4 § 1 mom. Digitaalisten palveluiden suunnittelu ja ylläpito
2 luvun 4 § 1 mom.

Viranomaisen on suunniteltava ja ylläpidettävä digitaaliset palvelunsa siten, että niiden tietoturvallisuus, tietosuoja, löydettävyys ja helppokäyttöisyys on varmistettu.

Lain 4 § sisältäisi viranomaisia koskevat digitaalisten palvelujen yleiset suunnitteluvelvollisuudet. Lain 4 §:n 1 momentin mukaan viranomaisen olisi **suunniteltava ja ylläpidettävä digitaaliset palvelunsa** siten, että **niiden tietoturvallisuus, tietosuoja**, löydettävyys ja helppokäyttöisyys **on varmistettu**. Lisäksi viranomaisen olisi varmistettava digitaalisten palvelujensa yhteensopivuus yleisesti käytettyjen ohjelmistojen ja tietoliikenneyhteyksien kanssa. Pykälässä **edellytetään, että viranomainen arvioi jo digitaalisen palvelun suunnitteluvaiheessa, miten palvelun käyttöön liittyvä tietoturvallisuus aiotaan järjestää**. Säännöksessä ei kuitenkaan ehdoteta säädettäväksi palvelujen suunnittelussa huomioitavista tietoturvallisuusvaatimuksista, koska vaatimukset muuttuvat teknisen kehityksen ja toimintaympäristön muutoksen myötä. Viranomaisen on **pystyttävä osoittamaan tietoturvallisuutta koskevalla suunnitteludokumentaatiollaan ja siihen liittyvillä testausraporteilla, että tietoturvallisuus on varmistettu riittävillä tietoturvatoimenpiteillä**. Osoitusvelvollisuus rinnastuu Euroopan unionin yleiseen tietosuoja-asetukseen (EU) 2016/679, jonka 5 (2) artiklan mukaan rekisterinpitäjä on pystyttävä osoittamaan se, että henkilötietojen käsittelyä koskevia perusperiaatteita, kuten tietojen eheyden ja luottamuksellisuuden varmistamista koskevia vaatimuksia, on noudatettu rekisterinpitäjän toiminnassa. Digitaalisten palvelujen tietoturvallisuuden toteuttamisen perusvaatimuksia on määritelty muun muassa valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän laatimassa ohjeessa Sähköisen asioinnin tietoturvallisuus (valtiovarainministeriön julkaisuja 25/2017). Perustietoturvavaatimuksia ovat esimerkiksi salassa pidettävien ja muiden käsittelyrajoituksia koskevien tietojen, kuten erityisiin henkilötietoryhmiin kuuluvien tietojen siirtäminen suojattua yhteyttä käyttäen tietoverkossa sekä tarvittaessa palvelun käyttäjän tunnistaminen palveluun kirjauduttaessa.

Euroopan unionin yleinen tietosuoja-asetus (EU) 2016/679

Digitaalisten palveluiden tarjoamista ja käyttöä sekä niihin kohdistuvaa luottamusta edesautetaan varmistamalla digitaalisten palveluiden löydettävyys ja laatu, johon sisältyvät myös palvelun helppokäyttöisyys, tietoturvallisuus ja tietosuoja. Digitaaliset palvelut suunnitellaan avoimiksi, kuitenkin huomioiden tietoturvan ja tietosuojan näkökulmat. Viranomainen arvioi jo digitaalisen palvelun suunnitteluvaiheessa, miten palvelun käyttöön ja ylläpitoon liittyvä tietoturvallisuus aiotaan järjestää. Digitaalisten palveluiden ylläpito sekä tietoturvallisuuden ja-suojan varmistaminen ovat jatkuvia prosesseja, joissa huomioidaan teknisen kehityksen ja toimintaympäristön muutoksen mukanaan tuomat uudet riskit ja tarpeet vaatimusten päivittämiselle. Läpi digitaalisen palvelun elinkaaren siihen liittyvät suojaustoimenpiteet suhteutetaan riskilähtöisesti palveluun kohdistuvien uhkatekijöiden mukaan. Osana digitaalisen palvelun laadun varmistamista ovat tietoturvallisuuteen ja –suojaan liittyvät säännöllisin väliajoin suoritettavat testaukset, minkä takia palveluita suositellaan muun muassa auditoivan säännöllisin väliajoin tietoturvan ja tietosuojan osalta joko sisäisen tai ulkoisen testaajan toimesta.

Tietoturvallisuus

Tietoturvallisuuden osalta tunnistetaan ne tekijät, jotka ovat digitaalisen palvelun kannalta merkittäviä, kuten asiakastiedon luottamuksellisuus, asiakkaan välittämien tietojen eheys, palvelun saatavuus sekä suoritettujen toimien ja tehtyjen päätösten kiistämättömyys. Tärkeät tekijät ja niihin kohdistuvat uhkat tunnistetaan ja niiden osalta määritetään digitaalisen palvelun suunnitteluvaiheessa ja suunnitteludokumentaatiossa riittävät suojauskeinot. Tietoturvallisuutta toteutetaan ja ylläpidetään

riskilähtöisesti, jolloin suojausratkaisut pienentävät tunnistettuja riskejä ja täyttävät asetettuja tietoturvavaatimuksia tarkoituksenmukaisesti ja kustannustehokkaasti. Suunnittelussa tunnistetaan keskeiset käyttötilanteet ja –tapaukset sekä palvelun tietojärjestelmäympäristö ja sen muodostama hyökkäyspinta-ala arvioiden näihin kohdistuvia uhkia. Uhkien ja tietoturvallisuuden tason arviointi ja hallinta ovat osa säännöllistä digitaalisen palvelun tietoturvallisuuden ylläpitoa.

Digitaalisessa palvelussa käsiteltävä salassa pidettävä tietoaineisto tunnistetaan ja varmistetaan, että ainoastaan käyttötarkoituksen kannalta tällaista aineistoa käsitellään palvelussa. Digitaalisessa palvelussa käsiteltävälle salassa pidettävälle aineistolle määritetään niiden suojausta koskevat periaatteet, jotka huomioivat koko käsittely-ympäristön käsittelyvaiheineen ja niihin liittyvine riskeineen. Tietoa suojataan muun muassa asianmukaisesti toteutetun käyttövaltuushallinnan, tarveanalyysiin perustuvan salauksen ja ympäristön teknisen koventamisen avulla.

Digitaalisen palvelun osalta tunnistetaan ja arvioidaan myös kiistämättömyyden merkitys. Osana digitaalisen palvelun suunnittelua ja toteutusta määritetään, miten merkittävässä roolissa on palvelun käyttäjän ja viranomaisen suorittamien toimien kiistämättömyys ja miten se varmistetaan. Tällaisiin toimiin lukeutuvat muun muassa käyttäjän antamat suostumukset ja muut tahdonilmaukset sekä viranomaisen tekemät päätökset. Tiedon eheyden ja tehtyjen toimien kiistämättömyyden varmistamisessa hyödynnetään esimerkiksi sähköistä allekirjoitusta ja riittävää lokitusta, joiden avulla varmistetaan tahdonilmaistuen ja suoritettujen toimien rekisteröinti sekä kyky osoittaa ne kiistämättömästi toteen.

Digitaalisen palvelun rakenne ja kontrolliympäristö

Suunnittelussa kiinnitetään huomiota digitaalisen palvelun viitearkkitehtuuriin ja rakenteeseen. Viitearkkitehtuuri ja rakenne huomioivat digitaalisen palvelun kannalta olennaiset tietoturvallisuuden osa-alueet minimoiden riskialttiita toimintoja, rajaten pääsyä tietoon ja suojaten digitaalista palvelua keskeisiltä uhkilta. Palvelun toteutuksessa käytetään vain tietoturvalliseksi arvioituja teknisiä ratkaisuja, eikä käytetty arkkitehtuuri ohjaa käyttämään vain tiettyjä tuotteita tai teknologioita.

On hyvä soveltaa modulaarista tai palvelukeskeistä arkkitehtuurimallia, jossa jokainen moduuli toteuttaa itsenäisesti tietyt toiminnallisuudet tai tarjoaa pääsyn digitaalisen palvelun tarvitsemaan tietoon tuottaen samalla tarvittavat ja tarkoituksenmukaiset tiedon luottamuksellisuutta, eheyttä ja saatavuutta suojaavat tietoturvakontrollit. Tämä tukee kerroksittaisen tietoturvan toteuttamista sekä viitearkkitehtuurin soveltamista erityyppisiin digitaalisiin palveluihin painottaen tarpeen mukaan eri tietoturvan näkökulmia eli luottamuksellisuutta, eheyttä ja saatavuutta. Tietoturvallisuuden huomioivassa modulaarisesti toteutetussa digitaalisessa palvelussa eri moduulien välillä ei ole automaattista luottamusta, vaan ne eri moduulit toteuttavat tarvittavia suojauksia itsenäisesti esimerkiksi osapuolten tunnistamisen ja syötteen validoinnin osalta. Tällöin esimerkiksi yhdessä komponentissa ilmenevä haavoittuvuus ei suoraan vaaranna koko digitaalista palvelua, vaan tietomurtoa ennaltaehkäisevät edelleen muut kompensoivat suojaukset.

Viranomaisen on huomioitava digitaalisten palveluiden suunnittelussa ja ylläpidossa palvelun eri osa-alueiden tietoturvallisuus. Digitaalisen palvelun tietojärjestelmäympäristön muodostuu eri osa-alueista kuten sen käyttäjistä (kansalaiset, viranomaiset, yritykset ja muut järjestelmät), päätelaitteista, sovelluskerroksesta, palomuuri- ja yhdyskäytäväratkaisuista, käyttöpalveluympäristöstä, palvelurajapinnoista, integraatioratkaisuista ja sanomaliikenteestä sekä tukipalveluista.

Käyttäjät

Digitaalinen palvelu suunnitellaan mahdollisimman helppokäyttöiseksi ja selkeäksi, mikä edesauttaa palvelun käyttäjälähtöisyyden ja käytettävyyden lisäksi myös sen turvallista käyttöä. Tätä tuetaan myös tarvittavalla opastuksella ja ohjeistuksella tietoturvatietoisuuden ja palvelun käyttöön liittyvän osaamisen varmistamiseksi. Suunnittelussa huomioidaan eritasoiset ja erilaiset käyttäjät ja helppokäyttöisyyden varmistamiseksi palveluiden suunnitteluun voidaan ottaa käyttäjiä mukaan.

Kun palvelun luonne sitä edellyttää, toteutetaan tarvittavat mekanismit käyttäjien luotettavan yksilöinnin ja sähköisen tunnistamisen toteuttamiseksi. Tällainen on tarpeen esimerkiksi tilanteissa, joissa palvelussa käsitellään ei julkista tietoa, palvelussa on mahdollista laittaa vireille huomattavaa oikeudellista ja taloudellista merkitystä omaavia asioita tai palvelun anonyymiin käyttöön liittyy ilmeinen riski haitanteosta. Käyttäjien yksilöinnin ja tunnistamisen lisäksi suunnitellaan myös asianmukainen asiointivaltuuksien hallinta ja riittävä käyttäjän todennus.

Päätelaitteet

Laajemmilla oikeuksilla tapahtuva digitaalisen palvelun hallinta- ja ylläpitokäyttö sekä viranomaiskäyttö tapahtuvat suunnitelmallisesti ja määritetyn päätelaitepolitiikan mukaisesti. Käsiteltävien tietojen pohjalta määritetään riskilähtöisesti, mitä tietoja, toimintoja, palvelun vaiheita ja siihen liittyviä eri ympäristöjä, on mahdollista käsitellä rajatusti vain tietyillä politiikan mukaisesti toteutetuilla ja hallituilla päätelaitteilla ja mitä on mahdollista käsitellä muiden käyttäjien, kuten kansalaisten, toimesta heidän omilla, viranomaisen hallinnan piirin ulottumattomissa olevilla, laitteilla. Suunnittelussa huomioidaan riskilähtöisesti digitaalisen palvelun luonne, siellä käsiteltävät tiedot ja rooli, jossa toimintoja ollaan toteuttamassa.

Sovelluskerros

Digitaaliseen palveluun liittyvät sovellukset suunnitellaan, toteutetaan ja ylläpidetään niin, että keskeiset uhkat ja hyökkäystavat, sovellushaavoittuvuudet, konfiguraatiovirheet ja muut tietoturvapuutteet hallitaan ja ennaltaehkäistään sekä niitä tunnistetaan läpi palvelun elinkaaren. Tämä edellyttää tietoturvallisuuden huomioimista aina sovellusten suunnittelu- ja kehitysvaiheista alkaen läpi koko niiden elinkaaren. Kehityksen aikana huomioidaan tarvittavat tietoturvallisuuden toteuttamista ja varmistamista tukevat tehtävät, kuten arkkitehtuuri- ja koodikatselmoinnit, uhkamallinnus sekä tietoturvatestaus, joista tuotetaan tarvittavat raportit ja kuvaukset osoittamaan osaltaan tietoturvallisuuden asianmukaista huomioimista kehityksen aikana.

Digitaalinen palvelu toteutetaan käyttäjäystävälliseksi ja mahdollisimman helppokäyttöiseksi sekä niin, että se herättää sen käyttäjissä luottamusta palvelun laadun ja tietoturvallisuuden suhteen. Palvelun nimi ja URL-osoite viittaavat palvelun omistavaan viranomaiseen ja se on selvästi tunnistettavissa aidoksi, luotetuksi, palveluksi. Se myös toimii luotettavasti ja loogisesti virhetilanteissa ja käyttäjän näkökulmasta tarpeelliset tietoturvaan ja tietosuojaan liittyvät ohjeet ja selosteet ovat selkeästi saatavilla.

Salassa pidettävää tietoa sisältävien viestien luottamuksellisuus varmistetaan digitaaliseen palveluun liittyvässä tietojen siirrossa itse palvelussa ja sen ulkoisissa viestintäkanavissa ja tukipalveluissa. Suunnittelussa ja ylläpidossa huomioidaan muun muassa [VAHTI Kortti 14 § 1 mom siirto tietoverkossa] määritetyt periaatteet.

Palomuuri- ja yhdyskäytäväratkaisut

Tietoverkkojen segmentoinnilla eriytetään digitaalisen palvelun eri osia toisistaan toteuttamalla tietoverkolle turvallinen rakenne, jossa esimerkiksi palvelu on eriytetty siihen liittyvistä taustapalveluista, tukipalveluista ja muista asiointipalveluista. Tarvittaessa käytetään lisäksi yhdyskäytäväratkaisuja, jos palvelu kytkeytyy korkeamman turvallisuustason taustajärjestelmiin ja kontrolloidumpi liikenteen suodatus on tarpeen. Palomuuri- ja yhdyskäytäväratkaisujen avulla suodatetaan ja rajoitetaan ympäristöjen välistä liikennettä, taltioidaan ja valvotaan tietoliikennettä sekä havaitaan ja estetään tunkeutumisyrityksiä.

Käyttöpalveluympäristö

Digitaalisen palvelun käyttöpalveluympäristön toteuttamisessa ja ylläpidossa huomioidaan riskilähtöisesti määritetyt suojauskeinot siihen kohdistuvien uhkien hallitsemiseksi. Palveluun liittyvät palvelinkomponentit, käyttöjärjestelmät, ohjelmistot, sovellukset, tietoliikennelaitteet sekä hallintatyöasemat ja hallintayhteyksien muodostamisessa käytetyt laitteistot ja ohjelmistot kovennetaan tehtyjen suunnitelmien ja määritysten mukaisesti.

Ympäristöjen koventaminen ja tarvittavien suojausten määrittely perustuu ympäristöjen käyttötarkoitukseen, käsiteltäviin tietoihin sekä tunnistettuihin riskeihin ja sitä sovelletaan kaikkiin ympäristöihin eli myös muihin, kuin vain tuotantoympäristöön. Tähän sisältyvät testi- ja kehitysympäristöt sekä tukipalvelut, kuten työtilat, versionhallinta ja komponenttikirjastot. Lisäksi käyttöpalveluympäristön koventamisessa ja rakenteessa on huomioitu mahdollisten palvelunestohyökkäysten riski sekä niihin liittyvä sieto- ja toipumuskyky.

Palvelurajapinnat, integraatioratkaisut ja sanomaliikenne

Digitaalisen palvelun palvelurajapintoja ja avoimeen dataan liittyviä rajapintoja käyttävät tietojärjestelmät ja käyttäjät tunnistetaan riittävän luotettavasti silloin, kun rajapinnassa välitetään salassa pidettävää tietoa, tiedon alkuperästä tulee voida varmistua tai kun rajapinnan käyttöä halutaan seurata ja tarvittaessa rajoittaa käyttäjäkohtaisesti. Vastaavasti myös palvelurajapintojen käyttöä rajoitetaan asianmukaisin valtuutuksin sallien oikeudet ainoastaan rajattuihin toimintoihin, rajapintaoperaatioihin ja tietoihin. Palvelurajanpinnat toteutetaan mahdollisimman teknologiariippumattomia protokollia ja standardeja hyödyntäen niiden käytettävyyden varmistamiseksi.

Digitaalisen palvelun suunnittelussa ja ylläpidossa on varauduttu siihen, että palvelun ulkoisiin rajapintoihin kohdistuu haitallista verkkoliikennettä johtuen esimerkiksi riittämättömästä syötetarkistuksesta palvelua kutsuvassa tietojärjestelmässä. Tyypillisimpiä uhkia ja haavoittuvuuksia vastaan on varauduttu muun muassa haittaohjelmasuojauksin ja sisällön suodatuksella.

Tukipalvelut

Digitaalisissa palveluissa hyödynnetään kansallisia tukipalveluita, joiden tietoturvallisuuden taso on jo tiedossa. Jos käytetään kaupallisia tukipalveluita, on niiden tietoturvallisuuden tasosta ja vaatimustenmukaisuudesta varmistuttava tai käsiteltävä palvelussa ainoastaan julkista tietoa. Tällöinkin tiedon saatavuuden ja eheyden turvaaminen voi kuitenkin olla kriittistä ja sen asianmukainen toteuttaminen varmistetaan. Digitaalisen palvelun suunnitteluun ja toteuttamiseen osallistuvat palvelutoimittajat ja yhteistyökumppanit sitoutetaan asetettuihin tietoturvatavoitteisiin ja –vaatimuksiin palvelun laadun ja turvallisuuden varmistamiseksi.

Tietosuoja

Digitaalisten palveluiden suunnittelussa ja ylläpidossa on huomioitava voimassa oleva tietosuojaa koskeva sääntely sekä viranomaisohjeistus. Digitaaliseen palveluun liittyvä henkilötietojen käsittely on suunniteltua ja lainmukaista sekä rekisteröidyn oikeudet ja asianmukaisen henkilötietojen suojan varmistavaa. Digitaalisessa palvelussa käsiteltävät henkilötiedot ja niihin liittyvä kokonaisuus on tiedossa ja dokumentoitu.

Digitaalinen palvelu on suunniteltu ja toteutettu niin, että siinä toteutuvat henkilötietojen käsittelyä koskevat yleiset periaatteet. Henkilötietojen käsittely on toteutettu lainmukaisesti ja asianmukaisesti eli se on kohtuullista. Kaikki henkilötietojen käsittely tapahtuu rekisteröidyn kannalta läpinäkyvästi ja siihen liittyvät rekisteröidyn informointivelvoitteet täyttyvät. Henkilötietoja käsitellään sitä tiettyä, nimenomaista ja laillista tarkoitusta varten, minkä takia ne on kerätty. Henkilötiedot ovat olennaisia ja tarpeellisia niiden käsittelytarkoituksiin nähden eli käsittelyssä toteutuu henkilötietojen minimoinnin periaate ja tarpeettomia tietoja käyttäjistä ei kerätä eikä tallenneta. Henkilötietojen täsmällisyyden varmistamiseksi on toteutettu kaikki mahdolliset kohtuulliset toimenpiteet, jotta epätarkat ja virheelliset henkilötiedot saadaan poistettua tai oikaistua viipymättä. Digitaalisessa palvelussa toteutuvat henkilötietojen säilytyksen rajoittamiseen liittyvät periaatteet, joiden mukaisesti henkilötiedot tuhotaan viiveettä, kun niiden säilyttämiselle ei ole enää perustetta.
Digitaaliseen palveluun liittyvien suojakeinojen avulla varmistetaan henkilötietojen asianmukainen turvallisuus suojaten niitä muun muassa luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.

Tietosuoja on suunniteltu ja toteutettu sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden mukaisesti. Digitaalisen palvelun suunnittelussa ja määrittämisessä sekä itse henkilötietojen käsittelyn yhteydessä toteutetaan tietosuojaperiaatteiden edellyttämät asianmukaiset ja tarvittavat toimenpiteet huomioiden käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset, käytetyn tekniikan ja teknologian sekä käsittelyn aiheuttamat riskit rekisteröityjen oikeuksille ja vapauksille. Lisäksi digitaalinen palvelu on toteutettu niin, että siinä käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja ja vain tarvittavassa laajuudessa sekä tarvittavat tietosuojaa ja yksityisyyttä koskevat asetukset ovat oletusarvoisesti aktivoituina.

Osana digitaaliseen palveluun liittyvän kiistämättömyyden toteuttamista huomioidaan myös mahdolliset henkilötietojen käsittelyyn liittyvät suostumukset ja niiden hallinta.

Osana digitaalista palvelua tuodaan henkilötietojen käsittelyyn liittyvän läpinäkyvyysperiaatteen mukaisesti selkeästi esiin kaikki tarvittavat kuvaukset ja selosteet koskien henkilötietojen käsittelyä. Tähän liittyvät muun muassa tietosuojaselosteet ja evästeitä koskevat selosteet. Tällä varmistetaan osaltaan henkilötietojen käsittelyn läpinäkyvyyttä ja rekisteröidyn oikeuksien toteutumista.

Löydettävyys

Digitaaliset palvelut on suunniteltu ja toteutettu niin, että ne ovat helposti ja selkeästi löydettävissä. Löydettävyyden varmistamiseksi viranomainen huolehtii siitä, että digitaalinen palvelu tietosisältöineen on selkeästi löydettävissä sen omien verkkosivustojen kautta sekä ajantasaisena löydettävissä esimerkiksi hakukoneiden avulla. Viranomaisen omat verkkosivustot on jäsennetty niin, että kaikki asiointiin liittyvät digitaaliset palvelut ovat helposti ja selkeästi löydettävissä sekä käytettävissä. Löydettävyyden varmistamiseksi verkkotunnukset ja verkko-osoitteet muodostetaan yleisiä käytäntöjä noudattaen siten, että ne ovat helposti muistettavia ja ymmärrettäviä.

Digipalvelulaki -kortti LUONNOS	
Kortti 4 § 1 mom. Digitaalisten palveluiden suunnittelu ja ylläpito	versio 0.xx/pvm

	Digitaalisten palveluiden käyttömahdollisuudesta tiedotetaan hallinnon asiakkaille lähetettävissä kirjeissä sekä muissa relevanteissa tiedotteissa. Lisäksi postitse tapahtuvassa viestinnässä ohjeistetaan tarpeen mukaan asiakasta, miten hän voi saada vastaavan kirjeen jatkossa digitaalisia palveluita käyttämällä. Digitaalinen palvelu on hyvä myös suunnitella ja toteuttaa niin, että se on ulkoasultaan yhdenmukainen sitä tarjoavan viranomaisen muiden verkkopalveluiden kanssa. **Helppokäyttöisyys** Digitaalisen palvelun helppokäyttöisyys varmistetaan osana sen suunnittelua ja ylläpitoa. Digitaalinen palvelu on riittävän yksinkertainen ja helposti opittavissa sekä sen toiminnot noudattavat yleisesti käytössä olevia toimintoja. Digitaalinen palvelu ei siis eroa olennaisesti muista palveluista ja sen käyttäminen on asioijalle selkeää ja tehokasta. Käytetyt navigointiratkaisut ja toiminnallisuudet ovat selkeitä ja digitaalisen palvelun käyttäjälle havaittavia. Lisäksi digitaalinen palvelu selkeästi ohjaa käyttäjää ja tunnistaa sekä antaa palautetta käyttäjän tekemistä virheistä. Virheilmoitukset eivät saa kuitenkaan paljastaa tietoturvallisuuden vaarantavia, mahdollista hyökkääjää edesauttavia, asioita.
	[Työkaluja ei suunnitella vielä tässä vaiheessa, mutta jos tällaisia sattuu suoraan olemaan, niin voidaan mainita] https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L1148&from=EN Sähköisen asioinnin tietoturvallisuus –ohje, VM 25/2017 http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80012/VM_25_2017.pdf?sequence=1&isAllowed=y EuroPriSe Criteria for the certification of IT products and IT-based services https://www.european-privacy-seal.eu/EPS-en/Criteria