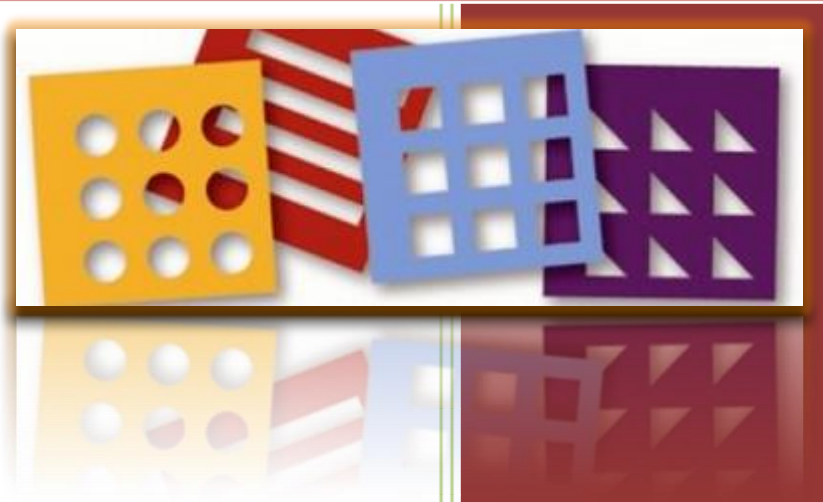
2018

Lupapalvelun tietoturvan itsearviointi



30.4.2018

Versiohistoria

Versio:	Pvm:	Laatijat:	Selitys:
Versio 1	9.4.2018	Henri Tenhunen	Dokumentin luonti
Versio 1.1	19.4.2018	Henri Tenhunen	Päivitetty osio 1.2
Versio 1.2	27.4.2018	Henri Tenhunen	Päivitetty osio 1.2
Versio 1.3	30.4.2018	Irma-Leena Notkola Henri Tenhunen	Pieniä päivityksiä eri kohtiin

Sisällys

1 Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

1.1 Tietoaineistojen sähköisen käsittelyn periaatteet

Vaatimus	Toteutuminen
Asiointipalvelussa käsitellään vain käyttötarkoituksen kannalta tarpeellista ei-julkista tietoa.	Kyllä
Henkilötietojen käsittelyssä noudatetaan lakia. Tarpeettomia tietoja käyttäjistä ei kerätä eikä tallenneta, ja henkilötiedot tuhotaan viiveettä, kun niiden säilyttämiselle ei ole enää perustetta.	Kyllä
Asiointipalvelu tukeutuu ensisijaisesti kansallisiin hallinnon sähköisen asioinnin tukipalveluihin, joiden tietoturvallisuuden taso on tiedossa. Kaupallisia, oletusarvoisesti ei-luotettuja tukipalveluita, voidaan kuitenkin käyttää, mikäli niiden vaatimuksenmukaisuus on mahdollista varmentaa tai niissä käsitellään ainoastaan julkista tietoa.	Suunnitelmana on toteuttaa lupapalveluun vahva tunnistautuminen Suomi.fi-palvelun kautta. Yhteys etätyöpöytään tulee toteuttaa Suomi.fi – palveluväylän kautta, mikäli etätyöpöytä ja lupapalvelu eivät sijaitse samassa sisäverkossa.

1.2 Asiointipalvelun tietoturvallinen rakenne ja kontrolliympäristö

Vaatimus	Toteutuminen
Asiointipalvelun määrämuotoinen riskianalyysi ohjaa palvelun rakenneratkaisujen, tietoturvatavoitteiden ja kontrolliympäristön suunnittelua. Suojausratkaisut pyritään valitsemaan ja toteuttamaan siten, että ne pienentävät tunnistettuja riskejä sekä täyttävät tietoturvatavoitteita ja tietoturvakontrolleja tarkoituksenmukaisesti ja kustannustehokkaasti.	Tietoturvaan liittyvät uhat ja riskit on huomioitu suunnittelussa. Palvelun rakenneratkaisut, tietoturvatavoitteet ja kontrolliympäristön suunnittelu pohjautuvat Kansallisarkiston sovelluskehittämisen linjauksiin, teknologiasuosituksiin sekä sisäiseen auditointiin. Tunnistettuja riskejä on havaittu ja dokumentoitu sekä tietoturvatavoitteita täyttäviä suojausratkaisuja on toteutettu järjestelmään koko kehityskaaren aikana.
Palvelu on eristetty internetistä DMZ-vyöhykkeellä. Asiointipalvelun käyttöympäristön tietoverkko on segmentoitu, ja palvelun komponentit on	Lupajärjestelmän omistajan tulee huolehtia edellä mainittujen ehtojen täyttymisestä.

sijoiteltu suojaustarpeen mukaisiin vyöhykkeisiin. Vyöhykkeiden välinen tiedonsiirto on kontrolloitu palomuurein tai yhdyskäytäväratkaisuin.	
Palvelun hyökkäyspinta-alan rajaamiseksi eri käyttäjäryhmille suunnatut käyttöliittymät ja palvelurajapinnat on eriytetty siten, että ne sisältävät vain tarvittavan minimitoiminnallisuuden ja rajatun pääsyn ei-julkiseen tietoon.	Lupapalvelussa on vain asiointiprosessin kannalta välttämättömät minimitoiminnallisuudet. Käyttäjäryhmille on suunnatut käyttöliittymät, joissa pääsy tietoon rajataan käyttäjäryhmän tietotarpeiden mukaisesti. Käyttöönoton yhteydessä pääsyä tietoon olisi syytä rajata rakenteellisesti siten, että viranomaisen ja pääkäyttäjän käyttämät toiminnot eristetään julkisen internetverkon asiakaskäyttöliittymästä.
Tiedon salausta käytetään tarveanalyysin mukaisesti kohteissa, joissa tiedon luottamuksellisuutta ei voida muutoin varmistaa. Salausratkaisulta vaadittava vahvuus on määritelty (mm. salausalgoritmin ominaisuudet, avainpituus), eritoten suhteessa vaadittuun salausaikaan. Salausratkaisu otetaan käyttöön oikein (asetukset, konfiguraatio). Varmenteita ja salausavaimia hallitaan huolellisesti.	Varsinaista tiedon salausta ei käytetä, mutta salasanat ja sähköpostivarmenteet tallennetaan tietokantaan kryptograafisen md5 –funktion tiivisteenä, jotta voidaan tarkistaa tiedon eheys, muuttumattomuus ja identtisyys.
Luottamuksellisessa asiakasviestinnässä käytetään ainoastaan kanavia ja tukipalveluita, joiden salauksen riittävä taso on todennettavissa. Sähköpostin käyttöä luottamuksellisessa viranomaisviestinnässä on syytä käyttää harkiten ja riskiarvioon perustuen suhteessa siirrettäviin tietoihin liittyviin riskeihin. Sähköpostiviestien alkuperän, eheyden ja luottamuksellisuuden varmistamiseen on syytä kiinnittää huomiota. Sähköpostin käyttö tulee lähtökohtaisesti rajata julkisen tiedon tai herätetietojen välittämiseen, ellei viestien luottamuksellisuutta ja eheyttä ole salattu erillisellä viranomaisen hyväksymällä salausmenetelmällä.	Lupajärjestelmän omistajan tulee huolehtia edellä mainittujen ehtojen täyttymisestä.
Mahdolliset palvelunestohyökkäykset on otettu huomioon mm. rakenneratkaisuissa ja käyttöpalveluympäristön koventamisessa. Palvelunestohyökkäyksen vaikutusten rajaaminen ja toiminta poikkeamatilanteissa on suunniteltu.	Kyllä

Lokien riittävästä tuottamisesta asiointipalvelun tapahtumista (mm. pääsynvalvonta- ja käyttölokitiedot eri lokilähteistä) ja lokien eheyden ja kirjausketjun suojaamisesta sekä lokitietojen poistoista on huolehdittu lokisuunnitelman mukaisesti. Asiointipalvelun lokitietoja seurataan ja niitä analysoidaan.	Lupajärjestelmä tuottaa useimmista tietokannan tauluista lisäyksen, muokkauksen ja poistamisen ajankohdat sekä viittaukset käyttäjään, joka on lisännyt/muokannut/poistanut tietoja. Tietokannassa on myös erillinen taulu muille lokitiedoille, joka sisältää tiedot sisään – ja uloskirjautumisista, hakemuksen poistamisesta, lausunnon sekä liitteiden avaamisesta. Lokitiedot on suojattu muutoksilta siten, että vain tietokannan pääkäyttäjä/ylläpitäjä voi tehdä muutoksia lokeihin. Lokitietojen säilytysaika on määriteltävissä. Tulevan lupapalvelun ylläpitäjän on varmistettava, että verkon laitteet ja yhdyskäytäväratkaisut tuottavat tietoturvallisuuden valvontaan tarvittavat lokitiedot.

1.3 Tunnistaminen, valtuuttaminen ja tahdonilmaukset

Vaatimus	Toteutuminen
Tarve palvelun asiakkaiden yksilöimiseksi ja tunnistamiseksi on arvioitu. Vaatimukset sähköisen tunnistamisen menetelmälle on määritelty ja tarkoituksenmukainen tunnistusratkaisu- tai palvelu on otettu käyttöön.	Vaatimukset vahvan tunnistamisen menetelmälle (Suomi.fi-tunnistus) on suunniteltu, mutta palvelua ei ole otettu käyttöön. Ulkomaalaisten käyttäjien tunnistamismenetelmää ei ole vielä ratkaistu.
Tunnistusvälineiden saatavuus on huomioitu. Tunnistusvälineiden tulee joko olla valmiiksi niitä tarvitsevien käyttäjien hallussa tai palvelun käyttäjillä tulee olla mahdollisuus hankkia tarvittavat tunnistusvälineet.	Kyllä
Asiointipalvelun käyttö noudattaa pienimmän käyttövaltuuden periaatetta kaikkien käyttäjäryhmien osalta, mukana lukien tietojärjestelmien käyttämät palvelurajapinnat. Käyttövaltuuksien hallinta on vastuutettu.	Kyllä
Palvelun omistaja on tunnistanut tarpeen asiakkaiden tahdonilmausten rekisteröintiin. Palvelun omistaja on arvioinut, kuinka todennäköisesti sen tulee kyetä osoittamaan toteen asiakkaan tekemä tahdonilmaus ja	Kyllä

mitä oikeusvaikutuksia palvelun tarjoajalle seuraa siitä, jos ettei se kykene tätä tekemään. Palvelun tarjoajan toteuttaa arvionsa perusteella ja sitä koskevan lainsäädännön mukaisesti tahdonilmausten rekisteröinnin joko luotettavalla sähköisellä allekirjoituksella tai siihen verrattavalla teknisellä menetelmällä.	

1.4 Suunnittelu, ylläpito ja muutoshallinta

Vaatimus	Toteutuminen
Palvelun toteutuksessa kiinnitetään huomiota yksinkertaisuuteen.	Kyllä
Palvelun ulkoasu on yhdenmukainen palvelua tarjoavan viranomaisen muiden verkkopalveluiden kanssa ja palvelun aitous on todennettavissa palvelinvarmenteen perusteella.	Kyllä hankevaiheessa, THL:n aineistokatalogin kanssa yhdenmukainen ulkoasu
Palvelun kannalta relevantit uhkatekijät on tunnistettu.	Kyllä
Palvelukehityksessä ja ylläpidossa sovelletaan menetelmiä, joissa tietoturvallisuuden varmistaminen on integroitu kiinteäksi osaksi palvelun kehittämistä, laadunvarmistusta ja ylläpitoa, ja joissa arvioidaan sovelluskerroksen tietoturvallisuutta mm. vertaisarvioinnein, koodikatselmoinnein, teknisellä haavoittuvuus- ja tunkeutumistestauksella, teknistä testaus täydentävillä manuaalisilla testausmenetelmillä, tietoturva-auditoinneilla.	Kyllä hankevaiheessa. Jatkokehityksen ja ylläpidon osalta vastuu jää palvelun omistajalle

Arviointipohja perustuu VAHTI-ohjeen ”Sähköisen asioinnin tietoturvallisuus –ohje” (Valtiovarainministeriön julkaisuja 25/2017) liitteeseen 4 ”Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista”.