DNA Mobiilivarmenne

VARMENNUSKÄYTÄNTÖ

DNA Oy:n varmennuskäytäntö mobiiliasiointivarmenteita varten
Versio 1.1
Voimassa 21.10.2011 lähtien

DNA Oy

Ansatie 6a B
PL 41
01741 Vantaa

Puhelin
044 0440

Y-tunnus
0592509-6

Kotipaikka
Vantaa

www.dna.fi

1 Yhteystiedot

1.1 Varmennuskäytäntöä hallinnoiva organisaatio

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

DNA Oy,
PL 41,
01741 Vantaa
Y-tunnus: 0592509-6

Sähköposti: mobiilivarmenne@dna.fi

1.2 Varmennuskäytännön tunnisteet

Tämän varmennuskäytännön nimi on

"DNA Oy: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 mobiili asiointivarmenteita varten".

Varmennepolitiikan tunniste (Object Identifier) on: 1.2.246.277.1.11.4.1.2.1

22.3.2010

Sisältö

2 Käsitteet ja termit

Finnish-language term used by DNA	Commonly used term in English	Description
Aktivointitieto, Tunnusluku	Activation Data	PIN code or password protecting the use of a personal key; the key can be activated by entering this code. Mobile certificates' personal keys are located on the phone SIM card.
Allekirjoituksen luomistie-dot	Signature Creation Data	Unique data package used by the signer for creating its electronic signature such as codes and personal keys.
Hakemistopalvelu	Directory Service	A service in the Public Key Infrastructure, comprising user certificates and possible related information as well as directories including revocation lists. Usually maintained by the authenticator him/herself.
Julkinen avain	Public Key	The public part of an asymmetric key pair that is used in public key encryption techniques. The public key is included in the certificate which the authenticator pub-lishes in the directory service.
Julkisen avaimen järjestelmä	Public Key Infrastructure (PKI)	A system enabling the use of public keys, in which the Certification Authority authenticates the public part of the key pair by means of its electronic signature, dis-tributes these certificates to other users, maintains a public key directory and revocation list, and possibly provides other services related to system use.
Julkisen avaimen menetelmä	Public key method	An asymmetric encryption method, in which each en-cryption user has two interrelated keys. One of the key pair keys is a public key published in a public directory, while the other one is a private key only possessed by the key pair user. Data encrypted using the private key can only be decrypted using the corresponding public key and vice versa.
Juurivarmentaja	Root CA	The highest trusted party in a Public Key Infrastructure that signs, distributes and, if necessary, cancels the certificates to lower-level Certification Authorities.
Kiistämättömyys	nonRepudiation	Use purpose of key for conferring contractual, legal validity upon an advanced electronic signature made

		using the key in question. Non-repudiation keys can be used for signing contracts. When a document is signed using a non-repudiation key, it becomes possible to verify the document's integrity and authenticity by using a certificate corresponding to said key. Cf. Electronic signature below.
Liittymäkortti (SIM)	Subscriber Identity Module	The card to which the phone subscription is tied. Usually referred to as a SIM card.
Loppukäyttäjä, Varmenteen omistaja	End Entity	The person to whom the authenticator has issued a certificate. The end entity uses the certificate and is in lawful possession of the private key corresponding to the public key included in the certificate as well as the codes required for using it.
Luottava osapuoli	Relying Party	Party providing electronic services for end entities. The relying party acts relying on the certificate and/or authenticating the digital signature by means of the certificate.
Luotettu varmenne	Trust Anchor	A certificate that relying parties position at the apex of their certificate hierarchy, certificates appearing under which they must authenticate.
Mobiilivarmenne	Mobile Certificate	The mobile certificate is a certificate based on private keys located on mobile terminal SIM cards. A mobile certificate complying with this Certificate Policy can be used for the electronic identification of a person as well as for encrypting communications and electronic signatures. The mobile certificate can be used in line with its purpose of use in administrative applications and services as well as those provided by private companies. In this Certificate Policy the capitalised term Mobile Certificate will be used in order to promote legibility, unless otherwise required by the context.
Mobiilivarmenne	Mobile Certificate	The term used for referring to the mobile certificate in this document.
Varmentaja	Registration Authority (RA)	The party in charge of identifying certificate applicants and for checking the information registered in the certificate application. The registration authority operates as a Certification Authority-certified part of the certificate organisation.
RSA	RSA	An asymmetric encryption algorithm used for creating

		an asymmetric key pair. The acronym is derived from the surnames of its inventors − Rivest, Shamir and Adleman.
Sulkulista	Certificate Revocation List (CRL)	A list of certificates in the Public Key Infrastructure that have been revoked. The Certification Authority publishes the revocation list in the directory service.
Suostumus	Consent	Authenticating a transaction or procedure using a key whose purpose of use is *digitalSignature* but not nonRepudiation.
Sähköinen allekirjoitus	Electronic signature	A person's legible signature on a computer, or its equivalent, such as a digital signature, as proof of the link between a document or message related to the signature and a specific person. In spoken language, electronic signature usually refers to a digital signature, which includes the key used for making nonRepudiation among its uses.
Todentaminen	Authentication; Verification	Verifying a system user (person, organisation or device) or, in communications, identification of the other party
Tunnistaminen	Identification	Identification of the other party while using services. At its simplest, a transaction answering the question: “Who are you?”
Tunnistusväline		The SIM card, including private keys and the related codes.
Vahvistaminen	Validation	Establishment of the authenticity of a certificate, an operation performed on the certificate, or its outcome.
Varmenne	Certificate	A certificate is a package comprising the person’s public key, name and other data included in the certificate which the Certification Authority has signed using its private key. The authenticity of a certificate can be verified by checking the Certification Authority’s digital signature.
Varmennehakemus	Certificate Application	A certificate application is a form including the certificate applicant’s personal, organisation and contact information that is filled in by the applicant, accepted by the application acceptor and, if necessary, signed by a trusted party.

Varmenneorganisaatio		Members of the certificate organisation include the Certification Authority, registration authority, card manufacturer, directory and revocation list service providers, and other service providers whose services the Certification Authority uses.
Varmennepalvelu		The authentication service is an identification and signature service based on certificates. The party relying on the certificates uses this service in providing services for the certificate owners.
Varmennepolitiikka	Certificate Policy (CP)	A specified set of rules enabling the assessment of the certificate's suitability to a specific purpose of use as well as the general safety and other requirements. **The Certificate Policy (CP)** is a description, drafted by the Certification Authority, concerning the procedures and principles that are followed when issuing certificates. The Certification Practice Statement is a more detailed description of the activities undertaken by the Certification Authority.
Varmennepolku	Certificate Path	A [logical] certificate chain required to authenticate the origin of the certificate, extending from the end entity's certificate to the root CA's certificate.
Varmennepyyntö	Certificate Request	A certificate request is a digital certificate creation and publishing request sent to the Certification Authority and created by the Registration Authority that is based on a certificate application.
Varmennuskäytäntö	Certification Practice Statement (CPS)	A detailed description of the practices used by the certification organisation when issuing and managing certificates. **The Certification Practice Statement depicts how the Certification Authority carries out its Certificate Policy, while also depicting in detail the procedures and practices followed by the Certification Authority.** The structure of the Certificate Policy and Certification Practice Statement follows, for the most part, IETF RFC 3647 [RFC3647].
Varmentaja	Certification Authority (CA)	The certification member that issues certificates by signing the certificate data using its private key.

Yksityinen avain	Private Key	The secret part of an asymmetric key pair used in Public Key encryption techniques. The private key is typically used for providing a digital signature or opening a message encrypted using the public key. In spoken language, the term secret key is also used. The certificate owner's private keys are stored on a SIM card in order to protect from unauthorised use.

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. Mobiilivarmennepalvelu täyttää vahvan sähköisen tunnistamisen vaatimukset, jotka on määritetty lainsäädännössä.

Mobiilivarmennepalvelun käyttöönotto vaatii DNA:n vahvaa tunnistautumista tukevan liittymäkortin. Palvelun käyttöönotto saattaa vaatia matkapuhelimen liittymäkortin vaihtoa.

Käyttäjä voi rekisteröidä Mobiilivarmennepalvelun käyttöönsä henkilökohtaisesti DNA:n hyväksymissä toimipisteessä. Rekisteröinnin yhteydessä DNA:n edustaja varmistaa käyttäjän henkilöllisyyden passilla, ajokortilla tai henkilökortilla.

Rekisteröinti on mahdollista myös 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 eivät joudu muiden ulottuville.

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

Palveluntarjoajat voivat liittyä valitsemansa operaattorin Mobiilivarmennepalveluun, ja heidän tarjoamansa palvelu tulee samalla kaikkien Mobiilivarmennepalvelua tarjoavien operaattorien Mobiilivarmenne-asiakkaiden saataville. Mobiilivarmennepalvelinliitännän käyttöönotto edellyttää sekä sopimuksen tekemistä operaattorin kanssa että tarvittavia sovellustason liityntöjä tietojärjestelmiin.

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

Mobiilivarmennepalvelu mahdollistaa uudenlaisten sähköisten palvelujen toteutuksen. Käyttäjä voidaan todentaa tietokoneella ja matkapuhelimella toimivissa internet-palveluissa. Todentaminen voidaan helposti ja luotettavasti tehdä myös erilaisissa puhelinpalveluissa ja asiakaspalvelutilanteessa.

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. Tämä mahdollistaa tuottavuuden kasvun ja paperien käsittelyn vähenemisenä.

5.2 Varmennuskäytäntö

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

5.3 DNA 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 verkkosivuilla:
www.dna.fi/mobiilivarmenne/

5.4 Varmennusorganisaatio

DNA varmentajan tiedot ovat saatavilla DNA verkkosivuilta:

www.dna.fi/mobiilivarmenne/

5.4.1 Varmentaja

5.4.2 Rekisteröijä

Rekisteröintipalvelusta vastaa DNA Oy.

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

Mobiilivarmenteen henkilökohtaisen rekisteröintipalvelun rekisteröijinä toimivat DNA:n paikalliset asiointipisteet sekä muut DNA:n kanssa rekisteröintiä koskevan sopimuksen tehneet organisaatiot.

Itsepalvelurekisteröintipalvelun rekisteröijänä toimii DNA.

Luettelo DNA:n rekisteröijistä on osoitteessa:
www.dna.fi/mobiilivarmenne/

5.4.3 Liittymäkortin liikkeellelaskija

DNA tai DNA:n Partneri toimittaa mobiilivarmenteen rekisteröinnissä tarvittavat tiedot liittymän loppukäyttäjälle. DNA:n liittymäkortin ajantasaiset tiedot ovat osoitteessa
www.dna.fi/mobiilivarmenne/

5.4.4 Sulkupalvelu

DNA:n sulkupalvelun tavoitat joko DNA:n asiakaspalveluun soittamalla tai sähköisesti DNA:n verkkosivujen kautta. DNA:n sulkupalvelun ajantasaiset tiedot ovat osoitteessa

www.dna.fi/mobiilivarmenne/

5.4.5 Hakemistopalvelu

DNA ylläpitää julkista hakemistopalvelua. Julkisessa hakemistopalvelussa ovat ne DNA:n mobiilivarmenteet, joiden julkaisemiseen on varmenteen omistajan suostumus. DNA sallii pääsyn julkisen hakemistopalvelun tietoihin mobiilivarmennepalvelunsa tuotepolitiikan mukaisesti. DNA ylläpitää tarpeen mukaan hakemistopalveluista erillisiä kopioita.
Tiedot DNA:n hakemistopalveluista ovat osoitteessa:

www.dna.fi/mobiilivarmenne/

5.4.6 Varmenteen omistaja

DNA myöntää Mobiilivarmenteen varmenteen omistajalle.

5.4.7 Varmenteeseen luottava osapuoli

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

5.4.8 DNA:n kumppani

DNA:n mobiilivarmennepalvelun kumppani on yritys tai yhteisö, jonka kanssa DNA:lla on Mobiilivarmenne-kumppanisopimus. DNA:n kumppani toimii tämän varmennuskäytännön mukaisesti.

DNA:n kumppanit on listattu osoitteessa:

www.dna.fi/mobiilivarmenne/

5.5 Varmenteen käyttäminen

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

5.6 Osapuolten vastuut ja velvollisuudet

DNA on sitoutunut noudattamaan Luottamusverkoston Varmentajien yhteistä varmennepolitiikkaa.

DNA edellyttää muiden osapuolten kanssa tekemissään sopimuksissa, että osapuolet 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 tuotepäätöksellä rajoittaa pääsyä sulkulistoille ja hakemistoihin.

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

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

www.dna.fi/mobiilivarmenne/

Varmenteet julkaistaan hakemistossa, jonne on pääsy vain varmentajan järjestelmillä. Osa varmenteista voidaan julkaista julkisessa hakemistossa (esim. julkisille puhelinnumeroille myönnetyt varmenteet).

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 pääsyä rajoitetaan.

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

Seloste DNA:n julkaisemista tiedoista on saatavilla DNA:n www-sivuilla.

6.2 Auditointi

DNA tarkastaa rekisteröijiensä toimitilat, laitteet ja toiminnan tarkoituksenmukaisella tavalla.

DNA tarkastaa tarvittaessa oman toimintansa ulkoisella auditoijalla.

6.3 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 Oy
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 allekirjoittaa DNA.n tai DNA:n nimeämän kumppanin varmennehakemuksen ja hyväksyy varmenteen käyttöehdot. Nämä yhdessä muodostavat Mobiilivarmenne-sopimuksen käyttäjän ja Varmentajan välille.

Käyttäjä sitoutuu huolehtimaan mobiilivarmenteen ja tunnuslukujen säilyttämisestä asianmukaisesti sekä ilmoittamaan mahdollisen väärinkäytön tai varmenteiden tai liittymäkortin katoamisesta. Varmennehakemuksessa on kuvattu osapuolien oikeudet ja velvollisuudet.

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.

8.1.1 Varmenteen rekisteröinti sähköisessä kanavassa

Käyttäjä on tilannut liittymäänsä DNA Mobiilivarmenne -lisäpalvelun ja vastaanottanut PKI liittymäkortin sekä tutustunut DNA mobiilivarmennesopimusehtoihin ja rekisteröintiohjeeseen.

Rekisteröinnin yhteydessä tarvitaan käyttäjän henkilökohtaiset TUPAS tunnukset.

Rekisteröinti etenee seuraavasti.

1) Käyttäjä ottaa selainyhteydenyhteyden rekisteröintiportaaliin
   Käyttäjä tunnistetaan pankkitunnisteella tai vastaavalla vahvalla tunnistuksella.
2) Käyttäjä hyväksyy käyttöehdot
   Järjestelmä hakee käyttäjän sähköisen asiointitunnuksen Väestörekisterikeskuksesta.
3) Käyttäjä syöttää matkapuhelinnumeronsa (liittymänumero)
4) Käyttäjä tarkistaa henkilötietonsa, etunimet, sukunimen ja henkilötunnuksen
5) Käyttäjä luo avaimet matkapuhelimessaan
   Järjestelmä käynnistää avainten luonnin SIM-kortilla
6) Käyttäjä allekirjoittaa varmennepyynnön matkapuhelimellaan
7) Käyttäjä hyväksyy tai kieltää varmenteen julkaisemisen hakemistossa
8) Rekisteröijä ilmoittaa mobiilivarmenteen hakijalle, että varmenne on rekisteröity ja käytettävissä
9) Mobiilivarmennepalvelun laskutus käynnistyy

8.1.2 Varmenteen rekisteröinti palvelupisteessä

Käyttäjä on joko uusi DNA:n asiakas, hänellä on DNA:n liittymä tai hän on tilannut liittymäänsä lisäpalvelun DNA Mobiilivarmenne ja vastaanottanut PKI SIM-kortin sekä tutustunut rekisteröintiohjeeseen.

Rekisteröinnin yhteydessä käyttäjä tarvitsee henkilöllisyystodistuksen.

Mikäli mobiilivarmenteen hakija on uusi DNA:n asiakas, hakija allekirjoittaa DNA:n liittymäsopimuksen.

Mikäli mobiilivarmenteen hakijalla ei ole soveltuvaa liittymäkorttia, käyttäjä saa palvelupisteessä uuden liittymäkortin ennen rekisteröintiä.

Kun mobiilivarmenteen hakija hakee varmennetta, hän

1) hyväksyy DNA:n mobiilivarmennesopimuksen ehdot,
2) todistaa henkilöllisyytensä,
3) tarkistaa rekisteröijän ilmoittamien henkilötietojensa oikeellisuuden,
4) hyväksyy tai kieltää varmenteen julkaisun hakemistossa,

Rekisteröijä lähettää tarvittavat avaintenluontipyynnöt käyttäjän ilmoittamaan liittymänumeroon. Käyttäjä luo tarvittavat yksityiset avaimet ja PIN-numerot matkapuhelimellaan.

5) hyväksyy avaintenluontipyynnön
6) antaa sellaisen PIN-numeron jokaiselle luodulle avaimelle, ja muistaa sen tai tallentaa PIN-numeron turvallisesti,

Käyttäjä allekirjoittaa varmennepyynnön luomillaan avaimilla ja PIN-numerolla.

7) allekirjoittaa varmennepyynnön sähköisellä allekirjoituksella
8) Rekisteröijä ilmoittaa mobiilivarmenteen hakijalle, että varmenne on rekisteröity ja käytettävissä
9) Mobiilivarmennepalvelun laskutus käynnistyy

Varmenteen haltija huolehtii mobiilivarmenteen ja tunnuslukujen säilyttämisestä sekä mahdollisen väärinkäytön tai varmenteiden tai liittymäkortin katoamisen ilmoittamisesta.

8.2 Varmenteen hakijan tunnistaminen

Mobiilivarmenteen hakija tunnistetaan joko käyttäen vahvaa sähköistä tunnistamista tai henkilökohtaisesti rekisteröijän asiointipisteessä.

8.2.1 Tunnistusvälineen toimittaminen

Tunnistusvälineen toimittaminen vaatii DNA:n liittymäkortin ja liittymäsopimuksen. DNA liittymäkortin voi tilata DNA:n myyntikanavien kautta. Myymälässä asioitaessa käyttäjä saa liittymäkortin mukaansa. Muiden kanavien kautta kortti toimitetaan käyttäjälle postitse kirjattuna kirjeenä.

Tunnistusväline on DNA:n liittymäkortti, jossa on varmenteen haltijan luomat yksityiset avaimet ja niihin liittyvät tunnusluvut. Kun liittymäkortti toimitetaan asiakkaalle, siinä ei ole yksityisiä avaimia tai niiden tunnuslukuja. Tunnistusväline voidaan ottaa käyttöön onnistuneen rekisteröinnin jälkeen.

DNA varmistaa, että liittymäasiakkaalle toimitetaan Mobiilivarmenteen käytön kannalta oikeantyyppinen liittymäkortti. Liittymäkortti toimitetaan varmenteen hakijalle postitse tai henkilökohtaisesti asiointipisteessä.

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 voidaan sulkea mobiilivarmenteen soittamalla maksuttomaan DNA:n sulkupalvelunumeroon, sähköisesti DNA:n rekisteröintiportaalissa tai asioimalla varmenteen rekisteröinti pisteessä.

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 käytettyn 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

Mobiilivarmenteen omistaja voi tehdä mobiilivarmenteen sulkupyynnön seuraavilla tavoilla:

a) Puhelinsoitolla DNA:n sulkupalveluun,
b) Käymällä rekisteröijän luona tai
c) DNA:n sähköisessä asiointipalvelussa.

Varmenteen sulkeminen tehdään aina tilapäisesti ja varmenteen käyttä 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 Varmenteen sulkeminen tilapäisesti

DNA tekee mobiilivarmenteen sulkemisen aina tilapäisesti. Sulkemisen syykoodiksi merkitään muiden syykoodien lisäksi *certificateHold*.

8.5.6 Tilapäisen sulkupyynnön tekijä

Tilapäisen sulkupyynnön tekijää koskevat samat säännöt kuin pysyvän sulkupyynnön tekijää.

8.5.7 Tilapäisen sulkupyynnön tekemistapa

Tilapäistä sulkupyyntöä koskevat samat säännöt kuin pysyvää sulkupyyntöä.

8.5.8 Tilapäisen sulun aikarajoitukset

Tilapäinen sulku on voimassa kunnes se peruutetaan. Tilapäisen sulun purkupyynnön tekijää ja hänen tunnistamistansa koskevat samat säännöt kuin sulkupyynnön tekijää.

8.5.9 Varmenteen tilapäisen sulun purkaminen

DNA tunnistaa varmenteen tilapäisen sulun purkajan joko käyttäen vahvaa sähköistä tunnistamista tai henkilökohtaisesti rekisteröijän asiointipisteessä.

Varmenteen tilapäisen sulun purkamista ei voi tehdä DNA:n sähköisessä asiointipalvelussa käytettävillä tunnuksilla tai puhelinpalveluissa.

8.5.10 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.

8.5.11 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.

8.5.12 Suorakäyttöinen varmenteen tilan tarkistaminen

Sulkulistan sijaan varmentaja voi käyttää OCSP-palvelua tai DSS-palvelua varmenteen tilan tarkastamiseen. OCSP ja DSS palvelut käyttävät samaa sulkulistatietoa.

8.6 Varmenteen uusiminen

8.6.1 Varmenteen uusiminen nimenmuutoksen vuoksi

Kun varmenteen omistaja ilmoittaa nimenmuutoksesta DNA:lle, uusii DNA varmenteen samalla avainmateriaalilla ja samalla voimassaolon päättymisajalla kuin voimassa oleva varmenne.

Uusittu varmenne julkaistaan hakemistoissa samoin edellytyksin kuin alkuperäinen varmenne. Koska avainmateriaali ei muutu, voidaan varmenteen rekisteröinti tehdä ilman käyttäjän interaktiota.

Uusimisen yhteydessä nimi tarkistetaan Väestötietojärjestelmästä samaan tapaan kuin uuden varmenteen rekisteröinnin yhteydessä.

8.6.2 Varmenteen uusiminen varmenteen vanhenemisen vuoksi

Kun varmenne vanhenee, on varmenteen omistajan rekisteröitävä varmenne uudelleen.

DNA voi ilmoittaa varmenteen omistajalle hyvissä ajoin ennen varmenteen vanhenemista. Rekisteröitäessä uutta varmennetta sähköisessä asiointipalvelussa, voi henkilö tunnistautua vielä voimassa olevalla mobiilivarmenteella.

Uusimisen yhteydessä nimi tarkistetaan Väestötietojärjestelmästä samaan tapaan kuin uuden varmenteen rekisteröinnin yhteydessä.

8.6.3 Varmenteen uusiminen uuden ensitunnistamisen vuoksi

DNA uusii varmenteen samalla avainmateriaalilla ja samalla voimassaolon päättymisajalla kuin voimassa oleva varmenne, mikäli DNA tekee uuden ensitunnistamisen kasvokkain.

Uusimisen yhteydessä nimi tarkistetaan Väestötietojärjestelmästä samaan tapaan kuin uuden varmenteen rekisteröinnin yhteydessä.

8.7 Järjestelmän valvonta

DNA:n varmennejärjestelmän valvonta kuvataan DNA:n varmentajan tietoturvaohjeistuksessa. Ohjeistus toimitetaan Viestintävirastolle ja se on nähtävillä DNA:n toimipisteessä.

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.

10 Toiminnalliset vaatimukset

10.1 Vastuunjako

DNA varmentajan tehtävät on jaettu tehtävänmukaisiin vastuualueisiin.

Vastuualueet on kuvattu yksityiskohtaisesti DNA:n varmenneorganisaatio kuvauksessa.

10.2 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.

10.3 Tehtäväkohtainen tunnistaminen

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

- Varmenteen rekisteröijä, sähköinen rekisteröinti; XML allekirjoitus sovelluksen avaimilla.
- Varmenteen rekisteröijä, henkilökohtainen rekisteröinti; DNA:n kauppiastunnukset ja varmennepyynnön mobiilivarmenne todennus
- Varmennejärjestelmän ylläpitäjä; varmennejärjestelmän käyttämä oma sisäinen vahva tunnistusmenetelmä
- Varmennejärjestelmän muut käyttösovellukset; sulkupyynnöt; sovelluksen XML allekirjoitus
- Varmennejärjestelmän muut käyttäjät; varmennejärjestelmän käyttämä oma sisäinen vahva tunnistusmenetelmä

11 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.

11.1 Henkilökuntaa koskevan taustaselvityksen tekeminen

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

11.2 Taustaselvityksen tekemisessä noudatettava menettely

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

11.3 Koulutukseen liittyvät vaatimukset

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

11.4 Asiantuntemuksen ja osaamisen ylläpito

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

11.5 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.

11.6 Henkilökunnan käyttöön annettavat asiakirjat

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

12 Tekniset turvatoimet

12.1 Avainparin luominen, tallettaminen ja käyttöönotto

12.1.1 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 totettaa 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.

12.1.2 Liittymäkortin luovuttaminen hakijalle

Liittymäkortin luovutusprosessi (OBKG) on kuvattu kohdassa 8.2.1 .

Liittymäkortin luovutusprosessi (Pregen) ei sisälly tähän varmennuskäytäntöön.

12.1.3 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.

12.1.4 Varmentajan julkisen avaimen jakelu

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

12.1.5 Avainten pituudet

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

12.1.6 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.

12.2 Varmentajan yksityisten avainten suojaaminen

12.2.1 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.

12.2.2 Varmentajan yksityisen avaimen käsittelyyn osallistuva henkilökunta

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

12.2.3 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.

12.2.4 Yksityisen avaimen arkistointi

DNA varmentajan tai käyttäjän yksityisiä avaimia ei arkistoida.

12.2.5 Yksityisen avaimen hallinnointi turvamoduulissa

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

12.3 Varmenteen omistajan avainten suojaaminen

12.3.1 Liittymäkorttia koskevat standardit

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

12.3.2 Yksityisen avaimen luovutus luotetun osapuolen huostaan

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

12.3.3 Yksityisen avaimen varmuuskopio

Mobiilivarmenteeseen liittyvistä yksityisistä avaimista ei ole kopioita.

12.3.4 Yksityisen avaimen arkistointi

Mobiilivarmenteeseen liittyvää yksityistä avainta ei arkistoida.

12.3.5 Yksityisen avaimen hallinnointi liittymäkortilla

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

12.4 Muut avainparin hallintaan liittyvät seikat

12.4.1 Julkisen avaimen arkistointi

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

12.4.2 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 .

12.5 Liittymäkortilla olevien yksityisten avainten tunnusluvut

12.5.1 Tunnusluvun luominen ja käyttöönotto

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

12.5.2 Tunnusluvun suojaus

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

12.6 Varmennejärjestelmän laitteiden käyttöön ja pääsyyn liittyvät turvallisuusvaatimukset

12.6.1 Laitteistoturvallisuus

DNA:n varmennejärjestelmän laitteistoina käytetään kyseiseen käyttötarkoitukseen sopivia laitteistoja.

12.7 Varmennejärjestelmän elinkaaren hallinta

12.7.1 Varmennejärjestelmän kehittämiseen liittyvä valvonta

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

12.7.2 Turvallisuuden hallinta

Varmentajan tietoturvallisuutta hallitaan varmentajan tietoturvapolitiikan mukaisesti.

12.7.3 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.

12.7.4 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.

13 Varmenne- ja sulkulistaprofiilit

13.1 Varmenteiden tekniset tiedot

13.1.1 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.

13.1.2 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.

13.1.3 Sulkulistaprofiili

DNA voi tarjota erilaisia sulkulistaprofiileita. Sulkulistaprofiilit on kuvattu DNA:n verkkosivulla:

www.dan.fi/mobiilivarmenne/sulkulista

14 Varmennuskäytännön hallinnointi

14.1 Muutosmenettely

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

Määritysten muutokset on kirjattava varmennuskäytäntöön seuraavassa kuvatulla tavalla.

14.1.1 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.

14.1.2 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.

14.1.3 Muutokset, joiden johdosta täytyy laatia uusi varmennepolitiikka

Varmennuskäytännön uudistuminen ei edellytä uuden politiikan laatimista.

14.1.4 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.

Versio	Päiväys	Kuvaus
1.0	1.11.2010	Versio 1

15 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."
