SOPIMUS ASIAKAS- JA POTILASTIETOJÄRJESTELMÄSTÄ

Liite B9

Tietoturvallisuus

VERSIOHISTORIA

Päivä	Versio	Kuvaus	Tekijä
12.3.15	*3.0*	*Tarjouspyynnön liite*	*Hanketoimisto*
24.4.2015	*3.01*	*Lopullisen tarjouspyynnön liite; kirjoitusvirheiden korjauksia, päivitetty viitattuja linkkejä, korjattu viitattuja vaatimuksien (ETV_/VAA_) otsikoita.*	*Hanketoimisto*

Sisällysluettelo

1. Johdanto

1.1. Dokumentin tarkoitus

Tämä liite taustoittaa Apotti -asiakas- ja potilastietojärjestelmän (järjestelmä) tietoturvallisuutta ohjaavia, pääosin ei-toiminnallisia vaatimuksia, joiden perimmäisenä tavoitteena on varmistaa järjestelmässä käsiteltävien asiakas- ja potilastietojen luottamuksellisuus, eheys ja saatavuus.

Tietoturvallisuusliite tarkentaa Apotti-kohdearkkitehtuurissa määriteltyjä tietoturvallisuuden keskeisiä periaatteita ja erityisesti Toimitus- ja Palvelusopimuksissa tietoturvallisuutta ja tietosuojaa sekä henkilötietojen käsittelyä koskevia periaatteita ja velvoitteita.

Tietoturvallisuusliite on luonteeltaan taustoittava dokumentti, joka kuvaa hankittavaan tietojärjestelmään, tietoverkkojen rakenteeseen, tietoliikenteeseen, käyttöympäristöön ja käyttöympäristön hallinnointiin liittyviä vaatimuksia yleisellä tasolla. Sen tarkoitus on selkeyttää liitteen B08 määriteltyjä tietoturvallisuutta koskevia vaatimuksia, joita käytetään vertailuperusteena järjestelmän hankinnassa.

Vaatimukset kuvaavat tietoturvallisuuden ja tiedon suojaamisen tavoitetilan, mutta ne eivät pääsääntöisesti määrittele keinoja ja toteutustapaa, joilla tavoitetila tulisi saavuttaa. Tällä menettelyllä halutaan varmistaa, että järjestelmätoimittajalle jää mahdollisuus täyttää vaatimukset tarkoituksenmukaisimmalla ja tilaajan kannalta kustannustehokkaimmalla mahdollisella tavalla.

Vaatimuksissa lähtökohta on, että tietoturvallisuus rakentuu kerroksittain toteutetuista suojauksista. Mikäli yksi suojaus pettää, muiden kerrosten suojauskeinot takaavat sen, ettei tietojen luottamuksellisuus, eheys tai saatavuus vaarannu. Tietoturvallisuuteen ja tietosuojaan liittyvät vaatimukset kohdentuvat erityisesti seuraaviin kohteisiin:

- Henkilöstö
- Tietoturvallisuuden hallintamalli, henkilöstön koulutus ja ohjeistus
- Toimitilat
- Tietoverkot ja verkon aktiivilaitteet (reitittimet, kytkimet, palomuurit)
- Palvelimet, levyjärjestelmät, tietokannat, tulostimet, päätelaitteet
- Käyttöjärjestelmät ja sovellusohjelmistot

Tietoturvallisuutta edistävät toimenpiteet tulee aina valita ja suunnitella siten, että ne mahdollistavat asiakas- ja potilastietojen tehokkaan ja tarkoituksenmukaisen hyödyntämisen sosiaali- ja terveydenhuollon palvelu- ja hoitoprosesseissa. Erityisen tärkeää on mitoittaa toimenpiteet niin, etteivät ne aiheuta merkittävää vaaraa potilasturvallisuudelle.

Luottamuksellisuus

Henkilötietolaki [1] luokittelee henkilön terveydentilaa, sairautta, vammaisuutta, häneen kohdistuvia hoitotoimenpiteitä, sosiaalihuollon tarvetta, hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia koskevat tiedot (myöhemmin ”asiakas ja potilastiedot”) arkaluonteisiksi tiedoiksi. Laki takaa kuitenkin henkilöä hoitaville sosiaali- ja terveydenhuollon ammattihenkilöille oikeuden käsitellä asiakas- ja potilastietoja hoitotoimenpiteiden ja asiakaspalvelun mahdollistamiseksi.

Tietoaineistojen luottamuksellisuusvaatimukset kohdistuvat järjestelmässä tiettyihin toimintoihin ja tietoihin. Järjestelmän tulee toteuttaa riittävät hallinnolliset ja tekniset suojaukset, jotta asiakas- ja potilastietojen luottamukselisuus säilyy nimetyllä käyttäjäryhmillä tai rooleilla. Erityisesti tulee huolehtia siitä, että:

- potilastietoja voidaan välittää tietoverkoissa salattuina, luottamuksellisuutta vaarantamatta
- tietojen näkyvyys järjestelmässä voidaan rajata vain valtuutetuille ammattihenkilöille riittävän hienojakoisen käyttövaltuusmäärittelyn ja pääsynvalvonnan avulla, ja kansalaisten osalta heidän omiin tietoihinsa
- järjestelmän ja potilastiedon valtuudeton tai sääntöjenvastainen käyttö voidaan havaita, ja tapahtuma voidaan jäljittää kiistämättömästi luonnolliseen henkilöön

Eheys

Asiakas- ja potilastietojen virheettömyys ja ajantasaisuus on palveluprosessien ja potilasturvallisuuden kannalta ensiarvoisen tärkeää. Järjestelmän tulee tarjota suojauskeinot, joilla taataan, että ainoastaan sosiaali- ja terveydenhuollon valtuutettu ammattihenkilöstö voi ylläpitää asiakas- ja potilastietoja. Lisäksi järjestelmän tulee sisältää mekanismit, joilla edesautetaan sitä, että asiakas- ja potilastietojen eheys säilyy tietoja päivitettäessä, koostettaessa niitä useista lähteistä ja välitettäessä tietoja tietoverkoissa.

Saatavuus

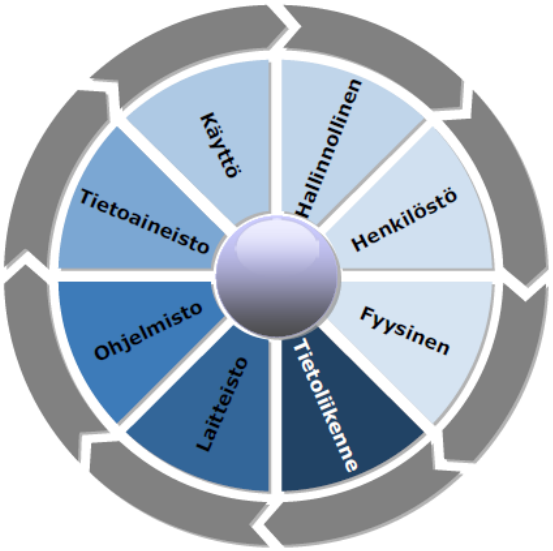
Järjestelmän tulee mahdollistaa sosiaali- ja terveystoimien ammattihenkilöille pääsy ajantasaisiin asiakas- ja potilastietoihin joustavasti hoito- ja palveluketjun eri vaiheissa. Erityisesti kliinisessä hoitotyössä järjestelmän ja sen sisältämien tietojen oikea-aikainen saatavuus on kriittistä, mikä tulee huomioida erityisesti teknisten tietoturvakontrollien toteutuksessa. Saatavuuden näkökulmasta olennaista on, että järjestelmä ei haittaa potilaan tarvitseman oikean hoidon saamista.

Toiminnallisuuksien tulee olla käytettävissä tarveperusteisesti myös monikanavaisesti. Sen tulee tukea tietoturvallisesti liikkuvaa työtä ja etäkäyttöä myös langattomilla päätelaitteilla. Etäkäyttöön kohdistuu tietoturvallisuuden osalta erikseen määriteltyjä vaatimuksia.

Järjestelmän kapasiteetti tulee mitoittaa järjestelmän käyttäjämäärän ja käyttötapausten perusteella siten, että tallennus-, laskenta- ja tiedonsiirtokapasiteetti on saatavuusvaatimusten mukainen.

1.2. Dokumentin rakenne

Tietoturvallisuuteen ja tietosuojaan kohdistuvat vaatimukset voidaan jaotella kahdeksaan keskeiseen osa-alueeseen (Kuva 1). Osa-alueisiin kohdistuvat vaatimukset on kuvattu yksityiskohtaisesti omissa päätason kappaleissaan.



Kuva 1 Tietoturvallisuuden osa-alueet (lähde: VAHTI)

Tietoturvallisuusliitteen tässä versiossa keskitytään määrittelemään pääsääntöisesti järjestelmään ja -järjestelmätoimittajaan kohdistuvia vaatimuksia seuraavien osa-alueiden osalta:

- Pääsynhallinta ja käyttövaltuushallinta
- Tietoliikenneturvallisuus
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Henkilöstöturvallisuus

Fyysistä, hallinnollista, käyttö- ja tietoaineistoturvallisuutta käsitellään tietoturvallisuusliitteen tässä versiossa pintapuolisesti, sillä niistä johdetut vaatimukset kohdentuvat pääosin tilaajaorganisaatioon ja järjestelmän palvelutuotannosta ja operoinnista vastaavaan toimittajaan – eivät niinkään valmisohjelmistoihin tai järjestelmä-toimittajaan. Osa-alueisiin liittyviä yksittäisiä vaatimuksia voidaan kuitenkin käsitellä muissa kappaleissa.

1.3. Rajaukset

Asiakas- ja potilastietojen luottamuksellisuuden, eheyden ja saatavuuden varmistaminen edellyttää, että vaaditut suojaukset toteutetaan yhdenmukaisesti tietojenkäsittelyn koko ketjussa. Tämä tarkoittaa, että järjestelmän lisäksi myös kaikki sitä käyttävät organisaatiot (esimerkiksi perusterveydenhuollon, sosiaalihuollon ja erikoissairaanhoidon organisaatiot) täyttävät vaaditun tason niin tietoturvallisuuden hallinnan kuin teknisten suojausten osalta.

Tietoturvallisuusliitteen tässä versiossa ei pyritä tyhjentävästi kuvaamaan asiakas- ja potilastietojärjestelmää käyttäviin organisaatioihin kohdistuva vaatimuksia. Vaatimusten perusta on kuitenkin sama kuin itse järjestelmän.

1.4. Sanasto

Käsite	Selitys
Kertakirjautuminen	Pääsynvalvonnan toteutustapa, jossa käyttäjä pääsee yhdellä tunnistautumisella kaikkiin saman pääsynvalvonnan piirissä oleviin palveluihin ja resursseihin käyttövaltuuksiensa puitteissa [14].
Monen tekijän todentaminen (engl. multi-factor auhentication)	Käyttäjän todentamismenetelmä, jossa käytetään useampaa kuin yhtä todennustapaa, esimerkiksi sähköistä varmennetta ja biometrista tunnistusta (vrt. yhden tekijän todentaminen) [14].

Käsite	Selitys
Palvelun tarjoaja (engl. service provider)	Federoidussa pääsynhallinnassa järjestelmäpalvelua tarjoava osapuoli, joka nojaa tunnistuslähteen suorittaman käyttäjän tunnistukseen ja sen välittämään tunnistusselosteeseen.
Provisiointi	Käyttäjä- ja käyttövaltuustiedon välittäminen palvelujärjestelmiin [14].
Rooli	Joukko käyttäjän ominaisuuksia, jotka liittyvät hänen tietotarpeittensa tai ja/tai toimivaltuuksiensa määrittelyyn [14]. Roolipohjaisessa käyttövaltuus-/pääsynhallinnassa roolien avulla määritellään käyttäjälle palvelujärjestelmässä myönnettävien käyttövaltuuksien joukko.
Tunnistuslähde (engl. identity provider)	Federoidussa pääsynhallinnassa osapuoli, joka vastaa käyttäjän tunnistamisesta ja välittää tunnistusselosteen palvelujärjestelmään [14].
Tunnistussseloste (engl. assertion)	Tunnistajan palvelujärjestelmälle toimittava selvitys, joka sisältää todennettua käyttäjäidentiteettiä vastaavia tietoja käyttäjästä [14].
Vahva todentaminen	Ks. monen tekijän todentaminen
Yhden tekijän todentaminen (engl. single-factor auhentication)	Käyttäjän todentaminen, joka hyödyntää vain yhtä seuraavista kolmesta tekijästä: mitä henkilö on, mitä henkilöllä on tiedossa ja mitä henkilöllä on halussa (vrt. monen tekijän todentaminen) [14].

2. Järjestelmän vaatimuksenmukaisuus

Asiakas- ja potilastietoa tulee käsitellä järjfestelmässä niiden sähköistä käsittelyä koskevan lainsäädännön mukaisesti. Järjestelmän tietoturvallisuusvaatimusten lähtökohtina ovat henkilötietolaki [1] sekä laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä [2], jotka säätelevät salassa pidettävien henkilö-, asiakas- ja potilastietojen käsittelyä.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa [4] (”tietoturvallisuusasetus”) määrittelee oheisen kaavion mukaisesti neljä suojaustasoa (Kuva 2).

LIITE 3: SUOJAUSTASOT JA MUITA MÄÄRITELMIÄ

1. **Suojaustasot ja turvallisuusluokkamerkinnät**

1.10.2010 voimaan tullut Valtionhallinnon tietoturva-asetus määrittää suojaustasot yksinkertaistettuna seuraavasti:

- mitä tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa?

- Suojaustasomerkintöjä voidaan täydentää turvallisuusluokitusmerkinnöillä silloin, kun turvallisuusluokittelulle on erityiset perusteet (vahinkoa kv. suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle, TTA 12§):

Suojaustaso I	Erityisen suurta vahinkoa yleiselle edulle
Suojaustaso II	Merkittävää vahinkoa yleiselle edulle
Suojaustaso III	Vahinkoa yleiselle tai yksityiselle edulle
Suojaustaso IV	Haittaa yleiselle tai yksityiselle edulle, viranomaisen toimintaedellytysten heikentyminen, rajoittava käyttötarkoitussidonnaisuus

Kuva 2 Tietoaineiston tietoturvallisuusasetuksen mukaiset suojaustasot (lähde; Katakri II [5])

Tietoturvallisuusasetus ei nimenomaisesti määrittele, mitä suojaustasoa asiakas- ja potilastiedon käsittelyssä tulee soveltaa: asianmukainen suojaustaso tulee johtaa tietoturvallisuusasetuksen 9 §:n 1 momentin perusteella suoritetussa vaikutusarvioinnissa. Järjestelmän kohdalla vaikutusarvioinnissa on päädytty siihen, että asiakas- ja potilastietojen käsittely suojaustason tulee olla III, jonka vaikutukset on tietoturvallisuusasetuksessa määritelty seuraavasti:

> *Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi* ***aiheuttaa vahinkoa*** *salassapitosäännöksessä tarkoitetulle* ***yleiselle tai yksityiselle edulle****.*

Tietoaineiston suojaustasoa III vastaavat sekä VAHTI-ohjeistuksessa ja Katakri-auditointikriteetistössä ”Korotettu taso”. Tämän dokumentin vaatimukset on pääsääntöisesti johdettu seuraavista ohjeista ja kriteeristöistä:

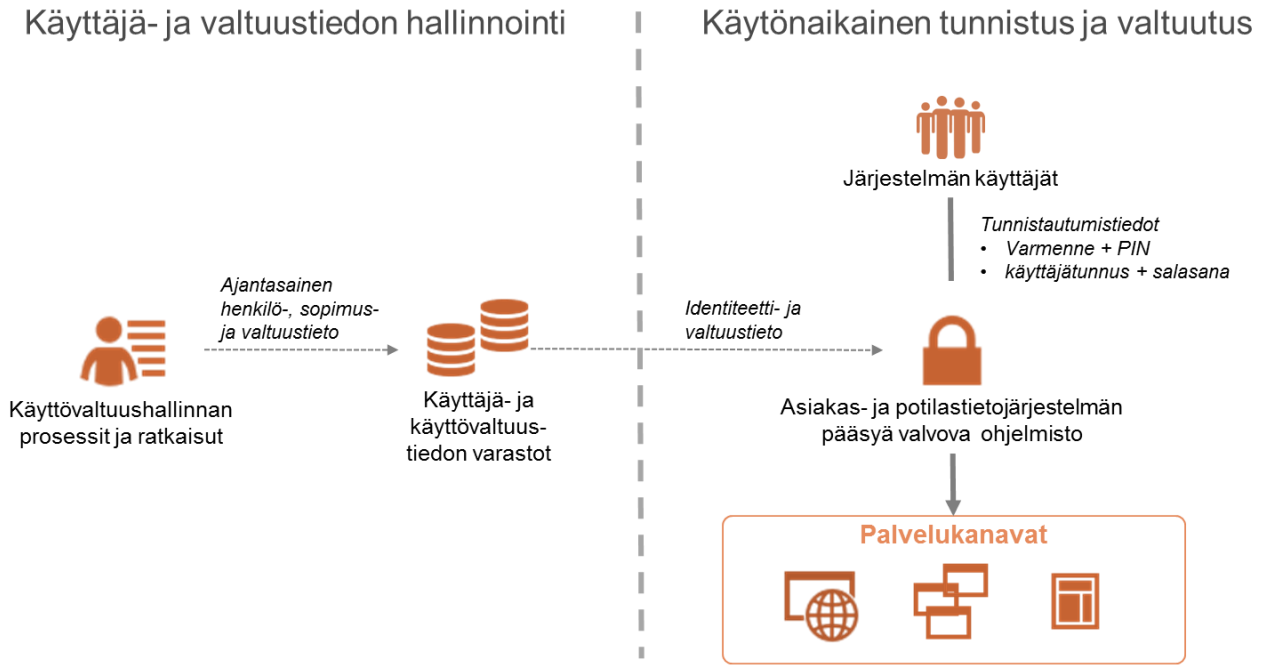
- Sovelluskehityksen tietoturvaohje, VAHTI 1/2013
- Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012
- ICT-varautumisen vaatimukset, Vahti 2/2012
- Määräys A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista tietoturva-vaatimuksista (THL)
- Kansalliset auditointivaatimukset potilastietojärjestelmille (STM)
- Kansalliset auditointivaatimukset välittäjille (STM)
- Kansallinen turvallisuusauditointikriteeristö (KATAKRI)

Viitteet kriteeristöihin löytyvät kappaleesta 11.

3. Pääsynhallinta ja käyttövaltuushallinta

Kappaleessa 1.2 esitellyssä luokittelussa pääsynhallinta ja käyttövaltuushallinta sisältyvät mm. henkilöstö-turvallisuuden ja käyttöturvallisuuden osa-alueisiin. Pääsyn- ja käyttövaltuushallinnan vaatimukset on tässä kuitenkin eriytetty kokonaan omaksi kappaleekseen, sillä ne ovat järjestelmän joustavan ja turvallisen käytön kannalta keskeisiä.

Asiakas- ja potilastiedon tehokas ja tietoturvallinen hyödyntäminen asiakas- ja hoitoprosessin eri vaiheissa edellyttää, että käyttäjät tunnistetaan yksilöidysti, käyttäjien henkilöllisyys todennetaan luotettavasti, ja että tietojen katselu- ja muokkausvaltuuksia kyetään hallinnoimaan joustavasti, käyttäjäkohtaisesti, käyttäjäroolikohtaisesti ja riittävän tarkalla tasolla. Kuva 3 havainnollistaa käyttövaltuushallinnan ja pääsynhallinnan ratkaisujen rooleja edellä mainittujen tavoitteiden saavuttamisessa.



Kuva 3 Käyttövaltuushallinta ja pääsynhallinta

Käyttövaltuushallinnalla (engl. identity management) tarkoitetaan prosesseja sekä niitä tukevia teknisiä apuvälineitä ja ratkaisuja, joilla ylläpidetään järjestelmän käyttäjä- ja käyttövaltuustiedot oikeina ja ajantasaisina kaikissa muutostilanteissa (esimerkiksi käyttäjän työ- ja palvelusopimussuhteen, työnkuvan, vastuiden tai tietotarpeiden muutokset). Pääsynhallinnan ratkaisuilla puolestaan rajataan pääsy tietojärjestelmään ainoastaan valtuutetuille käyttäjille, heille myönnettyjen valtuuksien rajoissa. Pääsynhallintapäätös suoritetaan aina järjestelmän käyttöhetkellä ja se perustuu i) käyttäjän hallussa oleviin tunnistusvälineisiin (toimikortti ja sille tallennettu varmenne, käyttäjätunnus-/salasanapari) sekä ii) käyttäjä- ja valtuustiedon varastossa oleviin valtuustietoihin.

Pääsynhallinnan ja käyttövaltuushallinnan kontrollivaateet voidaan jakaa karkeasti ehkäiseviin ja havaitseviin. Pääosa tämän liitteen vaatimuksista määrittää ehkäiseviä kontrolleja, joilla pyritään estämään asiakas- ja potilastietojen valtuudeton käyttö ennakolta mutta mahdollistetaan toisaalta järjestelmän vaivaton käyttö asiakas- ja hoitoprosesseihin osallistuville sosiaali- ja terveydenhuollon ammattihenkilöille.

Tärkeimpiä esimerkkejä ehkäisevistä kontrolleista ovat:

- Käyttövaltuuksien hallintaprosessi ja sitä tukevat tekniset ratkaisut edistävät **pienimmän käyttövaltuuden periaatteen** toteutumista. Periaatteen mukaisesti kullakin käyttäjällä tulee olla järjestelmässä vain ne käyttövaltuudet, joita hän tarvitsee työtehtäviensä suorittamiseksi – ei enempää. Valtuuksien tulee olla linjassa käyttäjän sen hetkisen organisaatioaseman, työnkuvan, vastuiden ja tietotarpeiden kanssa. Työnkuvassa ja vastuissa tapahtuvat muutokset ja muutosten vaikutukset käyttövaltuuksiin kyetään havaitsemaan viiveettä ja niitä vastaavat muutokset käyttövaltuuksiin kyetään toteuttamaan hallitusti.
- Järjestelmän tulee tukea **käyttäjien elinkaarenhallintaa** siten, että oikeus järjestelmän käyttöön voidaan johtaa ulkoisissa tietojärjestelmissä ylläpidettävistä ammattihenkilöiden palvelussuhdetiedoista. Järjestelmän käyttö estetään teknisesti ilman tarpeetonta viivytystä perusteen päätyttyä.
- **Käyttäjän todentamisessa** sovelletaan järjestelmässä käsiteltävän tietoaineiston suojaustasosta johdettua riittävän vahvaa ja luotettavaa menettelyä.
- Käyttövaltuusmallin tulee tukea **vastuiden eriyttämistä** siten, ettei käyttäjä voi saada tahattomasti järjestelmässä sellaista kiellettyä käyttövaltuuksien yhdistelmää, joka mahdollistaa asiakas- ja potilastietojen väärinkäytön tai voi vaarantaa potilasturvallisuuden.

Terveydenhuollon käyttötapauksissa ehkäisevät kontrollit eivät ole yksinään riittävän joustavia. Vaikka asiallinen syy-yhteys ammattihenkilön ja potilaan välillä on edellytys salassa pidettävien henkilötietojen katselulle, käyttäjien valtuuksia on käytännössä vaikeaa rajata potilas- ja hoitotapahtumakohtaisesti niin, ettei potilasturvallisuus vaarantuisi. Potilaan hengen ollessa kyseessä tietoturvakontrollien on joustettava. Jotta tätä joustoa ei käytettäisi väärin, tarvitaan myös täydentäviä havaitsevia kontrolleja. Pääsynhallinnan yhteydessä merkittävin havaitseva kontrolli on kirjautumistapahtumien ja järjestelmäkäytön tapahtumien tallentaminen (lokitus), jolla voidaan todentaa jälkikäteen käyttäjien suorittamat epäonnistuneet ja onnistuneet kirjautumiset sekä käyttäjän suorittamat järjestelmätoiminnot. Pääsynvalvonta- ja käyttölokien avulla voidaan todentaa sellainen potilastietojen katselu, jossa asiallinen syy-yhteys potilaaseen puuttuu.

Käyttövaltuushallinnan ja pääsynhallinnan ehkäisevät kontrollit voidaan toteuttaa mielekkäästi joko kiinteästi osana järjestelmää, tai vaihtoehtoisesti ulkoistaa ne järjestelmään integroituihin erillisiin käyttövaltuus- ja pääsynhallinnan järjestelmiin. Asiakas- ja potilastietojärjestelmätoteutuksen pohjana olevien valmisohjelmistojen sisältämiä valtuus- ja pääsynhallinnan kyvykkyyksiä on suositeltavaa hyödyntää mahdollisimman laajasti.

Havaitsevat kontrollivaatimukset kohdistuvat kiinteämmin järjestelmään. Yksittäisen toiminnon lokitus on tehtävä järjestelmässä itsessään, sillä toimintoa ja käyttökontekstia on todennäköisesti vaikeaa – ellei mahdotonta – päätellä järjestelmän ulkopuolisessa pääsynhallintaratkaisussa.

3.1. Järjestelmän käyttäjät

Taulukko **1** sisältää yhteenvedon järjestelmän keskeisistä käyttäjäryhmistä.

Käyttäjäryhmä	Kuvaus

	Sosiaali- ja terveydenhuollon ammattihenkilöt	Sosiaali- ja terveydenhuollon ammattihenkilöt käyttävät järjestelmän toimintoja hoito- ja asiakastyön prosesseissa pääosin ammattilaisen sähköisen työpöydän kautta. Ammattihenkilöiden pääsy järjestelmän sisältämään tietoon ja toimintoihin on rajattu mm. organisaation, työnkuvan ja asiakas-/hoitosuhteen perusteella.
	Palveluntuottajien ammattihenkilöt	Käyttäjäorganisaatioille ostopalveluita tuottavien palveluntuottaja-organisaatioiden ammattihenkilöt käyttävät järjestelmän selain-käyttöisen portaalin tarjoamia toiminnallisuuksia tuotettavan palvelu-sopimuksen määrittelemässä laajuudessa. Heidän käyttövaltuuksian hallinnoi palvelusopimuksen tilaajaosapuoli.
	Kansalaiskäyttäjät	Kansalaiskäytättäjät käyttävät järjestelmän asiakas-/potilasportaalia asioidessaan sähköisesti sosiaali- ja terveydenhuollon kanssa.

Taulukko 1 **Järjestelmän käyttäjäryhmät**

3.2. Pääsynhallinta

Kaikki järjestelmän sisältämä tietoaineisto on lähtökohtaisesti ei-julkista. Järjestelmän käyttö edellyttää siten, että käyttäjä tunnistetaan yksilöidysti kaikissa käyttötapauksissa ja että käyttäjän henkilöllisyys todennetaan luotettavasti[1].

Järjestelmän kaikkien toimintojen käytön tulee tapahtua henkilökohtaisella käyttäjätunnuksella. Henkilökohtaisia käyttäjätunnuksia, varmennekorttia tai niihin liittyviä salasanoja ja PIN-koodeja ei saa luovuttaa toiselle henkilölle. Minkään järjestelmän toiminnon ei tule edellyttää kirjautumista yhteiskäyttöisellä ryhmätunnuksella. Vaatimus kohdistuu sekä loppukäyttäjätoimintoihin että järjestelmän hallinnointiin ja ylläpitoon.

Tuetut todennusmenetelmät

Järjestelmän pääsyä valvovan ohjelmiston tai muun pääsynhallinnassa käytettävän teknisen ratkaisun tulee tukea teknisesti vaihtoehtoisia käyttäjien todennusmenetelmiä, joita voidaan soveltaa eri käyttäjäryhmille ja eri palvelukanavissa käyttötapauksesta ja käsiteltävän tietoaineiston luonteesta riippuen.

Useimmissa käyttötapauksissa järjestelmän käyttö edellyttää käyttäjän luotettavaa tunnistamista yhdistettynä monen tekijän todentamismenetelmään (engl. *multi-factor authentication*), jolloin todennuksen tulee perustua käyttäjän hallussa olevaan luotettavan tahon myöntämään varmenteeseen tai muuhun yhtä luotettavaan tilaajan hyväksymään todennusmenetelmään. Tunnistamisen ja todentamisen luotettavuus tarkoittaa minimissään, että:

- tunnistetiedot ovat aina salatussa muodossa, kun ne välitetään tietoverkon ylitse

[1] Poikkeuksen muodostavat ainoastaan erikseen määritellyt käyttötapaukset, jotka kansalaisten tulee voida suorittaa nimettömästi (esimerkiksi lastensuojeluilmoitukset).

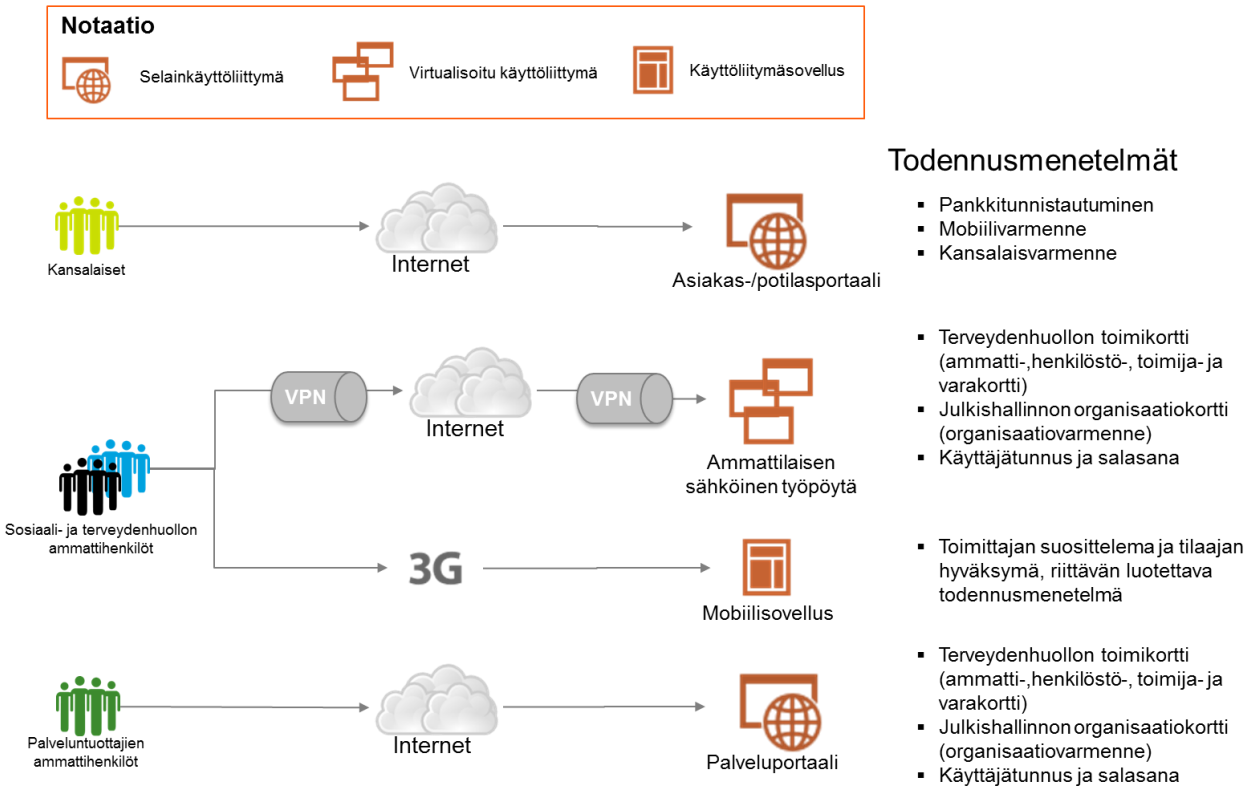
- todennusmenetelmä on suojattu välimieshyökkäyksiltä (engl. *man-in-the-middle*)
- todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä (engl. *replay attacks*) vastaan
- todennusmenetelmä on suojattu *brute force* -hyökkäyksiä vastaan

Perusteena monen tekijän todennuksen vaatimukselle on käsiteltävän aineiston luokittelu suojaustasolle III. Sosiaali- ja terveydenhuollon ammattihenkilöiden kohdalla vaatimus täyttyy, kun kirjautuminen suoritetaan Väestörekisterikeskuksen myöntämällä henkilökohtaisella ammatti- tai henkilöstökortilla, jolle on tallennettu sähköinen varmenne[2]. Kansalaisten sähköisten palveluiden osalta vahva todentaminen tulee toteuttaa Väestörekisterikeskuksen myöntämään kansalaisvarmenteeseen, pankkitunnistautumiseen[3] tai mobiilivarmenteeseen perustuen.

Riskianalyysiin perustuen käyttäjän todennuksessa voidaan tapauskohtaisesti käyttää myös yhden tekijän (engl. *single-factor authentication*) käyttäjätunnus-/salasanapariin perustuvaa menetelmää. Näin voidaan menetellä esimerkiksi silloin, kun järjestelmäkokonaisuudessa on tunnistettavissa osajärjestelmä, jonka kautta käsitellään ainoastaan matalan suojaustason tietoaineistoa. Käyttäjä-/salasanatunnistusta voidaan käyttää myös salassa pidettävien tietojen osalta, mikäli tiedon luottamuksellisuus voidaan taata kompensoivilla suojauksilla (esim. käyttö on sallittu vain tilasta, jonka johon pääsy on rajoitettu ja valvottu). Monen tekijän todennus on kuitenkin suositeltava kaikissa käyttötapauksissa, ja ehdoton edellytys järjestelmän etäkäytölle.

Kuva 4 haivannollistaa järjestelmän eri käyttökanavissa tuettuja käyttäjien todennusmenetelmiä.

[2] Kirjoitushetkellä Väestörekisterikeskuksen varmennepalvelut ovat ainoa hyväksyttävä varmennepalveluiden tuottaja, mutta tilanne voi muuttua järjestelmän elinkaaren aikana.
[3] Pankkitunnistautuminen on käytännössä ainoa Suomessa laajasti kansalaisten käyttämä monen tekijän todennusmenetelmä. Vaikka sirulliset henkilökortit voivat yleistyä, kansalaisille suunnatussa sähköisessä palvelukanavassa pankkitunnistautumiselle ei kirjoitushetkellä ole todellisia vaihtoehtoja.



Kuva 4 Tuetut tunnistamis- ja todentamismenetelmät

Varmenteisiin pohjautuvassa todennuksessa pääsyä valvovan ohjelmiston (tai muun teknisen ratkaisun) tulee tarkistaa todennuksessa käytettävien varmenteiden eheys, voimassaolo ja mahdollinen sulkulistalla olo varmenteen myöntäjän tiedoista. Sulkulista on päivitettävä pääsyä valvovan ohjelmiston käyttöön vähintään kerran vuorokaudessa.

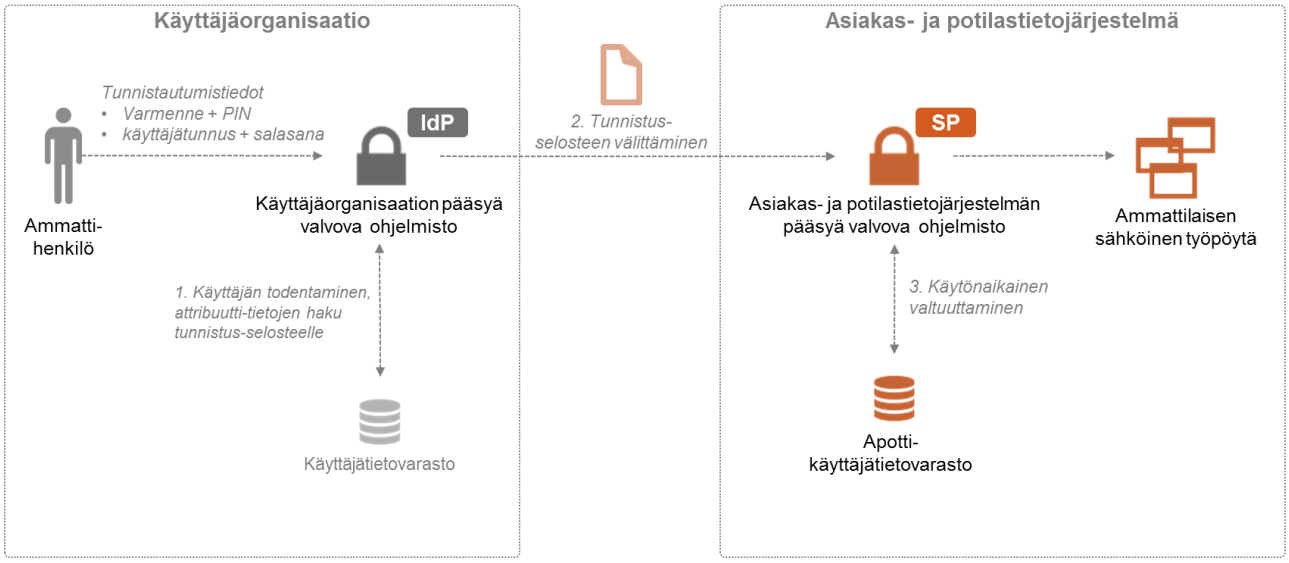
Ammattihenkilöiden pääsynhallinta

Ammattihenkilöiden pääsynhallinnan tulee lähtökohtaisesti perustua federoidun identiteetin periaatteelle. Järjestelmää käyttävän organisaation (tunnistuslähde, engl. identity provider, IdP) ja järjestelmäpalvelun tarjoajan (engl. service provider, SP) välille muodostetaan luottosuhde, jonka puitteissa käyttäjien tunnistaminen ja heidän identiteettinsä luotettava todentaminen vastuutetaan käyttäjän kotiorganisaation tehtäväksi. Käyttäjäorganisaatio välittää todennetun käyttäjän käyttäjätiedot määrämuotoisena tunnistusselosteena (engl. assertion) asiakas- ja potilastietojärjestelmään. Järjestelmän pääsyä valvova ohjelmisto tulkitsee tunnistusselosteen sisältämät identiteettiä ja käyttövaltuuksia kuvaavat attribuuttitiedot ja rajaa käyttäjälle sallitut katselu- ja muokkausoikeudet niiden mukaisesti.

Käyttäjäorganisaatioon delegoitu käyttäjien tunnistaminen selkeyttää tunnistuslähteen ja järjestelmäpalvelun välistä vastuunjakoa ja tarjoaa seuraavat konkreettiset edut:

- Asiakas- ja potilastietojärjestelmän **käyttöoikeus voidaan sitoa tehokkaasti käyttäjäorganisaation toimiviin elinkaarenhallinnan prosesseihin** – olivat ne sitten manuaalisia tai automatisoituja. Sopimussuhteen päättyessä pääsy järjestelmään estyy viiveettä, kun käyttäjän primääri käyttäjätunnus keskitetyssä käyttäjähakemistossa deaktivoidaan.
- **Tarve ylläpitää käyttäjäkohtaisia salasanoja asiakas- ja potilastietojärjestelmässä poistuu**. Niissä käyttötapauksissa, joissa todennus voidaan riskianalyysiin perustuen suorittaa käyttäjätunnuksella ja salasanalla, salasanojen ylläpitovastuu on käyttäjäorganisaatiolla.
- Federoituun identiteettiin perustuva **pääsynhallinta ei edellytä käyttäjäorganisaatioiden käyttäjähakemistojen suoria integraatioita** (eikä integraatioiden edellyttämiä tietoliikenneavauksia) asiakas- ja potilastietojärjestelmään, mikä voi olla ristiriidassa organisaatiokohtaisten tietoturvapolitiikkojen kanssa.
- **Tunnistustietojen välittäminen standardimuotoisena tunnisteselosteena mahdollistaa löyhän kytkennän (engl. loose coupling) tunnistuslähteen ja järjestelmän välillä**. Tunnistusselosteen perustuu yleisesti käytettyyn federointistandardiin (esimerkiksi SAML, engl. Security Assertion Markup Language), jolloin käyttäjäorganisaatiot voivat itse päättää, millä teknologisilla ratkaisuilla (Identity Provider -toteutus) tunnisteseloste muodostetaan. Käyttäjäorganisaatioiden työasemille ei ole tarpeen asentaa ja ylläpitää järjestelmätoimittajan määrittelemää pääsynhallinnan ohjelmistokomponenttia.

Kuva 5 havainnollistaa federoituun identiteettiin perustuvaa pääsynhallinnan ratkaisua.



Kuva 5 Federoituun identiteettiin perustuva pääsynhallinta

Ammattihenkilön kirjautuminen ammattilaisen sähköiselle työpöydälle sisältää seuraavat vaiheet:

- Ammattihenkilö käynnistää asiakas- ja potilastietojärjestelmän työasemallaan. Järjestelmän pääsyä valvova ohjelmisto ohjaa ammattihenkilön tunnistautumaan käyttäjäorganisaation pääsyä valvovaan ohjelmistoon.

- Ammattihenkilö suorittaa kirjautumisen toimikortilla tai vaihtoehtoisesti käyttäjätunnuksella ja salasanalla. Käyttäjäorganisaation pääsyä valvova ohjelmisto tarkistaa ammattikortilla olevan varmenteen alkuperän ja voimassaolon suorittamalla vertailun varmenteiden sulkulistaan.
- Käyttäjäorganisaation pääsyä valvova ohjelmisto muodostaa tunnistusselosteen perustuen organisaation käyttäjätietovarastoissa ylläpidettäviin käyttäjätietoihin ja välittää sen asiakas- ja potilastieto-järjestelmään. Seloste sisältää potilas- ja asiakastietojärjestelmän tarvitsemat henkilön yksilöinti-, attribuutti- ja roolitiedot. Seloste allekirjoitettaan sähköisesti, jotta sen alkuperä on mahdollista todentaa asiakas- ja potilastietojärjestelmässä.
- Asiakas- ja potilastietojärjestelmän pääsyä valvova ohjelmisto tarkistaa tiedot käyttäjien ammatti-oikeuksista ja ammattioikeuksien rajoituksista Valviran ylläpitämästä sanomapohjaisesta attribuuttipalvelusta. Järjestelmän tulee estää käyttäjältä toiminnot, jotka ovat ammattioikeuksien rajoitusten piirissä[4].
- Asiakas- ja potilastietojärjestelmän pääsyä valvova ohjelmisto rajaa käyttäjän pääsyn järjestelmässä vain hänen identiteettinsä ja käyttövaltuuksiensa mukaisiin tietoihin ja toimintoihin. Käytön rajaaminen (engl. authorization) perustuu i) tunnisteselosteen sisältämiin tietoihin ja ii) asiakas- ja potilastietojärjestelmän käyttäjätietovarastossa ylläpidettäviin rooli- ja valtuustietoihin[5].

Vaihtoehtoiset pääsynhallinnan ratkaisut

Federoidun identiteetin periaatteelle perustuvan pääsynhallintaratkaisun keskeinen perustelu on pääsynhallinta-päätöksen vieminen lähellä käyttäjäorganisaatioiden käyttäjähakemistoa, jolloin organisaatiokohtaisten elin-kaarenhallinnan prosessien vaikutus järjestelmänkäyttöoikeuteen on mahdollisimman välitön. Sama tavoite on mahdollista toteuttaa myös vaihtoehtoisin teknisin menetelmin, esimerkiksi:

- Asiakas- ja potilastietojärjestelmän pääsyä valvova ohjelmisto (tai sen osa) asennetaan käyttäjien työ-asemille osana käyttäjäorganisaation työasemaympäristön keskitettyä ohjelmistojakelua. Ohjelmisto käyttää suoraan organisaation varmenneinfrastruktuuria ja käyttäjähakemistoja.
- Asiakas- ja potilastietojärjestelmän pääsyä valvova ohjelmisto sijaitsee järjestelmän palvelinpäässä, mutta se integroidaan teknisesti käyttäjäorganisaatioiden käyttäjähakemistoihin (tai käyttäjäorganisaation hake-miston tietosisältö synkronoidaan säännöllisesti järjestelmän paikalliseen tietovarastoon). Vaihtoehto ei ole toivottava, sillä lähtökohtaisesti käyttäjäorganisaatiot eivät halua avata käyttäjätietovarantojaan organisaation tietoverkon ulkopuolelle.

[4] Ammattioikeuksien rajoitukset on teknisesti mahdollista tarkistaa myös käyttäjäorganisaation pääsyä valvovassa ohjelmistossa. Koska tarkistus edellyttää integraatiota Valviran attribuuttipalveluun, se on kuitenkin yksinkertaisinta toteuttaa kertaalleen asiakas- ja potilastietojärjestelmän pääsyä valvovassa ohjelmistossa.
[5] Tunnistusselosteessa on teknisesti mahdollista välittää identiteettitiedon lisäksi myös rooli- ja valtuustietoa. Tämä edellyttää kuitenkin rooli- ja valtuusrakenteiden vakiointia ja synkronointia käyttäjäorganisaation käyttövaltuushallinnan ja pääsynhallinnan järjestelmiin.

Järjestelmätoimittajan ehdottama vaihtoehtoista pääsynhallinnan ratkaisua voidaan pitää hyväksyttävänä, jos se toteuttaa pääosin tämän kappaleen alussa listatut federoidun identiteetinhallinnan edut, tarjoaa hyväksyttävän kirjautumistapahtuman vasteajan sekä mahdollistaa ammattihenkilöiden työasemaympäristöihin asennettavien ohjelmistokomponenttien tehokkaan etähallinnan.

Kertakirjautuminen

Järjestelmän tulee tukea käyttäjien kertakirjautumista siten, että käyttäjän pääsee yhdellä tunnistautumisella järjestelmän kaikkiin osajärjestelmiin ja resursseihin käyttövaltuuksiensa puitteissa. Järjestelmä välittää käyttäjäkontekstin osajärjestelmien välillä, jolloin käyttäjälle kyetään tarjoamaan sujuva käyttökokemus riippumatta järjestelmän sovellusarkkitehtuurista.

Tämä lisäksi järjestelmä mahdollistaa optiona toimialuekertakirjautuminen siten, että käyttäjä pääsee järjestelmään ilman erillistä tunnistautumista tunnistauduttuaan ensin käyttäjäorganisaation Windows-toimialueelle. Työpöytäkertakirjautumisen ehtona on, että toimialuekirjautumisessa on käytetty riittävän luotettavaa todennusmenetelmää.

Palveluntuottajien pääsynhallinta

Terveyden- ja sosiaalihuollon palveluntuottajille suunnattuun palveluntuottajaportaaliin tuettuja kirjautumistapoja ovat:

1. Terveydenhuollon varmenteet (terveydenhuollon palveluntuottajat)
2. Väestörekisterikeskuksen myöntämä organisaatiovarmenne (sosiaalihuollon palveluntuottajat) tai Väestörekisterin myöhemmässä vaiheessa sosiaalihuollon ammattihenkilöille myöntämä ammattivarmenne
3. Käyttäjätunnus-salasanapariin perustuva kirjautuminen käyttötapauksissa, joissa palveluntuottajan henkiköstö ei käsittele salassa pidettävää potilas- ja asiakastietoa

Organisaatiovarmenne on rinnastettavissa terveydenhuollon varmenteisiin. Toisin kuin terveydenhuollon varmenteita, organisaatiovarmenteiden käyttö sosiaalihuollossa on kirjoitushetkellä vähäistä.

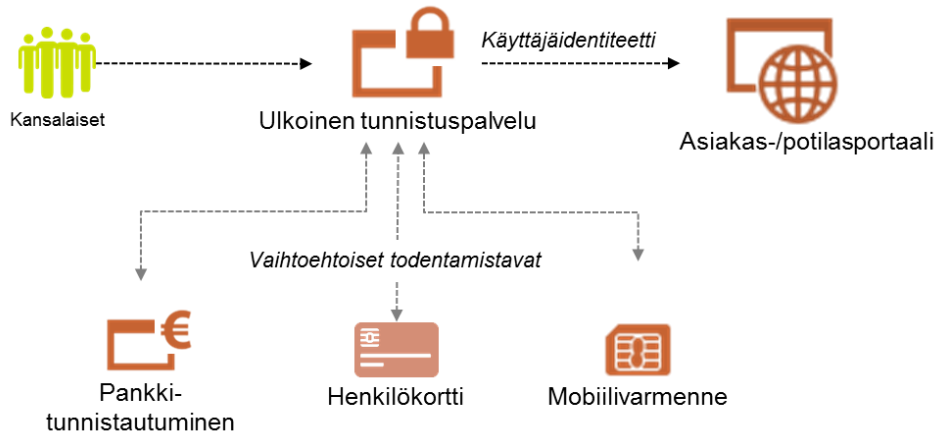
Palveluntuottajien henkilöstö, joka käyttää työtehtävissään ammattihenkilöiden sähköistä työpöytää, kirjautuu työpöydälle kappaleessa ”Ammattihenkilöiden pääsynhallinta” kuvatulla tavalla.

Kansalaiskäyttäjien pääsynhallinta

Apotin sähköisen asioinnin kanavaa (”asiakas-/potilasportaali”) käyttävät kansalaiset kirjautuvat asiakas- ja potilasportaaliin jollakin seuraavista vaihtoehtoisista tavoista:

1. Pankkitunnistus
2. Mobiilivarmenne
3. Kansalaisvarmenne (henkilökortti)

Järjestelmä tulee voida integroida ulkoiseen tunnistautumispalveluun, joka toteuttaa edellä kuvatut todentamismenetelmät. Kansalaisten kirjautumisessa voidaan hyödyntää esimerkiksi julkishallinnon yhteistä verkkotunnistamisen ja maksamisen palvelua (VETUMA), joka tarjoaa edellä kuvatut todentamismenetelmät yhdenmukaisesti samassa palvelussa.



Kuva 6 Kansalaiskäyttäjien kirjautuminen ulkoisessa tunnnistautumispalvelussa

Viitteet järjestelmähankinnan ei-toiminnallisiin vaatimuksiin

Vaatimusalue	Viitteet ei-toiminnallisiin vaatimuksiin
Tunnistusvälineiden henkilökohtaisuus Käyttäjän tunnistamisessa käytetyt tunnistusvälineet ovat aina henkilökohtaisia.	• ETV_0031 - Käyttäjätunnusten, käyttövaltuuksien, toimikorttien ja salasanojen henkilökohtaisuus
Käyttäjien tunnistaminen ja todentaminen Kaikki järjestelmän sisältämä tietoaineisto on lähtökohtaisesti ei-julkista. Ammatti- ja kansalaiskäyttäjät tulee tunnistaa yksilöidysti ja käyttäjän henkilöllisyys tulee todentaa luotettavasti. Pääsyä valvovan ohjelmiston (tai muun pääsynhallinnassa käytettävän teknisen ratkaisun) tulee tukea Suomessa käytössä olevia monen tekijän todennusratkaisuja.	• • ETV_0028 - Ammattihenkilöiden tunnistamisen ja todentamisen tuetut menetelmät • ETV_0028_01 – Ammattioikeuksien ja niihin liittyvien rajoitusten tarkistaminen • ETV_0029 – Kansalaiskäyttäjien tunnistamisen ja todentamisen tuetut menetelmät • ETV_0037 – Tuetut monen tekijän todennusmenetelmät (ammattihenkilöt) • ETV_0037_01 – Varmenteiden validointi • ETV_0037_02 – Ylläpitohenkilöstön tunnistautuminen ja todentaminen monen tekijän menetelmällä • ETV_0117 – Tunnistautumiskytkentä

Vaatimusalue	Viitteet ei-toiminnallisiin vaatimuksiin
Sisäänkirjautumisen lokitus ja pääsynvalvontalokilokien suojaaminen Pääsyä valvova ohjelmisto (tai muu pääsynhallinnassa käytettävä tekninen ratkaisu) kirjoittaa lokia sekä onnistuneista että epäonnistuneista kirjautumisyrityksistä siten, että yksittäisen käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti. Lokitiedot ja niiden kirjauspalvelut ovat suojattuja väärentämiseltä ja luvattomalta pääsyltä. Lokitiedoista otetaan varmuuskopiot säännöllisesti.	• ETV_0035 – Pääsynvalvontaloki • ETV_0036 - Pääsynvalvontalokin suojaaminen
Hyvän salasanapolitiikan soveltaminen Pääsyä valvova ohjelmisto (tai muu pääsynhallinnassa käytettävä tekninen ratkaisu) asettaa salasanan komplek-sisuudelle vähimmäisvaatimukset ja pakottaa salasanan vaihdon määräajoin. Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen. Salasanojen vanhenemisvaatimus ei koske teknisiä salasanoja.	• ETV_0033 - Hyvän salasanapolitiikan soveltaminen
Tuki kertakirjautumiselle Järjestelmän tulee tukea käyttäjien kertakirjautumista siten, että käyttäjän todennettua itsensä potilastietojärjestelmään, hän voi käyttää sen muita osajärjestelmiä ilman uudelleenkirjautumista.	• ETV_0004 – Järjestelmän sisäinen kertakirjautuminen • ETV_0004_02 – Tuki toimialuekertakirjautumiselle • ETV_0004_03 – Kirjautuminen yhteiskäyttöiseltä työasemalta
Tuki käyttäjäfederoinnille Järjestelmän tulee mahdollistaa ns. federoidun identiteetin käyttöskenaario. Skenaariossa järjestelmän tarjoavan ja sitä käyttävien organisaatioiden välille muodostetaan luottosuhde, jonka puitteissa käyttäjien todennus luotetaan käyttäjän kotiorganisaation tehtäväksi.	• ETV_0040 – Ammattihenkilöiden federoitu pääsynhallinta • ETV_0040_01 – Roolitiedon välittäminen tunnisteselosteessa
Käyttäjän ja päätelaitteen vahva tunnistus etäyhteydellä Käyttäjän tunnistamiseen etäyhteydellä voidaan soveltaa edellä kuvattuja vahvan todennuksen menetelmiä tai muuta yhtä hyvän turvatason tuottavaa ratkaisua, joka estää esimerkiksi varastetun laitteen tai identiteetin kautta palvelun väärinkäyttämisen	• ETV_0038 – Käyttäjän vahva tunnistaminen ja todentaminen etäyhteydellä • ETV_0039 – Päätelaitteen tunnistaminen

3.3. Käyttövaltuushallinta

Käyttövaltuushallinnan ratkaisujen avulla käyttäjäorganisaatioiden vastuuhenkilöt voivat lisätä, muokata ja poistaa käyttäjien valtuuksia järjestelmässä. Asiakas- ja hoitoprosessien sujuvuus edellyttää, että käyttäjien tarvitsemien käyttövaltuuksien haku-, hyväksyntä- ja myöntökäytännöt ovat vaivattomia ja viiveettömiä. Terveydenhuollon

erityispiirteet, erityisesti osa-aikaisten työntekijöiden runsaus ja käyttäjien moniedustuksellisuus[6], vaativat käyttövaltuushallinnan menettelyiltä joustavuutta.

Hajautettu käyttäjähallinta

Ammattihenkilön oikeus järjestelmän käyttöön perustuu luonnollisen henkilön ja järjestelmää käyttävän käyttäjä- tai palveluntuottajaorganisaation väliseen työ- tai palvelusopimussuhteeseen. Koska sopimusten hallinta on käyttäjäorganisaatioiden vastuulla, myös vastuu käyttäjähallinnan prosesseista sekä valtuustapahtumien lokituksesta ja jäljitettävyydestä kuuluu luontevasti käyttäjäorganisaatioille. Asiakas- ja potilastietojärjestelmän tulee mahdollistaa käyttäjäorganisaatioihin hajautettu käyttäjä- ja käyttövaltuushallinta siten, että:

1) organisaatiot voivat hyödyntää omia toimivia käytäntöjään ja teknisiä ratkaisujaan oman henkilöstönsä ja palveluntuottajiensa käyttövaltuuksien hallinnassa, seurannassa ja raportoinnissa, ja
2) asiakas- ja potilastietojärjestemä tarjoaa käyttäjäorganisaatioille rajapinnat, joiden kautta muutokset henkilön sopimussuhteen tilassa (elinkaarenhallinta) sekä henkilö- ja valtuustiedoissa on mahdollista päivittää järjestelmään.

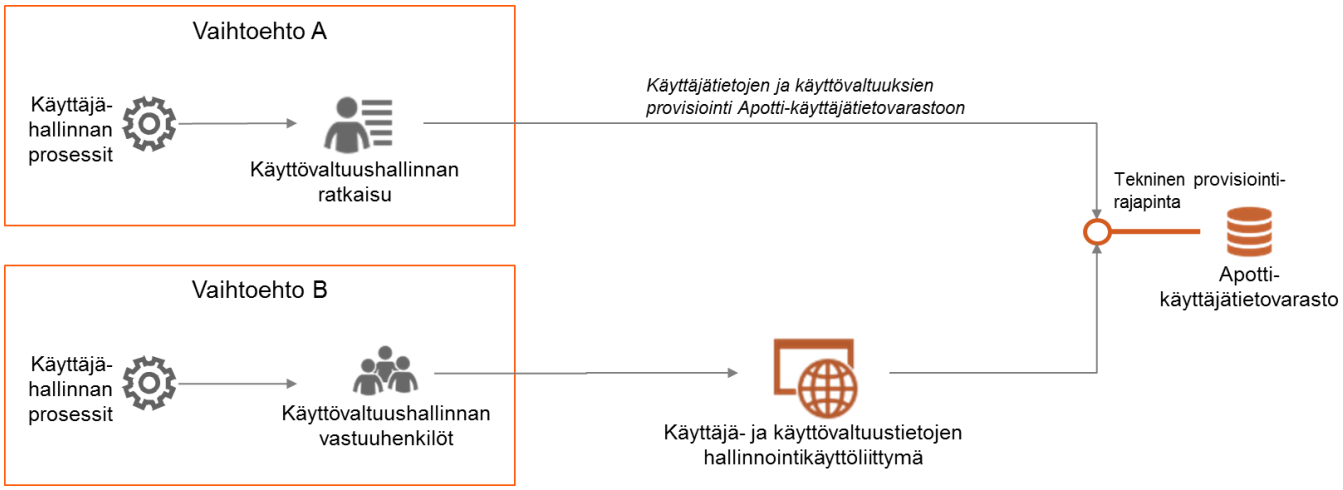
Käyttäjähallinnan edellä kuvattu hajauttaminen asettaa asiakas- ja potilastietojärjestelmälle seuraavat vaatimukset:

- Järjestelmän tulee tarjoata tekninen provisiointirajapinta, jonka kautta käyttäjäorganisaation identiteetinhallinnan järjestelmä voi luoda, muokata ja poistaa organisaation henkilöstön ja sen palveluntuottajien käyttäjä- ja valtuustietoja järjestelmässä[7]. Rajapinnan käytettävyyden tulee olla korkea ja käyttäjäprovisoinnin viiveiden lyhyitä (lähes tosiaikainen provisiointi).
- Järjestelmän tulee lisäksi toteuttaa käyttäjä- ja käyttövaltuustietojen hallinnointikäyttölittymä, joiden avulla käyttäjäorganisaation nimetyt käyttövaltuushallinnan vastuuhenkilöt voivat ylläpitää organisaationsa sekä palveluntuottajiensa käyttäjä- ja valtuustietoja järjestelmässä. Rajapinnan käytettävyyden tulee olla korkea ja viiveiden lyhyitä.
- Järjestelmätoimittajan tulee dokumentoida järjestelmän rooli-/käyttövaltuusmalli sillä tarkkuudella, että käyttäjäorganisaatiot kykenevät dokumentaation perusteella hallinnoimaan omien käyttäjiensä rooleja ja käyttövaltuuksia järjestelmässä. Toimittajan tulee myös sitoutua ylläpitämään dokumentaatiota aina, kun järjestelmästä tai sen osasta julkaistaan uusi versio, jonka seurauksena rooli-/käyttövaltuusmalli muuttuu.

Kuva 7 havainnollistaa hajautetun käyttäjähallinnan vaihtoehtoisia ratkaisumalleja.

[6] Moniedustuksellisuus tarkoittaa tilannetta, jossa sama luonnollinen henkilö toimii samanaikaisesti eri rooleissa, ja järjestelmässä tulee soveltaa istuntokohtaisesti eri valtuuksia roolista riippuen.

[7] Kappaleessa ”Ammattihenkilöiden pääsynhallinta” kuvatussa federoidun identiteetin skenaariossa on teknisesti mahdollista välittää järjestelmään tunnisteselosteessa identiteettitiedon lisäksi myös rooli- ja valtuustietoa. Käytännössä potilas- ja asiakastietojärjestelmän valtuusmalli on suurella todennäköisyydellä niin monimutkainen, että käyttäjien valtuuttaminen (engl. authorization) järjestelmässä pelkästään tunnisteselosteen tietojen pohjalta ei ole mahdollista.



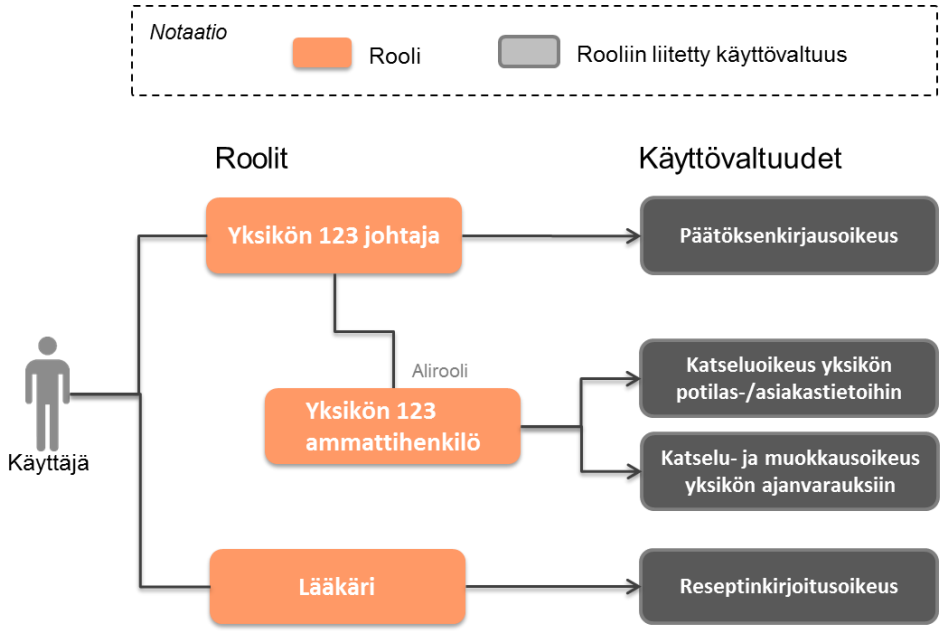
Kuva 7 Järjestelmän käyttäjien elinkaarenhallinnan vaihtoehdot

Käyttäjäorganisaatioden vaihtoehtoiset tavata oman henkilöstönsä ja palveluntuottajaverkostonsa käyttövaltuuksia järjestelmässä ovat:

- **Vaihtoehto A – Identiteetinhallinan järjestelmäintegraatio** Asiakas- ja potilastietojärjestelmän käyttäjäroolit on mallinnettu käyttäjäorganisaation omaan käyttövaltuushallinnan (identiteetinhallinnan) järjestelmään, johon on toteutettu myös käyttäjien elinkaarenhallinnan prosessit, valtuuksien haku- ja hyväksyntätyönkulut sekä valtuuksien raportointitoiminnot. Käyttövaltuushallinnan järjestelmä integroituu asiakas- ja potilastietojärjestelmään sen tarjoaman teknisen provisiointirajapinnan kautta ja ylläpitää automatisoidusti käyttäjä- ja valtuustietoja.
- **Organisaatio B – Manuaalinen hallinnointi** Organisaation käyttäjähallinta perustuu suurelta osin manuaalisiin prosesseihin ja siltä puuttuu kyvykkyys provisoida käyttäjätietoa teknisen provisiointirajapinnan kautta. Organisaation vastuutetut henkilöt ylläpitävät oman henkilöstönsä että ulkoisten palveluntuottajiensa käyttäjä- ja valtuustiedot ajantasaisina järjestelmän tarjoamassa hallinnointikäyttöliittymässä. Organisaatio on myös tässä tapaksessa vastuussa mm. käyttövaltuuspyyntöjen hyväksyntöjen ja myöntöperusteiden jäljitettävyydestä (ks. kappale ”Käyttövaltuuksien jäljitettävyys”).

Käyttövaltuuksien roolipohjainen hallinta

Järjestelmän tulee mahdollistaa roolipohjainen käyttövaltuuksien hallinta siten, että eri rooleilla on erilaiset oikeudet järjestelmän sisältämään tietoon ja sen tarjoamiin toimintoihin. Kukin rooli voi pitää sisällään useita käyttövaltuuksia, ja roolien yhdistelmillä on mahdollista hallita tehokkaasti ja virheettömästi laajan käyttäjäpopulaation käyttövaltuuksia. Yksittäinen käyttäjä voidaan liittää hänen toimenkuvaansa, tietotarpeitaan, toimivaltuuksiaan tai muuta ryhmittelevää tekijää vastaaviin rooleihin. Kuva 8 havainnollistaa roolipohjaisen käyttövaltuushallinnan periaatetta yksinkertaistetun esimerkin kautta.



Kuva 8 Roolipohjaisen käyttövaltuushallinnan periaate

Roolipohjaisen hallintamallin tulee olla valtuushallinnan pääasiallinen lähestymistapa, sillä erityisesti sairaala-ympäristöissä roolimallista poikkeavat erilliskäyttövaltuudet ovat tapahtumien jäljitettävyyden ja auditoinnin kannalta ongelmallisia. Lisäksi Apotti-kohdearkkitehtuuri määrittelee, että esimerkiksi ammattilaisen työpöydän personoinnin tulee perustua ammattirooleihin.

Järjestelmän tulee mahdollistaa organisaatioyksikköä ja ammattinimikkeitä (ja muita vastaavia ryhmitteleviä tekijöitä) vastaavien käyttövaltuuksien määrittely yleiskäyttöisinä rooleina siten, että henkilön liittäminen yksikköä/ammattinimikettä vastaavaan rooliin antaa hänelle ko. vastuun edellyttämät käyttövaltuudet järjestelmässä. Oheinen taulukko sisältää esimerkkejä roolipohjaissa valtuushallinnassa hyödynnettävistä ryhmittelevistä tekijöistä.

Ryhmittelevä tekijä	Sovellusesimerkkejä
Ammattiryhmä	• Reseptinkirjoitusoikeus järjestelmässä myönnetään lääkäreiden ammatti-ryhmää edustavan roolin kautta • Oikeus tehdä lääketilauksia ja hyväksyä lääkemääräyksiä määritellään omana roolinaan. Rooliin liitetään ainoastaan lääketilausprosessin määritellyt ammattiryhmät.
Organisaatioyksikkö tai toimipiste	• Asiakas- ja potilastietojen katselu- ja muokkausvaltuudet rajataan toimipistekohtaisesti
Hallinnollinen vastuu/asema	• Ainoastaan organisaatioyksikön hallinnollinen esimies voi kirjata tiettyjä päätöksiä

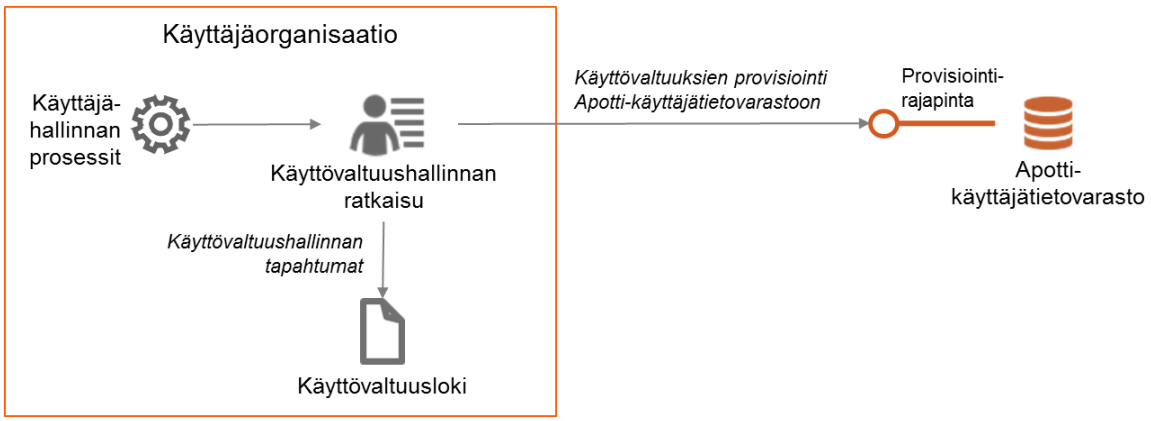
Järjestelmässä tulee olla mahdollisuus määritellä sääntöjä, joiden perusteella rooli myönnetään käyttäjille automaattisesti ilman erillistä pyyntöä tai hyväksyntää. Säännöt voivat perustua edellä kuvattuihin, järjestelmän käytössä oleviin ryhmitteleviin tekijöihin.

Järjestelmässä tulee voida määritellä joustavasti uusia rooleja ja niihin liittyviä käyttövaltuuksia sosiaali- ja terveydenhuollon prosessien toiminnallisen vastuunjaon mukaisesti.

Käyttövaltuuksien jäljitettävyys

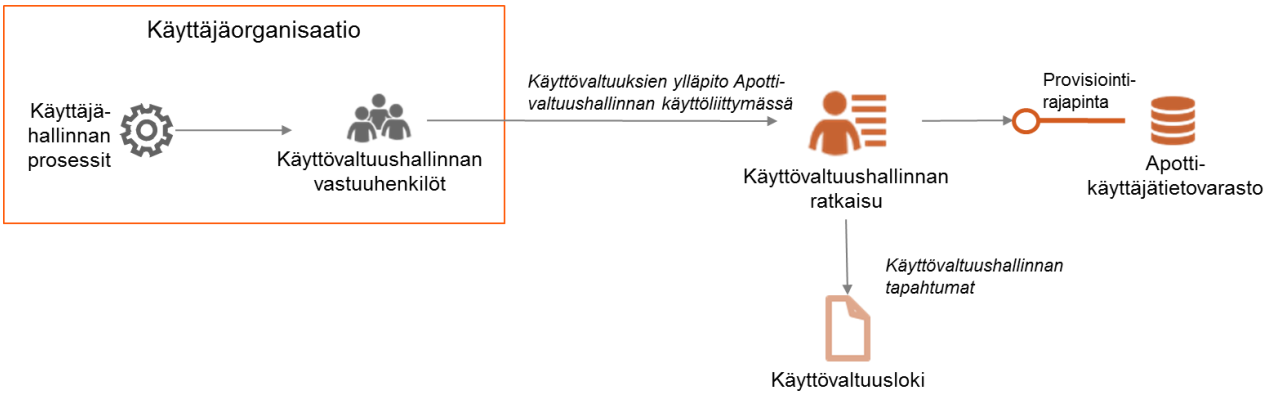
Käyttövaltuushallinnan tapahtumista (myönnetyistä käyttövaltuuksista ja niihin tehdyistä muutoksista) on pidettävä lokia (”käyttövaltuusloki”), jonka avulla on mahdollista jälkikäteen selvittää käyttäjän tietyllä ajanhetkellä voimassa olleet käyttövaltuudet järjestelmässä. Käyttövaltuuslokiin on tallennettava tiedot anotuista, hyväksytyistä, toteutetuista, muutetuista ja poistetuista käyttövaltuuksista. Lokitettavista tapahtumista on tallennettava tapahtuman nimi/tunniste, tekijä, hyväksyjä, myöntöperuste ja aikaleima.

Lähtökohtaisesti käyttäjien valtuuttaminen tarvittavine hyväksyntöineen suoritetaan kokonaisudessaan käyttäjäorganisaatioissa hyödyntäen organisaation omia käyttövaltuushallinnan ratkaisuja, jolloin lokitusvastuu on organisaatiolla itsellään (Kuva 9). Valtuutusprosessin lopputulema, hyväksytyt käyttövaltuudet, provisioidaan asiakas- ja potilastietojärjestelmään sen tarjoaman teknisen provisiointirajapinnan kautta.



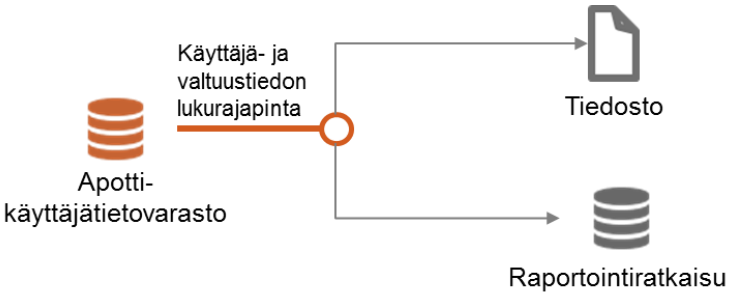
Kuva 9 Käyttövaltuuslokitus käyttäjäorganisaation omassa käyttövaltuushallinnan ratkaisussa

Mikäli asiakas- ja potilastietojärjestelmä itsessään sisältää edistyneet käyttövaltuuksien hyväksyntätyönkulku- ja lokitustoiminnot käyttäjäorganisaatioiden valtuushallinnan vastuuhenkilöiden käyttöön (ks. Kuva 7, Käyttäjäorganisaatio B), kyseinen ratkaisu tuottaa käyttövaltuuslokin (Kuva 10).



Kuva 10 Käyttövaltuuslokitus asiakas- ja potilastietojärjestelmän käyttövaltuushallinnan ratkaisussa

Järjestelmän tulee molemmissa edellä kuvatuissa skenaarioissa tarjota avoin tekninen integraatiorajapinta, jonka kautta on mahdollista lukea rakenteisessa muodossa tiedot voimassa olevista käyttäjätunnuksista sekä niihin liittyvistä rooleista ja valtuuksista järjestelmän ulkopuolella tapahtuvaa analysointia ja raportointia varten.



Kuva 11 Käyttäjä- ja valtuustiedon lukurajapinta

Viitteet järjestelmähankinnan toiminnallisiin ja ei-toiminnallisiin vaatimuksiin

Vaatimusalue	Viitteet vaatimuksiin
Hajautettu käyttäjähallinta Järjestelmän käyttäjien elinkaari tulee voida sitoa ulkoisessa tietovarastossa hallinnoitaviin sopimus- ja henkilötietoihin. Järjestelmän tulee tarjota integraatiorajapinta-/pinnat, joiden kautta järjestelmän käyttäjiä voidaan ylläpitää käyttäjäorganisaation omasta henkilöstöhallinnon ja/tai käyttövaltuushallinnan järjestelmästä tai vaihtoehtoisesti erillisisen hallinnointikäyttöliittymän kautta.	• ETV_0041 - Tuki useille ulkoisille identiteetinhallinta-ratkaisuille/henkilötiedon lähdejärjestelmille • ETV_0042 – Käyttäjä- ja käyttövaltuustiedon provisiointrajapinta • VAA_5891 – Käyttövaltuustiedon halllinnointikäyttöliittymä • VAA_5892 – Hallinnointikäyttöliittymän valtuushallinta
Käyttövaltuuksien roolipohjainen hallinta Järjestelmäkokonaisuudessa hyödynnetään kauttaaltaan roolipohjaista käyttövaltuuksienhallintaa siten, että eri rooleilla on erilaiset oikeudet tietoon että toimintoihin.	• ETV_0044 – Käyttövaltuuksien roolipohjainen hallinta • ETV_0044_01 – Rooli- ja käyttövaltuusmallin dokumentointi • VAA_2513 – Käyttäjien sääntöpohjainen valtuuttaminen • ETV_0044_02 – Käyttövaltuuksien tilapäinen ohitus poikkeustilanteissa • VAA_0349 – Ulkoisten palveluntuottajien valtuushallinta • VAA_0350 – Ryhmittelevien tekijöiden hyödyntäminen valtuushallinnassa • VAA_0351 – Käyttövaltuuksien voimassaolon rajaaminen • VAA_0352 – Valtuuksien kopiointi • VAA_0355 – Käyttövaltuuksien raportointi • VAA_5893 – Uusien roolien määrittely
Kiellettyjen työyhdistelmien havaitseminen ja estäminen Kielletyt työ- ja rooliyhdistelmät on dokumentoitu ja valtuuksia myönnettäessä tai muutettaessa kiellettyjen yhdistelmien syntymistä seurataan ja estetään.	• ETV_0045 – Kiellettyjen työyhdistelmien havaitseminen ja estäminen
Käyttövaltuuksien jäljitettävyys Järjestelmä mahdollistaa käyttäjä- ja käyttövaltuustiedon jäljitettävyyden käyttövaltuuslokien avulla ja mahdollistaa em. tiedon siirron rakenteisena järjestelmän ulkopuolelle analysointia ja raportointia varten.	• ETV_0043 – Valtuutustapahtumien lokitus ja jäljitettävyys • ETV_0043_01 – Käyttäjä- ja valtuustiedon tekninen lukurajapinta

4. Tietoliikenneturvallisuus

Järjestelmässä käsiteltävän tietoaineiston eheys ja luottamuksellisuus tulee varmistaa kaikissa tiedonsiirron ja tiedon käsittelyn vaiheissa. Tässä kappaleessa esitellään tietoverkon rakenteeseen, verkon aktiivilaitteisiin, tiedon salaukseen, tietoverkon valvontaan sekä tietoliikenteen monitorointiin kohdistuvat vaatimukset. Vaatimukset pätevät tietoliikenteen koko ketjuun aina asiakas- ja potilastiedon tietovarastoista käyttäjien päätelaitteisiin asti.

Tietoliikenneturvallisuuteen kohdistuvat vaatimukset kohdistuvat erityisesti seuraaviin tietoliikenteen skenaarioihin:

- Tiedonsiirto eri luottamustason tietoverkkojen välillä (esim. DMZ-alueen ja Internet-verkon välillä)
- Tiedonsiirto päätelaitekerroksen ja palvelinkerroksen välillä
- Kansallisen palveluväylän kautta reititettävä tiedonsiirto järjestelmän ja Sote-organisaatioiden tietoverkkojen ja tietovarantojen välillä
- Tiedonsiirto järjestelmän osajärjestelmien välillä (esim. sovelluspalvelinten ja tietokantojen välillä)

Tietoliikenteen turvaaminen edellyttää tietoturvatoimenpiteitä myös ohjelmisto- ja laitteistotasolla, tyypillisesti silloin, kun salaus puretaan selväkieliseen muotoon tiedon katselua ja päivitystä varten. Näitä täydentäviä vaatimuksia on käsitelty kappaleissa 5 Laitteistoturvallisuus ja 6 Ohjelmistoturvallisuus.

Sovellettavien tietoliikenneratkaisujen tulee täyttää tässä kappaleessa kuvatut vaatimukset, riippumatta ratkaisun perustana mahdollisesti käytettävän ohjelmistotuotteen sovellusarkkitehtuurista.

4.1. Tietoliikenneverkon rakenne

Tietoliikenneverkko on jaettu turvavyöhykkeisiin ja segmentteihin käyttötarpeiden mukaan siten, että eri suojaustarpeen (osa)järjestelmät on sijoitettu erillisiin verkkoalueisiin. Eri turvatason vyöhykkeitä voidaan kytkeä toisiinsa ainoastaan erikseen määriteltyjen yhdysliikenneratkaisujen avulla. Eri suojaustason verkkojen välistä liikennettä rajoitetaan ja suodatetaan siten, että vain luvallinen liikenne sallitaan; luvaton tietoliikenne kyetään tunnistamaan ja estämään.

Julkisen Internet-verkon on oltava erotettu palomuurilla järjestelmäpalvelua tarjoavan organisaation tietoverkoista (”sisäverkko”) ja -järjestelmistä. Sisäverkkoon ja palveluihin liittyminen on mahdollista ainoastaan sallituilla laitteistolla.

4.2. Tietoliikenteen salaus

Salassa pidettävän tietoaineiston (esimerkiksi asiakirjat, sähköiset lääkemääräykset sekä asiakkaille ja potilaille välitettävät viestit) luottamuksellisuus ja eheys tulee varmistaa kaikissa tiedonsiirron ja tiedon käsittelyn vaiheissa. Tietoliikenne tulee salata käyttäen etukäteen sovittuja vahvoja salausmenetelmiä ja -algoritmeja, esimerkiksi TLS 1.1 (engl. *Transport Layer Security*).

Palvelinten välisessä TLS-salatussa tietoliikenteessä osapuolten molemminpuolisessa tunnistamisessa tulee käyttää asiakas- ja palvelinvarmenteisiin perustuvaa autentikointia palveluväärennösten ja tietojen kalasteluyritysten estämiseksi. Salaukseen liittyvien käytänteiden (mm. varmenteiden hallinta) tulee toteuttaa tietoturvallisesti.

Tilanteissa, joissa tietoliikenteen salaus joudutaan purkamaan, tulee tietoaineiston luottamuksellisuuden säilymisestä varmistua kompensoivilla suojauksilla.

Kansallisen palveluväylän kautta reititettävässä tieto-liikenteessä tulee hyödyntää palveluväylän tarjoamia palveluita, erityisesti osapuolten keskinäistä tunnistamista.

4.3. Tietoliikenteen suodatus ja monitorointi

Tietoverkoista tulevien uhkien torjunnassa verkkojen toiminnallinen eriyttäminen ja liikenteen suodattaminen on keskeisessä roolissa. Kaikki tietoliikenne on oletusarvoisesti estetty molempiin suuntiin; sallittu liikenne mahdollistetaan erikseen määriteltävillä palomuurisäännöillä. Yleisiin verkkohyökkäyksiin varaudutaan valvomalla verkon liikennettä normaalista poikkeavien tapahtumien varalta.

Tietoliikenneverkon liikennettä suodatetaan ja monitoroidaan palomuureilla ja tavittaessa IDS/IPS[8] laitteilla. Palomuurien ja IDS/IPS-laitteiden sääntöjen lisääminen, muokkaaminen ja poistaminen on selkeästi vastuutettu ja organisoitu. Säännöt dokumentoidaan ja dokumentaation ajantasaisuus tarkistetaan säännöllisin väliajoin.

4.4. Tietoverkon aktiivilaitteiden hallinta ja kovennukset

Aktiivilaitteiden kovennuksilla varmistetaan, että tietoliikenneverkon komponentit ovat tietoturvallisesti suojattuja. Verkon aktiivilaitteet on kovennettu yhtenäisen menettelytavan mukaisesti, ja laitteiden kovennuksen tulee kattaa minimissään seuraavat asiat:

- Oletussalasanat on vaihdettu ja ainoastaan tarvittavat palvelut ovat päällä
- Aktiivilaitteiden hallinta edellyttää ylläpitäjän luotettavaa tunnistamista
- Aktiivilaitteiden hallinnointiin liittyvä tietoliikenne on eriytetty muusta liikenteestä ja/tai tietoliikenteen eheys ja luottamuksellisuus on salattu. Hallinnointi on sallittu vain etukäteen määritetyistä lähteistä.
- Aktiivilaitteiden konfiguroinnissa noudatetaan laitevalmistajien ja luotettavien tahojen suosituksia.
- Aktiivilaitteiden päivitykset pidetään ajan tasalla sovittujen käytänteiden mukaisesti.
- Verkkolaitteiden asetuksiin tehdyistä muutoksista muodostetaan riittävät lokimerkinnät.

[8] Intrusion Detection/Prevention System

4.5. Langaton tiedonsiirto

Langattomasti tapahtuva tiedonsiirto tulee toteuttaa yhtä luotettavasti kuin langallinen tiedonsiirto. Päätelaitteen tiedonsiirron tulee tapahtua turvallisiksi todennetuilla tiedonsiirtoprotokollilla. Asiakas- ja potilastietojen siirto tulee voida teknisesti rajata turvallisiin protokolliin.

Salassa pidettävän tiedon välittäminen salaamattomana langattomassa tietoverkossa on lähtökohtaisesti kiellettyä. Se voidaan sallia erillisen riskianalyysin perusteella, mikäli tiedon luottamuksellisuudesta huolehditaan kompnesoivin suojauksin.

Langatonta verkkoyhteyttä tulee käsitellä kuin julkista tietoverkkoa, ja sen ylitse tapahtuva tiedonsiirto edellyttää vahvan päästä-päähän -salauksen käyttöä. Tiedonsiirto on sallittu ainoastaan tunnistetuilla ja hyväksytyillä päätelaitteilla.

4.6. Viitteet järjestelmähankinnan ei-toiminnallisiin vaatimuksiin

Vaatimusalue	Viitteet ei-toiminnallisiin vaatimuksiin
Tietoliikenneverkon rakenne Tietoliikenneverkko on jaettu turvavyöhykkeisiin ja segmentteihin käyttötarpeiden mukaan siten, että eri suojaustarpeen järjestelmät ja verkot on sijoitettu erillisiin verkkoalueisiin (looginen tai fyysinen eriyttäminen).	• ETV_0046 – Tietoliikenneverkon rakenne
Tietoliikenteen salaus Salassa pidettävän tietoaineiston luottamuksellisuus ja eheys varmistetaan kaikissa tiedonsiirron ja tiedon käsittelyn vaiheissa vahvalla salauksella.	• ETV_0050_01 – Osapuolten varmennepohjainen tunnistaminen palvelinten välisessä tietoliikenteessä • ETV_0047 – Tietojen luottamuksellisuus ja tietoliikenteen salaus • ETV_0048 – Hyväksytyt salausalgoritmit • ETV_0048_01 - Salausalgoritmien FIPS-hyväksyntä • ETV_0049 – Salausalgoritmin vaihtaminen
Tietoliikenteen suodatus ja monitorointi Tietoverkoista tulevien uhkien torjunnassa verkkojen toiminnallinen eriyttäminen ja liikenteen suodattaminen on keskeisessä roolissa. Tietoliikenneverkon liikennettä tulee suodattaa ja monitoroida palomuureilla ja tarvitaessa IDS/IPS[9] laitteilla.	*Järjestelmähankintaan kohdistuvia eksplisiittiä ei-toiminnallisia vaatimuksia vaatimusalueen osalta ei ole tunnistettu.*
Tietoverkon aktiivilaitteiden hallinta ja kovennukset Verkon aktiivilaitteiden yhdemukaisilla kovennuksilla varmistetaan, että tietoliikenneverkon komponentit ovat tietoturvallisesti suojattuja.	*Järjestelmähankintaan kohdistuvia eksplisiittiä ei-toiminnallisia vaatimuksia vaatimusalueen osalta ei ole tunnistettu.*

[9] Intrusion Detection System/Intrusion Prevention System

Vaatimusalue	Viitteet ei-toiminnallisiin vaatimuksiin
Langaton tiedonsiirto Salassa pidettävän tiedon välittäminen salaamattomanan langattomassa tietoverkossa on lähtökohtaisesti kiellettyä. Se voidaan erillisen riskianalyysin perusteella sallia, mikäli tiedon luottamuksellisuudesta huolehditaan. Tällöin langatonta verkkoyhteyttä käsitellään kuin julkista verkkoa.	• ETV 0050 – Tiedonsiirron päästä päähän –salaus • ETV_0050_01 - Osapuolten varmennepohjainen tunnistaminen palvelinten välisessä tietoliikenteessä

5. Laitteistoturvallisuus

Laitteistoturvallisuus kattaa Apotti-järjestelmäpalvelun tuottamiseen ja käyttöön tarvittavien teknisten laitteiden suojaamiseen tähtäävät tietoturvallisuustoimenpiteet. Laitteistoturvallisuuden kannalta tärkeitä kohteita ovat palvelimet, kannettavat tietokoneet, älypuhelimet, muut langattomat päätelaitteet sekä tulostimet.

Laitteistoturvallisuuden vaatimusten tavoitteena on varmistaa, että:

i. Palvelun tuottamisen kannalta kriittisen laitteiston häiriötön ja luotettava toiminta on turvattu mm. huolehtimalla varavoimansaannista, laitteiden huollosta ja vikaantuvien komponenttien kahdentamisesta.
ii. Kaikki tekniset palvelimet ja päätelaitteet on suojattu tarkoituksenmukaisesti sellaisia laitteisto- ja ohjelmistovirheitä sekä haavoittuvuuksia vastaan, joita on mahdollista hyödyntää mm. palvelunesto-hyökkäyksissä ja tietomurroissa ja jotka voivat siten vaarantaa salassa pidettävän tiedon luottamuksellisuuden, eheyden tai saatavuuden.

5.1. Palvelimet

Palvelinten laitteistoturvallisuuden osalta keskeisiä tehtäviä ovat:

- Palvelinten hallinta, ml. laiterekisterin ylläpito ja elinkaarenhallinta (esimerkiksi käytöstä poisto ja salassa pidettävää tietoaineistoa sisältävien tallennuslaitteiden tuhoaminen), laitetilojen lämmitys, ilmastointi ja häiriötön sähkönsyöttö sekä säännöllinen huoltotoiminta
- Palvelinten suojaaminen tietoturvahaavoittuvuuksilta

Tietoturvallisuusliitteen tässä versiossa keskitytään haavoittuvuuksien aiheuttamien tietoturvauhkien aiheuttamien uhkien ehkäisemiseen asianmukaisin suojauksin.

5.2. Päätelaitteet

Kohdearkkitehtuurissa tehdyn linjauksen mukaan järjestelmän tulee tukea monikanavaista käyttöä ja asiointia. Palveluja tulee voida käyttää erilaisiin käyttöympäristöihin suunnitelluilta langattomilla päätelaitteilla tarveperustaisesti tukien yhtenäistä käyttöliittymäajattelua ja työpöytäratkaisuja. Langattomalla etäkäytöllä voidaan parantaa asiakas- ja hoitoprosessien tehokkuutta ja laatua tietojen paremman saatavuuden kautta.

Tietojen suojaustaso III asettaa päätelaitteiden hallinnalle erityisvaatimuksia, joilla pyritään estämään mm. päätelaitteiden katoamisten, varkauksien ja haavoittuvuuksien aiheuttamat uhat järjestelmälle ja sitä kautta asiakas- ja potilastiedon luottamuksellisuudelle, eheydelle ja saatavuudelle. Keskeisiä tavoitteita päätelaitteiden tietoturvallisuuden parantamisessa ovat erityisesti:

- Määritellä tuetut päätelaitteet, vakioida tuettujen laitteiden tietoturvallinen käyttöympäristö sekä määritellä menettelyt laitekonfiguraatioiden ja sovellusversioiden keskitettyyn hallinnointiin

- Rajoittaa käyttäjien toimia päätelaitteessa (esimerkiksi estää luvattomien sovellusten asennus). Laitteiden käyttösäännöt on lisäksi kirjallisesti sovittu esimerkiksi työsopimuksen yhteydessä tehtävässä tietosuoja - ja tietoturvasitoumuksessa.
- Minimoida laitteelle paikallisesti tallennettavan salassa pidettävän tiedon määrä, suojata salassa pidettävä tietoaineisto riittävän vahvalla salausalgoritmilla sekä havaita tiedon valtuudeton muokkaaminen
- Estää ja havaita haittaohjelmien toiminta

5.3. Viitteet järjestelmähankinnan ei-toiminnallisiin vaatimuksiin

Vaatimusalue	Viitteet ei-toiminnallisiin vaatimuksiin
Palvelinten kovennukset Kovennuksilla pyritään estämään turvattomia palveluita ja haavoittuvuuksia hyödyntävät palvelunestohyökkäykset ja tietomurrot. Käyttöjärjestelmät tulee koventaa haavoittuvuuksien eliminoimiseksi ja niitä hyödyntävien verkkohyökkäysten ehkäisemiseksi. Kovennus kattaa vähintään seuraavat toimenpiteet: • tarpeettoman toiminnallisuuden ja käyttöjärjestelmäpalveluiden käytöstä poistaminen • turvattomien oletusarvojen muuttaminen turvallisiksi (esim. salasanat, tietoliikenneportit, salaamattomat tietoliikenneprotokollat)	ETV_0051 – Keskitetyn palvelinympäristön koventaminen
Vakioidut, keskitetysti hallinnoidut päätelaitteet Sosiaali- ja terveydenhuollon ammattihenkilöiden käyttämät päätelaitteet ovat Apotti-organisaation, käyttäjäorganisaation tai muun luotetun yhteistyökumppanin hallitsemia ja hallinnoimia. Laiteympäristö on vakioitu.	ETV_0058 – Haittaohjelmasuojaus

Vaatimusalue	Viitteet ei-toiminnallisiin vaatimuksiin
Hyväksytyt kovennetut päätelaiteympäristöt Salassa pidettäviä asiakas- ja potilastietoja tulee käsitellä vain erikseen hyväksytyillä päätelaitteilla, joille on toteutettu tietoturvalliset asetukset ja kovennukset. Kovennuksilla pyritään eliminoimaan päätelaitteiden turvattomat palvelut ja haavoittuvuudet, joiden kautta i) päätelaitteella sijaitsevia tietoja voidaan varastaa tai ii) joiden avulla päätelaitetta voidaan käyttää hyökkäyskanavana itse järjestelmään. Päätelaite on kovennettu haavoittuvuuksien ja verkko-hyökkäysten ehkäisemiseksi. Kovennus kattaa vähintään seuraavat toimenpiteet: • Päätelaitekohtainen palomuuri on käytössä ainakin organisaation sisäverkon ulkopuolella toimittaessa, mikäli laiteympäristöön on saatavilla palomuuri-ohjelmisto. • Laitteelle voi asentaa ainoastaan hyväksyttyjä ohjelmia; luvattomien sovellusten asennus on estetty teknisesti. • Päätelaitteiden turvapäivitykset pidetään ajan tasalla. *Kovennusvaatimukset voidaan toteuttaa myös vaihto-ehtoisin keinoin, esim. eriyttämällä etälaitteen käyttöympäristö USB-muistilta ladattavaksi ja suoritettavaksi.*	*Järjestelmähankintaan kohdistuvia eksplisiittiä ei-toiminnallisia vaatimuksia vaatimusalueen osalta ei ole tunnistettu.*
Salassa pidettävän tiedon suojaaminen päätelaitteessa Keskeisiä vaatimuksia: • Tarve asiakas- ja potilastietojen tallennukseen paikallisesti päätelaitteelle on minimoitu. Ratkaisu voi esimerkiksi hyödyntää pääteistuntoja (esimerkiksi Citrix, Microsoft Terminal Server), jolloin päätelaitteeseen ei tallennu mitään sellaisia tietoja, jotka voisivat vaarantaa pääteyhteyden kautta käsiteltyjen tietoaineistojen tietoturvallisuuden. • Kannettavien työasemien kiintolevyt on salattu • Päätelaitteessa on käytössä sovellus- tai muu palvelukohtainen salaus koskien päätelaitteeseen tallentuvia salassa pidettäviä tietoaineistoja • Päätelaitteessa on käytössä apumuistin salaus (esim. ulkoinen Flash-muisti) <u>Järjestelmään ja järjestelmätoimittajaan kohdistuvat vaatimukset</u> • Toimittajan tulee kuvata, miten millä teknisillä ratkaisuilla tietoja suojataan päätelaitteissa	*Järjestelmähankintaan kohdistuvia eksplisiittiä ei-toiminnallisia vaatimuksia vaatimusalueen osalta ei ole tunnistettu.*

Vaatimusalue	Viitteet ei-toiminnallisiin vaatimuksiin
Päätelaitteiden etähallinta Päätelaite on organisaation ohjelmistojakelun ja laitehallinnan piirissä, jolloin: • siihen voidaan asentaa etäältä tarvittavat ohjelmisto-päivitykset • päätelaitteen käyttö voidaan estää etäältä, jos ohjelmistoversio ei ole riittävällä tasolla tai laite on ilmoitettu kadonneeksi/varastetuksi.	*Järjestelmähankintaan kohdistuvia eksplisiittiä ei-toiminnallisia vaatimuksia vaatimusalueen osalta ei ole tunnistettu.*
Järjestelmän etäkäyttö Järjestelmän hyväksytyt etäkäytön menettelyt on sovittu ja dokumentoitu. Mikäli järjestelmässä otetaan käyttöön uusi etäkäyttöratkaisu, se tulee auditoida ennen käyttöönottoa tilaajan ja toimittajan sopimalla menettelyllä	*Järjestelmähankintaan kohdistuvia eksplisiittiä ei-toiminnallisia vaatimuksia vaatimusalueen osalta ei ole tunnistettu.*

6. Ohjelmistoturvallisuus

Tässä kappaleessa esitellyt tietoturvavaatimukset kohdistuvat asiakas- ja potilasjärjestelmän palvelin- ja väli- ja asiakasohjelmistojen sovellusarkkitehtuuriin, teknologioihin, protokolliin ja kehitysmenetelmiin. Vaatimuksilla pyritään mm. minimoimaan sellaiset sovellusten haavoittuvuudet ja tietoturva-aukot, jotka voivat vaarantaa asiakas- ja potilastiedon luottamuksellisuuden, eheyden ja saatavuuden.

Ohjelmistoihin kohdistuvat tietoturvallisuusvaatimukset ovat erityisen keskeisiä 1) tietojärjestelmän teknisissä rajapinnoissa, joiden kautta järjestelmä integroituu muihin tietojärjestelmiin sekä 2) käyttöliittymäkerroksessa. Vaikka järjestelmä voidaan suojata esimerkiksi verkkohyökkäyksiltä palomuurein ja verkkoteknisin suojauksin, ohjelmistokerrokset tietoturvakontrollit tuovat lisäsuojaa, mikäli nämä suojaukset syystä tai toisesta pettävät.

6.1. Tietoturvallinen järjestelmäkehitys

Tietoturvaan liittyvät vaatimukset tulee huomioida jo järjestelmän suunnitteluvaiheessa. Tietoturvan lisääminen järjestelmään jälkikäteen ei ole aina mahdollista tai siitä syntyvät kustannukset ovat korkeat.
Tietoturva on sisäänrakennettu kaikkiin järjestelmäkehityksen vaiheisiin:

- Järjestelmän tietoturvavaatimukset tunnistetaan suunnitteluvaiheessa toteutettavan riskianalyysin yhteydessä.
- Kehitystyö tapahtuu ennalta laaditun kirjallisen kehitysprosessin mukaisesti, jossa jokaisessa vaiheessa on esitetty käytänteet tietoturvan todentamiselle. Kehitystyössä tulee noudattaa turvallisen ohjelmoinnin periaatteita, esimerkiksi OWASP- tai SANS-ohjeistuksia.
- Järjestelmässä käytetään ainoastaan hyväksyttyjä teknisiä tietoturvaratkaisuja esimerkiksi käyttäjä-tunnistuksen ja tiedon salaamisen osalta.
- Järjestelmän tietoturva testataan säännöllisesti kehitysprosessin eri vaiheissa sekä ennen tuotantoon käyttöönottoa yleisimpien tietoturvauhkien osalta.

- Kehitys-, testaus- ja tuotantoympäristöt on eriytetty toisistaan. Ei-tuotannollisissa ympäristöissä ei käsitellä todellista asiakas- tai potilastietoa.

Sovelluskehityksestä vastuussa olevien henkilöiden riittävästä tietoturvaosaamisesta on varmistuttu sovelluskehityksen tietoturvaan liittyvien koulutusten kautta.

6.2. Lokitapahtumien muodostus ja hallinta

Lokitietojen avulla voidaan tunnistaa järjestelmän häiriötilanteet ja tietoturvapoikkeamat. Järjestelmän tulee tuottaa sellaista kiistatonta lokitietoa, jonka kautta saadaan riittävästi tietoa ympäristön ja verkon toiminnasta.

Erityyppisiä lokeja kerätään, säilytetään ja käsitellään etukäteen sovittujen käytänteiden mukaisesti. Erityishuomiota tulee kiinnittää lakien asettamiin vaatimuksiin ja oikeuksiin (kts. VAHTI 3/2009 – Lokiohje). Lokien luvaton käsittely ja muokkaaminen tulee estää.

6.3. Haittaohjelmasuojaus

Haittaohjelmien asianmukaisella torjunnalla varmistetaan, että järjestelmäympäristön laitteet pysyvät turvallisina ja toimintakuntoisina. Järjestelmän osat on suojattu asianmukaisesti haittaohjelmilta:

- Haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat yleisesti alttiita haittaohjelmatartunnoille.
- Haittaohjelmatunnisteet päivittyvät säännöllisesti ja automaattisesti.
- Haittaohjelmien tuottamaa lokia seurataan mahdollisten tartuntojen tunnistamiseksi.

6.4. Järjestelmän ylläpito- ja päivityskäytänteet

Järjestelmän ja tähän liittyvien teknisten alustojen ja komponenttien päivittäminen tulee olla toteutettuna siten, että ympäristö ei altistu tunnistetuille tietoturvahaavoittuvuuksille.

Järjestelmälle sekä tähän liittyville teknisille ratkaisuille on määritetty ja dokumentoitu ylläpito- ja päivityskäytänteet, joiden toteutumista seurataan:

- Järjestelmäympäristö on rakennettu sellaisista komponenteista, jotka tukevat nopeaa päivittämistä.
- Järjestelmän tulee mahdollistaa ohjelmiston elinkaaren huomioiminen ohjelmistoversioissa. (=Järjestelmän käyttämien ohjelmistokomponenttien sekä varusohjelmistojen päivittäminen/vaihtaminen järjestelmän tukemien ohjelmistoversioiden välillä pitää olla mahdollista).
- Kovakoodatut konfiguraatioarvot ovat kiellettyjä.
- Tekniset alustat ja ratkaisut päivitetään säännöllisesti ja ajallaan sovittujen käytänteiden mukaisesti. Päivitystarpeiden seuranta on vastuutettu.
- Päivitysten toimivuus testataan testiympäristössä ennen tuotantoympäristön päivittämistä.

6.5. Viitteet järjestelmähankinnan ei-toiminnallisiin vaatimuksiin

Vaatimus	Viitteet ei-toiminnallisiin vaatimuksiin
Tietoturvallinen järjestelmäkehitys	*Järjestelmähankintaan kohdistuvia eksplisiittiä ei-toiminnallisia vaatimuksia vaatimusalueen osalta ei ole tunnistettu.*
Lokitapahtumien muodostus ja hallinta Järjestelmä tuottaa sellaista kiistatonta lokitietoa, jonka kautta saadaan riittävästi tietoa ympäristön ja verkon toiminnasta, ja jonka avulla voidaan todentaa mahdolliset väärinkäytökset.	• ETV_0035 - Pääsynvalvontaloki
Haittaohjelmasuojaus Haittaohjelmien asianmukaisella torjunnalla varmistetaan, että järjestelmäympäristön laitteet pysyvät turvallisina ja toimintakuntoisina.	• ETV_0058 – Haittaohjelmasuojaus
Järjestelmän ylläpito- ja päivityskäytänteet Järjestelmän ja tähän liittyvien teknisten alustojen ja komponenttien päivittäminen tulee olla toteutettuna siten, että ympäristö ei altistu tunnistetuille tietoturvahaavoittuvuuksille. Järjestelmälle sekä tähän liittyville teknisille ratkaisuille on määritetty ja dokumentoitu ylläpito- ja päivityskäytänteet, joiden toteutumista seurataan.	• ETV_0059 - Järjestelmän ylläpito- ja päivityskäytänteet

7. Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstöstä aiheutuvien riskien salassapito- ja käytettävyysriskien hallintaa tietoja ja tietojärjestelmiä käytettäessä. Järjestelmän osalta henkilöstöriskejä on tarpeen hallita sekä järjestelmää käyttävien että järjestelmäpalveluiden tuottamiseen osallistuvien organisaatioiden henkilöstön osalta.

Tietoturvallisuusliitteen tässä versiossa keskitytään järjestelmäpalveluiden tuottamiseen osallistuvaan henkilöstöön. Järjestelmän loppukäyttäjien osalta järjestelmän käyttäjorganisaatiot ovat pääasiallisessa vastuussa omasta henkilöstöstään; nämä henkilöstöturvallisuuden vaatimukset kuvataan toisaalla.

Henkilöstöturvallisuuden perustan muodostavat henkilöstön toimenkuvien ja niihin liittyvien tietoturvavastuiden selkeä määrittely ja kuvaaminen. Lisäksi tarvitaan riittävällä tasolla määriteltynä olevat henkilöstöhallinnon prosessit ja muut prosessit, joissa kuvataan työtehtävät niin tarkasti, että avainhenkilöriskien syntyminen vältetään. Henkilöstöturvallisuuden kannalta keskeisiä järjestelmän käyttöpalveluissa ja operoinnissa huomioitavia asioita ovat:

- Työhönottoon, toimenkuvien merkittäviin muutoksiin ja palvelussuhteen päättymiseen liittyvät prosessit
- Tehtävien vaativuudesta ja luottamuksellisuudesta riippuen rekrytoitavan henkilön taustan, sopivuuden ja osaamisen selvittäminen ennen työhönottoa
- Salassapito- ja käytettävyysriskien kannalta keskeisten avainhenkilöiden tunnistaminen ja varmistuminen heidän käytettävyydestään eri tilanteissa (mm. varautuminen lomiin ja poissaoloihin)

- Kiellettyjen (vaarallisten) työyhdistelmien tunnistaminen ja poistaminen työtehtävien eriyttämisellä, jolla ehkäistää sekä tahattomia virheitä että tahallisia väärinkäytöksiä.

7.1. Henkilöstön nimeäminen, hyväksyminen ja vaihtaminen

Järjestelmätoimittajan tulee nimetä sopimuksen kohteen toteuttamiseen riittävä määrä henkilöitä, joilla on heidän tehtäviensä edellyttämä kokemus ja pätevyys. Asiakkaalla on perustellusta syystä oikeus olla hyväksymättä Järjestelmätoimittajan sopimuksen kohteen toteuttamiseen ehdottamaa henkilöä.

Järjestelmätoimittaja sitoutuu käyttämään projektisuunnitelmissa mainittuja avainhenkilöitä niissä tehtävissä, joihin heidät on nimetty. Avainhenkilöiden vaihtaminen on sallittua vain Toimitus- ja Palvelusopimuksissa eritellyissä tapauksissa ja ainoastaan sopimuksissa määriteltyjen ehtojen täyttyessä. Projektin avainhenkilön vaihtuessa Järjestelmätoimittaja on kaikissa tapauksissa velvollinen Toimitus- ja Palvelusopimuksissa määritellyllä tavalla osoittamaan vaihtuvan Projektin avainhenkilön tilalle toisen vähintään yhtä kokeneen ja pätevän henkilön.

7.2. Salassapito

Järjestelmätoimittaja pitää salassa haltuunsa saamansa luottamuksellisiksi merkityt tiedot sekä liikesalaisuudeksi tai muuten luottamuksellisiksi katsottavat tiedot Toimitus- ja Palvelusopimuksissa määritellyllä tavalla eikä käytä käytä tietoja muihin kuin sopimuksen mukaisiin tarkoituksiin. Järjestelmätoimittaja vastaa siitä, että kaikki sen palveluksessa olevat henkilöt samoin kuin alihankkijat ja niiden palveluksessa olevat henkilöt noudattavat salassapitovelvoitteita.

7.3. Turvallisuusselvitykset

Tilaajalla on perustellusta syystä oikeus edellyttää turvallisuusselvityslain (726/2014) mukaisen turvallisuus-selvityksen teettämistä yksittäisistä sopimuksen kohteen toteuttamiseen osallistuvista Järjestelmätoimittajan tai sen alihankkijan palveluksessa olevista henkilöistä Toimitus- ja Palvelusopimuksissa määritellyllä tavalla.

7.4. Tiedon saannin rajaaminen

Pääsääntöisesti järjestelmän ylläpitäjillä ei saa olla pääsyä järjestelmässä käsiteltäviin tietoaineistoihin. Järjes-telmän normaalit, päivittäiset valvonta- ja ylläpitotoimet tulee voida suorittaa rajatuin käyttövaltuuksin, jotka eivät salli tietosisällön katselua.

Käyttövaltuuksista ja niihin tehdyistä muutoksista on pidettävä kirjaa/lokia. Lokiin on tallennettava anotut, hyväksytyt, toteutetut, muutetut ja poistetut käyttövaltuudet.

Kielletyt ylläpidon työ- ja rooliyhdistelmät on dokumentoitu ja valtuuksia myönnettäessä tai muutettaessa kiellettyjen yhdistelmien syntymistä seurataan ja estetään. Kriittisten toiminnallisuuksien tunnistaminen ja harkinnan mukaan kovennettu valvonta. Kriittisissä hallintatehtävissä toimivien henkilöiden taustatarkistukset.

7.5. Viitteet järjestelmähankinnan muihin hankinta-asiakirjoihin

Vaatimusalue	Viitteet muihin hankinta-asiakirjoihin
Henkilöstön nimeäminen, hyväksyminen ja vaihtaminen Järjestelmätoimittajan velvollisuudet ja Tilaajan oikeudet henkilöstön nimeämisen, hyväksymisen ja vaihtamisen osalta on määritelty Toimitus- ja Palvelusopimuksissa.	• Liite 3 Toimitussopimus • Liite 4 Palvelusopimus
Turvallisuusselvitykset Tilaajalla on perustellusta syystä oikeus edellyttää turvallisuus-selvityslain mukaisen turvallisuusselvityksen teettämistä yksittäisistä henkilöistä Toimitus- ja Palvelusopimuksissa kuvatulla tavalla.	• Liite 3 Toimitussopimus • Liite 4 Palvelusopimus
Salassapito Järjestelmätoimittaja sitoutuu pitämään salassa sille luovutetut, salassa pidettäväksi säädetyt tiedot eikä käytä tietoja muihin kuin sopimuksen mukaisiin tarkoituksiin. Järjestelmätoimittajan tulee viestiä henkilöstölleen salassapitovelvoitteet ja tietojen huolellisen käsittelyn merkitys.	• Liite 3 Toimitussopimus • Liite 4 Palvelusopimus
Tiedon saannin rajaaminen Järjestelmän normaalit, päivittäiset valvonta- ja ylläpitotoimet tulee voida suorittaa rajatuin käyttövaltuuksin, jotka eivät salli tietosisällön katselua. Järjestelmän valvonnan ja ylläpidon kiellettyt työ- ja rooliyhdistelmät tulee dokumentoida ja valtuuksia myönnettäessä tai muutettaessa vaarallisten/kiellettyjen yhdistelmien syntymistä seurataan ja estetään. Valtonta- ja ylläpitohenkilöstln käyttövaltuuksista ja niihin tehdyistä muutoksista on pidettävä kirjaa.	*Valvonta- ja ylläpitotoimien vastuiden eriyttämistä, henkilöstön käyttövaltuuksien seurantaa sekä kiellettyjen työyhdistelmien seurantaa ja estämistä koskevia vaatimuksia tarkennetaan käyttöpalveluiden hankinnan yhteydessä.*

8. Tietoaineistoturvallisuus

Tietoaineistoturvallisuuden osalta järjestelmän seikkaperäiset vaatimukset (mm. tietoaineiston luovutuksiin, arkistointiin ja tuhoamiseen) on kuvattu järjestelmän toiminnallisissa vaatimuksissa.

8.1. Tietoaineistojen eheyden ja alkuperän varmistaminen

Tietojen eheyden ja aluperän varmistaminen ja näyttäminen käyttäjille esim. metatietoina kullakin sivulla (kuka on luonut, milloin, kuka on viimeksi muokannut ja milloin, tarvittaessa koko muutoshistoria oltava katsottavissa).

8.2. Tietoaineistojen elinkaaren hallinta

Tietoaineistojen käsittelyn elinkaari tulee olla määritelty ja tietojen poistaminen tulee toteuttaa luotettavalla menetelmällä. Krittiset tiedot tulee tunnistaa ja niiden ajantasaisuuden varmistaminen tulee ottaa huomioon suunnittelussa ja toteutuksessa. Esimerkiksi kriittisten tietojen tarkistaminen rekisteristä aina ennen käyttöä, tai

jos se ei ole mahdollista, käyttöliittymässä tulisi olla huomautus käyttäjälle että tietojen ajantasaisuus pitää tarkistaa manuaalisesti esim. puhelimitse toiselta viranomaiselta.

9. Hallinnollinen turvallisuus

Järjestelmän hallinnollista turvallisuutta koskevat vaatimukset kohdentuvat pääosin tilaajaorganisaatioon sekä järjestelmän palvelutuotannosta vastaavaan tahoon – eivät ensisijaisesti valmisohjelmistoihin tai järjestelmätoimittajaan. Fyysisen turvallisuden vaatimuksia tullaan tarkentamaan tämän dokumentin myöhemmissä versioissa mm. käyttöpalveluiden hankinnan yhteydessä.

Palveluun kohdistuvat lakisääteiset ja muut viranomaisvaatimukset sekä sopimusvaatimukset on tunnistettava ja dokumentoitava. Vaatimusten muutoksia on seurattava säännöllisesti esim. lain tai asetuksen muuttuessa, jolloin on arvioitava vaikutus järjestelmän toiminnan kannalta.

Järjestelmäalustan käyttö- ja kapasiteettipalvelujen tuottamisesta laaditaan palvelukuvaus, joka määrittelee palvelutason sekä teknisen tietoturvallisuuden ja toimintaprosessien turvatason. Palvelutasoa ja tietoturvapoikkeamia seurataan ja niistä raportoidaan säännöllisesti.

Järjestelmäkokonaisuuden hallinnassa tulee hyödyntää kauttaaltaan roolipohjaista käyttövaltuuksien hallintaa. Eri rooleilla on erilaiset, mahdollisimman rajatut oikeudet tietoon että toimintoihin, mikä edesauttaa ylläpitotehtävien eriyttämistä. Järjestelmäkokonaisuuden ylläpito- ja hallintatunnuksista ja -valtuuksista pidetään kirjaa ja niistä raportoidaan tilaavalle organisaatiolle säännöllisesti.

10. Fyysinen turvallisuus

Järjestelmäpalvelun tuotantotilojen on täytettävä palvelun jatkuvuuden ja poikkeustilanteista toipumisen osalta lähtökohtaisesti VAHTI-ohjeen 2/2013 liitteen 4 korotetun tason tietoturvavaatimukset. Laitteiden ja ohjelmistojen valtonta- ja hallintayhteydet tulee eristää muusta tietoliikenteestä.

Fyysistä turvallisuutta koskevat vaatimukset kohdentuvat pääosin järjestelmän palvelutuotannosta vastaavaan toimittajaan – eivät niinkään valmisohjelmistoihin tai järjestelmätoimittajaan. Fyysisen turvallisuden vaatimuksia tullaan tarkentamaan tämän dokumentin myöhemmissä versioissa.

11. Viitteet

[1] Henkilötietolaki (523/1999), http://www.finlex.fi/fi/laki/ajantasa/1999/19990523
[2] Laki asiakastietojen sähköisestä käsittelystä sosiaali- ja terveydenhuollossa (159/2007), http://www.finlex.fi/fi/laki/ajantasa/2007/20070159

[3] Laki sähköisestä lääkemääräyksestä (61/2007), http://www.finlex.fi/fi/laki/ajantasa/2007/20070061
[4] Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, http://www.finlex.fi/fi/laki/ajantasa/2010/20100681
[5] Kansallinen turvallisuusauditointikriteeristö (Katakri II), http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf
[6] Sovelluskehityksen tietoturvaohje (VAHTI 1/2013), https://www.vahtiohje.fi/c/document_library/get_file?uuid=03c32520-f3f8-4621-b0d4-ec4ca8edafb3&groupId=10128&groupId=10229
[7] Teknisen ICT-ympäristön tietoturvataso-ohje (VAHTI 3/2012), https://www.vahtiohje.fi/c/document_library/get_file?uuid=5a273c6e-2935-4bbf-a4c6-f00e0f878db5&groupId=10128&groupId=10229
[8] ICT-varautumisen vaatimukset (VAHTI 2/2012), https://www.vahtiohje.fi/c/document_library/get_file?uuid=c99a95f5-c150-49b6-aa5c-a90a821da13e&groupId=10128&groupId=10229
[9] Määräys A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista tietoturvavaatimuksista (THL/1305/4.09.00/2014) 30.1.2015
[10] Kansalliset auditointivaatimukset potilastietojärjestelmille (STM), http://www.kanta.fi/documents/12105/3983179/Kansalliset+auditointivaatimukset+potilastietoj%C3%A4rjestelmille+v1.0.pdf/eb5d069c-60c9-40b6-969e-1acdb7e2af30
[11] Kansalliset auditointivaatimukset välittäjille (STM), http://www.kanta.fi/documents/12105/3983179/Kansalliset+auditointivaatimukset+v%C3%A4litt%C3%A4j%C3%A4lle+v1.0.pdf/f29678fe-bb81-44a4-8abb-61d12213e832
[12] Uudistettu potilas- ja lääkehoidon turvallisuussanasto, THL https://www.thl.fi/documents/10531/102913/potilasturvallisuuden_sanasto_071209.pdf
[13] Toimitilojen tietoturvaohje (VAHTI 2/2013), http://www.finlex.fi/data/normit/41654-Toimitilojen_tietoturvaohje_VAHTI_2_2013_netti.pdf
[14] Valtionhallinnon tietoturvasanasto (VAHTI 8/2008), https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto
[15] Toimikortit terveydenhuollolle ja julkishallinnolle, http://www.fineid.fi/julkaisut/VRK_toimikortit2013/index.html