Danske Bank

Danske Bank –konserni
Varmennepolitiikka
1.6.2011

Sisällysluettelo

Asiakirjan historiatiedot

Versio	Päiväys	Huomautukset
1.0	19-05-2011	Versio 1.0
1.1	16-06-2011	Käännetty englannista suomeksi ja muokattu vastaamaan Suomessa yleisesti käytössä olevaa käsitteistöä.

Johdanto

Tämä asiakirja on suomenkielinen versio ja käännös Danske Bank-konsernin englanninkielisestä varmennepolitiikasta (jäljempänä myös "CP"). Tämä versio on käytössä ainoastaan Suomessa tarjottavien varmennepalvelujen yhteydessä. Mikäli englannin ja suomenkielisen version välillä on eroja, noudatetaan mahdollisessa tulkintatilanteessa mitä englanninkielisessä varmennepolitiikassa on asiasta mainittu.

Tämä asiakirja määrittelee säännöt, joilla Danske Bank-konsernin varmentaja (jäljempänä myös "CA") jakaa ja hoitaa yhteisten turvavaatimusten mukaisesti avaimia ja varmenteita sisäisille ja ulkoisille käyttäjilleen.

Danske Bank-konserni on pohjoiseurooppalainen finanssipalvelujen tuottaja Tanskassa, Suomessa, Norjassa, Ruotsissa, Irlannissa, Isossa-Britanniassa ja Luxemburgissa. Danske Bank-konserni varmentajaorganisaationa on juurivarmentaja, jolla on kussakin yllä olevista maista erillinen maakohtainen ali-juurivarmentaja, joka tukee tilaajille tuotettuja pankkipalveluja. Juurivarmentaja allekirjoittaa alivarmentajan varmenteen ja alivarmentaja myöntää varmenteita määrittelemilleen loppukäyttäjille.

Danske Bank-konserni tuottaa palveluja, jotka tukevat varmennepalvelujen tilaajien käyttämiä toimintoja. Tässä asiakirjassa mainituista palveluista käytetään nimitystä varmennepalvelut.

Danske Bank-konserni tuottaa erilaisia finanssipalveluja niiden tilaajille tässä varmennepolitiikassa määritellyillä varmenteilla. Näistä palveluista käytetään tässä asiakirjassa nimitystä finanssipalvelut.

Tämä varmennepolitiikka koskee finanssipalveluja. Se täyttää EPC:n varmennepolitiikan vaatimukset ja siihen on lisätty ETSI TS – ESI runkorakenteen tiettyjä osia kuitenkin huomioiden seuraavat poikkeukset:

- Pääsääntöisesti varmennepolitiikassa viitataan seikkaperäisempään varmennekäytäntöasiakirjaan (CPS). Sellaista ei ole vielä luotu, joten viittauksiakaan ei ole tässä lueteltu;
- varmenteiden peruuttamistoimintoa ei mainita, koska tätä ei pidetä välttämättömänä finanssipalveluiden luonteen vuoksi;
- luottavia osapuolia (relying parties) ei asiakirjassa mainita, koska ainoastaan varmentaja ja tilaajat ovat osallisia varmenteita vaativassa maksuliikenteessä, ja
- ISO 27006:ssa määritellyt tarkastukset eivät koske varmentajaa.

Varmennepolitiikan hallinnointi

2.1 Yleiskatsaus

Tämä asiakirja kuvaa varmennepolitiikan, jota noudatetaan kaikkien finanssipalvelujen tilaajien kohdalla. Varmennepolitiikalle tehdään aika ajoin versiomuutoksia. Varmennepolitiikka on luettavissa osoitteesta Danske Bank/Yritysasiakkaat/Ehdot

2.2 Asiakirjan nimi ja tunnistaminen

Tämä asiakirja on nimeltään “Danske Bank –konserni varmennepolitiikka”. Kaikki varmentajan myöntämät varmenteet ovat tämän varmennepolitiikan mukaisia.

2.3 Yhteystiedot

Varmennepolitiikkaa käsittävien asioiden yhteyshenkilö on:

Poul Otto Schousboe
Ejby Industrivej 41
2600 Glostrup
Puhelin +45 45 14 19 52
Matkapuhelin +45 25 26 73 50
pos@danskebank.dk

2.4 Kattavuus

Varmennepolitiikan mukaisia varmenteita saa käyttää vain finanssipalvelujen tilaajat. Varmenteita annetaan kiistämättömyyden, luottamuksellisuuden ja todentamisen todistamiseksi.

Varmenteita saa käyttää ainoastaan finanssipalveluja varten. Varmenteita ei saa käyttää laittomia tarkoitusperiä varten.

Lähdeviitteet

ETSI TS 102 042 v 1.2.1. (2005-05):"Electronic signatures and infrastructures; Policy requirements for certification authorities issuing public key certificates".(Sähköiset allekirjoitukset ja infrastruktuurit; Menettelytapavaatimukset julkisia avainvarmenteita myöntäville varmennevastaaville)

ETSI SR 002 176 V1.1.1 (2003-03): "Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures. (Sähköiset allekirjoitukset ja infrastruktuurit (ESI); Algoritmeja ja parametreja turvallisia sähköisiä allekirjoituksia varten)

EPC291-09 V 1.0 (2009-11):Requirements and Specifications for EPC Approved Server Cas for e-Mandate Services". EPC:n (Sähköinen tuotekoodi) hyväksymiä vaatimuksia ja määrittelyjä juurivarmenteeesta sähköisissä toimeksiannoissa

ISO/IEC 27002 (2005): "Information technology – Security techniques – Code of practice for information security management". (Tietotekniikka - Turvatekniikat – Tietoturvan käsittelysäännöt"

ISO/IEC 15408: "Information technology – Security techniques – Evaluation criteria for IT security". (Tietotekniikka – Turvatekniikat – tietoturvan arviointikriteerit)".

FIPS PUB 140-2 (2001): Federal Information Processing Standard Publication -"Security Requirements for Cryptographic Modules". (Yleinen tietojen käsittelystandardin julkaisu – Salaustekniikoille asetetut vaatimukset).

CWA 14167 -2 (2004): CEN Workshop Agreement -- "Security requirements for trustworthy systems managing certificates for electronic signatures". (CEN workshop-sopimus – Sähköisiä allekirjoituksia hallinnoivien luotettavien järjestelmien turvallisuusvaatimukset).

Määrittelyt ja lyhenteet

4.1 Määrittelyt

Varmennepolitiikka (engl. Certificate Policy, CP) on varmentajan laatima kuvaus menettelytavoista ja toimintaperiaatteista, joita varmenteita myönnettäessä noudatetaan.

Varmennekäytäntö (engl. Certificate Practice Statement, CPS) on varmennepolitiikkaa yksityiskohtaisempi kuvaus menettelytavoista, joita varmenneorganisaatio käyttää myöntäessään ja hallinnoidessaan varmenteita.

Varmentaja (eng. Certification Authority, CA) on varmenneorganisaation osapuoli, joka luo, myöntää, allekirjoittaa ja hallinnoi varmenteita

Rekisteröijä (engl. Registration Authority, RA) on varmenteen hakijan tunnistamisesta ja varmennehakemukseen rekisteröitävien tietojen tarkistamisesta vastaava osapuoli. Rekisteröijä toimii varmentajan valtuuttamana varmenneorganisaation osana. Rekisteröijä ei allekirjoita eikä myönnä varmenteita.

Sähköinen varmenne (engl. Digital certificate) **Tilaajan julkinen avain, yhdistettynä tunnistetiedot sekä muita erilaisia tietoja juurivarmentajan yksityiseen varmenteeseen**

Sähköinen allekirjoitus (engl. Digital signature) on **s**ähköisessä muodossa oleva tieto, joka on liitetty tai on loogisesti yhteenkuuluva muuhun sähköiseen tietoon ja joka toimii oikeuksien varmentajana ja kyseisen tiedon eheyden menetelmänä.

Tilaaja (engl. Subscriber) on oikeushenkilö, joka on allekirjoittanut varmentajan kanssa sopimuksen, jolla pyydetään myöntämään varmenteet palvelujen tai tuotteiden käyttämiseksi.

Luottamuksellisuus (engl. Confidentiality) on **t**ietoturvaperiaate, joka varmistaa, että käyttöoikeus tietoon on ainoastaan käyttöoikeuteen valtuutetuilla tahoilla.

Kiistämättömyys (engl. Non Repudiation) on periaate, jonka mukaan yksi maksutapahtuman osapuoli ei voi kieltää vastaanottaneensa maksutapahtumaa eikä myöskään toinen osapuoli voi kieltää lähettäneensä maksutapahtumaa. Sähköisen allekirjoituksen sopimuksellinen sitovuus lain edessä.

Eheys (engl. Integrity) tarkoittaa tietoturvassa, että tieto pysyy muuttumattomana koko prosessin aikana.

Todentaminen (engl. Authentication) on järjestelmän käyttäjän (henkilön, organisaation tai laitteen) tai viestinnässä toisen osapuolen tunnistuksen varmistaminen.

4.2 Lyhenteet

Tässä dokumentissa käytetään alla mainittuja lyhenteitä, jotka tarkoittavat seuraavaa:

Lyhenne	englanniksi, suomeksi
CP	Certificate Policy, Varmennepolitiikka
EPC	European Payments Council, Euroopan maksuneuvosto
ETSI	European Telecommunications Standards Institute, Eurooppalainen telekommunikaation standardointielin
ESI	Electronic Signatures and Infrastructures, Sähköiset allekirjoitukset ja infrastruktuurit
TS	Technical Specification, Tekninen määrittely
OID	Object Identifier, Kohteen tunnistin
PKI	Public Key Infrastructure, Julkisen avaimen järjestelmä
RA	Registration Authority, Rekisteröijä
RFC	Request for Comment, Kommenttipyyntö
CA	Certificate Authority, Varmentaja
HSM	Hardware Security Module, Laiteturvamoduuli
EDI	Electronic data interchange, Sähköisten tietojen vaihto
CPS	Certificate practice statement, Varmennekäytäntö
CRL	Certificate revocation list, Varmenteiden sulkulista

4.3 Huomioitavaa

Tämän varmennepolitiikan vaatimukset sisältävät:

Pakolliset vaatimukset, jotka pitää täyttää. Tällaisten vaatimusten kohdalla käytetään sanaa ”pitää”.

Vaatimukset, jotka pitäisi täyttää. Jos näitä vaatimuksia ei täytetä, asiasta on annettava perustelu. Tällaisten vaatimusten kohdalla käytetään sanaa ”pitäisi”.

5. Käsitteet

5.1 Varmentaja (CA)

Danske Bank-konserni on varmenneorganisaatio, joka myöntää sähköisiä varmenteita ja toimii luotettuna kolmantena osapuolena sellaisille käyttäjille ja osapuolille, jotka luottavat varmennepalveluun. Varmentajalla on kokonaisvastuu palveluiden säännöistä, jotka ovat välttämättömiä varmenteiden julkistamista ja ylläpitoa varten.

5.2 Rekisteröijä (RA)

Rekisteröijä (RA) on yksikkö, joka on vastuussa varmennettavien tunnistamisesta ja oikeaksi todentamisesta, mutta joka ei allekirjoita eikä myönnä varmenteita.

Danske Bank-konsernin julkisen avaimen infrastruktuurissa (PKI), Danske Bank-konsernin rekisteröijät toimivat varmentajan valvonnassa ja valtuuttamin sekä hyväksyvät Danske Bank-konsernin tilaajien varmennehakemukset.

Danske Bank-konsernin rekisteröijien pitää tunnistaa Danske Bank-konsernin varmennettavat henkilöllisyys ja todentaa hakemuksiin sisältyvät tiedot. Jos tieto on todettu oikeaksi, rekisteröijä lähettää varmentajalle pyynnön myöntää kohteelle Danske Bank-konsernin varmenne.

5.3 Varmennepalvelut

Tämän varmenteita koskevan menettelytavan mukaisesti annetaan seuraavat palvelut:

Rekisteröinti: Rekisteröijä todentaa kohteen identiteetin sekä sen mahdolliset erityispiirteet.

Varmenteen luominen: Tilaajat luovat avainparit omilla tietokoneillaan olevalla ohjelmistolla tai HSM:llä. Varmentaja allekirjoittaa tilaajan luoman julkisen avaimen.

Välityspalvelu: Tilaajan julkinen avain, jonka varmentaja on allekirjoittanut, välitetään tilaajille varmennepalvelun kautta.

Varmenteen peruutus: Varmenteiden peruuttamista koskevien pyyntöjen vastaanotto ja käsittely.

Varmenteiden tila: Finanssipalveluihin liitettyjen varmenteiden tila todennetaan varmentajan palveluissa.

5.4 Tilaaja ja käyttäjä

Tilaajat ovat osapuolia, jotka solmivat Asiakassopimuksen Danske Bank-konsernin kanssa varmenteiden myöntämiseksi varmentajan toimesta.

Käyttäjillä tarkoitetaan tahoja, jotka toimivat tilaajan lukuun ja puolesta. Tällaisia käyttäjiä ovat luonnolliset henkilöt tai oikeushenkilöt. Myös muut organisaatiot, laitteet ja järjestelmät, jotka toimivat tilaajan lukuun ovat tässä yhteydessä käyttäjiä.

5.5 Luotettavat osapuolet (relying parties)

Sähköisiä palveluja varmenteiden loppukäyttäjille tarjoava taho. Luotettava osapuoli toimii luottaen varmenteeseen ja/ tai todentaa sähköisen allekirjoituksen varmenteen avulla. Kyseessä olevan palvelun kahden välisestä luonteesta johtuen finanssipalvelujen kautta toisiinsa kytketyt tilaajat luottavat varmentajan myöntämiin varmenteisiin. Muita luottavia osapuolia ei tähän liity.

6. Velvoitteet, vastuut ja yhdenmukaisuus

6.1 Velvoitteet

6.1.1 Varmentajan velvollisuudet

Varmentajan pitää tähän varmennepolitiikkaan kuuluvien toimintojen suhteen

- varmistaa, että kaikki tämän asiakirjan osiossa 7 luetellut vaatimukset täytetään,
- varmistaa, että yhteistyörekisteröijä täyttää omat velvollisuutensa,
- varmistaa, että myönnetyt varmenteet ovat kaikkien finanssipalveluja käyttävien osapuolten käytettävissä,
- hyväksyä ja vahvistaa peruutuspyynnöt sellaisilta yksiköiltä, jotka pyytävät varmenteen peruuttamista ja laittaa varmentajan juurivarmenne voimaan.
- varmistaa, että yksityistä avainta käytetään varmenteiden myöntämiseen tarkoitetulla tavalla ja varmenteen peruuttamisen tilatiedon toimittamiseen ja
- noudattaa kohdassa 6.3 lueteltuja tarkastusvaatimuksia varmistamaan, että käytetyt menetelmät noudattavat tätä varmennepolitiikkaa

6.1.2 Tilaajan velvollisuudet

Tilaajien pitää solmia varmentajan kanssa sopimus, jossa määritellään tilaajalle seuraavat velvollisuudet:

- antaa varmentajalle tilaajan oikeita ja täydellisiä tietoja koskien heidän varmenteitaan, tunnistamisiaan ja todentamisiaan sekä välittömästi ilmoittaa varmentajalle näissä tiedoissa esiintyvistä muutoksista tai myönnetyissä varmenteissa esiintyvistä virheistä.
- luoda, säilyttää ja käyttää allekirjoitus- ja salausvarmenteet varmentajan määräysten mukaisesti.
- välittömästi ilmoittaa, jos tilaajalla on syytä uskoa, että salausavain on vaarannettu tai hävinnyt, tai jos tilaaja ei enää tarvitse varmennetta.
- suojata varmennetta ja yksityisavainta salasanalla ja varmistaa, että mahdolliset yksityisavainten varmuuskopiot säilytetään turvallisesti.
- välittömästi ilmoittaa varmentajalle, jos yksityisavaimia luodaan ja säilytetään HSM -salauslaitteen ulkopuolella.
- käytetään varmenteita ainoastaan sovittuja tarkoitusperiä varten varmennepolitiikkaa noudattaen.

6.2 Vastuu

Tämän varmennepolitiikan julkaisemisella ja ylläpidolla Danske Bank-konserni pyrkii yhdenmukaistamaan ja virallistamaan finanssipalveluiden alueella olevaa yhteistyötä ja turvasääntöjen käyttöä.

Siksi osapuolten vastuut määritellään kunkin yksittäisen finanssipalvelun käyttöä koskevissa Danske Bank-konsernin ja asiakkaan välisissä sopimuksissa.

6.3 Yhdenmukaisuusvaatimus

Varmentajan varmenteiden pitää olla yhdenmukaisia varmentajan voimassa olevan varmennepolitiikan sääntöjen kanssa, mikäli varmentajalla on varmennepolitiikassa myönnettyihin varmenteisiin liittyvä yhdenmukaisuuden arvionti. Arviointi voi olla varmentajan toiminnoista riippumaton, kansainvälisen tarkastusyrityksen tekemä, tarkastus ja arviointiraportin pitäisi olla tilaajien käytettävissä.

Jos varmenteet eivät täytä yhdenmukaisuusvaatimusta, varmentajan pitäisi lopettaa varmenteiden myöntäminen toistaiseksi ja pyrkiä yhdenmukaistamaan toimintansa kohtuullisessa ajassa.

Varmentajan määräysten noudattaminen pitää tarkistaa säännöllisesti ja aina, kun varmennepolitiikkaan tehdään suuria muutoksia.

Yhdenmukaisesti toimivan varmentajan pitää tarvittaessa näyttää toteen, että se täyttää tässä politiikassa mainitut velvoitteensa. Varmentajan tulee järjestää asiaa koskevien vaatimusten mukaiset riittävät kontrollikeinot. Alueet, joissa näitä kontrolleja tarvitaan, on yksilöity tämän asiakirjan 7 -luvussa.

7. Varmentajan varmennekäytännön vaatimukset

7.1 PKI – avainten hallinnan elinkaari

7.1.1 Varmentajan avaimen luominen

CA-avain pitää luoda valvotuissa olosuhteissa seuraavien vaatimusten mukaisesti:

- Varmentajan juuriavain ja salausavain pitää luoda turvallisissa olosuhteissa vähintään kahden varmentajan valtuuttaman luotettavan työntekijän toimesta
- varmentajan avaimen luonti pitää suorittaa salausmoduulissa, joka täyttää yhden seuraavista vaatimuksista:
- FIPS PUB 140-2, vähintään tasoa 3,
- CEN Workshop-sopimus – vähintään tasoa CWA 14167-2,
- Luotettava, vähintään EAL 4-tason täyttävä ISO/IEC 15408 mukainen järjestelmä
- varmentajan juurivarmenne pitää luoda toimialan tunnistamalla algoritmilla (RSA), jonka avainpituus on vähintään 2048 bittiä. Varmentajan salausavain pitää luoda käyttäen vähintään 1024 bittiä.

7.1.2 Varmentajan avaimen säilytys, varmuuskopio ja palauttaminen

Varmentajan pitää varmistaa, että varmentajan juuriavain ja salausavain säilytetään alla olevien vaatimusten mukaan.

- varmentajan juuriavain ja varmuuskopio pitää säilyttää ja käyttää turvallisissa salausmoduuleissa, jotka täyttävät yhden seuraavista vaatimuksista:
- FIPS PUB 140-2, vähintään tasoa 3,
- CEN Workshop-sopimus – vähintään tasoa CWA 14167-2,
- Luotettava, vähintään EAL 4-tason täyttävä, ISO/IEC 15408 mukainen järjestelmä
- vähintään kahden varmentajan valtuuttaman luotettavan työntekijän pitää säilyttää ja palauttaa varmentajan juuriavaimet, salausavaimet ja niiden varmuuskopiot turvalliseen ympäristöön.
- vanhentunut tai peruutettu varmentajan allekirjoitusavain pitää tuhota tai arkistoida.

7.1.3 Varmentajan julkisen avaimen jakelu

Varmentajan julkinen avain toimitetaan tilaajille allekirjoitetussa zip-tiedostossa (käyttäen sitä varten luotua VeriSign varmennetta), joka voidaan myös ladata pankin kotisivuilta. Vaihtoehtoisesti tämä zip -tiedostoa voidaan lähettää sähköpostilla suoraan tilaajille.

7.1.4 Varmentajan avaimen käyttö

Varmentaja sitoutuu ylläpitämään valvontajärjestelmiä, jotka varmistavat, että varmentajan avaimia käytetään ainoastaan:

- varmenteiden allekirjoittamiseen
- varmenteen tilan päivittämiseen.

7.2 PKI – varmenteen hallinnoinnin elinkaari

7.2.1 Rekisteröinti

Varmentajan pitää varmistaa, että tilaajien ja varmenteiden käyttäjien tunnistamiseen liittyvät rekisteritiedot ja muu tunnistamiseen liittyvä tieto tutkitaan ja todennetaan asianmukaisin valtuuksin toimivien tahojen toimesta.

Varmentaja vaatii, että tilaajat luovuttavat varmenteen hakemuslomakkeen ja että rekisteröijän pitää todentaa tilaajan identiteetti seuraavaa prosessia noudattaen:

- yksityishenkilö -tilaaja ilmoittaa nimensä ja henkilötunnuksensa. Oikeushenkilö -tilaajat ilmoittavat yrityksen tai muun yhteisön nimen ja kansallisen yritysrekisterissä olevan numeronsa.
- rekisteröijä varmentaa tilaajan identiteetin kansallisen rekisterin tai kansallisen yritysrekisterin kautta.
- jos tilaaja on jo asiakas voi todentamisprosessi poiketa yllä olevasta prosessista.

Ennen kuin varmentaja solmii sopimuksen tilaajan kanssa varmentajan pitää ilmoittaa tilaajalle osiossa 7.2.4 säädetyt varmenteen käytöstä annetut säännöt.

Mikäli käyttäjä, joka toimii tilaajan puolesta, on yksityishenkilö, pitää tälle henkilölle ilmoittaa hänen vastuunsa ja velvoitteensa.

Tilaajan pitää ilmoittaa osoite ja yhteystiedot, joista käy ilmi, miten tilaajaan voi saada yhteyttä.

Varmentajan pitää dokumentoida tilaajien kanssa solmittu allekirjoitettu sopimus, jonka pitäisi sisältää:

- varmentajan oikeus saada rekisteröinnissä käytettäviä tietoja,
- tilaajan sopimus käsittäen hänen velvoitteensa,
- varmentajan oikeus prosessoida tilaajan henkilöllisyys-/yritystiedot sillä aikaa kun ne todennetaan.

Varmentajan pitää säilyttää tilaajan hakemustiedot laissa säädetyn ajan. Niitä tulee voida käyttää näyttönä mahdollisessa varmennepalveluun liittyvässä oikeusprosessissa.

7.2.2 Varmenteen uusiminen, uudelleen syöttäminen ja päivittäminen

Varmentaja ylläpitää valvontajärjestelmiä voidakseen taata, että vain oikeat ja asianmukaisin valtuuksin tehdyt varmenteiden uusimiset prosessoidaan:

- Varmenteiden vanhenemispäivän tilan todennustoiminto
- Varmenteiden uusimisen toiminto. Varmenteen uusintapyyntö käsitellään ainoastaan, jos tilaajalla on jo voimassa oleva varmenne.

Kun tilaajavarmenne on peruutettu tai vanhentunut, tarvitsee tilaajan käydä läpi rekisteröintiprosessi saadakseen uuden varmenteen.

7.2.3 Varmenteen luominen

Varmentajan varmenteet luodaan sitä varten tehdyillä tietojärjestelmillä laiteturvamoduulin (HSM) sisällä.

Varmentajan julkaisemien varmenteiden pohjalta tilaajat luovat kaksi varmennetta, toisen allekirjoittamista ja toinen salausta varten. Tilaajat luovat nämä varmenteet omissa järjestelmissään ETSI SR002 176 ja FIPS 140-2 tasoja noudattaen.

Varmentaja suosittelee, että tilaajat luovat ja säilyttävät avaimet käyttäen HSM:ää tietokoneohjelman sijaan.

Tilaajien pitää luoda avainpari varmentajan hyväksymällä algoritmilla ja avaimen pituudella. Anomukset hyväksyttyä pituutta lyhyempiä avaimen pituuksia varten hylätään.

Varmenteen luonnissa tulisi varmenteisiin sisällyttää seuraavat ominaisuudet:

- myöntävän varmentajan tunnistamistiedot sekä maa, jossa varmentaja on perustettu,
- tieto varmenteen hallussapitäjästä,
- hallussapitäjän tunnistetiedot,
- varmenteen myöntö- ja vanhentumispäivät,
- varmenteen uniikki tunnusnumero (sarjanumero),
- viittaus tähän varmennepolitiikkaan (CP),
- hallussapitäjän julkinen avain sekä
- varmentajan sähköinen allekirjoitus.

7.2.4 Sääntöjen julkaiseminen

Varmentajan pitää varmistaa, että varmenteen käyttöä koskevat säännöt ovat tilaajien saatavilla ilmoittamalla seuraavat seikat:

- käytössä oleva varmennepolitiikka,
- varmenteen käyttörajoitukset,
- tilaajan velvollisuudet,
- varmentajan vastuurajoitukset,
- säännöt tilaajan rekisteröintitietojen säilyttämiseksi ja
- käytettävä laki.

Sääntöjen pitää olla saatavilla pysyvällä kommunikaatiovälineellä. Ne voidaan välittää sähköisesti tai henkilökohtaisesti ja kaikkien osapuolten tulee ymmärtää ne.

Varmentajan pitää ilmoittaa tilaajalle, että yksityisavainta ei saa käyttää allekirjoittamiseen silloin kun kyseessä on peruuttamispyyntö, peruuttamisilmoitus tai seuraava erääntymispäivä.

Varmentajan pitää ilmoittaa tilaajalle, että myönnettyä varmennetta ei saa käyttää muiden varmenteiden allekirjoittamiseen.

7.2.5 Varmenteen peruuttaminen tai lakkauttaminen

Varmentaja ei tue lakkauttamispalveluja.

Varmentajan pitää peruuttaa varmenne jos:

- tilaaja pyytää peruuttamista, koska se ei enää tarvitse ko. palvelua,
- tilaaja on unohtanut yksityisavaimen salasanan,
- tilaajan ominaisuudet muuttuvat,
- tilaaja pyytää peruuttamista, koska yksityisavain on vaarantunut tai tilaaja voi epäillä sen vaarantuneen,
- tilaajan käyttäjä on kuollut, tai
- tilaaja rikkoo velvollisuuksiaan tai tässä varmennepolitiikassa säädettyjä sääntöjä.

Peruutusta pyytävä tilaaja pitää tunnistaa. Tunnistettu hakemus voi olla tilaajan lähettämä, digitaalisesti allekirjoittama viesti, jossa on voimassa oleva allekirjoitusavain. Vaihtoehtoisen menetelmän mahdollisessa käytössä tilaajan on todistettava henkilöllisyytensä.

Varmentajan pitää peruuttaa tilaajan varmenne 24 tunnissa peruutuspyynnön saatuaan.

7.3 Varmentajan hallinnointi ja toiminta

7.3.1 Turvallisuuden hallinnointi

CA ylläpitää tietoturvallisuutta ja tarkistuksia alan tunnistettujen standardien, ISO/IEC 27002:n mukaisesti.

Varmentajan tietohallinnolla pitää olla turvallisuuspolitiikka, joka ohjaa tietoturvallisuutta.

Jos varmentaja ulkoistaa kaikki tietojärjestelmänsä kokonaisuudessaan tai osan niistä alihankkijalle, huomioidaan varmentajan turvallisuusvaatimukset asianmukaisessa sopimuksessa ja varmentajalla on lopullinen vastuu niiden noudattamisesta.

Varmentajan pitää toimittaa riskikartoitukset liiketoiminnallisten riskien arvioimiseksi ja päättää tarvittavat vaatimukset ja operatiiviset toiminnot.

Varmentajan toimitiloja, järjestelmiä ja tietojen saantia koskevat turvatarkistukset ja toimintamenetelmät edellyttävät, että varmennepalvelut pitää olla ajan tasalla ja dokumentoitu. Muutokset varmentajan järjestelmiin on vahvistettava ja niiden pitää läpäistä muutoshallintaprosessi.

7.3.2 Toiminnan hallinnointi

Varmentaja ylläpitää valvontajärjestelmiä, joilla asianmukaisesti varmistetaan, että varmentajan tietojärjestelmät on turvattu ja että järjestelmähäiriöt on minimoitu.

Varmentajan tietojärjestelmiin liittyvät turvallisuusriskit tai toimintahäiriöt on minimoitava vahingonhallinnointiprosessia käyttäen.

Varmentajan pitää toteuttaa prosessit, joilla voidaan arvioida varmennetoiminnan tietojärjestelmien kapasiteettia. Varmentaja ylläpitää valvontajärjestelmiä , joilla asianmukaisesti varmistetaan, että viestintävälineitä säilytetään turvallisesti ja ne on suojeltu vahingoilta, varkauksilta ja luvattomalta käytöltä.

Varmentajan pitää toteuttaa kaikki luotettavuus- ja hallinnointimenetelmät, jotka vaikuttavat varmennepalvelujen ehtoihin.

7.3.3 Järjestelmään pääsy

Varmentajan pitää rajoittaa pääsy varmentajan järjestelmiin asianmukaisesti hyväksyttyihin järjestelmäkäyttäjiin.

Varmentajan sisäinen verkko pitäisi erottaa ja suojata määritellyllä ja ylläpidetyllä palomuurilla.

Varmentajalla on varmentamiseen liittyviä sovelluksia, tietokantoja ja käyttöjärjestelmiä, joihin liittyen varmentajan on ylläpidettävä käyttäjähallintajärjestelmiä. Varmentajan on ylläpidettävä valvontajärjestelmiä, joilla taataan, että vain niillä henkilöillä on pääsy varmennejärjestelmiin, jotka sitä työtehtäviensä hoitoon liittyen tarvitsevat.

Varmentajan järjestelmät pitäisi varustaa tapahtumaluettelolla, josta järjestelmiin kirjaaminen voidaan jäljittää ja vastuullistaa.

7.3.4 Liiketoiminnan jatkuvuus

Varmentajan pitää ylläpitää liiketoiminnan jatkuvuussuunnitelmia voidakseen taata toiminnan jatkuvuuden.

Liiketoiminnan jatkuvuussuunnitelmat pitää testata säännöllisesti niiden ajantasaisuuden ja tehokkuuden varmistamiseksi.

Jos vahinko tai suuronnettomuus tapahtuisi, varmentajan järjestelmien varmuuskopiot pitää säilyttää turvallisessa paikassa ja niiden pitäisi pystyä varmistamaan nopea toiminnan palautuminen.

7.3.5 Laillisten vaatimusten täyttäminen

Varmentaja valvoo toimintaansa turvatakseen toimintansa laillisuuden. Varmentajan pitää varmistaa, että tilaajien henkilö- ja muita tietoja käytetään ainoastaan varmenne toimintaa varten.

Tilaajan tietoja saa paljastaa vain tilaajan kirjallisella suostumuksella tai lain määräysten niin edellyttäessä.