksi varmentaja voi julkaista muita varmennetoimintaa ohjaavia asiakirjoja. Tällaisia asiakirjoja ovat muun muassa käyttöohjeet ja varmennetoiminnan yleisesitykset kuluttajia, asiakasorganisaatioita ja palvelunrakentajien tarpeita varten.

Kansalaisvarmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja ennen kansalaisvarmennehakemuksen allekirjoittamista annettavissa yleisissä käyttöohjeissa, jotka muodostavat kansalaisvarmenteen hakijan kanssa tehtävän sopimuksen. Hakemusasiakirjassa on tiedot kummankin osapuolen oikeuksista ja velvollisuuksista. Kun kansalaisvarmenteen hakija hakee varmennetta, hän hyväksyy samalla yleiset käyttöehdot.

Hakemusasiakirjassa ja käyttöohjeissa mainitaan selkeästi, että kansalaisvarmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy tunnustusvarmenteen luomisen ja julkaisun julkisessa hakemistossa. Samalla hakija hyväksyy kansalaisvarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii kansalaisvarmenteen ja PIN-tunnusten säilyttämisestä sekä mahdollisen väärinkäytön tai varmenteiden/mikrosirun katoamisen ilmoittamisesta.



Varmennekuvaus on varmentajan käyttöehtojen osa, joka liittyy julkisen avaimen järjestelmän toimintaan. Varmentajana toimiva Digi- ja väestötietovirasto julkaisee varmennekuvauksen sekä varmenteen hakijan että varmenteeseen luottavien osapuolien saataville.

6.4 Varmenteen hakija

Varmenteen hakija voi hakea varmennetta omissa nimissään tapahtuvaa käyttöä var-
ten tai mahdollisesti yhteisön jäsenenä allekirjoittaessaan asiakirjoja yhteisön ni-
missä. Tämä ero on kuvattu tässä asiakirjassa silloin, kun sen erottelemine on vält-
tämätöntä. Varmennetta haettaessa kuitenkin tunnistetaan aina yksityinen henkilö
henkilökohtaisella tavalla.

Kansalaisvarmenteen hakija on aina henkilökohtaisella tavalla tunnistettu yksityishen-
kilö.

7 Johdanto varmennepolitiikkoihin

7.1 Yleistä

Varmennepolitiikalla tarkoitetaan periaatteita, jotka osoittavat tietyn varmenteen so-
veltuuden tietyille yhteisölle. Varmennepolitiikassa on kuvattu myös yhteisesti so-
vellettavat turvallisuusvaatimukset.

Tässä asiakirjassa menettelytapavaatimukset määritellään varmennepolitiikkojen mu-
kaan. Nämä varmennepolitiikat koskevat Asetuksessa määritellyn mukaisia allekirjoit-
usvarmenteita.

Tämän asiakirjan mukaisesti myönnetty varmenteet sisältävät varmennepolitiikan
OID-yksilöintitunnuksen, jonka avulla varmenteeseen luottavat osapuolet voivat mää-
rittää varmenteen käyttökelpoisuuden ja luotettavuuden tiettyyn käyttötarkoitukseen.
Tässä asiakirjassa määritetään:

yleisölle myönnettäviä allekirjoitusvarmenteita koskeva varmennepolitiikka, jossa
edellytetään turvallisten allekirjoituksen luomisvälineiden käyttöä.

Tässä asiakirjassa yleisökäsitteen tulkinta määräytyy tilanteeseen sovellettavan kan-
sallisen lainsäädännön mukaan. Varmentaja voidaan katsoa yleisölle varmenteita
myöntäväksi, jos kyseisten varmenteiden käyttöä ei ole rajoitettu osanottajien välisin
vapaaehtoisin yksityisoikeudellisin sopimuksin.

Digi- ja väestötietovirasto laatii erillisen varmennepolitiikan jokaiselle myöntämälleen
varmennetyypille sekä varmennuskäytännön jokaista eri teknistä alustaa koskien.
Varmennepolitiikka kuvaa varmennetyypeittäin käytettävät menettelytavat, käyttöeh-
dot, vastuiden jaon ja muut varmenteen käyttöön liittyvät näkökulmat yleisellä tasolla.
Varmennuskäytäntö kuvaa noudatettavat menettelytavat yksityiskohtaisella tasolla.

Tämän varmennepolitiikan nimi on Varmennepolitiikka Digi- ja väestötietoviraston
kansalaisvarmennetta varten, jonka OID on 1.2.246.517.1.10.302 ja
1.2.246.517.1.10.352.





Tämä varmennepolitiikka viittaa varmentajan varmennepolitiikkaan, jonka OID on 1.2.246.517.1.10.301 ja 1.2.246.517.1.10.351. Digi- ja väestötietovirasto noudattaa Asetuksen N:o (EU) 910/2014 luottamuspalveluiden mukaista yleisölle myönnettäviä allekirjoitusvarmenteita koskevaa varmennepolitiikkaa. Asiakirjan viitetiedot ovat ETSI EN 319 411-1 [2] QCP-n-qscd mukaisesti; OID: 0.4.0.194112.1.2. Tämän varmennepolitiikan mukaisesti myönnettäviä allekirjoitusallekirjoitusvarmenteita voi käyttää sellaisten sähköisten hyväksytyjen allekirjoitusten vahvistamisessa, jotka vastaavat Asetuksessa kuvattuja sähköisten allekirjoitusten hyväksytyjä varmenteita ja luontivälaineitä kuten Asetuksen 28 artiklassa säädetään.

Sekä varmennepolitiikka että varmennuskäytäntö ovat saatavilla osoitteesta www.dvv.fi/cps_

Tämän varmennepolitiikan on rekisteröinyt Digi- ja väestötietovirasto. Se on henkilörekisteriä ylläpitävä viranomainen, jonka Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) mukainen tehtävä on tuottaa muiden tehtäviensä lisäksi varmennettuja sähköisen asiointin palveluita. Digi- ja väestötietovirasto vastaa tämän varmennepolitiikan hallinnoinnista ja päivityksistä.

Tätä varmennepolitiikkaa koskevat kysymykset lähetetään seuraavaan osoitteeseen:

Digi- ja väestötietovirasto

PL 123 (Lintulahdenkuja 2)

Puh. +358 295 535 001

00531 Helsinki

Fax. +358 9 876 4369

Y-tunnus: 0245437-2

kirjaamo@dvv.fi

Varmennepolitiikkaan liittyviin kysymyksiin sekä näihin asiakirjoihin liittyvästä viestinnästä vastaa Digi- ja väestötietoviraston kirjaamo, sähköpostiosoite kirjaamo@dvv.fi.

Digi- ja väestötietovirasto (DVV) Varmennepalvelut

PL 123

00531 Helsinki

www.dvv.fi

Digi- ja väestötietovirasto omistaa kaikki kansalaisvarmenteisiin ja dokumentaatioon liittyvät tiedot teknisten toimitussopimusten mukaisesti. Digi- ja väestötietovirasto omistaa täydet omistus- ja käyttöoikeudet tähän varmennepolitiikkaan.



7.2 Yksilöintitunnukset

Digi- ja väestötietovirasto noudattaa Asetuksen N:o (EU) 910/2014 luottamuspalveluiden mukaista yleisölle myönnettäviä allekirjoitusvarmenteita koskevaa varmennepoliitiikkaa. Asiakirjan viitetiedot ovat ETSI EN 319 411-1 [2] QSCD mukaisesti; OID: 0.4.0.194112.1.2. Tämän varmennepoliitiikan mukaisesti myönnettäviä allekirjoitusvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka vastaavat Asetuksessa kuvattuja sähköisten allekirjoitusten hyväksytyjä varmenteita ja luontivälineitä kuten Asetuksen 28 artiklassa säädetään.

Tämän varmennepoliitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta allekirjoitusvarmenteele asettamat vaatimukset.

Tämä varmennepoliitiikka astuu voimaan 13.3.2023.

Varmentaja sisällyttää noudattamiensa varmennepoliitikkojen OID-yksilöintitunnukset myös varmenteen hakijoiden ja varmenteeseen luottavien osapuolten saataville asetettaviin käyttöehtoihin ja tällä tavoin ilmaisee noudattavansa kyseistä varmennepoliitiikkaa.

7.3 Käyttäjyhteisö ja sovellettavuus

7.3.1 QCP-n QSCD -varmennepoliitiikka

Digi- ja väestötietovirasto noudattaa EU-asetuksen N:o (EU) 910/2014 luottamuspalveluiden mukaista yleisölle myönnettäviä allekirjoitusvarmenteita koskevaa varmennepoliitiikkaa. Asiakirjan viitetiedot ovat ETSI EN 319 411-1 [2] QSCD mukaisesti; OID: 0.4.0.194112.1.2. Tämän varmennepoliitiikan mukaisesti myönnettäviä allekirjoitusvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka vastaavat Asetuksessa kuvattuja sähköisten allekirjoitusten hyväksytyjä varmenteita ja luontivälineitä.

Tämän varmennepoliitiikan mukaisesti myönnettäviä allekirjoitusvarmenteita voi käyttää sellaisten sähköisten allekirjoitusten vahvistamisessa, jotka vastaavat hyväksytyiltä sähköisten allekirjoitusten varmenteilta ja luontivälineiltä edellytettäviä vaatimuksia kuten Asetuksen 28 artiklassa säädetään.

7.4 Vaatimustenmukaisuus

7.4.1 Yleistä

Varmentajalla on oikeus käyttää allekirjoitusvarmennepoliitiikan yksilöintitunnusta vain, jos varmentaja ilmaisee noudattavansa yksilöityä allekirjoitusvarmennepoliitiikkaa ja asettaa pyynnöstä tilaajan ja varmenteeseen luottavien osapuolten saataville todisteita vaatimustenmukaisuudesta.

Vaatimustenmukaisuuden osoittamiseen vaadittavat keinot voivat vaihdella varmentajan sijoittautumisvaltion lainsäädännön mukaan. Varmentajan



vaatimustenmukaisuus tarkistetaan säännöllisesti sekä aina, kun varmentajan toiminta muutetaan merkittävästi.

7.4.2 QCP n + QSCD -allekirjoitusvarmennepolitiikka

Vaatimusten mukaisen varmentajan on osoitettava, että

- a) se täyttää sille määritellyt vaatimukset
- b) se on ottanut käyttöön hallintakeinot, jotka täyttävät kaikki esitetyt vaatimukset.

8 Velvollisuudet ja vastuu sekä vastuunrajoitukset

Tämän kohdan vaatimuksia sovelletaan **QCP-n-qscd**-varmennepolitiikkaan, ellei muuta mainita.

8.1 Varmentajan velvollisuudet

Varmentaja varmistaa, että kaikki varmentajalle valittua varmennepolitiikkaa koskevat vaatimukset toteutetaan.

Varmentaja on vastuussa varmennepolitiikassa määrättyjen menettelyjen noudattamisesta, vaikka varmentajan toimintaa toteutettaisiin toimeksiantosopimuksin.

Varmentaja tarjoaa kaikki varmennepalvelu osa-alueet varmennuskäytännössään mainitun mukaisesti.

8.1.1 Varmentajan velvollisuudet

Digi- ja väestötietovirastolla on lakiin perustuva tehtävä toimia varmentajana.

Varmentaja noudattaa toiminnassaan voimassaolevaa lainsäädäntöä.

Varmentaja toimii huolellisesti, luotettavasti ja asianmukaisesti.

Varmentajalla on riittävät tekniset taidot ja taloudelliset voimavarat varmennetoiminnan asianmukaiseksi järjestämiseksi sekä mahdollisen vahingonkorvausvastuun kattamiseksi.

Varmentaja vastaa kaikista varmennetoiminnan osa-alueista, myös varmentajan apunaan käyttämien teknisten toimittajien tai henkilöiden, kuten rekisteröijien ja kortinvalmistajien tuottamien palveluiden ja tuotteiden luotettavuudesta ja toimivuudesta.

Varmentaja laatii ja ylläpitää varmennepolitiikkaa, joka kuvaa kansalaisvarmenteen myöntämisessä, ylläpidossa ja hallinnoinnissa käytettävät menettelytavat, käyttöehdot, vastuuden jaot ja muut kansalaisvarmenteen käyttöön liittyvät näkökulmat yleisellä tasolla.

Varmentaja laatii ja ylläpitää varmennuskäytäntöjä, jotka kuvaavat, miten varmentaja soveltaa varmennepolitiikkaa.

Varmentaja noudattaa varmennepolitiikkaa ja varmennuskäytäntöä.



Varmentaja julkaisee varmennepolitiikan ja varmennuskäytännön yleisesti saataville.

Varmentaja pitää palveluksessaan riittävästi henkilökuntaa, jolla on varmennepalvelujen tuottamisen edellyttämä asiantuntemus, kokemus ja pätevyys.

Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu oikeudettomalta käytöltä.

Varmentaja pitää yleisesti saatavilla kansalaisvarmennetta ja varmennetoimintaa koskevat tiedot, joiden perusteella varmentajan toiminta ja luotettavuus voidaan arvioida.

Varmentaja turvaa allekirjoituksen luomistietojen luottamuksellisuuden.

Varmentaja ei tallenna tai jäljennä allekirjoittajalle luovutettuja allekirjoituksen luomistietoja.

8.1.2 Rekisteröijää koskevat velvollisuudet

Rekisteröijä toimii varmentajan vastuulla ja lukuun sekä noudattaa varmentajan kanssa sovittuja rekisteröintiin liittyviä menettelytapoja.

Rekisteröijä noudattaa rekisteröinnin yhteydessä varmennepolitiikkaa ja varmennuskäytäntöä.

Rekisteröijä tunnistaa varmenteen hakijan henkilökohtaisesti ja luotettavasti varmennuskäytännössä kuvatulla tavalla siten, että hakijan henkilöllisyys ja muut varmenteen myöntämisessä tarpeelliset hakijan henkilöön liittyvät tiedot tulevat huolellisesti tarkastetuiksi.

Rekisteröijä huolehtii henkilötietojen huolellisesta käsittelystä ja luottamuksellisudesta.

Rekisteröijä antaa varmenteen hakijalle tiedot varmenteen käyttöehdoista.

8.2 Varmenteen hakijan velvollisuudet

Varmentaja velvoittaa sopimuksella varmenteenhakijaa noudattamaan kaikkia seuraavassa mainittavia velvollisuuksia. Jos allekirjoittaja ja varmenteen hakija ovat eri tahoja, varmenteen hakijan on saatettava allekirjoittajan tietoon kaikki allekirjoittajaan sovellettavat velvollisuudet.

Digi- ja väestötietoviraston myöntämän kansalaisvarmenteen käyttötarkoitus on määriteltävä kunkin varmennetyypin varmennepolitiikassa, varmennuskäytännössä sekä varmenteen haltijan käyttöohjeissa. Varmennetta saa käyttää vain sen käyttötarkoituksen mukaisesti sähköiseen allekirjoitukseen, todentamiseen tai tiedon salaamiseen.

Kansalaisvarmenteen haltija vastaa siitä, että kansalaisvarmennetta haettaessa ilmoitetut tiedot ovat oikeita.

Kansalaisvarmenteen haltija on vastuussa kansalaisvarmenteen käytöstä, kansalaisvarmenteella tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.



Allekirjoitusvarmenteen osalta noudatetaan, mitä Asetuksessa ja laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista on säädetty.

Kansalaisvarmenteen haltija säilyttää mikrosirulla olevat yksityiset avaimensa ja niiden käyttämiseen tarvittavat tunnusluvut erillään sekä pyrkii estämään yksityisten avaintensa katoamisen, joutumisen ulkopuolisten käsiin, muuttamisen tai luvattoman käytön. Mikrosirun luovuttaminen tai PIN-tunnuksen paljastaminen toiselle henkilölle esim. lainaamalla vapauttaa varmentajan ja kansalaisvarmenteeseen luottavan osapuolen kansalaisvarmenteen käyttämisestä mahdollisesti aiheutuvista vastuista.

Kansalaisvarmennetta käsitellään ja suojataan noudattaen samaa huolellisuutta kuin muita vastaavia mikrosiruja, kortteja tai asiakirjoja, kuten esimerkiksi luottokortteja, ajokorttia ja passia. Henkilökohtaiset PIN-tunnukset on säilytettävä fyysisesti eri paikassa kuin kansalaisvarmenteen ja yksityiset avaimet sisältävä mikrosiru.

Mikrosirun ja kortin häviämisestä tai väärinkäytön mahdollisuudesta on ilmoitettava viipymättä varmentajalle soittamalla maksuttomaan sulkupalveluun +358 800 162 622.

8.3 Tiedottaminen varmenteeseen luottaville osapuolille

Asetukseen perustuvaa, yleisölle allekirjoitusvarmenteita myöntävän varmentajan vastuuta sovelletaan osapuoliin, jotka perustellulla tavalla tukeutuvat varmenteeseen.

Tunnistusvarmenteet julkaistaan yleisesti saatavilla olevassa julkisessa hakemistossa ja suljetut kansalaisvarmenteet sulkulistalla, josta varmenteeseen luottavan osapuolen on tarkistettava sen voimassaolotieto. Varmenteen tilatieto voidaan tarkastaa myös OCSP-palvelusta.

Varmenteeseen luottavan osapuolen velvollisuus on varmistaa, että varmennetta käytetään sen käyttötarkoituksen mukaisesti. Allekirjoitusvarmenteen käyttötarkoitus on sähköinen allekirjoitus. Todentamis- ja salausvarmenteen käyttötarkoitus on henkilön todentaminen ja tiedon salaus.

Varmenteeseen luottavan osapuolen on noudatettava varmennepoliitikkaa ja varmennuskäytäntöä.

Kansalaisvarmenteeseen luottava osapuoli voi vilpittömässä mielessä luottaa kansalaisvarmenteeseen, kun hän on tarkistanut, että **kansalaisvarmenne on voimassa**. Kansalaisvarmenteeseen luottavalla osapuolella on velvollisuus tarkistaa varmenteen tilatieto. Kansalaisvarmenteen voimassaolon luotettavuuden varmistamiseksi kansalaisvarmenteeseen luottavan osapuolen on noudatettava alla esitettyjä sulkulistan tarkistustoimia, jos tilatieto varmistetaan sulkulistalta.

Jos kansalaisvarmenteeseen luottava osapuoli kopioi sulkulistan hakemistosta, sen on varmistettava sulkulistan aitous tarkistamalla sulkulistan varmentajan sähköinen allekirjoitus. Lisäksi on tarkistettava sulkulistan voimassaoloaika.

Mikäli uusinta sulkulistaa ei voida saada hakemistosta laitteiston tai hakemistopalvelun toimintahäiriön vuoksi, kansalaisvarmennetta ei pidä hyväksyä, mikäli viimeisen saadun sulkulistan voimassaoloaika on päättynyt. Kaikki kansalaisvarmenteen



hyväksymiset tämän voimassaoloajan jälkeen tapahtuvat kansalaisvarmenteeseen luottavan osapuolen omalla riskillä.

8.4 Vastuu

Yleisölle allekirjoitusvarmenteita myöntäviä varmentajia koskee Asetuksessa ja laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädetyn mukainen vastuu. Vahvan sähköisen tunnistamisvälineen tai -palvelun tarjoavia palveluntarjoajia koskee laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädetyn mukainen vastuu.

8.4.1 Varmentajan vastuut

Digi- ja väestötietovirasto vastaa varmentajana koko varmennejärjestelmän turvallisuudesta. Varmentaja vastaa toimeksiantona hankkimistaan palveluista samoin kuin olisi itse tuottanut palvelun.

Digi- ja väestötietovirasto vastaa siitä, että kansalaisvarmenne on luotu noudattaen väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa, laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, laissa sähköisestä asioinnista viranomaistoiminnassa ja varmennepolitiikassa sekä varmennuskäytännössä esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti. Digi- ja väestötietovirasto vastaa ainoastaan niistä tiedoista, jotka se on tallettanut kansalaisvarmenteeseen.

Digi- ja väestötietovirasto vastaa siitä, että kun kansalaisvarmennetta käytetään asianmukaisesti, se on käytettävissä luovutushetkestä koko sen voimassaoloajan. Kansalaisvarmenne on luovutettu henkilölle, joka on tunnistettu kansalaisvarmenteelta edellytettävällä tavalla. Varmenteen haltijalle on luovutettu ennen sopimuksen allekirjoitusta kansalaisvarmenteen käyttöön liittyvät käyttöohjeet ennen sopimuksen allekirjoittamista.

Allekirjoittaessaan kansalaisvarmenteen yksityisellä avaimellaan varmentaja vakuuttaa tarkistaneensa kansalaisvarmenteessa olevat henkilötiedot varmennepolitiikassa ja varmennuskäytännössä esitettyjen menettelyjen mukaisesti.

Varmentaja vastaa siitä, että sulkulistalle viedään oikean henkilön kansalaisvarmenne ja että ne ilmestyvät tässä varmennepolitiikassa mainitussa ajassa sulkulistalle.

8.4.2 Rekisteröijän vastuut

Kansalaisvarmenteen rekisteröijänä toimii rekisteröintipiste, joka rekisteröi varmenteen hakijan varmentajana toimivan Digi- ja väestötietoviraston lukuun ja vastuulla. Rekisteröinnin osalta noudatetaan väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain ja vahvasta sähköisestä tunnistamisesta ja sähköisen allekirjoituslain vaatimuksia sekä henkilökorttilain vaatimuksia silloin, kun kansalaisvarmenne on henkilökortilla.



8.4.3 Kansalaisvarmenteen haltijan vastuut

Kansalaisvarmenne on haltijansa sähköinen henkilöllisyys eikä sitä tämän vuoksi saa luovuttaa toisen henkilön käytettäväksi

Kansalaisvarmenteen haltija on vastuussa sen käytöstä, sillä tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.

Mikrosirun sisältävän kortin jättäminen lukijalaitteeseen saattaa mahdollistaa kansalaisvarmenteen väärinkäytön. Lopettaessaan pääteistunnon tai jättäessään päätelaitteen valvomatta kansalaisvarmenteen haltijan vastuulla on poistaa kansalaisvarmenteen sisältävä mikrosiru lukijalaitteesta ja sulkea käytetyt sovellukset asianmukaisesti tai muuten katkaistava kansalaisvarmenteen käyttämiseksi tarvittava tekninen yhteys.

Kansalaisvarmenteen haltijan vastuu sen käyttämisestä päättyy, kun hän on ilmoittanut sulkupalveluun tarvittavat tiedot sen sulkemiseksi ja saatuaan puhelun vastaanotaneelta virkailijalta sulkemista koskevan ilmoituksen. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

8.4.4 Kansalaisvarmenteeseen luottavan osapuolen vastuut

Kansalaisvarmenteeseen luottava osapuoli ei voi luottaa siihen ja sähköisen allekirjoituksen oikeellisuuteen vilpittömässä mielessä, mikäli kansalaisvarmenteen voimassaoloa ei ole tarkastettu OCSP-palvelusta tai sulkulistalta. Jos varmenteen tilatietoa ei ole tarkastettu, kansalaisvarmenteen hyväksyminen vapauttaa Digi- ja väestötietoviraston vastuusta. Kansalaisvarmenteeseen luottavan osapuolen on tarkistettava, että myönnetty varmenne vastaa käyttötarkoitustaan siinä oikeustoimessa, jossa sitä on käytetty.

8.4.5 Vastuiden rajoitukset

Digi- ja väestötietovirasto ei vastaa PIN-tunnusten, aktivointitunnusluvun ja kansalaisvarmenteen haltijan yksityisten avainten paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu Digi- ja väestötietoviraston välittömästä toiminnasta.

Digi- ja väestötietovirasto vastaa kansalaisvarmenteen haltijalle ja kansalaisvarmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston välittömästä toiminnasta.

Digi- ja väestötietovirasto ei vastaa kansalaisvarmenteen haltijalle aiheutuneista välillisistä tai seurannaisvahingoista. Digi- ja väestötietovirasto ei myöskään vastaa kansalaisvarmenteeseen luottavan osapuolen tai kansalaisvarmenteen haltijan muun sopimuskumppanin mahdollisesti kärsimistä välillisistä tai seurannaisvahingoista.

Digi- ja väestötietovirasto ei vastaa yleisten tietoliikenneyhteyksien eikä tietoverkkojen, esimerkiksi Internetin toimivuudesta eikä siitä, jos oikeustoimen suorittaminen estyy kansalaisvarmenteen haltijan käyttämän laitteen tai ohjelmiston toimimattomuudesta eikä siitä, että kansalaisvarmennetta käytetään vastoin sen käyttötarkoitusta.

Varmentajalla on oikeus keskeyttää palvelu muutos- ja huoltotoimien ajaksi. Sulkulistaa koskevista muutoksista tai huoltotoimista ilmoitetaan etukäteen.



Varmentajalla on oikeus kehittää edelleen varmennepalvelua. Kansalaisvarmenteen haltijan tai kansalaisvarmenteeseen luottavan osapuolen on vastattava tämän vuoksi aiheutuvista omista kustannuksistaan eikä varmentaja ole velvollinen korvaamaan kansalaisvarmenteen haltijalle tai kansalaisvarmenteeseen luottavalle osapuolelle tällaisesta varmentajan kehittämistyöstä aiheutuvista kustannuksista.

Varmentaja ei vastaa varmennetta käytettäessä kansalaiselle ja organisaatiolle tarkoitetun varmenteeseen pohjautuvan verkkopalvelun tai sovelluksen virheistä tai niistä aiheutuvista kustannuksista.

8.4.6 Muut osapuolet

Kansalaisvarmenteeseen luottava osapuoli voi luottaa kansalaisvarmenteen ja sähköisen allekirjoituksen oikeellisuuteen, jos hän on tarkastanut, ettei varmenteen voimassaoloaika ole päättynyt eikä hänellä ole muita syitä perustellusti epäillä varmenteen käytön oikeellisuutta.

Varmentaja vastaa kansalaisvarmenteesta sen mukaisesti kuin varmentaja on sitoutunut tässä varmennepolitiikassa ja kansalaisvarmennetta koskevassa varmennuskäytännössä.

Varmennepalveluiden tuottamiseen liittyvä Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy varmenteen hakijan kanssa tehdyn palvelusopimuksen mukaisesti. Digi- ja väestötietovirastoa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) sovelletaan myös vahingonkorvauslakia (412/1974).

Sähköisestä henkilökortista on säädetty henkilökorttilaissa. Hallinnon asioinnista on säädetty myös sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003).

Digi- ja väestötietovirasto vastaa kansalaisvarmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston toiminnasta.

9 Varmentajan toimintaa koskevat vaatimukset

Tätä kohtaa sovelletaan yksilöityyn allekirjoitusvarmennepolitiikkaan QCP n + QSCD -allekirjoitusvarmennepolitiikkaan, ellei muuta mainita.

Varmentajan toteuttaa seuraavat vaatimukset täyttävät hallintakeinot.

Tämä asiakirja koskee allekirjoitusvarmenteita myöntävänä varmentajana toimivaa Digi- ja väestötietovirastoa. Tässä asiakirjassa kuvatun palvelun toteuttamiseen sisältyy rekisteröintipalvelujen tarjoaminen, varmenteiden luominen, varmenteiden jakelu, varmenteiden peruuttamisen hallinta ja sulkutilasta tiedottaminen. Jos vaatimus liittyy varmentajan tiettyyn palvelualueeseen, se kuvataan vastaavien alaotsikoiden alla. Mikäli seuraavassa ei yksilöidä palvelualueita tai jos mainitaan "varmentaja yleisesti", vaatimus koskee varmentajan yleistä toimintaa.

Näiden menettelytapavaatimusten tarkoituksena ei ole rajoittaa varmentajan palveluista veloittamista.



Esitettävät vaatimukset koskevat turvallisuustavoitteita sekä niiden saavuttamiseen käytettäviä hallintakeinoja, joiden osalta esitetään yksityiskohtaisia vaatimuksia, mikäli se on katsottu tavoitteiden täyttymisen kannalta tarpeelliseksi.

9.1 Varmennuskäytäntö

Varmentaja varmistaa, että se osoittaa varmennepalvelujen tarjoamisen edellyttämän luotettavuuden, joka on kuvattu Asetuksessa.

Tässä asiakirjassa kuvattuihin toimenpiteisiin liittyvä yksityiskohtainen menettely on kuvattu jokaista varmennetyyppiä ja tallennus-alustaa koskevassa varmennuskäytännössä.

9.2 Julkisen avaimen järjestelmässä käytettävien avainten elinkaaren hallinta

9.2.1 Varmentajan avaimen luominen

Varmenteiden luominen

Varmentaja varmistaa, että varmentajan avaimet luodaan turvallisissa olosuhteissa, jotka on kuvattu Asetuksessa.

Varmentaja luo tarkoituksenmukaisen ajan ennen varmentajan allekirjoitusavaimen voimassaolon päättymistä (esimerkiksi varmentajan varmenteessa ilmoitettuna ajankohtana) uuden avainparin varmenteen allekirjoittamiseen ja tekee kaikki tarpeelliset toimet, ettei kyseiseen varmentajan avaimeen mahdollisesti luottavien yhteisöjen toimintaan aiheutuisi häiriöitä. Uusi varmentajan avain luodaan ja sen jakelu toteutetaan näiden menettelytapojen mukaisesti.

Nämä toimet tehdään riittävän ajoissa, jotta kaikki varmentajaan jossakin suhteessa toimivat osapuolet (allekirjoittajat, varmenteen hakijat, varmenteeseen luottavat osapuolet, ylemmällä tasolla toimivat varmentajat) saavat ajoissa tiedon varmentajan avainparin vaihtamisesta ja jotta ne voivat toteuttaa toiminnan häiriöttömän jatkumisen kannalta tarvittavat toimet. Tämä ei koske varmentajaa, joka lopettaa toimintansa ennen sen oman varmentajan varmenteen viimeistä voimassaolopäivää.

9.2.2 Varmentajan avaimen tallennus, varmuuskopiointi, ja palauttaminen

Varmenteiden luominen

Varmentaja varmistaa, että varmentajan yksityisten avainten luottamuksellisuus ja eheys säilyvät Asetuksen mukaisesti.

Digi- ja väestötietovirasto luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimet.

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa, jotka täyttävät turvallisuusstandardin vaatimukset.



Varmentaja huolehtii siitä, että varmentajan yksityiset avaimet on suojattu paljastumisel-
seltä ja luvattomalta käytöltä. Varmentajan yksityisistä avaimista otetaan varmuusko-
pio kriittisen tietoturvallisuuden edellyttämällä tavalla.

Yksityisen avaimen luontiin ja käyttöön liittyvään ympäristöön vaaditaan vähintään
kahden henkilön samanaikainen läsnäolo tai toiminnan aktivoiminen.

Digi- ja väestötietoviraston kansalaisvarmenteessa olevista yksityisistä avaimista ei
luoda kopiota.

9.2.3 Varmentajan julkisen avaimen jakelu

Varmenteiden luominen ja jakelu

Kansalaisvarmenteen luomisen yhteydessä mikrosirun julkisia avaimia käyttäen suo-
ritetaan varmenteen luontipyyntö, jossa varmenteen hakijan rekisteröintitiedot yhdis-
tetään kyseessä olevaan julkiseen avaimeseen.

Kansalaisvarmentajan julkinen avain on osa varmentajan varmennetta. Kansalaisvar-
menne sisältää varmenteen haltijan julkisen avaimen.

Varmentajan varmenne on saatavilla julkisessa hakemistossa. Jos kansalaisvar-
menne sijaitsee toimikortilla, varmentajan varmenne sijoitetaan myös toimikortin mik-
rosirulle.

Varmentajan varmenne sisältää varmentajan julkisen avaimen. Varmentajan var-
menne talletetaan julkiseen hakemistoon. Varmenteen haltijan varmenne talletetaan
niin ikään julkiseen hakemistoon. Varmentajan varmenne on saatavilla varmentajan
julkisesta hakemistosta sekä varmentajan www-sivuilta.

Varmentaja arkistoi kaikki varmentamansa julkiset avaimet.

9.2.4 Vara-avainjärjestelmä

Digi- ja väestötietoviraston kansalaisvarmenteessa olevista yksityisistä avaimista ei
luoda kopiota.

9.2.5 Varmentajan avaimen käyttö

Varmentajan vastaa siitä, että varmentajan yksityisiä allekirjoitusavaimia käytetään
ainoastaan käyttötarkoituksensa mukaisesti.

Varmentajan varmenne:

Käyttötarkoitus: Varmenteiden ja sulkulistojen allekirjoitus. Tekninen kuvaus on FI-
NEID -määrityksissä.

9.2.6 Varmentajan avaimen elinkaaren päätyminen

Varmentajan varmistaa, ettei varmentajan yksityisiä allekirjoitusavaimia käytetä ni-
den elinkaaren päättymisen jälkeen Asetuksen mukaisesti.



9.2.7 Varmenteiden allekirjoittamisessa käytettävän salauslaitteiston elinkaaren hallinta

Varmentaja varmistaa salauslaitteiston turvallisuuden koko sen elinkaaren ajan jälkeen Asetuksen mukaisesti.

9.2.8 Varmentajan tarjoamat allekirjoittajan avaimen hallintapalvelut

Varmentaja varmistaa, että kaikki sen luomat allekirjoittajan avaimet luodaan turvallisesti ja että allekirjoittajan yksityisen avaimen luottamuksellisuus on turvattu Asetuksen mukaisesti.

Varmenteiden luominen

Kansalaisvarmenteen allekirjoittamiseen käytetty varmentajan yksityinen avain sekä sitä vastaava julkinen avain ovat vähintään 4096-bittisiä RSA-avaimia.

Kansalaisvarmenteen haltijan yksityiset ja julkiset avaimet ovat vähintään 3072-bittisiä RSA-avaimia ja 384-bittisiä ECC-avaimia.

Varmenteen tietosisällössä käyttötarkoituksen määräävä kenttä määrittelee varmenteisiin liittyvän avaimen käyttötarkoituksen. Avaimen käyttö rajataan käytettäväksi vain ilmoitettuun käyttötarkoitukseensa.

Varmentajan varmenne:

Käyttötarkoitus: Varmenteiden ja sulkulistojen allekirjoitus. Tekninen kuvaus on FI-NEID S2 -määrityksissä www.dvv.fi/.

Varmenteen haltijan todentamis- ja salausvarmenne:

Käyttötarkoitus: Sähköisen henkilöllisyyden todentaminen tai tiedon salaus.

Varmenteen haltijan allekirjoitusvarmenne:

Käyttötarkoitus: Sähköinen allekirjoitus

9.2.9 Turvallisen allekirjoituksen luomisvälineen valmistaminen

Jos varmentaja myöntää turvallisia allekirjoituksen luomisvälineitä (QSCD), varmentajan on varmistettava sen turvallinen toteuttaminen Asetuksen mukaisesti.

Erillisyyks voidaan saada aikaan varmistamalla, että aktivointitietojen jakelu ja turvallisen allekirjoituksen luomisvälineen toimittaminen tapahtuvat eri aikoina tai eri reittejä.

Turvallisen allekirjoituksen luomisvälineen valmistamista koskevat edellä luetellut vaatimukset voidaan täyttää esimerkiksi käyttämällä soveltuvaa suojausprofiilia, joka on määritelty ISO/IEC 15408 -standardin mukaisesti tai vastaavasti.



9.3 Julkisen avaimen järjestelmässä käytettävien varmenteiden elinkaaren hallinta

9.3.1 Allekirjoittajan rekisteröinti

Varmentaja varmistaa, että allekirjoittajat tunnistetaan ja todennetaan asianmukaisesti ja että allekirjoittajan varmennepyynnöt ovat virheettömiä, paikkansapitäviä ja jotka perustuvat asianmukaiseen valtuutukseen Asetuksen mukaisesti.

Kansalaisvarmenteen hakijan oikeudet ja velvollisuudet on mainittu hakemusasiakirjassa ja yleisissä käyttöehdoissa, jotka muodostavat varmenteen hakijan kanssa tehtävän sopimuksen. Hakemusasiakirjassa on tiedot kummankin osapuolen oikeuksista ja velvollisuuksista.

Hakemusasiakirjassa ja käyttöehdoissa mainitaan selkeästi, että kansalaisvarmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy varmenteen luomisen ja julkaisun julkisessa hakemistossa. Samalla hakija hyväksyy kansalaisvarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii kansalaisvarmenteen ja niiden PIN-tunnusten säilyttämisestä sekä mahdollisen väärinkäytön tai kortin katoamisen ilmoittamisesta.

Kansalaisvarmenteen hakija vastaa siitä, että kaikki kansalaisvarmenteen kannalta olennaiset tiedot, jotka kansalaisvarmenteen hakija on antanut varmentajalle tai rekisteröijälle, ovat oikeita. Kansalaisvarmenteen haltijan on käytettävä kansalaisvarmennetta vain sen käyttötarkoitusten mukaisesti.

Kun varmentaja myöntää kansalaisvarmenteen, se samalla hyväksyy varmennehakemuksen.

Varmentaja vastaa myöntäessään kansalaisvarmenteen, että sen tietosisältö on oikea sen luovuttamishetkellä.

Kansalaisvarmenteella olevat tiedot määrittelevät kansalaisvarmenteen haltijan yksikäsitteisesti. Varmentaja selvittää tarvittaessa varmenteen hakijan virallisen henkilöllisyyden.

Kansalaisvarmenteeseen liittyvät, mikrosirulla tai muussa turvallisessa ympäristössä luodut yksityiset avaimet toimitetaan kansalaisvarmenteen hakijalle luovutuksen yhteydessä.

Kansalaisvarmenteen hakijalle korostetaan varmenteen luovutushetkellä, että yksityisistä avaimista ei ole eikä niistä voi myöhemminkään valmistaa kopiota.

Kansalaisvarmenne voidaan noutaa henkilökohtaisesti rekisteritoimipisteestä.

Kansalaisvarmenteen haltijan vastuulla on estää hänelle kuuluvien yksityisten avaintensa ja niihin liittyvien aktivointitunnusten käyttäminen käyttööheitojen vastaisella tavalla huolehtimalla niistä käyttöehdoissa mainitulla tavalla.

Digi- ja väestötietoviraston kansalaisvarmenteen haltijan avainpari luodaan turvatiiloissa. Julkista avainta käytetään varmenteen luomiseen ja yksityinen avain säilytetään luku- ja kirjoitusuojattuna mikrosirulla.



Henkilökortin käyttö sähköisessä asiointissa edellyttää aktivointia aktivointitunnusluvun avulla. Aktivointitunnusluvun avulla käyttäjä pystyy aktivoimaan saamansa henkilökortin. Kun henkilökorttia käytetään ensimmäisen kerran sähköisessä asiointissa esimerkiksi omalla kotitietokoneellaan, käynnistetään kortinlukijaohjelmiston toimesta automaattisesti henkilökortin aktivointiprosessi. Tämän prosessin aikana käyttäjältä ensin kysytään aktivointitunnusluku, jonka jälkeen käyttäjä voi aktivoida ja määritellä omat, henkilökohtaisen PIN-tunnuslukunsa. Aktivointiprosessin jälkeen käyttäjä pystyy käyttämään henkilökorttiaan sähköisessä asiointissa.

Aktivoituja tunnuslukuja on kaksi. Perustunnusluku, jonka avulla käyttäjä kontrolloi henkilökortin ylläpitoa ja sähköistä tunnistautumista. Allekirjoitustunnusluku, jonka avulla käyttäjä voi tehdä sähköisen allekirjoituksen. Mikäli käyttäjä antaa tunnusluvun viisi kertaa väärin, kortti lukittuu eikä tunnusluvun suojaamaa toimintoa voi enää käyttää. Perustunnusluvun lukittuminen estää kaikkien tunnusluvun suojaamien sovellusten käytön. Allekirjoitustunnusluvun lukittuminen estää sähköisen allekirjoituksen käytön. Lukkiutuneet tunnusluvut vapautetaan aktivointitunnusluvulla.

Kortinvalmistaja luo avainten käytön mahdollistavat aktivointitiedot.

Aktivointitunnukset on suojattu niin, ettei niitä voi lukea tai kopioida kortilta. Varmenteen haltijan vastuulla on suojata avaintensa käyttö huolehtimalla mikrosirustaan tai kortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla.

Kansalaisvarmenteen käyttämiseksi tarvittavia aktivointitunnuksia käsitellään turvallisuuden takaamiseksi siten, etteivät ne ole yhtä aikaa samassa paikassa ennen toimintusta ja toimituksessa varmenteen hakijalle.

Kansalaisvarmenteen haltija voi ladata Digi- ja väestötietoviraston www-sivuilta kortinlukijaohjelmiston, jolla kansalaisvarmennetta voidaan käyttää sähköisissä asiointipalveluissa.

Kansalaisvarmenteen hakija voi halutessaan tallettaa sähköpostiosoitteen sekä kansalaisvarmenteeseen että väestötietojärjestelmään. Sähköpostiosoite merkitään sekä kansalaisvarmenteeseen että väestötietojärjestelmään hakijan ilmoittamassa muodossa. Kansalaisvarmenteeseen merkitty sähköpostiosoite talletetaan julkiseen hakemistoon samoin kuin muu tunnistusvarmenteen tietosisältö. Sähköpostiosoitetta ei voi muuttaa kansalaisvarmenteen voimassaoloaikana.

9.3.2 Varmenteen uusiminen, sen avainparin vaihtaminen ja varmenteen päivittäminen

Kansalaisvarmenteella olevia julkisia avaimia ja sirulla olevia yksityisiä avaimia ei voi uusia. Uusien avainparien muodostaminen edellyttää uuden kansalaisvarmenteen hakemista. Tällöin noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa. Menettelytavat on kuvattu yksityiskohtaisesti varmennuskäytäntö -asiakirjassa.

9.3.3 Varmenteiden luominen

Varmentaja varmistaa, että se myöntää varmenteita turvallisesti niiden aitouden säilyttämiseksi Asetuksen mukaisesti.



Kansalaisvarmenteen haltijoiden yksityiset avaimet luodaan turvallisesti allekirjoitusvarmenteen vaatimukset täyttävällä tavalla. Varmenteen haltijan itsensä luomia avainpareja ei hyväksytä. Yksityisistä avaimista ei tehdä kopioita niiden luontivaiheessa, eivätkä ne ole siirrettävissä tai kopioitavissa mikrosirulta. Varmentajalla ja kortinvalmistajalla ei ole pääsyä varmenteen haltijoiden yksityisiin avaimiin.

Avainten luontivaiheessa avaimia ei ole vielä kohdistettu kenellekään henkilölle.

Varmentajan yksityiset avaimet ja niiden varmuuskopiot säilytetään vahvasti salatuina kriittisen tietoturvallisuuden vaatimukset täyttävissä laitteissa.

Varmenteen haltijan yksityisistä avaimista ei ole kopioita.

Varmentajan yksityisiä avaimia säilytetään varmentajan hallinnoimissa turvamoduuleissa.

Varmentajan yksityiset allekirjoitusavaimet suojataan korkean luotettavuuden fyysisillä ja loogisilla turvatoimilla. Niitä käytetään vain turvalliseen ympäristöön sijoitettussa järjestelmässä.

9.3.4 Käyttöehtojen jakelu

Varmentaja varmistaa, että käyttöehdot ja ohjeet asetetaan tilaajien ja varmenteeseen luottavien osapuolten saataville Asetuksen mukaisesti.

Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta allekirjoitusvarmenteelle asettamat vaatimukset.

Tiedot voidaan toimittaa tilaajan tai varmenteeseen luottavan osapuolen sopimuksen osana. Käyttöehdot voidaan sisällyttää varmennuskäytäntöön niin, että lukijan on ne helppo havaita ja tunnistaa.

Yleisölle myönnettäviä varmenteita koskevien sopimusehtojen osalta otetaan huomioon kuluttajalainsäädännön vaatimukset, myös kuluttajasopimusten kohtuuttomista ehdoista annettu direktiivi 93/13/ETY

Kansalaisvarmenteen haltija voi ladata Digi- ja väestötietoviraston www-sivuilta kortinlukijaohjelmiston, jolla kansalaisvarmennetta voidaan käyttää sähköisissä asiointipalveluissa.

Kansalaisvarmennetta haetaan sen mukaisesti kuin varmennuskäytännössä on kuvattu.

Sähköisen henkilökortin hankintahinta määräytyy kulloinkin voimassa olevan valtiovainministeriön asetuksen Digi- ja väestötietoviraston suoritteista mukaisesti.

Muilla mikrosiruilla olevat kansalaisvarmenteet on hinnoiteltu voimassaolevan Digi- ja väestötietoviraston liiketaloudellisia suoritteita koskevan hinnaston mukaisesti.



Varmentaja ei erikseen veloita kansalaisvarmenteen haltijaa kansalaisvarmenteiden, sulkupalvelun tai julkisen hakemiston käytöstä. Yksittäiset verkkopalveluntarjoajat saattavat veloittaa oman palvelunsa käytöstä. Kansalaisvarmenteiden käyttö ei edellytä erillistä ilmoitusta tai lupaa varmentajalta.

Kansalaisvarmenteen ilmoittaminen sulkulistalle on maksutonta. Myös sulkulisten noutaminen hakemistosta sekä kansalaisvarmenteen voimassaolon tarkistaminen sulkulistalta on maksutonta.

Neuvontapalvelun käytöstä peritään erillinen maksu voimassaolevan hinnaston mukaisesti.

Jos palveluntarjoaja haluaa järjestää tietohuoltopalvelun kansalaisvarmenteiden yksilöivän tunnisteen ja oman taustajärjestelmänsä tunnistetietojen tai muiden päivitystietojen välillä, palveluntarjoaja voi hakea tietopalveluun tietojenluovutuslupaa Digi- ja väestötietoviraston. Tämä palvelu hinnoitellaan voimassa olevan maksuperustelain ja valtiovaraministeriön asetuksen rekisterihallinnon suoritteista mukaisesti.

Kansalaisvarmenteen käyttöön liittyvät ohjeet ja käyttöehdot annetaan varmenteen hakijoiden tutkittaviksi ennen varmennetta koskevan sopimuksen ja myöntämispäätöksen tekemistä sekä rekisteröintipisteessä että Digi- ja väestötietoviraston verkkosivuilla.

9.3.5 Varmenteiden jakelu

Varmentaja varmistaa, että varmenteet asetetaan tarvittavalla tavalla tilaajien, allekirjoittajien ja varmenteeseen luottavien osapuolten saataville Asetuksen mukaisesti.

Juurivarmenteen, varmentajan varmenteiden ja varmenteen haltijan varmenteiden tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla varmentajan www-sivuilla <https://dvv.fi/fineid-maaritykset>.

Varmentaja julkaisee kaikki kansalaisvarmenteen tunnistusvarmenteet ja sulkulistat maksuttomassa, yleisesti saatavilla olevassa julkisessa hakemistossa. Varmentaja julkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvauksen (PDS) sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit www-sivuillaan.

Tunnistusvarmenne julkaistaan julkisessa hakemistossa heti, kun se on luotu, ja se on hakemistossa koko voimassaolonsa ajan. Varmentaja julkaisee sulkulistan, joka on voimassa kahdeksan tuntia julkaisemisestaan. Tämä sulkulista päivitetään kerran tunnissa uudella sulkulistalla.

Hakemisto- ja sulkulistatiedot ovat yleisesti saatavilla. Varmentajan julkaisemat julkiset FINEID-määritykset ovat saatavilla varmentajan www-sivuilla. Varmennepolitiikat ja varmennuskäytännöt ovat niin ikään saatavilla varmentajan www-sivuilla.

9.3.6 Varmenteen peruuttaminen ja asettaminen keskeytystilaan

Varmentaja varmistaa, että varmenteet peruutetaan oikea-aikaisesti valtuutettujen ja vahvistettujen varmenteiden peruutuspyyntöjen perusteella Asetuksen mukaisesti.

Kansalaisvarmenteen voimassaoloaika on enintään viisi vuotta. Varmenne voidaan sulkea sen voimassaoloaikana. Allekirjoitusvarmennetta voidaan käyttää



allekirjoituksen todentamiseen varmenteen vanhenemisen tai sulkemisen jälkeen, jos varmennettu allekirjoitus on luotu ennen varmenteen sulkemista tai vanhenemisai-
kaa.

Varmenteen haltijan on ilmoitettava välittömästi kansalaisvarmenteensa sulkupalve-
luun, mikäli hän epäilee, että sopimusehtojen vastainen käyttö tai muu väärinkäyttö
on tullut mahdolliseksi.

Kansalaisvarmenteen haltija voi halutessaan saada varmenteen suljettavaksi ennen
kansalaisvarmenteen voimassaoloajan päättymistä.

Kansalaisvarmenteiden voimassaoloa ei voi keskeyttää tilapäisesti. Suljettua kansa-
laisvarmennetta ei voi palauttaa käyttöön.

Varmenteen haltijan vastuulla on suojata yksityisten avaintensa käyttö huolehtimalla
mikrosirustaan tai kortistaan ja tunnusluvuistaan käyttöehdoissa mainitulla tavalla.
Varmenteen haltijan on ilmoitettava varmenteet välittömästi suljetuiksi, mikäli hän
epäilee, että sopimusehtojen vastainen käyttö on tullut mahdolliseksi.

Varmenteen sulkupyynnön tekee ensisijaisesti varmenteen haltija huomatessaan var-
menteen kadonneen tai jos niiden väärinkäyttö on tullut mahdolliseksi. Sulkupyynnön
voi kuitenkin tehdä esimerkiksi kortinvalmistaja tai rekisteröijä.

Sulkupyynnön on tehtävä välittömästi, kun on syytä epäillä kansalaisvarmenteen vää-
rinkäyttöä esimerkiksi katoamisen tai anastamisen vuoksi. Kansalaisvarmenne voi-
daan sulkea soittamalla maksuttomaan yleiseen sulkupalvelunumeroon +358 800
162 622. Sulkupyynnön on tehtävä välittömästi sen jälkeen, kun epäily väärinkäytön
mahdollisuudesta on syntynyt.

Kaikki sulkupyynnot, sulkemisen perusteet, sulkupyynnön tekijän tunnistustapa ja
pyyntöä seuranneet varmentajan toimenpiteet arkistoidaan. Sulkupyynnöt ja koskevat
puhulut nauhoitetaan.

Kansalaisvarmenteen sulkupyynnön tekee ensisijaisesti sen haltija. Mikäli soittaja on
eri henkilö kuin suljettavan varmenteen haltija, tunnistetaan haltijan lisäksi myös soit-
taja.

Sulkupyynnön voi tehdä myös varmentaja, kortinvalmistaja tai rekisteröijä. Varmen-
teen sulkemista pyytäneen henkilön todentamiseen käytetty menetelmä kirjataan.

Varmenteen sulkemisen perusteet, ajankohta ja suorittajan tiedot talletetaan.

Kansalaisvarmenteen sulkupyynnön voidaan tehdä seuraavilla tavoilla:

- a) Puhelinsoitolla sulkupalveluun
- b) Käymällä rekisteröijän luona

Tieto varmenteen viennistä sulkulistalle on julkisesti saatavilla viimeistään tunnin ku-
luttua siitä, kun sulkupyynnön on todettu päteväksi ja hyväksytyksi. Sulkulista on voi-
massa kahdeksan tuntia.



Varmenteen sulkeminen ja sen vaikutukset on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Varmenteiden sulkeminen Digi- ja väestötietoviraston pyynnöstä

Digi- ja väestötietovirasto sulkee varmenteet aina silloin, kun se on saanut tiedon varmenteen haltijan kuolemasta. Digi- ja väestötietovirasto tekee sulkemista koskevan ilmoituksen kuolleen varmenteen haltijan oikeudenomistajille.

Digi- ja väestötietovirasto sulkee myöntämänsä varmenteet, mikäli varmenteiden tietosisällössä havaitaan virhe.

Digi- ja väestötietovirasto voi sulkea käyttämällään yksityisellä avaimellaan allekirjoitetut varmenteet, mikäli on syytä epäillä Digi- ja väestötietoviraston yksityisten avainten paljastuneen tai joutuneen väärin käsiin.

Kaikki paljastuneella avaimella myönnettyt ja voimassa olevat varmenteet on suljettava yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun varmenteen voimassaoloaika on päättynyt.

Mikäli Digi- ja väestötietoviraston varmenteiden luonnissa käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, Digi- ja väestötietoviraston on ilmoitettava tapahtuneesta kaikille kortinhaltijoille ja Traficomille asianmukaisella tavalla.

Digi- ja väestötietovirasto voi sulkea varmenteen erityisestä syystä.

Varmenteen sulkeminen toteutetaan välittömästi sulkupyynnön yhteydessä.

9.3.7 Sulkulistan julkaisu tiheys

Tieto varmenteen viennistä sulkulistalle on julkisesti saatavilla viimeistään tunnin kuluuttua siitä, kun sulkupyynnö on todettu päteväksi ja hyväksytyt. Sulkulista on voimassa kahdeksan tuntia.

Sulkulista sisältää seuraavan sulkulistan julkaisuajankohdan.

Uusi sulkulista julkaistaan viimeistään voimassaolevan sulkulistan voimassaolon päättymisajankohtaan mennessä.

Järjestelmäpäivityksissä ja muissa poikkeavissa tilanteissa DVV voi julkaista sulkulistoja eri julkaisu tiheyksillä ja pidennetyillä voimassaoloajoilla.

Varmentaja tarjoaa suora käyttöisen varmenteen tilan tarkistuspalvelua eli OCSP-palvelun. Varmentaja julkaisee suljetuista varmenteista sulkulistan.

9.4 Avainparin uusiminen varmenteen sulkulistalle asettamisen jälkeen

Kansalaisvarmenteella olevia julkisia avaimia ja sirulla olevia yksityisiä avaimia ei voi uusia. Uusien avainparien muodostaminen edellyttää uutta kansalaisvarmennetta.

Kansalaisvarmenteen uusimisessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa.



Varmentajan julkaisemien sulkulistojen tietosisällöt on kuvattu dokumentissa FINEID S2. Dokumentti on saatavilla varmentajan [www-sivuilla](http://www.sivuilla) www.dvv.fi/cps_

9.5 Varmentajan johtamis- ja toimintakäytännöt

9.5.1 Turvallisuuden hallinta

Varmentaja varmistaa, että se noudattaa asianmukaisia ja tunnustettujen standardien mukaisia hallinnollisia ja liikkeenjohdollisia menettelytapoja Asetuksen mukaisesti.

Varmistaja varmistaa tietoturvallisuuden säilymisen, mikäli varmentaja hankkii palveluita toiselta organisaatiolta tai yhteisöltä.

9.5.2 Varantojen luokittelu ja hallinta

Varmentaja varmistaa, että sen tietovarantojen ja tietojen suojaustaso on tarkoituk-
senmukainen Asetuksen mukaisesti.

Digi- ja väestötietoviraston julkaisemat tiedot ovat saatavilla varmentajan www-sivuilla. Varmennejärjestelmän salaiset tiedot on talletettu varmentajan omaan, luottamukselliseen tietovarastoon. Varmentajan tiedot arkistoidaan voimassaolevien arkistosäännösten mukaisesti. Henkilötietojen käsittelyyn kiinnitetään erityistä huolellisuutta ja Digi- ja väestötietovirasto on julkaissut varmennepalveluiden tuottamisesta erityiset henkilötietolain mukaiset käytäntösäännöt. Varmentaja on valmistellut myös varmennejärjestelmän henkilötietolain mukaisen rekisteriselosteen henkilötietojen käsittelyä osalta.

Varmennejärjestelmän tiedot ovat salaisia, elleivät ne perustu henkilötietolain, viranomaisten julkisuudesta annetun lain, Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) tai vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain säännöksiin tietojen luovuttamisesta tai varmennepoliitikassa tai varmennuskäytännössä määriteltyihin tarkoituksiin.

Julkisen hakemiston ja sulkulistan tiedot ovat julkisia, samoin varmennuskäytännöt ja varmennepoliitikassa määritellyt tiedot sekä julkaistut FINEID-määritykset.

Kansalaisvarmenteen voimassaoloaika on merkitty kansalaisvarmenteeseen. Kesken voimassaoloajan suljetut kansalaisvarmenteet julkaistaan yleisesti saatavilla olevalla sulkulistalla.

Viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti.

Varmennejärjestelmän tietoja ei luovuteta kuin edellä tässä asiakirjassa mainittuihin tarkoituksiin.

Varmenteen haltijalla on oikeus saada häntä koskevia tietoja, esimerkiksi henkilötietoja, voimassaolevan lainsäädännön mukaisesti.

Varmentajan luotettavuuden vuoksi on olennaista, että Digi- ja väestötietovirasto huolehtii kaikin keinoin sille varmennetoiminnan yhteydessä tulevan luottamuksellisen aineiston salassa pitämisestä ja hyvästä tietojenhallintatavasta, ellei viranomaisten oikeudesta saada tietoa varmennejärjestelmän toiminnasta muuta johdu.



Digi- ja väestötietovirasto noudattaa henkilötietojen käsittelyssä henkilötietolakia sekä erityislainsäädäntöä. Digi- ja väestötietovirasto on valmistellut käytäntesäännöt sekä tietojen luovuttamisesta että varmennetoiminnan yhteydessä tapahtuvasta henkilötietojen käsittelystä. Henkilötietojen käsittelyssä noudatetaan erityistä huolellisuutta.

Digi- ja väestötietoviraston tuottamat varmennepalvelut ovat sellaisen taloushallinnollisen järjestelmän ja valvonnan piirissä kuin on erikseen säädetty. Varmentajan taloushallinnon toteuttaminen on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Yksityiskohtaiset vaatimukset on kuvattu ISO/IEC 17799 -standardissa.

9.5.3 Henkilöstö ja tietoturva

Varmentaja varmistaa, että henkilöstö ja rekrytointikäytännöt edistävät ja tukevat varmentajan toiminnan luotettavuutta Asetuksen mukaisesti.

Digi- ja väestötietovirasto toimii varmentajana, joka vastaa varmennetoiminnasta. Teknisten palveluiden toimittajien valinta perustuu julkisiin hankintoihin liittyvään kilpailutusmenettelyyn ja ne toimivat Digi- ja väestötietoviraston vastuulla ja lukuun.

Digi- ja väestötietovirasto kiinnittää erityistä huomioita sekä oman henkilökuntansa että teknisten palveluiden toimittajien ja rekisteröijien luotettavuuteen ja tehtävien suorittamiseen tarvittaviin taitoihin.

Digi- ja väestötietovirasto teettää omasta henkilöstöstään sekä teknisten toimittajien varmennetietojärjestelmän kanssa työskentelevistä henkilöistä perusmuotoisen turvallisuus selvityksen.

Henkilökunnan työkokemus kartoitetaan työhönottovaiheessa. Henkilöön kohdistetaan turvallisuus selvitys antamiensa tietojen perusteella määrämuotoisella lomakkeella.

Turvallisuus selvitysmenettely on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Digi- ja väestötietoviraston henkilökunnan koulutus suunnitellaan ja toteutetaan siten, että tehtävän hoitaminen parhaalla mahdollisella tavalla on mahdollista. Digi- ja väestötietovirastossa on koulutus suunnitelma, jonka toteuttamisesta vastaa Digi- ja väestötietoviraston hallinto ja johdon tuki -yksikkö.

Kun varmentajan tehtävissä suunnitellaan tehtäväkiertoa, tehtävät organisoidaan siten, että henkilö voi huolehtia uusista tehtävistään parhaalla mahdollisella tavalla. Tehtäväkierron toteuttamisessa on otettava huomioon hyvän tietojenhallintatavan säilyminen ja riittävän tehtäväkohtaisen osaamistason ylläpitäminen.

Myös tehtäväkierrossa noudatetaan Digi- ja väestötietoviraston tietoturvapoliittikkaa ja tietoturvasuunnitelmaa sekä Digi- ja väestötietoviraston muita yleisiä ohjeita.

Digi- ja väestötietoviraston henkilökunta toimii tehtävissään virkavastuulla ja Digi- ja väestötietoviraston sisäisten ohjeiden mukaisesti. Virkamiehen asemasta on säännelty valtion virkamieslaissa (750/1994).

Henkilökuntaa rekrytoitaessa on huolehdittava siitä, että henkilökunta vastaa taidoiltaan tehtävän edellyttämiä vaatimuksia ja että henkilön taustaselvityksestä ei ilmene



mitään sellaista, että henkilön tehtävät ovat ristiriidassa varmennepalveluiden tuottamisen kanssa.

Henkilökunnalla on aina käytössään Digi- ja väestötietoviraston laatu- ja turvallisuusasiakirjat.

9.5.4 Fyysinen ja ympäristön turvallisuus

Varmentajan on varmistettava, että fyysistä pääsyä kriittisiin palveluihin valvotaan ja että varantoja koskevat fyysiset riskit minimoidaan Asetuksen mukaisesti.

Digi- ja väestötietovirastolle on myönnetty tietoturvasertifikaatti, joka varmentaa, että DVV:n tietoturvaluus täyttää standardin ISO/IEC 27001 vaatimukset. Digi- ja väestötietovirasto käyttää teknisiä palveluomittajia varmennepalvelun tietoteknisten tehtävien hoitamiseen. DVV vastaa varmentajana varmennetuotannon turvallisuudesta ja toiminnasta asianmukaisella tavalla sen kaikilla osa-alueilla.

Varmentajan järjestelmät sijaitsevat korkean turvatason konesaliloissa ja täyttävät tietokonekeskuksille annetut turvallisuutta koskevat ohjeet ja määräykset.

Toimitilaturvallisuus on toteutettu siten, että asiattomien pääsy toimitiloihin on estetty.

Toimitiloihin, joissa tehdään varmennejärjestelmän tuotannollisia tehtäviä, on valvottu pääsy. Kulunvalvontajärjestelmä havaitsee sekä luvallisen että luvattoman sisäänmenon. Konesaliloihin vaaditaan henkilön tunnistautuminen, jolloin henkilö tunnistetaan ja pääsyoikeudet tarkistetaan sekä tapahtumat rekisteröidään. Konesaliloja vartioidaan vuorokauden ympäri.

Laitteistoratkaisut on toteutettu hyvän tiedonhallintatavan mukaisesti siten, että järjestelmän pettäessä voidaan siirtyä käyttämään varajärjestelmää vaarantamatta järjestelmään sisältyvien tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä.

Toiminnan kannalta kriittisten laitteiden varaosien saanti ja huolto on varmistettu.

Varmentajan yksityisen avaimen luominen, aktivointi, varmuuskopiointi ja palauttaminen suoritetaan valvotusti kahden järjestelmän ylläpitotehtäviin oikeutetun henkilön läsnä ollessa.

Varmentajan yksityisen avaimen peruuttaminen on mahdollista vain kahden oikeutetun henkilön valvonnassa.

Varmentajan yksityisen avaimen turvamuodulin alustuksessa on läsnä vähintään kaksi järjestelmän ylläpitotehtäviin oikeutettua henkilöä.

Järjestelmän käyttämiseen vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.

Kansalaisvarmenteen rekisteröiminen ja hakijan tunnistaminen vaatii yhden henkilön läsnäolon.

Kansalaisvarmenteen rekisteröijän, varmennejärjestelmän ylläpitäjän ja varmennejärjestelmän käyttäjän tunnistaminen ja tehtäväkuvaus on kuvattu yksityiskohtaisesti varmennuskäytännössä.



9.5.5 Toiminnan hallinta

Varmentajan on varmistettava, että varmentajan järjestelmät ovat turvalliset ja että niitä käytetään asianmukaisesti toimintahäiriöriskit minimoiden Asetuksen mukaisesti.

Digi- ja väestötietovirasto käyttää varmennetuotannon rekisteröinti- ja tietoteknisiin tehtäviin teknisiä palvelutoimittajia. Digi- ja väestötietovirasto toimii varmentajana, joka vastaa varmennetoiminnasta.

Varmentajan tehtävät on jaettu tehtävämukaisiin vastuualueisiin, jotka on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Varmentajan turvallisuudesta vastaava taho johtaa näitä vastuualueita, mutta käytännön toiminnassa käyttöhenkilökunta toteuttaa niitä valvonnan alaisena turvallisuutta koskevan asianmukaisen menettelytapaohjeen sekä roolit ja vastuualueet määrittävien asiakirjojen mukaisesti.

Digi- ja väestötietovirasto tarkastaa teknisten toimittajiensa toimitilat, laitteet ja toiminnan tarkoituksenmukaisella tavalla.

Digi- ja väestötietoviraston tietoturvatarkastuksen tekee Digi- ja väestötietoviraston tietoturvapäällikkö tai ulkopuolinen tarkastaja, joka on erikoistunut varmennepalveluihin liittyvien teknisten toimittajien auditointiin.

Digi- ja väestötietovirastolle on myönnetty tietoturvasertifikaatti, joka varmentaa, että DVV:n tietoturvallisuus täyttää standardin ISO/IEC 27001 vaatimukset.

Tarkastuksen kohteet määräytyvät laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista tai Digi- ja väestötietoviraston suorittaessa tarkastusta tietoturvastandardin ISO/IEC 27001, Digi- ja väestötietoviraston tietoturvapoliittikan tai teknisten toimitussopimusten mukaisesti.

Tarkastus tehdään ottaen huomioon tietoturvan kahdeksan osa-alueen toteutus. Tarkastettavia tietoturvallisuuden ominaisuuksia ovat luottamuksellisuus, eheys ja käytettävyys.

Tarkastuksessa verrataan politiikkaa, varmennuskäytäntöä ja soveltamisohjeita koko varmenneorganisaation ja -järjestelmän toimintaan. Digi- ja väestötietoviraston valvoo, että soveltamisohjeet ovat yhdenmukaiset varmennepoliittikan kanssa.

Tarkastuksissa otetaan huomioon hallinnollisen tietoturvallisuuden lisäksi palveluntoimittajat.

Havaitut poikkeamat kirjataan tarkastusraporttiin ja niihin reagoidaan lain, tietoturvastandardin ISO/IEC 27001 ja voimassa olevien toimitussopimusten mukaisesti.

Tarkastuksen tuloksesta tiedotetaan lain, tietoturvastandardin ISO/IEC 27001, Digi- ja väestötietoviraston tietoturvapoliittikan ja voimassa olevien toimitussopimusten mukaisesti. Sisäiseen käyttöön tarkoitettu yksityiskohtainen määrämuotoinen tarkastustulos on luottamuksellinen eikä siitä anneta tietoja julkisuuteen. Määrämuotoiset raportit laaditaan erikseen organisaation ulkopuoliseen käyttöön.



Digi- ja väestötietovirasto tiedottaa tarkastuksen tuloksista Traficomille vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain sekä Traficomien määräysten ja suositusten mukaisesti.

Allekirjoitusvarmentajia valvova Traficom voi tarkastaa varmentajan toiminnan laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista säädettyin edellytyksin.

Tarkastus kattaa Traficomien antamat määräykset varmentajan toiminnan tietoturvasuudesta.

9.5.6 Järjestelmiin pääsyn hallinta

Varmentaja varmistaa, että vain asianmukaisesti valtuutetuilla henkilöillä on pääsy varmentajan järjestelmään Asetuksen mukaisesti.

Digi- ja väestötietoviraston tietoturvasuutta hallitaan Digi- ja väestötietoviraston tietoturvapoliittikan ja standardin ISO/IEC 27001 mukaisesti.

Tietoliikenneturvallisuus on toteutettu siten, että varmennejärjestelmän tietoverkko on yhtenäinen kokonaisuus, joka on eriytetty muista tietoverkoista ja jonka kriittiset osat on kahdennettu.

9.5.7 Luotettavien järjestelmien käyttöönotto ja ylläpito

Varmentaja käyttää luotettavia järjestelmiä ja tuotteita, jotka on suojattu muutostoilta Asetuksen mukaisesti.

9.5.8 Liiketoiminnan jatkuvuuden hallinta ja häiriötilojen käsittely

Varmentaja varmistaa hätätilanteen sattuessa, esimerkiksi varmentajan yksityisen allekirjoitusavaimen vaarantumistilanteessa, että toiminta palautetaan mahdollisimman pian Asetuksen mukaisesti.

Varmentaja ilmoittaa jokaisessa varmennuskäytännössä ne toimenpiteet, joihin varmenteen haltijoiden, varmenteeseen luottavan osapuolen ja rekisteröijien ja varmentajan työntekijöiden on ryhdyttävä, mikäli varmentajan yksityinen avain on paljastunut tai tullut muutoin käyttökelvottomaksi.

Väestörekisterikeskuksella on poikkeusoloja koskeva jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa Digi- ja väestötietoviraston toiminnan jatkuvuuden.

Digi- ja väestötietoviraston turvapoliittikassa on otettu huomioon ulkoisen turvallisuuden vaarantumisen aiheuttamat toimenpiteet. Digi- ja väestötietovirasto on saanut ISO 27001

-tietoturvasertifikaatin, joka asettaa vaatimukset Digi- ja väestötietoviraston toiminnalle myös mahdollisen katastrofin tapahduttua.

9.5.9 Varmentajan toiminnan lakkauttaminen

Varmentaja varmistaa, että sen varmennepoliittikan alaisten palvelujen lakkauttamisesta tilaajille ja varmenteeseen luottaville osapuolille aiheutuvat mahdolliset häiriöt





minimoidaan ja että sellaisia tietoja ylläpidetään jatkuvasti, joilla varmentamista koskevia todisteita voidaan esittää oikeudellisissa menettelyissä Asetuksen mukaisesti.

Varmentajan lakkauttamisena pidetään tilannetta, jossa kaikki varmentajan varmenteen myöntämiseen liittyvät palvelut lakkautetaan pysyvästi. Varmentajan lakkauttamisella ei tarkoiteta tilannetta, jossa varmennepalvelu siirretään organisaatiolta toiselle.

Varmentaja ilmoittaa varmennepalveluiden lakkauttamisesta mahdollisimman pian, kuitenkin vähintään yhtä kuukautta ennen lakkauttamisen ajankohtaa.

9.5.10 Lainsäädäntöön perustuvien vaatimusten noudattaminen

Varmentajan on varmistettava, että lainsäädäntöön perustuvia vaatimuksia noudatetaan.

Yleisölle myönnettäviä varmenteita koskevien sopimusehtojen osalta otetaan huomioon kuluttajalainsäädännön vaatimukset, myös kuluttajasopimusten kohtuuttomista ehdoista annettu direktiivi 93/13/ETY .

Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta allekirjoitusvarmenteelle asettamat vaatimukset.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) on säädetty allekirjoitusvarmenteella tehdyistä sähköisistä allekirjoituksista. Sähköisestä henkilökortista on säädetty henkilökorttilaissa ja Digi- ja väestötietoviraston myöntämistä varmenteista on säädetty Digi- ja väestötietoviraston varmennepalveluista annetussa laissa (661/2009).

Soveltuvien osin Digi- ja väestötietovirasto noudattaa vahingonkorvauslain (412/1974) säännöksiä ja sähköisestä asioinnista viranomaistoiminnassa annetun lain (13/2003) mukaisia vaatimuksia.

Sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaan allekirjoitusvarmenteella voidaan aina asioida viranomaishallinnossa tarjottavissa sähköisissä palveluissa.

Digi- ja väestötietovirasto noudattaa henkilötietolain (523/1999) mukaista henkilötietojen hyvää tietojenkäsittelytapaa ja viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaista hyvää tiedonhallintatapaa. Digi- ja väestötietovirastossa tietoturvallisuus turvataan mm. jatkuvalla koulutuksella. Digi- ja väestötietovirasto on myös valmistellut käytäntösäännöt sekä tietopalveluille että varmennepalveluille.

Digi- ja väestötietovirasto hankkii rekisteröintiin ja henkilön tunnistamiseen liittyvät tehtävät erillisellä rekisteröintitoimia koskevalla yksityisoikeudellisella sopimuksella. Digi- ja väestötietovirasto voi hankkia palvelun esimerkiksi noudattamalla julkisen hallinnon yhteispalvelusta annetussa laissa (2007/223) noudatettuja säännöksiä.

Digi- ja väestötietoviraston asemasta on säädetty laissa Digi- ja väestötietovirastosta (304/2019). Allekirjoitusvarmentajia valvoo Suomessa Traficom.



9.5.11 Allekirjoitusvarmenteita koskevan tiedon säilyttäminen

Varmentaja varmistaa, että kaikki allekirjoitusvarmennetta koskevat tiedot tallennetaan tarkoituksenmukaiseksi ajaksi, erityisesti jotta se voi esittää varmentamista koskevia todisteita oikeudellisissa menettelyissä Asetuksen mukaisesti.

Kansalaisvarmenteen arkistoinnissa sovelletaan yleislakina arkistolain (831/1994) säännöksiä. Oikeus tietojensaantiin määräytyy viranomaisen toiminnan julkisuudesta annetun lain (621/1999) mukaisesti. Varmenteiden arkistoinnissa osalta sovelletaan lisäksi, mitä sähköisen asioinnin lainsäädännössä on arkistoinnista määrätty. Varmentajarekisterin tiedot säilytetään 10 vuoden ajan varmenteiden voimassaolon päätymisestä.

Varmentajan arkistoimat tiedot on kuvattu yksityiskohtaisesti varmennuskäytännössä.

Arkistotiedot säilytetään varmentajana toimivaa viranomaista koskevien säännösten mukaisesti.

Arkistoitava tieto säilytetään korkean turvatason tiloissa, joissa on pääsynvalvonta.

Varmuuskopiot varastoidaan fyysisesti erilliseen tilaan alkuperäisistä tiedoista.

Varmentaja varmistaa arkistojen tavoitettavuuden ja lukukelpoisuuden siinäkin tapauksessa, että varmentajan toiminta keskeytyy tai päättyy.

9.6 Organisaatioon liittyvät vaatimukset

Varmentajan on varmistettava, että sen organisaatio on luotettava Asetuksen mukaisesti.

Tämän varmennepolitiikan mukaisesti myönnetty allekirjoitusvarmenne täyttää Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta allekirjoitusvarmenteelle asettamat vaatimukset.

Digi- ja väestötietovirasto noudattaa henkilötietolain (523/1999) mukaista henkilötietojen hyvää tietojenkäsittelytapaa ja viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaista hyvää tiedonhallintatapaa. Digi- ja väestötietovirastossa tietoturvallisuus turvataan mm. jatkuvalla koulutuksella. Digi- ja väestötietovirasto on myös valmistellut käytäntesäännöt sekä tietopalveluille että varmennepalveluille.

Digi- ja väestötietovirasto hankkii rekisteröintiin ja henkilön tunnistamiseen liittyvät tehtävät erillisellä rekisteröintitoimia koskevalla yksityisoikeudellisella sopimuksella. Digi- ja väestötietovirasto voi hankkia palvelun esimerkiksi noudattamalla julkisen hallinnon yhteispalvelusta annetussa laissa (2007/223) noudatettuja säännöksiä.

Digi- ja väestötietovirasto vastaa siitä, että kansalaisvarmenteet on luotu noudattaen väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa, laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, laissa sähköisestä asioinnista viranomaistoiminnassa ja varmennepolitiikassa esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti.



Henkilötietojen käsittely osalta Digi- ja väestötietovirasto noudattaa henkilötietolakia. Digi- ja väestötietovirasto on jatkuvassa yhteistyössä henkilötietojen käsittelyn osalta tietosuojavaltuutetun kanssa.

Valitusten ja riitojen ratkaisussa sekä hallinnollisessa valvonnassa ja lainkäytössä noudatetaan voimassaolevaa lainsäädäntöä.

Myönnetty henkilökorttikortti on osoitus myönteisestä hallintopäätöksestä. Tähän päätökseen tyytymätön voi hakea muutosta hallinto-oikeudelta kirjallisella valituksella. Valitusosoitusasiakirja annetaan hakijalle henkilökortin kielteisen hakupäätöksen yhteydessä. Valitus tehdään sille hallinto-oikeudelle, jonka tuomiopiirissä poliisilaitos sijaitsee. Poliisilaitokset kirjaavat asiakirjaan oman alueensa hallinto-oikeuden tiedot, jos asiakas haluaa valittaa hallintopäätöksestä. Valitusaika alkaa kulua siitä hetkestä, kun valitusosoitus on asianmukaisesti liitetty päätökseen ja annettu tiedoksi asiakkaalle.

Digi- ja väestötietovirasto vastaa kansalaisvarmenteita myöntäessään siitä, että kansalaisvarmenne täyttää tässä kansalaisvarmennetta koskevassa varmennepolitiikassa esitetyt vaatimukset. Mahdolliset erimielisyydet ratkaistaan Suomen oikeusjärjestyksen mukaisesti.

Sähköisen henkilökortin hankintahinta määräytyy kulloinkin voimassa olevan valtiovainministeriön asetuksen Digi- ja väestötietoviraston suoritteista mukaisesti.

Muilla mikrosiruilla olevat kansalaisvarmenteet on hinnoiteltu voimassa olevan Digi- ja väestötietoviraston liiketaloudellisia suoritteita koskevan hinnaston mukaisesti.

10 Määrittelypuitteet muita varmennepolitiikkoja varten

Digi- ja väestötietoviraston kansalaisvarmenteet ovat allekirjoitusvarmenteita, minkä vuoksi tätä kohtaa ei sovelleta tämän kansalaisvarmenteen tarjoamiseen liittyen.

10.1 Varmennepolitiikan hallinta

Digi- ja väestötietovirasto voi muuttaa määräyksiä lainsäädännöllisten tai toiminnallisten vaatimusten vuoksi. Määritysten muutokset kirjataan varmennepolitiikka- ja varmennuskäytäntö -asiakirjoihin tässä kohdassa kuvatulla tavalla.

Digi- ja väestötietovirasto julkaisee varmennepolitiikan ja varmennuskäytännön, jotka ovat saatavilla Internet-sivuilla www.dvv.fi/cps_

Digi- ja väestötietoviraston julkiset varmenteiden tuotantoon liittyvät määräykset ovat saatavilla samoilla Internet-sivuilla.

Tietoteknisten toimittajien kanssa tehdyt varmenteiden toimittamista koskevat sopimukset sekä tuotantojärjestelmien kuvaukset ja tuotteisiin liittyvät määräykset ovat luottamuksellisia.

Digi- ja väestötietovirasto hyväksyy sekä kansalaisvarmennetta koskevan varmennepolitiikan että varmennuskäytännöt. Asiakirjoja voidaan muuttaa Digi- ja väestötietoviraston sisäisin muutosmenettelyin.



Digi- ja väestötietovirasto ilmoittaa muutoksista hyvissä ajoin ennen niiden voimaantuloa sekä Traficomille että omilla www-sivuillaan.

Digi- ja väestötietovirasto pitää asiakirjoista versionhallintaa sekä arkistoi kaikki varmennepolitiikka- ja varmennuskäytäntöasiakirjat. Typografiset korjaukset ja yhteystietojen muutokset ovat mahdollisia välittömästi.

Kaikkia varmennepolitiikan ja varmennuskäytännön kohtia voidaan muuttaa ilmoittamalla tulevista pääasiallisista muutoksista 30 päivää ennen muutosten voimaan astumista.

Kohtia, jotka Digi- ja väestötietoviraston mielestä eivät merkittävästi vaikuta varmenneiden haltijoihin ja luottaviin osapuoliin, voidaan muuttaa ilmoittamalla niistä 14 päivää aikaisemmin.

10.2 Poikkeukset varmennepolitiikkoihin, jotka koskevat muille kuin yleisölle myönnettäviä allekirjoitusvarmenteita

Digi- ja väestötietoviraston kansalaisvarmenteet sisältävät allekirjoitusvarmenteen ja vahvan sähköisen tunnistamisen välineen. Tämän vuoksi tätä kohtaa ei sovelleta tämän kansalaisvarmenteen tarjoamiseen liittyen.

10.3 Lisävaatimukset

Tilaaajille ja varmenteeseen luottaville osapuolille on ilmoitettava vaatimusten täyttämistä,

- a) mikäli varmennepolitiikka ei koske yleistä käyttöä ja sovelletaanko poikkeuksia
- b) mikäli varmennepolitiikka sisältää vaatimuksia turvallisen allekirjoituksen luomisvälineen käytöstä
- c) millä tavoin kyseinen politiikka lisää tai tiukentaa tässä asiakirjassa määritellyn varmennepolitiikan vaatimuksia.

10.4 Vaatimustenmukaisuus

Varmentaja saa ilmaista toimivansa tämän asiakirjan ja sovellettavan varmennepolitiikan mukaisesti vain,

- a) jos varmentaja ilmaisee noudattavansa yksilöityä varmennepolitiikkaa ja asettaa pyynnöstä tilaaajan ja varmenteeseen luottavien osapuolten saataville selvityksen vaatimustenmukaisuudesta tai

Selvityksenä voi olla esimerkiksi auditoijan kertomus, jossa vahvistetaan varmentajan noudattavan yksilöidyn varmennepolitiikan vaatimuksia. Kyseessä voi olla varmentajan organisaation sisäinen auditoija, mutta auditoija ei saa olla hierarkkisessa suhteessa varmentajan toimintaa toteuttavaan osastoon.



[Yksikkö] / Kytölä Sanni

**Digi- ja väestötietoviraston
kansalaisvarmennetta var-**

ten
[Tarkenne]

13.3.2023

47 (48)

[Numero]





[Yksikkö] / Aarnio Ville

**Digi- ja väestötietoviraston
kansalaisvarmennetta var-
ten**

[Tarkenne]

6.5.2021

[Numero]

[Liite]

48 (48)

