Tietoturvakuvaus

31.1.2019

JULKINEN

Sisällysluettelo

1 Johdanto

Palvelun tietoturva on Signomille ensiarvoisen tärkeää, ja se on huomioitu kaikessa yrityksemme toiminnassa. Allekirjoitusten varmentamiseksi ja luottamuksellisten tietojen suojaamiseksi käytämme useita menetelmiä.

Tämän dokumentin tarkoitus on kuvata keskeiset periaatteet ja tekniset ratkaisut, joilla Signom-allekirjoituspalvelun tietoturva on toteutettu.

2 Hallinnollinen tietoturva

2.1 Noudattaako Signom jotakin tietoturvastandardia?

Signom noudattaa tietoturvan hallinnoinnissa ISO27001-standardin mukaista tietoturvan johtamisjärjestelmää.

ISO27001 kattaa seuraavat osa-alueet:

- A.5 Tietoturvapolitiikka
- A.6 Tietoturvan organisointi
- A.7 Omaisuuden hallinta
- A.8 Henkilöstöturvallisuus
- A.9 Fyysinen turvallisuus
- A.10 Viestintä- ja operatiivinen turvallisuus
- A.11 Pääsynhallinta
- A.12 Tietojärjestelmien turvallisuus
- A.13 Poikkemamien hallinta
- A.14 Liiketoiminnan jatkuuvuden hallinta
- A.15 Sääntelyn noudattaminen

Tietoturvan johtamisesta vastaa tietoturvan johtoryhmä, joka valvoo tietoturvan toteutumista ja hyväksyy tietoturvaa koskevat käytännöt ja prosessit.

2.2 Onko tietoturvasta tehty ulkoinen auditointi?

Nixu Certification Oy on tehnyt ISO27001-standardin mukaisen auditoinnin ja myöntänyt auditoinnin perusteella Signomille ISO27001-sertifikaatin. Sertifiointiin kuuluu vuosittainen seuranta-auditointi.

ISO27001 sertifikaatti on nähtävillä sivulla https://company.signom.com/tietoturva/

2.3 Onko tietoturvasta tehty sisäinen auditointi?

Sisäinen auditointi suoritetaan kerran vuodessa. Merkittävien muutosten tai tietoturvapoikkeamin jälkeen suoritetaan lisäksi ylimääräinen sisäinen tarkastus.

Sisäisestä auditoinnista laaditaan raportti, joka käsitellään tietoturvan johtoryhmässä.

3 Ohjelmistokehitys

Tietoturva huomioidaan läpi koko ohjelmistokehityksen elinkaaren.

3.1 Miten tietoturva on huomioitu ohjelmistokehityksessä?

Kaikille Signomin ohjelmistokehittäjille pidetään vuosittain koulutus seuraavista aiheista:

1. Yrityksen tietoturvaohjeet ja -käytännöt
2. Henkilötietojen käsittelyä koskeva lainsäädäntö ja menettelyohjeet
3. Ohjeistus tietoturvalliseen sovelluskehitykseen (pohjautuu OWASP ohjeisiin ja yleisimpiin haavoittuvuuksiin)

Ennen tuotantoasennusta jokaiselle ohjelmistokomponentille tehdään tietoturvakatselmointi.

3.2 Miten käytettyjen ohjelmistojenkomponenttien tietoturvallisuus on varmistettu?

Kaikki käytetyistä ohjelmistokomponenteista pidetään kirjaa. Ennen uuden ohjelmistokomponentin käyttöönottoa sille tehdään tietoturvakatselmointi, ja käyttöönotto vaatii pääohjelmoijan hyväksynnän.

Käytettyjen ohjelmistokomponenttien tietoturvatiedotteita seurataan aktiivisesti.

3.3 Miten ohjelmakoodi on suojattu?

Ohjelmakoodia säilytetään GIT-versionhallintajärjestelmässä Google Cloud Source Repositories -palvelussa. Kaikista muutoksista ohjelmakoodiin jää pysyvä merkintä versiohistoriaan.

Pääsy ohjelmakoodiin on suojattu 2-vaiheisella tunnistuksella ja työntekijöiden rooliin pohjautuvalla pääsynhallinnalla. Google Cloud Source Repositories -palvelun tietoturva on ISO27001 sertifioitu.

3.4 Miten ohjelmakoodia ja konfigurointia katselmoidaan?

Ennen kuin projekti siirretään tuotantokäyttöön, projektin ohjelmakoodille ja konfiguraatiolle suoritetaan tietoturvakatselmointi.

Katselmoinnin järjestämisestä projektipäällikkö ja siihen osallistuu projektin ohjelmoija, vanhempi ohjelmoija ja tietoturvavastaava.

Projektipäällikkö laatii tietoturvakatselmoinnista raportin.

3.5 Miten palvelua testataan?

Palvelun toimintaa testataan kehityksen aikana manuaalisilla testeillä ja valmiin toiminnallisuuden osalta noin tuhannella automatisoidulla testitapauksella. Testitapaukset suoritetaan Selenium-ohjelmiston avulla.

Kaikki testitapaukset suoritetaan automaattisesti jokaisen palvelun ohjelmakoodin tehdyn muutoksen jälkeen.

4 Käyttöoikeudet

4.1 Kenellä on pääsy asiakirjoihin?

Käyttäjillä on pääsy ainoastaan asiakirjoihin, joissa he ovat osapuolina tai joihin heillä on yritysroolin kautta myönnetty pääsy.

Yritysratkaisussa asiakkaan valtuuttamat pääkäyttäjät voivat lisätä palveluun käyttäjiä ja määrittää heille käyttöoikeudet yrityksen asiakirjoihin.

Asiakirjan tallennetaan palvelimille salatussa muodossa, ja ne ovat myös konesalioperaattorin varmuuskopioissa salatussa muodossa.

Signomin toimistoverkossa käsitellään ainoastaan käyttäjätietoja, jotka ovat välttämättömiä laskutusta ja asiakastukea varten. Signomin henkilöstön pääsy asiakastietoihin on rajattu kunkin henkilön kannalta vain välttämättömiin tietoihin. Asiakastietojen käsittelystä palvelun ylläpitoa, laskutusta ja käyttäjätukea varten kerätään lokitietoa.

4.2 Onko Signomin työntekijöillä pääsy asiakirjoihin?

Laskujen muodostamiseen ja käsittelyyn osallistuvilla henkilöillä on pääsy laskutuksen kannalta tarpeellisiin tietoihin. Näihin tietoihin kuuluvat sopimusten ja allekirjoitusten määrät.

Tukitehtävissä työskentelevillä henkilöillä on pääsy asiakirjatietoihin tukipyyntöihin vastaamiseksi. Kaikesta asiakastietojen käsittelystä kerätään lokitiedot.

4.3 Miten kauan asiakirjatiedostoja säilytetään?

Asiakirjatiedostoja eli allekirjoitettavia PDF-tiedostoja säilytetään palvelussa allekirjoitusprosessin ajan. Asiakirjatiedostot poistetaan Signomin palvelimelta heti, kun asiakirjan säilytys allekirjoitusprosessin kannalta ei ole enää välttämätöntä. Kun kaikki osapuolet ovat allekirjoittaneet asiakirjan, tiedostot poistetaan palvelimelta määrätyn viiveen kuluttua. Asiakirjan luoja voi valita viiveen (1 - 90 vuorokautta).

Asiakirjatiedostojen tunnistetiedot (tiedostojen nimet, koot ja tiivistearvot) tallennetaan palvelun tietokannassa pysyvästi, jolloin asiakirjan allekirjoituksen todentaminen jälkeenpäin on mahdollista, vaikka itse asiakirjatiedostoa ei ole palvelussa tallennettuna.

Palvelu voidaan integroida asiakkaan tietojärjestelmiin siten, että kaikki allekirjoitetut asiakirjat siirretään automaattisesti talteen asiakkaan dokumentinhallintajärjestelmään tai vastaavaan tietoarkistoon. Kaikki tiedostointegraatiot toteutetaan käyttäen salattuja tiedonsiirtoyhteyksiä. Mikäli asiakkaan kanssa on sovittu tiedostojen automattisesta siirrosta tietojärjestelmään, tiedostot poistetaan Signomin järjestelmästä vasta kun siirto on suoritettu onnistuneesti.

5 Palvelinympäristö

5.1 Minkä toimittajan konesalissa palvelu toimii?

Palvelun tuottamisessa käytämme seuraavia konesalipalveluntarjoajia:

Palvelintarjoajan nimi ja osoite	**Käytettävät palvelut**	**Palvelinkeskusten sijainti**	**Alihankkijat**
Cygate Oy Perkiöntie 2 00620 Helsinki	Konesalipalvelut	Suomi	Ei ole.
Google Cloud Google Ireland Limited Gordon House Barrow Street Dublin 4, Ireland	Virtuaalikone-, tallennus- ja tietokantapalvelut	Belgia, Suomi	https://cloud.google.com/terms/subprocessors
Amazon Web Services EMEA SARL 5 rue Plaetis L-2338 Luxembourg	Sähköpostiviestien ja SMS-viestien välitys	Irlanti	https://aws.amazon.com/compliance/third-party-access/

Kaikissa konesaleissa on kahdennetut palvelinlaitteet ja automaattinen valvonta seuraa palveluiden saatavuutta jatkuvasti. Konesaleissa on ympärivuorokautinen päivystys, elektroninen kulunvalvonta, kahdennettu jäähdytys, Internet-yhteys ja sähkönsyöttö.

Kaikki käytetyt palvelinkeskukset sijaitsevat EU-alueella.

Kaikkien konesalipalveluiden tietoturva on ISO 27001 -sertifioitu.

5.2 Miten tuotantoympäristön palvelimet on suojattu?

Palvelimille on tehty tietoturvavaatimusten mukainen konfigurointi (ns. kovennus) Signomin ohjeiden mukaisesti.

Tietoturvallinen konfigurointi sisältää seuraavat asiat:

- Tietoturvapäivitykset asennetaan automaattisesti päivittäin
- Kaikki ylimääräiset palvelut on poistettu ajosta
- Ylläpitäjien kirjautuminen palvelimelle tapahtuu käyttäen henkilökohtaisia 2048-bittisiä RSA-avainpareja
- Kaikki ylläpitäjien antamat komennot tallennetaan järjestelmälokiin

5.3 Miten palvelu on haittaohjelmasuojattu?

Kaikki palvelussa käsiteltävät PDF-tiedostot tarkistetaan ajantasaisen virustorjuntaohjelmiston avulla.

5.4 Miten ohjelmistojen haavoittuvuuksia tarkkaillaan ja hallitaan?

Kaikki palvelimet on asetettu asentamaan tietoturvapäivitykset automaattisesti päivittäin.

Signomin ylläpito seuraa jatkuvasti haavoittuvuustiedotteita. Kaikki käytössä olevat ohjelmistokomponentit on luetteloitu, jolloin on mahdollista nopeasti tunnistaa mitkä haavoittuvuudet vaikuttavat palvelun toimintaan.

Palvelua koskevan haavoittuvuuden löytyessä käynnistetään tietoturvapoikkeamaa koskeva prosessi ja ryhdytään välittömästi toimenpiteisiin.

5.5 Kerätäänkö palvelinten lokeja keskitetysti?

Kyllä, palvelinten käyttöjärjestelmän lokit ja sovelluslokit kerätään keskitetylle lokipalvelimelle. Lokit ovat saatavilla vaikka itse palvelimet eivät ole saatavilla.

Voimme toimittaa lokitietoja erillisestä pyynnöstä esim. tietoturvaloukkauksen tai väärinkäytöksen tutkimiseksi.

5.6 Onko asiakirjojen asiakkaan järjestelmään siirtämiseen käytetty yhteys salattu?

Asiakirjatiedostot siirretään asiakkaan tiedostopalvelimelle SFTP-protokollalla.

SFTP-yhteys salataan käyttäen asiakaskohtaista 2048-bittistä RSA-avainparia.

Ottaessa yhteyden asiakkaan palvelimeen, palvelimen identiteetti varmistetaan tarkastamalla että palvelimen julkinen RSA-avain vastaa ennalta tallennettua avainta.

6 Sähköpostit

6.1 Mihin sähköpostia käytetään palvelussa?

Allekirjoituspalvelun käyttäjille lähetetään ilmoitus uudesta asiakirjasta. Mikäli allekirjoitusta ei tehdä, lähetetään käyttäjille muistutusviesti. Käyttäjälle lähetetään myös ilmoitus, kun asiakirjan suhteen tehdään muita toimenpiteitä, esimerkiksi kun jokin muu osapuoli allekirjoittaa tai hylkää asiakirjan.

Sähköposti-ilmoitukset voidaan räätälöidä yrityskohtaisessa ratkaisussa halutun kaltaisiksi.

Sähköposti-ilmoitukset voidaan ottaa myös kokonaan pois käytöstä, mikäli asiakas näin haluaa.

6.2 Lähetetäänkö sähköpostit salattua yhteyttä pitkin?

Signomin sähköpostipalvelin välittää sähköpostit käyttäen TLS-salattua yhteyttä, mikäli vastaanottajan sähköpostipalvelin tukee TLS-salausta. Emme kuitenkaan voi tietää tukeeko vastaanottajan sähköpostipalvelin TLS-salausta, joten emme voi taata että kaikki viestit lähetetään salattua yhteyttä pitkin.

Sähköpostissa ei välitetä luottamuksellisia tietoja, vaan asiakirjat ovat saatavilla palvelusta vasta vahvan tunnistuksen jälkeen, ellei asiakaskohtaisesti ole muuta sovittu.

6.3 Miten käyttäjä voi suojautua huijausviesteiltä?

Signomin lähettämien sähköpostiviestien lähettäjä on varmistettu SPF- ja DKIM-tunnisteilla. Näiden tunnisteiden avulla vastaanottajan sähköpostipalvelin voi varmistua, että viestit tulevat Signomilta.

Mikäli tunnisteet, eivät täsmää, yleisimmät sähköpostiohjelmat näyttävät käyttäjälle varoituksen, että viestin lähettäjätiedot saattavat olla väärennetty.

Kaikki sähköpostipalvelut eivät kuitenkaan tarkasta viestien tunnisteita, joten on mahdollista että ulkopuolinen taho voi lähettää huijausviestin, jonka lähettäjän verkkotunnuksena on signom.com.

Tämän vuoksi on tärkeää, että käyttäjä varmistaa, että aina klikatessa sähköpostissa olevia linkkejä verkkotunnus, jossa asioidaan, alkaa www.signom.com.

7 WWW-käyttöliittymä

7.1 Tapahtuuko asiointi palvelussa käyttäen salattua yhteyttä?

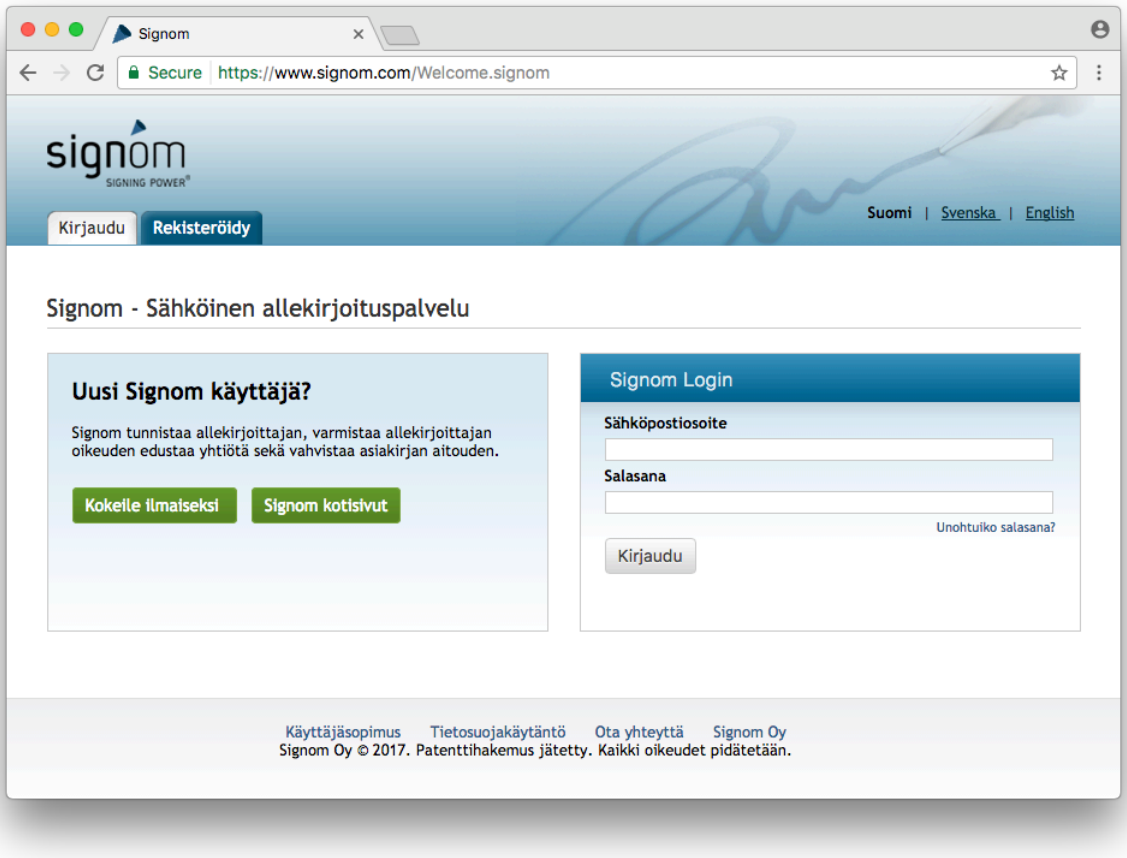
Palvelun käyttäminen tapahtuu TLS-tekniikalla salattua HTTPS-yhteyttä pitkin. Kaikki sivuilla oleva informaatio ja sopimustiedostot siirretään salattua yhteyttä käyttäen. Palvelua ei ole mahdollista käyttää ilman salausta.

Sivuston salaus perustuu 2048-bittisellä RSA-avaimella luotuun varmenteeseen. Varmenteen avulla selainohjelmisto varmistaa, että yhteys on muodostettu Signomin aitoon palvelimeen ja muodostaa salatun yhteyden. Selainohjelmisto ilmoittaa salatusta yhteydestä käyttäjälle näyttämällä lukko-kuvakkeen.

7.2 Miten käyttäjä voi suojautua huijaussivustoilta?

Ulkopuoliset tahot saattavat yrittää harhauttaa käyttäjää ja luoda huijaussivustoja (ns. phishing-sivustoja), jotka näyttävät Signomin sivustolta ja verkkotunnus on muistuttaa Signomin nimeä. Huijaussivustojen tarkoitus on kerätä käyttäjänimiä ja salasanoja mahdollista väärinkäyttöä varten. Huijaussivuja ei ole toistaiseksi havaittu, mutta niiden mahdollisuus on syytä pitää mielessä.

Huijaussivustolta suojautumiseksi on tärkeää, että palvelun käyttäjä varmistaa, että aina asioidessa Signom-palvelussa selaimessa näkyvä osoite alkaa verkkotunnuksella https://www.signom.com ja että selaimessa näkyy lukko-ikoni salatun yhteyden merkiksi. Kuva 1 seuraavalla sivulla näyttää esimerkin salatusta yhteydestä.



Kuva 1: Salattu yhteys www.signom.com -palveluun

8 Tunnistus

8.1 Miten palvelun käyttäjät tunnistetaan?

Lähtökohtaisesti kaikki allekirjoituspalvelun käyttäjille tehdään vahva sähköinen tunnistus, ellei asiakaskohtaisesti ole muuta sovittu.

8.2 Mitä tarkoittaa vahva sähköinen tunnistaminen?

Vahvan sähköisen tunnistamisen kriteerit on määritelty laissa vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista (617/2009).

Vahvan sähköisen tunnistamisen tulee käyttää vähintään kahta seuraavista kolmesta tekijästä:

1. Tietoon perustuvaa todentamistekijää (esim. asiakasnumero tai PIN-koodi, jonka vain käyttäjä tietää)
2. Hallussapitoon perustuvaa todentamistekijää, jonka käyttäjän on osoitettava olevan hallussaan (esim. tunnuslukulaite tai SIM-kortti)
3. Luontaista todentamistekijää, joka perustuu johonkin käyttäjän fyysiseen ominaisuuteen (esim. sormenjälki tai iiris)

Vahva sähköinen tunnistaminen sitoo henkilön vahvasti asiakirjaan. Todisteet tunnistustapahtumasta ovat saatavissa nopeasti ilman erillisiä kustannuksia.

Tunnistuspalvelun tarjoaminen on luvanvaraista toimintaa, ja toimintaa valvova viranomainen on Viestintävirasto.

8.3 Miksi palveluun täytyy rekisteröityä henkilökohtaisilla pankkitunnuksilla?

Vain vahvalla sähköisellä tunnistamisella (pankkitunnistus tai mobiilivarmenne) voidaan palvelua käyttävä henkilö tunnistaa luotettavasti.

Vahva sähköinen tunnistaminen on osa palvelun tietoturvaa, ja estää sen, ettei kukaan toinen voi rekisteröityä palveluun käyttäjän henkilötiedoilla ja näin päästä käsittelemään sopimuksia toisen henkilön nimissä.

8.4 Mitä tietoa palveluun välittyy tunnistuksen yhteydessä?

Vahvan sähköisen tunnistamisen (pankkitunnistus tai mobiilivarmenne) yhteydessä palveluun välittyy käyttäjän koko nimi ja henkilötunnus. Mikäli tunnistamiseen käytetään pankkitunnistusta, mitään käyttäjän pankkiasiakkuuteen liittyviä tietoja ei välity palveluun.

Tunnistuksen jälkeen palvelu hakee käyttäjän yritysroolit kaupparekisteristä.

8.5 Onko palvelua mahdollista käyttää ilman suomalaisia pankkitunnuksia?

Lähtökohtaisesti palvelun käyttö edellyttää suomalaista vahvaa sähköistä tunnistamista (pankkitunnistus tai mobiilivarmenne).

Asiakaskohtaisesti voidaan sallia myös Ruotsin ja Norjan sähköinen tunnistus.

Asiakaskohtaisesti voidaan myös sallia palvelun käyttö ilman vahvaa tunnistamista, mikäli asiakas on katsonut tämän aiheelliseksi.

8.6 Miten nimenkirjoitusoikeus tarkastetaan?

Vahvasti tunnistetun käyttäjän nimenkirjoitusoikeus tarkastetaan salatun yhteyden välityksellä Patentti- ja rekisterihallituksen ylläpitämästä kaupparekisteristä henkilötunnuksen perusteella.

Henkilön pääsy näkemään asiakirjatiedostoja voidaan rajoittaa vahvan tunnistuksen lisäksi siihen, että henkilöllä on yrityksen nimenkirjoitusoikeus yksin tai yhdessä toisen henkilön kanssa.

Signom tukee myös jaettua nimenkirjoitusoikeutta, jolloin tarvitaan useamman nimenkirjoitusoikeutetun allekirjoitus yrityksen edustamiseksi.

9 Henkilötietojen käsittely

9.1 Mitä tietoja palvelun käyttäjästä kerätään?

Palvelun käyttäjästä kerättävät tiedot on kuvattu tietosuojakäytännössä, johon pääsee sivun alareunassa olevan ”Tietosuojakäytäntö” linkin kautta.

9.2 Kuinka kauan tietoja säilytetään?

Henkilötietojen säilytysaika vaihtelee palvelukohtaisesti. Kerättävät tiedot ja niiden säilytysajat on kuvattu tietosuojakäytännössä, johon pääsee sivun alareunassa olevan ”Tietosuojakäytäntö”-linkin kautta.

9.3 Voiko poistaa itseäni koskevat tiedot?

Käyttäjällä on oikeus pyytää omien henkilötietojensa poistoa palvelusta. Poistopyynnön toteuttamiseksi pyydämme ottamaan yhteyttä asiakaspalveluun support@signom.com.

10 Allekirjoitus

10.1 Miten sähköisen allekirjoitus tarkalleen teknisesti muodostuu?

Allekirjoitus muodostuu seuraavasti:

1. Osapuolet tunnistetaan Signom vahvalla sähköisellä tunnistamisella ja tunnistamisesta tallennetaan lokitiedot.
2. Osapuolten allekirjoitusoikeus tarkistetaan kaupparekisteristä tai Signomin valtuusrekisteristä.
3. Järjestelmä laskee allekirjoitettavista tiedostoista SHA-256 ja SHA-512 tiivistekoodit. Tiivistekoodien avulla allekirjoitetut asiakirjat voidaan tunnistaa, vaikka itse asiakirjatiedostoja ei ole tallennettuna palveluun.
4. Palvelu luo käyttäjille sähköisesti leimatun PDF-dokumentin. Dokumentin allekirjoitussivulla on tiedot allekirjoittajista. Sähköisen leiman avulla PDF-tiedoston haltija voi varmistua siitä, että dokumentti on peräisin Signom-palvelusta eikä sen sisältöä ole muutettu.

10.2 Onko Signomin allekirjoitus kehittynyt sähköinen allekirjoitus?

Signomin allekirjoitus täyttää kehittyneen sähköisen allekirjoituksen kriteerit.

Kehittynyt sähköinen allekirjoitus on määritelty eIDAS-asetuksen (EU 910/2014) 26 artiklassa seuraavasti:

Kehittyneen sähköisen allekirjoituksen on täytettävä seuraavat vaatimukset:

a) se liittyy yksilöivästi allekirjoittajaansa;
b) sillä voidaan yksilöidä allekirjoittaja;
c) se on luotu käyttäen sähköisen allekirjoituksen luontitietoja, joita allekirjoittaja voi korkealla varmuustasolla käyttää yksinomaisessa valvonnassaan; ja
d) se on liitetty sillä allekirjoitettuun tietoon siten, että tiedon mahdollinen myöhempi muuttaminen voidaan havaita.

Lisäksi Viestintävirasto on ottanut kantaa kehittyneisiin sähköisiin allekirjoituksiin määräyksen 72/2016 sähköisistä tunnistus- ja luottamuspalveluista perusteluosassa.

Signomin allekirjoituspalvelu täyttää kehittyneen sähköisen allekirjoituksen vaatimukset seuraavasti:

a) Allekirjoittajat tunnistetaan vahvalla tunnistuksella ja siten asiakirja liittyy yksilöivästi allekirjoittajaan. Avaintietoja hallinnoidaan Signomin palvelussa.
b) Vaatimus allekirjoittajan yksilöinnistä on toteutettu vahvalla sähköisellä tunnistamisella.
c) Allekirjoituksen luontitietojen säilyminen allekirjoittajan yksinomaisessa valvonnassa on toteutettu vahvalla sähköisellä tunnistamisella.
d) Tiedon muuttumisen havaitseminen on toteutettu asiakirjoista laskettavalla tiivistekoodilla (ns. hash-koodi). Signom laskee kaikista asiakirjoista SHA-256 ja SHA-512 tiivistekoodit, jolloin asiakirjojen myöhempi muuttaminen voidaan havaita, vaikka itse asiakirjoja ei säilytetä pysyvästi palvelussa.

10.3 Miten sähköisen allekirjoituksen voidaan jälkeenpäin varmentaa?

Mikäli kaikki allekirjoittajat ovat allekirjoittaneet asiakirjan, allekirjoitukset voi helpoiten varmistaa PDF-dokumentin sähköisen leiman avulla. Kappaleessa 12.3 on esitetty, miten loppukäyttäjä voi varmistaa sähköisen leiman Adobe PDF Reader -ohjelmassa.

Mikäli vain osa allekirjoittajista on allekirjoittanut asiakirjan, allekirjoitetun asiakirjan aitouden voi varmistaa allekirjoituspalvelun ”Varmista aitous” -toiminnon avulla.

Mikäli asiakirjan allekirjoittaja kiistää allekirjoituksen, Signomilta voi pyytää vahvan tunnistuksen lokitiedot, joita voi käyttää todisteena allekirjoittajan liittämisessä allekirjoitettavaan asiakirjaan.

10.4 Onko sähköinen allekirjoitus yhtä pätevä kuin käsin tehty allekirjoitus?

Kyllä, Signomin sähköinen allekirjoitus on yhtä pätevä kuin käsin tehty perinteinen allekirjoitus.

Käsin allekirjoitetussa asiakirjassa kiistämättömyyden osoittamiseksi tarvitaan allekirjoitusten vertailua. Allekirjoituksen kiistämistilanteessa käsialatutkimus aiheuttaa viivettä ja kustannuksia, eikä tuloksena saada varmaa tietoa allekirjoittajasta. Korkeimmillaan käsialanäytteet voidaan olevan ”erittäin todennäköisesti” saman henkilön tekemiä.

Sen sijaan vahva sähköinen tunnistus sitoo allekirjoittajan vahvasti asiakirjaan, ja tekniset todisteet ovat helposti ja nopeasti saatavilla ilman lisäkustannuksia.

Näin ollen voidaan perustellusti väittää, että sähköisesti allekirjoitetun asiakirjan kiistämättömyys on jopa parempi kuin perinteisen käsin allekirjoitetun asiakirjan.

10.5 Voiko Signomin kautta allekirjoitettuja asiakirjoja käyttää viranomaisasioinnissa?

Kyllä, Signomin kautta allekirjoitettuja asiakirjoja voi käyttää myös viranomaisasioinnissa.

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) 5 § määrää perusperiaatteen, jonka mukaan *viranomaisen, jolla on tarvittavat tekniset, taloudelliset ja muut valmiudet, on tarjottava kaikille mahdollisuus lähettää viranomaiselle sähköinen viesti. Viranomaisen on pyrittävä käyttämään asiakkaan kannalta teknisesti mahdollisimman yhteensopivia ja helppokäyttöisiä laitteistoja ja ohjelmistoja.*

Lain 9 § mukaan sähköinen asiakirja täyttää kirjallisen muodon vaatimuksen.

Lisäksi eduskunnan oikeusasiamies on ratkaisussaan 3355/2006 ottanut kannan, että viranomaisella ei ole oikeutta säännönmukaisesti vaatia asiakirjoihin omakätistä allekirjoitusta.

11 Valtuudet

11.1 Mitä valtuus tarkoittaa?

Valtuus tarkoittaa yrityksen laillisen nimenkirjoittajan myöntämää asemavaltuutta. Valtuuksien käyttö parantaa allekirjoituksen oikeusvarmuutta, koska tällöin sopimuksen vastapuoli voi varmistua siitä, että asiakirjan allekirjoittaneella toimihenkilöllä on valtuus tehdä sopimus edustamansa yrityksen puolesta. Allekirjoittajan valtuuden kuvaus ja valtuuttajan nimi tulevat näkyviin allekirjoitussivulle. Valtuuksien avulla yritys voi varmistua, etteivät valtuutetut voi ylittää heille annettuja rajoituksia, koska valtuuteen liittyvät rajoitukset tulevat näkyviin allekirjoitussivulle.

Valtuuden myöntäjä voi valtuutta myöntäessään antaa henkilön käyttöön tietyn tehtävänimikkeen esim. ”Myyntiedustaja” tai halutessaan rajata tarkemmin valtuuden sisällön, esimerkiksi kirjoittamalla ”Myyntiedustaja, oikeus tehdä myyntisopimuksia 10 000 € asti Pohjoismaissa”.

11.2 Mitä tarkoittaa pääkäyttäjä?

Yrityksen nimenkirjoittaja voi halutessaan valtuuttaa pääkäyttäjän, joka myöntää varsinaiset valtuudet. Tällöin nimenkirjoittajan ei tarvitse itse myöntää jokaista valtuutta, vaan yksittäisten valtuuksien käsittely on delegoitu pääkäyttäjälle.

Jaetulla nimenkirjoittajalla ei ole oikeutta myöntää tai poistaa valtuutta yksin, sillä hän voi käyttää nimenkirjoitusoikeuttaan vain yhdessä muiden nimenkirjoittajien kanssa yhtiöjärjestyksen nimenkirjoituslausekkeen mukaisesti. Jaettujen nimenkirjoittajien on ensin valtuutettava pääkäyttäjä, joka myöntää yksittäiset valtuudet. Pääkäyttäjä voi olla yksi jaetun nimenkirjoitusoikeuden haltijoista.

11.3 Kenellä on oikeus myöntää ja poistaa valtuus?

Yrityksen kaupparekisteriin nimetyillä nimenkirjoittajilla ja valtuutetuilla pääkäyttäjillä on oikeus myöntää ja poistaa valtuuksia.

11.4 Miten valtuutettu työntekijä valitsee allekirjoittaako hän valtuutettuna vai henkilökohtaisesti?

Allekirjoituksen yhteydessä käyttäjälle näytetään selkeä valikko, josta käyttäjä voi valita, missä roolissa hän allekirjoittaa asiakirjan.

Yrityskohtaisessa ratkaisussa allekirjoittamista voi olla myös rajoitettu siten, että yrityksen valtuutettu henkilö ei voi kirjoittaa yrityksen asiakirjoja henkilökohtaisessa roolissa.

12 PDF-tiedostojen sähköinen leima

12.1 Mikä on sähköinen leima?

Sähköinen leima on PDF-tiedostoon lisätty digitaalinen allekirjoitus, jolla voidaan varmistaa PDF-tiedoston alkuperä.

Kaikki allekirjoitetut PDF-tiedostot on varustettu sähköisellä leimalla, jonka avulla voidaan varmistaa, että tiedosto on peräisin Signom allekirjoituspalvelusta eikä tiedoston sisältöä ole muutettu.

Leima perustuu Adobe Approved Trust List (AATL) -ohjelmaan. Adoben hyväksymä varmennepalvelujen tarjoaja (GlobalSign) on myöntänyt Signomille varmenteen asiakirjojen sähköistä leimaamista varten.

12.2 Kuinka luotettava sähköinen leima on?

Sähköinen leima on erittäin luotettava ja mahdoton väärentää.

Varmenteen myöntämisen yhteydessä varmennepalvelujen tarjoaja (GlobalSign) tunnistaa varmenteen saajan (Signom Oy) AATL-standardin vaatimusten mukaisesti. Ulkopuolinen taho ei siis voi hankkia Signom Oy:n nimissä olevaa varmennetta.

Leimaamisen yhteydessä Signomin palvelin laskee asiakirjasta SHA-256 tiivistekoodin ja lisää PDF-asiakirjaan varmenteesta lasketun sähköisen leiman. Mikäli PDF-asiakirjaa muokataan leimauksen jälkeen, sen tiivistekoodi muuttuu, jolloin leima ei enää ole voimassa.

Sähköisen leiman luomisen aikana asiakirjaa ei lähetetä Adobelle tai muulle ulkopuoliselle taholle.

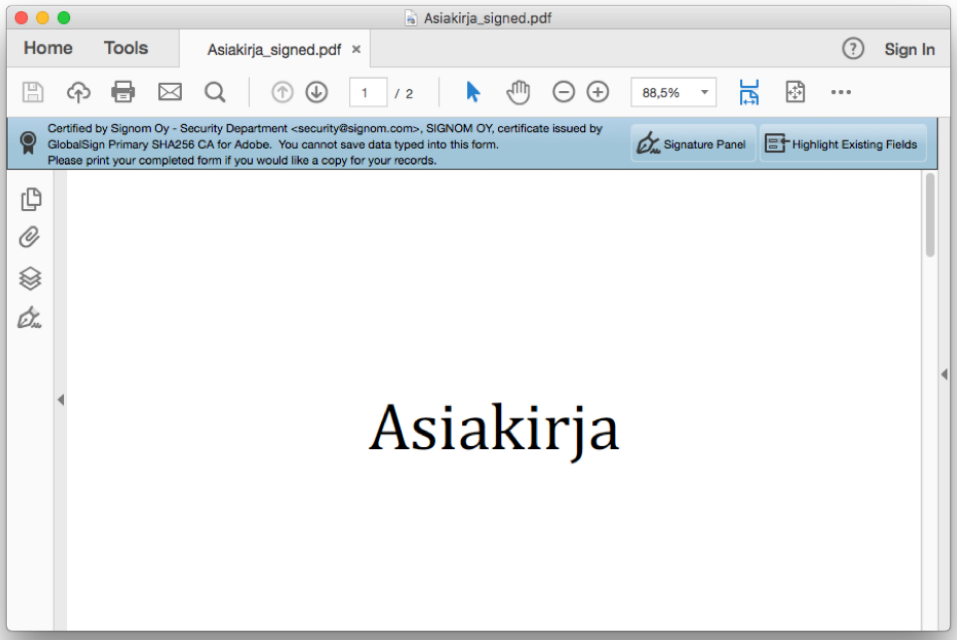
Mikäli Signomin hallussa oleva sähköisten leimojen luomiseen käytetty varmenne päätyisi tietomurron takia ulkopuolisen haltuun, se ilmoitetaan sulkulistalle, jonka jälkeen sillä tehdyt leimat eivät enää ole voimassa.

12.3 Miten loppukäyttäjä voi varmistaa leiman aitouden?

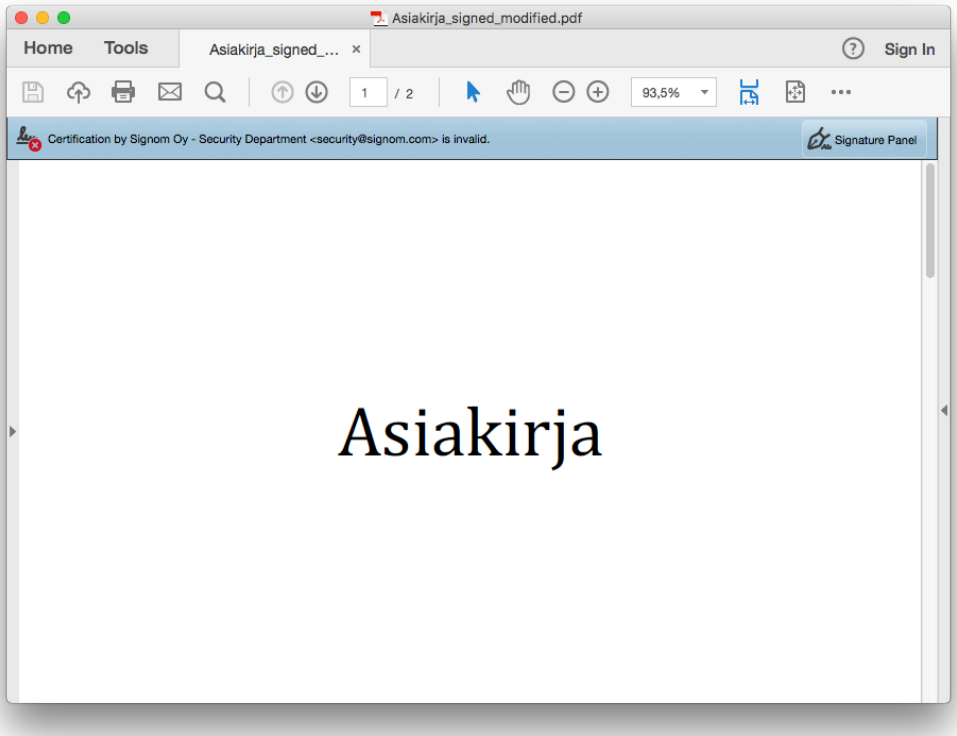
Kun loppukäyttäjä avaa leimatun PDF-tiedoston, Adobe Reader tarkistaa, että asiakirjassa oleva leima vastaa asiakirjan sisältöä. Lisäksi Adobe Reader tarkistaa, ettei leiman luomisessa käytetty varmenne ole sulkulistalla.

Kuvassa 2 seuraavalla sivulla näkyy esimerkki PDF-tiedostosta, jossa on sähköinen leima. Leiman tunnistaa sinisestä palkista, jossa varmenteen haltija on Signom Oy ja varmenteen myöntäjä on GlobalSign. Lisätietoja leimasta saa klikkaamalla ”Signature Panel” -painiketta.

Kuvassa 3 seuraavalla sivulla on esimerkki PDF-tiedostosta, jota on muokattu sähköisen leiman lisäämisen jälkeen. Sininen palkki ilmoittaa, että leima ei kelpaa.



Kuva 2: PDF-dokumentti, jossa on varmennettu sähköinen leima.



Kuva 3: PDF-dokumentti, jonka sähköinen leima ei ole voimassa.

12.4 Voiko sähköisesti leimatun PDF-asiakirjan tulostaa?

PDF-asiakirjan voi tulostaa, mutta sähköinen leima ei ole enää varmennettavissa paperille tulostusta PDF-tiedostosta.

Jotta allekirjoitus on varmennettavissa, käyttäjän täytyy aina säilyttää myös allekirjoitettu PDF-tiedosto, jossa on sähköinen leima.

12.5 Miten allekirjoitukset ovat varmistettavissa, jos Signom Oy:n toiminta loppuu?

Allekirjoituspalvelussa luotujen asiakirjojen aitous on varmennettavissa PDF-dokumentissa olevan sähköisen leiman avulla myös siinä tilanteessa, että Signomin toiminta loppuu. Sähköisen leiman varmentamisessa ei tarvita yhteyttä Signomin palvelimiin.