

DNA Mobiilivarmenne  
**VARMENNUSKÄYTÄNTÖ**

DNA Oy:n varmennuskäytäntö mobiiliasiointivarmennei tavarten  
Versio 1.1  
Voimassa 21.10.2011 lähtien



**DNA Oy**

Ansatie 6a B  
PL 41  
01741 Vantaa

**Puhelin**

0440440

**Y-tunnus**

0592509-6

**Kotipaikka**  
Vantaa

[www.dna.fi](http://www.dna.fi)

## 1 Yhteystiedot

### 1.1 Varmennuskäytäntöhallinnoiva organisaatio

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

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

Sähköposti: [mobiilivarmente@dna.fi](mailto:mobiilivarmente@dna.fi)

### 1.2 Varmennuskäytännöntunnisteet

Tämän varmennuskäytännön nimion

"DNA Oy:n varmennuskäytäntö mobiilivarmenteita varten".

Varmennuskäytännöntunniste (ObjectIdentifier) on:

1.3.6.1.4.1.36036.1.1.2.1

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

Varmennuskäytännöntunnistetieto on sijoitettu varmenteeseen X.509v3-määrityksen [X.509] mukaiseen varmennuskäytännöntunnistetietokenttään (Certificate Policy OID). Tämä kenttä on avullavarmenteeseen luotettavaosapuolivoivarmistuv varmenteensopivuudesta käytettävässä olevaan käyttötarkoitukseen.

### 1.3 Varmennepolitiikantunnisteet

DNA:n varmennuskäytäntö noudattaa suomalaisten mobiilioperaattoreiden yhteistä varmennepolitiikkaa, ja sentunnisteet ovat:

Varmennepolitiikan nimion "MOBIILIASIOINTIVARMENNE -VARMENNEPOLIITIIKKA-Operaattoreiden mobiiliasiointivarmenteita varten".

Varmennepolitiikantunniste (ObjectIdentifier) on :1.2.246.277.1.11.4.1.2.1



## Sisältö

1 Yhteystiedot.....	2
1.1 Varmennuskäytäntöhallinnoivaorganisaatio..	2
1.2 Varmennuskäytännötunnisteet.....	2
1.3 Varmennepoliitikantunnisteet.....	2
2 Käsitteetjatermit.....	6
3 Lyhenteet.....	10
4 Roolit.....	11
5 Johdanto.....	11
5.1 Mobiilivarmennepalvelu.....	11
5.2 Varmennuskäytäntö.....	12
5.3 Mobiilivarmenne.....	12
5.4 Varmennusorganisaatio.....	13
5.4.1 Varmentaja.....	13
5.4.2 Rekisteröijä.....	13
5.4.3 Liittymäkortinliikkeellelaskija.....	13
5.4.4 Sulkupalvelu.....	13
5.4.5 Hakemistopalvelu.....	14
5.4.6 Varmenteenomistaja.....	14
5.4.7 Varmenteeseenluottavaosapuoli.....	14
5.4.8 DNA:n kumppani.....	14
5.5 Varmenteenkäyttäminen.....	14
5.6 Osapuolten vastuutjavelvollisuudet.....	14
6 Yleiset ehdot.....	16
6.1 Tietojen julkaiseminen jasaatavuus.....	16
6.1.1 Varmentajantietojen julkaiseminen.....	16
6.1.2 Tietojensaataavuus.....	16
6.1.3 Tietovarastot.....	16
6.2 Auditointi.....	17
6.3 Tietojen luottamuksellisuusjulkisuus.....	17
7 Varmentajanyksilöinti.....	18
7.1 Varmentajannimeäminen.....	18
7.2 Avainparin uusiminen varmenteensulkemisen jälkeen.....	18
8 Toiminnalliset vaatimukset.....	18
8.1 Varmenteenhakeminen.....	18
8.1.1 Varmenteenrekisteröintisähköisessäkanavassa.....	19
8.1.2 Varmenteenrekisteröintipalvelupisteessä..	19
8.2 Varmenteenhakijantunnistaminen.....	20
8.2.1 Tunnistusvälineentoimittaminen.....	20
8.3 Varmenteenmyöntäminen.....	20
8.4 Varmenteenluominen.....	21
8.5 Varmenteenvoimassaolon päättyminenjaskemien en.....	21
8.5.1 Varmenteensulkemisen edellytykset.....	21
8.5.2 Sulku pyynnön tekijä.....	21
8.5.3 Sulku tapahtuma.....	22
8.5.4 Sulku tapahtuman ajoitus.....	22

8.5.5	Varmenteensulkeminentilapäisesti.....	22
8.5.6	Tilapäisensulkupyynnöntekeijä.....	22
8.5.7	Tilapäisensulkupyynnöntekestapa.....	23
8.5.8	Tilapäisensulunaikarajoitukset.....	23
8.5.9	Varmenteentilapäisensulunpurkaminen.....	23
8.5.10	Sulkulistanjulkaisutiheys.....	23
8.5.11	Sulkulistanjakelupisteet.....	23
8.5.12	Suorakäyttöinenvarmenteentilantarkistaminen.....	23
8.6	Varmenteenuusiminen.....	24
8.6.1	Varmenteenuusimennimenmuutoksenvuoksi.....	24
8.6.2	Varmenteenuusiminenvarmenteenvanhenemisen vuoksi.....	24
8.6.3	Varmenteenuusiminenuudenensitunnistamisen vuoksi.....	24
8.7	Järjestelmänvalvonta.....	25
8.8	Varmenteisiinliittävientietojenarkistointi.....	25
8.8.1	Tallennettavaaineisto.....	25
8.8.2	Arkistojensuojaus.....	25
8.8.3	Arkistojenvarmistusmenettelyt.....	25
8.8.4	Arkistotietojenhankinta-javarmistusmenettelyt.....	25
8.9	Varmentajanavaintenuusiminen.....	26
8.10	Toiminnanjatkumisenhallintajapoikkeustapaus tenkäsittely.....	26
8.10.1	Varmentajanyksityinenavainonpaljastunut taivarmentajanvarmenneonsuljettu.....	26
8.10.2	Turvallisuudenvaarantumisenluonnonmullistuskentaimuunkatastrofinseurauksena.....	26
8.11	Varmentajatoiminnanlakkauttaminen.....	26
9	Fyysiset,toiminnallisetjahrenkilöstöturvallisuuteenliittyvätvaatimukset.....	28
9.1	Fyysinenturvallisuus.....	28
9.1.1	Sijaintijarakennustenominaisuudet.....	28
9.1.2	Fyysinenpääsytoimitilaan.....	28
9.1.3	Varajärjestelyt.....	28
10	Toiminnallisetvaatimukset.....	29
10.1	Vastuunjako.....	29
10.2	Tehtäviinvaadittavienhenkilöidenlukumäärä.....	29
10.3	Tehtäväkohtaintunnistaminen.....	29
11	Henkilöturvallisuus.....	29
11.1	Henkilökuntaakoskevantaustaselvityksentekeminen.....	30
11.2	Taustaselvityksentekemisessänoudatettavamenettely.....	30
11.3	Koulutukseenliittyvätvaatimukset.....	30
11.4	Asiantuntemuksenjaosaamisenylläpito.....	30
11.5	Poikkeamistajohtuvattoimenpiteet.....	30
11.6	Henkilökunnankäyttöönannettavatasiakirjat.....	30
12	Teknisetturvatoimet.....	31
12.1	Avainparinluominen,tallettaminenjakäyttöönotto.....	31
12.1.1	Avainparinluominen.....	31
12.1.2	Liittymäkortinluovuttaminenhakijalle.....	31
12.1.3	Varmenteenhakijanjulkisenavaimentoimittaminenvarmentajalle.....	31
12.1.4	Varmentajanjulkisenavaimenjaku.....	32
12.1.5	Avaintenpituudet.....	32
12.1.6	Avaintenkäyttötarkoitukset.....	32

12.2	Varmentajanyksityistenavaintensuojaaminen .....	32
12.2.1	Turvamoduuliakoskevatstandardit .....	32
12.2.2	Varmentajanyksityisenavaimenkäsittelyyno sallistuvahenkilökunta .....	33
12.2.3	Yksityisenavaimenvarmuuskopio .....	33
12.2.4	Yksityisenavaimenarkistointi .....	33
12.2.5	Yksityisenavaimenhallinnointiturvamoduuli ssa .....	33
12.3	Varmenteenomistajanavaintensuojaaminen... ..	33
12.3.1	Liittymäkorttiakoskevatstandardit .....	33
12.3.2	Yksityisenavaimenluovutusluotetunosapuol enhuostaan .....	33
12.3.3	Yksityisenavaimenvarmuuskopio .....	33
12.3.4	Yksityisenavaimenarkistointi .....	34
12.3.5	Yksityisenavaimenhallinnointiliittymäkort illa .....	34
12.4	Muutavainparin hallintaan liittyvät seikat.. ..	34
12.4.1	Julkisenavaimenarkistointi .....	34
12.4.2	Julkisten jayksityistenavainten voimassaol o aika .....	34
12.5	Liittymäkortilla olevien yksityistenavainten tunnusluvut .....	34
12.5.1	Tunnusluvun luominen ja käyttöön otto .....	34
12.5.2	Tunnusluvun suojaus .....	34
12.6	Varmenne järjestelmän laitteiden käyttöön ja pä äsyyn liittyvät turvallisuusvaatimukset .....	34
12.6.1	Laitteistoturvallisuus .....	34
12.7	Varmenne järjestelmän elinkaaren hallinta... ..	35
12.7.1	Varmenne järjestelmän kehittä miseen liittyvä valvonta .....	35
12.7.2	Turvallisuuden hallinta .....	35
12.7.3	Tietoverkon turvallisuus .....	35
12.7.4	Turvamoduulin käytön valvonta .....	35
13	Varmenne-jasulkulistaprofiilit .....	35
13.1	Varmenteiden tekniset tiedot .....	35
13.1.1	Yhteiset attribuutit .....	35
13.1.2	Varmentajakohdaiset attribuutit .....	36
13.1.3	Sulkulistaprofiili .....	36
14	Varmennuskäytännön hallinnointi .....	36
14.1	Muutosmenettely .....	36
14.1.1	Kohdat, joiden muutos vaikuttaa ilmantiedon antoa käyttäjille ja palveluntarjoajille .....	36
14.1.2	Kohdat, joiden muutos vaikuttaa tiedonannon käyttäjille ja palveluntarjoajille .....	36
14.1.3	Muutokset, joiden johdosta täytyy laatia uusi ivarmennepolitiikka .....	36
14.1.4	Julkaiseminen ja tiedottaminen .....	36
15	Viiteluettelo .....	37
16	.....	37

## 2 Käsitteet ja termit

Finnish-language term used by DNA	Commonly used term in English	Description
Aktivointitieto, Tunnusluku	ActivationData	PINcodeorpasswordprotectingthe useofapersonal key;thekeycanbeactivatedbyenteringthiscode . Mobilecertificates'personalkeysarelocatedont he phoneSIMcard.
Allekirjoituksenluomistiedot	SignatureCreation Data	Uniquedatapackageusedbythesignerforcreating itselectronicssignaturesuchascodesandpersonal keys.
Hakemistopalvelu	DirectoryService	Aserviceinth ePublicKeyInfrastructure,comprising usercertificatesandpossiblerelatedinformation as wellasdirectoriesincludingrevocationlists.Usually maintainedbytheauthenticatorhim/herself.
Julkisenavain	PublicKey	Thepublicpartofan asymmetrickeypairthat isused inpublickeyencryptiontechniques.Thepublickey is includedinthecertificatewhichtheauthenticator publishesinthedirectoryservice.
Julkisenavaimen järjestelmä	PublicKey Infrastructure (PKI)	Asystemenablingtheuseofpublickeys,inwhich the CertificationAuthorityauthenticatesthepublicpartof thekeypairbymeansofitselectronicssignature, distributes these certificates to other users, maintains a publickeydirectoryandrevocationlist,andpossibly providesotherservicesrelatedtosystemuse.
Julkisenavaimen menetelmä	Publickeymethod	An asymmetric encryption method, in which each encryption 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	RootCA	The highest trusted party in a PublicKeyInfrastructure 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, Varmenteenomistaja	End Entity	The person to whom the authenticator has issued a certificate. The end entity uses the certificate 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.
Luottavaosapuoli	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.
Luotettuvarmenne	Trust Anchor	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 cryptological algorithm used for creating

		anasymmetrickeypair. Theacronymisderivedfromthesurnamesofitsinventors–Rivest, ShamirandAdleman.
Sulkulista	Certificate RevocationList (CRL)	AlistofcertificatesinthePublicKeyInfrastructurethat havebeenrevoked. TheCertificationAuthoritypublishestherevocationlistinthedirectoryservice.
Suostumus	Consent	Authenticatingatransactionorprocedureusingakey whosepurposeofuseis <i>digitalSignature</i> butnotnon-Repudiation.
Sähköinenallekirjoitus	Electronic signature	Aperson'slegiblesignatureonacomputer, oritsequivalent, suchasadigitalsignature, asproofofthelinkbetweenadocumentormessagerelatedtothesignatureandaspecificperson.  Inspokenlanguage, electronicsignatureusuallyrefers toadigitalsignature, whichincludesthekeyused for makingnonRepudiationamongitsuses.
Todentaminen	Authentication; Verification	Verifyingasystemuser(person, organisationordevice)or, incommunications, identificationofthe other party
Tunnistaminen	Identification	Identificationofthe otherpartywhileusingservices. At its simplest, atransactionansweringthequestion: "Whoareyou?"
Tunnistusväline		TheSIMcard, includingprivatekeysandtherelated codes.
Vahvistaminen	Validation	Establishmentoftheauthenticityofacertificate, an operationperformedonthecertificate, oritsoutcome.
Varmenne	Certificate	Acertificateisapackagecomprisingtheperson's publickey, nameandotherdataincludedinthecertificatewhichtheCertificationAuthorityhasassignedto itsprivatekey. Theauthenticityofacertificate canbe verifiedbycheckingtheCertificationAuthority's digital signature.
Varmennehakemus	CertificateApplication	Acertificateapplicationisaformincludingthecertificateapplicant'spersonal, organisationandcontact informationthatisfilledinbytheapplicant, accepted bytheapplicationacceptorand, ifnecessary, signed byatrustedparty.

Varmenneorganisaatio		Members of the certification organisation include the Certification Authority, registration authority, card manufacturer, directory and revocation lists 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)	<p>A specified set of rules enabling the assessment of the certificate's suitability to a specific purpose of uses as well as the general safety and other requirements.</p> <p><b>The Certificate Policy (CP)</b> 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.</p>
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)	<p>A detailed description of the practices used by the certification organisation when issuing and managing certificates.</p> <p><b>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.</b></p> <p>The structure of the Certificate Policy and Certification Practice Statement follows, for the most part, IETF RFC 3647 [RFC 3647].</p>
Varmentaja	Certification Authority (CA)	The certification member that issues certificates by signing the certificated data using its private key.

Yksityinen avain	PrivateKey	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 jättämisen mahdollistava palvelualusta.
OCSP	Online Certificate Status Protocol	Reaaliaikainen sulkutietoprotokolla
OID	Object Identifier	Varmennepolitiikan tunnistetieto
PDS	PKI Disclosure Statement	Yksinkertaistettu kuvaus varmenteen käyttöehdoista ja rajoituksista.
PIN	Personal Identification Number	Tunnusluku, PIN-koodi
PKI	Public Key Infrastructure	Julkisen avaimenvarmennejärjestelmä
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

Liittymäntilaaaja	Vastalaskujenmaksusta. Luonnollinen henkilö tai yritys, joka sallii liittymän palvelut. Voi olla samakuin liittymän käyttäjä.
Liittymän käyttäjä	Liittymän palveluiden käyttäjä, luonnollinen henkilö, joka on merkitty liittymän haltijaksi. Käyttäjä voi olla samakuin liittymäntilaaaja.
Varmenteenhakija	Ainasamaluonnollinen henkilö, joka on liittymän käyttäjä. Liittymän haltijaksi on oltava merkittynä varmenteenhakija.
Varmenteenomistaja	Luonnollinen henkilö, jolle on myönnetty mobiilivarmenne. Ainasamaluonnollinen henkilö, joka on varmenteenhakija eli liittymän käyttäjä.

#### 5 Johdanto

##### 5.1 Mobiilivarmennepalvelu

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

Palvelutarjoajille mobiilivarmennepalvelu mahdollistaa käyttäjien henkilöllisyyden luotettavan todentamisen sekä palveluun liittyvien, asiakkaan hyväksyntää vaativien, tapahtumien vahvistamisen asiakkaan sähköisellä allekirjoituksella. Mobiilivarmennepalvelu täyttää vahvan sähköisennestämisen vaatimukset, jotka on määrätty lainsäädännössä.

Mobiilivarmennepalvelun käyttöönotto vaatii DNA:n vahvaa tunnistautumista tukevan liittymäkortin. Palvelun käyttöönottoa vaati matkapuhelimen liittymäkortinvaihto.

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

Rekisteröinti on mahdollista myös DNA:n itsepalvelu-kanavassa, jolloin DNA:n rekisteröintisovellus varmistaa käyttäjän henkilöllisyyden pankkitunnuksilla.

Mobiilivarmennepalvelu on sidottu käyttäjän henkilöllisyyteen ja mahdollistaa asiointin kaikissa mobiilivarmennepalvelua 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 väärinkäsiin, on käyttäjän ilmoitettava viivytyksellä asiasta DNA:lle. Ilmoituksen voi tehdä joko soittamalla DNA:n asiakaspalveluun tai sähköisesti. DNA sulkee käyttäjän Mobiilivarmennepalvelun ilmoituksensaatuun.

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

Käyttäjän yksilöivä identiteetti perustuu sähköiseen asiointitunnukseen, jonka palveluntarjoaja voitallenta myösomaan 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 asiakaspalvelutilanteissa.

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 paperien käsittelyn vähentämisenä.

## 5.2 Varmennuskäytäntö

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

## 5.3 DNA Mobiilivarmenne

Mobiilivarmenne on DNA:n liittymäsopimusasiakkaille toimitettava lisäpalvelu. DNA:n mobiilivarmennteet ovat päätelaitteen liittymäkorkeilla oleville käyttäjän salaisille avaimille DNA:n myöntämiä varmennteita.

Mobiilivarmennteiden myöntäminen vaatii sopimuksen DNA:n javarmennten hakijan välille.

DNA:n mobiilivarmennteiden myöntäjänä on DNA Mobile-IDCA, jonka yksilöivät tiedot löytyvät jokaisen myönnetyn varmennten myöntäjä (Issuer) -kentästä. DNA:n Mobile-IDCA varmennten on allekirjoittanut varmennepalvelun juurivarmentaja DNARootCA.

DNA:n mobiilivarmenne noudattaa varmennepolitiikkaa määriteltyä X.509v3 varmenneprofiilia. Varmennten tekniset yksityiskohdat on kuvattu DNA:n verkkosivuilla:

[www.dna.fi/mobiilivarmenne/](http://www.dna.fi/mobiilivarmenne/)



## 5.4 Varmennusorganisaatio

DNA varmentajantiedotovatsaavilla DNA verkkosivuilta:

[www.dna.fi/mobiilivarmenne/](http://www.dna.fi/mobiilivarmenne/)

### 5.4.1 Varmentaja

### 5.4.2 Rekisteröijä

Rekisteröintipalvelustavastaa DNA Oy.

Rekisteröijällä tarkoitetaan tahoa, joka toimii DNA:n toimeksiannostajana 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 toimi miiDNA.

Luettelo DNA:n rekisteröijistä on osoitteessa:

[www.dna.fi/mobiilivarmenne/](http://www.dna.fi/mobiilivarmenne/)

### 5.4.3 Liittymäkortin liikkeellelaskija

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

[www.dna.fi/mobiilivarmenne/](http://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 ajantasaisesti tiedotovatoiteessa

[www.dna.fi/mobiilivarmenne/](http://www.dna.fi/mobiilivarmenne/)



#### 5.4.5 Hakemistopalvelu

DNA ylläpitää julkista hakemistopalvelua. Julkisessa hakemistopalvelussa ovat ne DNA:n mobiilivarmennot, joiden julkaisemiseen on varmentajan 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/](http://www.dna.fi/mobiilivarmenne/)

#### 5.4.6 Varmenteenomistaja

DNA myöntää mobiilivarmennot varmenteenomistajalle.

#### 5.4.7 Varmenteeseen luottava osapuoli

Varmenteeseen luottava osapuoli on henkilö tai organisaatio, joka luottaa varmenteentietoihin, ja joka käyttää varmennetta sen omistajan henkilöllisyyden todentamiseen tai varmenteenomistajan tekemänsä 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 kumppanin löydät osoitteesta:

[www.dna.fi/mobiilivarmenne/](http://www.dna.fi/mobiilivarmenne/)

#### 5.5 Varmenteenkäyttäminen

DNA:n mobiilivarmennetta voidaan käyttää tämän varmennuskäytännön mukaisesti henkilöllisyyden sähköiseen todentamiseen, viestintänsalaamiseen, 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 jäsenvarmennepoliittisissa asetettuja vaatimuksia.

Varmennusorganisaation eri osapuoliin liittyvät vastuut ja velvollisuudet on kuvattu Varmennepoliittikanliitteessä 2.



## 6 Yleiset ehdot

### 6.1 Tietojen julkaiseminen jasaatavuus

#### 6.1.1 Varmentajantietojen julkaiseminen

DNA (varmentaja) julkaisee sulkulistan 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 varmennepalveluntuottamiseen liittyvät dokumentit [www-sivuillaan](http://www.dna.fi).

[www.dna.fi/mobiilivarmenne/](http://www.dna.fi/mobiilivarmenne/)

#### 6.1.2 Tietojensaataavuus

DNA voituotepäätöksellä rajoittaa pääsyä sulkulistalle hakemistoihin.

DNA:n sulkulista ovat kaikkien niiden saatavilla, jotka tarvitsevat niitä mobiilivarmennepalveluntuottamiseen.

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

[www.dna.fi/mobiilivarmenne/](http://www.dna.fi/mobiilivarmenne/)

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

#### 6.1.3 Tietovarastot

DNA on laatinut henkilötietolain mukaisen rekisteriselosteen henkilötietojen käsittelystä varmennejärjestelmässä.

DNA arkistoi rekisteröinnissä kerätyt henkilön tunnistamistiedot voimassa olevien arkistosäännösten mukaisesti.

DNA tallentaa mobiilivarmenteet tietovarastoihin, joihin pääsy rajoitetaan.



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

SelosteDNA:njulkaisemistatiedoistaonsaatavilla DNA:nwww-sivuilla.

## 6.2 Auditointi

DNA tarkastaarekisteröijien säätömitilat, laitteet ja toiminnan tarkoituksen mukaisesti.

DNA tarkastaa tarvittaessa omatoimintansa ulkoisella auditoinnilla.

## 6.3 Tietojen luottamuksellisuus ja julkisuus

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

Muut viranomaisille luovutettavat tiedot määritellään voimassaolevan lainsäädännön mukaisesti.



## 7 Varmentajanyksilöinti

### 7.1 Varmentajannimeäminen

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

DNA:nvarmentajanimikoostuuseuraavistaattribuu teista:

Attribuutti	Sisältö
<i>commonName(CN)</i>	DNAMobile-IDCA
<i>Organization(O)</i>	DNAOy
<i>Country(C)</i>	FI

### 7.2 Avainparin uusiminen varmenteensulkemisen jälkeen

Avainparin uusiminen johtaa aina uuteen varmenteeseen uusilla avaimilla. Vanhavarmenneja avainparipysyvät mitätöityinä.

## 8 Toiminnalliset vaatimukset

### 8.1 Varmenteenhakeminen

Mobiilivarmenteen rekisteröintitapahtuman yhteydessä käyttäjä allekirjoittaa DNA:n tai DNA:n nimeämän kumppanin varmennehakemuksen ja hyväksyy varmenteen käyttöehdot. Nämä yhdessä muodostavat Mobiilivarmenteen-sopimuksen käyttäjän ja Varmentajan välille.

Käyttäjä sitoutuu huolehtimaan mobiilivarmenteen ja tunnuslukujen säilyttämisestä asianmukaisesti sekä ilmoittamaan mahdollisesta väärinkäytöstä tai varmenteiden tai liittymäkortin katoamisesta. Varmennehakemuksessa on kuvattava osapuolien oikeudet ja velvollisuudet.

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



### 8.1.1 Varmenteenrekisteröintisähköisessä kanavassa

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

Rekisteröinninyhteydessä tarvitaan käyttäjän henkilökohtaiset TUPA Stunnukset.

Rekisteröintitieteneeseuraavasti.

- 1) Käyttäjä ottaa seläinyhteyden yhteyden rekisteröintiportaaliin  
Käyttäjätunnistetaan pankkitunnisteella tavastaa tavallavahvalla tunnistuksella.
- 2) Käyttäjä hyväksyy käyttöehdot  
Järjestelmähakee käyttäjänsä sähköisen asiantunnuksen Väestörekisterikeskuksesta.
- 3) Käyttäjä syöttää matkapuhelinnumeron (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 julkaisemisihakemistossa
- 8) Rekisteröijä ilmoittaa mobiilivarmenteen hakijalle, että varmenne on rekisteröity ja käytettävissä
- 9) Mobiilivarmenne palvelun laskutus käynnistyy

### 8.1.2 Varmenteenrekisteröintipalvelupisteessä

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.

Rekisteröinninyhteydessä käyttäjä tarvitsee henkilöllisyystodistuksen.

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

Mikäli mobiilivarmenteen hakijalla ei ole soveltuva liittymäkorttia, käyttäjä saapalvelupisteessä 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 ainten luontipyyntö käyttäjän ilmoittamaan liittymän numeroon. Käyttäjäläluotarvittavat yksityiset avaimet ja PIN-numerot matkapuhelimellaan.

5) hyväksyy ainten luontipyyntö

6) antaa sellaisen PIN-numeron jokaiselle luodulle avaimelle, jamaistaasen taitallentaa PIN-numeron turvallisesti,

Käyttäjälle kirjoitetaan varmennepyyntö luomillaan avaimilla ja PIN-numerolla.

7) allekirjoittaa varmennepyyntönsä sähköisellä kirjoituksella

8) Rekisteröijä ilmoittaa mobiilivarmenteen hakijalle, että varmenne rekisteröity jakäytettävissä

9) Mobiilivarmenteen palvelun laskutus käynnistyy

Varmenteen haltija huolehtii mobiilivarmenteen ja tunnuslukujen säilyttämisestä sekä mahdollisesta väärinkäytöstä varmenteiden tallennuksen ja ylläpidon 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 tietosisältöön hakemuksen mukainen luovuttamishetkellä.



## 8.4 Varmenteenluominen

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

## 8.5 Varmenteen voimassaolon päättymisen ja sulkemisen

### 8.5.1 Varmenteen sulkemisen edellytykset

DNA asettaa mobiilivarmenteen sulkulistalle, kun on syytä epäillä väärinkäyttöä esimerkiksi silloin, kun liittymäkortin kadonnutta iänastettu.

DNA sulkee mobiilivarmenteen, mikäli sitä vastaava liittymä suljetaan. Suljettaessa liittymä tilapäisesti tehdään varmenteelle kintilapäinensulku, ellei perusteltu asyitä muuhun ole.

Varmenteen omistaja voi voidaan sulkea mobiilivarmenteen soittamalla maksuttomaan DNA:n sulkupalvelunumeroon, sähköisesti DNA:n rekisteröintipisteessä tai asioiden kautta.

Mobiilivarmenteen omistajan on tehtävä sulkupyynnön välittömästi, kun epäily väärinkäytön mahdollisuudesta on syntynyt.

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

DNA sulkee myöntämänsä varmenteet, mikäli varmenteiden tietosisällössä havaitaan virhe.

DNA voi sulkea käyttämällä avainta yksittäisellä avaimella tai avainparilla, mikäli on syytä epäillä DNA:n yksityisten avainten paljastuneen tai joutuneen väärinkäyttöön.

DNA sulkee kaikki paljastuneet salaisella avaimella tai avainparilla varmenteet, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun varmenteen voimassaoloaika on päättynyt.

Mikäli DNA:n varmenteiden luonnissa käytetty tekninen 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 mobiilivarmennekumppanit.



DNA kirjaa varmenteen sulkemista pyytäneen henkilön todentamiseen käytettyn menetelmän, varmenteensulkemisen perusteet, ajankohtajasuoritustajantiedot.

Varmenteenomistajatodennetaansamoillaperiaatteilla kuin käyttäjän tehdessä liittymän muuta hallinnointia.

Viranomaintodennetaansamoillaperiaatteilla kuin muut viranomaispyynnöt.

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

### 8.5.3 Sulkutapahtuma

Mobiilivarmenteenomistajavoitehdä mobiilivarmenteensulkupyynnön seuraavilla tavoilla:

- a) Puhelinsoitolla DNA:n sulkupalveluun,
- b) Käymällä rekisteröijän luonatai
- c) DNA:n sähköisessä asiointipalvelussa.

Varmenteen sulkeminen tehdään aina tilapäisesti ja välittömästi. Tieto varmenteen sulkemisesta on julkisesti saatavilla sen jälkeen, kun uusi sulkulistajulkaistaan.

DNA tekee sulkemista koskevan ilmoituksen kuolleen varmenteen omistajan oikeudenomistajille.

### 8.5.4 Sulkutapahtuman ajoitus

DNA toteuttaa mobiilivarmenteensulkemisen viipymättä teknisen sulkemisen heti ja sulkutapahtuma päivitetään julkiseen sulkulistaan sen julkaisun yhteydessä.

DNA:n sulkulistajulkaistaan 60 minuutin välein.

### 8.5.5 Varmenteensulkeminentilapäisesti

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

### 8.5.6 Tilapäisensulkupyynnön tekijä

Tilapäisensulkupyynnön tekijää koskevatsamatsään nöt kuin pysyvänsulkupyynnön tekijää.



### 8.5.7 Tilapäisen sulkupyynnön tekemistapa

Tilapäistä sulkupyyntöä koskevat samat säännöt kuin pysyvää sulkupyyntöä.

### 8.5.8 Tilapäisen sulun aikarajoitukset

Tilapäisen sulun voimassa kunnnesse peruutetaan. Tilapäisen sulun purkupyynnön tekijä ja  
hänen tunnistamistansakoskevat samat säännöt kuin sulkupyynnön tekijää.

### 8.5.9 Varmenteen tilapäisen sulun purkaminen

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

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

### 8.5.10 Sulkulistan julkaisu tiheys

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  
julkaisu tiheyksillä 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 käyttävätsamaa sulkulistatietoa.



## 8.6 Varmenteenuusiminen

### 8.6.1 Varmenteenuusiminen nimenmuutoksen vuoksi

Kun varmenteenomistaja ilmoittaa nimenmuutoksesta DNA:lle, uusii DNA varmenteensamalla avainmateriaalilajasamalla 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 Varmenteenuusiminen varmenteen vanhenemisen vuoksi

Kun varmenne vanhenee, on varmenteenomistajan rekisteröitävä varmenne uudelleen.

DNA voi ilmoittaa varmenteen omistajalle hyvissä ajoin ennen varmenteen vanhenemistä. 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 Varmenteenuusiminen uuden ensitunnistamisen vuoksi

DNA uusii varmenteensamalla avainmateriaalilajasamalla 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 Järjestelmänvalvonta

DNA:n varmennejärjestelmän valvonta kuvataan DNA:n varmentajan tietoturvaohjeistuksessa. Ohjeistustoimitetaan Viestintävirastolle jaseon nähtävillä DNA:n toimipisteessä.

## 8.8 Varmenteisiin liittyvien tietojen arkistointi

### 8.8.1 Tallennettavaaineisto

DNA tallentaa mobiilivarmennetapahtumistaseuraavat tiedot:

- 1) yksittäisen tunnistustapahtuman sähköisenä alkuperäisenä tallennettuna tapahtuman todentamiseksi tarvittavat tiedot, ns. teletunnistustiedot;
- 2) tarvittavat tiedot hakijan ensitunnistamisesta sekä siihen käytettyä asiakirjastasekään mahdolliset kopiot asiakirjoista;
- 3) tiedot tunnistusvälineen käyttöön mahdollisesti liittyvästä estoistajakäyttörajoituksista; sekä
- 4) varmenteen tietosisältö.

DNA säilyttää edellä 1 kohdassa tarkoitettuja tietoja viisi vuotta tunnistustapahtumasta tai kuitenkin siten, kuin viranomais määräykset kulloinkin inasiastamääräävät.

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

Tiedot tallennetaan sähköiseen arkistoon, joka ei ole osa leaktiivisestiverkossa (offline).

### 8.8.2 Arkistojensuojaus

Arkistoitava tieto säilytetään korkean turvatason tietokoneissa. Pääsyn valvonta toteutetaan tapauskohtaisesti siten, ettei asiattomilla ole pääsyä arkistoituihin tietoihin.

### 8.8.3 Arkistojen varmistusmenettelyt

Arkiston varmuuskopioita varastoidaan fyysisesti erillisessä tilassa.

### 8.8.4 Arkistotietojen hankinta- ja varmistusmenettelyt

DNA varmistaa arkistojen tavoitettavuuden ja lukuvälisyyden siinäkin tapauksessa, että varmentajan tai arkistojen toimintakeskeytyksiä tapahtuu.



### 8.9 Varmentajan avainten uusiminen

Varmentajan avainten uusiminen tapahtuu DNA:n varmentajan tietoturvaohjeistuksen mukaisesti.

### 8.10 Toiminnan jatkumisen hallintajapoikkeustapauksen 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 avainonpaljastunut tai varmentajan varmenneon suljettu

Mikäli DNA varmentajan yksityinen avainonpaljastunut tai on suljettu, on käytettävä seuraavia toimenpiteitä:

DNA tekee viipymättä seuraavat ilmoitukset:

1. Viestintävirasto; Ilmoitus varmentajan varmenneon vaarantumisesta
2. Luottamusverkoston osapuolet; Ilmoitus varmentajan varmenneon vaarantumisesta
3. Luottavatosapuolet, joilla on suorasopimus DNA:n kanssa; Ilmoitus varmentajan varmenneon vaarantumisesta
4. Mobiilivarmennekumppanit; 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 myönnetty varmenneetsulkulistalle ja aloittaa muutelpymissuunnitelman mukaiset toimenpiteet.

#### 8.10.2 Turvallisuuden vaarantuminen luonnonmullistuksen tai ihmisen aiheuttaman katastrofin seurauksena

DNA varautuu luonnonmullistukseen tai muuhun katastrofiin hajautussuunnitelmalla, jotta järjestelmän haavoittuvuus yhden pisteenvikaantumisen sijaan on mahdollisimain 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 kuuttakuukautta ennen lakkauttamisen ajankohtaa.

Ennen DNA varmentajan lakkauttamista suoritetaan vähintäänkin seuraavat toimenpiteet:



- Kaikki DNA-varmentajan myöntämät jätkevoinmassa olevat varmenteet suljetaan DNA-varmentajan sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeistensuljetun varmenteen voimassaoloaika on päättynyt.
- DNA-varmentajan lakkauttaessa kaikkisopimus kumppanien osavaltuudet suoritetaan varmenteiden myöntämisen prosessiin liittyviä tehtäviä varmentajan puolesta.
- DNA-varmentajan varmistaa, että kohdassa 8.8 mainittu saatavuus varmentajan arkistoihinsäilyy varmentajan lakkauttamisen jälkeenkin.
- DNA-varmentajan huolehtii sähköisen allekirjoituslaajennuksen mukaisesti tietojen arkistoinnista sekä noudattaa muutoinkin arkistolainsäätännöksi tietojen arkistoinninosalta.



## **9 Fyysiset, toiminnalliset ja henkilöstöturvallisuuteen liittyvät vaatimukset**

### **9.1 Fyysinen turvallisuus**

DNA varmentaja huolehtii varmennetuotannon turvallisuudesta ja toiminnasta asianmukaisella tavallaseenkaikilla osa-alueilla.

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

#### **9.1.1 Sijaintijarakennusten ominaisuudet**

DNA varmentajan järjestelmät sijaitsevat korkean tuotantotason konesaliloissa ja täyttävät tietokonekeskuksille annettua turvallisuutta koskevia ohjeetjämääräykset.

Toimitilaturvallisuus toteutettuna siten, että satunnaisien pääsytoimitiloihin on estetty.

#### **9.1.2 Fyysinen pääsytoimitilaan**

Toimitiloihin, joissa tehdään DNA varmennejärjestelmän tuotannollisia tehtäviä, on valvottu pääsy. Kulunvalvontajärjestelmä havaitsee sekä luvattoman sisääntulon että luvattoman sisäänmenon. Konesaliloihin vaaditaan henkilön tunnistautuminen, jolloin henkilö tunnistetaan ja pääsy oikeudettarkistetaan sekä tapahtumarekisteröidään.

Konesaliloihin varustetaan 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 saantijaholtoon on varmistettu.



## 10 Toiminnalliset vaatimukset

### 10.1 Vastuunjako

DNA varmentajan tehtävään jaettujen tehtävien mukaisesti vastuualueisiin.

Vastuualueen kuvattuihin yksityiskohtaisesti DNA:n varmenneorganisaatiokuvauksessa.

### 10.2 Tehtäviin vaadittavien henkilöiden lukumäärä

DNA varmentajan yksityisen avaimen luominen, aktiivinen, varmuuskopiointi ja palauttaminen suoritetaan valvotusti kahden järjestelmän ylläpito tehtäviin oikeutetun henkilön läsnäollessa.

Varmentajan yksityisen avaimen peruuttaminen on mahdollistava kahden oikeutetun henkilön valvonnassa.

Varmentajan yksityisen avaimen turvamoduulin alustuksessa on läsnä vähintään kaksi järjestelmän ylläpito tehtäviin oikeutettua henkilöä.

Järjestelmän käyttämiseen vaadittavien oikeutetun henkilön läsnäolo.

### 10.3 Tehtäväkohtainen tunnistaminen

Mobiilivarmenteen rekisteröijän, varmennejärjestelmän ylläpitäjän ja varmennejärjestelmän käyttäjän tunnistaminen ja tehtävänkuvauksen seuraavasti:

- Varmenteen rekisteröijä, sähköinen rekisteröinti; XML-lälekirjoitussovelluksen avaimilla.
- Varmenteen rekisteröijä, henkilökohtainen rekisteröinti; DNA:n kauppiaastunnuksella varmennepyynnön mobiilivarmentodennus
- Varmennejärjestelmän ylläpitäjä; varmennejärjestelmän käyttämä oma sisäinen vahva tunnistusmenetelmä
- Varmennejärjestelmän muutkäyttösovellukset; sulku pyynnöt; sovelluksen XML-lälekirjoitus
- Varmennejärjestelmän muutkäyttäjät; varmennejärjestelmän käyttämä oma sisäinen vahva tunnistusmenetelmä

## 11 Henkilöturvallisuus

DNA on kiinnittänyt erityistä huomiota sekaoman henkilökuntansa etäteknisten toimittajien rekisteröijien luotettavuuteen ja tehtäviensä suorittamiseen tarvittaviin taitoihin.



DNA on laatinut DNA-tietoturvaohjeistuksen erivarmenneorganisaation jäsenille.

DNA:n henkilökohtaisen rekisteröintipalvelun henkilöstöä sertifioidaan toimintaa ennen kuin henkilövoimavaroja rekisteröintiin.

### **11.1 Henkilökuntaa koskeva taustaselvityksen tekeminen**

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

### **11.2 Taustaselvityksen tekemisessä noudatettavat vaatimukset**

DNA teettää varmennepalvelun avainhenkilöstöstä turvallisuus selvityksen henkilön antamien tietojen perusteella määrämällä muotoisella 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 tehtävään 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 koulutusei oletettavasti täytä heidän työnsä 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 käyttö

#### 12.1.1 Avainparin luominen

##### Varmentaja:

DNA varmentaja luo yksityiset allekirjoitusavaimensa ja yksityisiä allekirjoitusavaimiaan vastaavat julkiset avaimet. Varmentajanyksityistä avaintasäilytetään turvamoduulissa.

##### Varmenteenomistaja:

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

##### 1. Avaimet voidaan luoda pyydettyäessä (OBKG).

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

##### 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 rapituspinalla, tai erilliseen PIN-kuoreen. Avainten generointitoimiin samoin kuin OBKG-sovelluksessa.

Avainten generointiohjelmiston toteutuksesta avainten liittymäkorttitoimittaja.

Liittymäkortilla on ainavähintään 1024-bittinen RSA-avain.

#### 12.1.2 Liittymäkortin luovuttaminen hakijalle

Liittymäkortin luovutusprosessi (OBKG) on kuvattu ohdassa 8.2.1.

Liittymäkortin luovutusprosessi (Pregen) on esillä tähän varmennuskäytäntöön.

#### 12.1.3 Varmenteen hakijan julkisen avaimen toimittaminen varmentajalle



DNA:n rekisteröintipalvelutoimittavat 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 rekisteröijätiedot.

DNA:lla on valmiudettehtaalla luotujen avainten (P-regen) toimitukseen.

Pregen kortin tapauksessa DNA toimittaa julkiset avaimet ja niitä vastaavat liittymäkortintiedot DNA varmentajalle. Julkisten avainteneheysuojata anvarmennukseenasti. 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 julkisen 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 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, josta vastikaksi varmennetta.

DNA voisi sisällyttää tunnistusavaimen käyttötarkoituksiinsa salauksen.

### 12.2 Varmentajan yksityisten avaintensuojaaminen

#### 12.2.1 Turvamoduuliakoskevat standardit

DNA varmentajan yksityisiä avaimia säilytetään DNA varmentajan hallinnoimissa turvamoduuleissa.



DNA varmentaja huolehtii siitä, että varmentajan yksityiset avaimet on suojattu paljastumiselta jaluvattomaltakäytöltä.

DNA varmentajan yksityisistä avaimista otetaan varmuuskopio kriittisen tietoturvallisuuden edellyttämällä tavalla.

#### **12.2.2 Varmentajan yksityisen avaimen käsittelyyn osallistuvahenkilökunta**

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

#### **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 käyttäjien yksityisiä avaimia ei arkistoida.

#### **12.2.5 Yksityisen avaimen hallinnointiturvamoduulissa**

DNA varmentajan yksityiset allekirjoitusavaimet suojataan korkean luotettavuuden fyysisillä ja loogisilla turvatoimilla. Niitä käytetään vain turvallisessa ympäristössä sijaitsevassa järjestelmässä.

### **12.3 Varmenteen omistajan avaintensuojaaminen**

#### **12.3.1 Liittymäkorttiakoskevat standardit**

DNA:n liittymäkorttien valmistettu GSM-A-SAS-sertifioidussa tehtaassa.

#### **12.3.2 Yksityisen avaimen luovutusluotetun osapuolen huostaan**

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

#### **12.3.3 Yksityisen avaimen varmuuskopio**

Mobiilivarmenteeseen liittyvistä yksityisistä avaimista ei ole kopioita.



### 12.3.4Yksityisen avaimen arkistointi

Mobiilivarmenteeseen liittyvä yksityistäväntä ei arkistoida.

### 12.3.5Yksityisen avaimen hallinnointiliittymäkortilla

Yksityistäväntä ei hallinnoida erityisesti. Yksityisen avaimen vainjaainoastaan liittymäkortilla.

### 12.4Muutavainparin hallintaan liittyvät seikat

#### 12.4.1Julkisen avaimen arkistointi

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

#### 12.4.2Julkisten yksityisten avainten voimassaoloaika

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

Varmenteensulkutapahtuma on käsitelty enemmän kohdassa 8.5.

### 12.5Liittymäkortilla olevien yksityisten avainten tunnusluvut

#### 12.5.1Tunnusluvun luominen ja käyttöön otto

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

#### 12.5.2Tunnusluvun suojaus

Liittymäkortin tunnusluvut on suojattu korttivalmistajan kortin käyttöjärjestelmätasolla niin, ettei niitä voi lukea taikopioidakortilta.

### 12.6Varmennejärjestelmän laitteiden käyttöön ja ääsyyn liittyvät turvallisuusvaatimukset

#### 12.6.1Laitteistoturvallisuus

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 jähvyksytyt ratkaisut siirretään tuotantoympäristöön.

### 12.7.2 Turvallisuuden hallinta

Varmentajantietoturvallisuutta hallitaan varmentajantietoturvaluokituksen 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 korkeansaatuuden menetelmillä.

### 12.7.4 Turvamoduulinkäytön valvonta

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

## 13 Varmenne-jasulkulistaprofiilit

### 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 voitarjota erilaisia sulkulistaprofiileita. Sulkulistaprofiiliton kuvattu DNA:n verkkosivulla:

[www.dan.fi/mobiilivarmenne/sulkulista](http://www.dan.fi/mobiilivarmenne/sulkulista)

## 14 Varmennuskäytännön hallinnointi

### 14.1 Muutosmenettely

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

Määritysten muutokset on kirjattava varmennuskäytännön seuraavassa kuvattavalla.

#### 14.1.1 Kohdat, joita voimuttaa ilmantiedonanto käyttäjille ja palveluntarjoajille

Tähän dokumenttiin voidaan tehdä oikeinkirjoitukseen ja ulkoasuun liittyviä korjauksia sekä muutoksia yhteystietoihin ilman ilmoitusta käyttäjille tai palveluntarjoajille. Dokumentista voidaan julkaista käännöksiä erikielillä ilman erillistä ilmoitusta. Käännöksen jäsuo menkielisen 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 muutosvaati tiedonannonkäyttäjille ja palveluntarjoajille

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

#### 14.1.3 Muutokset, joiden johdosta täytyy laatia uusivarmennepolitiikka

Varmennuskäytännön uudistuminen ei edellytä uuden politiikan laatimista.

#### 14.1.4 Julkaiseminen ja tiedottaminen

DNA julkaisee varmennuskäytännön, jaseonsaatavilla varmentajien Internet-sivuilta.



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

Versio	Päiväys	Kuvaus
1.0	1.11.2010	Versio 1

### 15 Viiteluettelo

- [RFC3647] S.Chokhani,W.Ford.,R.Sabett,C.Merrill,S.Wu.“InternetX.509PublicKeyInfrastructureCertificatePolicyandCertificationPracticesFramework”. IETF RFC3647,November2003.URL <http://tools.ietf.org/html/rfc3647>.
- [RFC5280] D.Cooper,S.Santesson,S.Farrell,S.Boeyen,R.Housley,W.Polk.“InternetX.509PublicKeyInfrastructureCertificateandCertificateRevocationList(CRL)Profile”.IETF RFC5280,May2008. 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."

---

