Varmennepalvelut)

3.4.2024

DVV Kansallinen Leima-palvelu

Leimapalvelun asiakassovelluk-sen tietoturvavaatimukset

3.4.2024

Dokumentinhallinta

Omistaja	
Laatinut	Annika Gibson
Tarkastanut	
Hyväksynyt	

Version hallinta

versionro	mitä tehty	pvm/henkilö
v 1.0	Dokumentti luotu	1.1.2024/AG
v 1.1	Stilisoivat muutokset	3.4.2024/AG

Sisällysluettelo

DVV Kansallinen Leimapalvelu

1 Johdanto

1.1 Tarkoitus

Tässä asiakirjassa esitetään tietoturvan vähimmäisvaatimukset asiakkaille, jotka lähettävät leimauspyyntöjä DVV leimapalveluun REST-rajapinnan kautta. Vaatimukset kattavat seuraavat osa-alueet:

- Fyysinen tietoturva
- Verkon tietoturva
- Laitteiston tietoturva
- Käyttöympäristön tietoturva
- Ohjelmiston tietoturva

Vaatimukset on laadittu leimapalvelun, asiakassovelluksen ja salaisuuksien (yksityiset avaimet ja muut ei-julkiset tiedot) sekä laitteiden ja verkkojen suojaamiseksi.

Asiakkaan on ymmärrettävä esitetyt vaatimukset, otettava käyttöön vaaditut tietoturvallisuuden hallintakeinot sekä esitettävä näyttöä hallintakeinojen käytöstä ennen leimauspyyntöjen lähettämistä leimapalveluun REST-rajapinnan kautta.

1.2 Vaatimusten noudattamisen arviointi

Vaatimusten noudattamisen arvioinnin tarkoituksena on varmistaa, että asiakas sitoutuu täyttämään tässä asiakirjassa esitetyt vaatimukset ja että tarvittavat tietoturvallisuuden hallintakeinot on otettu käyttöön. Vaatimusten noudattamisen arviointi etenee seuraavasti:

1. DVV toimittaa tämän asiakirjan ja siihen liittyvän asiakassovelluksen tietoturva-vaatimusten tarkistuslistan Asiakkaalle.

2. Asiakas vertaa käyttämiään tietoturvallisuuden hallintakeinoja tähän asiakirjaan ja ottaa mahdolliset puuttuvat hallintakeinot käyttöön.

3. Asiakas täyttää asiakassovelluksen tietoturvavaatimusten tarkistuslistan ja toimittaa sen DVV:lle.

4. DVV käy täytetyn asiakassovelluksen tietoturvavaatimusten tarkistuslistan läpi, antaa siitä palautetta ja tarvittaessa neuvoo Asiakasta puuttuvien hallintakeino-jen käyttöönotossa.

5. DVV hyväksyy asiakassovelluksen tietoturvavaatimusten tarkistuslistan, kun asianmukaiset hallintakeinot on otettu käyttöön.

Tarkistuslista sisältää seuraavat tiedot:

- **Tunnus:** Viittaus tämän asiakirjan luvun numeroon, jossa kerrotaan kyseisestä vaatimuksesta (esimerkiksi 2.1)
- **Vaatimus:** Viittaus vaatimuksen nimeen
- **Hallintakeino käytössä:** Valintaruutu, jonka avulla Asiakas osoittaa täyttäneensä vaatimuksen eli ottaneensa vaaditut tietoturvallisuuden hallintakeinot käyttöön.
- **Kuvaus:** Lyhyt kuvaus käytetyistä tietoturvallisuuden hallintakeinoista (tai selvitys siitä, miksi hallintakeinoja ei ole otettu käyttöön)

1.3 Asiakirjan rakenne ja merkinnät

Vaatimusten määritelmät on jaettu osioihin Kuvaus, Perusteet ja Esimerkkejä:

- Kuvaus kertoo varsinaisen vaatimuksen
- Perusteissa kerrotaan syyt vaatimukselle
- Esimerkeissä on lueteltu esimerkkejä vaatimuksen mukaisista tietoturvallisuuden hallintakeinoista

Asiakirja sisältää kahdenlaisia vaatimuksia: **pakollisia** ja **valinnaisia**.

- **Pakollisten** vaatimusten kuvauksissa käytetään ilmaisuja "TULEE”/”TÄYTYY”.
- **Valinnaiset** vaatimukset ovat DVV:n suosituksia, ja niiden kuvauksissa käytetään ilmaisuja ”TULISI”/”PITÄISI” tai ”SUOSITELLAAN”.

2 Yleiset tietoturvavaatimukset

2.1 Asiakassovelluksen ympäristö varataan vain leimapalvelun käyttöön

2.1.1 Kuvaus

Asiakassovelluksen ympäristö (asiakaspalvelimet, jotka luovat leimattavasta ohjelmistopaketista tiivisteen ja lähettävät sen leimapalveluun; Hardware Security Moduulit (HSM), joihin tallennetaan avaintietoja jne.) TULEE varata vain leimauspalveluun liittyville toiminnoille. Näitä toimintoja ovat mm.

- todentaminen leimapalveluun
- avaintietojen (esim. todennusavain) säilytys
- tiivisteen luominen leimattavasta tietosisällöstä
- leimauspyynnön (tiivisteen) lähettäminen leimapalveluun ja vastaanottaminen

2.1.2 Perusteet

Asiakassovellusta käytetään tietoturvallisuuden varmistamiseen, joten sen ympäristö tulee pitää mahdollisimman yksinkertaisena ja rajattuna. Asiakassovellusympäristö sisältää salaisuuksia, kuten rajapintavarmenteen yksityisen avaimen. Asiakassovellusympäristön rinnakkainen käyttö jaettuna resurssina muuhun tarkoitukseen saattaa vaikuttaa sen toimintaan, jolloin ympäristö ei välttämättä toimi niin kuin pitäisi.

3 Fyysiset tietoturvavaatimukset

3.1 Asiakassovellusympäristön fyysisen pääsyn rajoittaminen

3.1.1 Kuvaus

Asiakassovellusympäristö (mm. asiakassovelluspalvelin ja HSM) TULEE suojata luvattomalta käytöltä. Fyysisen tietoturvallisuuden hallintakeinojen TÄYTYY pystyä torjumaan, estämään tai havaitsemaan asiakassovellusympäristöön tallennettujen arkaluonteisten tietojen ja järjestelmien luvaton käyttö tai paljastuminen. Tätä vaatimusta TULISI soveltaa myös etäjärjestelmiin, kuten etähallintapäätteisiin.

3.1.2 Perusteet

Jos asiakassovellus on rajoituksetta kenen tahansa käytettävissä, haitalliset toimijat pystyvät helpommin paljastamaan arkaluonteisia tietoja tai vaikuttamaan ohjelman toimivuuteen. Tämän vaatimuksen tarkoituksena on varmistaa, ettei laitteiston tai siirrettävien tietovälineiden luvatonta käyttöä sallita ja että mahdollinen luvaton käyttö havaitaan.

3.1.3 Esimerkkejä

- Luettelo työntekijöistä, joilla on pääsyoikeus järjestelmään.
- Portit ja ovet estävät pääsyn laitteiden luokse.
- Tiloihin pääsyä hallitaan kaksivaiheisen kulunhallinnan avulla.
- Pääsyä tiloihin valvotaan videovalvonnalla ja mahdollisista tietoturvaloukkauksista lähtee automaattisesti ilmoitus.
- Tiloihin sisään- ja uloskirjautumiset merkitään automaattisesti lokiin.
- Vartijat tarkistavat henkilöllisyyden ennen tiloihin päästämistä.

3.2 Fyysistä pääsyä asiakassovelluksen varmuuskopioihin rajoitetaan

3.2.1 Kuvaus

Asiakassovellusympäristön varmuuskopiot TÄYTYY suojata luvattomalta käytöltä. Varmuuskopioiden luvaton käyttö ja varmuuskopioihin pääsy TULEE pystyä torjumaan, estämään tai havaitsemaan fyysisen tietoturvallisuuden hallintakeinoilla.

3.2.2 Perusteet

Varmuuskopiot säilytetään tavallisesti erillään varsinaisesta järjestelmästä, jotta ne ovat käytettävissä, vaikka ensisijainen järjestelmä tuhoutuisi. Varmuuskopioissa on samat arkaluonteiset tiedot kuin varsinaisessa asiakassovelluksessa, joten ne on suojattava yhtä huolellisesti.

3.2.3 Esimerkkejä

- Luettelo työntekijöistä, joilla on pääsyoikeus järjestelmään.
- Portit ja ovet estävät pääsyn laitteiden luokse.
- Tiloihin pääsyä hallitaan kaksivaiheisen tunnistautumisen avulla.
- Varmuuskopioihin pääsyä valvotaan ja siitä pidetään lokia.
- Pääsyä tiloihin valvotaan videovalvonnalla ja mahdollisista tietoturvaloukkauksista lähtee automaattisesti ilmoitus.
- Tiloihin sisään- ja uloskirjautumiset merkitään automaattisesti lokiin.
- Vartijat tarkistavat henkilöllisyyden ennen tiloihin päästämistä.

4 Laitteiston tietoturvavaatimukset

4.1 Asiakassovellusympäristöllä on oma, vain sen käyttöön varattu laitteisto

4.1.1 Kuvaus

Leimauspyyntöjen käsittelyyn liittyvät järjestelmät TULISI asentaa omaan laitteistoonsa, jota käytetään vain leimaustoimintoihin.

4.1.2 Perusteet

Koska asiakassovellusta käytetään tietoturvallisuuden varmistamiseen, uhkavektorit tulee minimoida. Kun asiakassovellusympäristö pidetään vain sille varatussa omassa laitteistossaan, muiden järjestelmien haavoittuvuudet tai puutteet (esimerkiksi liiallinen resurssien kulutus) eivät vaikuta siihen.

4.1.3 Esimerkkejä

- Asiakassovelluspalvelin (käyttöjärjestelmä ja ohjelmisto) on asennettu vain sille varattuun laitteistoon.
- Asiakassovelluspalvelin (käyttöjärjestelmä ja ohjelmisto) on asennettu virtuaalikoneeseen. Virtuaaliympäristössä on ainoastaan muita leimaustoimintoihin käytettäviä virtuaalipalvelimia (esim. varajärjestelmät, kuormantasaus).

5 Verkon tietoturvavaatimukset

5.1 Asiakassovelluksen ja leimapalvelun välillä on suojattu yhteys

5.1.1 Kuvaus

Asiakassovelluksen ja leimapalvelun välinen tiedonsiirto TÄYTYY suojata käyttämällä alan hyväksyttyjä ja hyväksi todettuja algoritmeja, joilla leimauspyynnöt ja -vastaukset suojataan väärinkäytöltä ja paljastumiselta.

5.1.2 Perusteet

Leimapalvelun ja asiakassovelluksen välisen tiedonsiirron suojaamisella varmistetaan, että yhteys leimapalveluun tulee tunnetulta taholta.

5.1.3 Esimerkkejä

- Asiakassovelluksen ja leimapalvelun välinen VPN (TLS) käyttää EC P-384 / AES-256 / SHA-384 -algoritmeja.

5.2 Yhteys leimapalveluun on rajattu vain asiakassovelluksen käyttöön

5.2.1 Kuvaus

Asiakassovellusympäristöstä leimapalveluun muodostettavien yhteyksien TÄYTYY olla ainoastaan asiakassovelluspalvelimen käynnistämiä. Asiakassovellusympäristön verkko on käytännössä lohkottava/suojattava/rajattava siten, että vain asiakassovelluspalvelin/-palvelimet voivat viestiä leimapalvelun kanssa VPN-tunnelin välityksellä.

5.2.2 Perusteet

Asiakassovelluspalvelin on ainoa ohjelmaympäristön komponentti, joka tarvitsee yhteyden leimapalveluun. Ympäristön muut palvelimet ja tietokoneet eivät yhteyttä tarvitse, joten niiden ei pitäisi pystyä muodostamaan yhteyttä leimapalveluun. Yhteys pitäisi katkaista asiakassovelluksen verkossa.

5.3 Yhteys asiakassovellusympäristöön on suojattu

5.3.1 Kuvaus

Asiakassovellusympäristön verkkolohkon koko TÄYTYY minimoida ja suojata tavallisimmilta verkkohyökkäyksiltä. Asiakassovellusympäristön verkon suojauksen vähimmäisvaatimukset ovat:

- Pääsy asiakassovellusympäristöön TÄYTYY suojata siten, että vain asiakassovelluksen välttämättömät palvelut altistuvat ulkoisille verkoille.
- Kaikkien verkon suojaukseen käytettävien laitteiden TÄYTYY estää muiden kuin välttämättömien palveluiden pääsy asiakassovellusympäristöön ja sieltä pois.
- Jos asiakassovelluspalvelinta tai muuta asiakassovellusympäristön osaa käytetään etäyhteyden välityksellä, etäyhteyspisteen ja asiakassovelluksen välinen tiedonsiirto TÄYTYY suojata.

5.3.2 Perusteet

Asiakassovellusohjelma sisältää arkaluonteisia tietoja, jotka on suojattava. Tarpeettomien palveluiden ja muiden uhkavektoreiden rajoittaminen minimoi järjestelmään murtautumisen riskin vaarantamatta liiketoiminnan jatkuvuutta.

5.3.3 Esimerkkejä

- Verkko lohkotaan palomuurin avulla siten, että asiakassovelluslaitteet sijaitsevat omassa suojatussa lohkossaan.
- Verkkojen välinen raja suojataan palomuuriratkaisulla, joka hyväksyy vain tarvittavien järjestelmien yhteydet.
- Tavallisimmat verkkohyökkäykset havaitaan ja estetään tunkeilijan havaitsemisjärjestelmien (IDS) tai murron estämisjärjestelmien (IPS) avulla.

6 Käyttöjärjestelmävaatimukset

6.1 Pääsyä asiakassovelluksen käyttöjärjestelmään rajoitetaan asianmukaisilla mekanismeilla

6.1.1 Kuvaus

Pääsyä asiakassovelluksen käyttöjärjestelmään TULEE rajoittaa asianmukaisilla mekanismeilla niin, että vain valtuutetut henkilöt pystyvät kirjautumaan järjestelmään. Vähimmäisvaatimukset:

- Jos kirjautumissalaisuutena käytetään salasanoja, salasanakäytännön TULEE olla riittävän vahva.
    - Salasanojen on oltava riittävän pitkiä
    - Salasanojen on oltava monimutkaisia
- Pääsy TULEE myöntää ainoastaan tarvittaessa.
- Järjestelmään pääsyä TÄYTYY valvoa siten, että järjestelmään kirjautumiset kirjataan lokiin.
- Pääsyoikeudet tarkastetaan säännöllisesti, ja pääsy järjestelmään estetään henkilöiltä, jotka eivät enää tarvitse pääsyoikeutta (esim. muuttuneet työtehtävät, eläkkeelle jäänti)

Kaksivaiheista tunnistusta SUOSITELLAAN

6.1.2 Perusteet

Asiakassovelluskäyttöjärjestelmän avulla voidaan vaikuttaa asiakassovelluksen toimintoihin (esim. arkaluonteisten tietojen paljastaminen tai varmennepyyntöjen pakottaminen). Siksi oikeus järjestelmän käyttöön tulisi rajata mahdollisimman pienelle ja luotettavalle joukolle.

6.1.3 Esimerkkejä

- Salasanan vähimmäispituus 12 merkkiä, salalauseiden käyttö salasanojen sijaan.
- Toimikorttipohjainen kirjautuminen.

- Pääsyoikeus asiakassovellusohjelmaan myönnetään AD-ryhmien perusteella, ja ryhmät tarkastetaan säännöllisesti.
- Kirjautumiset asiakassovelluskäyttöjärjestelmään kirjataan lokiin ja lokit lähetetään ulkoiseen lokienhallintapalveluun esimerkiksi syslog-protokollaa käyttäen.

6.2 Asiakassovellusjärjestelmän käyttöoikeuksien laajuus minimoidaan

6.2.1 Kuvaus

Asiakassovellusjärjestelmän käyttöoikeuksien laajuus TULEE minimoida. Asiakassovellusjärjestelmän käyttöoikeuksien käsittelyn vähimmäisvaatimukset:

- Koko henkilöstön TULEE käyttää kirjautumiseen henkilökohtaista kirjautumistiliä yhteisen tilin (esim. root) sijaan.
- Jokaisella (henkilö-)käyttäjällä TÄYTYY olla erillinen kirjautumistili, jaettuja tilejä EI TULE käyttää kirjautumiseen.
- Asiakassovelluksen hallintaoikeudet TULEE myöntää ainoastaan hallintahenkilöstölle.
- Palveluille TÄYTYY tarpeen mukaan olla erilliset palvelutilit, palveluiden ei pitäisi käyttää root/administrator-tiliä.
- Laajennettuja käyttöoikeuksia (esim. sudo tai Administrator) TULEE käyttää ainoastaan tarvittaessa.

6.2.2 Perusteet

Kun järjestelmän käyttöoikeuksien laajuus minimoidaan, myös virhemääritysten ja väärinkäytön mahdollisuudet minimoidaan.

6.3 Asiakassovelluskäyttöjärjestelmän koventaminen

6.3.1 Kuvaus

Käyttöjärjestelmä TULEE koventaa siten, että se sisältää vain välttämättömät sovellukset ja palvelut. Vähimmäisvaatimukset:

- Kaikki tarpeettomat verkkoportit ja -palvelut TULEE sammuttaa ja poistaa järjestelmästä.
- Palveluita ja sovelluksia EI PITÄISI lisätä oletusmäärityksillä. Määritykset TÄYTYY sen sijaan tarkistaa ja palveluiden ylimääräiset toiminnallisuudet poistaa.
    - Ssh:n kaltaisten palveluiden oletusmääritykset eivät välttämättä täytä tietoturvavaatimuksia.
- USB-portit TULEE poistaa käytöstä, ellei niille ole selkeää liiketoiminnan kannalta tärkeää käyttötarkoitusta.

6.3.2 Perusteet

Asiakassovellusympäristön palvelut ovat ensisijainen hyökkäysreitti asiakassovellusympäristöön. Tarpeettomien porttien ja palveluiden poistaminen järjestelmästä minimoi uhkavektorit, mikä tekee ympäristöön hyökkäämisestä vaikeampaa.

6.4 Asiakassovelluksen käyttöjärjestelmä päivitetään säännöllisesti

6.4.1 Kuvaus

Käyttöjärjestelmät TULEE pitää ajan tasalla. Erityisesti tietoturvakorjaukset TULISI asentaa järjestelmään niiden julkaisun jälkeen mahdollisimman pian. Päivitykset TULISI hakea yrityksen omasta keskitetystä sijainnista, kuten WSUSista tai Spacewalkista.

6.4.2 Perusteet

Järjestelmän asianmukainen päivittäminen auttaa suojautumaan tunnetuilta haavoittuvuuksilta.

6.4.3 Esimerkkejä

- Käyttöjärjestelmät päivitetään kuukausittain tai aina kun merkittäviä tietoturvapäivityksiä julkaistaan.
- Käyttöjärjestelmän korjaustiedostotasoa hallinnoidaan keskitetysti, ja eri käyttöjärjestelmien korjaustiedostotason kulloinenkin tila on aina tiedossa.

6.5 Asiakassovelluksen käyttöjärjestelmää valvotaan

6.5.1 Kuvaus

Käyttöjärjestelmätasolla suoritettavia toimintoja TULEE seurata ja toiminnot TULEE kirjata lokiin. Lokeihin täytyy kirjata vähintään seuraavat tiedot:

- Käyttöjärjestelmään ja sieltä ulos kirjautuminen
- Pääsynvalvonnan muutokset
- Käyttöoikeuksien korottaminen normaaleista oikeuksista hallintaoikeuksiksi
- Hallintaoikeuksin tehdyt toiminnot (komennot), kuten ohjelmiston asennus
- Epäonnistuneet / luvattomat käyttöyritykset
- Hallintaoikeuksien muutokset
    - esim. sudo-oikeudet

Keskitetyn lokipalvelimen käyttöä salatun yhteyden välityksellä SUOSITELLAAN paikalliseen palvelimeen tallentamisen sijaan.

6.5.2 Perusteet

Järjestelmätapahtumien tallennuksen avulla järjestelmänvalvojat pystyvät päättelemään, käytetäänkö järjestelmää luvattomasti.

6.5.3 Esimerkkejä

- Käyttöjärjestelmän tapahtumat kerätään rsyslog-protokollan avulla. Lokit lähetetään keskitettyyn lokienhallintajärjestelmään.

6.6 Asiakassovelluksen käyttöjärjestelmää valvotaan ja suojataan haittaohjelmien varalta

6.6.1 Kuvaus

Käyttöjärjestelmä TULISI suojata haittaohjelmilta asianmukaisilla suojaustyökaluilla. Näitä voivat olla esim. paikalliset virustorjuntaohjelmat, paikalliset tai verkkopohjaiset murron estämisjärjestelmät (HIPS) , jotka havaitsevat palvelimen mahdollisen vaarantumisen.

6.6.2 Perusteet

Virustorjuntaohjelmat ja muut HIPS-järjestelmät estävät yleisiä haittaohjelmia leviämästä ja aiheuttamasta ongelmia suojatun ympäristön muissa osissa.

6.6.3 Esimerkkejä

- Paikalliset käyttöjärjestelmät suojataan HIPS:n avulla.
- Asiakassovellusverkon IDS-järjestelmä ilmoittaa esim. haittaohjelmatartunnoista.