Tietoturvakuvaus

eKirje

1 Sovellettavat lait ja asetukset

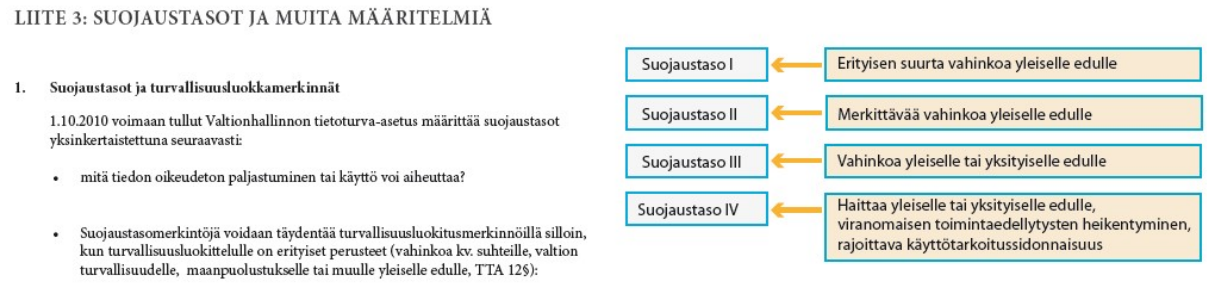
Palvelussa käsitellään salassa pidettäviä terveydenhuollon potilastietoja sekä sosiaalihuollon asiakastietoja. Potilas- ja asiakastietojen käsittelemisestä, käsittelemiseen liittyvistä vastuista ja velvollisuuksista sekä salassapidosta ja vaitiolovelvollisuudesta säädetään useissa eri laeissa ja asetuksissa.

Toimittaja vastaa siitä, että sopimuksen kohde täyttää Euroopan unionin ja Suomen lainsäädännön asiakas- ja potilastietojen käsittelylle asettamat vaatimukset, mukaan lukien vuoden 2018 toukokuusta eteenpäin sovellettavan Euroopan unionin yleisen tietosuoja-asetuksen (2016/679) asettamat vaatimukset.

Toimittaja vastaa siitä, että sopimuksen kohde on kulloinkin voimassa olevan lainsäädännön vaatimusten mukainen, ottaen erityisesti huomioon tietojärjestelmien oletusarvoisen ja sisäänrakennetun tietosuojan. Toimittaja huolehtii käsittelemiensä tietojen asianmukaisesta suojaamisesta varmistaakseen tilaajan aineiston luottamuksellisuuden, eheyden ja saatavuuden.

2 Tietoturvatasot

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (”tietoturvallisuusasetus”) määrittelee tietoturvan neljä suojaustasoa (”tietoturvatasot”). Asetus velvoittaa sitovasti valtionhallinnon organisaatioita, mutta myös muu julkishallinto voi soveltaa sitä. Sote-uudistuksen ja maakuntahallinnon myötä myös Apotti saattaa tulevaisuudessa olla valtion budjettirahoituksessa, jolloin asetus saattaa velvoittaa myös Apottia ja sen oheisjärjestelmiä. Näin ollen tietoturvatasoja sovelletaan myös tässä palvelussa.



LIITE 3: SUOJAUSTASOT JA MUITA MÄÄRITELMIÄ

1. **Suojaustasot ja turvallisuusluokkamerkinnät**

1.10.2010 voimaan tullut Valtionhallinnon tietoturva-asetus määrittää suojaustasot yksinkertaistettuna seuraavasti:

- mitä tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa?

- Suojaustasomerkintöjä voidaan täydentää turvallisuusluokitusmerkinnöillä silloin, kun turvallisuusluokittelulle on erityiset perusteet (vahinkoa kv. suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle, TTA 12§):

Palvelun vaikutusarvioinnissa on päädytty siihen, että käsiteltävien tietojen edellyttämä tietoturvataso on suojaustaso III. Tätä suojaustasoa vastaa sekä valtionhallinnon VAHTI-ohjeistuksessa että KATAKRI-auditointikriteeristössä korotettu taso. Palvelun tulee täyttää tätä vastaavat tietoturvavaatimukset.

Korotetun tason tietoturvavaatimukset on koottu tämän asiakirjan lukuun 3 ”Tietoturvatasovaatimukset”,. Vaatimukset perustuvat VAHTI-ohjeeseen 3/2011 Valtion ICT-hankintojen tietoturvaohje ja niiden tarkemman tulkinnan apuna käytetään tarpeen mukaan muita soveltuvia VAHTI-ohjeita. Tällaisia ohjeita ovat ainakin:

- Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012
- Sovelluskehityksen tietoturvaohje, VAHTI 1/2013
- ICT-varautumisen vaatimukset, Vahti 2/2012

Korotetun tason tietoturvavaatimusten ohella palvelun tulee täyttää palvelukohtaiset eritellyt tietoturvavaatimukset. Nämä vaatimukset on esitetty tämän asiakirjan luvusta 4 alkaen.

3 Tietoturvatasovaatimukset

ID	Vaatimus
1. Tietoturvallisuuden hallinnan vaatimukset	
1.1 Johtajuudelle asetettavat vaatimukset	
S1	Mikäli hankinnan kohdetta koskeva lainsäädäntö muuttuu, tilaaja tiedottaa siitä toimittajalle, joka sitoutuu tiedottamaan muutoksesta hankinnan kohteen tuottamisesta vastaavalle henkilöstölleen sekä alihankkijoilleen hankinnan kohteen tuottamisen edellyttämässä laajuudessa.
S2	Toimittaja määrittelee hankinnan kohteeseen liittyvät toimittajan ydintoimintojen ja -prosessien vastuut ja tehtävät hankinnan edellyttämällä tavalla.
S3	Toimittaja laatii kirjallisen hankinnan kohteeseen liittyvän tietoturvakäytännön sisältäen vähintään palveluun liittyvät tietoturvariskit ja niihin varautumisen, palveluun soveltuvat lait ja viranomaismääräykset ja niiden vaikutukset tietoturvavaatimuksiin sekä tietoturvaan liittyvät toiminnalliset vaatimukset.
S4	Toimittaja vastuuttaa hankinnan kohteeseen liittyvän tietoturvatyön henkilöstölleen ja/tai alihankkijoilleen.
S5	Toimittaja nimeää tietoturvavastaavan, joka vastaa sopimuksen mukaisen palvelun tietoturvallisuudesta sopimuskauden aikana.
S6	Toimittaja vastaa siitä, että sillä on hankinnan kokoon ja tavoitteisiin nähden riittävästi hankinnan kohteeseen liittyvää tietoturvahenkilöstöä.
S7	Toimittajan tietoturvavastaava osallistuu säännöllisesti (vähintään kerran vuodessa tai tarvittaessa esim. merkittävien tietoturvapoikkeamien jälkeen) hankinnan kohteen tietoturva-asioita käsittelevään yhteistyöryhmään Tilaajan edustajien kanssa.
S8	Toimittaja määrittelee tehtävät ja vastuut sekä nimeää henkilöt hankinnan kohteeseen liittyvistä Tilaajaan vaikuttavista tietoturva-asioista raportointiin sekä tietoturvapoikkeamista tiedottamiseen. Toimittaja ulottaa tämän myös palvelun toimittamiseen liittyviin alihankkijoihin.
S9	Toimittaja raportoi Tilaajalle tietoturvallisuudesta puolivuosittain tai muulla erikseen sovittavalla aikavälillä.
S10	Toimittaja käyttää tietoturvaraportointiin Tilaajan antamaa tai muuta yhdessä sovittua mallipohjaa.

ID	Vaatimus
S11	Toimittaja määrittelee tehtävät ja vastuut sekä nimeää henkilöt hankinnan kohteeseen liittyvien tietoturvapoikkeamien käsittelyyn ja organisointiin.
S12	Toimittaja reagoi hankinnan kohteeseen liittyviin vakaviin tietoturvapoikkeamiin viivytyksettä, pitää niistä kirjaa ja raportoi ne Tilaajalle. Toimittaja raportoi Tilaajalle tietosuojapoikkeamista 72 tunnin kuluessa havaitsevisesta.
S13	Toimittaja laatii kirjallisen menettelyohjeen hankinnan kohteeseen liittyvien tietoturvapoikkeamien käsittelyyn ja hyväksyttää sen Tilaajalla. Toimittaja vastuuttaa tietoturvapoikkeamien selvittämisen, tarvittavan viranomaisyhteydenpidon ja tiedottamisen.
S14	Toimittaja tekee hankinnan kohdetta koskevista tapahtuneista tietoturvapoikkeamista jälkikäteisanalyysin ja Tilaajan hyväksyttyä toimenpiteet käynnistää tarvittavat korjaavat toimenpiteet tietoturvapoikkeaman uusiutumisen ehkäisemiseksi. Toimittajan tulee ilmoittaa näistä poikkeamista ja toimenpiteistä Tilaajalle viiveettä.
S15	Toimittajan tietoturvallisuuden vastuuhenkilö lähettää tietoturvaraportin Tilaajan tietoturvallisuuden vastuuhenkilöille aina ongelmatilanteiden ilmetessä, kuitenkin vähintään puolivuosittain.
S16	Toimittaja kuvaa tietoturvallisuuden raportointiin sovellettavan menettelyn kirjallisesti.
1.2 Toiminnan suunnittelulle asetettavat vaatimukset	
S17	Toimittaja tunnistaa hankinnan kohteeseen liittyvien tietojen käsittelyyn liittyvät toimintaympäristöt (esimerkiksi toimitilat, kehitys-, testi- ja tuotantoympäristöt), niihin kuuluvat järjestelmät ja toiminnot.
S18	Toimittaja tunnistaa kunkin hankinnan kohteeseen liittyvän toimintaympäristön erityisvaatimukset ja tavoitteet tietoturvallisuuden osalta.
S19	Toimittaja dokumentoi hankinnan kohteeseen liittyvät toimintaympäristöt ja niihin kuuluvat järjestelmät.
S20	Toimittaja katselmoi ja tarvittaessa päivittää vuosittain hankinnan kohteeseen liittyvät ympäristö- ja järjestelmäkuvaukset (asset management, omaisuuden hallinta).
S21	Toimittaja sitoutuu noudattamaan Tilaajan kullekin hankinnan kohteeseen liittyvän ydintoiminnon ja –prosessin tietoturvallisuuden kannalta suojattavalle kohteelle laatimaa luokitusta ja sen mukaisia käsittelysääntöjä.
S22	Toimittaja huomioi sopimuksen mukaista palvelua Tilaajalle toimittaessaan palvelun tietoturvatavoitteet erityisesti luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta.
S23	Toimittajalla on kirjalliset karkean tason toiminto- tai prosessikuvaukset vastuullaan olevista hankinnan kohteen ydintoiminnoista ja -prosesseista.
S24	Toimittaja arvioi säännöllisesti (vuosittain) hankinnan kohteen tietoturvallisuuteen liittyviä riskejä.
S25	Toimittaja parantaa tietoturvallisuutta riskiarvioinnin perusteella Tilaajan kanssa yhteistyössä sovituilla toimenpiteillä.
S26	Toimittaja arvioi tarvittaessa yhteistyössä Tilaajan kanssa hankinnan kohteeseen liittyviä tietoturvariskejä vähintään kerran vuodessa.

ID	Vaatimus
S27	Toimittaja sopii yhdessä Tilaajan kanssa menetelmän ja ohjeistuksen, joita käytetään hankinnan kohteeseen liittyvien tietoturvariskien arviointiin.
S28	Toimittajalla on kirjallinen hankinnan kohteen tietoturvallisuuskuvaus, josta toimitetaan aina ajantasainen versio Tilaajalle ja jossa on määritelty mitä teknisiä ja hallinnollisia toimia ja prosesseja Toimittaja käyttää tietoturvallisuuden toteuttamiseksi palvelussa ja havaittujen tietoturvariskien hallitsemiseksi.
S29	Toimittaja ylläpitää tietoa palvelua toimittavista alihankkijoista ja yhteistyökumppaneista. Toimittaja luovuttaa Tilaajalle kirjallisesti pyydettäessä tiedon siitä, mitkä sen alihankkijat käsittelevät mitäkin hankinnan kohteen tietoturvallisuuden kannalta tärkeää tietoa ja missä rooleissa.
S30	Toimittaja sopii Tilaajan kanssa hankittavan palvelun jatkuvuussuunnitteluun liittyvistä vastuista ja vastaa omalta osaltaan hankinnan kohteeseen liittyvän jatkuvuussuunnitelman tai –suunnitelmien päivittämisestä ja ajantasaisen version toimittamisesta Tilaajalle.
S31	Toimittaja on vastuuttanut ja organisoinut hankinnan kohteeseen liittyvän jatkuvuussuunnitelman päivityksen ja katselmoinnin.
S32	Mikäli Tilaaja niin edellyttää, Toimittaja testaa, harjoittelee ja arvioi hankinnan kohteeseen liittyvän jatkuvuussuunnitelman toimivuutta Tilaajan kanssa. Kustannusten jaosta sovitaan erikseen.
1.3 Henkilöstölle asetettavat vaatimukset	
S33	Toimittaja järjestää hankinnan kohteen toimittamiseen osallistuville henkilöille säännöllisesti (vuosittain tai lainsäädännön muuttuessa) tietoturvakoulutusta. Toimittaja kehittää ja ylläpitää kyseisen henkilöstön tietoturvaosaamista ja tiedottaa henkilöstölle muuttuneista tietoturvaohjeista ja -käytännöistä.
S34	Toimittaja seuraa tietoturvallisuudesta annettujen sääntöjen noudattamista ja puuttuu poikkeamiin.
S35	Toimittaja kuvaa hankinnan kohteeseen liittyvien tietoturvamääräysten ja –ohjeiden rikkomisen seuraukset ja tiedottaa niistä hankinnan kohteen tuottamiseen osallistuville henkilöille.
S36	Toimittajalla on menettely, jolla voidaan varmistaa, että hankinnan kohteen tuottamiseen osallistuvilla henkilöillä on riittävä tietoturvaosaaminen.
S37	Toimittaja organisoi ja vastuuttaa hankinnan kohteeseen liittyvien tietoturvatoimenpiteiden toteuttamisen (henkilöresurssit).
S38	Toimittaja tunnistaa ja nimeää hankinnan kohteen tietoturvallisuudelle tärkeät henkilöroolit ja nimeää niihin varahenkilö(t).
S39	Toimittajan tulee laatia ja hyväksyttää Tilaajalla luettelo hankinnan kohdetta koskevista tietoturvaprosesseista tai -toimenpiteistä sekä niiden vastuuhenkilöistä.
S40	Toimittaja kouluttaa hankinnan kohteen tietoturvallisuuden varmistamiseen myös varahenkilöt.
S41	Toimittajalla on olemassa menettely, jolla se huolehtii hankinnan kohteeseen liittyvien sähköisten viestien, sähköpostien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä myös tietoturvapoikkeamatilanteita

ID	Vaatimus
	selvitettäessä (sähköisen viestinnän tietosuojalaki 4 § ja 5 § sekä laki yksityisyyden suojasta työelämässä 6 luku).
S42	Toimittaja huolehtii siitä, että hankinnan kohteen tuottamiseen osallistuva henkilöstö tietää kenelle hankinnan kohteeseen kohdistuvista tietoturvapoikkeamista ja -tapauksista tai niiden uhkista tulee ilmoittaa.
S43	Toimittaja kouluttaa hankinnan kohteen tietoturvapoikkeamia selvittävät henkilöt tehtäviinsä.
1.4 Kumppanuuksille ja resurssien hallinnalle asetettavat vaatimukset	
S44	Mikäli Toimittaja käyttää alihankkijoita, se sitoutuu vastaamaan alihankkijoidensa suorituksista kuten omistaan. Toimittaja tekee alihankkijoidensa kanssa sopimukset, joissa määritellään myös yhteistyön tai hankinnan kohteen tietoturvavaatimukset alihankinnan osalta sekä se, miten hankinnan kohdetta koskeva tietoturvallisuuden valvonta, seuranta, auditointi ja raportointi tapahtuu.
S45	Toimittaja on ulottanut hankinnan kohdetta koskevat tietoturvallisuusvaatimukset alihankkijaansa hankinnan kohteen tietoturvallisuustason mukaisina.
S46	Toimittaja valvoo hankittavan palvelun tietoturvallisuuden toteutumista, kirjaa poikkeamat ja raportoi ne Tilaajalle välittömästi sekä aloittaa korjaustoimet sovitusti. Toimittaja velvoittaa myös alihankkijansa myötävaikuttamaan tämän vaatimuksen toteutumiseen.
S47	Tietoturvapoikkeaman käsittelyssä Toimittaja käyttää yhdessä Tilaajan kanssa laatimiaan ohjeita. Poikkeamasta ja sen syystä tehdään kirjallinen raportti.
S48	Toimittaja osallistuu Tilaajan pyytäessä Tilaajan jatkuvuusharjoituksiin. Tilaaja maksaa tästä aiheutuneet kulut (enintään 1000€/henkilö/päivä) ja ilmoittaa harjoituksesta vähintään 30 päivää ennen harjoitusta. Tilaaja vastaa jatkuvuusharjoituksen sisällöstä ja toteutustavasta. Tilaaja määrittää ne henkilöroolit, joiden oletetaan osallistuvan Toimittajan puolelta harjoitukseen.
1.5 Toiminnan prosesseille asetettavat vaatimukset	
S49	Toimittaja antaa luottamuksellisen ja salassa pidettävän aineiston vain niiden henkilöiden saataville, jotka tarvitsevat tietoa palvelun tuottamisessa Tilaajalle ja huolehtii siitä, että kyseiset henkilöt tietävät, miten aineistoa koskevasta tietoturvasta huolehditaan. Mikäli Tilaaja niin haluaa, näistä henkilöistä tulee voida tehdä turvallisuusselvitykset.
S50	Toimittaja merkitsee hankinnan kohdetta koskeviin asiakirjoihinsa asiakirjan laatijan nimen ja laatimisajan.
S51	Toimittaja tuhoaa hävitettäväksi tarkoitetut asiakirjat niin, että niiden luottamuksellisuus ja tietosuoja on varmistettu.
S52	Toimittaja tekee itse tuottamiinsa asiakirjoihin merkinnän luottamuksellisuudesta, mikäli asiakirja sisältää luottamuksellista tai salasssa pidettävää tietoa.
1.6 Toiminnan arvioinnille ja todentamiselle asetettavat vaatimukset	
S53	Mikäli Tilaaja sitä pyytää, Toimittaja arvioi ja auditoi hankinnan kohteena olevaan palveluun liittyvää tietoturvallisuutta suhteessa siltä edellytettyyn tietoturvallisuustasoon. Toimittaja raportoi tulokset Tilaajalle kunkin vuoden loppuun mennessä. Kulujen kattamisesta ja arvioinnin laajuudesta sovitaan etukäteen.

ID	Vaatimus
S54	Toimittaja pitää kirjaa palvelua koskevien auditointien tai arviointien lopputuloksena tulevista suosituksista ja seuraa parannustoimenpiteiden toteutumista.
S55	Tilaajalla on oikeus teettää palveluun valitsemansa kolmannen osapuolen toimijan toteuttama tietoturvaauditointi kerran vuodessa. Tilaaja maksaa kolmannelle osapuolelle suoritettavat auditointikustannukset. Toimittaja osallistuu auditointiin omalla kustannuksellaan ja toimittaa auditoinnissa tarvittavan dokumentaation ja muut siinä tarvittavat tiedot kohtuullisessa ajassa veloituksetta.
S56	Tietoturva-auditoinnissa havaitut puutteet korjataan viiveettä. Toimittajan on korjattava kriittiset puutteet mahdollisimman pian, muiden osalta aikataulu sovitaan Tilaajan kanssa erikseen.
2. Tietojärjestelmien hallinnan vaatimukset	
2.1 Raportointi tietoturvavastaavalle	
S57	Toimittaja raportoi palveluun liittyvien tietojärjestelmien ja niiden hallinnan tietoturvallisuuden tilasta Tilaajalle säännöllisesti, vähintään kerran vuodessa ja aina kun tietoturvallisuudessa esiintyy poikkeamia.
S58	Toimittaja raportoi palveluun liittyvistä vakavista tietoturvatapahtumista Tilaajalle välittömästi.
S59	Toimittajan tekemä tietoturvaraportti on kirjallinen.
2.2 Omaisuuden hallinta	
S60	Toimittaja luetteloi hankinnan kohteena olevan palvelun toteuttamiseen käytettävät fyysiset ja virtuaaliset laitteet, tietojärjestelmät, palvelut, ohjelmistot, virtuaalipalvelimet ja lisenssit.
S61	Hankinnan kohteena olevan palvelun toteuttamiseen käytettävien Toimittajan laitteiden, rekistereiden ja tietojärjestelmien omistajuus on organisoitu ja vastuutettu.
S62	Toimittaja organisoi ja vastuuttaa hankinnan kohteena olevan palvelun tuottamiseen käytettävien laitteiden, tietojärjestelmien, palvelujen ja ohjelmistojen luetteloinnin ja kuvausten päivityksen.
S63	Toimittaja dokumentoi hankinnan kohteena olevan palvelun tuottamiseen käytettävien laitteiden, tietojärjestelmien ja rekistereiden tietosisällön.
S64	Toimittaja luokittelee Palvelun tuottamiseen käytettävät laitteet hankinnan kohteena olevan palvelun edellyttämän tietoturvallisuustason mukaisesti.
S65	Toimittaja katselmoi laite-, rekisteri-, palvelu- ja ohjelmistoluetteloiden sisällön vuosittain.
2.3 Tietojenkäsittely-ympäristöjen käyttöönotto ja poisto	
S66	Toimittaja huomioi hankinnan kohteena olevan tietojärjestelmän käyttöönottoasennuksessa ja käytöstä poistamisessa järjestelmän tietosisällön tietoturvavaatimukset ja vastuuttaa ja organisoi näihin liittyvät toimenpiteet.
S67	Toimittaja laatii hankinnan kohteena olevan tietojärjestelmän (ja työasemien) esiasennuksesta ja käytöstä poistosta kirjallisen ohjeiston, jossa kerrotaan mm. eri turvatasoilla käytettävät tietoturva-asetukset (koventamisohjeet) sekä laitteiden käsittelyn

ID	Vaatimus
	ja massamuistien tyhjennyksen menettelyt silloin kun ne siirtyvät ympäristöstä toiseen tai poistuvat organisaation hallinnasta.
S68	Toimittaja vastuuttaa yllä olevassa vaatimuksessa tarkoitettujen ohjeiden päivityksen.
2.4 Tietojenkäsittely-ympäristöjen päivitys ja muutoshallinta	
S69	Toimittaja vastuuttaa ja organisoi hankinnan kohteen tuottamisessa käytettävien laitteiden ja tietojärjestelmien päivitys- ja muutostarpeen seurannan, päivityspäätösten teon ja päivitysten asennuksen erityisesti tietoturvapäivitysten osalta.
S70	Toimittaja ja Tilaaja sopivat yhdessä, mitkä päivitykset voidaan ajaa välittömästi ilman erillistä sopimista ja mitkä edellyttävät riskitason mukaista tarveharkintaa.
S71	Toimittaja tekee muut kuin kiireelliset päivitykset ja muutokset vain etukäteen palvelutasosopimuksessa sovittuna aikana (ns. huoltoikkuna).
S72	Toimittaja ei saa asentaa tai liittää hankinnan kohteena olevaan tai sen apuna käytettävään tietojärjestelmään muita kuin sen tuottamisessa tarvittavia ohjelmia ja laitteita.
S73	Toimittaja dokumentoi tietojärjestelmien ja laitteiden päivitys- ja muutosperiaatteet.
2.5 Tietoturva-alueiden muodostus ja niiden välinen suodatus	
S74	Toimittaja tunnistaa ja eriyttää hankintaan liittyvän tietoverkon eri suojaustasoa vaativat osat. Eri suojaustason verkkojen välillä on palomuuri.
S75	Toimittaja vastuuttaa ja organisoi hankinnan kohteeseen liittyvien palomuurien ja muiden tietoliikennelaitteiden sääntöjen lisäämisen, muuttamisen ja poistamisen.
S76	Toimittaja dokumentoi palomuurien ja muiden suodatuslaitteiden suodatussäännöt.
S77	Toimittaja suodattaa ja rajoittaa julkisesta verkosta Tilaajan organisaatioon sisäänpäin tulevaa liikennettä "kaikki liikenne on kielletty ellei erikseen sallittu" -periaatteella. Myös Tilaajan organisaatiosta julkiseen verkkoon lähtevää liikennettä suodatetaan.
S78	Toimittaja laatii kirjallisen palomuuri- ja liikenteensuodatuspolitiikan sekä kirjallisen sääntöjen päivitysprosessin.
S79	Toimittaja katselmoi palomuurien ja muiden suodatuslaitteiden säännöstöjen ajantasaisuutta vähintään vuosittain.
S80	Toimittaja saa liittää hankinnan kohteeseen liittyviin Tilaajan tietoverkkoihin vain palvelun tuottamiseen tarkoitettuja, palvelun tietoturvatasoa vastaavia laitteita.
2.6 Pääsynvalvonta	
S81	Tilaajalla on oikeus päättää, kuinka luotettavaa identiteettiä ja vahvaa tunnistamista hankinnan kohteena olevan järjestelmän sisältämien tietojen käyttöön tarvitaan. Tästä mahdollisesti aiheutuvista kustannuksista sovitaan erikseen. Toimittaja toteuttaa hankinnan kohteena olevan tai siihen liittyvän tietojärjestelmän käyttäjien tunnistamisen tavalla, joka suojaa järjestelmän sisältämät tiedot oikeudettomalta käsittelyltä. Mahdollisen vahvan (monen tekijän) todentamisen kustannuksista sovitaan erikseen.

ID	Vaatimus
S82	Hankinnan kohteena oleva tai siihen liittyvä tietojärjestelmä kirjoittaa lokiin sekä onnistuneet että epäonnistuneet sisäänkirjautumiset niin, että yksittäisen käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti.
S83	Palvelun tuottamisessa käytettävissä tietojärjestelmissä pitää pystyä vaikuttamaan salasanan laatuvaatimuksiin (esimerkiksi pituus, eri merkkisarjojen käyttö eli kompleksisuus, vaihtoväli).
S84	Palvelun tuottamisessa käytettävissä tietojärjestelmissä on oltava käytössä asianmukaiset tekniset tunnistusmenetelmät, tunnusten lukitus- ja avausperiaatteet sekä salasanan tai muiden tunnisteiden laatuvaatimukset ja vaihtoperiaatteet.
S85	Toimittaja säilyttää hankinnan kohteeseen liittyvät pääsynvalvontalokit niin, ettei niitä päästä jälkikäteen muuttamaan.
S86	Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin hankinnan kohteena oleviin järjestelmiin tai palveluihin aiheuttaa tunnuksen lukittumisen.
2.7 Käyttäjien ja käyttövaltuuksien hallinta	
S87	Hankinnan kohteena olevan tietojärjestelmän tunnusten ja valtuuksien myöntö, muuttaminen ja poisto organisoidaan Tilaajan kanssa yhdessä sovittavalla tavalla.
S88	Hankinnan kohteena olevan tietojärjestelmän käyttövaltuudet ovat henkilö- tai roolikohtaisia.
S89	Käyttövaltuudet perustuvat kirjalliseen sopimukseen tai palvelussuhteeseen ja järjestelmien käyttö estetään teknisesti ilman tarpeetonta viivytystä, kun tämä peruste on päättynyt (esim. palveluntoimittajan työntekijän vaihdettua työpaikkaa).
S90	Yksittäisen käyttäjän käyttövaltuudet voidaan selvittää.
S91	Toimittaja tekee hankinnan kohteena olevalle järjestelmälle kirjallisen käyttövaltuuspolitiikan ja hallintaprosessin.
S92	Jokaisella käyttövaltuudella on omistaja. Tämä koskee sekä henkilö- tai roolikohtaisia että teknisten järjestelmien välisiä tunnuksia.
S93	Hankinnan kohteena olevan järjestelmän käyttövaltuudet katselmoidaan (yhteistyössä Tilaajan kanssa) vähintään kerran vuodessa ja tarpeettomat tunnukset, roolit ja valtuudet suljetaan tai poistetaan.
S94	Hankinnan kohteena olevan järjestelmän käyttäjävaltuuksien myöntämismekanismi on sellainen, että niiltä osin, kun prosessi on Toimittajan vastuulla, myöntöprosessista jää jälki, josta nähdään, millä perusteella käyttäjälle on myönnetty käyttövaltuus.
S95	Hankinnan kohteena olevan järjestelmän käytössä Toimittajan vastuulla olevien käyttöoikeuksien osalta vaaralliset työ- ja rooliyhdistelmät on dokumentoitu ja valtuuksia myönnettäessä tai muutettaessa vaarallisten yhdistelmien syntymistä seurataan ja estetään.
2.8 Haittaohjelmasuojaus	
S96	Palvelun tuottamisessa käytettävissä tietojärjestelmissä on oltava ajantasainen haittaohjelmien suodatus. Palvelussa käsiteltävien tietojen haittaohjelmen suodatuksesta sovitaan erikseen.

ID	Vaatimus
S97	Haittaohjelmakuvaukset päivittyvät automaattisesti.
S98	Hankinnan kohteena olevan tietojärjestelmän tarjoamiseen liittyvälle Toimittajan henkilöstölle on ohjeistettu, miten haittaohjelmien leviäminen tunnistetaan ja estetään sekä mitä tulee tehdä haittaohjelmaepäilytilanteessa.
S99	Hankinnan kohteeseen liittyvien järjestelmien suojaamiseen käytettävien haittaohjelmakuvausten ajantasaisuutta valvotaan.
2.9 Fyysisen ympäristön suojaus	
S100	Palvelussa tulee voida käsitellä suojaustason III -luokan aineistoa. Suojaustasot on määritelty tietoturva-asetuksessa.
S101	Toimittaja päästää hankinnan kohteeseen liittyviin laitetiloihin vain niitä henkilöitä, joiden työnkuvaan se kuuluu tai jotka Tilaaja on hyväksynyt.
S102	Toimittaja suojaa hankinnan kohteeseen liittyvät laitetilat suojaustaso III -luokan mukaisesti.
S103	Toimittaja suojaa hankinnan kohteeseen liittyvän tietoliikennelaitteiden, -yhteyksien ja -kytkentäpisteiden sijainnin suojaustaso III –luokan mukaisesti.
2.10 Varmuuskopiointi	
S104	Toimittaja organisoi ja vastuuttaa hankinnan kohteeseen liittyvän varmuuskopioiden ottamisen yhdessä Tilaajan kanssa sovitulla tavalla.
S105	Toimittaja tunnistaa yhteistyössä Tilaajan kanssa hankinnan kohteeseen liittyvän varmuuskopioinnin kannalta olennaiset suojattavat kohteet ja ottaa niistä varmuuskopioita suunnitelman mukaisesti. Toimittaja suunnittelee myös varmuuskopioiden palauttamisen.
S106	Toimittaja laatii kirjallisen varmuuskopiointipolitiikan ja -prosessin, jotka muodostetaan ottaen huomioon palvelun vaatimukset ja jossa ohjeistetaan varmuus- ja suojakopioiden käsittely siirron ja varastoinnin aikana.
S107	Toimittaja ottaa hankinnan kohteen kannalta tärkeimmistä järjestelmistä suojakopioita ja säilyttää suojakopioita eri palotilassa kuin varsinaisia varmuuskopioita.
2.11 Tietoturvapoikkeamien valvonta	
S108	Toimittaja varmistaa, että hankinnan kohteeseen liittyvät laitteet, ohjelmistot sekä tietojärjestelmät tekevät riittäviä lokeja ja kirjausketjuja toiminnastaan.
S109	Toimittaja huolehtii hankinnan kohteen lokien keräyksestä, hälytyksistä ja seurannasta palvelun vaatimusten mukaisesti, jotka sovitaan yhdessä Tilaajan kanssa.
2.12 Tietojärjestelmien toipuminen häiriöstä	
S110	Toimittaja organisoi ja vastuuttaa ICT-järjestelmien häiriöiden selvittämisen ja niistä toipumisen hankinnan kohteeseen liittyen.
S111	Toimittaja laatii tärkeimpien palveluun liittyvien järjestelmien häiriöille yleisen toipumisstrategian ja –suunnitelman.
S112	Toimittaja dokumentoi hankinnan kohteen kannalta tärkeimmät järjestelmät ja sopii Tilaajan kanssa kirjallisten toipumissuunnitelmien laatimisesta.
2.13 Tietojärjestelmäkehityksen ja sovellusylläpidon hallinta	

ID	Vaatimus
S113	Toimittaja testaa hankinnan kohteena olevan järjestelmän toimivuuden ennen tuotantokäyttöön ottamista.
S114	Toimittaja tekee ennen palvelun tuotantokäyttöön ottamista hankinnan kohteesta kirjallisen turvallisuussuunnitelman ja käyttäjän ohjeen, joissa kerrotaan, miten järjestelmä suojataan tuotantokäytössä ja millaiset ovat käyttäjiltä vaadittavat tietoturvatoimenpiteet.
S115	Ennen järjestelmän käyttöönottoa Toimittaja auditoi järjestelmän määritykset ja toteutukset tietoturvallisuuden osalta.

4 Hallinnollinen tietoturva

4.1 Henkilöstö

Toimittajan on määriteltävä henkilöstönsä tietoturvaan liittyvät velvollisuudet ja vastuut sekä varmistettava henkilöstönsä soveltuvuus tietoturvaan liittyviin tehtäviin tämän sopimuksen kattamien tehtävien ja tietojen käsittelyn osalta.

Toimittajan on vältettävä työtehtävien ja vastuiden yhdistämistä, jos yhdistämisestä syntyy tietoturvariskejä tämän sopimuksen soveltamisen osalta.

Toimittajan on toteutettava sopimuksen kohde siten, että käyttöoikeudet tilaajan aineistoon sekä siihen liittyviin loki-, hallinta- ja konfiguraatiotietoihin annetaan vain henkilöille, jotka tarvitsevat näitä oikeuksia sopimuksen mukaisten työtehtäviensä suorittamiseen. Oikeudet myönnetään pienimmän oikeuden periaatteen mukaisesti.

Toimittaja pitää kirjaa järjestelmäkohtaisesti siitä, keillä on pääsy sopimuksen kohteen toteuttavaan järjestelmään, mitkä oikeudet henkilöllä ovat ja millä perusteella oikeus on annettu. Toimittaja poistaa käyttöoikeudet välittömästi tilanteen mukaan (esimerkiksi työntekijän poistuessa toimittajan tai alihankkijan palveluksesta) ja tarkistaa aktiiviset käyttöoikeudet vähintään kerran vuodessa.

4.2 Tietoturvan hallinta

Toimittaja varmistaa sopimuksen kohteen toimittamiseen käyttämiensä tietojärjestelmien ja tietoliikennejärjestelmien tietoturvan. Toimittaja käyttää sopimuksen kohteen toimittamiseen vain sellaisia tietojärjestelmiä ja tietoliikenneratkaisuja, joiden tietoturvariskejä toimittaja pystyy valvomaan ja hallitsemaan, ja joiden tietoturva myös tilaajan on mahdollista auditoida.

4.3 Tilaajan aineisto

Toimittaja määrittelee henkilöstönsä pääsyn tilaajan aineistoon käyttäjäkohtaisesti. Toimittaja saa käsitellä tilaajan aineistoa vain sopimuksen kohteen toteuttamiseksi. Tilaajan aineiston käyttäminen toimittajan omaan liiketoimintaan on kiellettyä.

Tilaajan aineistoa käsitellessään toimittaja noudattaa voimassaolevaa Suomen ja Euroopan Unionin lainsäädäntöä. Toimittajan on muistutettava henkilöstään siitä, että tietosuojaa koskevan lainsäädännön rikkominen saattaa johtaa rikosoikeudelliseen vastuuseen.

Käsitellessään henkilötietoja ulkomailla toimittaja noudattaa Suomen lakia ja viranomaismääräyksiä. Toimittaja takaa saman tietoturvan ja tietosuojan tason riippumatta tiedon käsittelymaasta.

Sopimuksen kohteen sisältämät tiedot sekä niiden varmuuskopiot voidaan tallentaa Euroopan talousalueella. Tietoja ei saa siirtää muihin maihin.

4.4 Tietojen hävittäminen

Sopimuksen tai tietyn palvelukokonaisuuden päättyessä tai purkautuessa toimittaja palauttaa tilaajalle tilaajan luovuttaman, ajan tasalla olevan aineiston tai muutoin tilaajan palvelua koskevan aineiston sekä hävittää omilta taltioiltaan tilaajan tietoaineiston, ellei muuta ole sovittu.

Tilaaja palauttaa osaltaan toimittajan aineiston takaisin toimittajalle ja hävittää mahdolliset jäljennökset aineistosta ja sen osista ellei muuta ole sovittu. Ohjelmaa tai aineistoa ei kuitenkaan saa hävittää, mikäli laki tai viranomaisten määräykset edellyttävät sen säilyttämistä.

Tilaajan aineiston toimittamisesta tämän kappaleen mukaisesti ei toimittajalla ole oikeutta erillisveloitukseen.

4.5 Tiedon antaminen ei-julkisista asiakirjoista

Toimittaja ei saa antaa tilaajan tietoja kolmansille osapuolille, kuten muille toimittajan asiakkaille tai viranomaisille. Toimittaja ohjaa tilaajan ei-julkisia tietoja koskevat tietopyynnöt välittömästi tilaajalle.

Toimittaja ei saa yhdistää tilaajan antamia ei-julkisia tietoja muihin tietoihin muussa tarkoituksessa kuin sopimuksen kohteen toteuttamiseksi tai tilaajan erikseen antamaa toimeksiantoa suorittaakseen.

4.6 Muutoksenhallinta

Toimittaja ei saa tehdä sopimuksen kohteeseen tietoturvan tasoa heikentävää muutosta, ellei siitä ole kirjallisesti etukäteen sovittu sopijapuolten kesken.

4.7 Toimittajan vastuu sopimuksen noudattamisesta ja käyttöoikeudet tilaajan tietojärjestelmiin

Toimittajan vastuulla on varmistaa, että kaikki sopimuksen kohteen kanssa työskentelevät henkilöt tuntevat tämän sopimuksen vaatimukset ja ovat sitoutuneet sopimuksen noudattamiseen. Toimittaja valvoo toiminnan sopimuksenmukaisuutta.

Jos toimittajan tai tämän alihankkijan palveluksessa oleva henkilö tarvitsee tunnukset tilaajan tietojärjestelmiin, tulee hänen esimiehensä täyttää ja allekirjoittaa tilaajan tunnushakemuslomake sekä toimittaa se sopimuksen yhdyshenkilölle.

Tilaajan tiloissa liikkuessaan toimittajan henkilöstön on käytettävä voimassa olevaa kuvallista henkilökorttia.

4.8 Pääsy tilaajan laitetiloihin

Toimittajan palveluksessa olevat henkilöt voivat päästä tilaajan toimitiloihin sekä käyttää tilaajan laitteita ja ohjelmistoja erikseen sovittavalla tavalla, jos se on välttämätöntä sopimuksen kohteen toteuttamiseksi. Toimittajan palveluksessa olevien henkilöiden tulee tällöin noudattaa tilaajan osoittaman vastuuhenkilön antamia ja muita tiloissa yleisesti noudatettavia ohjeita sekä käyttää henkilökorttia.

5 Tietoturva-auditoinnit

Tilaajalla on oikeus tehdä itse tai teettää riippumattomalla kolmannella osapuolella toimittajan tietoturvakäytäntöjen tai toimituksen kohteen tietoturva-auditointi kerran vuodessa.

Mikäli auditointi toteutetaan tilaajan valitseman kolmannen osapuolen toimesta, tilaaja maksaa kolmannelle osapuolelle suoritettavat korvaukset. Toimittaja on kuitenkin velvollinen osallistumaan auditointiin siten, että toimittaja toimittaa auditoinnin tekevälle taholle auditoinnissa tarvittavan dokumentaation ja muut auditoinnin kannalta välttämättömät tiedot kohtuullisessa ajassa ilman erillistä veloitusta.

Mikäli auditoinnissa paljastuu merkittäviä tietoturvapuutteita, toimittaja sitoutuu korjaamaan puutteet viipymättä ilman erillistä veloitusta.

Tarkastus on suoritettava siten, että toimittajan turvallisuusjärjestelyt eivät vaarannu.

6 Toimittajan raportointivelvollisuudet

6.1 Ilmoitusvelvollisuus

Sopijapuolen on ilman aiheetonta viivytystä ilmoitettava toiselle sopijapuolelle sellaisista sopijapuolen tietoon tulleista seikoista, jotka voivat vaikuttaa sopimuksen kohteen toteuttamisen tietoturvallisuuteen. Velvollisuus koskee muun ohella tietoturvariskejä ja muutoksia turvajärjestelyissä.

Toimittajan on ilmoitettava tilaajalle tiedossaan olevat sopimuksen kohteen tai sen toteutusteknologian tai komponenttien haavoittuvuudet sekä niiden korjausmahdollisuudet ja toimenpiteet, joilla tietoturvan heikentyminen voidaan minimoida.

Toimittajan tulee viipymättä ilmoittaa tilaajalle havaitsemansa tietoturvaloukkaukset tai tietoturvaa uhkaavat tekijät, jotka koskevat sopimuksen kohdetta tai tilaajaa, sekä kyseisten uhkien tai loukkausten aiheuttamat toimenpiteet.

Uhkaavia tekijoitä ovat esimerkiksi:

1. vanhentuneet salausmenetelmät
2. vanhentuneet ohjelmistoversiot ja puuttuvat päivitykset
3. palvelunestohyökkäykset
4. toimittajan joutuminen tietomurron kohteeksi

Lisäksi toimittajan tulee ilmoittaa viipymättä sopimuksen kohteen poikkeavaan käyttöön liittyvät seuraavat tilanteet:

1. vakiintuneesta normaalitasosta äkillisesti kohonnut tai muuttunut käyttövolyymi, resurssien käyttö tai virheilmoitusten määrä
2. järjestelmän tai sovelluksen verkkoliikenteen äkillinen muuttuminen.

Toimittajan tulee ilmoittaa tilaajalle tietoturvaan liittyvässä dokumentaatiossa tapahtuneet muutokset ja toimittaa viipymättä tilaajalle ajan tasalla oleva dokumentaatio.

6.2 Määräajoin suoritettava raportointi

Toimittajan on raportoitava tilaajale tilaajan pyynnöstä sekä mahdollisen tietoturvaloukkauksen selvityksen yhteydessä seuraavat seikat:

1. Ylläpitotunnuksien luettelo (henkilöiden nimet) ja tunnusten tila.
2. Käyttäjätunnuksien lukumäärä ja tila.
3. Asennettujen tietoturvapäivityksien suhde julkaistuihin.
4. Ylläpitomenettelyjen ajantasaisuus: ylläpitomenettelyissä tapahtuneet muutokset tai se, että muutoksia ei ole tapahtunut.
5. Asennettujen ohjelmistojen ajantasaisuus ja muuttumattomuus.
6. Palautumissuunnitelman ajantasaisuus ja arvio palautuksen toteutuksen kestosta.
7. Varmenteiden ajantasaisuus.

8. Laitteiston ajantasaisuus. Toimittajan on pidettävä yllä laitteista, niiden kokoonpanosta ja ohjelmistoasennuksista ajantasaista muutoshallintadokumentaatiota, joka on oltava saatavilla ja siirrettävissä tilaajalle viivytyksettä.

7 Varautuminen yleisesti tunnettuihin tietoturvauhkiin

Toimittajan tulee tilaajan pyynnöstä antaa tilaajalle vuosittain vapaamuotoinen selvitys sopimuksen kohteeseen liittyvistä yleisistä tietoturvauhkista sekä siitä, miten tarjoaja on ratkaisussaan varautunut yleisiin tietoturvauhkiin.

8 Koventaminen

Tuotantokäyttöön siirryttäessä ratkaisusta on passivoitava testaus- ja asennuskäyttöön perustetut käyttäjätunnukset ja palvelut sekä palvelut ja ominaisuudet, joita tilaaja ei aio ottaa käyttöön. Lisäksi tuotantokäytön alkaessa ratkaisusta on passivoitava asennusta ja testausta varten käytössä olleet tietoliikenneportit sekä ohjelmistopalvelut ja -komponentit. Toimittaja vastaa, että sopimuksen kohteen toteuttamisen kannalta turhia palveluita ei asenneta (esimerkiksi ftp, smtp).

9 Haittaohjelmasuojaus

Jokaisessa sopimuksen kohteen toteuttamisessa käytettävässä tietoverkkoon liitettävissä olevassa laitteessa on oltava ajantasainen haittaohjelmasuojaus (”virustorjunta”). Toimittaja vastaa siitä, että järjestelmän haittaohjelmasuojaus on ajan tasalla ja raportoi tilaajalle haittaohjelmasuojauksen tilasta säännöllisesti.

10 Pääsyn- ja käyttövaltuuksien hallinta

10.1 Yleiset vaatimukset

Käyttövaltuuksien hallinta perustuu roolipohjaiseen käyttövaltuuksien hallintaan. Sopimuksen kohteen ylläpidon ja käytön tulee tapahtua yksilöidyillä henkilökohtaisilla käyttäjätunnuksilla, joiden käyttö voidaan tarvittaessa jäljittää. Kaikkien tunnusten on oltava dokumentoituja. Sopimuksen kohteessa ei saa olla pysyvästi koodattuja tunnuksia ja salasanoja. Tilaajan on pystyttävä vaihtamaan tarvittaessa kaikki salasanat.

Sopimuksen kohteen toteutuksessa tulee olla pääsynvalvontamekanismi, joka estää muita kuin käyttäjiä, joille on annettu käyttövaltuudet, käyttämästä järjestelmää. Jos

pääsynvalvontamekanismi on käyttäjätunnus/salasana-autentikaatio, toteutuksen on oltava sellainen, että järjestelmä ei säilytä salasanoja selväkielisinä.

Sopimuksen kohteen tavanomaisen käytön ei tule edellyttää ylläpitotunnuksia. Ylläpitotunnuksia käytetään ainoastaan asentamisessa ja ylläpidossa.

Toimittajan henkilökunta saa käyttöoikeudet tilaajan järjestelmiin tilaajan käyttövaltuuksien hallintamenettelyn mukaisesti.

Tilaajalla on oikeus rajoittaa käyttäjän käyttöoikeuksia tai sulkea käyttäjätunnus, jos tilaajalla on esimerkiksi syytä epäillä, että käyttäjätunnus on kaapattu tai sitä käytetään vahingollisella tavalla. Sopimuksen kohde on toteutettava niin, että edellä mainitut ylläpitotoimet voidaan tehdä ohjeistetusti ja tarvittaessa välittömästi joko tilaajan pääkäyttäjän toimesta tai tilaajan palvelupyynnön perusteella.

11 Tietoliikenne

11.1 Yleiset tietoliikennevaatimukset

Toimittajan on ilmoitettava tarkat tiedot ratkaisun tietoliikenneyhteyksistä, mukaan lukien tietoliikenneprotokollat, palveluportit ja yhteydenmuodostussuunnat.

Langatonta ja langallista verkkoa käyttävien palvelujen tulee riittävän käytettävyyden takaamiseksi olla teknisesti toteutettu niin, että palvelut toipuvat tilapäisistä tietoliikennekatkoista.

12 Yhteyksien suojaus

Sopimuksen kohteen toteutuksessa tietoliikenneyhteyksien tulee olla salattuja. Toimittajan konesalin sisäiset lähiverkkoyhteydet voivat kuitenkin olla salaamattomia. Käytetyt salausratkaisut pitää pystyä tarvittaessa vaihtamaan.

13 Kryptografiset vaatimukset

Sopimuksen kohteessa käytettävien salausmenetelmien on täytettävä viimeisimmän Viestintäviraston ohjeen "Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset suojaustasot" vaatimukset tasolle ST IV.

13.1 Tietoturvaprotokollat

Sopimuksen kohteeseen liittyvät tietoliikenne suojataan salauksella. Suojaamisen käytetään lähtökohtaisista uusinta vakaata protokolla- ja algoritmiversiota. Tällä hetkellä vaatimustasona ovat seuraavat:

- Sovellusliikenteen salauksessa käytetään TLS-versiota 1.2 tai uudempaa
- Toimipisteiden väliseen liikenteeseen käytetään jotain seuraavista:
    - IPsec-tunnelointia (IKEv2)
    - TLS-protokollaa.

13.2 Varmenteet

Salauksen toteuttamiseen voidaan käyttää mm. seuraavia, tilaajan kautta saatavia varmenteita:

1. Tilaajan AD-domainin varmennepalvelussa tuotetut varmenteet, joihin tilaajan hallinnassa olevat laitteet luottavat. Tilaaja vastaa näiden varmenteiden sulkulistan julkaisemisest säännönmukaisesti.
2. Kaupallisista varmenteista käytetään tällä hetkellä VRK:n, Geotrustin, Entrustin ja Verisignin varmenteita.