Varmennuskäytäntö

DNA Oyj:n varmennuskäytäntö mobiilivarmenteita varten

Versio 1.2

Voimassa 29.8.2017 lähtien

1 Yhteystiedot

1.1 Varmennuskäytäntöä hallinnoiva organisaatio

Tämä varmennuskäytäntö on DNA Oyj:n varmennuskäytäntö. Varmennuskäytäntöön liittyviin kysymyksiin vastaa DNA Oyj.

DNA Oyj,
PL 10,
01044 DNA
Y-tunnus: 0592509-6

Sähköposti: mobiilivarmenne@dna.fi

1.2 Varmennuskäytännön tunnisteet

Tämän varmennuskäytännön nimi on

"DNA Oyj:n varmennuskäytäntö mobiilivarmenteita varten".

Varmennuskäytännön tunniste (Object Identifier) on:

1.3.6.1.4.1.36036.1.1.2.1

(iso.org.dod.internet.private.enterprise.dna.ca.mss.cps.version1)

Varmennuskäytännön tunnistetieto on sijoitettu varmenteen X.509 v3 määrityksen [X.509] mukaiseen varmennuskäytännön tunnistetietokenttään (Certificate Policy OID). Tämän kentän avulla varmenteeseen luottava osapuoli voi varmistua varmenteen sopivuudesta kyseessä olevaan käyttötarkoitukseen.

1.3 Varmennepolitiikan tunnisteet

DNA:n varmennuskäytäntö noudattaa suomalaisten mobiilioperaattoreiden yhteistä varmennepolitiikkaa ja sen tunnisteet ovat:

Varmennepolitiikan nimi on "MOBIILIASIOINTIVARMENNE - VARMENNEPOLITIIKKA - Operaattoreiden mobiiliasiointivarmenteita varten".

Varmennepolitiikan tunniste (Object Identifier) on: 1.2.246.277.1.11.4.1.2.1

Sisällys

2 Käsitteet ja termit

Tässä dokumentissa käytetty suomenkielinen termi	Yleisesti käytössä oleva englanninkielinen termi	Selitys
Aktivointitieto, Tunnusluku	Activation Data	Yksityisen avaimen käyttöä suojaava PIN-koodi tai salasana, joka syöttämällä aktivoidaan yksityinen avain. Mobiiliasiointivarmenteen yksityiset avaimet sijaitsevat puhelimen SIM-kortilla.
Allekirjoituksen luomistiedot	Signature Creation Data	Allekirjoittajan sähköisen allekirjoituksen luomisessa käyttämä ainutkertainen tietokokonaisuus, kuten koodit ja yksityiset avaimet
Hakemistopalvelu	Directory Service	Julkisen avaimen järjestelmässä palvelu, joka sisältää käyttäjien varmenteita ja niihin mahdollisesti liittyvää muuta tietoa sekä sulkulistoja sisältäviä hakemistoja. Yleensä varmentajan itsensä ylläpitämä.
Julkinen avain	Public Key	Julkinen osa epäsymmetrisestä avainparista, jota käytetään julkisen avaimen salaustekniikoissa. Julkinen avain sisältyy varmenteeseen, jonka varmentaja julkaisee hakemistopalveluun.
Julkisen avaimen järjestelmä	Public Key Infrastructure (PKI)	Julkisen avaimen menetelmän käytön mahdollistava järjestelmä, jossa varmentaja, varmentaa avainparin julkisen osan digitaalisella allekirjoituksellaan ja jakaa näitä varmenteita muille käyttäjille, ylläpitää julkisten avainten hakemistoa ja sulkulistaa sekä mahdollisesti antaa muita järjestelmän käyttöön liittyviä palveluja.
Julkisen avaimen menetelmä	Public key method	Epäsymmetrinen salausmenetelmä, jossa kullakin salakirjoituksen käyttäjällä on kaksi toisiinsa liittyvää avainta. Toinen avainparin avaimista on julkisessa hakemistossa julkaistu julkinen avain, toinen on vain avainparin käyttäjän hallussa oleva yksityinen avain. Yksityisellä avaimella salakirjoitettu tieto voidaan avata vain vastaavalla julkisella avaimella, ja päinvastoin.
Juurivarmentaja	Root CA	Julkisen avaimen järjestelmässä ylin luotettu taho, joka allekirjoittaa, jakelee ja tarvittaessa peruuttaa varmenteet alemman tason varmentajille.
Kiistämättömyys	nonRepudiation	Avaimen käyttötarkoitus, jolla annetaan mainittua avainta käyttäen tehdylle kehittyneelle sähköiselle allekirjoitukselle sopimuksellinen sitovuus lain edessä. Kiistämättömyysavaimella on mahdollista allekirjoittaa sopimuksia. Allekirjoitettaessa dokumentti kiistämättömyysavaimella saavutetaan mahdollisuus todeta dokumentin eheys ja aitous käyttäen kyseistä avainta vastaavaa varmennetta. Katso *Sähköinen allekirjoitus* alla.

Liittymäkortti	Subscriber Identity Module	Kortti, johon puhelinliittymä on sidottu. Puhekielessä yleensä SIM-kortti.
Loppukäyttäjä, Varmenteen omistaja	End Entity	Henkilö, jolle varmentaja on myöntänyt varmenteen. Loppukäyttäjä käyttää varmennetta ja hänellä on laillisesti hallussaan varmenteen sisältämää julkista avainta vastaava yksityinen avain ja sen käyttöön tarvittavat tunnusluvut.
Luottava osapuoli	Relying Party	Sähköisiä palveluja varmenteiden loppukäyttäjille tarjoava taho. Luottava osapuoli toimii luottaen varmenteeseen ja/tai todentaa digitaalisen allekirjoituksen varmenteen avulla.
Luotettu varmenne	Trust Anchor	Varmenne, jonka luottavat osapuolet määrittelevät varmennehierarkiansa huipuksi ja jonka alapuolella olevat varmenteet he joutuvat varmentamaan.
Mobiiliasiointivarmenne		Mobiiliasiointivarmenne on mobiilipäätelaitteen liittymäkorteilla sijaitseviin yksityisiin avaimiin perustuva asiointivarmenne. Tämän varmennepolitiikan mukaista mobiiliasiointivarmennetta voidaan käyttää henkilön sähköiseen tunnistamiseen, viestinnän salaamiseen ja sähköiseen allekirjoitukseen. Mobiiliasiointivarmennetta voidaan käyttää käyttötarkoituksensa mukaisesti sekä hallinnollisissa että yksityisten organisaatioiden tarjoamissa sovelluksissa ja palveluissa. Tässä varmennepolitiikassa luettavuuden helpottamiseksi käytetään termiä Mobiilivarmenne isolla kirjoitettuna, ellei asiayhteys anna aihetta muuhun.
Mobiilivarmenne	Mobile Certificate	Tässä dokumentissa käytetty termi Mobiiliasiointivarmenteelle
Rekisteröijä	Registration Authority (RA)	Varmenteen hakijan tunnistamisesta ja varmennehakemukseen rekisteröitävien tietojen tarkistamisesta vastaava osapuoli. Rekisteröijä toimii varmentajan valtuuttamana varmenneorganisaation osana.
RSA	RSA	Epäsymmetrinen salausalgoritmi, jota käytetään epäsymmetrisen avainparin luontiin. Lyhenne tulee keksijöidensä sukunimistä; Rivest, Shamir ja Adleman.
Sulkulista	Certificate Revocation List (CRL)	Julkisen avaimen järjestelmässä käytöstä poistettujen varmenteiden luettelo. Varmentaja julkaisee sulkulistan hakemistopalvelussa.
Suostumus	Consent	Tapahtuman tai toimenpiteen vahvistaminen käyttäen avainta, jonka käyttötarkoitus on *digitalSignature* mutta ei *nonRepudiation*.
Sähköinen allekirjoitus	Electronic signature	Tietokoneen luettavassa muodossa oleva henkilön nimikirjoitus tai sen vastine, esimerkiksi digitaalinen allekirjoitus, todisteena nimikirjoitukseen liittyvän asiakirjan tai viestin yhteydestä tiettyyn henkilöön. Puhekielessä sähköisellä allekirjoituksella tarkoitetaan yleensä digitaalista allekirjoitusta, jonka tekemiseen

		käytetyn avaimen käyttötarkoituksiin kuuluu *nonRepudiation*.
Todentaminen	Authentication; Verification	Järjestelmän käyttäjän (henkilön, organisaation tai laitteen) tai viestinnässä toisen osapuolen tunnistuksen varmistaminen.
Tunnistaminen	Identification	Asioinnissa toisen osapuolen identiteetin selvittäminen. Yksinkertaisimmillaan tapahtuma, jossa vastataan kysymykseen: "Kuka sinä olet?"
Tunnistusväline		Liittymäkortti yksityisine avaimineen ja niihin liittyvät tunnusluvut.
Vahvistaminen	Validation	Varmenteen, varmenteella tehdyn operaation tai sen lopputuotoksen oikeellisuuden toteaminen.
Varmenne	Certificate	Varmenne on henkilön julkisesta avaimesta, nimitiedoista, sekä muista varmenteeseen sisällytettävistä tiedoista muodostuva kokonaisuus, jonka varmentaja on allekirjoittanut omalla yksityisellä avaimellaan. Varmenteen aitous on todennettavissa tarkistamalla varmentajan digitaalinen allekirjoitus.
Varmennehakemus	Certificate Application	Varmennehakemus on varmenteen hakijan täyttämä varmenteen hakijan henkilö-, organisaatio- ja yhteystiedot sisältävä, hakemuksen hyväksyjän hyväksymä ja tarvittaessa luotetun henkilön allekirjoittama lomake.
Varmenneorganisaatio		Varmenneorganisaation osapuolia ovat varmentaja, rekisteröijä, kortinvalmistaja, hakemisto- ja sulkulistapalvelujen tuottajat sekä muut palvelun tuottajat, joiden palveluja varmentaja käyttää.
Varmennepalvelu		Varmennepalvelu on varmenteisiin perustuva tunnistus- ja allekirjoituspalvelu, jota varmenteisiin luottava osapuoli hyödyntää varmenteen omistajille tarjoamissaan palveluissa.
Varmennepolitiikka	Certificate Policy (CP)	Nimetty joukko sääntöjä, joiden perusteella on mahdollista arvioida varmenteen soveltuvuus tiettyyn käyttötarkoitukseen ja yleiset turvallisuus- ja muut vaatimukset. **Varmennepolitiikka** (engl. *Certificate Policy, CP*) on varmentajan laatima kuvaus menettelytavoista ja toimintaperiaatteista, joita varmenteita myönnettäessä noudatetaan. Varmennuskäytäntö on varmennepolitiikkaa yksityiskohtaisempi kuvaus varmentajan toiminnasta.
Varmennepolku	Certificate Path	Varmenteen alkuperän varmistamiseksi tarvittava varmenteiden [looginen] ketju, joka ulottuu loppukäyttäjän varmenteesta juurivarmentajan varmenteeseen.
Varmennepyyntö	Certificate Request	Varmennepyyntö on varmentajalle lähetettävä, rekisteröijän muodostama, varmennehakemuksen perusteella tehty digitaalinen varmenteen muodostamis- ja julkaisupyyntö.

Varmennuskäytäntö	Certification Practice Statement (CPS)	Yksityiskohtainen selostus menettelytavoista, joita varmenneorganisaatio käyttää myöntäessään ja hallinnoidessaan varmenteita. **Varmennuskäytäntö** kuvaa kuinka varmentaja toteuttaa varmennepolitiikkaansa ja kuvaa yksityiskohtaisesti varmentajan noudattamat käytännöt ja toimintatavat. Varmennepolitiikan ja varmennuskäytännön rakenne noudattaa pääosin IETF RFC 3647:n [RFC3647] mukaista jaottelua.
Varmentaja	Certification Authority (CA)	Varmenneorganisaation osapuoli, joka myöntää varmenteita allekirjoittamalla varmennetiedot omalla yksityisellä avaimellaan.
Yksityinen avain, henkilökohtainen avain	Private Key	Salainen osa epäsymmetrisestä avainparista, jota käytetään julkisen avaimen salaustekniikoissa. Yksityistä avainta käytetään tyypillisesti digitaaliseen allekirjoittamiseen tai julkisella avaimella salatun viestin avaamiseen. Puhekielessä käytetään usein myös käsitettä salainen avain. Varmenteen omistajan yksityiset avaimet on talletettu liittymäkortille niiden suojaamiseksi oikeudettomalta käytöltä.

3 Lyhenteet

Lyhenne	**Selitys**	**Tässä dokumentissa käytetty merkitys**
CA	Certification Authority	Varmentaja
CPS	Certification Practice Statement	Varmennuskäytäntö
CRL	Certification Revocation List	Sulkulista
MSISDN	Mobile Subscriber ISDN Number	Matkapuhelimen puhelinnumero
MSSP	Mobile Signature Service Provider	Matkapuhelimessa tehtävän allekirjoituksen ja tunnistamisen mahdollistava palvelualusta.
OCSP	Online Certificate Status Protocol	Reaaliaikainen sulkutietoprotokolla
OID	Object Identifier	Varmennepolitiikan tunnistetieto
PDS	PKI Disclosure Statement	Yksinkertaistettu kuvaus varmenteen käytön ehdoista ja rajoituksista.
PIN	Personal Identification Number	Tunnusluku, PIN-koodi
PKI	Public Key Infrastructure	Julkisen avaimen varmennejärjestelmä
PKIX	-	IETF:n määrittelemä X.509 pohjainen PKI –järjestelmä standardi.
PUK	Personal Unblocking Key	PUK-koodi

RA	Registration Authority	Rekisteröijä
RSA	Rivest, Shamir ja Adleman,	Salausalgoritmi
X.509	-	Varmenteen rakenteen määrittelevä standardi.

4 Roolit

Liittymän tilaaja	Vastaa laskujen maksusta. Luonnollinen henkilö tai yritys, joka sallii liittymän palvelut. Voi olla sama kuin liittymän käyttäjä.
Liittymän käyttäjä	Liittymän ja palveluiden käyttäjä, luonnollinen henkilö, joka on merkitty liittymän haltijaksi. Käyttäjä voi olla sama kuin liittymän tilaaja.
Varmenteen hakija	Aina sama luonnollinen henkilö kuin liittymän käyttäjä. Liittymän haltijaksi on oltava merkittynä varmenteen hakija.
Varmenteen omistaja	Luonnollinen henkilö, jolle on myönnetty Mobiilivarmenne. Aina sama luonnollinen henkilö kuin varmenteen hakija eli liittymän käyttäjä.

5 Johdanto

5.1 Mobiilivarmennepalvelu

Suomalaiset teleoperaattorit ovat yhdessä luoneet Mobiilivarmennepalvelun, jota matkapuhelimia käyttävät kuluttajat voivat hyödyntää asioidessaan palveluntuottajien erilaisissa sähköisissä palveluissa. Palvelu tarjoaa kuluttajille helpon ja turvallisen tavan tunnistautua palveluihin sekä varmistautua asioinnin yhteydessä tekemiensä sitoumusten sisällöstä ja kiistämättömyydestä.

Palveluntarjoajille Mobiilivarmennepalvelu mahdollistaa käyttäjien henkilöllisyyden luotettavan todentamisen sekä palveluun liittyvien, asiakkaan hyväksyntää vaativien, tapahtumien vahvistamisen asiakkaan sähköisellä allekirjoituksella. Mobiilivarmennuspalvelu täyttää vahvan sähköisen tunnistamisen vaatimukset, jotka on määritetty lainsäädännössä.

Mobiilivarmennepalvelun käyttöönotto vaatii DNA:n liittymäkortin, joka tukee vahvaa tunnistamista. Palvelun käyttöönotto saattaa vaatia matkapuhelimen liittymäkortin vaihtoa.

Käyttäjä voi rekisteröidä mobiilivarmennepalvelun käyttöönsä DNA:n itsepalvelukanavassa, jolloin DNA:n rekisteröintisovellus varmistaa käyttäjän henkilöllisyyden pankkitunnuksilla.

Mobiilivarmennepalvelu on sidottu käyttäjän henkilöllisyyteen ja mahdollistaa asioinnin kaikissa Mobiilivarmennuspalvelua hyödyntävissä palveluissa. Käyttäjän on noudatettava erityistä huolellisuutta, jotta matkapuhelin ja siihen liittyvä henkilökohtainen tunnusluku ei ole muiden käytettävissä.

Jos käyttäjä kadottaa liittymäkortin tai käyttäjä epäilee, että henkilökohtainen tunnusluku on joutunut vääriin käsiin, on käyttäjän ilmoitettava viivytyksettä asiasta DNA:lle. Ilmoituksen voi tehdä soittamalla DNA:n asiakaspalveluun. Kun DNA saa ilmoituksen, DNA sulkee käyttäjän mobiilivarmennepalvelun.

Palveluntarjoajat voivat liittyä valitsemansa operaattorin mobiilivarmennepalveluun, jolloin heidän palvelunsa on saatavilla kaikkien palvelua tarjoavien operaattorien käyttäjille. Mobiilivarmennesovellusliitynnän käyttöönotto edellyttää sopimuksen tekemistä operaattorin kanssa sekä tarvittavia sovellustason liityntöjä tietojärjestelmiin.

Käyttäjän yksilöivä identiteetti perustuu sähköiseen asiointitunnukseen, jonka palveluntarjoaja voi tallentaa myös omaan järjestelmäänsä.

Sähköisellä allekirjoituksella voidaan hyväksyä maksutapahtumia ja toimeksiantoja sekä vahvistaa tilauksia. Sähköisellä allekirjoituksella voidaan varmistaa allekirjoitetun sähköisen dokumentin muuttumattomuus. Kun

dokumentti vahvistetaan sähköisellä allekirjoituksella, eri osapuolten ei tarvitse olla samassa paikassa samaan aikaan.

5.2 Varmennuskäytäntö

Tämä varmennuskäytäntö kuvaa DNA:n noudattamat käytännöt DNA:n myöntämissä mobiilivarmenteissa.

5.3 Mobiilivarmenne

Mobiilivarmenne on DNA:n liittymäsopimusasiakkaille toimitettava lisäpalvelu.

DNA:n mobiilivarmenteet ovat päätelaitteen liittymäkorteilla oleville käyttäjän salaisille avaimille DNA:n myöntämiä varmenteita.

Mobiilivarmenteiden myöntäminen vaatii sopimuksen DNA:n ja varmenteen hakijan välille.

DNA:n mobiilivarmenteiden myöntäjänä on DNA Mobile-ID CA, jonka yksilöivät tiedot löytyvät jokaisen myönnetyn varmenteen myöntäjä (Issuer) –kentästä. DNA:n Mobile-ID CA varmenteen on allekirjoittanut varmennepalvelun juurivarmentaja DNA Root CA.

DNA:n mobiilivarmenne noudattaa varmennepolitiikassa määriteltyä X.509v3 varmenneprofiilia. Varmenteen tekniset yksityiskohdat on kuvattu DNA:n verkkosivuilta:

www.dna.fi/mobiilivarmenne/

5.4 Varmennusorganisaatio

DNA varmentajan tiedot ovat saatavilla DNA verkkosivuilta:

www.dna.fi/mobiilivarmenne/

5.4.1 Rekisteröijä

Rekisteröintipalvelusta vastaa DNA Oyj.

Rekisteröijällä tarkoitetaan tahoa, joka toimii DNA:n toimeksiannosta ja vastuulla ja hoitaa varmennehakemusten käsittelyyn liittyvää käytännön työtä noudattaen tätä varmennuskäytäntöä.

Itsepalvelurekisteröintipalvelun rekisteröijänä toimii DNA.

5.4.2 Liittymäkortin liikkeellelaskija

DNA tai DNA:n Partneri toimittaa mobiilivarmenteen rekisteröinnissä tarvittavat tiedot liittymän loppukäyttäjälle.

5.4.3 Sulkupalvelu

DNA:n sulkupalveluna toimii DNA:n asiakaspalvelu.

5.4.4 Varmenteen omistaja

DNA myöntää Mobiilivarmenteen varmenteen omistajalle.

5.4.5 Varmenteeseen luottava osapuoli

Varmenteeseen luottava osapuoli on henkilö tai organisaatio, joka luottaa varmenteen tietoihin ja joka käyttää varmennetta varmenteen omistajan henkilöllisyyden todentamiseen tai varmenteen omistajan tekemän sähköisen allekirjoituksen tarkastamiseen.

5.4.6 Varmenteen käyttäminen

DNA:n mobiilivarmennetta voidaan käyttää tämän varmennuskäytännön mukaisesti henkilön sähköiseen todentamiseen, viestinnän salaamiseen, sähköisen suostumuksen antamiseen ja sähköiseen allekirjoitukseen käyttötarkoituksensa mukaisesti erilaisissa sovelluksissa ja palveluissa.

5.4.7 Osapuolten vastuut ja velvollisuudet

DNA on sitoutunut noudattamaan Luottamusverkoston Varmentajien yhteistä varmennepolitiikkaa.

DNA edellyttää muiden osapuolten kanssa tekemissään sopimuksissa, että nämä noudattavat varmennuskäytännössään ja varmennepolitiikassa asetettuja vaatimuksia.

Varmennusorganisaation eri osapuoliin liittyvät vastuut ja velvollisuudet on kuvattu Varmennepolitiikan liitteessä 2.

6 Yleiset ehdot

6.1 Tietojen julkaiseminen ja saatavuus

6.1.1 Varmentajan tietojen julkaiseminen

DNA (varmentaja) julkaisee sulkulistat yleisesti saatavilla olevalla palvelimella. Varmenteet julkaistaan varmentajien ja Mobiilivarmenteeseen luottavien palveluntarjoajien saataville sekä mahdollisesti yleisesti saatavilla olevassa hakemistossa.

DNA julkaisee varmennepolitiikan, varmennuskäytännöt, varmennekuvauksen (PDS) sekä muut julkiset varmennepalvelujen tuottamiseen liittyvät dokumentit www-sivuillaan.

www.dna.fi/mobiilivarmenne

6.1.2 Tietojen saatavuus

DNA voi rajoittaa pääsyä sulkulistoille ja hakemistoihin tuotepäätöksellä.

DNA:n sulkulistat ovat kaikkien niiden saatavilla, jotka tarvitsevat niitä mobiilivarmennepalvelujen tuottamiseen.

Varmennepolitiikka ja varmentajien varmennuskäytännöt sekä varmennekuvaus (PDS) ovat julkisesti saatavilla olevia dokumentteja, jotka ovat jaossa DNA:n verkkosivulla:

www.dna.fi/mobiilivarmenne/

6.1.3 Tietovarastot

DNA on laatinut henkilötietolain mukaisen rekisteriselosteen henkilötietojen käsittelystä varmennejärjestelmässä.

DNA arkistoi rekisteröinnissä kerätyt henkilön tunnistamistiedot voimassaolevien arkistosäännösten mukaisesti.

DNA tallentaa mobiilivarmenteet tietovarastoihin, joihin DNA rajoittaa pääsyä.

DNA kerää mobiilivarmennepalvelun liikenteestä lokitietoja, joita tarvitaan laskutukseen ja palvelun laadun valvontaan. Lokitiedot varastoidaan Viestintäviraston antamien määräysten mukaisesti.

Tiedot DNA:n julkaisemista tiedoista ovat saatavilla DNA:n www-sivuilla.

6.1.4 Auditointi

DNA tarkastaa rekisteröijiensä toimitilat, laitteet ja toiminnan tarkoituksenmukaisella tavalla.

DNA tarkastaa tarvittaessa oman toimintansa ulkoisella auditoijalla.

6.1.5 Tietojen luottamuksellisuus ja julkisuus

DNA:n varmennejärjestelmän tiedot ovat luottamuksellisia. DNA luovuttaa tietoja vain henkilötietolain, sähköisistä allekirjoituksista annetun lain, varmennepolitiikan tai varmennuskäytännön määrittelemiin tarkoituksiin.

Muut viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti.

7 Varmentajan yksilöinti

7.1 Varmentajan nimeäminen

DNA:n varmentajan nimi on DNA CA:n varmenteesta *Subject*-kentässä, sekä kaikkien DNA:n myöntämien varmenteiden *Issuer* - kentästä.

DNA:n varmentajan nimi koostuu seuraavista attribuuteista:

Attribuutti	**Sisältö**
commonName (CN)	DNA Mobile-ID CA
Organization (O)	DNA Oyj
Country (C)	FI

7.2 Avainparin uusiminen varmenteen sulkemisen jälkeen

Avainparin uusiminen johtaa aina uuteen varmenteeseen uusilla avaimilla. Vanha varmenne ja avainpari pysyvät mitätöityinä.

8 Toiminnalliset vaatimukset

8.1 Varmenteen hakeminen

Mobiilivarmenteen rekisteröintitapahtuman yhteydessä käyttäjä hyväksyy varmenteen käyttöehdot

Käyttäjä sitoutuu huolehtimaan mobiilivarmenteen ja tunnuslukujen säilyttämisestä asianmukaisesti sekä ilmoittamaan mahdollisen väärinkäytön tai varmenteiden tai liittymäkortin katoamisesta.

DNA tallentaa mobiilivarmenteeseen varmenteen hakijan henkilötiedot siten, kuin ne esitetään väestötiedoissa Väestörekisterin tietopalvelussa. Rekisteröijä ilmoittaa havaitsemistaan eroista henkilötodistuksen tietojen ja väestötietojen välillä varmenteen hakijalle rekisteröinnin yhteydessä.

8.2 Varmenteen hakijan tunnistaminen

Mobiilivarmenteen hakija tunnistetaan käyttäen vahvaa sähköistä tunnistamista.

8.3 Varmenteen myöntäminen

DNA myöntää mobiilivarmenteen varmenteen rekisteröinnin jälkeen. DNA vastaa siitä, että varmenteen tietosisältö on hakemuksen mukainen sen luovuttamishetkellä.

8.4 Varmenteen luominen

Mobiilivarmenne luodaan rekisteröitymisen yhteydessä. Mobiilivarmenne on käytettävissä onnistuneen rekisteröinnin jälkeen.

8.5 Varmenteen voimassaolon päättyminen ja sulkeminen

8.5.1 Varmenteen sulkemisen edellytykset

DNA asettaa mobiilivarmenteen sulkulistalle, kun on syytä epäillä väärinkäyttöä esimerkiksi silloin, kun liittymäkortti on kadonnut tai anastettu.

DNA sulkee mobiilivarmenteen, mikäli sitä vastaava liittymä suljetaan. Suljettaessa liittymä tilapäisesti tehdään varmenteellekin tilapäinen sulku, ellei perusteltua syytä muuhun ole.

Varmenteen omistaja voi sulkea mobiilivarmenteen soittamalla maksuttomaan DNA:n asiakaspalveluun.

Mobiilivarmenteen omistajan on tehtävä sulkupyyntö välittömästi, kun epäilys väärinkäytön mahdollisuudesta on syntynyt.

DNA sulkee varmenteet silloin, kun se on saanut tiedon varmenteen omistajan kuolemasta.

DNA sulkee myöntämänsä varmenteet, mikäli varmenteiden tietosisällössä havaitaan virhe.

DNA voi sulkea käyttämällään yksityisellä avaimellaan allekirjoitetut varmenteet, mikäli on syytä epäillä DNA:n yksityisten avainten paljastuneen tai joutuneen vääriin käsiin.

DNA sulkee kaikki paljastuneella salaisella avaimella myönnetyt ja voimassa olevat varmenteet, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun varmenteen voimassaoloaika on päättynyt.

Mikäli DNA:n varmenteiden luonnissa käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, DNA ilmoittaa tapahtuneesta varmenteen omistajille, palveluntarjoajille, Viestintävirastolle ja varmentajille asianmukaisella tavalla.

DNA voi sulkea varmenteen erityisestä syystä, esimerkiksi kryptografisten hyökkäysmenetelmien kehityksestä johtuen.

8.5.2 Sulkupyynnön tekijä

Mobiilivarmenteen sulkupyynnön tekee ensisijaisesti sen omistaja Sulkupyynnön voi tehdä myös DNA tai DNA:n mobiilivarmennekumppani tai viranomainen.

DNA kirjaa varmenteen sulkemista pyytäneen henkilön todentamiseen käytetyn menetelmän, varmenteen sulkemisen perusteet, ajankohta ja suorittajan tiedot.

Varmenteen omistaja todennetaan samoilla periaatteilla kuin käyttäjän tehdessä liittymän muuta hallinnointia.

Viranomainen todennetaan samoilla periaatteilla kuin muut viranomaispyynnöt.

DNA:n henkilöstö ja DNA:n vuokrahenkilöstö todennetaan samoilla periaatteilla kuin DNA:n asiakaspalveluhenkilöstö.

8.5.3 Sulkutapahtuma

Varmenteen sulkeminen tehdään aina tilapäisesti ja varmenteen käyttö estetään teknisesti välittömästi. Tieto varmenteen sulkemisesta on julkisesti saatavilla sen jälkeen, kun uusi sulkulista julkaistaan.

DNA tekee sulkemista koskevan ilmoituksen kuolleen varmenteen omistajan oikeudenomistajille.

8.5.4 Sulkutapahtuman ajoitus

DNA toteuttaa mobiilivarmenteen sulkemisen viipymättä saatuaan sulkupyynnön. DNA toteuttaa teknisen sulkemisen heti ja sulkutapahtuma päivitetään julkiseen sulkulistaan sen julkaisun yhteydessä.

DNA:n sulkulistat julkaistaan 60 minuutin välein.

8.5.5 Sulkulistan julkaisutiheys

Tieto varmenteen viennistä sulkulistalle on julkisesti saatavilla, kun sulkupyyntö on suoritettu. Sulkulista julkaistaan 60 minuutin välein ja on voimassa 24 tuntia. Sulkulista sisältää seuraavan sulkulistan julkaisuajankohdan.

Järjestelmäpäivityksissä ja muissa poikkeavissa tilanteissa DNA voi julkaista sulkulistoja eri julkaisutiheyksillä ja pidennetyillä voimassaoloajoilla.

8.5.6 Sulkulistan jakelupisteet

DNA:n sulkulista julkaistaan kahdessa erillisessä pisteessä, joista kahteen on viittaukset CA varmenteessa.

Sulkulistan sijasta voidaan käyttää myös suorakäyttöistä varmenteen tilan tarkistamista OCSP-protokollalla tai DSS-protokollalla.

8.6 Varmenteen uusiminen

8.6.1 Varmenteen uusiminen nimenmuutoksen vuoksi

Varmenteen omistajan nimen muuttuessa on varmenteen omistajan rekisteröitävä varmenne uudelleen.

8.6.2 Varmenteen uusiminen varmenteen vanhenemisen vuoksi

Kun varmenne vanhenee, on varmenteen omistajan rekisteröitävä varmenne uudelleen.

8.7 Järjestelmän valvonta

DNA:n varmennejärjestelmän valvonta kuvataan DNA:n varmentajan tietoturvaohjeistuksessa.

8.8 Varmenteisiin liittyvien tietojen arkistointi

8.8.1 Tallennettava aineisto

DNA tallentaa mobiilivarmennetapahtumista seuraavat tiedot:

1) yksittäisen tunnistustapahtuman ja sähköisen allekirjoittamisen tapahtuman todentamiseksi tarvittavat tiedot, ns. teletunnistetiedot;
2) tarvittavat tiedot hakijan ensitunnistamisesta sekä siinä käytetystä asiakirjasta sekä mahdolliset kopiot asiakirjoista;
3) tiedot tunnistusvälineen käyttöön mahdollisesti liittyvistä estoista ja käyttörajoituksista; sekä
4) varmenteen tietosisältö.

DNA säilyttää edellä 1 kohdassa tarkoitetut tiedot viisi vuotta tunnistustapahtumasta tai kuitenkin siten, kuin viranomaismääräykset kulloinkin asiasta määräävät.

Kohtien 2,3 ja 4 tarkoitetut tiedot säilytetään viisi vuotta varmentajan ja varmenteen omistajan välisen asiakassuhteen päättymisestä.

Tiedot tallennetaan sähköiseen arkistoon, joka ei ole aktiivisesti verkossa (offline).

8.8.2 Arkistojen suojaus

Arkistoitava tieto säilytetään korkean turvatason tiloissa. Pääsynvalvonta toteutetaan tapauskohtaisesti siten, ettei asiattomilla ole pääsyä arkistoituun tietoon.

8.8.3 Arkistojen varmistusmenettelyt

Arkiston varmuuskopiot varastoidaan fyysisesti erilliseen tilaan.

8.8.4 Arkistotietojen hankinta- ja varmistusmenetelmät

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

8.9 Varmentajan avainten uusiminen

Varmentajan avainten uusiminen tapahtuu DNA:n varmentajan tietoturvaohjeistuksen mukaisesti.

8.10 Toiminnan jatkumisenhallinta ja poikkeustapausten käsittely

DNA varmentajalla on jatkuvuus- ja valmiussuunnitelma, joka mahdollistaa varmentajan toiminnan jatkuvuuden. Jatkuvuus- ja varasuunnitelma kuvataan DNA:n varmentajan valmiussuunnitelmassa.

Poikkeustapauksiin varautuminen on kuvattu varmennuskäytännössä.

8.10.1 Varmentajan yksityinen avain on paljastunut tai varmentajan varmenne on suljettu

Mikäli DNA varmentajan yksityinen avain on paljastunut tai tullut muutoin käyttökelvottomaksi,

DNA tekee viipymättä seuraavat ilmoitukset:

1. Viestintävirasto; Ilmoitus varmentajan varmenteen vaarantumisesta
2. Luottamusverkoston osapuolet; Ilmoitus varmentajan varmenteen vaarantumisesta
3. Luottavat osapuolet, joilla on suora sopimus DNA:n kanssa; Ilmoitus varmentajan varmenteen vaarantumisesta
4. Mobiilivarmenne kumppanit; Ilmoitus varmennepalvelun keskeytyksestä
5. DNA:n loppukäyttäjät; Ilmoitus varmennepalvelun keskeytyksestä
6. DNA:n rekisteröijät; Ilmoitus varmennepalvelun keskeytyksestä
7. DNA:n henkilöstö ja vuokrahenkilöstö; Ilmoitus varmennepalvelun keskeytyksestä

DNA sulkee rekisteröintipalvelun ja asettaa kaikki myönnetyt varmenteet sulkulistalle

ja aloittaa muut elpymissuunnitelman mukaiset toiminnat.

8.10.2 Turvallisuuden vaarantuminen luonnonmullistuksen tai muun katastrofin seurauksena

DNA varautuu luonnonmullistukseen tai muuhun katastrofiin hajautussuunnitelmalla, jotta järjestelmän haavoittuvuus yhden pisteen vikaantumiselle olisi minimoitu.

8.11 Varmentajan toiminnan lakkauttaminen

Tilanteissa, joissa DNA varmentajan toiminta lakkautetaan, DNA varmentaja ilmoittaa varmennepalveluiden lakkauttamisesta muille luottamusverkoston varmentajille ja asiakkailleen mahdollisimman pian, kuitenkin vähintään kuutta kuukautta ennen lakkauttamisen ajankohtaa.

Ennen DNA varmentajan lakkauttamista suoritetaan vähintäänkin seuraavat toimenpiteet:

- Kaikki DNA varmentajan myöntämät ja voimassa olevat varmenteet suljetaan DNA varmentajan sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisten suljetun varmenteen voimassaoloaika on päättynyt.
- DNA varmentaja lakkauttaa kaikki sopimuskumppaniensa valtuudet suorittaa varmenteiden myöntämisprosessiin liittyviä tehtäviä varmentajan puolesta.
- DNA varmentaja varmistaa, että kohdassa 8.8 mainittu saatavuus varmentajan arkistoihin säilyy varmentajan lakkauttamisen jälkeenkin.
- DNA varmentaja huolehtii sähköisen allekirjoituslain mukaisten tietojen arkistoinnista sekä noudattaa muutoinkin arkistolain säännöksiä tietojen arkistoinnin osalta.

9 Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset

9.1 Fyysinen turvallisuus

DNA varmentaja huolehtii varmennetuotannon turvallisuudesta ja toiminnasta asianmukaisella tavalla sen kaikilla osa-alueilla.

Yksityiskohtainen kuvaus turvallisuuteen liittyvistä järjestelyistä on kuvattu DNA:n turvallisuusohjeistuksessa.

9.1.1 Sijainti ja rakennusten ominaisuudet

DNA varmentajan järjestelmät sijaitsevat korkean turvatason konesalitiloissa ja täyttävät tietokonekeskuksille annetut turvallisuutta koskevat ohjeet ja määräykset.

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

9.1.2 Fyysinen pääsy toimitilaan

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

Konesalitiloja vartioidaan vuorokauden ympäri.

9.1.3 Varajärjestelyt

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

Tärkeiden laitteiden varaosien saanti ja huolto on varmistettu.

9.2 Toiminnalliset vaatimukset

9.2.1 Vastuunjako

DNA varmentajan tehtävät on jaettu tehtävänmukaisiin vastuualueisiin.

Vastuualueet on kuvattu yksityiskohtaisesti DNA:n varmenneorganisaatio kuvauksessa.

9.2.2 Tehtäviin vaadittavien henkilöiden lukumäärä

DNA 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 turvamoduulin alustuksessa on läsnä vähintään kaksi järjestelmän ylläpitotehtäviin oikeutettua henkilöä.

Järjestelmän käyttämiseen vaaditaan yhden tehtävään oikeutetun henkilön läsnäolo.

9.2.3 Tehtäväkohtainen tunnistaminen

Mobiilivarmenteen rekisteröijän, varmennejärjestelmän ylläpitäjän ja varmennejärjestelmän käyttäjän tunnistaminen ja tehtäväkuvaus on seuraava:

- Varmenteen rekisteröijä, sähköinen rekisteröinti; XML allekirjoitus sovelluksen avaimilla.
- Varmennejärjestelmän ylläpitäjä; varmennejärjestelmän käyttämä oma sisäinen vahva tunnistusmenetelmä
- Varmennejärjestelmän muut käyttösovellukset; sulkupyynnöt; sovelluksen XML allekirjoitus
- Varmennejärjestelmän muut käyttäjät; varmennejärjestelmän käyttämä oma sisäinen vahva tunnistusmenetelmä

9.3 Henkilöturvallisuus

DNA on kiinnittänyt erityistä huomioita sekä oman henkilökuntansa että teknisten

toimittajien ja rekisteröijien luotettavuuteen ja tehtävien suorittamiseen tarvittaviin taitoihin.

DNA on laatinut DNA tietoturvaohjeistuksen eri varmenneorganisaation jäsenille.

DNA:n henkilökohtaisen rekisteröintipalvelun henkilöstö certifioidaan toimintaa ennen kuin henkilö voi osallistua rekisteröintiin.

9.3.1 Henkilökuntaa koskevan taustaselvityksen tekeminen

DNA teettää omasta varmennepalveluhenkilöstöstään sekä edellyttää teknisiä toimittajia teettämään varmennetietojärjestelmän parissa työskentelevistä henkilöistään tarvittavat turvallisuus- ja taustaselvitykset.

9.3.2 Taustaselvityksen tekemisessä noudatettava menettely

DNA teettää varmennepalvelun avainhenkilöstöstä turvallisuusselvityksen henkilön antamien tietojen perusteella määrämuotoisella lomakkeella.

9.3.3 Koulutukseen liittyvät vaatimukset

DNA varmentajan henkilökunnan koulutetaan siten, että tehtävän hoitaminen on mahdollista.

9.3.4 Asiantuntemuksen ja osaamisen ylläpito

DNA suunnittelee ja toteuttaa henkilökunnan koulutuksen siten, että tehtävän hoitamiseen liittyvä asiantuntemus on tehtävän edellyttämällä tasolla.

9.3.5 Poikkeamista johtuvat toimenpiteet

DNA:lla on lista niistä ulkopuolisista henkilöistä, joita voidaan käyttää varmennejärjestelmän poikkeustilanteissa.

DNA voi käyttää poikkeustilanteissa varmentajan tehtäviin väliaikaisesti henkilöstöä, jonka koulutus ei ole täydellistä, mutta heidän työtänsä on ohjattava erityisen huolellisesti.

9.3.6 Henkilökunnan käyttöön annettavat asiakirjat

DNA:n henkilökunnalla on käytössään DNA:n Intranetissä ajantasainen DNA varmentajan laatu- ja turvallisuusohjeet.

10 Tekniset turvatoimet

10.1 Avainparin luominen, tallettaminen ja käyttöönotto

10.1.1 Avainparin luominen

Varmentaja:

DNA varmentaja luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimet. Varmentajan yksityistä avainta säilytetään turvamoduulissa.

Varmenteen omistaja:

Avainten luonti voidaan toteuttaa kahdella eri tavalla. Tämä riippuu käytetystä liittymäkortin ohjelmistoversiosta. DNA:lla on valmiudet toteuttaa molemmat tavat.

1. Avaimet voidaan luoda pyydettäessä (OBKG).

Rekisteröinnin yhteydessä rekisteröijä pyytää käyttäjää luomaan itse omat avaimensa. Pyyntö lähetetään käyttäjän liittymäkortille. Liittymäkortti avaa käyttäjälle avaintenluontisovelluksen ja pyytää käyttäjää valitsemaan avaimelle haluamansa PIN-koodin. Liittymäkortti lähettää luotuja salaisia avaimia vastaavat julkiset avaimet rekisteröijälle samalla mekanismilla kuin se vastaanotti avaintenluontipyynnön.

2. Avaimet voidaan luoda liittymäkorttitoimittajan tiloissa (Pregen).

Liittymäkortin valmistuksen yhteydessä valmistaja generoi avainparit ja niitä vastaavat PIN-koodit liittymäkortilla valmistusprosessin yhteydessä. PIN-koodit tulostetaan joko kortilla olevalle turva-alueelle, joka peitetään rapituspinnalla, tai erilliseen PIN-kuoreen. Avainten generointi toimii samoin kuin OBKG-sovelluksessa.

Avainten generointi ohjelmiston toteutuksesta vastaa liittymäkorttitoimittaja.

Liittymäkortilla on aina vähintään 1024-bittinen RSA-avain.

10.1.2 Liittymäkortin luovuttaminen hakijalle

Liittymäkortin luovutusprosessi (OBKG) on kuvattu kohdassa **Error! Reference source not found.**.

Liittymäkortin luovutusprosessi (Pregen) ei sisälly tähän varmennuskäytäntöön.

10.1.3 Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle

DNA:n rekisteröintipalvelut toimittavat varmenteen hakijan julkisen avaimen DNA varmentajalle TLS-salatulla yhteydellä. Julkinen avain on osana varmennepyyntöä, jossa ovat lisäksi varmenteen hakijan varmenteen Subject -kenttä, varmenteen hakijan allekirjoitus ja rekisteröijän tiedot.

DNA:lla on valmiudet tehtaalla luotujen avainten (Pregen) toimitukseen.

Pregen kortin tapauksessa DNA toimittaa julkiset avaimet ja niitä vastaavat liittymäkortin tiedot DNA varmentajalle. Julkisten avainten eheys suojataan varmennukseen asti. Mobiilivarmenteen rekisteröinnin yhteydessä rekisteröijä hakee varmenteen hakijan korttia vastaavat julkiset avaimet varmentajalta. Avainten ja kortin oikea yhdistelmä varmistetaan varmenteen hakijan allekirjoittamalla varmennepyynnöllä.

Kortilla luotujen avainten tapauksessa hakijan julkinen avain toimitetaan varmentajalle osana varmenteen hakuprosessia.

10.1.4 Varmentajan julkisen avaimen jakelu

DNA varmentajan varmenne sisältää varmentajan julkisen avaimen. Varmentajan varmenne talletetaan julkiseen hakemistoon, josta se on saatavilla.

10.1.5 Avainten pituudet

DNA:n mobiilivarmenteen allekirjoittamiseen käytetty varmentajan yksityinen avain sekä sitä vastaava julkinen avain on vähintään 2048-bittinen RSA-avain.

10.1.6 Avainten käyttötarkoitukset

Varmenteen tietosisällössä käyttötarkoituksen määräävä kenttä määrittelee varmenteisiin liittyvien avainten käyttötarkoituksen (todentaminen ja kiistämättömyys). Avainten käyttö rajataan vain näihin käyttötarkoituksiinsa.

Varmenteen hakijan kortille luodaan avaimet erikseen sähköistä allekirjoitusta eli kiistämättömyyttä varten ja tunnistamista varten.

Asiointivarmenteeseen liittyy kaksi avainparia ja vastaavasti kaksi varmennetta.

DNA voi sisällyttää tunnistusavaimen käyttötarkoituksiin salauksen.

10.2 Varmentajan yksityisten avainten suojaaminen

10.2.1 Turvamoduulia koskevat standardit

DNA varmentajan yksityisiä avaimia säilytetään DNA varmentajan hallinnoimissa turvamoduuleissa.

DNA varmentaja huolehtii siitä, että varmentajan yksityiset avaimet on suojattu paljastumiselta ja luvattomalta käytöltä.

DNA varmentajan yksityisistä avaimista otetaan varmuuskopio kriittisen tietoturvallisuuden edellyttämällä tavalla.

10.2.2 Varmentajan yksityisen avaimen käsittelyyn osallistuva henkilökunta

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

10.2.3 Yksityisen avaimen varmuuskopio

DNA varmentajan yksityiset avaimet ja niiden varmuuskopiot säilytetään vahvasti salattuina kriittisen tietoturvallisuuden vaatimukset täyttävissä laitteissa.

Varmenteen omistajan yksityisistä avaimista ei ole kopioita.

10.2.4 Yksityisen avaimen arkistointi

DNA varmentajan tai käyttäjän yksityisiä avaimia ei arkistoida.

10.2.5 Yksityisen avaimen hallinnointi turvamoduulissa

DNA varmentajan yksityiset allekirjoitusavaimet suojataan korkean luotettavuuden fyysisillä ja loogisilla turvatoimilla. Niitä käytetään vain turvalliseen ympäristöön sijoitetussa järjestelmässä.

10.3 Varmenteen omistajan avainten suojaaminen

10.3.1 Liittymäkorttia koskevat standardit

DNA:n liittymäkortti on valmistettu GSMA-SAS -sertifioidussa tehtaassa.

10.3.2 Yksityisen avaimen luovutus luotetun osapuolen huostaan

Varmenteen omistajan yksityistä avainta ei luovuteta kenellekään muulle kuin sen hakijalle.

10.3.3 Yksityisen avaimen varmuuskopio

Mobiilivarmenteeseen liittyvistä yksityisistä avaimista ei ole kopioita.

10.3.4 Yksityisen avaimen arkistointi

Mobiilivarmenteeseen liittyvää yksityistä avainta ei arkistoida.

10.3.5 Yksityisen avaimen hallinnointi liittymäkortilla

Yksityistä avainta ei hallinnoida erityisesti. Yksityinen avain on vain ja ainoastaan liittymäkortilla.

10.4 Muut avainparin hallintaan liittyvät seikat

10.4.1 Julkisen avaimen arkistointi

Varmentaja arkistoi kaikki myöntämänsä varmenteet, jonka mukana julkinen avain tulee arkistoiduksi.

10.4.2 Julkisten ja yksityisten avainten voimassaoloaika

DNA:n myöntamän mobiilivarmenteen voimassaoloaika on enintään viisi vuotta. Varmenteen voimassaoloaika voi olla lyhyempikin, mikäli käytettävissä olevan avainpituuden ei katsota pysyvän turvallisena täyttä viiden vuoden jaksoa. Varmenne voidaan sulkea sen voimassaoloaikana.

Varmenteen sulkutapahtumaa on käsitelty enemmän kohdassa 8.5 .

10.5 Liittymäkortilla olevien yksityisten avainten tunnusluvut

10.5.1 Tunnusluvun luominen ja käyttöönotto

Liittymäkortin yksityisten avainten käyttö on suojattu tunnusluvulla, jonka käyttäjä valitsee avainten luonnin yhteydessä (OBKG). Tätä tunnuslukua käytetään yksityisten avaimen aktivointitietona.

Liittymäkortin yksityisten avainten käyttö on suojattu tunnusluvulla, joka toimitetaan käyttäjälle kortin luovutuksen yhteydessä (Pregen). Tunnusluku toimitetaan sellaisenaan kuin se korttitehtaalta on vastaanotettu joko suljetussa PIN-kuoressa tai raaputuspintaisella liittymäkortilla. Tunnusluku on suojattu siten, että sen lukeminen vaatii toimenpiteitä, josta seuraa pysyvä jälki. Näin varmistutaan siitä, että jos tunnusluku on luettu ennen kortin käyttöönottoa, se on nähtävissä ja osoitettavissa helpoilla keinoilla.

Tätä tunnuslukua käytetään yksityisten avaimen aktivointitietona.

10.5.2 Tunnusluvun suojaus

Liittymäkortin tunnusluvut on suojattu korttivalmistajan kortin käyttöjärjestelmätasolla niin, ettei niitä voi lukea tai kopioida kortilta.

10.6 Varmennejärjestelmän laitteiden käyttöön ja pääsyyn liittyvät turvallisuusvaatimukset

10.6.1 Laitteistoturvallisuus

DNA:n varmennejärjestelmän laitteistoina käytetään kyseiseen käyttötarkoitukseen sopivia laitteistoja.

10.7 Varmennejärjestelmän elinkaaren hallinta

10.7.1 Varmennejärjestelmän kehittämiseen liittyvä valvonta

Järjestelmän kehitys ja testaus tapahtuu erillisessä testiympäristössä. Ainoastaan testatut, toimivat ja hyväksytyt ratkaisut siirretään tuotantojärjestelmään.

10.7.2 Turvallisuuden hallinta

Varmentajan tietoturvallisuutta hallitaan varmentajan tietoturvapolitiikan mukaisesti.

10.8 Tietoverkon turvallisuus

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

10.9 Turvamoduulin käytön valvonta

DNA varmentaja huolehtii siitä, että varmentajan yksityiset avaimet on suojattu paljastumista ja luvatonta käyttöä vastaan. Varmentajan yksityisistä avaimista otetaan varmuuskopio kriittisen tietoturvallisuuden edellyttämällä tavalla.

11 Varmenneprofiilit

11.1 Varmenteiden tekniset tiedot

11.1.1 Yhteiset attribuutit

DNA:n julkaisema mobiilivarmenne noudattaa X.509 v.3 suositusta ja sisältö on normaalin käytännön mukainen. Käyttäjän sähköinen asiointitunnus talletetaan *Subject*-kenttään *SerialNumber*-attribuuttiin ja liittymäkortin ICCID talletetaan *eidSmartCardSerialNumber*-attribuuttiin.

Lisäksi varmenteen myönnön yhteydessä tehdyn ensitunnistuksen mahdollisen ketjutuspolun pituus on talletettu attribuuttiin *identificationPathLength*, jonka arvo on nolla, jos henkilöllisyys on todettu henkilökohtaisesti kirjallisista asiakirjoista. Muussa tapauksessa sen arvo kertoo ensitunnistuksen tunnistusketjun pituuden. Varmenteen tietosisältö on kuvattu varmennepolitiikan liitteessä 1.

11.1.2 Varmentajakohtaiset attribuutit

DNA voi lisätä varmenteeseen tarpeelliseksi katsomiaan RFC-5280:n mukaisia kenttiä, joista kerrotaan erikseen varmennuskäytännössä. Toiminnallisen yhteensopivuuden varmistamiseksi kyseiset laajennuskentät eivät ole kriittisiä.

12 Varmennuskäytännön hallinnointi

12.1 Muutosmenettely

DNA voi kirjallisella päätöksellä muuttaa määrityksiä lainsäädännöllisten tai toiminnallisten vaatimusten vuoksi.

Määritysten muutokset on kirjattava varmennuskäytäntöön seuraavassa kuvatulla tavalla.

12.1.1 Kohdat, joita voi muuttaa ilman tiedonantoa käyttäjille ja palveluntarjoajille

Tähän dokumenttiin voidaan tehdä oikeinkirjoitukseen ja ulkoasuun liittyviä korjauksia sekä muutoksia yhteystietoihin ilman ilmoitusta käyttäjille tai palveluntarjoajille. Dokumentista voidaan julkaista käännöksiä eri kielillä ilman erillistä ilmoitusta. Käännöksen ja suomenkielisen tekstin ollessa ristiriidassa keskenään suomenkielinen teksti on voimassa.

Kohtia, jotka DNA:n mielestä eivät merkittävästi vaikuta mobiilivarmennepalveluun, varmenteiden omistajiin ja luottaviin osapuoliin, voidaan muuttaa ilman ilmoitusta.

Uusien osapuolien liittyminen luottamusverkostoon ei muuta varmennuskäytäntöä.

12.1.2 Kohdat, joiden muutos vaatii tiedonannon käyttäjille ja palveluntarjoajille

Kaikkia varmennuskäytännön kohtia voidaan muuttaa ilmoittamalla tulevista pääasiallisista muutoksista käyttäjille ja palveluntarjoajille vähintään 60 päivää ennen muutosten voimaan astumista.

12.1.3 Muutokset, joiden johdosta täytyy laatia uusi varmennepolitiikka

Varmennuskäytännön uudistuminen ei edellytä uuden politiikan laatimista.

12.2 Julkaiseminen ja tiedottaminen

DNA julkaisee varmennuskäytännön, ja se on saatavilla varmentajien Internet-sivuilta.

DNA pitää asiakirjoista versionhallintaa sekä arkistoi kaikki varmennuskäytäntöversiot ja ne ovat pyydettäessä saatavilla.

Viiteluettelo

[RFC3647] S. Chokhani, W. Ford., R. Sabett, C. Merrill, S. Wu. “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. IETF RFC3647,November 2003. URL http://tools.ietf.org/html/rfc3647.

[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk. “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. IETF RFC5280,May 2008. URL http://tools.ietf.org/html/rfc5280.

[X.509] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1997, "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework."