VAHTI

Ohje Luonnos 16.1.2017

LUONNOS

VAHTI 3/2017

Sähköisen asioinnin tietoturvallisuus -ohje

VALTIOVARAINMINISTERIÖ

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

SISÄLLYSLUETTEO

1 Johdanto

Tämä ohje käsittelee kansalaisille, yrityksille ja viranomaisille tarjottavien sähköisten asiointipalveluiden tietoturvallisuutta.

1.1 Ohjeistuksen tausta

Julkisen hallinnon palveluiden sähköistäminen on yksi Sipilän hallituksen kärkihankkeista. Tavoitteena on rakentaa julkisen hallinnon palvelut käyttäjälähtöisiksi ja ensisijaisesti digitaalisiksi toimintatapoja uudistamalla. Internetissä tapahtuvan sähköisen asiakaspalvelun merkitys korostuu, ja sähköinen asiointi tulee olemaan monilla hallinnonaloilla viranomaisten pääasiallinen palvelukanava kansalaisten, yritysten ja viranomaisten suuntaan.

Digitalisaatio tehostaa merkittävästi julkisen hallinnon palveluita kansalaisille ja yrityksille, sekä parantaa julkishallinnon ICT-toimintojen yhteentoimivuutta ja kustannustehokkuutta kokonaisuutena. Asiointipalveluiden sähköistäminen tulee kuitenkin toteuttaa siten, että palvelut ovat tietoturvallisia ja edistävät kansalaisten ja yritysten luottamusta julkishallinnon toimintaan myös sähköisissä verkkoympäristöissä.

Toimintatapojen uudistamiseen liittyy tietoturvallisuuden näkökulmasta keskeisiä haasteita:

- **Yhden luukun palvelumalli**
  - Käyttäjälähtöinen asiointipalvelu tulee pyrkiä rakentamaan siten, että asiakkaan tarvitsee asioida suoraan vain yhden viranomaisen kanssa ja luovuttaa itseään koskevia perustietoja viranomaisille vain kerran. Viranomaisilla tulee siksi olla käytössään välineet ja tukipalvelut, jotka mahdollistavat tietojen jakamisen hallitusti, tehokkaasti ja tietoturvallisesti poikkihallinnollisissa asiointiprosesseissa.
- **Internet-verkon uhkatekijät**
  - Ei-julkisen tietoaineiston sähköinen käsittely edellyttää asiointipalveluiden omistajilta kykyä seurata internetin alati muuttuvaa uhkaympäristöä ja suojautua palvelun kannalta olennaisilta uhkatekijöiltä. Poikkihallinnallinen asiointi edellyttää kaikilta tietojen käsittelyyn osallistuvilta toimijoilta yhdenmukaista tietoturvallisuuden tasoa.
- **Kustannustehokkuus**
  - Asiointipalveluiden tietoturvallisuus rakentuu suurelta osin vakioiduista toiminnallisuuksista, esimerkkinä käyttäjien sähköinen tunnistaminen. Keskitetyt, uudelleenkäytettävät sähköisen asioinnin tukipalvelut ovat tärkeässä roolissa sähköisten asiointipalveluiden suunnittelussa, toteuttamisessa ja ylläpidossa, sillä ne nopeuttavat palveluprosessien sähköistämistä ja madaltavat yksittäisten sähköisten asiointipalveluiden perustamis-, kehittämis- ja ylläpitokustannuksia.

Tämä ohje määrittää yleisiä periaatteita ja tarjoaa konkreettisia ohjeita kaikille julkisen hallinnon sähköisten asiointipalveluiden hankintaan, suunnitteluun, toteuttamiseen, kehittämiseen ja ylläpitoon osallistuville päätöksentekijöille ja asiantuntijoille sähköisten asiointipalveluiden tietoturvallisuuden varmistamiseksi.

Ohje korvaa valtiovarainministeriön vuonna 2001 antaman Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohjeen (VAHTI 4/2001) sekä vuonna 2006 antaman ohjeen Tunnistaminen julkishallinnon verkkopalveluissa (VAHTI 12/2006). Ohjeen sisältöä on täydennetty ja ajanmukaistettu sekä sen rakennetta on selkeytetty. Uutta sisältöä ohjeessa ovat sähköisten asiointipalveluiden tietoturvaperiaatteet ja viitearkkitehtuuri, kansallisten sähköisen asioinnin tukipalveluiden kuvaukset sekä liitteen 6 case-esimerkit.

1.2 Ohjeen tavoite

Asiointipalveluiden suunnittelijoilla, toteuttajilla, kehittäjillä ja ylläpitäjillä on suuri vastuu huolehtia siitä, että palvelun saatavuutta sekä tietojen eheyttä ja asioinnin luottamuksellisuutta turvaavat ratkaisut ovat linjassa palvelun tietosisällön ja käyttötarkoituksen sekä niistä johdettujen tietoturva-, saatavuus- ja jatkuvuusvaatimusten kanssa käyttötarkoitukseen tunnistetut riskit huomioiden. Tämä ohje on laadittu tukemaan palveluiden suunnittelua, toteuttamista ja kehittämistä, ja sen keskeisenä tavoitteena on:

- tarjota yhteenveto sähköisen asioinnin tietoturvallisuutta säätelevistä laeista ja viitekehyksistä
- auttaa muodostamaan kokonaisnäkemys sähköisen asioinnin keskeisistä tietoturvauhista
- tarjota käytännön ohjeita sähköisen asiointipalvelun tietoturvallisista rakenneratkaisuista ja toimintamalleista, ja havainnollistaa niitä sähköisen asioinnin viitearkkitehtuurin ja julkishallinnon konkreettisten case-esimerkkien kautta
- tarjota perustiedot julkisen hallinnon sähköisen asioinnin tukipalveluista ja niiden tarjoamista hyödyistä tietoturvallisuuden varmistamisessa erityisesti seuraavilta osin: tukipalveluiden standardinmukainen tietoturvallisuus ja laatu sekä asiointipalveluiden yhteentoimivuus.

Ohje kokoaa sähköisiä asiointipalveluita tarjoaville tahoille velvoittavat vaatimukset sekä tarjoaa suositusluonteisia ohjeita ja hyviä käytäntöjä.

Ohjeessa on huomioitu sen sovellettavuus julkishallinnon eri viranomaisten toimintaympäristöihin ja sovellusarkkitehtuureihin yleisellä tasolla. Ohje kattaa tietoturvallisen sähköisen asiointipalvelun keskeiset kontrollitavoitteet, jotka on kuitenkin mahdollista saavuttaa vaihtoehtoisin, kussakin toimintaympäristössä tarkoituksenmukaisin hallinnollisin ja teknisin ratkaisuin.

Ohjeessa on pyritty keskittymään sähköiselle asioinnille tunnusomaisiin tietoturvahaasteisiin. Niillä tietoturvallisuuden osa-alueilla, jotka ovat yleispäteviä kaiken tyyppisiin tietojärjestelmiin, viitataan muuhun VAHTI-ohjeistoon.

Ohjeessa käsitellään teknologisten ratkaisujen yksityiskohtia vain siinä laajuudessa kuin se on ohjeen ymmärrettävyyden ja sovellettavuuden kannalta tarpeen. Tällä on pyritty vähentämään ohjeen tiheää päivitystarvetta.

1.3 Ohjeen kohderyhmä

Ohje on tarkoitettu julkishallinnon organisaatioissa kaikille päätöksentekijöille ja asiantuntijoille, joiden työtehtäviin kansalaisille, yrityksille ja viranomaisille suunnattujen sähköisten asiointipalveluiden järjestäminen, suunnittelu, toteuttaminen, kehittäminen ja ylläpito kuuluvat, erityisesti:

1. ICT-arkkitehdit
2. sovelluskehittäjät
3. ohjelmistojen, ICT-palveluiden ja laitteiden hankinnasta vastaavat asiantuntijat
4. käyttöpalveluiden ja järjestelmien operatiivisesta palvelutuotannosta vastaavat asiantuntijat
5. tietoturva- ja tietosuoja-asiantuntijat
6. sekä muut tietohallinnon asiantuntijat ja päättäjät.

Ohje soveltuu sekä valtionhallinnon että kuntien sähköisten asiointipalveluiden suunnittelun ja toteuttamisen tueksi. Myös yritykset voivat hyödyntää ohjetta sähköisten palveluidensa kehittämisessä, sillä mm. osa kansallisen palveluarkkitehtuurin tuottamista tukipalveluista on myös yritysten käytettävissä.

1.4 Ohjeen rakenne

Tämä ohje on jaettu kahdeksaan lukuun ja kuuteen liitteeseen. Lukujen keskeinen sisältö on seuraava:

- Johdanto; kuvaa ohjeen taustan ja sen keskeiset tavoitteet.
  - Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset; kuvaa viranomaisten sähköistä asiointia säätelevän keskeisen lainsäädännön, EU-laajuiset asetukset sekä muut suositeltavat viitekehykset.
- Sähköiset asiointipalvelut; sisältää sähköisen asiointipalvelun määritelmän, rajaukset ja suuntaa-antavan luokittelun tavalla, joka palvelee ohjeen myöhemmissä kappaleissa annettavaa ohjeistusta.
- Sähköisen asiointipalvelun tietoturvaperiaatteet; kuvaa joukon yleisiä periaatteita, joita noudattamalla voidaan suojata palvelua väärinkäytöksiltä ja rajata toteutuneiden väärinkäytösten haittavaikutuksia palvelun koko elinkaaren ajan.
- Sähköisen asiointipalvelun viitearkkitehtuuri; kuvaa pääosin teknisestä näkökulmasta sähköisen asiointipalvelun kontrolliympäristön ja tarjoaa hyviä käytäntöjä kontrollitavoitteiden toteuttamiseksi. Viitearkkitehtuuri viittaa laajalti luvussa 6 kuvattuihin sähköisen asioinnin kansallisiin tukipalveluihin.
- Käyttäjien tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa; kuvaa sähköisen tunnistusmenetelmän varmuustasot sekä päätöksentekoprosessin, jota noudattaen palvelun omistaja määrittelee palvelun käytön edellyttämän varmuustason.
  - Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely; kuvaa sähköisen allekirjoituksen keskeiset käyttötapaukset sähköisessä asioinnissa ja sisältää toteutusohjeita sähköisen allekirjoituksen tai muun tiedon alkuperän ja eheyden varmistamisen mahdollistamiseksi.
- Sähköisen asioinnin kansalliset tukipalvelut; kuvaa hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain mukaiset keskeiset tukipalvelut, joita julkishallinnon tulee ensisijaisesti hyödyntää sähköisen asioinnin verkkopalveluidensa suunnittelussa ja toteuttamisessa.

Liite 1 sisältää ohjeessa käytetyn keskeisen sanaston.

Liite 2 sisältää kaupallisten tukipalveluiden tietoturvallisuuden tarkastuslistan.

Liite 3 sisältää sähköisen asiointipalvelun tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

Liite 4 sisältää tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslistan.

Liite 5 sisältää yhteenvedon sähköisen tunnistamisen menetelmien varmuustasoista.

Liite 6 sisältää valikoituja case-esimerkkejä hyvistä tietoturvallisuuden käytännöistä julkishallinnon sähköisiin asiointipalveluihin liittyen.

2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003, 534/2016)

Laki sähköisestä asioinnista viranomaistoiminnassa säätää viranomaisten velvollisuudesta tarjota sähköistä asiointipalvelua teknisten ja taloudellisten valmiuksiensa rajoissa. Laissa säädetään erityisesti viranomaisen velvollisuudesta:

- tarjota kansalaisille mahdollisuus lähettää sähköisesti viesti asian vireille saattamiseksi tai käsittelemiseksi sekä varmistaa tiedonvaihdon tietoturvallisuus
- varmistaa viestin tai asiakirjan alkuperä – tarvittaessa sähköisellä allekirjoituksella, jos viestin tai asiakirjan alkuperäisyyttä tai eheyttä on syytä epäillä
- allekirjoittaa viranomaisen laatima päätösasiakirja kehittyneellä sähköisellä allekirjoituksella tai *muuten sellaisella tavalla, että asiakirjan alkuperäisyydestä ja eheydestä voidaan varmistua*
- varmistaa valtakirjalla viestin lähettäneen asiamiehen toimivalta, jos viranomaisella on aihetta epäillä asiamiehen toimivaltaa tai sen laajuutta
- huolehtia asiakkaan informoimisesta, tunnistamisesta ja toimituksen todisteellisuudesta silloin, kun asiakirja toimitetaan asiakkaan suostumuksella tiedoksi sähköisenä viestinä

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (7.8.2009/617, 533/2016) ja eIDAS-asetus

Euroopan parlamentin ja neuvoston asetuksessa N:o 910/2014 (eIDAS-asetus) säädetään jäsenvaltioiden rajat ylittävästä sähköisestä tunnistamisesta, tunnistamisen varmuustasoista sekä luottamuspalveluista. Asetuksen voimaantulo on huomioitu kesällä 2016 uudistetussa kansallisessa laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (533/2016). Uudistettu laki:

- mahdollistaa luottamusverkostoon perustuvan tunnistamisen mallin, jossa tunnistus- ja luottamuspalveluita on mahdollista käyttää keskitetyn tunnistamisen välityspalvelun kautta.
- määrittelee viittauksin eIDAS-asetukseen ja sen varmuustasoihin sen, mitä Suomessa pidetään vahvana sähköisenä tunnistamisena
- velvoittaa tunnistusvälineen tarjoajan ja luottamuspalvelua tarjoavan varmentajan hankkimaan ja päivittämään luonnollisten henkilöiden tarvittavat tiedot väestötietojärjestelmästä ja oikeushenkilöiden tiedot yritys- ja yhteisörekisteristä
- antaa määräyksiä tunnistus- ja luottamuspalvelujen vaatimustenmukaisuuden arvioinnista.

Syyskuusta 2018 alkaen eIDAS-asetus velvoittaa EU-alueen julkisen sektorin organisaatiot huomioimaan myös toisesta jäsenvaltiosta EU-notifioidulla tunnistusvälineellä saapuvat käyttäjät.

Henkilötietolainsäädäntö ja EU:n yleinen tietosuoja-asetus

Suomen henkilötietolainsäädäntö ja Euroopan Unionin uudistettu yleinen tietosuoja-asetus säätelevät henkilötietojen käsittelyä pyrkien suojaamaan kansalaisten yksityisyyden suojaa. Koska sähköiset asiointipalvelut muodostavat useimmissa tapauksissa henkilötietorekisterin, henkilötietolaki ja EU:n yleinen tietosuoja-asetus velvoittavat myös sähköisen asiointipalveluiden omistajia. Henkilötietolaki säätää tietojen käsittelystä erityisesti seuraavaa:

- Käsiteltävien henkilötietojen tulee olla rekisterinpitäjän toiminnan kannalta tarpeellisia ja tarkoituksen mukaisia (HetiL 6§)
- Rekisterinpitäjä ei saa käyttää tai luovuttaa henkilötietoja tarkoituksiin, jotka eivät ole yhteensopivia tietojen alkuperäisen tarkoituksen kanssa (HetiL 8§)
- Arkaluonteisten henkilötietojen kuten rekisteröidyn etnistä alkuperää tai terveydentilaa kuvaavien tietojen käsittely on kielletty (HetiL 11§) laissa erikseen määritellyin poikkeuksin (HetiL 11§)

EU:n yleinen tietosuoja-asetus velvoittaa lisäksi rekisterinpitäjiä seuraavasti:

- Henkilötietojen sähköiseen käsittelyyn on saatava henkilön suostumus, ellei rekisterinpitäjä ole viranomainen, jolla on lakisääteisen tehtävänsä perusteella oikeus henkilötietojen käsittelyyn
- Rekisterinpitäjän tulee informoida henkilöitä, joiden tietojen luottamuksellisuus on vaarantunut
- Tietojen automaattiseen käsittelyyn perustuva päätöksenteko (profilointi) ilman luonnollisen henkilön osallistumista ei ole pääsääntöisesti sallittua
- Henkilötietojen siirtäminen EU-maiden ulkopuolelle on kielletty
- Henkilöillä on oikeus vaatia tietoa omien tietojensa käsittelystä sekä niiden oikaisua, sekä tietojen poistamista silloin, kun viranomaisella ei ole lain suomaa oikeutta tai velvoitetta säilyttää tietoja

EU-tietosuojan kokonaisuudistus -raportti (VAHTI 1/2016) tarjoaa lisätietoa ja toimenpidesuosituksia EU:n yleiseen tietosuoja-asetukseen liittyen.

Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (29.6.2016/571)

Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (Kapa-laki) sisältää säädöksiä sähköisen asioinnin tukipalveluiden (mm. Suomi.fi-palvelut) tuottamisesta sekä organisaatioiden velvollisuudesta tai oikeudesta käyttää niitä sähköisessä asioinnissa. Laissa säädetään erityisesti seuraavaa:

- Tukipalveluiden tuottajat ja niiden vastuut palveluidensa laadusta, kustannustehokkuudesta, suorituskyvystä, käytettävyydestä, esteettömyydestä, tietoturvallisuudesta ja häiriöttömistä muutoksista
- Valtion hallintoviranomaisten, virastojen, laitosten, liikelaitosten, tuomioistuinten ja muiden laink äyttöelimien sekä kunnallisten viranomaisten velvollisuudesta käyttää asioinnin tukipalveluita. Kunnallisilla viranomaisilla velvoite on rajattu laissa säädettyihin tehtäviin.
- Muiden julkishallinnon organisaatioiden ja yksityisten oikeudesta käyttää tukipalveluita
- Tukipalveluiden käyttöönottoon liittyvät siirtymäajat.

Suomi.fi-tukipalveluiden käytön velvoitteita ja oikeuksia sekä niiden käyttöönottoa on käsitelty palvelukohtaisesti tämän ohjeen luvussa 8.

3 Sähköiset asiointipalvelut

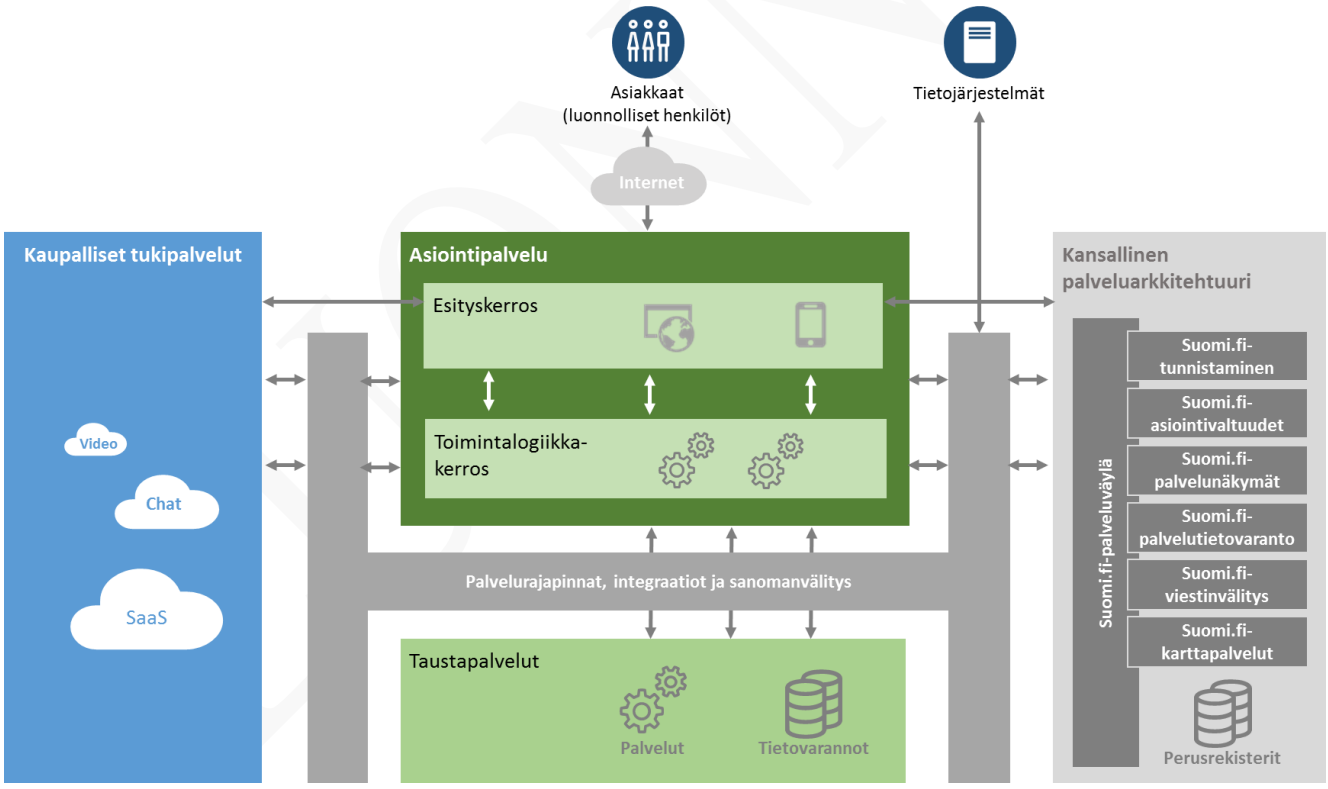
3.1 Sähköisen asiointipalvelun määritelmä ja rajaus

Sähköisellä asiointipalvelulla tarkoitetaan tässä ohjeessa verkkopalvelua, jossa asiakkaat voivat asioida viranomaisen kanssa tietoverkon avulla. Esimerkkejä sähköisistä asiointipalveluista ovat erilaiset tieto- ja tiedottamispalvelut, palautteenantopalvelut, asiakkaiden osallistamiseen tähtäävät palvelut, viranomaisen ja asiakkaan välisen vuorovaikutteisen asioinnin mahdollistavat palvelut sekä lakisääteisten ilmoitusten lähettämisen ja vastaanottamisen mahdollistavat palvelut.

Asiakkaalla tarkoitetaan sähköistä asiointipalvelua käyttävää luonnollista henkilöä tai tietojärjestelmää. Palvelun asiakkaita voivat siten olla:

- *kansalaiset*, jotka asioivat yksityishenkilöinä itsensä tai edustamansa henkilön puolesta
- *yritysten edustajat*, jotka yritys on valtuuttanut asioimaan puolestaan
- *viranomaiset*, jotka asioivat palvelussa suorittaessaan viranomaistehtävää tai edustavat toista viranomaistahoa (palvelun omistava viranomainen tai toinen viranomainen)
- *tietojärjestelmät*, jotka käyttävät sähköistä asiointipalvelua teknisen palvelurajapinnan kautta

Kuva 1. havainnollistaa sähköisen asiointipalvelun yleistä rakennetta suhteessa palvelun asiakkaisiin, palvelua tarjoavan organisaation tietojärjestelmiin ja -varantoihin, ulkoisiin sähköisen asioinnin tukipalveluihin ja sekä muihin tietojärjestelmiin.



Kuva 1 Sähköisen asiointipalvelun yleinen rakenne

Sähköinen asiointipalvelu rakentuu tyypillisesti seuraavista kerroksista ja elementeistä:

- *Esityskerros* toteuttaa asiakkaille suunnatut *verkkoselaimella käytettävät sovellukset* ja päätelaitteille asennettavat *natiivisovellukset* (esimerkiksi sovelluskaupasta ladattavat mobiilisovellukset tai perinteiset *client-server* -sovellukset). Toteutustavasta riippuen esityskerros voi sisältää myös asiointiprosessin toimintalogiikkaa.

– *Toimintalogiikkakerros* kattaa sähköisen asiointipalvelun sisäiset tietovarannot ja tuotepohjaiset tai räätälöidyt palvelinsovellukset, jotka toteuttavat sähköiseen asiointiprosessiin liittyvää toimintalogiikkaa.

Sähköinen asiointipalvelu tukeutuu useimmissa tapauksissa seuraaviin ulkoisiin palveluihin:

– *Taustapalvelut* kattavat sähköistä asiointipalvelua tarjoavan organisaation asiointipalveluprosessia tukevat yhteiskäyttöiset järjestelmäpalvelut ja tietovarannot.
– Sähköinen asiointipalvelu integroituu taustapalveluihin sekä ulkoisiin sähköisen asioinnin tukipalveluihin ja kansallisiin perusrekistereihin tyypillisesti *palvelurajapintojen* sekä *integraatio- ja sanomavälityspalveluiden* välityksellä. Sähköinen asiointipalvelu voi tarjota palvelurajapintoja myös organisaation ulkopuolisille tietojärjestelmille, esimerkiksi avoimen datan julkaisemiseksi tai muiden viranomaisten sähköisten asiointipalveluiden käyttöön poikkihallinnollisessa asioinnissa.
– *Kansallinen palveluarkkitehtuuri* kattaa kansalliset, keskitetysti toteutetut julkishallinnon sähköisen asioinnin tukipalvelut.
– *Kaupalliset tukipalvelut* kattavat laajan kirjon sähköistä asiointia tukevia palveluita, esimerkiksi viranomaisen ja asiakkaan välistä suoraa vuorovaikutusta mahdollisesti tukevat viestintäratkaisut tai palvelun käytön seurantaa tukevat analytiikkapalvelut.

Edellä esitetty rajaus sähköisen asiointipalvelun ja muiden järjestelmien välillä on suuntaa antava yksinkertaistus, joka kuitenkin palvelee tämän ohjeen käyttötarkoitusta.

Integraatio- ja sanomavälitysratkaisujen teknisiä ratkaisuvaihtoehtoja ja tietoturvallisuutta käsitellään tässä ohjeessa rajatusti, sillä mainitut ratkaisut toteutetaan usein yleiskäyttöisinä. Palvelun suunnittelussa tulee kuitenkin varmistua siitä, että käytettävät ratkaisut:

– toteuttavat riittävän vahvan tieto- ja sanomaliikenteen salauksen,
– toteuttavat tarvittaessa sanomatasoisen sähköisen allekirjoituksen, jolla voidaan varmistua tietojen alkuperästä ja eheydestä myös silloin, kun sanoma välitetään useamman pisteen kautta,
– toteuttavat järjestelmien välisen luotettavan tunnistamisen,
– mahdollistavat tietoliikenteen seurantatietojen tallentamisen tietoturvaloukkausten tai vika- ja häiriötilanteiden selvittämiseksi, ja
– eristävät sähköisen asiointipalvelun viranomaisen taustapalveluista ja palvelin- ja työasemaympäristöstä niin, että sähköisen asiointipalvelun kautta välittyvien uhkien torjunta on suunniteltu ja toteutettu, ja mahdolliset jäännösriskit on hallittu.

Sähköiseen asiointipalveluun liitettävien taustapalveluiden ja tietovarantojen tietoturvallisuudesta vastaa ja niiden tietoturvallista käyttöä ja hyödyntämistä ohjeistaa lähtökohtaisesti kyseisen palvelun omistaja. Näiden palveluiden tietoturvallisuus on rajattu tämän ohjeen ulkopuolelle.

3.2 Sähköisen asioinnin uhkaympäristö

Julkisen hallinnon asiointipalveluiden sähköistäminen ja niiden verkottuminen lisäävät palveluiden omistajien vastuuta palveluidensa laadusta ja tietoturvallisuudesta erityisesti seuraavista syistä:

1. Sähköinen asiointipalvelu on väistämättä alttiina internetin kautta välittyville uhkatekijöille joko suoraan tai välillisesti. Palveluun tai käyttäjän käyttämään päätelaitteeseen voi kohdistua opportunistisia tai kohdennettuja hyökkäyksiä ja väärinkäyttöyrityksiä, joiden motiivit vaihtelevat luottamuksellisen tiedon urkkimisesta viranomaisen toiminnan tahalliseen häirintään tai muuhun väärinkäyttöön.

2. Toisen osapuolen omistamien tietojen hyödyntäminen sähköisessä asiointipalvelussa edellyttää palvelun omistajalta kykyä suojata tietojen luottamuksellisuutta tiedon omistajan edellyttämällä tasolla
3. Yhteiskäyttöisten hallinnon tukipalvelujen ja tietovarantojen laajamittainen hyödyntäminen asettaa aiempaa korkeammat vaatimukset tietojen laadulle ja eheydelle sekä sähköisen asioinnin tukipalveluiden saatavuudelle
4. Sähköisten asiointipalveluiden verkottuminen edellyttää niiltä vikasietoisuutta, minkä lisäksi palvelun omistajalla ja sen käyttäjillä tulee olla selkeät yhteistoimintamenettelyt häiriöiden ja tietoturvapoikkeamien hallinnalle. Palveluiden käyttäjien tulee lisäksi ymmärtää palveluiden mahdollisista häiriöistä ja poikkeamatilanteista omaan toimintaansa aiheutuvat jatkuvuusriskit, ja toisaalta välttää itse käyttämiensä asiointipalveluiden tarpeetonta kuormittamista
5. Toiminta digitalisoituvassa toimintaympäristössä edellyttää käyttäjien säännöllistä ohjeistusta ja koulutusta.

Sähköisen asiointipalvelun keskeiset uhkatilanteet kohdistuvat palvelun ja siinä käsiteltävien tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen:

1. **Tietomurto**
    - Hyökkääjä murtautuu tai hankkii muuten pääsyn sähköiseen asiointipalveluun päästäkseen valtuudetta käsiksi ei-julkisiin tietoihin. Murtautumisen motiivina voi olla pyrkimys saavuttaa taloudellista hyötyä esimerkiksi arkaluonteisia henkilötietoja myymällä tai sillä uhkaamalla (ks. myös Kiristäminen).
2. **Tietovuoto**
    - Ei-julkisia tietoja päätyy suunnittelemattomasti sähköisen asiointipalvelun ulkopuolelle ja niitä käytetään käyttötarkoituksen vastaisesti esimerkiksi mainonnan kohdentamiseen. Tietovuodon riski ja tarvittavat riskienhallintatoimet tulee huomioida etenkin ulkoisten tukipalveluiden yhteydessä.
3. **Palvelunesto**
    - Hyökkääjä häiritsee tai estää kokonaan sähköisen asiointipalvelun normaalin käytön haitatakseen viranomaisen normaalia toimintaa tai tahratakseen viranomaisen mainetta.
4. **Kiristäminen**
    - Hyökkääjä uhkaa sähköisen asiointipalvelun omistajaa tai tuottajaa palvelunestolla, kiristyshaittaohjelmalla[1], tietomurrolla tai muulla laajamittaisella vahingonteolla, ja vaatii palvelun omistajalta tai tuottajalta lunnaita, jotka maksamalla hyökkäykseltä ilmoitetaan voivan välttyä.
5. **Tietojen valtuudeton muokkaaminen**
    - Hyökkääjä, tai palvelun yksittäinen valtuutettu käyttäjä, muuttaa sähköisen asiointipalvelun haavoittuvuutta hyödyntämällä sen sisältämiä tietoja. Motiivina voi olla esimerkiksi taloudellinen hyötyminen (ks. Oman edun tavoittelu) tai viranomaisen maineen tahraaminen.
6. **Oman edun tavoittelu**
    - Yksittäinen käyttäjä tavoittelee henkilökohtaista, yleensä taloudellista, hyötyä esimerkiksi ohjaamalla sähköisessä asiointipalvelussa tai sen kautta etuuksia väärälle vastaanottajalle muokkaamalla valtuudetta maksuyhteistietoja tai vaikuttamalla väärillä tiedoilla viranomaisten päätöksiin.

[1] Kiristyshaittaohjelma aiheuttaa paikallisen palvelunestotilan salaamalla tiedot käyttökelvottomiksi salausavaimella, joka on ainoastaan hyökkääjän tiedossa. Tyypillisessä tapauksessa hyökkääjä lupaa purkaa salauksen maksua vastaan.

Vaikka tässä ohjeessa keskitytään sähköisen asiointipalvelun tietoturvallisuuteen, palvelun suunnittelun lähtökohtana tulee olla palvelua tarjoavan organisaation ydintoimintojen riskit sekä palvelusta ja sen toimintaympäristöstä tunnistetut uhkatekijät kokonaisuutena. Hyökkääjien motiiveja ja päämääriä määrittävät ennen kaikkea organisaation toiminnan luonne, julkisuuskuva ja sen käsittelemät tiedot.

Yksittäinen sähköinen asiointipalvelu voi valikoitua hyökkäyksen kohteeksi siksi, että se haavoittuvana tarjoaa helpon väylän murtautua palvelun omistajan tai palveluun kytkettyihin tietoverkkoihin ja toteuttaa tietomurto tai palvelunestohyökkäys johonkin kriittisempään kohteeseen. Siksi sähköisen asiointipalvelun tulee olla niin hyvin suojattu ja eriytetty viranomaisen muusta tietoteknisestä ympäristöstä, että sen hyödyntäminen laajemmassa vahingoittamistarkoituksessa olisi mahdollisimman hankalaa.

Luku 4 kuvaa keskeiset periaatteet, joita noudattamalla sähköistä asiointipalvelua voidaan suojata tehokkaasti yleisimmiltä uhkatekijöiltä. Keskiössä on palvelun suunnittelijoiden, ylläpitäjien, kehittäjien ja käyttäjien tietoturvatietoisuus.

3.3 Asiointipalvelun riskiperusteinen suojaaminen

Sähköisen asiointipalvelun omistajan tulee tunnistaa, mitkä tekijät ovat palvelun tietoturvallisuuden kannalta keskeisiä, esimerkiksi asiakastiedon luottamuksellisuus tai asiakkaan välittämien tietojen eheys. Palvelun suojaustoimenpiteet tulee pyrkiä suhteuttamaan määrämuotoisen riskienarviointimenettelyn kautta siten, että ne ovat palvelun uhkatekijät huomioiden riittävät mutta eivät ylimitoitetut. Riskienarvioinnissa voidaan käyttää esimerkiksi VAHTI 1/2017 Ohje riskienhallintaan kuvattua prosessia ja mallia.

Sähköisen asiointipalveluiden tarkoituksenmukaista suojausta arvioidessaan palvelun omistaja voi käyttää apuna esimerkiksi seuraavia kysymyksiä:

- Käsitelläänkö palvelussa luottamuksellista tietoa, esimerkiksi henkilötietoja tai yrityksen luottamuksellisia tietoja, joiden luottamuksellisuuden suojaamiseen tulee kiinnittää erityishuomiota?
- Käyttääkö asiakas palvelua ehkä vain kerran vai toistuvasti? Tuleeko edellisen asiointitapahtuman tietojen olla myöhemmin asiakkaan itsensä tai asiointia hoitavan viranomaisen käytettävissä? Kertyykö asioinnissa mittava määrä yksittäisiin asiakkaisiin liittyvää luottamuksellista tietoa?
- Mitä ei-julkista tietoa asiakkaalle on tarpeen välittää sähköisesti? Mitkä viestintäkanavat ovat tiedon välittämiseen riittävän turvallisia?
- Onko palvelun tarpeen käyttää korkeamman suojaustason tietoja, tietovarantoja tai tietojärjestelmiä, joihin liittyminen edellyttää erityisjärjestelyjä (mm. yhdyskäytäväratkaisut)?
- Onko palveluun liitetty ulkoisia tietojärjestelmiä teknisten rajapintojen kautta? Mitä tietoja rajapinnoissa välitetään? Millä tavalla tietojen käsittely liitetyissä järjestelmissä on turvattu?
- Kuinka tärkeää on taata palvelussa välitettävän tiedon eheys, tai toisaalta osoittaa asiakkaan tai viranomaisen suorittamien toimien kiistämättömyys?

Julkishallinnon sähköisessä asioinnissa on tunnistettavissa joukko yleisiä tietoturvallisuuteen ja tietosuojaan liittyviä vaatimuksia:

- Käyttäjien yksilöinti ja tunnistaminen
- Asiointivaltuuksien hallinta
- Viestinnän luottamuksellisuus
- Viranomaisen vastaanottamien viestien ja asiakirjojen alkuperän ja eheyden varmistaminen
- Viranomaisen julkaiseman tiedon eheyden turvaaminen
- Asiakkaiden suostumusten ja tahdonilmausten sekä niihin liittyvien asiakkaan antamien tietojen kiistämättömyys
- Viranomaispäätösten, tai viranomaisen toimeksiannosta tehtävien päätösten, kiistämättömyys

– Asiointipalvelun saatavuustavoitteiden määrittäminen ja asettaminen

Taulukko **1** havainnollistaa esimerkkien kautta, kuinka tiedon luottamuksellisuus, eheys ja saatavuus painottuvat erityyppisissä asiointipalveluissa. Esimerkkipalveluiden painotukset ovat suuntaa-antavia.

Esimerkkipalvelu	Yksilöinti ja tunnistaminen	Asiointivaltuuksien hallinta	Viestinnän luottamuksellisuus	Viestien alkuperän ja eheyden varmistaminen	Viranomaisen julkaiseman tiedon eheyden turvaaminen	Suostumusten ja tahdonilmausten rekisteröinti ja kiistämättömyys	Viranomaispäätösten kiistämättömyys	Saatavuus ja vikasietoisuus
Toimeentulotuen hakupalvelu (vuorovaikutteinen luottamuksellinen asiointi) Palvelussa käsitellään asiakkaiden arkaluonteisia henkilötietoja. Asiointi on toistuvaa, ja yksittäinen asiointitapahtuma voi olla pitkäkestoinen sisältäen asiakkaan ja viranomaisen luottamuksellista tiedonvaihtoa.	X	(X)	X	X		X	X	X
Säteilytietojärjestelmä (tietopalvelut) Palvelussa jaetaan yleisölle julkista tietoa. Keskeistä on tiedon hallittu päivittäminen ja julkaistun tiedon eheys. Palvelulta voidaan edellyttää lisäksi korkeaa saatavuutta.	X*	X			X			X
Huvilupien hakupalvelu (vuorovaikutteinen ei-luottamuksellinen asiointi) Palvelun avulla asiointitapahtumassa käsitellään vuorovaikutteisesti muita kuin asiakkaan tai yrityksen luottamuksellisia tietoja.	X*	X					X	X
Kansalaisten palautepalvelu (yksisuuntainen asiointi) Kansalaiset antavat viranomaiselle palautetta palveluista tai osallistuvat keskusteluun, jolla pyritään kehittämään yhteiskunnan toimintaa. Käyttäjiä ei tyypillisesti tarvitse tunnistaa luotettavasti, mutta käyttäjät tulee voida yksilöidä, jottei palautetta voida luoda koneellisesti tai vääristellä palautteita käyttötarkoituksen vastaisesti.	X**							X
Lakisääteisten ilmoitusten toimittaminen viranomaisille (järjestelmärajapinta) Yksityishenkilö tai yritys lähettää lakisääteisiä ilmoituksia viranomaiselle joko esityskerroksen tai teknisen rajapinnan kautta. Ilmoitusten lähettäminen voi liittyä monivaiheiseen prosessiin, johon liittyy esim. viranomaisen päätöksiä. Päätökset puolestaan aiheuttavat usein asiakkaalle taloudellisia seuraamuksia. Tiedon saatavuus on muiden asioiden lisäksi keskeisellä sijalla, koska prosessin on edettävä nopeasti ja luotettavasti.	X	X	X	X			X	X

Taulukko 1 Esimerkkejä erityyppisten asiointipalveluiden yleisistä tietoturvavaatimuksista

4 Sähköisen asiointipalvelun tietoturvaperiaatteet

Tässä luvussa on kuvattu yleisiä periaatteita tietoturvallisen sähköisen asiointipalvelun suunnittelun ja toteuttamisen tueksi.

4.1 Tietojen luokittelua ja turvallista sähköistä käsittelyä ohjaavat periaatteet

Sähköisen asioinnin riskejä voidaan olennaisesti ehkäistä jo suunnitteluvaiheessa rajaamalla tietojen sähköinen käsittely asiointipalvelussa vain sen käyttötarkoituksen kannalta välttämättömään tietojoukkoon. Lisäksi palvelun omistajan on suositeltavaa määritellä tietoturvalliset toimintatavat sekä palvelun suunnitteluun, kehittämiseen ja ylläpitoon osallistuville henkilöille, että palvelun asiakkaille.

Tietoturvaperiaate	Kuvaus
Määrittele ei-julkisen tiedon käsittely-periaatteet	Palvelun omistajan tulee tunnistaa palvelun käyttötarkoitus huomioiden siinä käsiteltävä ei-julkinen tietoaineisto ja määritellä käsittelyperiaatteet erityisesti: – tiedon suojaamiselle asiointipalvelun sovellus- ja käyttöpalveluympäristössä – asiointipalvelun ja taustajärjestelmien väliselle turvalliselle tiedonvaihdolle – turvalliselle tiedonvaihdolle toisen viranomaisen tai organisaation asiointipalvelun kanssa – tiedon käsittelylle ei-luotetuissa ympäristöissä, esimerkiksi pilvipalveluissa tai asiakkaiden päätelaitteilla
Tunnista asiointipalvelun keskeiset käyttötilanteet	Palvelun omistajan tulee tunnistaa palvelun keskeiset käyttötilanteet ja kaikki liittymät, niin käyttöliittymät kuin tekniset integraatiorajapinnat, joiden kautta palvelua käytetään tai hallinnoidaan ja kehitetään. Olennaista on tunnistaa palvelun ns. hyökkäyspinta-ala, ts. missä laajuudessa ja missä tietoverkoissa, missä palvelimilla ja millä päätelaitteilla ei-julkisia tietoja käsitellään ja säilytetään. Erityistä huomiota edellyttävät: – poikkihallinnollisen tai usean organisaation yhteisen asioinnin käyttötilanteet, joissa ei-julkista tietoa luovutetaan muille osapuolille käsittelyluvissa tai sopimuksissa eksplisiittisesti määritetyin ehdoin – ei-julkisen tiedon rajatun käsittelyn mahdollistaminen ei-luotetuilla päätelaitteilla tai palveluilla, esimerkiksi kansalaisten omilla päätelaitteilla tai käyttämillä erilaisilla viestintäpalveluilla – palvelun omistajan, palvelutuottajan tai palvelua kehittäjän tahon mahdolliset pääkäyttäjä- ja muut hallinta- sekä kehittämistilanteet
Arvioi ja hallitse säännöllisesti asiointipalveluun kohdistuvia uhkia	Asiointipalvelun omistajan tulee uudelleenarvioida säännöllisesti palveluun kohdistuvia uhkia, niiden vaikutuksia ja merkittävyyttä sekä varmistaa palvelun riittävä turvallisuuden taso ja vaatimuksenmukaisuus – tarvittaessa turvakontrolleja päivittämällä, vaatimuksenmukaisuutta seuraamalla ja varautumalla. Uhka-arvion uusiminen on tarpeen erityisesti seuraavissa tilanteissa: – palvelussa käsiteltävä tietoaineisto muuttuu tai laajenee olennaisesti – palveluun lisätään uusia toimintoja tai ulkoisia rajapintoja – palvelu integroidaan toisen viranomaisen tai organisaation asiointipalveluun – palveluun liitetään uusia kaupallisia tai kansallisen palveluarkkitehtuurin tukipalveluita – palveluun, palvelun omistajaan tai palveluntuottajaan kohdistuu merkittävä uhka tai muutos, jonka seurauksena palveluun voi kohdistua ei-toivottuja vaikutuksia Uhkamallinnuksessa on syytä huomioida sekä ulkoiset että sisäiset uhkatekijät sekä pohtia myös tahallisten väärinkäytösten mahdollisia motiiveja.
Sitouta asiointipalvelun suunnittelijat ja toteuttajat tietoturvatavoitteisiin	Palvelun omistajan tulee varmistua, että tietoturva-, tietosuoja- ja palvelun jatkuvuuden turvaamisen tavoitteet ja vaatimukset on viestitty asiointipalvelun suunnittelusta ja toteutuksesta vastaaville tahoille, ja että vaatimukset on ymmärretty ja

ja -vaatimuksiin	huomioitu palvelun suunnittelussa, kehittämisessä, toteutuksessa ja ylläpidossa. Erityisesti suunnittelussa tulee huomioida tietoturvallisen tietojenkäsittelyn lakisääteiset vaatimukset.
Sitouta palvelutoimittajat ja yhteistyökumppanit asiointipalvelun tietoturvatavoitteisiin ja -vaatimuksiin	Palvelutoimittajien ja yhteistyökumppaneiden toiminta turvallisen sähköisen asiointipalvelun järjestämisessä on keskeinen. Palvelun omistajan tai sen lukuun toimivan tahon tulee varmistaa sopimuksin, käsittelyluvin ja eksplisiittisin sanktioin, että kaikki palvelun tuottamiseen, kehittämiseen ja tietojen käsittelyyn osallistuvat osapuolet ymmärtävät palvelun omistajaa sitovat velvoitteet ja ovat sitoutuneet niihin omassa palveluun liittyvässä toiminnassaan. Palvelutoimittajien ja kumppaneiden palveluun liittyvän toiminnan vaatimuksenmukaisuuden arviointiin on syytä panostaa erityisesti silloin, kun palvelun omistajan omistamia tietoja käsitellään palvelun omistavan organisaation ulkopuolella, esimerkiksi: – palvelutoimittajalle ulkoistetussa käyttöpalveluympäristössä – SaaS-palvelussa tai muussa ei-luotetussa ulkoisessa palvelussa – toisen viranomaisen tai organisaation asiointipalvelussa. Usean organisaation vastuulle jakaantuvan sähköisen asioinnin suunnittelussa tulee varmistua siitä, että kaikki ei-julkisen tiedon käsittelyyn osallistuvien organisaatioiden palveluun liittyvä toiminta on riittävällä turvallisuuden tasolla.
Varmista tietoturvallisuuden riittävä koordinointi ja seuranta	Tietoturvallisuutta koskevien tehtävien vastuuttamisen merkitys nimetyille vastuuhenkilöille tai -rooleille korostuu poikkihallinnollisessa asioinnissa sekä palveluiden tuottamisessa usean toimijan kesken. Tietoturvallisuuden osalta keskeisiä koordinoitavia tehtäviä ovat erityisesti häiriötilanteiden ja tietoturvapoikkeamien käsittelyn johtamis- ja muut menettelytavat sekä ei-julkisen tiedon käsittelysäännöt ml. luovutuskäytännöt ja seuranta (esim. lokitus).
Opasta asiakkaita asiointipalvelun turvalliseen käyttöön	Palvelun käyttäjät voivat omilla toimillaan vaikuttaa itseään koskevien tietojen suojaamiseen asiointipalvelussa tai palveluketjussa. Palvelun omistajan tulee tarjota palvelun käyttäjille riittävät ohjeet ja tuki palvelun turvalliseen käyttöön. Esimerkiksi tunnistusvälineiden tietoturvallinen käsittely, päätelaitteiden suojaaminen haittaohjelmilta ja asiointipalvelun turvalliset käyttötilanteet on syytä ohjeistaa. Lisäksi palvelussa tulee huolehtia tietoturvauhista ja tapahtuneista loukkauksista ilmoittamisesta sekä käyttäjille, muille yhteistyötahoille että viranomaisille.

4.2 Asiointipalvelun rakenteellista suunnittelua ohjaavat periaatteet

Sähköisen asiointipalvelun suunnittelussa tulee soveltaa rakenteita, jotka rajaavat käyttäjien pääsyä ei-julkiseen tietoaineistoon heidän tietotarpeidensa perusteella ja madaltavat siten riskejä mm. tietovuodoista ja tietomurroista. Lisäksi turvallisilla rakenneratkaisuilla tulee pyrkiä rajaamaan yksittäisen haavoittuvuuden väärinkäytöstä aiheutuvia sähköiseen asiointipalveluun ja palvelun omistavaan organisaation kohdistuvia haittavaikutuksia sekä vaikutusten leviämistä. Tietoihin pääsyn rajaamisen ratkaisut eivät kuitenkaan saa tarpeettomasti haitata tiedon tarkoituksenmukaista saatavuutta.

Tietoturvaperiaate	Kuvaus
Minimoi riskialttiit toiminnot ja pääsy tietoon	Asiointipalvelun tulee toteuttaa vain asiointiprosessin kannalta välttämättömät toiminnot. Pääsy tietoon tulee rajata mahdollisimman suppeaan tiedon osajoukkoon käyttäjän tietotarpeiden, esimerkiksi hallinnollisen vastuualueen mukaisesti. Palvelussa tulee huolehtia käyttövaltuuksien hallinnasta pienimmän käyttövaltuuden periaatteen mukaisesti. Asiakkaiden puolesta-asiointivaltuudet on syytä kohdentaa vain rajattuihin käyttötapauksiin. Myös valtuuksien muuttuminen ajan saa-

	tossa on syytä huomioida. Lisäksi pääsyä tietoon on syytä rajata rakenteellisesti, esimerkiksi eriyttämällä viranomaisen käyttämät ylläpitotoiminnot julkisen internetverkon asiakaskäyttöliittymistä ja välttämällä ei-julkisen tiedon välivarastointia itse asiointipalvelussa.
Sovella modulaarista arkkitehtuuria	Asiointipalvelussa on suositeltavaa soveltaa modulaarista tai palvelukeskeistä arkkitehtuurimallia, jossa jokainen moduuli toteuttaa itsenäisesti tarvittavat ja tarkoituksenmukaiset tiedon luottamuksellisuutta, eheyttä ja saatavuutta suojaavat tietoturvakontrollit. Moduulikohtaiset kontrollit täydentävät toisiaan ja edistävät siten kerroksellisen tietoturvallisuuden toteutumista.
Käytä asiointipalvelussa vain tietoturvallisiksi arvioituja teknisiä ratkaisuja	Palvelussa tulee käyttää vain testattuja ja tietoturvallisiksi arvioituja tai todennettuja ohjelmistoja, ohjelmistokirjastoja, sovelluskehikkoja ja tukipalveluita. Erityisosaamista vaativien tietoturvaratkaisujen, esimerkiksi salausalgoritmien, räätälöityjä toteutuksia on syytä välttää. Lisätietoa VAHTI 2/2015 Ohje salauskäytännöistä. Avointa lähdekoodia käytettäessä tulee arvioida, onko kehittäjä- ja käyttäjäyhteisö riittävän laaja ja aktiivinen, jotta vertaisarviointi on riittävää mahdollisten haavoittuvuuksien tai virheiden havaitsemiseksi ja korjaamiseksi. Lisäksi korkeamman riskitason ympäristöissä on suositeltavaa keskittää avoimen lähdekoodin alkuperän tarkistus-, hallinta- ja versiopäivitystoimet, jolloin voidaan rajata riskiä koodin kautta tapahtuvista haavoittuvuus- ja virhetilanteista. Ensisijaisesti sähköisissä asiointipalveluissa tulee käyttää tietoturvallisia kansallisia hallinnon tukipalveluita, tai vaihtoehtoisesti tai niiden lisäksi organisaatiossa, palvelukeskittymissä tai hallinnonalalla keskitetysti toteutettuja tukipalveluita. Kaupallisissa tukipalveluissa tulee varmistua niiden tietoturvallisuudesta ja vaatimustenmukaisuudesta jo ennen sopimuksia tai käyttöehtojen hyväksyntää, ettei käyttöönoteta tukipalvelua, jonka tietojen käsittelystä, turvallisuuden tasosta tai palvelun jatkuvuudesta ei voida varmistua.
Suojaa asiointipalvelun ympäristöt, tukijärjestelmät ja ylläpitäjät tietoturvauhilta	Asiointipalvelun tekniset ympäristöt tulee suojata tunnistetuilta tietoturvauhilta. Palvelun suunnittelussa ja toteutuksessa tulee huomioida tuotantopalvelun ylläpidon sekä ei-tuotannollisten ympäristöjen ja palvelun tukijärjestelmien tietoturvallisuus. Asiointipalvelun ylläpito tulee suorittaa ympäristössä, joka on suojattu uhkatekijöiltä vähintään yhtä hyvin kuin itse asiointipalvelu. Esimerkiksi palvelun teknisten ympäristöjen altistuminen haittaohjelmille ja ylläpitohenkilöstön altistuminen tietojen kalastelulle tulee minimoida. Ei-tuotannolliset ympäristöt (esim. kehitys- ja testiympäristöt) sekä tukijärjestelmät, kuten sähköiset ryhmätyötilat ja dokumentaatiot, versionhallinta ja komponenttikirjastot, voivat tarjota hyökkääjille arvokasta tietoa palvelun rakenteesta, suojaratkaisujen toteutuksista sekä palvelun haavoittuvuuksista, ja laajentaa palvelun hyökkäyspinta-alaa merkittävästi. Siksi myös ne on syytä suojata valtuudettomalta katselulta ja muutoksilta, ja niiden käyttöä on syytä valvoa. Erityisesti ei-julkisen tiedon välittyminen tuotantoympäristöstä heikommin suojattuihin ympäristöihin ja tukijärjestelmiin tulee estää tai pienentää kyseisen käyttötilanteen mukanaan tuomia riskejä hyväksyttävälle tasolle. Korkeamman riskitason palvelun tuotantoympäristöön heikommin suojatuista ympäristöistä mahdollisesti tuotavien tietojen, konfiguraatioiden tai lähdekoodin tietoturvallisuudesta, erityisesti eheydestä, on varmistuttava.
Arvio säännöllisesti asiointipalvelun tietoturval-	Asiointipalvelun omistajan tulee kyetä arvioimaan, ja tarvittaessa todentamaan, tietoturvallisuuden riittävä taso koko asiointipalvelun palvelutuotantoketjussa. Ar-

lisuuden tasoa	vioinnin laajuus ja tiheys on syytä perustaa palvelun uhkiin ja riskiarviointiin. Palvelun kehityksessä ja ylläpidossa tulee ennen kaikkea määritellä tietoturvallisuuden testauskäytännöt sekä hyväksyntäkriteerit muutostilanteissa. Arvioinnin säännöllisyys palvelun koko elinkaaren ajan on ensiarvoisen tärkeää, sillä esimerkiksi palvelun perustamisvaiheessa valitut tietoturvalliset ohjelmistot ja avoimen lähdekoodin komponentit voivat uhkaympäristön muuttuessa ja uusien haavoittuvuuksien myötä osoittautua turvattomiksi tai edellyttää esimerkiksi haavoittuvuuksien rajaukseen toimenpiteitä. Mahdollisia arviointimenetelmiä ovat omaehtoinen itsearviointi ja tietoturvatestaus, haavoittuvuusskannaus, muutoshallinnassa riskiarviointi, riippumattoman osapuolen suorittama tietoturva-arviointi tai erikseen nimetyn oikeutetun tahon suorittama palvelun arviointi tai akkreditointi. Palvelun omistajan tulee riskiarvionsa perusteella päättää, suoritetaanko palvelulle riippumattoman tahon tietoturva-auditointi/arviointi/akkreditointi esimerkiksi Viestintäviraston tai sen valtuuttaman hyväksytyn arviointilaitoksen toimesta. Palvelun tietoturvallisuuden itsearviointi, tietoturvatestaukset ja muutoshallinnassa riskiarviointi ovat suositeltavia toimenpiteitä kaikissa sähköisissä asiointipalveluissa. Niiden avulla voidaan tunnistaa tietoturvapuutteita kehityssyklin aikaisessa tai muutoksen vaiheessa, jolloin korjaustoimenpiteiden aikataulu- ja kustannusvaikutukset ovat mahdollisimman pienet sekä myös myöhemmin testattaessa tai arvioitaessa laajempaa osuutta.

4.3 Tietoturvapoikkeamien hallintaa koskevat periaatteet

Ennaltaehkäisevistä suojauskeinoista huolimatta on aina olemassa mahdollisuus, että sähköinen asiointipalvelu joutuu hyökkäyksen tai muun väärinkäytöksen kohteeksi. Palvelun omistajalla tulee olla valmiudet havaita palvelun normaalista toiminnasta tapahtuva tietoturvapoikkeama ja käsitellä poikkeamatilanne tehokkaasti.

Tietoturvaperiaate	Kuvaus
Kerää asiointipalvelun tapahtuma- ja lokitietoja riittävän kattavasti	Riittävät lokitiedot tapahtumista asiointipalvelussa ovat välttämätön edellytys asiointipalvelun tietoturvallisuuden valvonnalle, poikkeamien havaitsemiselle sekä niiden jälkikäteisselvitykselle. Asiointipalvelun suunnittelussa tulee varmistaa, että tapahtumista kerätään riittävässä laajuudessa ja tarkkuudessa lokitietoja ja että lokitiedot ovat tarvittaessa palvelun omistajan saatavilla. Lokitiedon tuottamisesta palvelun eri lokilähteistä tulee suunnitelmallisesti huolehtia, sopia ja varmistaa tapahtumien ja palvelussa tehtävien toimien lokikirjausketjut, paitsi itse asiointipalvelun, myös siihen liitetyiden tietojärjestelmien, integraatioratkaisujen ja tukipalveluiden osalta.
Tunnista asiointipalvelun normaali toiminta ja siitä tapahtuvat poikkeamat	Palvelun suunnittelussa tulee tunnistaa asiointipalvelun komponenttien välinen kommunikointi normaalissa tuotantokäytössä sekä käyttötilanteissa asiointipalvelussa tapahtumien normaali eteneminen. Kun palvelun normaalit käyttöprofiilit ja käyttötilanteissa tapahtumien vaiheet ja tilatiedot ovat tiedossa, myös poikkeamien tunnistaminen ja niihin reagoiminen on mahdollista. Sähköisessä asioinnissa huomioitavia poikkeamatilanteita ovat esimerkiksi: 1. automatisoidut, palvelun sisältämien tietojen laajamittaiseen keräämiseen tähtäävät hyökkäykset 2. palvelunestohyökkäykset 3. *Command and control* -haittaohjelmatartunnat, jotka voidaan havaita saastuneiden laitteiden ja komentopalvelimien välisestä kommunikoinnista

	4. asiointipalvelun tai palveluketjun osan haavoittuvuuden hyväksikäyttö omaksi eduksi (esim. pankkitilitietojen valtuudeton muuttaminen).
Varaudu tietoturvapoikkeamiin ja niistä palautumiseen	Tietoturvapoikkeaminen käsittely ja niistä palautuminen edellyttää eri osapuolten suunniteltua ja tehokasta yhteistoimintaa. Sähköisessä asiointipalvelussa oleellisia asioita ovat: – varajärjestelmät tai typistetyt asiointipalvelut, jotka voivat olla toiminnallisesti rajatummat kuin normaalitilanteessa tarjottava asiointipalvelu – staattinen, suorituskykyinen kriisisivusto, johon käyttäjät ohjataan automaattisesti, kun asiointipalvelu ei ole saatavilla – sähköisen asioinnin korvaavat varajärjestelyt; esimerkiksi asioinnin mahdollistaminen asiakaspalvelupisteessä tai tiettyjen asiakasryhmien tai asioinnin käyttötilanteiden priorisointi – tietoturvapoikkeamien ilmoittaminen Viestintävirastolle – rikosilmoitukset poliisille – tietosuojaloukkausten ilmoittaminen tietosuojavaltuutetulle, Viestintävirastolle ja loukkauksen kohteeksi joutuneille henkilöille – häiriöilmoitukset sähköisen asioinnin tukipalvelun palvelutuottajalle, jos tukipalveluun liitettyyn asiointipalveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka voi vaarantaa tukipalvelun tietoturvallisuuden tai toimivuuden tai häiritä sitä olennaisesti – toipumissuunnitelma ja viestintäsuunnitelma palvelukatkojen ja tietoturvapoikkeamatilanteiden varalle.

5 Sähköisen asiointipalvelun viitearkkitehtuuri

5.1 Johdanto

Sähköisten asiointipalveluiden tietoturvallisuutta voidaan hahmottaa tässä luvussa kuvatun viitearkkitehtuurin avulla. Viitearkkitehtuuri on käytännönläheinen apuväline, joka auttaa asiointipalvelun suunnittelusta, toteutuksesta ja kehittämisestä vastaavia tahoja soveltamaan käytännössä luvussa 4 kuvattuja tietoturvaperiaatteita. Viitearkkitehtuuri lähestyy asiointipalvelun suunnittelua seuraavista näkökulmista:

1. **Palvelun tietoturvallinen rakenne**
    - Käyttöpalveluympäristön ja asiointisovelluksen arkkitehtuuriin tulee kiinnittää erityistä huomiota jo palvelua suunniteltaessa, sillä turvattomiksi osoittautuneita rakenteellisia ratkaisuja on usein vaikeaa ja kallista korjata jälkikäteen.
2. **Kontrolliympäristö**
    - Rakenneratkaisujen ohella palvelun omistajan tulee tehdä joukko suunnittelupäätöksiä yksittäisten tietoturvakontrollien toteutuksesta. Kappale 5.3 sisältää hyviä käytäntöjä niin käyttäjiä kuin sovellus- ja käyttöpalveluympäristöä koskevien kontrollitavoitteiden toteuttamiseksi.

Viitearkkitehtuurin laadinnassa on noudatettu seuraavia periaatteita:

– **Kattavuus**
    - Viitearkkitehtuuri kattaa kaikki sähköisen asioinnin tietoturvallisuuden kannalta olennaiset osa-alueet, esimerkiksi käyttäjien tunnistamisen ja valtuuttamisen, tietoliikenteen ja tietovarantojen luottamuksellisuuden varmistamisen salausratkaisuin sekä palvelun saatavuuden turvaamisen.
– **Modulaarisuus**

  - Viitearkkitehtuuri on sovellettavissa erityyppisiin asiointipalveluihin. Tietoaineiston ja palvelun luottamuksellisuus, eheys ja saatavuus painottuvat eri tavoin eri asiointiprosesseissa, ja viitearkkitehtuurista voidaan valita juuri tarkasteltavassa palvelussa olennaiset osuudet.

– **Teknologia- ja tuoteriippumattomuus**
  - Viitearkkitehtuuri ei ohjaa palvelun omistajia käyttämään tiettyjä ohjelmistotuotteita- tai teknologioita.

Viitearkkitehtuuria ei ole kaikissa asiointipalveluissa tarkoituksenmukaista soveltaa koko laajuudessaan. Asiointipalvelun suunnitteluun, toteuttamiseen ja kehittämiseen osallistuvia tahoja kannustetaan kuitenkin tutustumaan siihen kokonaisuudessaan ja valikoimaan suorittamansa riskiarvion perusteella palvelun kannalta riittävät, tarkoituksenmukaiset, riittävän turvalliset ja kustannustehokkaat ratkaisut.

Asiointipalvelun omistajan tulee kuitenkin aina huolehtia siitä, että palvelu täyttää vähintään siihen kohdistuvat lakisääteiset minimivaatimukset.

5.2 Tietoturvallisen asiointipalvelun rakenne

Tämä kappale esittelee keskeiset rakenteelliset keinot, joilla luottamuksellista tietoa voidaan suojata sähköisessä asiointipalvelussa, mutta tarvittaessa myös jakaa hallitusti esimerkiksi usean viranomaisen vastuulle haarautuvassa poikkihallinnollisessa tai usean organisaation asiointiprosessissa:

– Modulaarinen ratkaisuarkkitehtuuri

– Käyttöliittymien eriyttäminen käyttäjien tietotarpeiden perusteella

– Tukipalveluiden tietoturvallisuus

Kansallisen palveluarkkitehtuurin ja hallinnon yhteisten sähköisen asioinnin tukipalveluiden merkitys koko julkishallinnon sähköisen asioinnin järjestämisessä on keskeinen ja mahdollistaa aiempaa paremman yhteentoimivuuden. Nämä huomioiden ja tukipalveluita käyttämällä on mahdollista suunnitella, toteuttaa ja kehittää oman asiointipalvelun rakenteesta tietoturvallinen.

5.2.1 Modulaarinen ratkaisuarkkitehtuuri

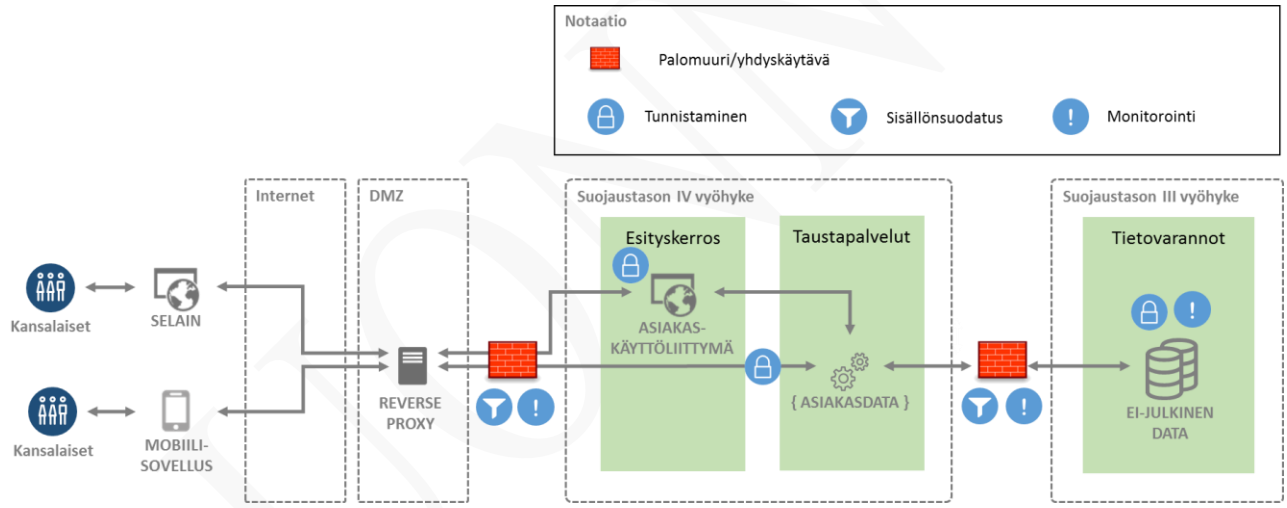
Asiointipalvelun suunnittelussa tulee soveltaa modulaarista arkkitehtuuria. Modulaarinen palvelu rakentuu määritellyin rajapinnoin eriytetyistä komponenteista tai palveluista, jotka toteuttavat itsenäisesti tietyn toiminnallisuuden tai tarjoavat pääsyn asiointipalvelun tarvitsemaan tietoon. Hajautetut mikropalvelut ovat esimerkki modulaarisesta, palvelukeskeisestä arkkitehtuurimallista. Tietoturvallisesti toteutetussa asiointipalvelussa eri moduulien välillä ei ole implisiittistä luottamusta vaan ne toteuttavat itsenäisesti tarvittavat suojaukset, esimerkkinä kutsuvan osapuolen tunnistaminen ja syötetietojen validointi. Palvelun suunnittelussa on syytä noudattaa seuraavia ohjeita:

- Moduulit sijoitellaan käyttöpalveluympäristössä suojaustarpeen mukaan eri vyöhykkeisiin. Vyöhykkeiden välinen tiedonsiirto on kontrolloitua ja hyödyntää toisiaan täydentäviä palomuuri-, yhdyskäytävä- ja monitorointiratkaisuja tiedon ja ympäristöjen suojaamiseksi.

- Taustapalvelut ja tietovarannot on eriytetty asiointipalvelun sovelluskerroksesta. Suojattavaa tietoa ei välivarastoida tarpeettomasti asiointipalvelussa vaan asiointitapahtumassa tarvittava rajattu tietojoukko haetaan käyttöhetkellä taustajärjestelmistä palvelurajapintojen kautta. Periaatteen vastaisia ratkaisuja, esimerkiksi vyöhykerajan ylittäviä suoria tietokantayhteyksiä, tulisi käyttää vain hyväksytyissä poikkeustapauksissa erillisen riskiarvioinnin ja täydentävien riskienhallintamenettelyjen toteuttamisen ja hyväksynnän jälkeen.
- Palvelurajapinnat piilottavat taustapalvelun tai tietovarannon rakenteen ja teknisen toteutuksen yksityiskohdat, mikä vaikeuttaa niissä piilevien haavoittuvuuksien väärinkäyttöä[2]. Palvelurajapinnoissa on suositeltavaa käyttää teknologiariippumatonta protokollaa tai standardia, jolloin kaikki käyttöliittymät ja tietojärjestelmät voivat käyttää samaa testattua ja turvallista palvelurajapintaa.
- Palvelun eri moduuleissa toteutetut suojaukset ja mahdolliset poikkeukset dokumentoidaan, jolloin asiointipalvelun omistajalla on valmiudet arvioida muutos- ja häiriötilanteiden vaikutusta palvelun tietoturvallisuuteen kokonaisuutena.

Modulaarinen arkkitehtuuri ja sen mahdollistama kerroksellinen tietoturvallisuus suojaavat palvelua tehokkaasti väärinkäytöksiltä, kun haavoittuvuus yhdessä komponentissa ei automaattisesti mahdollista murtautumista järjestelmään kompensoivien suojausten täydentäessä sitä.

Kuvan 2 yksinkertaistettu esimerkki havainnollistaa palvelukeskeisen arkkitehtuurin mukaista monikerroksista asiointipalvelua ja sen moduulikohtaisia tietoturvakontrolleja.



Kuva 2 Esimerkki palvelukeskeisestä arkkitehtuuria noudattavasta asiointipalvelusta

Esimerkki: Palvelukeskeisen arkkitehtuurin mukainen asiointipalvelu (Kuva 2)

Reverse proxy-, web-, sovellus- ja tietokantapalvelut on sijoiteltu eri suojaustason vyöhykkeisiin. DMZ- ja ST IV -vyöhykkeiden välinen yhdyskäytäväratkaisu huolehtii mm. asiakkailta peräisin olevien liitetiedostojen sisällönsuodatuksesta ja haittaohjelmasuojauksesta sekä internet-tietoliikenteen monitoroinnista. ST IV ja ST III -vyöhykkeiden välinen yhdyskäytäväratkaisu varmistaa, ettei korkeamman suojaustason ympäristön ei-julkisen tiedon varastosta siirry hallitsemattomasti suojaustason III aineistoa asiointipalveluun. ST IV -vyöhykkeelle sijoitetut asiointipalvelun omat tietovarannot eivät sisällä kopioita ST III -vyöhykkeellä tallennettavasta ei-julkisesta tiedosta.

Mobiilisovellus ja selainkäyttöinen asiakaskäyttöliittymät käyttävät ei-julkista tietovarantoa REST-arkkitehtuurimallin mukaisen palvelurajapinnan kautta. Palvelurajapintoja käyttävät sovellukset ja väliohjelmistot tunnistetaan varmenteella.

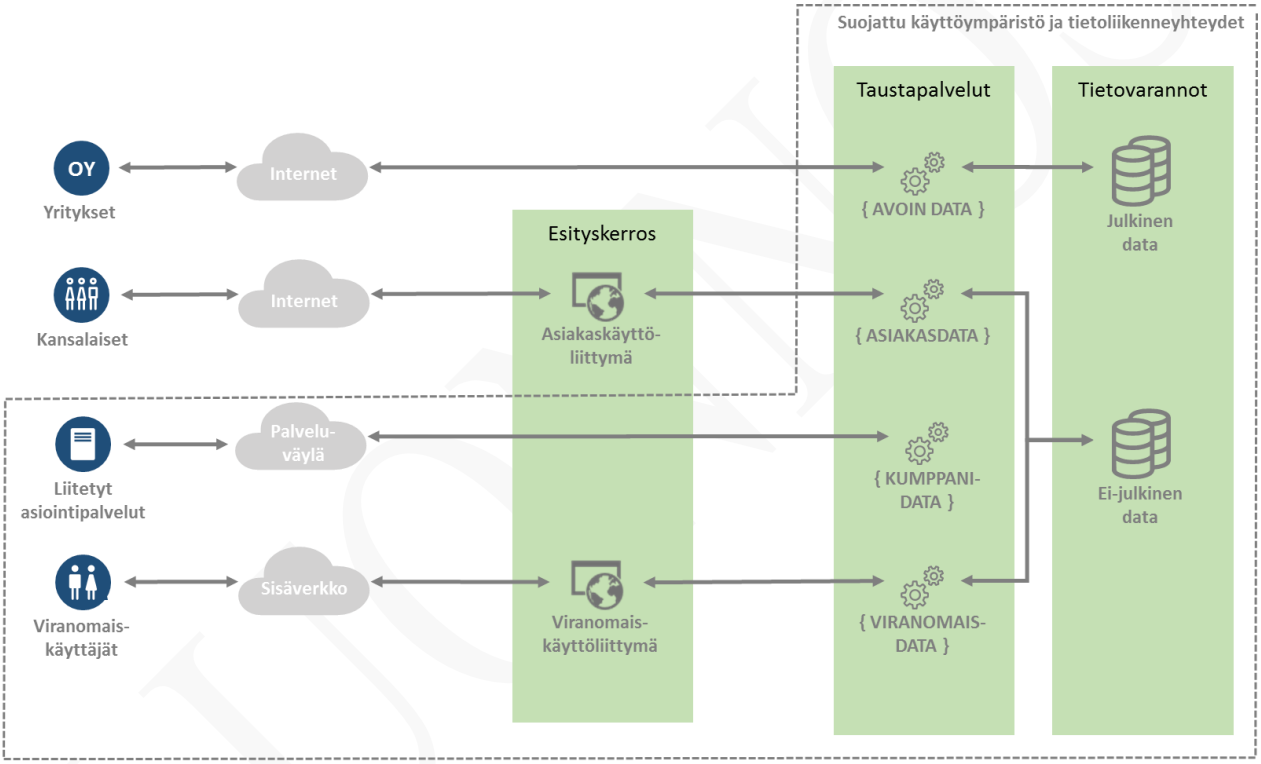
[2] Esimerkiksi injektiohyökkäykset ja järjestelmä- ja sovellushaavoittuvuuksia hyödyntävien haittaohjelmien tartuttaminen.

5.2.2 Käyttöliittymien ja palvelurajapintojen eriyttäminen

Asiointipalvelun eri käyttäjäryhmien tietotarpeet poikkeavat tyypillisesti toisistaan. Kansalaiset käsittelevät yleensä vain itseään koskevaa tietoa, kun taas asiointitapahtuman viranomaiskäyttäjät tarvitsevat usein laajemmat valtuudet tiedon katseluun ja muokkaamiseen. Viranomaisen vastuut voidaan edelleen eriyttää vastuurooleittain, esimerkkinä rekisterinpitäjät ja sovellusylläpitäjät.

Tietoriskien minimoimiseksi eri käyttäjäryhmille suunnatut käyttöliittymät tulee pyrkiä eriyttämään, ja kukin käyttöliittymä on syytä rajata toiminnallisesti sisältämään vain käyttäjäryhmän tarvitsema minimitoiminnallisuus. Käyttöliittymien lisäksi tietotarpeeseen perustuvan eriyttämisen periaatetta on suositeltavaa soveltaa myös asiointipalvelun teknisiin rajapintoihin, esimerkkinä toisille viranomaisille ja yrityksille tarjottavat palvelurajapinnat ja avoimen datan rajapinnat. Eriytetyt käyttöliittymät ja palvelurajapinnat voivat hyödyntää samaa koodiperustaa, josta koostetaan julkaisuprosessissa erilliset käyttöliittymät ja palvelurajapinnat.

Kuva 3 havainnollistaa esimerkillä edellä kuvattua eriyttämisen periaatetta.



Kuva 3 Esimerkki käyttöliittymien ja palvelurajapintojen eriyttämisestä

Käyttöliittymien rakenteellisen eriyttämisen merkittävimmät hyödyt ovat seuraavat:

- Toiminnallisesti laajemmat viranomaiskäyttöliittymät ja palvelurajapinnat voidaan sijoitella käyttöpalveluympäristöön, johon sallitaan pääsy ainoastaan viranomaisen sisäverkosta ja viranomaisen hyväksymiltä päätelaitteilta
- Palvelun laajamittainen väärinkäyttö varastettua identiteettiä tai käyttäjävaltuutuksen haavoittuvuuksia hyödyntäen[3] vaikeutuu, kun julkisen internetverkon asiakaskäyttöliittymistä on riisuttu laajat katselu- ja muokkaustoiminnot
- Palvelun omistavan organisaation viranomaistoimintaa koskevat tietoturvallisuuden erityisvaatimukset on helpompi toteuttaa eriytetyissä käyttöliittymissä ja rajapinnoissa
- Kansalaisten ja viranomaisten tunnistaminen voidaan toteuttaa tarkoituksenmukaisesti eriytetyissä liittymissä

[3] Niin kutsutut *privilege escalation -hyökkäykset*

- Eriytetyt käyttöliittymät voivat käyttää taustapalveluita ja tietovarastoja eri teknisillä tunnuksilla, joiden käyttöoikeudet on rajattu pienimmän käyttövaltuuden periaatteen mukaisesti
- Palvelunestohyökkäyksissä julkisen internetverkon asiakaskäyttöliittymät on helppo eristää taustajärjestelmistä, jolloin haittavaikutukset asiointipalvelun omistajan muun toiminnan jatkuvuudelle on mahdollista rajata.

Käyttöliittymien eriyttämistä puoltavat tietoturvallisuuden lisäksi usein myös toiminnalliset syyt. Tiettyyn käyttötarkoitukseen voi olla tarkoituksenmukaista tarjota mobiilipäätelaitteelle asennettava sovellus, joka mahdollistaa vaikkapa paikkatiedon hyödyntämisen asiointipalvelussa käyttäjän luvalla.

Esimerkki 1: Legacy-järjestelmän asiointilaajennos

Hakemuspalvelu on toteutettu laajennoksena viranomaisen vanhaan asianhallintajärjestelmään siten, että uusi asiointisovellus kattaa ainoastaan kansalaisille suunnatut verkkoasiointitoiminnot. Viranomaiset suorittavat hakemusten käsittelyn kokonaisuudessaan asianhallintajärjestelmässä.

Kansalaisten asiointisovellus on liitetty asianhallintajärjestelmään palvelurajapinnoin integraatioväylän välityksellä ja tiedonvälitys perustuu XML-sanomaliikenteeseen. Asiointisovelluksen tietoturvatestauksessa on varmistettu erityisesti, ettei asiointisovelluksen sovelluskoodi sisällä XML-injektiohaavoittuvuuksia.

Esimerkki 2: Ohjelmistotuotteeseen perustuva asiointipalvelu

Asiakkaiden ja viranomaisten käyttöliittymien toiminnallinen eriyttäminen ei ole mahdollista johtuen käytetyn valmisohjelmiston sovellusarkkitehtuurista. Palvelun omistajan tulee tällöin kiinnittää ohjelmiston tietoturvatestauksessa erityistä huomiota loogisen pääsynhallinnan ja istunnonhallinnan toteutukseen. Riskiarvion perusteella asiointipalvelun osia voidaan toteuttaa erillään ohjelmistotuotteesta.

5.2.3 Tukipalveluiden tietoturvallisuus

Valtaosa sähköisistä asiointipalveluista edellyttää mm. käyttäjien tunnistamista ja valtuuttamista sekä luottamuksellista tiedon vaihtoa asiakkaan ja asiointipalvelun välillä. Nämä toiminnot on useimmiten tarkoituksenmukaista toteuttaa uudelleenkäytettävinä ja vakioituina tukipalveluina, hyödyntäen esimerkiksi kansallisen palveluarkkitehtuurin tuottamia hallinnon sähköisiä tukipalveluita.

Koska sähköisen asioinnin muodot kehittyvät nopeasti, kansallisen palveluarkkitehtuurin ei voi olettaa tarjoavan valmiita ratkaisuja kaikkiin nykyisiin ja tuleviin tarpeisiin eri käyttötilanteissa. Siksi asiointipalveluiden tarjoajat käyttävät myös kaupallisten toimijoiden tarjoamia palveluita ja ratkaisuja, joilla voidaan rikastaa sähköisen asioinnin käyttökokemusta ja mahdollistaa kokonaan uusia asiakaslähtöisiä vuorovaikutuksen ja palvelukehityksen tapoja. Esimerkkejä kaupallisista tukipalveluista ovat:

1. Vuorovaikutteiset asiakaspalvelu- ja viestintäratkaisut (mm. chat- ja videoneuvottelupalvelut)
2. Palvelun käyttöstatistiikan keruu- ja analytiikkapalvelut
3. Sovellusten liitännäiset ja lisäosat (esimerkiksi sosiaalisen median palveluiden toiminnot, kuten jakaminen tai tykkäys tunnistettavien painikkeiden avulla)
4. Ohjelmistorobotiikkapalvelut, jotka jalostavat tietoa ja automatisoivat asiointiprosessiin liittyviä rutiininomaisia tehtäviä tai niiden osia.

Edellä kuvattujen palveluiden käyttöönotto on usein houkuttelevan helppoa ja edullista mikäli palveluille ei aseteta erityisiä vaatimuksia. Asiointipalvelun suunnittelussa tulee kuitenkin pitää kaupallisia palveluita oletusarvoisesti ei-luotettuina. Palveluiden perusajatuksena on pitkälle viety vakiointi ml. käyttöehdot, eivätkä niiden tietoturvallisuuden ja tietosuojan taso välttämättä vastaa juuri Suomen tai muiden maiden ja yhteisöjen viranomaisvaatimuksia varsinkaan silloin, kun palvelun tarjoaja toimii ja tuottaa palveluita tai niiden osia Suomen ja EU/ETA-alueen ulkopuolella.

Ei-luotettujen palveluiden käyttöön liittyy erityisesti tietojen luottamuksellisuuden ja asiakkaiden tietosuojan näkökulmasta huomionarvoisia seikkoja, joista on laadittu ohjeen liitteeseen 2 tiivis tarkistuslista. Palveluiden valinnassa tulee varmistua, ovatko sopimus- tai käyttöehdot neuvoteltavissa asiakaskohtaisesti, ja onko puutteita palvelun tietoturvallisuudessa ja muussa vaatimuksenmukaisuudessa mahdollista kehittää asiakaskohtaisesti.

Asioinnin tukipalveluiden valinnassa on syytä noudattaa seuraavaa päätöksentekoketjua:

1. Asiointipalvelussa käytetään ensisijaisesti kansallisia hallinnon sähköisen asioinnin tukipalveluita aina, kun palvelun omistavalla organisaatiolla on velvoite tai oikeus tukipalveluiden käyttöön. Tukipalvelut on kuvattu luvussa 8.
2. Jos kansallista tukipalvelua ei ole saatavilla, saatavilla oleva tukipalvelu ei vastaa asiointipalvelun tarpeita tai organisaatio ei ole oikeutettu tukipalvelun käyttöön, asiointipalvelun omistaja voi toteuttaa keskitetyn tukipalvelun itse tai yhdessä, esimerkiksi organisaation sisäisessä tai hallinnonalan palvelukeskittymässä.
3. Muussa tapauksessa asiointipalvelun omistaja voi harkita kaupallisen tukipalvelun käyttöä asiointipalvelussa varmistuttuaan riittävän luotettavasti tukipalvelun tietoturvallisuudesta ja vaatimuksenmukaisuudesta (huomioitava käytön edellyttämät sopimus- tai käyttöehdot ja erityisesti niiden mukaiset rajaukset).
4. Ellei tietoturvallisuuden ja vaatimuksenmukaisuuden varmistaminen ole mahdollista, palvelun omistajan tulee rajoittaa tietojenkäsittely ei-luotetussa tukipalvelussa julkisiin tietoihin. Tällöinkin on mahdollisesti rajattava tukipalvelussa tietojenkäsittelyä julkisten tietojen osalta vain niihin julkisiin tietoihin, joihin on tukipalvelun sopimus- tai käyttöehtojen arvioitu olevan riittävät ko. tietojen eheyden ja saatavuuden osalta (arvioitava riskit ja hyväksyttävissä oleva riskitaso).

Esimerkki: Asiakaspalvelu videoyhteydellä

Terveydenhuollon viranomainen tarjoaa asiakaspalvelua videoyhteydellä. Jos asiakaspalvelutilanteessa käsitellään suurella todennäköisyydellä arkaluonteisia henkilötietoja, videoneuvotteluratkaisun vaatimuksenmukaisuus tulee varmentaa ennen käyttöönottoa. Tarvittaessa viranomainen voi porrastaa vuorovaikutteiset videoneuvontapalvelunsa eri vaiheisiin siten, että yleinen esimerkiksi ajanvarausta koskeva asiakaspalvelu tapahtuu hallittuna SaaS- tai pilvipalveluna, kun taas arkaluonteisen henkilötiedon käsittelyn mahdollistava henkilökohtainen neuvonta edellyttää vahvaa sähköistä tunnistamista ja siirtymistä paremmin suojattuun asiointipalveluun tai asiointipalvelun osaan (esimerkiksi paikallisesti toteutettu videoneuvottelupalvelu).

Esimerkki: Analytiikkapalvelut

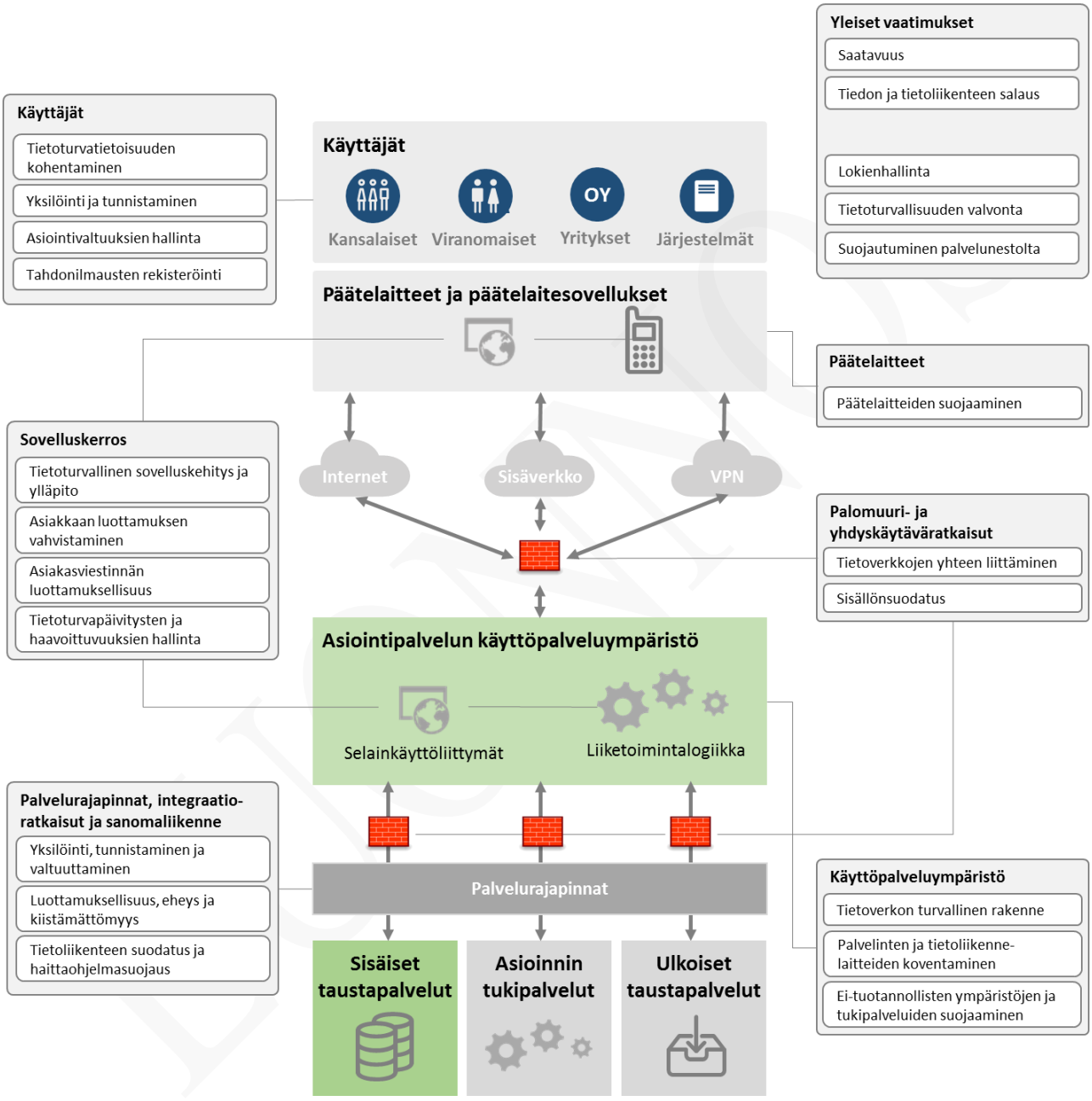
Asiointipalvelun kehittämisen tueksi on tarpeen kerätä käyttöstatistiikkaa. Analytiikkavälineiden valinnassa ja konfiguroinnissa tulee varmistua, etteivät ne paljasta asiointipalvelun käyttäjistä tietoja osapuolille, jotka voivat käyttää tietoja muuhun kuin niiden alkuperäiseen käyttötarkoitukseen.

Esimerkiksi pilvipalvelupohjainen analytiikkapalvelu tallettaa usein kaiken keräämänsä tiedon palveluntarjoajan pilvipalveluun ja sopimus- tai käyttöehtojen mukaan voi yhdistää tietoja muihin tietoihin. Asiointipalvelun omistajan on syytä arvioida, voidaanko palvelun käyttöä seurata riittävällä tarkkuudella vaihtoehtoisella ratkaisulla, jolla kerätty tilastotieto on rajattua ja tiedot eivät päädy asiointipalvelun ulkopuolelle.

5.3 Kontrolliympäristö

Tämä kappale tarkentaa edellä kuvattua tietoturvallisen asiointipalvelu rakennetta noudattavan asiointipalvelun suunnittelua yksittäisten tietoturvakontrollien osalta.

Kuva 4 sisältää yhteenvedon keskeisistä kontrolleista kattaen niin palvelun käyttäjät kuin sovellus- ja käyttöpalveluympäristönkin.



Kuva 4 Kontrolliympäristö

5.3.1 Yleiset kontrollit

Tässä kappaleessa kuvataan tietoturvakontrollit, jotka tulee huomioida kokonaisvaltaisesti asiointipalvelun suunnittelussa ja ylläpidossa.

Kontrolli	Toteuttamisohje
Saatavuus	Yhtenä asiointipalvelun suunnittelun keskeisenä lähtökohtana on palvelulta vaadittu saatavuustaso. Saatavuusvaatimuksia määritellessään palvelun omistajan tulee tunnistaa kaikki saatavuuteen vaikuttavat osatekijät ja huolehtia niiden saatavuudesta niin, ettei yksittäisiä heikkoja lenkkejä ole. Esimerkiksi poikkihallinnollisessa asioinnissa kaikkien asiointipalveluiden saatavuuden tulee olla yhdenmukainen, ja myös liitettyjen tukipalveluiden tulee toteuttaa olennaisesti samat saatavuusvaatimukset kuin itse asiointipalvelun. Palvelun eri osien erilaiset saatavuusvaatimukset, esimerkiksi avoimen datan liittymät, on syytä huomioida rakenteellisia ratkaisuja valittaessa (ks. Käyttöliittymien ja palvelurajapintojen eriyttäminen). Palvelun saatavuusajan ohella palvelun omistajan tulee määritellä poikkeamatilanteiden RPO- ja RTO-vaatimukset. Palvelutoimittajien vastuulla olevien palveluiden osalta sopimuksissa tulee määritellä vaatimukset häiriöiden ratkaisuajoille. VAHTI-ohjeet Toiminnan jatkuvuuden hallinta (VAHTI 2/2016) ja ICT-varautumisen vaatimukset (VAHTI 2/2012) tarjoavat lisäohjeistusta saatavuuden ja jatkuvuuden turvaamiseen.
Tiedon ja tietoliikenteen salaus	Salausratkaisut suojaavat luottamuksellista tietoa paljastumiselta ja muuntelulta tallennettaessa sitä tietovarastoissa ja siirrettäessä tietoja ei-luotetun tietoliikenneyhteyden ylitse. Asiointipalvelussa tulee huolehtia siitä, että käytetyt salausratkaisut ovat organisaation tietoturvaperiaatteiden ja käsiteltävien tietojen suojaustasoluokittelun mukaisia. Asiointipalvelun suunnittelussa tulee huolehtia asianmukaisesta tiedon salauksesta erityisesti seuraavissa tilanteissa: – Selaimen ja web-palvelimen välillä – Mobiili-/natiivisovellusten ja palvelurajapintojen välillä – Eri tietoverkkojen, ja tarvittaessa myös eri verkkosegmenttien, välillä Tietoliikenteen päästä päähän -salaaminen ei ole aina tarkoituksenmukaista, esimerkiksi tilanteissa, joissa sanomaliikenteelle on tarpeen suorittaa syntaktisia muunnoksia tai sisällönsuodatusta luotetun palvelun toimesta. VAHTI-ohjeet Ohje salauskäytännöistä (VAHTI 2/2015) ja Sisäverkko-ohje (VAHTI 3/2010) tarjoavat lisäohjeistusta salausratkaisujen valintaan ja tietoliikenteen suojaamiseen.
Tietoturvallisuuden valvonta	Palvelun omistajan tulee arvioida asiointipalvelun käyttötarkoituksen ja palvelun riskiarvion pohjalta, missä laajuudessa ja kuinka automatisoidusti asiointipalvelun tietoturvallisuutta on tarpeen valvoa. Valvonnan tarvetta on syytä tarkastella erityisesti seuraavista näkökulmista: 1. normaalista poikkeavan valtuutetun käytön havaitseminen, esimerkiksi a. viranomaiskäyttäjän tarpeettoman laaja arkaluonteisten henkilötietojen katselu tai työnkuvan vastainen tietojen katselu tai muokkaus b. asiakkaiden tavallisuudesta poikkeava tietojen katselu tai muokkaus, joka voi indikoida identiteettivarkautta c. ylläpitovaltuuksin, esimerkiksi tietovarastotasolla, suoritettu tietojen katselu, joka ei vastaa ylläpitäjän työnkuvaa. 2. verkkohyökkäysten havaitseminen, esimerkiksi tietoliikenteen normaalista käyttöprofiilista poikkeavat yhteydet tai protokollat, joiden avulla voidaan tunnistaa

Kontrolli	Toteuttamisohje
	esimerkiksi ulkoisesta IP-osoitteesta tehtävä tietomurto tai sisäverkon murretulta palvelimelta lähtöisin oleva haitallinen tietoliikenne. Valvonnan suunnittelussa ja toteutuksessa tulee kiinnittää huomioita erityisesti palvelun normaalikäytön mukaisen toiminnan määrittelyyn, lokienhallintaan ja poikkeamatilanteiden automaattiseen, sääntöpohjaiseen, havaitsemiseen ja reagoinnin mahdollistamiseen (esim. kriittiset toimet estetään ja ylläpitäjälle valvontahälytykset yrityksistä).
Lokienhallinta	Asiointipalvelun tulee tuottaa palvelussa tapahtumista ja tehdyistä toimenpiteistä riittävää lokitietoa ja noudattaa lokienkirjausketjuja lokisuunnitelmaan perustuen, jotta palvelun käyttöä on mahdollista valvoa ja normaalista poikkeava käyttö voidaan havaita sekä jälkikäteen osoittaa kiistämättömästi tapahtumat. Lokien muodostuksessa, keruussa ja hallinnassa tulee huolehtia erityisesti siitä, että: – eri osapuolten vastuut lokien muodostamisessa, keräämisessä ja hallinnassa on määritelty; esimerkiksi että asiointipalveluun liitetyt ulkoiset tukipalvelut ja toisen viranomaisen asiointipalvelut tuottavat tarvittaessa lokitietoja, jotka ovat tarvittaessa asiointipalvelun omistajan käytettävissä – lokitietoja ei kerätä tarpeettoman laajasti ja suunnittelematta vaan rekisterinpitäjän tarpeisiin ja teknisten vikatilanteiden havaitsemiseksi suunnitelmien mukaisesti – lokeihin ei kirjoiteta tietoturvallisuuden valvonnan kannalta tarpeetonta tietoa, esimerkiksi asiointipalvelussa käsiteltäviä arkaluonteisia henkilötietoja – lokitiedot on suojattu valtuudetonta muokkaamista vastaan, esimerkiksi o kopioimalla lokitiedot lähdejärjestelmistä ja -palvelimilta keskitettyyn lokienhallintajärjestelmään o eriyttämällä lokienhallintajärjestelmän käyttövaltuudet normaalista järjestelmäkäytöstä. Lisäohjeita lokienhallinnan toteuttamiseksi tarjoaa Lokiohje (VAHTI 3/2009).
Suojautuminen palvelunestohyökkäyksiltä	Suojautuminen asiointipalveluun kohdistuvilta palvelunestohyökkäyksiltä on haastava tehtävä. Erityisesti hajautetun volyymipohjaisen palvelunestohyökkäyksen (*volumetric attack*) erottaminen palvelun normaalista (tai ruuhka-ajan) käytöstä voi olla haasteellista. Palvelun omistaja voi kuitenkin varautua palvelunestohyökkäyksiin seuraavasti: – organisaatio kehittää kykyään tunnistaa sisäiset ja ulkoiset hyökkäykset, ja käytetyt tekniikat (ks. Tietoturvallisuuden valvonta) ja edellyttää vastaavaa kykyä myös palveluntarjoajiltaan – tunnetut protokollahyökkäykset (mm. *flooding*-hyökkäykset) estetään sovellus- ja käyttöpalveluympäristö tietoturvallisella konfiguroinnilla (mm. aika- ja nimipalveluiden konfigurointi ja kovennus) – organisaatio suunnittelee ennakolta menettelyt, joilla palvelunestohyökkäyksen vaikutuksia voidaan rajata; esimerkiksi julkisen internetverkon käyttöliittymän tilapäinen käytöstä poisto – organisaatio sopii ennakolta yhteistyömenettelyt (esimerkiksi tietojen luovutus ja viranomaiskontaktit) hyökkäystilanteessa tietoliikenneoperaattorin ja muiden yhteistyökumppaneidensa kanssa – tarvittaessa organisaatio sopii tietoliikenteen sisällönsuodatuksesta (*scrubbing*) tietoliikenneoperaattorin runkoverkossa. Yksityiskohtaisia ohjeita tarjoaa Tietoturvapoikkeamatilanteiden hallinta -ohje (VAHTI 2/2017).

5.3.2 Käyttäjät

Käyttäjille tarjottava ohjeistus muodostaa perustan asiointipalvelun tietoturvalliselle käytölle. Monia tietoturvauhkia voidaan ehkäistä tehokkaimmin vaikuttamalla käyttäjien toimintaan, opastamalla heitä toisaalta toimimaan vastuullisesti (mm. huolehtimaan päätelaitteidensa päivityksistä ja haittaohjelmasuojauksesta) ja toisaalta välttämään haitallisia toimintamalleja (mm. tunnistusvälineiden luovuttaminen toiselle henkilölle). Ohjeistusta laadittaessa tulee huomioida myös palvelun omistavan viranomaisen oma henkilöstö, joka voi toiminnallaan edesauttaa uhkien torjuntaa.

Palvelun omistajan tulee useimmissa asiointipalveluissa myös huolehtia käyttäjien luotettavasta yksilöinnistä ja tunnistaminen, käyttövaltuuksien hallinnasta – erityisesti viranomaiskäyttäjien ja ylläpitäjien kohdalla – sekä käytönaikaisesti valtuuttamisesta sekä asiakkaiden tahdonilmausten rekisteröinnistä ja jäljitettävyydestä.

Kontrolli	Toteuttamisohje
Tietoturvatietoisuuden kohentaminen	Asiointipalvelun omistajan tulee tarjota palvelun asiakkaille kattavat ohjeet palvelun tietoturvalliseen käyttöön. Ohjeistuksen on syytä kattaa vähintään seuraavat asiat: – Sähköisen asioinnin yleiset tietoturvakäytänteet, esimerkiksi o jaettujen päätelaitteiden turvallinen käyttö o asioinnissa käytetyt turvalliset sähköiset viestintäkanavat o palvelun lähettämät ilmoitukset mm. puolesta-asiointitilanteissa – Omien päätelaitteiden tietoturvallisuudesta huolehtiminen (mm. tietoturvapäivitykset); ohjeistusta voidaan täydentää palvelussa esimerkiksi näyttämällä eituettuja internet-selainversioita käyttäville asiakkaille kehote päivittää internetselain – Henkilökohtaisista tunnistusvälineistä huolehtiminen identiteettivarkauksien ehkäisemiseksi – Käyttäjään kohdistuvien huijaus- ja kalasteluyritysten tunnusmerkit; laajamittaisten kalastelukampanjoiden aikana asiointipalvelussa voidaan julkaista käyttäjille suunnattuja tiedotteita ja varoituksia – Sisältää selkeät toimintaohjeet ja yhteystiedot käyttäjän epäillessä asiointipalvelun väärinkäyttöä tai muuta tietoturvapoikkeamaa. Myös palvelun omistajan, palveluntuottajan ja palvelua kehittävän tahon henkilöstölle tulee tarjota tarvittavat ohjeet ja koulutus. Edellä lueteltujen asioiden lisäksi keskeisiä ohjeistettavia asioita ovat: – tietoturvapoikkeamien käsittelyprosessi ja menettelyt, joilla henkilöstö voi omalla toiminnallaan estää haittavaikutusten leviäminen organisaatiossa ja ilmoittaa poikkeamista tai niiden epäilyistä – sosiaalisen median käyttö ja siihen liittyvät uhkatekijät. Liite 6 sisältää esimerkin asiointipalvelun asiakkaille suunnatusta tietoturvaohjeesta. Henkilöstön tietoturvaohje (VAHTI 4/2013) puolestaan käsittelee henkilöstön tietoturvaohjeistusta.
Yksilöinti ja tunnistaminen	Asiointipalvelun tulee toteuttaa luotettava käyttäjien yksilöinti ja sähköinen tunnistaminen aina, kun: – palvelussa käsitellään ei-julkista tietoa, tai kun – palvelussa on mahdollista laittaa vireille asioita, joilla on huomattavaa oikeudellista tai taloudellista merkitystä, tai kun – asiointipalvelun anonyymiin käyttöön liittyy ilmeinen riski haitanteosta. Luku 6 tarjoaa ohjeita luonnollisen henkilön sähköisen tunnistusmenetelmän valintaan. Käyttäjien tunnistamista palvelurajapinnoissa on käsitelty kappaleessa 5.3.6 Palvelurajapinnat, integraatioratkaisut ja sanomaliikenne.

Kontrolli	Toteuttamisohje
	Esimerkki 1: Suomi.fi-tunnistaminen Kansalaiset kirjautuvat palveluun Suomi.fi-tunnistuspalvelussa käyttäen sähköistä henkilökorttia, verkkopankkitunnuksia, mobiilivarmennetta tai muuta tunnistuspalveluun liitettyä asetetun varmuustason mukaista tunnistusvälinettä. Keskitetty tunnistuspalvelu helpottaa asiointipalvelun suunnittelua ja käyttöä, kun käyttäjillä on jo valmiiksi hallussaan tunnistamiseen tarvittavat tunnistusvälineet. Suomi.fi-tunnistaminen -palvelu on kuvattu tarkemmin luvussa 7. **Esimerkki 2: organisaation omien viranomaiskäyttäjien tunnistaminen** Asiointipalvelun omistaja on eriyttänyt viranomaisten käyttöliittymän ja rajannut sen käytön sisäverkkoon. Viranomaiskäyttäjät tunnistetaan viranomaisen hallinnoimalla käyttäjätunnuksella ja salasanalla sekä sisäverkon päätelaitteilla. Salasanat noudattavat organisaation salasanapolitiikkaa.
Asiointivaltuuksien hallinta	Asiointipalvelun omistajan on suositeltavaa käyttää Suomi.fi-asiointivaltuudet -tukipalvelua yksityishenkilöiden ja yritysten puolesta-asioinnissa. Tukipalvelu mahdollistaa käytönaikaisen valtuuttamisen perustuen o kansallisissa perusrekistereissä ylläpidettäviin huoltajuussuhteita ja yritysten nimenkirjoitusoikeuksia koskeviin tietoihin, sekä o keskitettyyn kansalliseen valtuusrekisteriin luotaviin sähköisiin valtakirjoihin. Suomi.fi-asiointivaltuudet -palvelu on kuvattu yksityiskohtaisemmin luvussa 7.
	Esimerkki 1: sähköinen asiointi alaikäisen huollettavan puolesta Väestötietojärjestelmässä ajantasaisina ylläpidettävät tiedot alaikäisten kansalaisten huoltajista riittävät sosiaalihuollon asiointipalvelun puolesta-asioinnin tarpeisiin. **Esimerkki 2: valtakirjaan perustuva puolesta-asiointi** Asiointipalvelun asiakas valtuuttaa luotettavaksi katsomansa henkilön tai yrityksen hoitamaan puolestaan erikseen määriteltyjä asioita (esim. asuntokauppa tai yrityksen kirjanpito) luomalla Suomi.fi-asiointivaltuudet -palveluun sähköisen valtakirjan.
Tahdonilmausten rekisteröinti	Asiointipalvelun omistajalla voi olla lainmukainen velvoite rekisteröidä asiakkaan asiointipalvelussa tekemä tahdonilmaus tai suostumus asian vireillepanosta. Lisäksi asiointipalvelun omistajan tulee tarvittaessa kyetä näyttämään suostumus toteen. Erityistapaus suostumusten rekisteröinnistä on sellaisten henkilötietojen käsittely, joiden käsittely edellyttää erityistä rekisteröidyn suostumusta. Tällöin omistajan tulee saada asiakkaalta selkeä suostumus, joka on osoitettavissa ja tarvittaessa myös peruttavissa. Suostumusten hallinnassa olennaista on tunnistaa asiakas luotettavasta ja varmistua tahdonilmaukseen liittyvien tietojen alkuperästä ja eheydestä. Luku 7 käsittelee vaihtoehtoisia menetelmiä tahdonilmausten rekisteröintiin.
	Esimerkki: Vahva tunnistaminen ja rekisteröinti asiointipalvelussa Tahdonilmauksen tiedot kerätään asiointipalvelussa ja talletetaan palvelun tietovarastoon. Käyttäjät tunnistetaan vahvasti, jolloin tietojen alkuperää ei ole syytä epäillä. Lisäksi varmistetaan esimerkiksi sanomatiivisteitä ja asymmetristä salausta käyttäen tahdonilmaisun sisällön eheydestä ja siitä että tahdonilmaisun hyväksymistä ja sitä edeltävää henkilön tunnistamista koskeva tieto pystytään yhdistämään tahdonilmaisun sisältöön.

5.3.3 Päätelaitteet

Asiointipalveluita laajemmilla oikeuksilla käyttävien viranomaiskäyttäjien ja ylläpitäjäkäyttäjien päätelaitteiden tulee noudattaa palvelun omistajan määrittelemää päätelaitepolitiikkaa ja käyttää vain sallittuja laitteita ja yhteyksiä. Muun muassa laitteiden vakioinnin ja hallinnan avulla voidaan olennaisesti alentaa päätelaiteiden kautta asiointipalveluun välittyvien uhkien aiheuttamia riskejä.

Kontrolli	Toteuttamisohje
Päätelaitteiden suojaaminen	Asiointipalvelun omistajan tulee määritellä, millä päätelaitteilla sen oma – ja mahdollisuuksien mukaan myös muiden valtuutettujen tahojen – henkilöstö voi käyttää asiointipalvelua ja käsitellä sen sisältämiä tietoja. Tärkeimmät asiointipalvelun suunnittelussa tehtävät päätökset päätelaitteisiin liittyen ovat siten: o asiointipalvelussa käsiteltävien tietojen tunnistaminen, suojaustasoluokittelu ja tarkoituksenmukaiset eriyttämiset mm. asiointipalvelun ympäristöille ja käyttöliittymille o asiointipalvelun riskiarvio ja eri käyttötilanteissa käytettävien päätelaitteiden hallinnan taso suhteessa niiden käytön riskeihin o organisaation päätelaitepolitiikan linjaus siitä, mitä asiointipalvelun tietoja, toimintoja, asiointipalvelun vaiheita tai asiointipalvelun eri ympäristöjä on sallittua käsitellä vain tietyillä päätelaitteella (esim. sisäverkon asiointipalvelun tuotantoympäristöä on sallittua käsitellä vain oman ja valtuutettujen tahon hallinnoimilla päätelaitteilla, päätelaitepolitiikan mukaan, sekä julkisen internetverkon asiointipalvelun osaa on sallittu käsitellä kansalaisten päätelaitteilla). Päätelaitteiden tietoturvaohje (VAHTI-ohje 5/2013) tarjoaa yksityiskohtaisia tietoja päätelaitteisiin liittyvistä uhkatekijöistä ja ohjeita niiltä suojautumiseen.
	Esimerkki: Viranomaiskäyttö keskitetysti hallinnoiduilla päätelaitteilla Organisaatio sallii riskiarvioonsa perustuen asiointipalvelun viranomaisosan tietojenkäsittelyn vain vakioiduilla ja keskitetysti hallinnoimilla päätelaitteilla: – jotka on varustettu ajantasaisella haittaohjelmasuojauksella – joihin käyttäjät itse eivät voi asentaa kuin keskitetysti sallittuja ohjelmia – joilta ei voi käyttää organisaation turvattomiksi katsomia verkkopalveluita – jotka on varustettu hallintaohjelmistolla, joka mahdollistaa laitteen ohjelmistojen päivitykset, tarvittavat konfiguraatiot ja tyhjentämisen varkaus- tai katoamistilanteissa. Palvelun omistaja velvoittaa (mahdollisuuksien mukaan) myös muut viranomaisosaa tarvitsevat tahot noudattamaan samaa tai vastaavaa päätelaitepolitiikkaa.

Internetin kautta asiointipalvelua käyttävien asiakkaiden kohdalla asiointipalvelun omistajalla on hyvin rajalliset keinot vaikuttaa asiakkaiden omien päätelaitteiden tietoturvallisuuteen. Päätelaitteilla voi siten olla haavoittuvia käyttöjärjestelmä-, sovellus- ja internet-selainversioita ja ne voivat olla pahimmillaan haittaohjelmien saastuttamia eikä asioiva asiakas välttämättä ole tietoinen asiointipalvelun käytöstä. Asiointipalvelun omistajan tulee siksi pitää asiakkaiden päätelaitteita lähtökohtaisesti turvattomina ja keskeisenä uhkalähteenä asiointipalveluiden ja viranomaisen tietoteknisen ympäristön tietoturvallisuudelle.

5.3.4 Sovelluskerros

Asiointipalvelun toteutuksessa ja ylläpidossa tulee toteuttaa riittävät toimenpiteet sellaisten sovellushaavoittuvuuksien, konfiguraationvirheiden tai muiden tietoturvapuutteiden tunnistamiseksi ja ehkäisemiseksi, jotka voivat väärinkäytettyinä vaarantaa tietojen luottamuksellisuuden, eheyden tai palvelun saatavuuden.

Toteutuksen, operoinnin ja kehittämisen tietoturvallisten menettelyjen tulee kattaa palvelun koko elinkaari siten, että haavoittuvuuksien synty esimerkiksi uhkaympäristön muuttuessa tai palvelun merkittävissä muutostilanteissa on ehkäisty.

Kontrolli	Toteuttamisohje
Tietoturvallinen sovelluskehitys ja ylläpito	Verkkohyökkäykset ja haittaohjelmat hyödyntävät tyypillisesti verkkopalveluiden teknisen infrastruktuurin ja sovelluskomponenttien tietoturvahaavoittuvuuksia. Haavoittuvuuksien esiintymistä voidaan olennaisesti ehkäistä nivomalla tietoturvallisuuden varmentaminen kiinteästi asiointipalvelun sovelluskehitys- ja ylläpitoprosesseihin. Asiointipalvelu omistajan tulee huolehtia vähintään seuraavista asioista: – Palveluun kohdistuvat olennaiset uhkatekijät on tunnistettu osana palvelun riskianalyysiä, ja uhkia sekä tunnistettujen riskienhallintakeinojen riittävyyttä uudelleenarvioidaan säännöllisesti. – Palvelun kehittämisessä ja ylläpidossa sovelletaan määrämuotoisia prosesseja, joissa määritellään tietoturvallisuuden tehtävät, vastuut ja hyväksyntäkriteerit palvelun elinkaaren kaikissa vaiheissa: o kehityksen aikaiset toimet; esimerkiksi vertaisarvioinnit sekä arkkitehtuuri- ja koodikatselmoinnit o tietoturvatestaus osana hyväksyntätestausta, esimerkkeinä haavoittuvuusskannaus ja tunkeutumistestaus (penetraatiotestaus) o tietoturvallisuuden regressiotestaus merkittävissä muutostilanteissa o tuotantokäytön aikaiset toimenpiteet, esimerkiksi tuotantoympäristön säännöllinen haavoittuvuusskannaus o eri vaiheissa, tyypillisesti vähintään käyttöönoton yhteydessä, suoritettu riippumaton tietoturva-arviointi. Sovellushaavoittuvuuksien tunnistamisessa kannattaa tukeutua yleisesti tunnettuihin ja säännöllisesti päivitettäviin viitekehyksiin ja standardeihin, esimerkiksi OWASP Top 10 -haavoittuvuuslistaukset ja teknologiakohtaiset tarkistuslistat (esim. REST Security Cheat Sheet ja Web Service Security Cheat Sheet). Sovelluskehityksen tietoturvaohje (VAHTI 1/2013) sisältää yksityiskohtaisia ohjeita turvallisen sovelluskehityksen tueksi.
Asiakkaan luottamuksen vahvistaminen	Sähköisessä asiointipalvelun toteutuksessa tulee varmistaa, että asiointipalvelu herättää kokonaisuutena käyttäjien luottamusta. Keskeisessä osassa ovat palvelun käyttöliittymät, joiden osalta tulee varmistaa erityisesti seuraavat asiat: – Palvelun käyttökokemus on mahdollisimman yksinkertainen; asiointitapahtuman kulku on looginen ja käyttäjää opastetaan koko tapahtuman ajan – Palvelun URL-osoite ja palvelun nimi ovat loogisia; viittaavat palvelun omistavaan organisaatioon myös silloin, kun palvelua tuottaa ulkoinen palveluntarjoaja – Palvelu on tunnistettavissa aidoksi palveluksi nimensä ja tälle nimelle hankitun varmenteen (luotettavalta varmentajalta) perusteella – Rekisteriselosteet ja tietosuojaselosteet – ja mahdolliset yhteenvetotiedot suoritetusta tietoturva-arvioinneista – ovat vaivatta asiakkaiden saatavilla

Kontrolli	Toteuttamisohje
	– Palvelu toimii luotettavasti ja esimerkiksi virhetilanteiden käsittely on loogista – Asiointipalveluun liitetyt tukipalvelut ovat luotettavuudeltaan yhdenmukaiset itse palvelun kanssa; asiakkaita ei esimerkiksi pakoteta käyttämään tukipalveluita, joiden käyttö edellyttää vaikeaselkoisten käyttöehtojen hyväksymistä.
Asiakasviestinnän luottamuksellisuus	Palvelun tarjoajan tulee estää kaikessa sähköisessä tietojen vaihdossa ei-julkisen tiedon paljastuminen ulkopuolisille suojaamalla viestit riittävän vahvalla salausmenetelmällä (ks. Tiedon ja tietoliikenteen salaus) sekä itse asiointipalvelussa että sen ulkoisissa viestintäkanavissa ja tukipalveluissa. Ei-julkisen tiedon välittämiseen tulee käyttää ainoastaan sellaisia asiointipalvelun ulkopuolisia viestintäkanavia, joiden tietoturvallisuudesta palvelun omistaja voi varmistua. Erityistä varovaisuutta tulee noudattaa sähköpostin, pilvipalvelupohjaisten ja sosiaalisen median viestintäratkaisujen käytössä. Jos organisaatiolla on käytössään turvapostipalvelu, sitä voidaan käyttää myös luottamuksellista sisältöä sisältävien viestin tai liitteiden välittämiseen. Erityisesti arkaluonteisia henkilötietoja ei tule lähettää muuta kuin sovituilla, turvallisiksi määritetyillä tavoilla.
	Esimerkki: Kansalaisen Suomi.fi-palvelunäkymä ja Suomi.fi-viestinvälitys Asiointipalvelu hyödyntää Suomi.fi-palvelunäkymiä ja Suomi.fi-viestinvälityspalvelua luottamuksellisessa asiakasviestinnässä. Palvelunäkymät edellyttävät asiakkaiden vahvaa tunnistamista ja viestinvälityspalvelu huolehtii viestien salauksesta asiointipalvelun puolesta.
Tietoturvapäivitysten ja haavoittuvuuksien hallinta	Tietoturvapäivitysten laiminlyönti altistaa asiointipalvelun ja mahdollisesti siihen liittyvät palvelut haavoittuvuuksille. Tietoturvapäivitysten seuranta ja oikea-aikainen asentaminen madaltavat merkittävästi haavoittuvuuksia hyödyntävien väärinkäytösten todennäköisyyttä. Asiointipalvelun omistajan tulee tunnistaa asiointipalvelun kriittiset laitteet ja ohjelmistot, ja kartoittaa jatkuvasti niiden päivitystarvetta, esimerkiksi seuraamalla ja analysoimalla aktiivisesti julkaistuja haavoittuvuustiedotteita sekä suorittamalla säännöllisiä haavoittuvuusskannauksia. Saatavilla olevat tietoturvapäivitykset tulee asentaa viiveettä. Mikäli viiveetön päivittäminen ei ole jostain syystä mahdollista, palvelun omistajan tulee toteuttaa tarvittavat palvelua suojaavat kompensoivat menettelyt, esimerkiksi yksittäisen haavoittuvuuden paikkaaminen sovelluspalomuurilla, ja varmistaa, että päivitys suoritetaan myöhemmin.

5.3.5 Käyttöpalveluympäristö

Kontrolli	Toteuttamisohje
Tietoverkon turvallinen rakenne	Tietoverkkojen segmentoinnilla voidaan eristää tehokkaasti niin palvelun eri arkkitehtuurikerrokset toisistaan kuin itse palvelu siihen liitetyistä taustapalveluista, tukipalveluista ja muista asiointipalveluista (ks. Modulaarinen ratkaisuarkkitehtuuri). Asiointipalveluun liittyvät tietoverkkojen segmentit on eriytetty palomuurein ja tarvittaessa niitä täydentävin yhdyskäytäväratkaisuin, joilla on mahdollista rajoittaa, suodattaa ja valvoa segmenttien välistä tietoliikennettä vain sallittuun ja oikean muotoiseen liikennöintiin. Segmenttien välinen tietoliikenne tulee rajoittaa *whitelis-*

Kontrolli	Toteuttamisohje
	ting -periaatteen mukaisesti, jolloin ainoastaan erikseen määritellyistä lähteistä peräisin ja määriteltyihin kohteisiin olevat yhteydet ja määritellyt tietoliikenneportit- ja protokollat ovat sallittuja ja muu tietoliikenne on oletusarvoisesti estettyä. Julkiseen internet-verkkoon näkyvät komponentit tulee eriyttää DMZ-verkkoalueeseen. Verkon laitteet ja yhdyskäytäväratkaisut tuottavat lokitietoja, joita voidaan hyödyntää asiointipalvelun tietoturvallisuuden valvonnassa. Tietojen vaihtoa tiettyjen segmenttien välillä on joissain tapauksissa perusteltua valvoa ja rajoittaa erikoistuneilla sisällönsuodatusratkaisuilla (ks. Palomuuri- ja yhdyskäytäväratkaisut). Yksityiskohtaisia ohjeita teknisen käyttöpalveluympäristön suojaamisesta tarjoaa mm. Teknisen ICT-ympäristön tietoturvataso-ohje (VAHTI 3/2012).
Käyttöpalveluympäristön koventaminen	Asiointipalvelun palvelinkomponentit, käyttöjärjestelmät, ohjelmistot, sovellukset, tietoliikennelaitteet sekä hallintatyöasemat ja hallintayhteyksien muodostamisessa käytetyt laitteistot ja ohjelmistot on kovennettu. Palvelun toiminnan kannalta tarpeettomat mm. järjestelmäpalvelut ja oletus tunnukset on poistettu käytöstä.
Ei-tuotannollisten ympäristöjen ja tukipalveluiden suojaaminen	Asiointipalvelun tuotantoympäristön lisäksi myös ei-tuotannollisten ympäristöjen ja tukipalveluiden (esimerkiksi sähköiset ryhmätyötilat, versionhallinta ja komponenttikirjastot) suojaaminen valtuudettomalta katselulta ja muokkaamiselta on suunniteltava, sillä ne voivat tarjota hyökkääjille arvokasta tietoa muun muassa palvelun rakenteesta, suojausten toteutuksista ja haavoittuvuuksista sekä laajentaa siten palvelun hyökkäyspinta-alaa. Tarpeelliset suojaukset tulee määritellä ympäristön käyttötarkoituksen ja käsiteltävien tietojen perusteella. Yleisenä ohjeena: 1. Tarkkoja teknisiä dokumentaatioita ja suojausten ratkaisukuvauksia sisältävät työtilat, versionhallintajärjestelmät ja binäärikomponenttivarastot (*binary repositories*) tulee suojata samalla tavalla kuin tuotantojärjestelmä mm. pääsynhallinnan osalta. 2. Kehitys- ja testausympäristöissä tulee käyttää pääsääntöisesti tarkoitusta varten luotua testidataa, erityisesti henkilötietojen osalta. Testidatan luonnissa voidaan käyttää lähtökohtana tuotantodataa, joka on kuitenkin joko pseudonymisoitava (käsitteltävä niin, ettei tietoja voida enää yhdistää tiettyyn henkilöön ilman lisätietoja kuten salausavainta) tai anonymisoitava (käsiteltävä niin, ettei niitä voida enää yhdistää tiettyyn henkilöön lainkaan). Asiointipalvelun ylläpito tulee suorittaa ympäristössä, joka on suojattu uhkatekijöiltä vähintään yhtä hyvin kuin itse asiointipalvelu. Ylläpitohenkilöstön altistuminen haittaohjelmille, tietojen kalastelulle ja muille sosiaalisen hakkeroinnin menetelmille tulee minimoida esimerkiksi seuraavasti: 1. palvelua hallinnoidaan eriytetyllä tai erityissuojatulla hallintatyöasemalla 2. hallintayhteydet tuotantopalvelimille otetaan eriytetystä hallintaverkosta 3. ylläpidon etäyhteydet rajataan, salataan ja suojataan tarkoituksen mukaisesti 4. tietojen kalastelun ja haittaohjelmien levityksen estämiseksi hallintaympäristössä ei käytetä sähköpostia eikä ympäristöä käytetä internet-selailuun

5.3.6 Palvelurajapinnat, integraatioratkaisut ja sanomaliikenne

Sähköisten asiointipalveluiden liittäminen viranomaisen omiin taustajärjestelmiin, muihin asiointipalveluihin, kansallisin perusrekistereihin ja asioinnin tukipalveluihin voidaan toteuttaa usein vaihtoehtoisin tavoin. Tarkoituksenmukaisimman integraatioratkaisun valinta on aina tapauskohtaista ja siihen vaikuttavat mm. osapuolet (sisäinen vs. ulkopuolinen), integraation luonne (synkroninen vs. asynkroninen) ja suorituskykyvaatimukset (vasteajat ja läpäisykyky). Asiointipalvelu voi myös hyödyntää useampia tapoja integroitua eri tarpeisiin ja käyttötilanteisiin, esimerkiksi:

- Suomi.fi-palveluväylää integroituessaan kansallisiin sähköisen asioinnin tukipalveluihin
- Valtorin VIA-integraatiopalvelua integroituessaan muun valtionhallinnon sisäverkkojen tietojärjestelmiin
- REST-palvelurajapintoja arkkitehtuurikerrosten välisissä integraatioissa ja organisaation yhteiskäyttöisten mikropalveluiden käytössä.

Tieturvallisuuden näkökulmasta yhteiskäyttöisten integraatio- ja sanomaliikenneratkaisujen hyötyinä voidaan pitää mahdollisuutta toteuttaa ja testata mm. tieto- ja sanomaliikenteen salaus ja osapuolten tunnistaminen kertaalleen keskitetysti useiden asiointipalveluiden hyödynnettäviksi. Vaadittu tietoturvallisuuden taso voidaan saavuttaa myös asiointipalvelukohtaisissa integraatio- ja sanomavälitysratkaisuissa, mutta tällöin palvelun omistajan suunnittelu- ja laadunvarmistusvastuu korostuvat.

Kontrolli	Toteuttamisohje
Tunnistaminen palvelurajapinnoissa	Asiointipalvelun palvelurajapintoja käyttävät ulkoiset tietojärjestelmät tulee tunnistaa luotettavasti, kun rajapinnassa välitetään ei-julkista tietoa tai kun – tiedon ollessa julkista – sen alkuperästä tulee voida varmistua. Avoimen datan rajapinnoissa voidaan edellyttää käyttäjien rekisteröinti ja tunnistaminen, mikäli rajapinnan käyttöä halutaan seurata ja tarvittaessa rajoittaa käyttäjäkohtaisesti. Ulkopuolisen osapuolen käytön tunnistamisen tulee yleisessä tapauksessa perustua luotettavan tahon myöntämään yksilöivään *client*-varmenteeseen, ja varmenneavainten hallintamenettelyn tulee minimoida virheellisen tunnistamisen riski. Yhtenä vaihtoehtona on käyttää ulkoisissa integraatioissa integraatiopalvelua, esimerkiksi Suomi.fi-palveluväylää, jossa osapuolten tunnistaminen on osa palvelua. Myös organisaation sisäisissä integraatioissa, esimerkiksi asiointipalvelun arkkitehtuurikerrosten välillä, kutsuva osapuoli tulee aina tunnistaa modulaarisen arkkitehtuurin periaatteiden mukaisesti, jotta tietoturvallisuuden kerroksellisuus toteutuu. Tunnistusmenetelmän varmuustaso tulee näissä tapauksissa suhteuttaa muuhun kontrolliympäristöön. Tunnistaminen esimerkiksi web-palvelimen ja taustapalvelun palvelurajapinnan välillä voi perustua *shared secret* -avaimeen.
Valtuuttaminen palvelurajapinnoissa	Palvelurajapintoja käyttävien tietojärjestelmien käyttöä tulee rajoittaa käyttövaltuuksin samalla tavalla kuin henkilöiden oikeuksia asiointipalvelun käyttöliittymissä perustuen rajapintaa käyttävälle tietojärjestelmälle sallittuihin toimintoihin, rajapintaoperaatioihin ja tietoihin.
Luottamuksellisuus, eheys ja kiistämättömyys	Tiedon ja tietoliikenteen salausta tulee käyttää organisaation tietoturvaperiaatteiden mukaisesti, erityisesti välitettäessä ei-julkista tietoa suojaamattoman tietoliikenneyhteyden ylitse – esimerkiksi DMZ-vyöhykkeen ja taustapalveluiden välillä. Salaus ei välttämättä ole tarpeen esimerkiksi sovelluskerroksen ja tietovaraston välillä, edellyttäen, että tarvittava tietoliikenne pysyy samassa käyttöpalveluympäristössä ja kyseinen ympäristö on suojattu mm. valtuudettomalta pääsyltä. Ulkoisissa rajapinnoissa tiedon eheydestä voidaan varmistua esimerkiksi välitettävien sanomien sähköisellä allekirjoituksella. Asiointipalvelun palvelurajapintojen, integraatioiden ja sanomaliikenteen suunni-

Kontrolli	Toteuttamisohje
	telmallisella ja riittävällä lokituksella voidaan tarvittaessa jälkikäteen osoittaa kiistämättömästi esim. tietyn sanoman lähetyksen onnistuminen asiointipalvelusta.
Haitta-ohjelmasuojaus	Asiointipalvelun tarjoajan tulee varautua siihen, että ulkoisiin palvelurajapintoihin voi kohdistua haitallista verkkoliikennettä, joka voi olla seurausta esimerkiksi riittämättömästä syötetarkistuksesta palvelua kutsuvassa tietojärjestelmässä. Palvelurajapinnan toteutusteknologiaa valittaessa on syytä huomioida, että ilmaisuvoimainen kuvauskieli tai protokolla mahdollistaa myös laajemman kirjon haavoittuvuuksia. Esimerkiksi SOAP-protokolla mahdollistaa ei-rakenteista tietoa (kuvia, PDF-dokumentteja) sisältävien liitetiedostojen välityksellä levitettävät haittaohjelmat ja XML-injektiohyökkäykset. Palvelun suunnittelussa tulee huomioida toteutusteknologiaan liittyvät tyypillisimmät haavoittuvuudet ja suojautua sekä varautua uhkiin esimerkiksi yhdyskäytäväratkaisulla, haittaohjelmasuojauksin ja integraatioratkaisussa toteutettavalla sisällön suodatuksella.

5.3.7 Palomuuri- ja yhdyskäytäväratkaisut

Tietoverkkojen segmentointi on lähtökohtana kaikkien sähköisten asiointipalveluiden teknisessä suunnittelussa. Segmentoinnilla voidaan eristää tehokkaasti niin palvelun eri arkkitehtuurikerrokset toisistaan kuin palvelu siihen liitetyistä taustapalveluista, tukipalveluista ja muista asiointipalveluista (ks. Tietoverkon turvallinen rakenne). Segmentoinnissa hyödynnetään tyypillisesti palomuureja ja niihin integroituja lisäpalveluita.

Erityisesti julkisissa internetissä käytettävissä asiointipalveluissa, jotka kytkeytyvät suojaustason III taustajärjestelmiin, tulee lisäksi soveltaa yhdyskäytäväratkaisuja, joilla estetään ylemmän suojaustason tiedon kulkeutuminen matalamman suojaustason ympäristöön. Viestintäviraston Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista[4] ja ratkaisumalleista tarjoaa yksityiskohtaisia ohjeita ja esimerkkejä tätä tarkoitusta palvelevien hyväksyttyjen yhdyskäytäväratkaisujen suunnitteluun ja valintaan.

Modernien palomuurien ja yhdyskäytäväratkaisujen avulla voidaan lisäksi toteuttaa esimerkiksi seuraavia edistyneitä suojauksia:

- taltioida tietoliikennetapahtumia ja tilastotietoa tietoturvavalvonnan tueksi
- suodattaa palveluun kohdistuvaa verkkoliikennettä yhdyskäytävän kautta kulkevien tietoliikennepakettien sisältöä tarkastelemalla (ns. *deep packet inspection*, *DPI*) esimerkiksi sovellustason hyökkäysten tunnistamiseksi
- estää yksittäisten, tunnettujen sovellushaavoittuvuuksien hyväksikäyttö (ns. *web application firewall)*
- havaita ja estää tunkeutumisyrityksiä (*Intrusion Detection/Prevention System*, *IDS, IPS*)

Edellä mainittujen toimintojen toteuttaminen on syytä tehdä riskiarvion ja kustannushyötyarvioinnin perusteella.

[4] https://www.viestintavirasto.fi/attachments/Yhdyskaytavaratkaisuohje.pdf

Kontrolli	Toteuttamisohje
Tietoverkkojen yhteenliittäminen	Muiden organisaatioiden tietojenkäsittely-ympäristöjä tulee lähtökohtaisesti pitää ei-luotettuina. Liitoksessa tulee huomioida liitettävien vyöhykkeiden korkein suojaustaso ja niiden asettamat vaatimukset. Asiointipalvelun integraatiot muiden organisaatioiden tietojärjestelmiin tulee toteuttaa ensisijaisesti julkishallinnon yhteiskäyttöisten ratkaisujen kautta, jolloin voidaan hyötyä niiden sisäänrakennetuista tietoturvapalveluista ja välttyä kahdenvälisten *ad hoc* -integraatioiden mahdollisilta tietoturvahaavoittuvuuksilta. Keskeisiä yhteiskäyttöisiä integraatiopalveluita ovat: – Suomi.fi-palveluväylä, joka mahdollistaa julkishallinnon eri toimijoiden palveluiden tietoturvalliseen yhteen liittämisen ja korkeintaan suojaustason IV aineiston välittämisen. – VIA-integraatiopalvelu, jonka avulla virastot voivat siirtää tietoja joko oman organisaation tietojärjestelmien välillä tai omien tietojärjestelmien ja muiden organisaatioiden tietojärjestelmien välillä sekä toteuttaa integraatiossa mahdollisesti tarvittavat muunnokset. Kaupallisten tukipalveluiden integraatioissa tulee kiinnittää erityishuomioita tietoliikenneyhteyden monitorointiin ja sopimus- ja käyttöehtojen seurantaan. Muun muassa Katakri 2015 (I 01) -auditointityökalu sisältää yksityiskohtaisia ohjeita koskien verkkojen tietoturvallisesta yhteen liittämisestä.
Sisällönsuodatus	Perinteiset palomuurit (*statefull firewalls*) suodattavat tietoliikennettä ensisijaisesti IP-osoitteiden sekä tietoliikenneprotokollien ja -porttien perusteella. Edistyneet verkkohyökkäykset hyödyntävät kuitenkin yhä enenevässä määrin tekniikoita, joissa haitallinen liikenne naamioidaan sovelluksen normaaliksi käytöksi tai haittaohjelmat piilotetaan liitetiedostoihin, ja joita on siten vaikea havaita, saati ehkäistä, perinteisin palomuuriratkaisuin. Asiointipalvelun omistajan on syytä arvioida palvelun riskitaso ja alttius edistyneille hyökkäystekniikoille sekä tunnistaa näistä uhkatekijöistä asiointipalveluun ja koko organisaatioon aiheutuvat riskit. Mikäli riskin todennäköisyys ja haittavaikutukset sen toteutuessa arvioidaan merkittäväksi, verkkoliikenteen monitorointia ja suodattamista on syytä tehostaa edistyneillä sisällönsuodatusratkaisuilla.
	Esimerkki 1 Asiointipalvelun asiakkaat voivat välittää palvelussa opinto- ja työtodistuksia liitetiedostoina. Jos liitetiedostoja käsitellään sisäverkossa, haittaohjelmariskin minimoimiseksi liitetiedostot tarkistetaan haittaohjelmien varalta asiointipalvelusta eriytetystä skannauspalvelussa ennen niiden välittämistä viranomaisen taustajärjestelmiin. **Esimerkki 2** Asiointipalvelu suojataan internet-verkosta yhdyskäytäväratkaisulla hyödyntäen tietoliikennepaketteja analysoivalla ja suodattavalla palomuurilla (*deep packet inspection*, DPI) tai erillisellä verkkoliikenteen tunkeutumisen havainnointi-/estojärjestelmällä (Intrusion Detection/Prevention System, IDS/IPS). Tehostettu suodatus kohdistetaan myös palvelurajapinnan kautta tapahtuviin järjestelmäintegraatioihin. Näin voidaan varmistua tietojen eheydestä ja eristämisestä internetverkon tai palvelurajapintaa käyttävien tahojen tietyiltä uhkatekijöiltä.

6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

Tämä luku käsittelee käyttäjien tunnistamista, valtuuttamista ja asiointivaltuuksien hallintaa sähköisessä asioinnissa.

6.1 Johdanto

Useimmissa sähköisissä asiointipalveluissa vaatimuksena on palvelun käyttäjien yksilöinti ja tunnistaminen. Asiointipalvelun omistajan tehtävä on määritellä, kuinka luotettavaa tunnistamisen menetelmää palvelun käyttö edellyttää.

Tämä tunnistamiselta vaadittu *varmuustaso* tulee suhteuttaa ennen kaikkea palvelussa käsiteltävien tietojen luottamuksellisuuteen ja väärinkäytöksestä aiheutuviin riskeihin. Esimerkiksi asiointipalvelussa, jossa käsitellään henkilötietolaissa eriteltyjä arkaluonteisia henkilötietoja, tunnistamisen tulee perustua luotettavaksi katsotun menettelyn kautta rekisteröityyn käyttäjäidentiteettiin, joka todennetaan palvelun käyttöhetkellä moneen tunnistustekijään perustuvalla menetelmällä. Varmuustasoa määritellessään palvelun omistajan tulee huomioida kaikki palvelua käyttävät asiakastyypit (ks. Sähköisen asiointipalvelun määritelmä ja rajaus) ja käyttötilanteet.

Tyypillisesti palvelun kaikki asiakastyypit tunnistetaan saman varmuustason vaatimukset täyttävillä menetelmillä. Käytännön syistä eri asiakastyyppien tunnistamisessa voi kuitenkin olla tarkoituksenmukaista soveltaa teknisesti eri sähköisen tunnistamisen menetelmää, esimerkiksi:

- yksityishenkilöiden tunnistaminen pankkitunnisteilla, mobiilivarmenteella tai HST-kortilla
- viranomaisten tunnistaminen Väestörekisterikeskuksen myöntämällä organisaatiovarmenteella
- tietojärjestelmän tunnistaminen Väestörekisterikeskuksen tai muun luotettavan tahon myöntämällä järjestelmävarmenteella.

Edellä kuvattu lähtökohta kaikkien asiakkaiden tunnistamisen yhdenmukaisesta varmuustasosta ei päde kaikissa käyttötapauksissa. Esimerkiksi julkisissa tietopalveluissa kansalaisia ei ole yleensä tarpeen tunnistaa lainkaan, kun taas tietojen julkaisemisesta vastaavien viranomaiskäyttäjien luotettava tunnistaminen on tietojen laadun ja eheyden kannalta keskeistä.

Tunnistamisen ohella sähköisessä asioinnissa toistuu vaatimus tarkistaa luotettavasta lähteestä henkilön tai yrityksen valtuudet, valtakirjat ja oikeudet asioida sähköisesti toisen henkilön tai edustamansa yrityksen puolesta.

6.2 Sähköisen tunnistamisen menetelmän varmuustaso

Sähköisen tunnistamisen menetelmän varmuustaso luonnehtii menetelmän luotettavuutta henkilön esitetyn henkilöllisyyden toteamisessa. Mitä korkeampi varmuustaso, sitä todennäköisemmin asiointipalveluun kirjautuva käyttäjä on tosiasiassa henkilö, jolle kyseinen henkilöllisyys ja siihen liitetyt tunnistusvälineet on osoitettu. Tunnistusmenetelmän varmuustasoon vaikuttavat eteenkin seuraavat seikat:

- Sähköisen käyttäjäidentiteetin ja tunnistusvälineiden haku ja rekisteröinti
    - mistä lähteistä hakijan yksilöivät tunnistetiedot kerätään?
    - miten hakijan henkilöllisyys varmennetaan (ns. ensitunnistaminen)?
    - kuinka tunnistusmenetelmän käytön ehdot ja edellytykset ohjeistetaan hakijalle?
    - kuinka tunnistusvälineet luovutetaan hakijalle?
        - kuinka tunnistusvälineiden hallussapito on mahdollista rajata vain niiden hakijaan?
- Sähköisen tunnistusmenetelmän ominaispiirteet
    - todentamistekijöiden lukumäärä
    - suojaukset tunnistusvälineiden toisintamiselta ja väärentämiseltä
        - suojaukset hyökkäyksiä vastaan (mm. *guessing*- ja *replay* -hyökkäykset)

Edellä kuvattuja tunnistusmenetelmän varmuustasoon vaikuttavia tekijöitä on käsitelty yksityiskohtaisemmin liitteessä 5.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (tunnistuslaki) määrittellään vahva sähköinen tunnistaminen viittaamalla eIDAS-asetuksessa tarkoitetun korotetun varmuustason ja korkean varmuustason vaatimukset täyttäviin sähköisen tunnistamisen menetelmiin. Heikolle (matalan varmuustason tunnistamiselle) ei ole asetettu vaatimuksia tunnistuslaissa. Taulukossa 2 on esitetty eIDAS-asetuksen kolmiportaisen varmuustasoluokitus. Liite 5 sisältää yhteenvedon eIDAS-luokituksen varmuustasojen minimivaatimuksista.

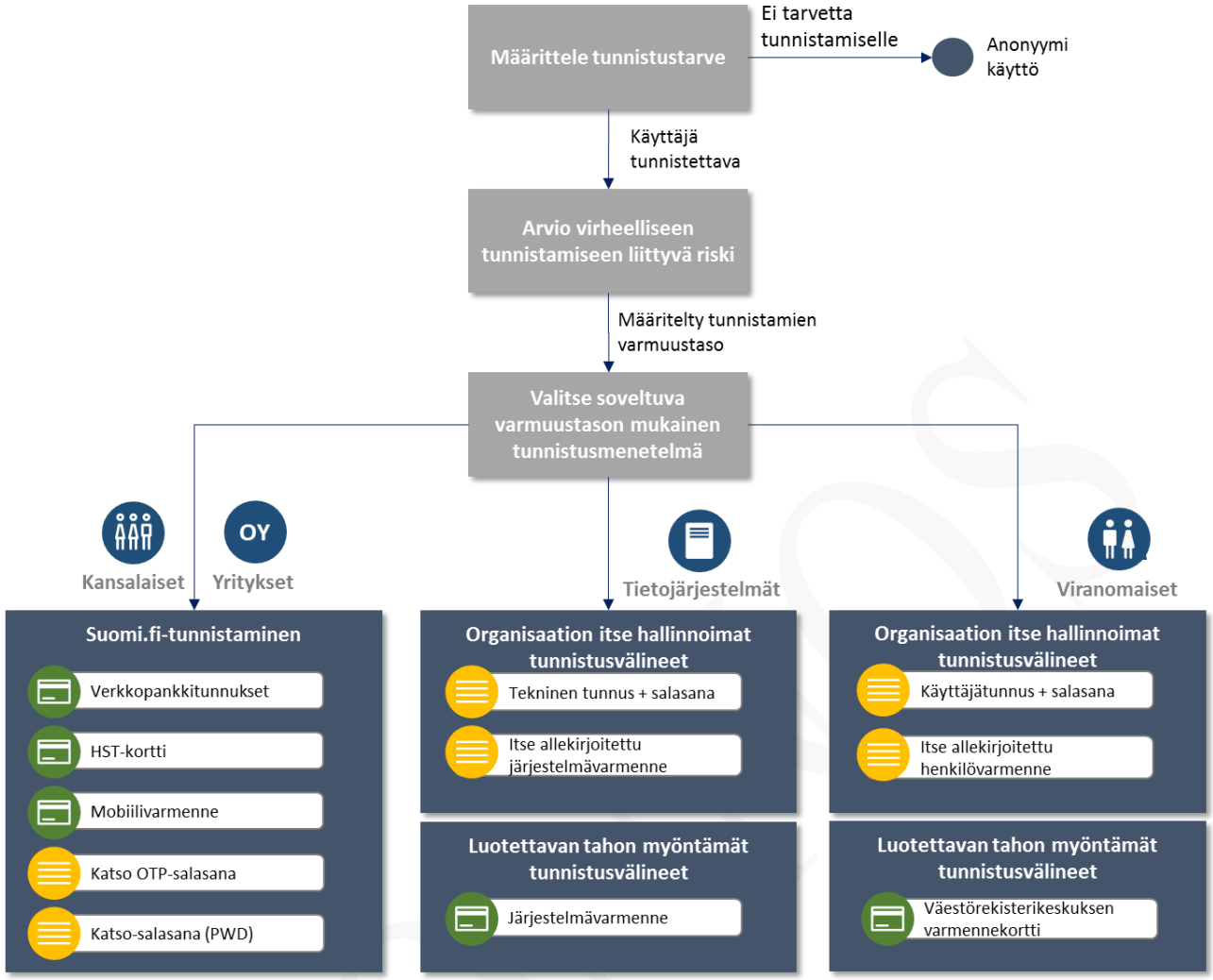
Varmuustaso	**Varmuustaso tarkoittaa sähköisen tunnistamisen menetelmää, joka…**	**Asiointipalvelun riskitaso**
Matala	– tarjoaa *rajoitetun luottamustason* henkilön väitetyn tai esitetyn henkilöllisyyden osalta, ja – *vähentää* henkilöllisyyden väärinkäytön ja muuttamisen riskiä	Virheelliseen tunnistukseen liittyy **kohtalainen** (moderate) riski
Korotettu	– tarjoaa *merkittävän luottamustason* henkilön väitetyn tai esitetyn henkilöllisyyden osalta, ja – *vähentää merkittävissä määrin* henkilöllisyyden väärinkäytön ja muuttamisen riskiä	Virheelliseen tunnistukseen liittyy **merkittävä** riski
Korkea	– tarjoaa *korkeamman luottamustason* henkilön väitetyn tai esitetyn henkilöllisyyden osalta *kuin korotetun varmuustason omaava sähköisen tunnistamisen menetelmä*, ja jonka – tarkoituksena on *estää* henkilöllisyyden väärinkäyttö ja muuttaminen	Virheelliseen tunnistukseen liittyy **korkea** (substantial) riski

Taulukko 2 Sähköisen tunnistemisen menetelmän varmuustasojen yhteenveto

Rekisteriä vahvan sähköisen tunnistamisen ja hyväksyttyjen luottamuspalveluiden tarjoajista ylläpitää Suomessa Viestintävirasto. Se ohjeistaa ja valvoo, että tunnistus- ja luottamuspalveluiden tarjoajat ovat luotettavia ja niiden toimintan ja tarjotut palvelut ovat tietoturvallisia. 1.5.2017 alkaen kansallisia tai eIDAS-notifioituja vahva sähköisen tunnistamisen menetelmiä ja palveluita voi tarjota vain tunnistamisen luottamusverkostoon liittynyt auditoitu toimija (ks. Suomi.fi-tunnistaminen).

6.3 Sähköisen tunnistamismenetelmän valinta

Kuva 5 havainnollistaa esimerkkiä päätöksentekoprosessista, jonka kautta asiointipalvelun omistaja voi valita palvelussa käytettävät sähköisen tunnistamisen menetelmät. Valintaa ohjaa ennen kaikkea asiointipalvelussa käsiteltävän ei-julkisen tietoaineiston luonne ja virheelliseen tunnistamiseen liittyvät riskit.



Kuva 5 Esimerkki sähköisen tunnistamisen menetelmän valintaprosessista

Päätöksenteon keskeiset vaiheet ovat:

- **Käyttäjien yksilöinti- ja tunnistustarpeen arviointi**
  - Asiointipalvelun omistajan tulee ensimmäiseksi arvioida ja määrittää, tarvitseeko palvelun käyttäjiä ylipäätään tunnistaa. Tunnistaminen on välttämätöntä erityisesti silloin, kun käyttäjä katselee tai käsittelee palvelussa ei-julkisia tietoja, voi laittaa palvelussa vireille asioita, joilla on oikeudellista tai huomattavaa taloudellista merkitystä, tai palvelun anonyymi käyttö voi aiheuttaa muuta haittaa tai vahinkoa[5]. Mikäli käyttäjiä ei ole tarpeen palvelun eri käyttökerroilla yksilöidä ja erottaa toisistaan, tunnistamiselle ei yleensä ole tarvetta.
- **Tunnistusmenetelmän varmuustason määrittely**
  - Kun tarve käyttäjien tunnistamiseksi on todettu, asiointipalvelun omistajan tulee arvioida henkilöllisyyden väärinkäyttöön ja muuttamiseen liittyvät riskit sekä palvelua tarjoavan organisaation että palvelun asiakkaiden kannalta. Riskien ollessa matalia, voidaan palvelussa käyttää matalan varmuustason (yhden todennustekijän) tunnistusmenetelmää. Tällöin puhutaan lähinnä henkilön yksilöinnistä, sillä matalan varmuustason menetelmän tarjoama luottamus käyttäjän todellisen henkilöllisyyden todentamisessa on

[5] Joissain tilanteissa saatavuuden turvaaminen voi edellyttää tunnistamisesta. Esimerkiksi avoimen datan liittymissä tunnistamisella voidaan kontrolloida rajapinnan kapasiteetin käyttöä ja ehkäistä palvelunesto-hyökkäyksiä.

rajallinen. Mikäli riski on merkittävä, tunnistamisessa tulee käyttää vahvaa tunnistamismenetelmää (korotettu tai korkea varmuustaso). Useissa tapauksissa, esimerkiksi arkaluonteisia henkilötietoja käsiteltäessä, vaatimus vahvasta sähköisestä tunnistamisesta määritellään laissa.

- **Soveltuvan tunnistusmenetelmän valinta**
  - Palvelun omistaja valitsee määritellyn varmuustason mukaisen ja palvelun toteutuksen kannalta tarkoituksenmukaisen sähköisen tunnistusmenetelmän tai tunnistusmenetelmät. Esimerkiksi asiointipalvelun yksityishenkilöille suunnatuissa käyttöliittymissä on perusteltua liittää palvelu Suomi.fi-tunnistamiseen. Viranomaisille suunnatuissa palvelun käyttöliittymissä käytetty tunnistusmenetelmä on tyypillisesti eri (ks. Viranomaiskäyttäjän tunnistaminen).

Taulukko 3 havainnollistaa esimerkkien kautta eri varmuustason tunnistusmenetelmien käyttöä asiointipalveluissa. Esimerkit ovat ohjeellisia ja saattavat sisältä useiden varmuustasojen valinnat, ja palvelua tarjoavan viranomaisen tuleekin aina päättää riskiarvioinnin pohjalta, millä varmuustasolla eri asiointipalvelun käyttötilanteissa käyttäjät tunnistetaan.

Esimerkki asiointipalvelusta tai käyttötilanteesta	**Anonyymi**	**Tunnistettu**		
		Matala varmuustaso	Korotettu varmuustaso	Korkea varmuustaso
Viranomaisen tiedottamispalvelu	x			
Asiakaspalaute ja kansalaisten osallistuminen	x	x		
Ei-luottamuksellinen vuorovaikutteinen asiointi		x		
Vireillepano		x[6]	x	
Luottamuksellinen vuorovaikutteinen asiointi			x	
Tietojärjestelmien välinen tietojenvaihto		x	x	(x)
Viranomaispalvelut		x	x	(x)

Taulukko 3 Esimerkkejä sähköisen tunnistusmenetelmän varmuustasosta eri tyyppisissä asiointipalveluissa ja käyttötilanteissa

6.4 Tunnistaminen ja valtuuttaminen eri käyttäjäryhmille

6.4.1 Yksityishenkilöt

Julkisen hallinnon viranomaisten on käytettävä asiointipalveluissaan yksityishenkilöiden tunnistamiseen Suomi.fi-tunnistamista, kun lainsäädäntö siihen velvoittaa ja palvelun riskitaso edellyttää vahvaa sähköistä tunnistamista. Julkisessa tehtävässä on suositeltavaa käyttää Suomi.fi-tunnistamista asiointitapahtumassa myös tilanteissa, joissa lainsäädäntö mahdollistaa Suomi.fi-tunnistamisen hyödyntämi-

[6] Tunnistuksessa voidaan käyttää vahvaa heikompaa (matalan varmuustason) tunnistusmenetelmää esimerkiksi, jos käyttäjän henkilöllisyys varmistetaan asiointiprosessin myöhemmässä vaiheessa. Vaikka käytännössä asioita pannaan vireille sähköpostilla, viranomaisen tehtävänä on varmistua, että henkilö tunnistetaan viimeistään siinä vaiheessa, kun hänelle esimerkiksi luovutetaan asiakkuutta koskevia tietoja.

sen ja palvelun riskitaso edellyttää vahvaa sähköistä tunnistamista. Suomi.fi-tunnistuspalvelu tarjoaa kansalaisten käyttöön vahvan tunnistusmenetelmän sekä muita tunnistusmenetelmiä kuin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (533/2016) tarkoitettua vahvaa sähköistä tunnistamista.

Asiointipalvelun omistaja määrittelee palvelussaan ainoastaan tunnistamisen varmuustason, jonka puitteissa Suomi.fi-tunnistaminen tarjoaa asiakkaille mahdollisuuden valita haluamansa tunnistusmenetelmän. Asiointipalvelun omistajan kannalta palvelun käyttöön liittyy monia etuja:

- omistajan ei tarvitse huolehtia eri tunnistusmenetelmien vaatimasta tekniikasta ja infrastruktuurista
- omistajan ei tarvitse huolehtia tunnistusvälineiden jakelusta
- Suomi.fi-tunnistamiseen myöhemmin liitettävät tunnistusvälineet tulevat automaattisesti asiointipalvelun asiakkaiden saataville.

Mikäli asiointipalvelussa on tarpeen mahdollista asiointi toisen henkilön puolesta, palvelun omistajan on suositeltavaa liittää asiointipalvelu Suomi.fi-asiointivaltuudet -palveluun. Suomi.fi-tunnistaminen ja Suomi.fi-asiointivaltuudet on kuvattu tarkemmin luvussa 8.

6.4.2 Viranomaiset

Kun toisen viranomaisorganisaation valtuuttama käyttäjä kirjautuu asiointipalveluun, palvelun on useimmiten varmistettava, paitsi käyttäjän henkilöllisyys, myös hänen yhteytensä organisaatioon ja valtuutensa toimia sen puolesta. Henkilökohtainen tunnistusväline ei siten yksinään riitä asiointiin.

Käyttäjän toimivalta hänen edustamassaan organisaatiossa voidaan varmistaa asiointipalvelussa seuraavin vaihtoehtoisin tavoin:

- **Tunnistaminen ja valtuuttaminen on eriytetty**
    - Tunnistaminen suoritetaan *henkilökohtaisella käyttäjäidentiteetillä ja tunnistusvälineillä*, joihin ei ole liitetty tietoja käyttäjän organisaatiosta tai toimivallasta. Asiointipalvelu tarkastaa *tunnistuksen jälkeen* käyttäjän ja organisaation välisen yhteyden sekä käyttäjän asiointivaltuudet erillisestä rekisteristä, johon ne on rekisteröity rinnakkaisen valtuushallinnan prosessin tuloksena. Valtuusrekisteri voi olla esimerkiksi keskitetty käyttäjähakemisto tai osa asiointipalvelun tietovarastoa.
- **Tunnistaminen ja valtuuttaminen tapahtuvat samanaikaisesti**
    - Tunnistaminen suoritetaan *työidentiteetillä* – esimerkiksi Väestörekisterikeskuksen myöntämällä organisaatiovarmenteella – joka sisältää henkilön tunnistetietojen lisäksi tiedon organisaatiosta, jossa hän työskentelee. Myös tässä vaihtoehdossa asiointipalvelun tulee tarkastaa käyttäjän asiointivaltuudet valtuusrekisteristä, mikäli asioinnin käyttötilanne edellyttää hienojakoisempaa valtuuttamista tiettyihin toimintoihin.

Molemmissa edellä kuvatuissa tapauksissa asiointipalvelun omistajan tulee päättää, millä identiteetillä (käyttäjäorganisaation hallinnoima vai kansallinen) viranomaiskäyttäjät tunnistetaan ja millaisen rekisteröinti- ja valtuutusprosessin kautta he saavat työtehtävissään tarvitsemansa valtuudet. Toisin kuin kansalaisilla ja yrityskäyttäjillä, käytettävissä ei ole keskitettyä kansallista valtuusrekisteriä, johon asiointipalvelu voitaisiin liittää.

Valtionhallinnon sisällä viranomaiskäyttäjien ja organisaation tunnistamisessa on mahdollista käyttää myös Virtu-luottamusverkostoa. Virtu toteuttaa ns. federoidun identiteetin periaatetta, jossa asiointipalvelua käyttävä organisaatio tunnistaa omat käyttäjänsä ja välittää käyttäjän ja organisaation yksilöintitiedot asiointipalveluun määrämuotoisessa SAML-tunnistusselosteessa. Tunnistaminen tapahtuu käyttäjäorganisaation hallinnoimilla tunnistusvälineillä. Tarvittaessa tunnistusselosteessa on mahdol-

lista välittää myös tietoa käyttäjän valtuuksista asiointipalveluun. Asiointipalvelun suunnittelijoiden on syytä huomioida, että vaikka toinen viranomainen olisikin osana Virtu-luottamusverkostoa, ei viranomainen välttämättä kuitenkaan käytä päätelaitteille tunnistautumiseen vahvaa tunnistamista vaikka organisaatioilla olisi käytössä vahvan tunnistautumisen ratkaisu ja välineet.

6.4.3 Yritykset

Kun asiointipalvelua käyttää yritys tai yrityksen edustaja – joko sen työntekijä tai muutoin valtuuttama henkilö – tunnistaminen voidaan toteuttaa seuraavilla vaihtoehtoisilla tavoilla:

– Tunnistaminen tapahtuu *yritykselle* rekisteröidyllä käyttäjäidentiteetillä ja tunnistusvälineillä. Palvelussa ei tällöin voida yksilöidä kirjautunutta henkilöä vaan ainoastaan yritys. Yrityskohtaiseen identiteettiin perustuvaa tunnistamista ei suositella esimerkiksi, jos palvelussa käsitellään henkilötietoja ja yksittäisen henkilön toimet palvelussa on kyettävä jäljittämään.
– Tunnistaminen tapahtuu *henkilökohtaisella* käyttäjäidentiteetillä ja tunnistusvälineillä. Identiteetti on lisäksi voitu liittää yrityksen Y-tunnukseen.

Molemmissa edellä kuvatuissa tapauksissa voi lisäksi olla tarpeen tarkistaa käyttäjän valtuudet asioida yrityksen puolesta asiointipalvelussa erillisestä valtuusrekisteristä.

Katso-tunnistus

Katso-tunnistus on yrityksiä varten luotu tapa tunnistautua viranomaisten sähköisiin palveluihin. Katso on asiointipalveluiden käytettävissä Suomi.fi-tunnistamisen kautta. Katsossa on mahdollista rekisteröidä kahden tyyppisiä tunnisteita: Katso-tunnisteita ja Katso-alitunnisteita.

Katso-tunniste on liitetty sekä yritykseen (Y-tunnus) että tunnuksen haltijaan (henkilötunnus). Tunnisteen haltija on tunnisteen saadakseen todistanut henkilöllisyytensä sähköisesti tai asioimalla henkilökohtaisesti Katso-asiakasrekisteröintipisteessä. Katso-tunnisteen haltija voi hallinnoida tunnisteeseen liittyviä tietoja (esim. salasana ja valtuutukset) Katso-palvelussa. Katso-tunniste voi sisältää pääkäyttäjäominaisuuden. Pääkäyttäjä voi luoda Katso-alitunnisteita sekä myöntää ja vastaanottaa valtuutuksia. Katso-tunniste sisältää käyttäjätunnuksen, salasanan ja kertakäyttösalasanan.

Katso-alitunniste on kytketty yritykseen muttei haltijansa henkilötunnukseen. Se soveltuu käytettäväksi tunnistamisessa tapauksissa, joissa yrityksen yksilöinti riittää eikä yrityksen puolesta asioivan henkilön tunnistaminen asiointipalvelussa ole tarpeen. Yrityksen nimenkirjoitusoikeudellinen pääkäyttäjä voi luoda Katso-alitunnisteita yrityksen työntekijöille. Katso-alitunnisteen haltija ei voi hallinnoida tunnisteeseen liittyviä tietoja (esim. salasana), vaan ne ovat ainoastaan pääkäyttäjän hallinnoitavissa. Katso-alitunnisteelle ei voi myöntää kaikkia Katso-järjestelmässä olevia rooleja. Katso-alitunniste sisältää käyttäjätunnuksen ja salasanan.

Taulukko 4 sisältää yhteenvedon Katson tarjoamista sähköisen tunnistamisen menetelmistä.

Tunnistus-menetelmä	Kuvaus	Tunniste
Katso PWD (*password*)	Yksilöivään käyttäjätunnukseen ja kiinteään salasananaan perustuva yhden todentamistekijän tunnistusmenetelmä	Katso-tunniste, Katso-alitunniste
Katso OTP (*one time password*)	Yksilöivään käyttäjätunnukseen, kiinteään salasananaan ja vaihtuvaan kertakäyttöiseen salasanaan perustuva kahden todentamistekijän tunnistusmenetelmä	Katso-tunniste

Taulukko 4 Katso-tunnistusmenetelmät

Asiointipalvelu voi käyttää Katso-palvelua myös pelkän asiointipalvelukohtaisen valtuustiedon kyselyyn Katso-palvelun tarjoaman Karva-roolikyselyrajapinnan kautta esimerkiksi silloin, kun yrityksen käyttäjä on tunnistettu HST-kortilla tai muulla menetelmillä, joka on yhdistetty käyttäjän henkilötunnukseen.

6.4.4 Tietojärjestelmät

Poikkihallinnollisen asioinnin yleistyessä lisääntyvät julkishallinnon sisällä tietojärjestelmien väliset integraatiot sekä julkishallinnon ja yritysten tietojärjestelmien väliset integraatiot. Näissä järjestelmäintegraatioissa tulee käyttää oletusarvoisesti vahvasti todennettua käyttäjäidentiteettiä sekä vahvaa sähköistä tunnistamista esimerkiksi seuraavien integraatiopalveluiden yhteydessä:

1. **Suomi.fi-palveluväylä** Asiointipalvelun järjestelmäasiakas tunnistetaan asiakasorganisaation liityntäpalvelimelle asennetun, Väestörekisterikeskuksen myöntämän varmenteen avulla. Varmenne on organisaatiokohtainen ja palveluväylään liittyville organisaatioille maksuton.
2. **VIA-integraatiopalvelu** Asiointipalvelun järjestelmäasiakas tunnistetaan VIA-integraatiopalveluun liitetyn asiakasjärjestelmän palvelukohtaisella varmenteella tai vaihtoehtoisesti sovittavalla tunnistamistavalla.

7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

Tässä luvussa käsitellään tilanteita, joissa sähköisen asiointipalvelun asiakkaan tai asiointitapahtumaan osallistuneen viranomaisen tekemä toimenpide tulee rekisteröidä ja näyttää tarvittaessa toteen. Asiointipalvelun omistajan tulee toteuttaa ratkaisut, joilla itse tapahtuma sekä siihen liittyvien tietojen alkuperä ja eheys voidaan varmistaa luotettavasti. Asiointitilanteesta riippuen vaatimus voidaan täyttää vaihtoehtoisin teknisin ratkaisuin, esimerkiksi sähköisellä allekirjoituksella.

7.1 Erityyppiset sähköiset allekirjoitukset

7.1.1 Sähköinen allekirjoitus (yleismääritelmä)

Sähköisellä allekirjoituksella tarkoitetaan eIDAS-asetuksen 3 artiklan 10 kohdan mukaan *”sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköisessä muodossa olevaan tietoon ja jota allekirjoittaja käyttää allekirjoittamiseen”*. Allekirjoituksen yleismääritelmään ei sisälly erityisiä aitouteen, alkuperään tai eheyteen liittyviä vaatimuksia, minkä vuoksi periaatteessa sähköpostin loppuun kirjoitettu nimikin on sähköinen allekirjoitus.

Allekirjoittaja on eIDAS-asetuksen mukaan luonnollinen henkilön tekemä. Siten esimerkiksi tietojärjestelmien tekemät tai oikeushenkilön yksilöivät, allekirjoitusta vastaavat toimenpiteet, eivät ole eIDAS asetuksen merkityksessä sähköisiä allekirjoituksia vaan pääsääntöisesti sähköisiä leimoja.

7.1.2 Kehittynyt sähköinen allekirjoitus

Kehittyneen sähköisen allekirjoituksen on eIDAS-asetuksen 26 artiklan mukaan täytettävä seuraavat vaatimukset:

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

Kehittynyt sähköinen allekirjoitus on määritelty tarkemmin eIDAS-asetuksen nojalla annetussa Komission täytäntöönpanoasetuksessa (EU) 2015/1506, eritelmien vahvistamisesta sellaisia kehittyneiden sähköisten allekirjoitusten ja kehittyneiden leimojen muotoja varten, jotka julkisen sektorin elinten on tunnustettava sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 27 artiklan 5 kohdan ja 37 artiklan 5 kohdan mukaisesti.

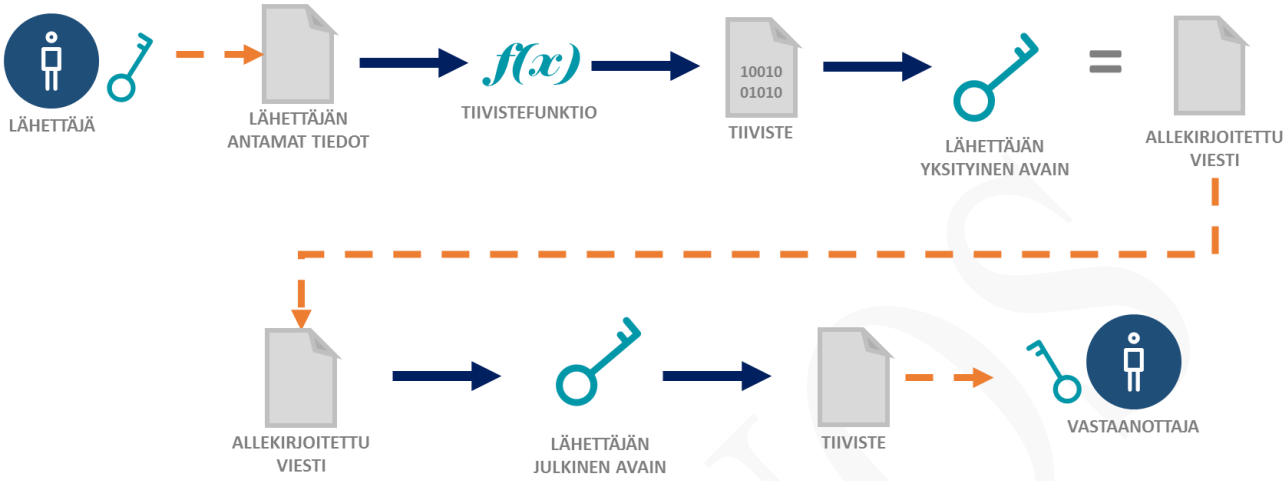
7.1.3 Julkisen avaimen tekniikka, ns. digitaalinen allekirjoitus

Digitaalista allekirjoitusta ei ole määritelty eIDAS-asetuksessa, mutta yleisesti sillä tarkoitetaan sähköistä allekirjoitusta, joka on luotu jotain salausmenetelmää – yleensä asymmetristä – käyttäen.

Julkisen avaimen tekniikkaan perustuva sähköinen allekirjoitus luodaan siten, että allekirjoitettavasta tiedosta muodostetaan (tiivistealgoritmillä) tiiviste, joka salataan avainparin yksityisellä avaimella. Salattu tiiviste tallennetaan allekirjoitetun tiedon tai sähköisen asiakirjan yhteyteen tai välitetään muulla tavoin tiedon vastaanottajalle. Vastaanottaja purkaa tiivisteen salauksen avainparin julkisella avaimel-

la, muodostaa uudelleen viestin tai asiakirjan tiedoista tiivisteen ja vertaa sitä allekirjoitukseen liitettyyn tiivisteeseen. Viestin sisältö on muuttumaton, mikäli tiivisteet ovat samat.

Virhe. Viitteen lähdettä ei löytynyt. havainnollistaa asymmetriseen avainpariin perustuvaa sähköisen allekirjoituksen periaatetta.



Kuva 6 Kehittyneen sähköisen allekirjoituksen toimintaperiaate

Asymmetriseen salaukseen perustuvan sähköisen allekirjoituksen käyttökelpoisuuden kannalta olennaista on, että tiedon vastaanottaja voi vaivattomasti yhdistää allekirjoituksen allekirjoittajaan, purkaa tiivisteen salauksen ja sitä kautta varmistua välitettyjen tietojen eheydestä. Hyvin toteutetun sähköisen allekirjoituksen suunnittelussa tulee huomioida esimerkiksi seuraavat allekirjoitusmenetelmään, -varmenteeseen ja varmentajaan (*certificate authority, CA*) liittyvät seikat:

1. Avaintenhallinta on järjestetty siten, että allekirjoituksen voi luoda ainoastaan taho, jolle allekirjoitusvarmenne on myönnetty. Tämä edellyttää yksityisten avainten teknisen suojaamisen lisäksi myös käyttäjien huolellisuutta yksityisen avaimen eli allekirjoituksen luomistietojen käsittelyssä. Esimerkiksi allekirjoituksen luomistiedot sisältäviä toimikortteja ja PIN-koodeja ei tule luovuttaa muiden henkilöiden käyttöön.

2. Vastaanottajalla tulee olla käytettävissään avainparin julkinen avain sekä keino tarkistaa varmenneketjun eheys aina juurivarmentajaan asti. Helpoiten tämä tapahtuu siten, että allekirjoittajan julkinen avain liitetään allekirjoitettuun asiakirjaan.

3. Allekirjoituksessa käytetään luotettaviksi katsottujen varmentajien myöntämiä varmenteita.

4. Allekirjoituksen toteutuksessa on huomioitu vaatimukset allekirjoituksen säilytysajalle. Sähköinen allekirjoitus on pystyttävä validoimaan sen luontihetkellä, mutta myös myöhemmin riippuen siitä, miten kauan allekirjoitus on pystyttävä näyttämään toteen.

Yksityiskohtaisempaa tietoa sähköisestä allekirjoituksesta tarjoaa Ohje salauskäytännöistä (VAHTI 2/2015).

7.1.4 Hyväksytty sähköinen allekirjoitus

Hyväksytyllä sähköisellä allekirjoituksella tarkoitetaan eIDAS-asetuksen 3 artiklan 12 kohdan mukaan: *”kehittynyttä sähköistä allekirjoitusta, joka on luotu hyväksytyllä sähköisen allekirjoituksen luontivälineellä ja joka perustuu sähköisten allekirjoitusten hyväksyttyyn varmenteeseen*”.

On huomattava, että hyväksytyn sähköisen allekirjoituksen määritelmään sisältyy kolme elementtiä:

- Sen on täytettävä edellä kuvatut kehittyneelle sähköiselle allekirjoituksella asetetut vaatimukset
- Sen on oltava luotu hyväksytyllä sähköisen allekirjoituksen luomisvälineellä
- Sen on perustuttava (hyväksytyn luottamuspalveluntarjoajan myöntämään) hyväksyttyyn varmenteeseen.

Hyväksyttyjä luottamuspalveluntarjoajia on Suomessa ainoastaan Väestörekisterikeskus (sen organisaatiovarmenteet, kansalaisvarmenteet ja terveydenhuollon ammattivarmenteet).

Hyväksytyn allekirjoituksen luomisvälineen on täytettävä eIDAS-asetuksessa ja sen nojalla säädetyt vaatimukset ja välineen vaatimustenmukaisuuden on oltava sertifioitu jäsenvaltion nimeämän tahon toimesta.

7.2 Sähköisesti annettujen suostumusten, muiden tahdonilmausten sekä viranomaispäätösten eheyden ja alkuperän varmistaminen

7.2.1 Sähköisen allekirjoituksen oikeusvaikutukset

Yleissäännös sähköisen allekirjoituksen oikeusvaikutuksista (eIDAS-asetuksen 25 artikla) kuuluu seuraavasti:

1. Sähköisen allekirjoituksen oikeusvaikutuksia ja käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sillä perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksyttyjen sähköisten allekirjoitusten vaatimuksia.
2. Hyväksytyllä sähköisellä allekirjoituksella on oltava samanlaiset oikeusvaikutukset kuin käsin kirjoitetulla allekirjoituksella.
3. Yhdessä jäsenvaltiossa myönnettyyn hyväksyttyyn varmenteeseen perustuva hyväksytty sähköinen allekirjoitus on tunnustettava hyväksytyksi sähköiseksi allekirjoitukseksi kaikissa muissa jäsenvaltioissa.

Erityislainsäädäntöön saattaa sisältyä tästä poikkeavia määritelmiä oikeusvaikutuksista.

7.2.2 Sähköisen allekirjoituksen tai sitä vastaavan eheyden ja alkuperän osoittamistavan valinta

Suomessa varsinaisia allekirjoitusvaatimuksia sisältyy lainsäädäntöön hyvin vähän.

Milloin laissa edellytetään allekirjoittamista, on tarkasteltava kyseisen säännöksen sisältöä ja tarkoitusta sekä arvioitava, millaisen varmuustason edellyttämää sähköistä allekirjoitusta on käytettävä. Ellei erityistä säännöstä allekirjoituksen laadusta ole, tulee sovellettavaksi eIDAS asetuksen 25 artikla, jonka mukaan hyväksytty sähköinen allekirjoitus vastaa käsin kirjoitettua allekirjoitusta mutta miltään muultakaan sähköiseltä allekirjoitukselta ei saa evätä merkitystä pelkästään siksi, että se on sähköisessä muodossa.

Mikäli hallinnossa asiointia koskevassa lainsäädännössä ei ole vaadittu tietynlaista allekirjoitusta, vaan yleisesti allekirjoitusta, tulee allekirjoituksen valinta Suomessa arvioitavaksi sillä perusteella, mitä pi-

detään riittävän luotettavana tapana osoittaa myöhemmin tietyn henkilön tahdonilmaisun tms. olemassa olo.

Mikäli laissa ei edellytetä allekirjoittamista eikä palvelun omistajalla ole ennestään valmiuksia sähköisen allekirjoituksen käyttöönotolle, voidaan esimerkiksi tahdonilmausten rekisteröinnissä katsoa riittäväksi kompensoiva menettely, jolla hälvennetään epäilys tietojen alkuperästä ja eheydestä. Tällöin asiointipalvelun suunnittelussa on varmistuttava seuraavista seikoista:

- käyttäjät on tunnistettu luotettavasti
- tapahtuman tarkka ajankohta on jäljitettävissä
- tapahtuma voidaan jäljittää ja toteennäyttää vielä pitkänkin ajan kuluttua. Säilytysaikavaatimus johdetaan tarvittaessa viranomaisen toimintaa säätelevästä lainsäädännöstä.
- tietojen muuttumattomuus on turvattu kaikissa sähköisen tiedonkäsittelyn vaiheissa, mukaan lukien arkistointi ja pitkäaikaissäilytys
- tapahtuman toteennäyttäminen on vaivatonta, etenkin jos on odotettavissa, että se joudutaan suorittamaan usein ja säännöllisesti (esim. vastineet asiakkaiden tietopyyntöihin).

Sähköistä asiointia hallinnossa koskevan yleislain eli sähköisestä asioinnista viranomaistoiminnassa annetun lain 9 §:n mukaan vireillepanossa ja asian muussa käsittelyssä vaatimuksen kirjallisesta muodosta täyttää myös viranomaiselle toimitettu sähköinen asiakirja eikä asiakirjaa tarvitse täydentää allekirjoituksella, jos asiakirjassa on tiedot lähettäjästä eikä asiakirjan alkuperäisyyttä tai eheyttä ole syytä epäillä.

On kuitenkin otettava huomioon, että viranomaisella on velvollisuus huolehtia henkilötietojen suojasta, hallinnon asiakkaan muusta oikeusturvasta ja että viranomaisen on yleensäkin varmistettava riittävä tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa.

Vaikka lainsäädännössä ei nimenomaisesti edellytettäisi allekirjoittamista, voidaan sähköistä allekirjoitusta (tai vastaavaa tarkoitusta palvelevaa yhdistettyä tunnistusta ja tietojärjestelmän allekirjoitusta) hyödyntää sen varmistamiseksi, että pystytään myöhemmin osoittamaan tietyn henkilön tahdonilmaisun olemassaolo. Kiistämättömästi toteen näytettäviä tapahtumia sähköisessä asioinnissa ovat tyypillisesti:

- asiakkaiden tahdonilmaukset, suostumukset ja hyväksynnät
- asiakkaiden lähettämät lakisääteiset ilmoitukset (esimerkiksi tullaustoiminnassa)
- toisen viranomaisen tietojärjestelmästä vastaanotetun sanoman alkuperä ja eheys
- asiakkaita koskevien viranomaispäätösten vahvistaminen allekirjoittamisella.

Viranomaispäätösten vahvistamisesta on erikseen säädetty sähköisestä asioinnista viranomaistoiminnassa annetun lain 16 §:ssä siten että viranomaisen on allekirjoitettava asiakirja kehittyneellä sähköisellä allekirjoituksella tai muuten sellaisella tavalla, että asiakirjan alkuperäisyydestä ja eheydestä voidaan varmistautua.

Edellä todetusta voidaan päätellä, että, ellei erityislainsäädännössä ole muuta säädetty (esimerkiksi vaadittu kehittynyttä tai hyväksyttyä allekirjoitusta taikka sallittu koneellinen allekirjoitus) yleisesti ottaen hallinnossa asioinnissa on käytettävä riittävän tietoturvallisia ja luotettavia tapoja asiakirjan alkuperän ja eheyden varmistamiseksi sekä varmistettava, että alkuperä ja eheys ovat osoitettavissa niin kauan kuin oikeustoimi tai muu tapahtuma on pystyttävä näyttämään toteen.

7.3 Esimerkkejä tavoista toteuttaa sähköinen allekirjoitus tai muu tahdonilmaisun kiistämättömyyttä sen antamiseen liittyvien tietojen eheyttä tukeva ratkaisu

7.3.1 Hallinnossa asioivan suostumuksen tai muun tahdonilmaisun rekisteröinti

Suostumukset ja muut tahdonilmaukset voidaan rekisteröidä asiointipalvelun käyttöliittymissä, joiden suojaamisessa on noudatettu tässä ohjeessa kuvattua viitearkkitehtuuria, esimerkiksi seuraavasti:

1. Toteuttamalla sähköisen allekirjoittamisen toiminto osana asiointipalvelua siten, että palvelu liittää esim. sanomatiivisteitä ja asymmetristä salausta hyödyntäen yhteen tiedon asiakkaan vahvasta tunnistamisesta sekä tahdonilmaisun sisällöstä ja sen antamisesta palvelussa – ja tallentaa nämä tiedot.
2. Toteuttamalla sähköisen allekirjoittamisen toiminto osana asiointipalvelua siten, että palvelun asiakkaat voivat luoda allekirjoituksia välineillä, jotka tukevat riittävän luotettavaa sähköistä allekirjoitusta.

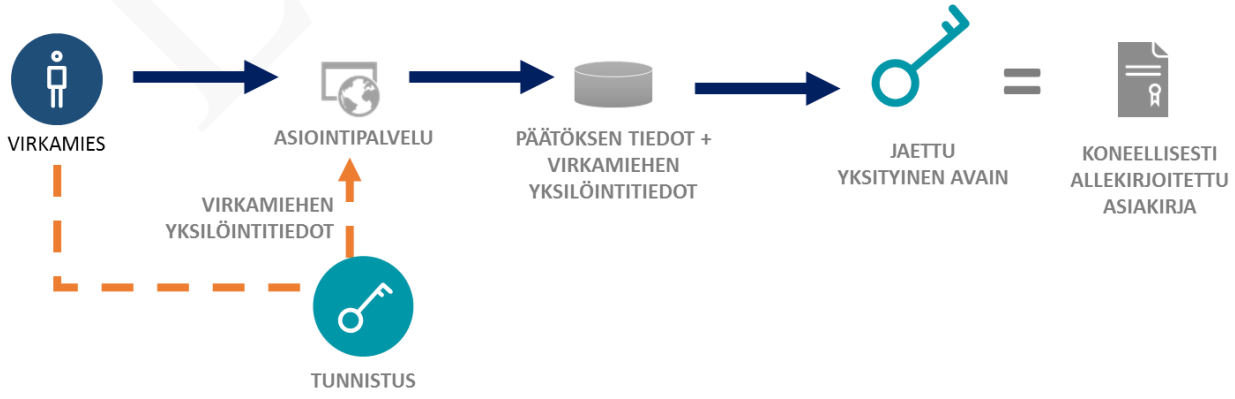
7.3.2 Viranomaispäätösten allekirjoittaminen

Kuten edellä on todettu, hallinnossa asiointia koskevan yleislain mukaan viranomaisen tekemät päätökset tulee (ellei erikseen muuta ole säädetty) allekirjoittaa kehittyneellä sähköisellä allekirjoituksella tai muuten sellaisella tavalla, että asiakirjan alkuperäisyydestä ja eheydestä voidaan varmistautua.

Kehittynyt sähköinen allekirjoitus voidaan toteuttaa esimerkiksi Väestörekisterikeskuksen myöntämillä allekirjoitusvarmenteen sisältävillä henkilökohtaisilla virkakorteilla, joille tallennettu allekirjoitusvarmenne sisältää yksilöintitiedot sekä viranomaisesta että kortin haltijasta. Virkakorttien käyttöön viranomaisopäätösten allekirjoituksessa liittyy kuitenkin tekijöitä, joilla on vaikutusta sähköisen asiointipalvelun toteutukseen sekä käyttöönotto- ja käyttökustannuksiin:

– Kaikilla päätöksiä tekevillä virkamiehillä tulee olla henkilökohtainen varmenteellinen virkakortti
– Virkakortti edellyttää allekirjoitustoiminnallisuuden teknistä toteutusta asiointipalvelussa tai asiointipalvelun liittämistä ulkoiseen sähköisen allekirjoitustoiminnon tarjoavaan tukipalveluun
– Allekirjoitus saattaa hidastaa asiointitapahtumaa; asiointipalvelun suunnittelussa on syytä arvioida tämän merkitys asioinnin sujuvuudelle.

Vaihtoehtoisesti silloin kun koneellisen allekirjoituksen käytöstä on erikseen säädetty, viranomaispäätökset voidaan allekirjoittaa koneellisesti keskitetyssä allekirjoituspalvelussa, jossa allekirjoitus tapahtuu henkilökohtaisen varmenteen sijaan esimerkiksi palveluvarmenteella. Koneellista allekirjoitusta (vrt. sähköinen leima) käytettäessä viranomaisen tulee kuitenkin huolehtia virkamiehen riittävän luotettavasta tunnistamisesta ja tapahtuman lokikirjausketjusta asiointipalvelussa, koska palveluvarmenteella tehty sähköinen allekirjoitus ei yksilöi viranomaispäätöksen tehnyttä virkamiestä. *Kuva 7* havainnollistaa koneellisen allekirjoituksen periaatetta.



Kuva 7 Viranomaispäätösten koneellisen sähköisen allekirjoituksen periaate

Viranomaispäätösten allekirjoittaminen koneellisesti sisältää seuraavat vaiheet:

1. Virkamies kirjautuu asiointipalveluun luotettavalla tunnistusmenetelmällä
2. Virkamies laatii asiakasta koskevan päätöksen. Palvelu tallentaa viranomaispäätöksen olennaiset tiedot sekä päätöksen tehneen henkilön yksilöintitiedot tietovarastoon.
3. Allekirjoituspalvelu luo taustalla päätöksen tiedoista sähköisen allekirjoituksen jaetulla, luotettavaksi katsotun tahon myöntämällä palveluvarmenteella.

Koneellisesti allekirjoitettu asiakirja voidaan tallentaa pitkäaikaissäilytykseen soveltuvaan tietovarastoon, esimerkiksi viranomaisen asianhallintajärjestelmään tai sähköiseen arkistopalveluun.

7.3.3 Viranomaisten välisen tiedonvaihdon eheyden ja alkuperän varmistaminen

Julkisen avaimen tekniikkaa (tiivistefunktiot ja asymmetrinen salaus) voidaan käyttää sanomatasolla myös viranomaisten välisessä tiedonvaihdossa tietojen eheyden ja alkuperän varmistamiseksi. Tällöin käytetään yleensä viranomaiselle (sen tietylle palvelimelle/tietojärjestelmälle) myönnettyjä varmenteita ja niihin liittyviä avainpareja, jotka jaetaan koneellisesti.

Esimerkiksi Valtorin VIA-integraatiopalvelun ja Suomi.fi-palveluväylän välityksellä integroitujen järjestelmien välillä välitettävä sanomat allekirjoitetaan ja aikaleimataan sähköisesti. Integraatiopalvelu lisää sanomiin tietylle tietojärjestelmälle myönnetyllä yksityisellä avaimella salatut tiivisteet, joilla taataan alkuperäisen vastinkumppanin identiteetti.

8 Sähköisen asioinnin kansalliset tukipalvelut

Tässä luvussa on kuvattu hallinnon yhteiset sähköisen asioinnin tukipalvelut, joiden tavoitteena on parantaa julkisten asiointipalveluiden saatavuutta, laatua, tietoturvallisuutta sekä edistää julkisen hallinnon toiminnan tehokkuutta ja tuottavuutta.

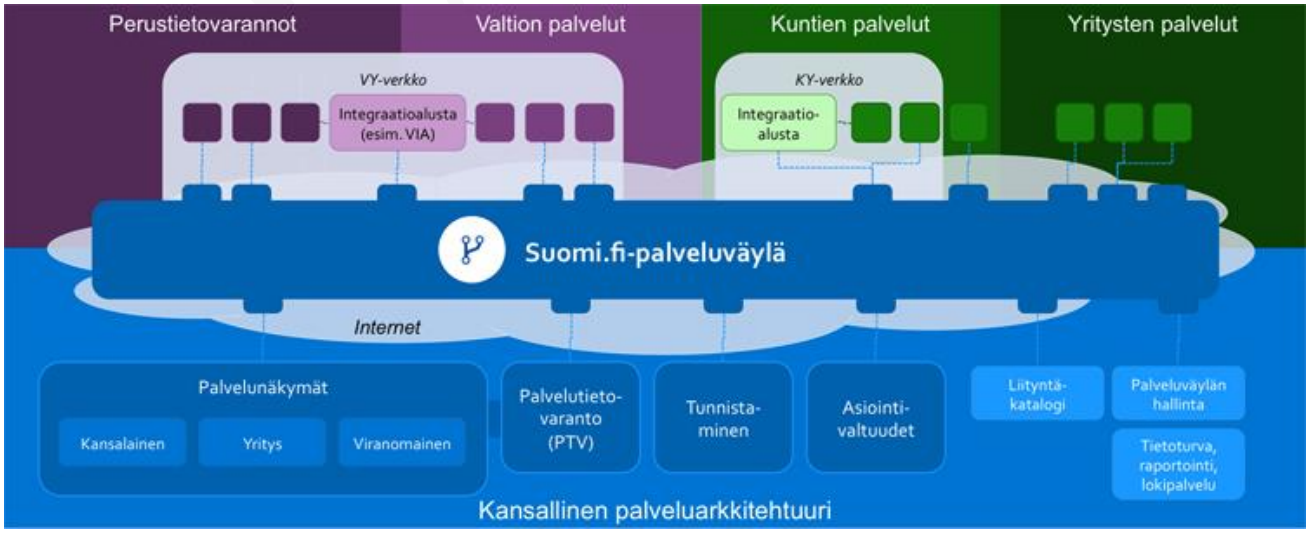
Tukipalvelut, palveluiden tuottamiseen liittyvät tehtävät, niiden käytön edellytykset sekä velvollisuudet ja oikeudet palveluiden käyttöön on määritelty laissa hallinnon yhteisistä sähköisen asioinnin tukipalveluista. Lain määrittelemät tukipalvelut ja niiden käyttövelvollisuuden alkamisajankohta on esitelty oheisessa taulukossa. Tässä ohjeessa esitellään taulukossa *kursivoidut* tukipalvelut.

Tukipalvelu	Palveluntuottaja	Käyttövelvoite alkaa viimeistään
Suomi.fi-asiointivaltuudet	Väestörekisterikeskus	-
Suomi.fi-palvelunäkymät	Väestörekisterikeskus	1.7.2017
Suomi.fi-palvelutietovaranto	Väestörekisterikeskus	1.7.2017
Suomi.fi-palveluväylä	Väestörekisterikeskus	15.7.2016
Suomi.fi-tunnistaminen	Väestörekisterikeskus	1.1.2018[7]
Suomi.fi-viestinvälitys[8]	Valtori	1.7.2017
Suomi.fi-karttapalvelu	Maanmittauslaitos	-
Verkkomaksamisen palvelu	Valtiokonttori	1.1.2018

Taulukko 5 Hallinnon yhteiset sähköisen asioinnin tukipalvelut

Palveluiden järjestäminen keskittyy pääsääntöisesti Väestörekisterikeskukseen. Tukipalveluiden käyttö on julkishallinnolle maksutonta. Osa hallinnon tukipalveluista on myös yksityisten yritysten käytettävissä, millä pyritään edistämään yksityissektorin sähköisen asioinnin kehitystä.

Taulukko 5 kuvastaa tilannetta tämän ohjeen julkaisuhetkellä. Sähköisen asioinnin järjestämisestä vastaavien tahojen on syytä seurata aktiivisesti tukipalveluiden kehittymistä.



[7] Velvoite ei koske vahvaa heikompia sähköisen tunnistamisen menetelmiä.
[8] Palvelu siirtyy Väestörekisterikeskuksen vastuulle 1.9.2017.

Kuva 8 Kansallinen palveluarkkitehtuuri

8.1 Oikeudet ja velvoitteet tukipalveluiden käyttöön

Tukipalveluita koskeva laki määrittelee julkishallinnolle ja yrityksille paitsi oikeuksia myös velvoitteita tukipalveluiden käyttöön. Tukipalveluiden laaja käyttöoikeus koskee julkishallintoa ja sekä julkishallinnon hallinnollisia tehtäviä itsenäisesti hoitamaan asetettuja tahoja. Velvoite käyttää tukipalveluita on rajattu suppeammin koskemaan vain osaa julkishallinnon viranomaisista (Taulukko 5). Yksityisellä sektorilla on rajoitettu käyttöoikeus tukipalveluihin riippuen organisaation luonteesta ja sen suorittamasta tehtävästä.

Tukipalvelua käyttävä organisaatiot	**Oikeus / velvoite**
Julkishallinto	
– Valtion hallintoviranomaiset ja virastot – Laitokset ja liikelaitokset – Kunnalliset viranomaiset niiden hoitaessa laissa niille säädettyjä tehtäviä – Tuomioistuimet ja muut lainkäyttöelimet	Velvoite käyttää seuraavia tukipalveluita: – Palvelunäkymät – Palvelutietovaranto – Palveluväylä – Tunnistaminen (vahvan tunnistamisen osalta) – Viestinvälitys – Verkkomaksamisen palvelu
Laissa säädetyn julkisen hallintotehtävän hoitamiseksi: – Julkisen hallinnon viranomaiset (mukaan lukien velvoitetut) – Itsenäiset julkisoikeudelliset laitokset – Eduskunta virastoineen – Valtioin talousarvion ulkopuoliset rahastot – Julkista hallintotehtävää itsenäisesti hoitamaan asetetut tahot[9] Kunnalliset viranomaiset ja kuntien yhteistyöelimet voivat käyttää palveluita myös muissa tehtävissään.	Oikeus käyttää kaikkia sähköisen asioinnin tukipalveluita
Yksityinen sektorin toimijat	
Lakiin perustuvan sopimuksen nojalla tai muulla perusteella julkista tehtävää hoitava taho	Oikeus käyttää toiminnassaan kaikkia tukipalveluita lukuun ottamatta seuraavia, joiden tarjoamisesta päättää tapauskohtaisesti kyseisen palvelun tuottaja: – Tunnistaminen – Viestinvälitys – Verkkomaksamisen palvelu
Yksityiset yhteisöt, säätiö ja elinkeinonharjoittajat	Oikeus käyttää toiminnassaan seuraavia palveluita: – Asiointivaltuudet – Palvelunäkymät – Palelutietovaranto – Palveluväylä – Avoindata.fi

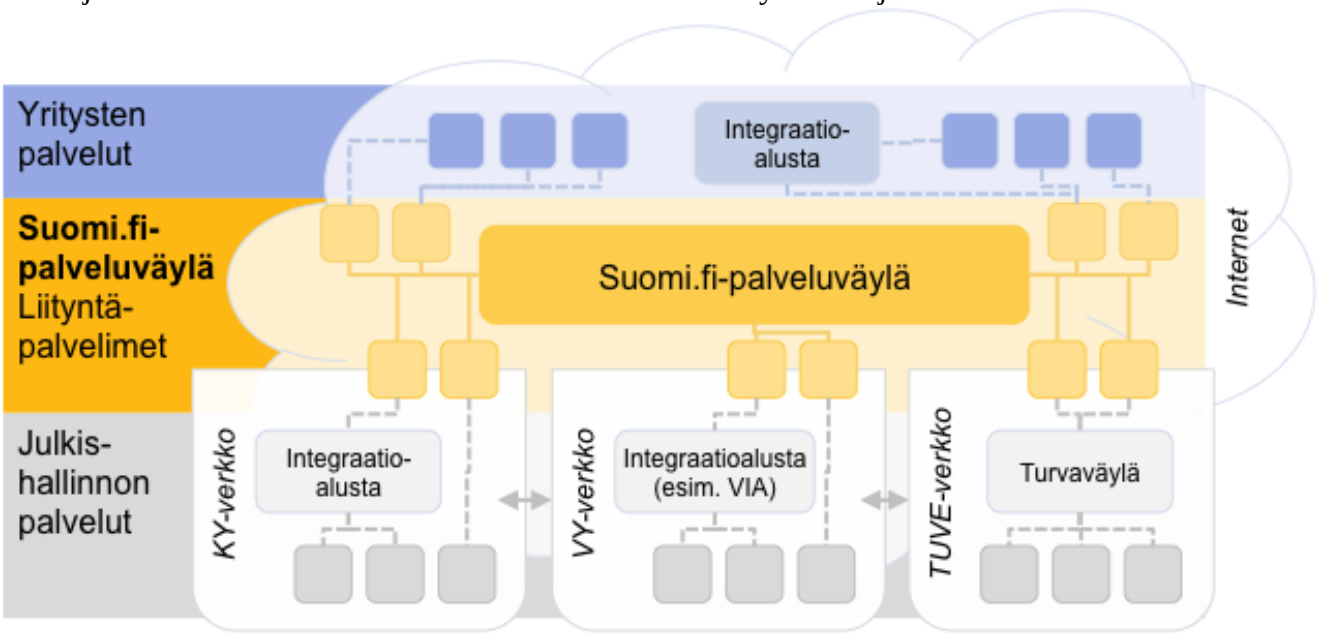
Taulukko 6 Tukipalveluiden käytön velvoitteet ja oikeudet

[9] Lailla, lain nojalla annetulla asetuksella tai lain nojalla annetulla valtion hallintoviranomaisen päätöksellä

Kun organisaatiolla on velvoite käyttää tukipalvelua, sen on otettava palvelu käyttöön laissa säädettyjen siirtymäsäännösten mukaisesti[10].

8.2 Suomi.fi -palveluväylä

Suomi.fi-palveluväylä on julkishallinnon yhteiskäyttöinen tiedonvälityskanava, joka mahdollistaa eri palveluita ja tietolähteitä yhdistelevien asiointipalvelukokonaisuuksien rakentamisen. Palveluväylä tarjoaa vakioidun ja tietoturvallisen tiedonsiirtokerroksen, jonka välityksellä käyttäjäorganisaatiot voivat siirtää ja luovuttaa tietoturvallisesti tietovarantoihinsa sisältyviä tietoja.



Kuva 9 Palveluväylän toimintaperiaate

Palveluväylään liittyäkseen organisaatio tarvitsee liityntäpalvelimen, jonka kautta tietojen vaihto muiden palveluväylään liittyneiden organisaatioiden kanssa reitittyy. Palveluväylä vastaa liittyneiden organisaatioiden ja niiden käyttämien liityntäpalvelinten todentamisesta ja muodostaa näin ollen liittyjistä koostuvan luottamusverkoston.

Suomi.fi-palveluväylän osana tarjottava *liityntäkatalogi* tuo kokonaisuudessa mukana olevien palveluiden rajapinta- ja sisältötiedot kaikkien saataville ja käytettäviksi. Liitynnän tekemisen jälkeen oman asiointipalvelun kehittämisessä voidaan hyödyntää kaikkia Suomi.fi-palveluväylään integroituja tietolähteitä ja palvelukomponentteja.

8.2.1 Soveltuvat käyttötilanteet

Suomi.fi-palveluväylä on suunnattu sekä julkishallinnon organisaatioille että yksityisen sektorin organisaatioille, jotka jakavat tietoa julkishallinnon kanssa. Palveluväylä soveltuu ensisijaisesti synkroniseen, tapahtumapohjaiseen tiedonvälitykseen. Asiointipalvelun suunnittelussa on syytä arvioida Suomi.fi-palveluväylään liittymistä erityisesti, kun yksi tai useampi seuraavista reunaehdoista täyttyy:

- asiointipalvelun omistaja hallinnoi rekistereitä tai tietovarantoja, joita muut viranomaistahot tai yritykset voivat hyödyntää toteuttaessaan omia sähköisiä asiointipalveluitaan
- tiedonsiirtotarve on synkroninen sanomaliikenne (vrt. eräajona tapahtuva massasiirto)
- asiointipalvelun omistavalla organisaatiolla on lain asettama velvoite käyttää palveluväylää
- siirrettävä tietoaineisto on julkista tai luokiteltu korkeintaan suojaustasolle IV

[10] Viranomaisen käyttövelvoitteesta on mahdollista hakea poikkeusta vain, jos muun palvelun käyttö on välttämätöntä teknisestä, toiminnallisesta, kustannustehokkuuteen tai tietoturvallisuuteen liittyvästä syystä.

- asiointipalvelu käyttää muita Suomi.fi-tukipalveluita – esimerkiksi Suomi.fi-palvelunäkymiä - jotka edellyttävät palveluväylään liittymistä
- olemassa olevia teknisiä ratkaisuja ei voida käyttää organisaatioiden väliseen tiedonsiirtoon esimerkiksi tietoturvallisuuteen liittyvien puutteiden vuoksi

8.2.2 Standardinmukainen tietoturvallisuus

Palveluväylä tarjoaa asiointipalveluille tietoturvallisen alustan synkronisten järjestelmäintegraatioiden toteuttamiseksi. Oheinen taulukko sisältää palveluväylän olennaiset ominaisuudet sähköisen asioinnin tietoturvallisuuden kannalta.

Tietoturvaominaisuus	Kuvaus ja hyödyt
Vakioitu tiedonsiirtotapa	Suomi.fi-palveluväylä määrittää vakioidun SOAP-protokollaan perustuvan synkronisen tavan tarjota liityntöjä ja käyttää niitä. SOAP mahdollistaa rakenteisen tiedon välittämisen XML-muodossa ja ei-rakenteisen tiedon välittämisen SOAP-liitteinä.
Tietojen alkuperän ja eheyden varmentaminen	Palveluväylän tietoliikenne reititetään liityntäpalvelinten kautta. Palveluväylä huolehtii osoitteiden hallinnasta ja sanomien reitityksestä. Rekisteröinnin yhteydessä liityntäpalvelimille asennetaan Väestörekisterikeskuksen myöntämät palvelin- ja allekirjoitusvarmenteet, joita käytetään liityntäpalvelinten tunnistamiseen ja sanomien sähköiseen allekirjoitukseen.
Tietojen ja palveluiden näkyvyys	Organisaation tarjoamien rajapintojen näkyvyys palveluväylässä on rajattavissa käyttötarkoituksen mukaisesti vain valtuutetuille osapuolille. Määritykset tehdään palveluväylän liityntäkatalogissa.
Tiedon luottamuksellisuuden suojaaminen	Palveluväylä mahdollistaa suojaustason IV aineiston siirtämisen edellyttämän yhteystason suojauksen.
Allekirjoitettujen ja aikaleimattujen sanomien lokitus	Väestörekisterikeskuksen tarjoama liityntäpalvelinohjelmisto sisältää palveluväylässä välitettävien, aikaleimattujen sanomien lokituksen sekä otsake- että sisältötasolla.

8.2.3 Tarkistuslista asiointipalvelun omistajalle

Suomi.fi-palveluväylän ajantasainen dokumentaatio, mukaan lukien liittymisohjeet, on saatavilla osoitteessa https://esuomi.fi/palveluntarjoajille/palveluvayla/. Alla on listattu keskeisimmät asiointipalveluun suunnittelussa huomioitavat asiat:

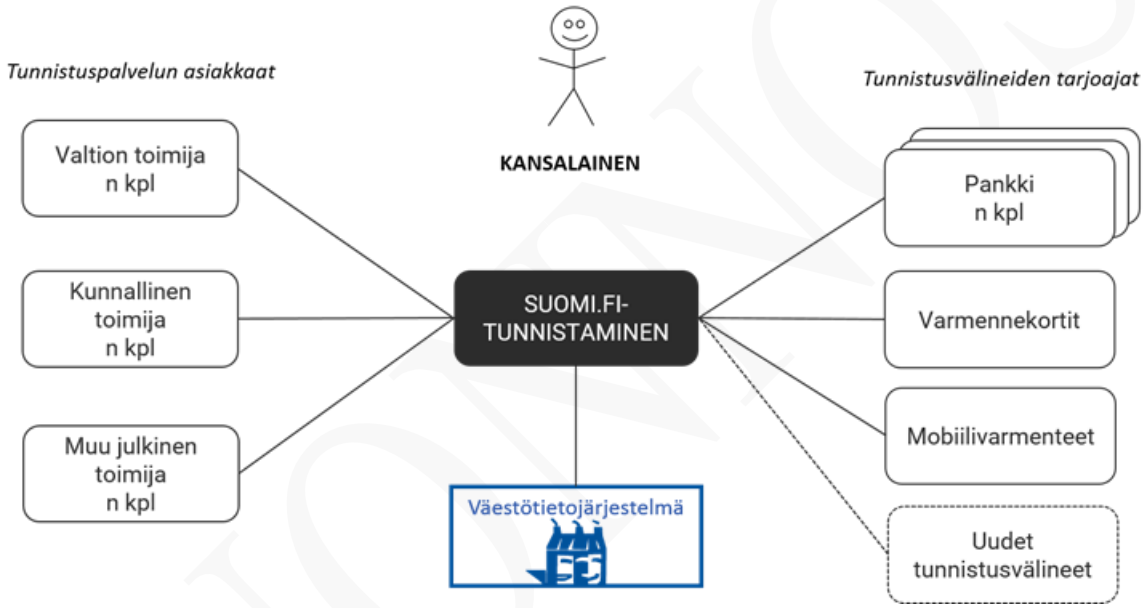
- Asiointipalvelun liityntärajapinnat tulee olla mahdollista toteuttaa SOAP-protokolalla. Muilla tekniikoilla toteutetut rajapinnat tulee muuntaa SOAP-muotoon.
- Liityntäpalvelinten mitoituksessa tulee sanomaliikenteen suorituskykyvaatimukset
- Liityntäpalvelimilla tulee olla käytössä aikaleimojen edellyttämät tarkat aikapalvelut.

8.3 Suomi.fi-tunnistaminen

Suomi.fi-tunnistaminen mahdollistaa luonnollisen henkilön sähköisen tunnistamisen asiointipalveluissa kattavalla, eri varmuustasojen mukaisella tunnistusvälinevalikoimalla sekä kertakirjautumisen tunnistuspalveluun liitettyjen asiointipalveluiden välillä. Tunnistuspalveluun voidaan liittää kaikki julkishallinnon sähköiset asiointipalvelut (ks. Oikeudet ja velvoitteet tukipalveluiden käyttöön).

Väestörekisterikeskus ylläpitää tunnistamispalvelun tuottajana tunnistusvälinevalikoimaa ja vastaa mahdollisista sopimuksista tunnistusvälineiden tarjoajien kanssa. Kaikki tunnistusvälineet tarjotaan yhdenmukaisen teknisen rajapinnan kautta asiointipalveluiden käyttöön.

Viestintävirasto vastaa Suomi.fi-tunnistamiseen liitettyjen tunnistusvälineiden luokittelusta kansallisiksi tai eIDAS-notifioiduiksi vahvoiksi sähköinen tunnistamisen välineiksi (ks. Sähköisen tunnistamisen menetelmän varmuustaso). Asiointipalvelun omistaja määrittelee, minkä varmuustason tunnistamista se palvelussaan edellyttää. Tunnistuspalvelu rajaa tunnistusvälineet tämän tason vaatimusten mukaisiin tunnistusvälineisiin.



Kuva 10 Suomi.fi -tunnistuspalvelun toimintaperiaate

Tämän ohjeen julkaisuhetkellä palveluun on liitetty seuraavat Viestintäviraston hyväksymät vahvat sähköisen tunnistamisen välineet:

- Pankkien verkkopankkitunnukset (TUPAS-tunnukset)
- DNA:n, Elisan ja TeliaSoneran tarjoamat mobiilivarmenteet
- Väestörekisterikeskuksen myöntämä HST-henkilökortti.

Lisäksi Suomi.fi-tunnistuspalvelu tarjoaa asiointipalveluiden käyttöön muita tunnistusmenetelmiä, esimerkiksi Katso-tunnukset.

8.3.1 Soveltuvat käyttötilanteet

Suomi.fi-tunnistaminen on suunnattu julkishallinnon sähköisille asiointipalveluille. Se tarjoaa asiointipalvelujen käyttöön sekä vahvoja että vahvaa heikompia tunnistusmenetelmiä[11]. Asiointipalvelun suunnittelussa on syytä arvioida Suomi.fi-tunnistamisen käyttöönottoa erityisesti, kun yksi tai useampi seuraavista reunaehdoista täyttyy:

- Asiointipalvelussa on tarve tunnistaa luonnollisia henkilöitä
- Asiointipalvelun käyttäjät tulee tunnistaa vahvasti

[11] Tämän ohjeen julkaisuhetkellä Suomi.fi-tunnistaminen ei tarjoa vielä vahvaa heikompia tunnistusmenetelmiä.

- Asiointipalvelun omistajalla on velvoite tai oikeus käyttää tunnistuspalvelua (ks. Oikeudet ja velvoitteet tukipalveluiden käyttöön)
- Palvelussa on tunnistettu tarve tunnistaa tulevaisuudessa myös muiden EU-maiden kansalaisia.

8.3.2 Standardinmukainen tietoturvallisuus

Suomi.fi-tunnistaminen helpottaa käyttäjien luotettavaa tunnistamista sähköisissä asiointipalveluissa. Oheinen taulukko kuvaa palvelun olennaiset ominaisuudet ja hyödyt tietoturvallisen asiointipalvelun suunnittelussa.

Tietoturvaominaisuus	Kuvaus ja hyödyt
Keskitetty sähköisen tunnistamisen välityspalvelu	Asiointipalvelu tarvitsee liittää vain yhteen ulkoiseen tunnistuspalveluun, jonka kautta se saa käyttöön laajan tunnistusvälinevalikoiman. Vahvan ja vahvaa heikomman tunnistamisen käyttöönotto asiointipalvelussa on määrämuotoista ja ohjeistettua.
Standardinmukaiset sähköisen tunnistamisen menetelmät	Tunnistuspalvelun kautta tarjottavat sähköisen tunnistamisen menetelmät ovat eIDAS-standardin mukaisia ja Viestintäviraston hyväksymiä.
Käyttäjäidentiteetin voimassaolon tarkistus ja ajantasaisten henkilötietojen päivittäminen	Vahvaa tunnistusmenetelmää käytettäessä Suomi.fi-tunnistaminen tarkistaa jokaisen tunnistustapahtuman yhteydessä väestötietojärjestelmästä, että henkilön identiteetti on voimassa. Menettelyn ansiosta asiointi esimerkiksi kuolleen henkilön identiteetillä ei ole mahdollista. Asiointipalvelu saa tunnistustapahtuman yhteydessä lisäksi väestötietojärjestelmästä ajankohtaiset henkilötiedot.
Laajeneva tunnistusvälinevalikoima	Suomi.fi-tunnistamiseen myöhemmin liitettävät tunnistusvälineet tulevat automaattisesti asiointipalvelun asiakkaiden käyttöön.
Valmiiksi käyttäjille jaetut tunnistusvälineet	Asiointipalvelun omistajan ei tarvitse huolehtia tunnistusvälineiden hankkimisesta ja jakelusta. Useissa tapauksissa voi olla järkevää soveltaa korotetun varmuustason tunnistusmenetelmää (vaikka palvelun riskiprofiili ei sitä edellyttäisi) siksi, että käyttäjällä on jo hallussaan tarvittava tunnistusväline.

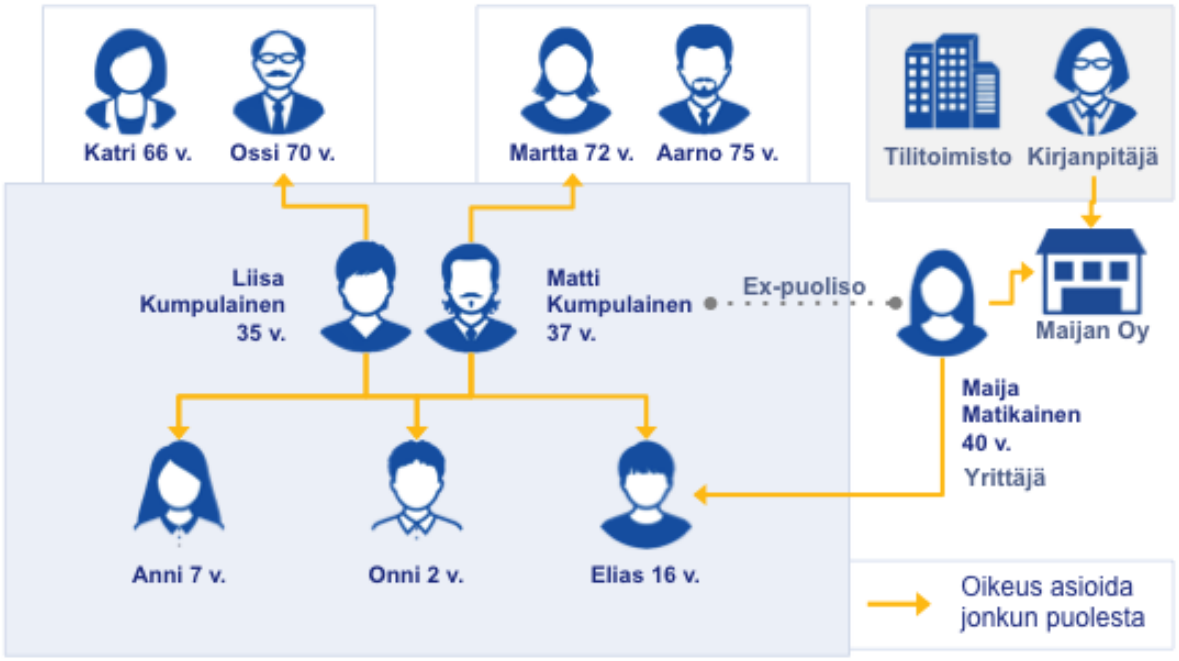
8.3.3 Tarkistuslista asiointipalvelun omistajalle

Suomi.fi-tunnistaminen -palvelun ajantasainen dokumentaatio on saatavilla osoitteessa https://esuomi.fi/palveluntarjoajille/tunnistaminen/. Alla on listattu keskeisimmät asiointipalveluun suunnittelussa huomioitavat asiat tunnistamisen osalta:

- asiointipalvelun omistavalla organisaatiolla tulee olla lakiin perustuva oikeus käsitellä henkilön yksilöiviä tunnistetietoja (nimi, henkilötunnus ja sähköinen asiointitunnus)
- Väestörekisterikeskus päättää tunnistamispalvelun käyttöoikeudesta tapauskohtaisesti, kun yksityisen sektorin toimija toteuttaa asiointipalvelua julkishallinnon organisaation puolesta.

8.4 Suomi.fi-asiointivaltuudet

Suomi.fi-asiointivaltuudet on palvelu, jossa henkilön valtuudet, valtakirjat ja oikeudet asioida toisen henkilön tai yrityksen puolesta voidaan luotettavasti tarkistaa. Asiointivaltuuksien tarkastaminen perustuu kansallisissa perusrekistereissä (mm. väestötietojärjestelmä sekä yritys- ja yhteisötietojärjestelmä) ylläpidettäviin valtuustietoihin sekä sähköisillä valtakirjoilla[12] erikseen annettaviin valtuutuksiin. Kuva 11 havainnollistaa asiointivaltuuspalvelun tukemia puolesta-asiointitapauksia.



Kuva 11 Suomi.fi-asiointivaltuudet -palvelun puolesta-asiointitapaukset

Niin julkishallinnon kuin yksityisen sektorin asiointipalvelut voivat käyttää Suomi.fi-asiointivaltuudet -tukipalvelua. Asiointipalveluun tulee toteuttaa kysely Suomi.fi-asiointivaltuudet -palveluun, joka palauttaa asiointihetkellä käyttäjän henkilötunnukseen liitetyt asiointivaltuudet perustietorekistereistä ja kansallisesta valtuutusrekisteristä[13].

Suomi.fi-asiointivaltuudet -palvelu parantaa merkittävästi mahdollisuuksia puolesta-asiointiin sähköisessä asioinnissa, koska asiointipalvelun omistajan ei tarvitse huolehtia asiointivaltuuksien hallinnoinnista itse ja ne voivat hyödyntää valmista kyselyrajapintaa. Keskitetyn valtuusrekisterin käyttö pienentää myös väärinkäytösten riskiä.

[12] Sähköiset valtakirjat eivät ole käytössä vielä Suomi.fi-asiointivaltuudet -palvelun tämän ohjeen julkaisuhetkellä. Valtakirjatoiminnallisuus tulee käyttöön Suomi.fi-asiointivaltuudet -palvelussa *arviolta* vuoden 2017 ensimmäisellä neljänneksellä.

[13] Sähköiseen valtakirjaan perustuva valtuutus tallennetaan Kansalliseen valtuusrekisteriin.

8.4.1 Standardinmukainen tietoturva

Suomi.fi-asiointivaltuudet edesauttaa puolesta-asioinnin järjestämistä ja tietoturvallisuutta seuraavin tavoin:

Tietoturvaominaisuus	Kuvaus ja hyödyt
Keskistetty kansallinen valtuusrekisteri	Asiointivaltuuksien tarkistaminen on mahdollista julkishallinnon keskitetysti hallinnoimasta tietoturvallisesta palvelusta.
Liityntä väestötietojärjestelmään ja kaupparekisteriin	Asiointipalvelu voi luotettavasti tarkistaa kansallisista perusrekistereistä, että valtuutetulla on oikeus asioida kyseisessä asiointipalvelussa toisen henkilön tai edustamansa yrityksen puolesta.

8.4.2 Soveltuvat käyttötilanteet

Asiointipalvelun suunnittelussa on syytä arvioida Suomi.fi-asiointivaltuudet -tukipalvelun käyttöönottoa erityisesti, kun yksi tai useampi seuraavista reunaehdoista täyttyy:

- Asiointipalvelun omistavalla organisaatiolla on lain määrittelemä oikeus käyttää tukipalvelua
- Puolesta-asiointi voidaan perustaa väestötietorekisterissä ylläpidettäviin huoltajuustietoihin. Esimerkiksi sosiaali- ja terveydenhuollossa tämä mahdollistaa asiakkaiden sujuvan itsepalvelun ja paremman palvelukokemuksen.
- Puolesta-asiointi voidaan perustaa kaupparekisterissä ylläpidettäviin yritysten nimenkirjoitusoikeuksiin. Esimerkiksi yrityksen toimitusjohtaja voi asioida sähköisesti asiointipalveluissa ja tehdä lakisääteisiä ilmoituksia yrityksen nimissä (vrt. Katso -palvelun roolit).
- Puolesta-asioinnin oikeutta (asian kohdennus) ei voi tarkistaa nykyisistä perusrekistereistä, jolloin henkilö tai yrityksen nimenkirjoittaja voi valtuuttaa luonnollisen henkilön tai yrityksen toimimaan puolestaan (kohdennetussa asiassa) laatimalla sähköisen valtakirjan. Sähköinen valtakirja tallennetaan kansalliseen valtuusrekisteriin vahvojen tunnistamisvälineiden avulla.

8.4.3 Tarkistuslista

Suomi.fi-asiointivaltuudet -palvelun ajantasainen dokumentaatio on saatavilla osoitteessa https://esuomi.fi/palveluntarjoajille/asiointivaltuudet/. Alla on listattu keskeisimmät asiointipalvelun suunnittelussa huomioitavat asiat:

- Asiointivaltuuksien hyödyntämistä varten asiointipalvelulla tulee olla vahvan tunnistamisen tunnistuspalvelu, esimerkiksi Suomi.fi-tunnistaminen
- Yksityisen sektorin organisaatiolla tulee olla oikeus käsitellä asiakkaidensa yksilöivää henkilötunnusta tai y-tunnusta
- Asiointipalvelu voi toteuttaa asiointivaltuuskyselyt joko Suomi.fi-palveluväylän kautta tai vaihtoehtoisesti Suomi.fi-asiointivaltuudet -palvelun REST-rajapinnan kautta: https://esuomi.fi/palveluntarjoajille/asiointivaltuudet/tekninen-aineisto/web-api-rajapinta-ja-valintakayttoliittyma/.

8.5 Suomi.fi-palvelunäkymät

Suomi.fi-palvelunäkymät tarjoaa loppukäyttäjän - kansalaisen, yrityksen ja viranomaisen – tarvitsemat keskeiset palvelut. Palvelunäkymät yhdistää nykyiset Suomi.fi ja Yrityssuomi.fi – verkkopalvelut yhdeksi yhteiseksi roolipohjaiseksi verkkopalveluksi.

Kuva 12 Suomi.fi-palvelunäkymien tuotevisio ja tärkeimmät komponentit

Kansalaisten, yritysten ja viranomaisten Suomi.fi-palvelunäkymissä käyttäjä:

- voi hakea palveluja ja niiden tietoja ja palvelukanavia helposti eri rooleissa (julkiset ja yksityiset palvelut) Suomi.fi-palvelutietovarannosta
- näkee kootusti omia tietojaan tai edustamansa organisaation tietoja julkisen hallinnon perusrekistereistä ja yksityisen sektorin tuottamista tietovarannoista
- voi käyttää sähköisen asioinnin palveluja kertakirjautumisella (Suomi.fi-tunnistaminen)
- saa herätteitä ja suosituksia itselleen tai edustamalleen organisaatiolle tarkoitetuista palveluista, velvoitteista ja mahdollisuuksista.

8.5.1 Standardinmukainen tietoturva

Suomi.fi-palvelunäkymät edesauttavat sähköisen asioinnin tietoturvallisuutta seuraavin tavoin:

Tietoturvaominaisuus	Kuvaus ja hyödyt
Ajantasainen tieto viranomaispalveluista	Suomi.fi-palvelunäkymien kautta käyttäjä löytää ajantasaiset tiedot palveluista ja niiden palvelukanavista. Tämä parantaa välillisesti myös palveluiden tietoturvallista käyttöä, koska käyttäjä voi paremmin luottaa löytyviin tietoihin (vrt. esim. huijaussivustot viranomaisten nimissä joita voi löytää hakukoneilla). Tiedot noudetaan Suomi.fi-palvelutietovarannosta.
Luottamuksellinen tiedoksiantojen välitys	Omat viestit -toiminnallisuus (ks. Suomi.fi-viestinvälitys) mahdollistaa tietoturvallisen tiedoksiantojen toimittamisen ja vuorovaikutteisen sähköisen viestinnän julkisen hallinnon asiakkaiden kanssa.
Turvallinen pääsy omiin tietoihin	Pääsy omiin tietoihin mahdollistaa loppukäyttäjälle omien tietojen katselun eri rekistereistä. Palveluihin ohjaus mahdollistaa rekistereissä olevan tiedon korjaamisen, mikä parantaa rekistereissä olevan tiedon eheyttä, laatua ja kattavuutta.

8.5.2 Soveltuvat käyttötilanteet

Julkisen hallinnon organisaation tulee tuottaa pääsy merkittäviin sähköisesti saataville oleviin asiakastietoihin palvelunäkymien kautta 31.6.2017 mennessä.

8.5.3 Tarkistuslista

Suomi.fi-palvelunäkymien ajantasainen dokumentaatio on saatavilla osoitteessa https://esuomi.fi/palveluntarjoajille/palvelunakymat/. Ennen palvelun käyttövelvoitteen alkamista julkishallinnon organisaation tulee kartoittaa, onko sillä rekistereitä, jotka sisältävät kansalaista (henkilötunnus) tai yritystä (y-tunnus) koskevaa merkityksellistä asiakkuustietoa. Mikäli on, tulee ko. rekisteri kytkeä Suomi.fi-palveluväylään ja tuoda tiedot Suomi.fi-palvelunäkymiin.

8.6 Suomi.fi-palvelutietovaranto

Suomi.fi-palvelutietovaranto (Palvelutietovaranto, PTV) on keskitetty tietovaranto, johon organisaatiot tuottavat tiedot tarjoamistaan palveluista ja asiointikanavista sekä palveluun kytkeytyvän organisaation tiedoista. Palvelutietovaranto sisältää yhdenmukaiset kuvailutiedot kaikista julkisista palveluista 31.6.2017 mennessä. Tiedot tarjotaan avoimena datana vapaaseen käyttöön. Suomi.fi-palvelunäkymät käyttää palvelutietovarantoa kaikkien palvelutietojen esittämiseen.

8.6.1 Standardinmukainen tietoturva

Suomi.fi-palvelutietovaranto edesauttaa sähköisen asioinnin tietoturvallisuutta seuraavin tavoin:

Tietoturvaominaisuus	Kuvaus ja hyödyt
Ajantasainen tieto viranomaispalveluista	Suomi.fi-palvelutietovarannosta julkisen hallinnon toimijat ja yksityiset toimijat voivat noutaa ajantasaiset tiedot julkisista palveluista ja niiden palvelukanavista myös omiin sähköisen asioinnin palveluihinsa ja verkkosivustoilleen (parantaa tiedon luotettavuutta).

8.6.2 Soveltuvat käyttötilanteet

Julkisen hallinnon organisaation

- tulee kuvata omat palvelunsa ja palvelukanavansa kansalliseen palvelutietovarantoon 31.6.2017 mennessä
- voi hyödyntää palvelutietovarantoa avoimen rajapinnan kautta omissa tietojärjestelmissään ja verkkosivustoissaan palvelutietojen masterdata-lähteenä.

8.6.3 Tarkistuslista

Suomi.fi-palvelutietovarannon ajantasainen dokumentaatio on saatavilla osoitteessa https://esuomi.fi/palveluntarjoajille/palvelutietovaranto/ . Alla on listattu keskeisimmät asiointipalveluun suunnittelussa huomioitavat asiat:

- Organisaatio on nimennyt palvelutiedoista vastaavan yhteyshenkilön ja toimittanut tiedot henkilöstä Väestörekisterikeskukseen.
- Organisaatio on valmistautunut kuvaamaan ja ylläpitämään järjestämiensä palvelujen ja niiden palvelukanavien tietoja kansallisessa palvelutietovarannossa 31.6.2017 mennessä.

8.7 Suomi.fi-viestinvälitys

Suomi.fi-viestinvälitys on viranomaisten keskitetty viestioperaattori, jonka avulla viranomainen ja hallinnon asiakas voivat lähettää toisilleen sähköisiä viestejä ja jota hyödyntäen asiakirja voidaan antaa tiedoksi sähköisesti tai postitse. Se tarjoaa nykyisen Asiointitilin liittymärajapinnat sekä OpusCapitan iPost-rajapinnat. Palvelussa on lisäksi rajapinta, josta hyväksytty ulkoinen palvelu voi lukea asiakkaan

viestejä asiakkaan suostumuksella. Kansallisessa palveluarkkitehtuurissa Viestinvälityksen avulla toteutetaan kansalaisen ja yrityksen *Omat viestit* Suomi.fi-palvelunäkymiin. Palvelunäkymien *Omat viestini* -osio on käyttäjän sähköinen postilaatikko, joka korvaa nykyisen Asiointitilin vuonna 2017.

8.7.1 Standardinmukainen tietoturva

Suomi.fi-viestinvälitys edesauttaa sähköisen asioinnin tietoturvallisuutta seuraavin tavoin:

Tietoturvaominaisuus	Kuvaus ja hyödyt
Luottamuksellinen tiedoksiantojen välitys	Suomi.fi-viestinvälityspalvelu mahdollistaa tietoturvallisen tiedoksiantojen toimittamisen ja vuorovaikutteisen sähköisen viestinnän julkisen hallinnon asiakkaiden (kansalainen, yritys) kanssa.

8.7.2 Soveltuvat käyttötilanteet

Julkisen hallinnon organisaation

- tulee ottaa viestinvälityspalvelu käyttöön sähköisen viestien ja tiedoksiantojen toimittamiseen uusissa palveluissa lain voimaantulosta alkaen (Laki yhteisistä sähköisen asioinnin palveluista)
- voi hyödyntää viestinvälityspalvelu muistuttaakseen asiakasta esimerkiksi tietystä määräpäivämäärästä (esimerkiksi asiakkaan toimenpide tai hyväksyntä on tehtävä tiettynä ajankohtana).

8.7.3 Tarkistuslista

Suomi.fi-viestinvälityspalvelun ajantasainen dokumentaatio on saatavilla osoitteessa https://esuomi.fi/palveluntarjoajille/viestinvalitys/. Alla on listattu keskeisimmät asiointipalveluun suunnittelussa huomioitavat asiat:

- Lähettääkö organisaatio tiedoksiantoja tai viestejä asiakkailleen paperipostina. Mikäli lähettää, tulee organisaation suunnitella viestinnän kytkeminen Suomi.fi-viestinvälityspalveluun palvelujen elinkaaren mukaan tai uusia palveluja kehitettäessä.
- Käyttääkö organisaatio paperipostitusta pyytääkseen asiakkaalta lisätietoja tai puuttuvia dokumentteja tai muistuttaakseen asiakasta esimerkiksi tietystä määräpäivämäärästä? Mikäli käyttää, tulee organisaation suunnitella viestinnän kytkeminen Suomi.fi-viestinvälityspalveluun palvelujen elinkaaren mukaan tai uusia palveluja kehitettäessä.

8.8 Suomi.fi-karttapalvelu

Suomi.fi-karttapalvelu tarjoaa julkishallinnolle keskitetyn palvelun paikkatietojen ja karttojen hyödyntämiseen. Karttoja ja paikkatietoa on mahdollista hyödyntää esimerkiksi omien toimipisteiden tai tietoaineistojen visualisointiin.

Suomi.fi-karttapalvelussa voi luoda karttakäyttöliittymän ja julkaista sen organisaation omilla verkkosivuilla tai hyödyntää sähköisen asiointipalvelun karttakomponenttina. Kartan koko, kartta-aineistot sekä käyttäjälle tarjottavat toiminnot ja työkalut ovat valittavissa ja muokattavissa tapauskohtaisesti.

Suomi.fi-karttapalvelun asiakasorganisaatio voi lisätä palveluun omia paikkatietoaineistojaan, jotka tallennetaan Suomi.fi-karttapalvelun tietokantaan. Aineiston tulee olla palvelun käyttöehtojen mukaan julkista tietoa.

Sähköiset asiointipalvelut voivat hyödyntää karttakomponenttia HTML5-pohjaisen RPC-ohjelmointirajapinnan (*remote procedure call*) kautta, jolloin kartan toimintoja voi räätälöidä monipuolisesti. Rajapinnan avulla asiointipalvelu voi lisätä asiointiin liittyvää tietoa karttanäkymään, esimerkiksi piirtää asiointitilanteeseen liittyvät kohteet kartalle tai poimia käyttäjän kartalta osoittamat kohteet asiointisovellukseen.

8.8.1 Standardinmukainen tietoturva

Suomi.fi-karttapalvelu edesauttaa puolesta-asioinnin järjestämistä ja tietoturvallisuutta seuraavin tavoin:

Tietoturvaominaisuus	Kuvaus ja hyödyt
Laadukas, ajantasainen kartta-aineisto	Asiointipalvelussa saa käyttöönsä ajantasaiset ja laadukkaat kansalliset kartta-aineistot. Laaja kirjo viranomaisten tuottamia paikkatietoaineistoja on asiointipalvelun saatavilla keskitetyn karttapalvelun-palvelun kautta.
Yhtenäinen käyttökokemus koko julkishallinnossa	Kaikki julkishallinnon asiointipalveluiden asiakkaat saavat visuaalisesti yhtenäistä kartta- ja paikkatietopalvelua. Kartta toimii myös mobiililaitteissa.
Palvelun saatavuus	Maanmittauslaitos vastaa palvelun ja sen teknisten rajapintojen saatavuudesta ja sekä aineistojen eheydestä.
Omien paikkatietoaineistojen suojaaminen	Suomi.fi-karttapalveluun liitettyjen omien aineistojen on suojattu valtuudettomalta katselulta ja muokkaamiselta. Muut Suomi.fi-karttapalvelun asiakkaat eivät näe aineistoa tai pysty lisäämään sitä omiin julkaistuihin karttoihinsa.
Ei-julkisen asiointiin liittyvän paikkatiedon suojaaminen	Asiointiin liittyvän tiedon käyttäminen karttanäkymässä tapahtuu selaimen sisäisesti (JavaScript HTML5 postMessage -pyyntönä). Asiointiin liittyvä ei-julkista tietoa ei välity lainkaan karttapalvelun palvelimille. Vastaavasti karttapalvelu itsessään ei tee suoria hakua suojattuihin rajapintapalveluihin.

8.8.2 Soveltuvat käyttötilanteet

Asiointipalvelun suunnittelussa on syytä arvioida Suomi.fi-karttapalvelun käyttöönottoa erityisesti, kun yksi tai useampi seuraavista reunaehdoista täyttyy:

- Asiointipalvelun omistavalla organisaatiolla on lain määrittelemä oikeus käyttää tukipalvelua; kyseessä on julkishallinnon viranomainen tai organisaatio, joka suorittaa sopimuksella julkista tehtävää[14].
- Suomi.fi-karttapalvelun kansallinen kartta-aineisto on riittävä asiointipalvelun tarpeisiin

[14] Yksityiset yhteisöt, säätiöt ja elinkeinonharjoittajat eivät voi käyttää Suomi.fi-karttapalvelua

- Asiointipalvelun omistaja haluaa turvata karttapalveluun lisäämiensä aineistojen ja asiointitapahtuman aikana karttanäkymässä näytettävän ei-julkisen paikkatiedon eheyden ja luottamuksellisuuden ja estää aineistojen vuotamisen kolmansille osapuolille.

8.8.3 Tarkistuslista

Suomi.fi-karttapalvelun ajantasainen dokumentaatio on saatavilla Maanmittauslaitoksen sivuilta osoitteessa https://esuomi.fi/palveluntarjoajille/palvelunakymat/hallinnon-karttapalvelu/. Alla on listattu keskeisimmät asiointipalveluun suunnittelussa huomioitavat asiat karttapalvelun osalta:

- Asiointipalvelun omistaja on hyväksynyt Suomi.fi-karttapalvelun käyttöehdot.

Liite 1: Keskeinen sanasto

Ohjeessa käytetyt keskeiset termit on kuvattu alla olevassa taulukossa.

Sana	Selitys
Anonymisointi	Ks. EU-tietosuojan kokonaisuudistus (VAHTI 1/2016)
Kiistämättömyys	Ks. Valtionhallinnon tietoturvasanasto VAHTI 8/2008
SaaS	Ks. Valtionhallinnon tietoturvasanasto VAHTI 8/2008
Tunnistamisen varmuustaso	Varmuustaso (*level of assurance*) luonnehtii sähköisen tunnistamisen menetelmän luotettavuuden astetta henkilön henkilöllisyyden toteamisessa. Varmuustaso riippuu sähköisen tunnistamisen menetelmän tarjoamasta luottamustasosta henkilön väitetyn tai esitetyn henkilöllisyyden suhteen ottaen huomioon toteutetut prosessit (esimerkiksi henkilöllisyyden todistaminen ja varmentaminen sekä todentaminen), hallinnolliset toimet (esimerkiksi sähköisen tunnistamisen menetelmän myöntävä toimija ja menettely tällaisen menetelmän myöntämiseksi) ja tekniset tarkastukset.
Kehittynyt sähköinen allekirjoitus	eIDAS asetuksen 26 artiklan mukainen sähköinen allekirjoitus.
Profilointi	Ks. EU-tietosuojan kokonaisuudistus (VAHTI 1/2016)
Pseudonymisointi	Ks. EU-tietosuojan kokonaisuudistus (VAHTI 1/2016)
Tunnistuksenvälityspalvelu	Tunnistuspalvelun tarjoaja, joka tarjoaa vahvan sähköisen tunnistamisen palveluita niitä käyttäville asiointipalveluille Teknisiä lisätietoja vahvan sähköisen tunnistuksenvälityspalvelun tarjoajista ja vaatimuksista heidän palveluilleen Viestintäviraston määräyskokoelmasta[15].
Vahva (sähköinen) tunnistaminen	Henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset. Teknisiä lisätietoja vahvan sähköisen tunnistamisen palveluntarjoajista ja vaatimuksista niiden tunnistuspalveluille Viestintäviraston määräyskokoelmasta[16].
Viranomaisliittymä	Asiointitapahtumassa viranomaista edustavalle henkilölle suunnattu käyttöliittymä tai päätelaitteelle asennettava sovellus, joka mahdollistaa viranomaisen tarvitsemien toimintojen käyttämisen.

[15] https://www.viestintavirasto.fi/ohjausjavalvonta/laitmaarayksetpaatokset/maaraykset/maarays72sahkoisistatunnistus-jaluottamuspalveluista.html
[16] https://www.viestintavirasto.fi/ohjausjavalvonta/laitmaarayksetpaatokset/maaraykset/maarays72sahkoisistatunnistus-jaluottamuspalveluista.html

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

Oheiseen taulukkoon on koostettu tiivis tarkistuslista asioista, joita sähköisen asiointipalvelun omistajan on erityisesti syytä huomioida harkitessaan asiointipalvelun liittämistä kaupalliseen tai ilmaiseen, lähtökohtaisesti ei-luotettuun tukipalveluun.

Yleisenä ohjeena tukipalvelun tulee täyttää siinä käsiteltävän tiedon suojaustasoluokittelun mukaiset vaatimukset. Jos palvelussa käsitellään ainoastaan julkista tietoa, vaatimukset ovat olennaisesti matalammat.

Osa-alue	Huomioitavat asiat
Vaatimuksenmukaisuus	Tukipalvelun tietoturvallisuuden hallinta on kuvattu palvelukuvauksissa siten, että asiakas voi varmistua palvelun vaatimuksenmukaisuudesta. Palveluntarjoajalla on osoittaa riippumattoman tahon myöntämä varmennuslausunto tai vastaava todistus palvelun tietoturvallisuuden tasosta, tai vaihtoehtoisesti asiakkaalla on mahdollisuus varmentaa vaatimuksenmukaisuus itse auditoinnein ja teknisin testausmenetelmin.
Tietojen tekninen suojaaminen	Asiakas voi varmistua, että sen omistama tiedon suojaamisessa sovelletaan riittäviä menettelyitä ja teknisiä ratkaisuja tiedon luottamuksellisuuden ja eheyden turvaamiseksi sekä hukkaamisen ehkäisemiseksi niin tietoa tallennettaessa (*data at rest*) kuin sitä siirrettäessä (*data in transit*). Tiedonsiirrossa asiointipalvelun ja tukipalvelun välillä käytetään standardeja tietorakenteita ja rajapintoja. Jaetuissa tukipalveluissa (ns. *multi-tenant* -palvelut) eri asiakkaiden tietojen eriyttäminen on varmistettu.
Lokienhallinta	Palvelu tuottaa asiakkaan toiminnan edellyttämät riittävän yksityiskohtaiset lokitiedot (mm. pääsynvalvonta-, käyttö- ja tiedonluovutuslokit), joita asiakas tarvitsee osoittaakseen oman toimintansa vaatimuksenmukaisuuden. Lokitiedot on suojattu muutoksilta. Lokien säilytysaika on riittävä, ja asiakkaalla on tarvittaessa pääsy palvelun tuottamiin lokitietoihin.
Yksityisyydensuoja	Tukipalvelun tietojen maantieteellinen tallennus- ja käsittelypaikka on määritelty. Henkilötietoja ei käsitellä eikä tallenneta EU-maiden ulkopuolella ellei siitä ole erikseen sovittu ja varmistettu vaadittavasta tietoturvallisuuden ja tietosuojan tasosta. Palvelu ei kerää eikä yhdistele tietoja asiointipalvelun käyttäjistä eikä käyttää kerättyjä tietoja muuhun kuin asiointipalvelun ensisijaiseen käyttötarkoitukseen Palvelu ei välitä tietoja asiointipalvelun asiakkaista kolmansille osapuolille, jotka voivat käyttää tietoja asiointipalvelun käyttötarkoituksen vastaisesti mm. mainonnan kohdentamisessa.

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

Käyttäjäidentiteetin ja tunnistusvälineiden hakeminen ja rekisteröinti

Käyttäjäidentiteetillä tarkoitetaan palveluntarjoajan tiedossa olevia käyttäjän henkilöllisyyttä yksilöiviä ja kuvaavia tietoja. Käyttäjäidentiteetti luodaan asiointipalveluun – tai asiointipalvelun käyttämään ulkoiseen tunnistuspalveluun – käyttäjän rekisteröinnin yhteydessä.

Jos käyttäjän henkilöllisyys selvitetään rekisteröinnin yhteydessä luotettavasti esimerkiksi henkilöllisyystodistuksesta, käyttäjäidentiteetin luotettavuus on korkeampi verrattuna tilanteeseen, jossa käyttäjä antaa henkilöllisyyttään kuvaavat tiedot itse eikä tietojen paikkaansa pitävyyttä tarkisteta.

Joissain tapauksissa henkilön todellisen henkilöllisyyden yksilöiminen ei ole olennaista, vaan se kuuluuko henkilö johonkin ryhmään (esimerkiksi kuntalaisuus) ja onko näin oikeutettu tietyn asiointipalvelun käyttöön. Käyttäjän ilmoittamat tiedot, kuten nimi, osoite ja sähköpostiosoite, riittävät monissa palveluissa sellaisenaan tunnistukseksi. Tarvittaessa tietojen luotettavuus voidaan varmistaa vertailemalla ilmoitettuja tietoja palvelun tarjoajan omissa tietojärjestelmissä oleviin tietoihin.

Sähköisen tunnistamisen luotettavuus perustuu suurelta osin siihen, että tunnistusvälineitä käyttää vain henkilö tai tietojärjestelmä, jolle ne on myönnetty. Tunnistamisen eri varmuustasot eroavat sen suhteen, kuinka menetelmän tarjoaja varmistuu siitä, että tunnistusvälineet toimitetaan vain hakijalle ja että niiden käyttäminen tunnistamisessa toisen henkilön tai murretun tietojärjestelmän toimesta on epätodennäköistä.

Sähköisen tunnistusmenetelmän ominaispiirteet

Keskeisin tunnistusmenetelmää määrittävä ominaispiirre on todentamistekijöiden lukumäärä. Todentaminen perustuu yhteen tai useampaan todentamistekijään, jotka voidaan jaotella seuraaviin luokkiin:

1. tiedossaoloon perustuvat todentamistekijät (”johonkin mitä käyttäjä tietää”); esimerkiksi henkilökohtaiseen käyttäjätunnukseen liitetty salasana
2. hallussapitoon perustuvat todentamistekijät (”johonkin mitä käyttäjällä on hallussaan”); tunnistusväline kuten sirukortti, jolle on tallennettu kryptografinen varmenne. Hallussapitoon perustuvan todentamistekijän keskeisiä turvaominaisuuksia ovat, että i) se on yksinomaan omistajansa hallinnassa ja että ii) sen jäljentäminen toiselle käyttäjällä on mahdotonta tai hyvin vaikeaa.
3. luontaiset todentamistekijät (”johonkin mitä käyttäjä itse on”); luonnollisen henkilön fyysiseen ominaisuuteen perustuva tekijä, esimerkiksi sormenjälki tai iiris.

Käyttäjätunnus-salasanapariin – tai salasanalauseeseen – perustuva todentaminen on yleisin esimerkki yhden tekijän todentamisesta. Monen tekijän todentaminen nojautuu vähintään kahden *eri luokkaan* kuuluvan todentamistekijän yhdistelmään. Tällaisia yhdistelmiä ovat esimerkiksi:

- käyttäjätunnus + kiinteä salasana + vaihtuvat salasanalistat (esimerkiksi verkkopankkitunnukset ja Katso OTP -tunnistaminen)
- käyttäjätunnus + kiinteä salasana + puhelinsoitto matkapuhelimeen
- mobiilitunnistaminen varmenteella tai tunnuslukusovelluksella
- varmenteellinen sirukortti + PIN-koodi
- varmenteellinen sirukortti + biotunnistus
- *hardware token* -pohjainen kertakäyttösalasana + PIN-koodi

Korotetun ja korkean varmuustason tunnistusmenetelmät edellyttävät vähintään kahden eri luokkaan kuuluvan todentamisvälineen käyttöä.

Todentamistekijöiden lukumäärän lisäksi tunnistusmenetelmän varmuuteen vaikuttavat oheisessa taulukossa kuvatut menettelyt, joilla tunnistusmenetelmän teknisessä toteutuksessa suojaudutaan todentamistekijään liittyviltä tyypillisiltä haavoittuvuuksilta ja hyökkäysmenetelmiltä.

Haavoittuvuus / hyökkäysmenetelmä	**Suojaava menettely**
Salasanan tai PIN-koodin arvaaminen	– vahva, salasanojen riittävän entropian varmistava salasanapolitiikka – epäonnistuneiden kirjautumisyritysten lukumäärän rajaaminen ja käyttäjätilin automaattinen lukitseminen määräajaksi rajan ylityttyä
Salasanan tai PIN-koodin kalastelu	– käyttäjät opastaminen kalasteluyritysten tunnistamiseksi
Tietoliikenteen salakuuntelu	– Tunnistetietojen ja salasanatiivisteiden välittäminen ainoastaan salatulla yhteydellä
Toisintaminen (*man in the middle* -hyökkäys)	– Salasanatiivisteiden satunnaistaminen (esimerkiksi *salting*) – Dynaaminen todentaminen, jossa jokaisessa todentamistilanteessa luodaan teknisin menetelmin yksilöllinen sähköinen todiste todentamisesta
Biometrisen todentamistekijän riittämätön yksilöllinen vaihtelu	– Sellaisen biometrisen todentamistekijän valinta, joka on yksilöllinen jokaiselle luonnolliselle henkilölle – Biometrinen todentamistekijän käyttö ainoastaan yhtenä tekijänä monen todentamistekijän tunnistamisessa
Läsnäolo varmentamispaikassa (biometriset tunnisteet)	– Todentamismenetelmän toteuttaminen siten, ettei todentaminen onnistu, jos biometrisen todentamistekijän haltija ei ole fyysisesti läsnä todentamispaikassa; esimerkiksi sormenjälkitunnistus ei onnistu pelkällä sormenjäljen kuvalla
Todentamistekijän rinnakkaiskäyttö	– Tunnistusmenetelmän toteutus siten, että todentamistekijä mahdollistaa vain yhden kirjautumistunnon kerrallaan; käyttäjä saa vähintäänkin tiedon rinnakkaisesta tunnistustapahtumasta.

Taulukko 7 Todentamistekijöiden ominaispiirteitä

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

Tietoaineistojen sähköisen käsittelyn periaatteet

- Asiointipalvelussa käsitellään vain käyttötarkoituksen kannalta tarpeellista ei-julkista tietoa.
- Henkilötietojen käsittelyssä noudatetaan lakia. Tarpeettomia tietoja käyttäjistä ei kerätä eikä tallenneta, ja henkilötiedot tuhotaan viiveettä, kun niiden säilyttämiselle ei ole enää perustetta.
- 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.

Asiointipalvelun tietoturvallinen rakenne ja kontrolliympäristö

- Asiointipalvelun määrämuotoinen riskianalyysi ohjaa palvelun rakenneratkaisujen ja kontrolliympäristön suunnittelua. Suojausratkaisut pyritään valitsemaan ja toteuttamaan siten, että ne pienentävä tunnistettuja riskejä tarkoituksenmukaisesti ja kustannustehokkaasti.
- Palvelu on eristetty internetistä DMZ-vyöhykkeellä. Asiointipalvelun käyttöympäristön tietoverkko on segmentoitu, ja palvelun komponentit on 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.
- 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.
- 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.
- Mahdolliset palvelunestohyökkäykset on otettu huomioon mm. rakenneratkaisuissa ja käyttöpalveluympäristön koventamisessa. Palvelunestohyökkäyksen vaikutusten rajaaminen ja toiminta poikkeamatilanteissa on suunniteltu.
- Lokien riittävästä tuottamisesta asiointipalvelun tapahtumista (mm. pääsynvalvonta- ja käyttölokitiedot eri lokilähteistä) ja lokien eheyden ja kirjausketjun suojaamisesta on huolehdittu suunnitelman mukaisesti. Lokeja analysoidaan ja valvotaan.

Tunnistaminen, valtuuttaminen ja tahdonilmaukset

- Tarve palvelun asiakkaiden yksilöimiseksi ja tunnistamiseksi on arvioitu. Vaatimukset sähköisen tunnistamisen menetelmälle on määritelty ja tarkoituksenmukainen tunnistusratkaisu- tai palvelu on otettu käyttöön.
- Tunnistusvälineiden saatavuus on huomioitu. Tunnistusvälineiden tulee joko olla valmiiksi niitä tarvitsevien käyttäjien hallussa tai palvelun käyttäjillä tulee olla mahdollisuus hankkia tarvittavat tunnistusvälineet.
- Asiointipalvelun käyttö noudattaa pienimmän käyttövaltuuden periaatetta kaikkien käyttäjäryhmien osalta, mukana lukien tietojärjestelmien käyttämät palvelurajapinnat. Käyttövaltuuksien hallinta on vastuutettu.

– Palvelun omistaja on tunnistanut tarpeen asiakkaiden tahdonilmausten rekisteröintiin. Palvelun omistaja on arvioinut, kuinka todennäköisesti sen tulee kyetä osoittamaan toteen asiakkaan tekemä tahdonilmaus ja 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.

Suunnittelu, ylläpito ja muutoshallinta

– Palvelun toteutuksessa kiinnitetään huomiota yksinkertaisuuteen.
– Palvelun ulkoasu on yhdenmukainen palvelua tarjoavan viranomaisen muiden verkkopalveluiden kanssa ja palvelun aitous on todennettavissa palvelinvarmenteen perusteella.
– Palvelun kannalta relevantit uhkatekijät on tunnistettu.
– 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.

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

Oheinen taulukko sisältää yhteenvedon matalan, korotetun ja korkean varmuustason sähköisen tunnistamisen menetelmien minimivaatimuksista eIDAS-määritykseen perustuen.

Varmuus-taso	Vaatimukset
Matala (Low)	**Käyttäjäidentiteetin ja tunnistusvälineiden hakeminen ja rekisteröinti** – Henkilöllisyystodistuksen hallussapito voidaan osoittaa fyysisesti tai sähköisesti, tai se voidaan osoittaa esittämällä henkilöön liittyviä tietoja, jotka eivät ole julkisia – Keskeisten käyttäjätietojen (sähköpostiosoite, puhelinnumero) paikkaansa pitävyys on tarkastettu
	Tunnistusvälineiden hallinta Ei tunnistettuja erityisvaatimuksia
	Tunnistusmenetelmän ominaispiirteet Menetelmässä käytetään vähintään yhtä todentamistekijää
Korotettu (Substantial)	**Käyttäjäidentiteetin ja tunnistusvälineiden hakeminen ja rekisteröinti** Matalan tason lisäksi: – henkilöllisyystodistuksen aitous on tarkistettu turvaominaisuuksia tarkastelemalla – menettelyt varastetun todistuksen väärinkäyttöä vastaan
	Tunnistusvälineiden hallinta – Toimitetaan henkilökohtaisesti, kirjatulla kirjeellä tai *<vastaavalla tavoin>*
	Tunnistusmenetelmän ominaispiirteet – Menetelmässä käytetään vähintään yhtä todentamistekijää – Tunnistuksen aikana välitettävät tiedot salataan
Korkea (High)	**Käyttäjäidentiteetin ja tunnistusvälineiden hakeminen ja rekisteröinti** Korotetun tason lisäksi – …
	Tunnistusvälineiden hallinta – …
	Tunnistusmenetelmän ominaispiirteet Korotetun tason lisäksi menetelmä on suojattu toisintamista ja väärentämistä vastaan.

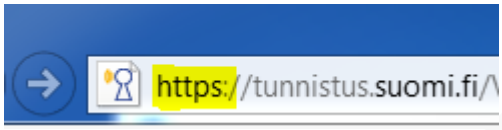
Liite 6: Case-esimerkit

Case A. Hyviä käytäntöjä sähköisen asioinnin tietoturvalliseen käyttöön

Tässä ohjeessa kuvataan toimia, joiden avulla sähköisen asiointipalvelun käyttäjä (myöhemmin Asiakas) voi suojata luottamuksellisia tietoja, henkilötietoja ja yksityisyyttään käyttäessään internetin kautta asiointipalvelua omalla tai yhteiskäyttöisellä päätelaitteella. Tässä ohjeessa kuvatut toimenpiteet eivät yksinään takaa tietojen salassa pysymistä ja tietoturvallisuutta. Vastuu luottamuksellisten tietojen ja henkilötietojen käsittelystä päätelaitteella on sähköisen palvelun Asiakkaalla. Palvelun toimittaja vastaa luottamuksellisten tietojen ja henkilötietojen turvallisesta käsittelystä asiointipalvelun käyttöliittymässä ja sen kautta tausta- ja tukijärjestelmien sisällä.

Salattu internet-yhteys

Varmista ennen luottamuksellisten tietojen ja henkilötietojen syöttöä, että sivuston käyttämä tietoliikenneyhteys on salattu ja palvelu tarkoittamasi palvelu. Salauksen käyttö ilmenee palvelun käyttämän internet-sivun osoitteesta ja internet-selaimen lukko-kuvakkeesta. Varmista aina samalla, että internet-sivun osoite on kirjoitettu oikein (ettei kyseessä ole huijaussivusto jossa esimerkiksi osoitteen yksikirjain onkin eri). Salatun internet-sivun osoitteen alku on https:// kun taas salaamattomassa http://.



Salasanojen tallennuksesta kieltäytyminen

Käytettäessä salasanalla suojattuja verkkopalveluja internet-selain saattaa ehdottaa käyttäjätunnusten ja salasanojen tallentamista. Salasanojen tallennusta ei kannata sallia, vaan salasanojen tallennuskyselyyn on vastattava: ei tässä sivustossa (tai vastaavaa – tämä riippuu internet-selaimen valmistajasta ja versiosta). Jos salasanojen tallennus sallitaan, voivat kaikki kyseistä päätelaitetta samalla kirjautumisistunnolla käyttävät käyttäjät, kuten muut perheenjäsenet, kirjautua palveluun ilman salasanan syöttämistä.

Uloskirjautuminen palveluista

Sähköisen asiointipalvelun käytön päättyessä on palvelusta kirjauduttava aina ulos. Erityisesti yhteiskäyttöisillä päätelaitteilla on olemassa mahdollisuus, että ilman uloskirjautumista seuraava laitteen käyttäjä voi päästä käyttämään edellisen kirjautuneen käyttäjän tietoja ja palveluita.

Internet-selaimen välimuistin tyhjennys

Selattaessa internet-sivuja internet-selain tallentaa ladatut sivut päätelaitteelle ns. välimuistiin. Välimuistin käyttö mahdollistaa mm. nopean siirtymisen edelliselle sivulle. Selaimen välimuistiin saattaa tallentua myös sähköisten asiointipalvelujen näyttämiä sivuja. Tällöin on mahdollista, että päätelaitteen käyttäjä pystyy tarkastelemaan edellisen käyttäjän lataamia sivuja ja saa näin ollen nähtäväkseen esim. sähköisen asiointipalvelun sisältämiä luottamuksellisia tietoja.

Erityisesti yhteiskäyttöisillä päätelaitteilla selaimen välimuisti on syytä tyhjentää aina sähköisen asiointipalvelun käytön jälkeen. Välimuistin tyhjentämismenettely riippuu käytetyn internet-selaimen valmistajasta ja versioista. Alla linkit yleisten internet-selainvalmistajien ohjeisiin:
Apple Safari
Google Chrome
Microsoft Internet Explorer
Mozilla Firefox

Case B. Hyviä käytäntöjä päätelaitteen suojaamiseen

Haittaohjelmien torjunta

Päätelaitteet kannattaa suojata haittaohjelmilta erillisen päivittyvän haittaohjelmien torjuntasovelluksen avulla. Haittaohjelmien torjunta ei takaa täydellistä suojaa haittaohjelmilta, mutta pienentää haittaohjelmien tartuntariskiä. Haittaohjelmien torjuntaohjelmistoa kannattaa käyttää myös älypuhelimissa ja tablet-laitteissa. Erityisesti Windows -työasemat ja Android -käyttöjärjestelmällä toimivat mobiililaitteet on syytä suojata päivittyvällä haittaohjelmien torjuntaohjelmistolla. Osa haittaohjelmien torjuntasovelluksista tarkistaa myös internet-selailun osoitteet ja suoritettavat tiedostot tunnetuista haitallisista sivustoista ja tiedostoista (saattaa edellyttää internet-yhteyttä torjuntasovelluksen palveluun).

Tietoturvapäivitykset

Internet-verkkoon yhteydessä olevien laitteiden ohjelmistoissa (mm. käyttöjärjestelmissä, ohjelmistoissa ja sovelluksissa) havaitaan päivittäin virheitä, joita hyväksikäyttämällä laitteiden tietoturvallisuus voidaan murtaa. Tällaisia havaittuja haavoittuvuuksia korjataan laitteisiin asennettavilla tietoturvapäivityksillä. Päivitysten asentaminen vähentää merkittävästi tietojen vuotamisen riskiä. Näin ollen kaikille päätelaitteille on asennettava niille tarjolla olevat tietoturvapäivitykset (mm. käyttöjärjestelmiin, ohjelmistoihin ja sovelluksiin). Mobiililaitteille tällaisia päivityksiä ovat käyttöjärjestelmäpäivitykset sekä sovellusten tietoturvapäivitykset. Edellä mainitut päivitykset kannattaa määritellä asentumaan automaattisesti tai asentaa ne aina päivityskehotuksen yhteydessä. Työasemille käyttöjärjestelmä-, ohjelmisto- ja sovellustoimittajat tarjoavat myös tietoturvapäivityksiä. Päivitykset kannattaa määrittää asentumaan automaattisesti tai asentaa ne päivitysilmoituksen ilmestyessä. Työasemien päivityksistä kriittisimpiä ovat käyttöjärjestelmän (kuten Windows) tietoturvapäivitykset sekä internet-selainten, Flash- ja Java-komponenttien päivitykset.

Tarkempia ohjeita päätelaitteiden turvalliseen käyttöön löytyy mm. Viestintäviraston Kyberturvallisuuskeskuksen internetsivulta:
https://www.viestintavirasto.fi/kyberturvallisuus/laitteenturvallinenkaytto.html