Teppo Salminen

IDENTITEETIN- JA KÄYTTÖVALTUUS-HALLINNAN KEHITTÄMINEN SIPOON KUNNASSA

Opinnäytetyö

Tekniikan ylempi ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus (ylempi amk)

2022

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (ylempi AMK)
Tekijä	Teppo Salminen
Työn nimi	Identiteetin- ja käyttövaltuushallinnan kehittäminen Sipoon kunnassa
Toimeksiantaja	Sipoon kunta
Vuosi	2022
Sivut	80 sivua, liitteitä 5 sivua
Työn ohjaaja	Vesa Kankare

TIIVISTELMÄ

Tässä opinnäytetyössä tutkittiin, mitä viranomaisvaatimuksia kohdistuu kunnan identiteetin- ja käyttövaltuushallinnan toteuttamiseen. Sipoon kunnalle on otettu käyttöön järjestelmä, jonka avulla on voitu automatisoida käyttäjätunnusten hallintaan liittyviä tehtäviä. Verrattain lyhyessä ajassa viranomaisvaatimukset ovat lisääntyneet EU:n yleisen tietosuoja-asetuksen ja tiedonhallintalain voimaantulon myötä. Tiedonhallintalain siirtymäaika tulee päättymään vuoden 2022 lopussa ja samanaikaisesti myös uutta kansallista ohjeistusta on laadittu käyttövaltuushallinnan vaatimusten mukaiseen toteuttamiseen.

Opinnäytetyön tavoitteena oli selvittää vaatimukset ja suositukset, vaikutukset tietoturvaan sekä tunnistaa kehityskohteet identiteettien hallinnoinnin vaatimusten mukaiseen tavoitetilaan pääsemiseksi.

Tutkimusmenetelmäksi valittiin tutkimuksellinen kehittämisprojekti ja tutkimuskysymysten kautta aluksi keskityttiin tutkimaan lainsäädännön, ohjeiden, suositusten ja standardien sekä parhaiden käytäntöjen vaatimuksia tai tehtäviä identiteettien hallinnoinnin toteuttamiseen. Vaatimuskehysten kautta luotiin vaatimuslista, jota vasten tutkittiin organisaation nykytilaa ja sen vaatimustenmukaisuutta. Havaintojen jälkeen luotiin kehityskohteet, joihin tulisi keskittyä.

Identiteettien hallinnoinnin toteuttamiseen löydettiin yhteensä 18 eri vaatimusta. Tärkeimpänä vaatimuskehyksenä kuntaorganisaatiolle toimii tiedonhallintalaki ja sitä tukemaan luotu tiedonhallintalautakunnan suosituskokoelma. Käyttäjätunnusten ja käyttöoikeuksien hallinta liittyy myös useisiin kyberuhkiin, joista erityisesti vähimpien oikeuksien periaatteen käyttöönottaminen on keskeinen yhdessä säännöllisen katselmoinnin kanssa. Kehityskohteina löytyi useita toimintaprosesseihin liittyviä tehtäviä ja identiteettien hallinnoinnin järjestelmän käyttöönoton jälkeen vain teknisimmät vaatimukset olivat toteutettu asianmukaisesti. Identiteettien hallinnoinnin järjestelmän käyttöönotto tulisi aloittaa toimintaprosessien ja pääsynhallintapolitiikan luomisella.

Asiasanat: käyttöoikeus, käyttäjätunnus, lait, asetukset (säädökset)

South-Eastern Finland University of Applied Sciences

Degree	Master of Engineering
Author	Teppo Salminen
Thesis title	Development of identity and access management in the municipality of Sipoo
Commissioned by	Municipality of Sipoo
Time	2022
Pages	80 pages, 5 pages of appendices
Supervisor	Vesa Kankare

ABSTRACT

This thesis examined what regulatory requirements are subject to the implementation of municipal Identity and Access Management. A system has been introduced to the municipality of Sipoo to automate tasks related to Identity Management. In a comparatively short period, regulatory requirements have increased with the entry into force of the EU General Data Protection Regulation and the Data Management Act. The transition period of the Data Management Act will expire at the end of 2022 and at the same time new national guidance has also been drawn up for Access Management compliant implementation.

The objective of the thesis was to find out requirements and recommendations, impact to information security, and identify development targets for Identity and Governance Administration (IGA) while ensuring compliance.

A research development project was selected as the research method and, through research issues, initially focused on exploring the requirements or tasks of legislation, guidelines, recommendations, standards, and best practices for implementing IGA. Through the requirement frameworks, a list of requirements was created against the current state of the organizations IGA and its compliance was examined. Following the observations, list of development tasks was created that should be focused on.

A total of 18 different requirements were found to implement IGA system. The main requirement framework for a municipal organization is the Information Management Act and the Information Management Board Recommendation Collection created to support it. Identity and Access Management is also associated with several cyber threats, notably the introduction of the Principle of Least Privilege in conjunction with regular assessment. Several tasks related to operational processes were found as development sites and, after the introduction of the IGA system, only the most technical requirements had been properly implemented. The implementation of the IGA system should begin with the creation of operational processes and access management policies.

Keywords: access right, username, laws, decrees

SISÄLLYS

1 JOHDANTO

Viranomaisen toimintaa tiedonhallinnassa säädetään useassa eri laissa tai asetuksessa ja sitä ohjataan ohjeilla ja suosituksilla. Viranomaisen tulee huolehtia, että se omassa toiminnassaan huomioi lain vaatimukset ja noudattaa niitä. Opinnäytetyön tarkoitus on selvittää vaatimukset identiteetin- ja käyttövaltuushallinnan toteuttamisille tutkimalla, mitä kansallisia lakeja, asetuksia, suosituksia ja standardeja kohdistuu identiteetin- ja käyttövaltuushallintaan ja miten niitä sovelletaan identiteettien hallinnoinnin järjestelmään, prosesseihin ja dokumentaatioon. Tutkimuksen kautta on tarkoitus myös selvittää, mitä vaikutuksia identiteettien ja käyttövaltuuksien hallinnoinnilla on organisaation tietoturvaan.

Tämän opinnäytetyön toimeksiantaja on Sipoon kunta, joka on 21 678 asukkaan kaksikielinen kunta, jossa on 1303 työntekijää (Sipoon kunta 2021). Opinnäyteyön aihe syntyi työssäni havaitusta identiteetin- ja käyttövaltuushallinnan ongelmallisesta ja riskialttiista tilasta, jossa hajautetun käyttöoikeushallinnan toteuttaminen edellytti erittäin paljon manuaalista tekemistä ja muistinvaraisuutta. Sivistyksen sekä sosiaali- ja terveysosastojen toimialalla tapahtuu vuosittain paljon henkilövaihdoksia ja lyhyitä sijaisuuksia, jotka ovat työllistäneet runsaasti IT-henkilöstöä. Sähköisten identiteettien perustamisen automatisoiminen ja käyttöoikeuksien roolittaminen on ollut myös oma kiinnostuksen kohteeni.

Sipoon kunnan identiteetin- ja käyttövaltuushallinta on kehittämisprojektissa automatisoitu työni kautta ja nyt halutaan varmistaa, että prosesseissa noudatetaan viranomaisen toimintaan kohdistuvia lakeja ja suosituksia. Useassa järjestelmässä olen havainnut edelleen olevan täysin itsenäisen käyttöoikeuksien hallinnan ja käyttöoikeuksien oikea-aikaisen ylläpitämisen ongelmaan haetaan myös suurta parannusta. Kunnan käytössä on runsas kirjo erilaisia järjestelmiä, ja kaikki eivät välttämättä ole kansallisten lakien vaikutuspiirissä. Tästä huolimatta kunnalla on kuitenkin intressi huolehtia näiden järjestelmien käyttöoikeuksista suositelluilla käyttövaltuushallinnan käytännöillä.

Käyttövaltuushallinnasta on olemassa ohjeistus käyttövaltuushallinnon periaatteet ja hyvät käytännöt (Valtiovarainministeriö 2006). Ohjeistus on monilta osin edelleen ajankohtainen, mutta vanhaan ohjeeseen perustuva toteutus identiteetin- ja käyttövaltuushallinnan prosesseissa ei välttämättä huomioi uusimpia viranomaisvaatimuksia. Tutkimuksessa selvitetään mitä reunaehtoja lait määrittelevät. Lisäksi tutkitaan lakeja, suosituksia ja ohjeita sekä muuta asiaan liittyvää viitekehystä ja selvitetään, miten viranomaisen tulee tehdä identiteetin- ja käyttövaltuushallinnan toteutusta.

2 TUTKIMUSONGELMA JA MENETELMÄT

Valtiovarainministeriö (2006) viittaa hyvän tiedonhallinnan vaatimuksen yhteydessä julkisuuslain eli laki viranomaisten toiminnan julkisuudesta 21.5.1999/621. Tietosuojalaki (Tietosuojalaki 5.12.2018/1050) edellyttää henkilötietojen suojaamista, tietojen tarpeellisuus- ja virheettömyysvaatimuksen, sekä käyttötarkoitussidonnaisuuden vaatimuksen huomioon ottamista.

Järjestelmien käyttöoikeuksien määrittäminen asianmukaisesti on edellytyksenä sille, että edellä mainitut vaatimukset sekä niiden valvonta voidaan suorittaa lain edellyttämällä tavalla. Käyttöoikeuksien ja niiden sisällön määrittäminen tulee käytännössä tehdä henkilötasolla. (Valtiovarainministeriö 2006.)

2.1 Tutkimusongelma

Työtehtävieni kautta on käynyt ilmi, että Sipoon kunnassa työntekijöiden käyttäjätunnukset ja niihin liitetyt käyttöoikeudet on hallittu lähes täysin manuaalisesti. Joissakin järjestelmissä on rakennettu komentoriviohjelmia, eli skriptejä, joilla on voitu automatisoida osa käyttöoikeushallinnasta. Ulkoistettu palkkahallinto tai sisäinen HR-yksikkö ovat tilanneet Active Directory (AD) -käyttäjätunnukset käsin erillisellä tilauslomakkeella itsepalveluportaalin kautta. Pääperiaate on ollut, että tunnuksen olemassaolo ja voimassaolo perustuvat työsuhteen mukaiseen aikaan, mutta käytännön toteutuksessa on ollut runsaasti virheitä.

Tunnusten tekemiseen liittyvät toimenpiteet ovat osin ohjeistettu, mutta ne ovat osoittautuneet käytännössä muistinvaraisiksi ja inhimillisten virheiden te-

keminen on ollut yleistä. Käyttäjätunnusten tekeminen on keskitetty käytännössä muutamalle tukihenkilölle, mutta poissaolo- ja ruuhkatilanteissa myös muu IT-henkilöstö, joiden päätyö ei ole tukitehtävissä ja tunnushallinnassa, ovat voineet auttaa tunnusten tekemisessä. Näissä akuuteissa tilanteissa viimeisintä voimassa olevaa ohjeistusta ei ole tarkistettu ja käyttäjätunnuksia ja varsinkin käyttöoikeuksia on saatettu antaa ohjeistuksen vastaisesti ja vanhentuneen käytännön mukaisesti. Käyttöoikeuksien määrittämiseen ei ole ollut todellisia perusteita eikä yhtenäistä prosessia. Ylläpitoa on tehty parhaan kyvyn mukaan.

Työntekijän käyttöoikeudet ovat perustuneet hyvin karkeaan roolimääritykseen ja käytännössä ne on kopioitu AD:ssa vastaavaa tehtävää tekevältä käyttäjältä. Tämänkaltainen toiminta sisälsi itsessään jo sisäänrakennetun virheen, koska työntekijän käyttöoikeudet eivät vastanneet todellista tarvetta. Lisäksi kopioinnissa käytetty toimintatapa sisälsi paljon virheen mahdollisuuksia. Käsin suoritettava tilausprosessi on koettu myös erittäin haavoittuvaksi ja inhimillisten virheiden takia käyttäjätunnuksia on jäänyt kokonaan tilaamatta sekä poistamatta työntekijän työsuhteen alkaessa tai päättyessä. AD:ssa valtaosa käyttäjäryhmistä olivat itsessään rooleja, mutta niitä ei ollut toteutettu sisäkkäisinä ryhminä (*Nested Group*). Esimerkiksi kaikki työntekijät -käyttäjäryhmä antoi useita eri oikeuksia eri järjestelmiin, eikä tästä ollut mitään dokumenttia mihin käyttöoikeuksia on määritelty. Poikkeustapauksissa kunnan ulkopuoliselle henkilölle, kuten järjestelmätoimittajan konsultille, piti antaa oikeuksia rajatusti vain yhteen paikkaan ja ainoa vaihtoehto oli lisätä käyttäjätunnus ryhmään kaikki työntekijät, jonka kautta sai huomattavasti suuremmat käyttöoikeudet, kun todellisuudessa oli tarpeen.

Kunnalla on ollut käytössä runsaasti perinteisiä järjestelmiä, niin sanottuja legacy-järjestelmiä, jotka hyödyntävät vanhempaa teknologiaa ja joihin ei ole ollut mahdollista rakentaa AD-integraatiota tai kertakirjautumista. Tällaisten järjestelmien käyttäjätunnukset ja käyttöoikeudet tai roolit on tilattu suoraan järjestelmien pääkäyttäjiltä, eikä niistä ole kerätty mitään keskitettyä rekisteriä. Järjestelmäkohtaiset käyttäjätunnukset on tilattu pääsääntöisesti esimiehen toimesta, mutta myös työntekijä on voinut itse tilata käyttäjätunnuksen itselleen. Prosessin kannalta kriittiset hyväksyntäpisteet tilauksista perusteluineen

ovat kuitenkin puuttuneet, eikä IT-yksikölle tulleita tilauksia ole kirjattu rakenteellisessa muodossa. Jälkikäteen tehtävän lokitarkastelun näkökulmasta tiedon etsiminen on ollut erittäin työlästä tai suorastaan mahdotonta. Osa järjestelmäkohtaisista käyttöoikeuksista on tilattu IT-yksikön ohi suoraan järjestelmän pääkäyttäjältä, omistajalta tai jopa järjestelmän toimittajalta, jolloin niistä ei ole kertynyt lainkaan lokitietoja. Automatisoidut skriptit eivät myöskään ole tuottaneet laadukasta lokia, jolla voitaisiin näyttää toteen, milloin työntekijällä on ollut käyttöoikeus järjestelmään.

Tietojärjestelmien omistajuus on Sipoon kunnassa rekisterinpitäjän mukaisesti hajautettu toimialoille (Tietosuojaselosteet ja henkilötietojen käsittelyn asiakirjat s.a.). Työssäni olen havainnut, että säännöllistä katselmointityötä ei ole aina toteutettu eikä katselmointityö ole keskitetysti koordinoitua ja dokumentoitua. Käyttövaltuuksien katselmointityö olisi myös vaikea toteuttaa ilman kattavaa rekisteriä kenellä käyttöoikeus tulisi olla. Vahti-ohjeen mukainen organisaation palveluksesta poistuneiden työntekijöiden käyttövaltuuksien poistaminen ei olisi riittävää, koska työntekijä voi olla edelleen kunnalla töissä toisessa työtehtävässä, eikä hänellä tulisi enää olla aktiivista käyttöoikeutta tietojärjestelmään (Valtiovarainministeriö 2006).

Käyttövaltuushallinnan automatisointiin on perustettu toteutusprojekti, jolla tähdätään automatisointiin ja virheettömään tunnushallintaan, jossa tunnuksien voimassaolo ja roolitus perustuu työsuhteen tietoihin. Toteutusprojektin ensimmäinen vaihe on saatu päätökseen ja käytössä on työsuhteen tietoihin pohjautuva automaattinen tunnustenhallintajärjestelmä, jossa käyttöoikeudet provisioidaan, eli määritellään käyttäjäobjektit automaattisesti kohdejärjestelmään, pääosin automaattisesti. Erillisille käyttöoikeustilauksille on rakennettu vakiomuotoinen hyväksyntäprosessi, josta pidetään kirjaa. Toteutusprojektin ensimmäisen vaiheen jälkeen on käynyt ilmi, että kunta ei ole tarkalleen selvittänyt, mitä vaatimuksia, suosituksia ja parhaita käytäntöjä käyttövaltuushallinnan toteuttamiseen liittyy. Lisäksi automatisoinnin ratkaisut eivät ole kaikilta osiltaan täydellisiä ja vaativat edelleen kehittämistä. Käyttövaltuushallinnan periaatteet ja toteutustapa, kuten koko toteutusprojekti on ollut IT-lähtöistä eikä toimialojen henkilöitä ollut otettu mukaan toteutusprojektiin.

Tämä opinnäytetyö pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

1. Mitkä viranomaisvaatimukset, lait tai asetukset asettavat reunaehtoja kunnan käyttövaltuushallinnalle?
2. Mitkä ovat suositukset ja parhaat käytännöt käyttövaltuushallinnan toteuttamiseen?
3. Mitä kehitystoimia Sipoon kunnan tulee tehdä täyttääkseen lakien ja asetuksien vaatimukset?
4. Mikä merkitys asianmukaisesti hoidetulla identiteetin- ja käyttövaltuushallinnan työllä on organisaation tietoturvallisuuteen?

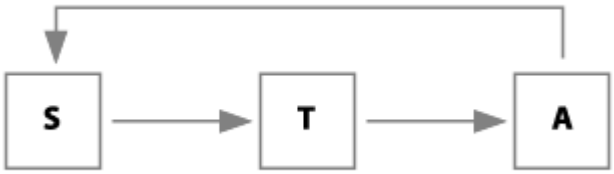
Tutkimuskysymykset on valittu siten, että niiden tuloksista voisi hyötyä myös muut kuntaorganisaatiot omassa toiminnassaan identiteetin- ja käyttövaltuushallinnon kehittämistyössä.

2.2 Tutkimusmenetelmät

Tutkimusmenetelmäksi valikoitui tutkimuksellinen kehittämisprojekti, koska kyseessä oli kehittämisprojekti, jonka tavoitteena oli kehittää Sipoon kunnan identiteetin- ja käyttövaltuushallinnan menetelmiä ja prosesseja. Kehittämisprojekti oli pääpiirteiltään ohjelmistotoimittajan vakiomuotoinen toteutusprojekti, mutta projektin keskeiset osat ja vaatimukset tuli luonnollisesti sovittaa Sipoon kunnan ympäristöön ja henkilöstötiedon lähdejärjestelmän asettamiin rajoituksiin. Kuten Ojasalo ym. (2015, 19) ovat todenneet, kehittämistyö eroaa tieteellisestä tutkimuksesta juuri kehitysprojektin tavoitteissa: tutkimuksellisessa kehittämistyössä halutaan saada tuloksena myös käytännön parannuksia tai kokonaan uusia ratkaisuja, siinä missä tieteellisessä tutkimuksessa päätuotos on uusi teoria. Tässä opinnäytetyössä päätavoite oli saada käytännön parannuksia identiteetin- ja käyttövaltuushallinnan hallinnollisen työn toteuttamiseen.

Interventiotutkimus nähdään yläkäsitteenä kaikille tutkimusmuodoille, joissa pyritään saavuttamaan muutosta. Kehittämistutkimus on yksi muutokseen pyrkivästä kolmesta tutkimusmuodosta toimintatutkimuksen ja konstruktiivisen tutkimuksen lisäksi. (Jönssön & Lukka 2005, Kanasen 2017, 10 mukaan.) Ilman tätä opinnäytetyötä ja sen tutkivaa otetta Sipoon kunnan identiteetin- ja käyttövaltuushallinnan projekti olisi ollut vain tavallista organisaation kehittämistyötä. Juuri tutkimuksellinen ote muuttaa tavallisen kehittämistyön kehittämistutkimukseksi (Kananen 2017, 18).

Sipoon kunnalle on otettu käyttöön kokonaan uutta teknologiaa ja työtä on tehty muutostyön prosessin mukaisesti (Ojasalo ym. 2015, 22). Muutostyön prosessi jakaantuu kolmeen vaiheeseen: suunnittelu-, toteutus- ja arviointivaihe (kuva 1). Vaikka varsinainen identiteetin- ja käyttövaltuushallintajärjestelmän käyttöönotto oli osin vesiputousmallin mukainen toteutus, jossa valmis tuote käyttöönotettiin kerralla, edistin toteutusprojektia järjestelmätoimittajan konsultin kanssa aktiivisesti ja seurantaa tehtiin viikoittaisilla palavereilla muutostyön prosessin mukaisesti.



Kuva 1. Muutostyön prosessi (Ojasalo ym. 2015, 23)

Kokonaisratkaisun eri osia rakennettiin pala kerrallaan testiympäristössä ja ne validoitiin säännöllisesti kattavilla testeillä, jonka jälkeen siirryttiin seuraavaan toteutusvaiheeseen. Virheitä kohdatessa tehtiin uudelleen arviointi ja uutta suunnitelmaa toteutusta varten. Ojasalon ym. (2015, 22) mukaan muutostyön prosessi auttaa suunnittelemaan jokaisessa vaiheessa valmiiksi saatavat tehtävät, toteuttamaan ne ja lopuksi arvioida niiden onnistuminen ennen seuraavaan vaiheeseen siirtymistä. Toteutusprojektin etenemistä seurattiin järjestelmätoimittajan kanssa jaetussa kanban-taulussa. Kanban on suosittu toiminnanohjauksen työkalu, jolla voidaan visualisoida työtehtävät ja rajoittaa yhtäaikaisen työn määrää (Contribyte 2016). Varsinkin toteutusprojektin loppuvaiheessa, jossa toimivaa tuotosta siirrettiin tuotantojärjestelmään, ja tehtiin tuotantotestauksia, kanbanin vahvuus oli huomattava. Kokonaisprojektin osalta ollaan nyt toteutuksen jälkeisessä arviointivaiheessa ja tavoitteena on saada havaintoja, joiden pohjalta voidaan taas aloittaa muutostyönprosessi uudelleen.

2.3 Tutkimuksen rajaukset ja terminologia

Opinnäytetyön tuloksena Sipoon kunnalle käyttöönotettiin identiteettien hallinnoinnin ratkaisu (Identity Governance and Administration, IGA), Efecte IGA.

Pääsynhallinta on olennainen osa identiteetin- ja käyttövaltuushallinnan kokonaisuutta ja asiaa käsitellään myös tutkimuksen kautta tässä opinnäytetyössä. Pääsynhallinnan toteuttamiseen liittyvät vaatimukset ja toimenpiteet rajattiin kuitenkin tästä tutkimuksesta pois, jotta käsiteltävästä aiheesta ei tulisi liian laaja. Tietosuoja ja tietoturva pidettiin koko aika tekemisen keskiössä, tietynlaisena tekemisen ajurina, mutta varsinaisesti tietosuojaan tai tietoturvaan liittyvää ohjeistusta ei tutkimuksella ollut tarkoitus saavuttaa. Opinnäytetyöstä rajattiin pois myös kyberuhkiin, kuten kalasteluun tai haittaohjelmiin liittyvien asioiden tarkempi käsittely. Edellä lueteltuja käsitellään suppeasti tietoturvallisuuteen liittyvässä luvussa. Lisäksi riskienhallintaan liittyviä asioita käsitellään hyvin pintapuolisesti, eikä erityistä riskilistaa ole tarkoitus tuottaa.

Huolimatta siitä, että IGA sekä identiteetin ja pääsynhallinta (Identity and Access Management, IAM) ovat hyvin samanlaisia, niiden toiminta kuitenkin eroaa toisistaan. Kummallakin ratkaisulla pyritään hallitsemaan identiteettejä ja pääsyoikeuksia, IAM-järjestelmällä on tarkoituksena hallita pääsyä toisiin järjestelmiin, kun taas IGA-järjestelmä mahdollistaa IAM-toiminnallisuudet, mutta tuo organisaatiolle lisäksi tarkastamiseen ja vaatimustenmukaisuuden osoittamiseen tarvittavat toiminnallisuudet. IGA-järjestelmällä voidaan siis kontrolloida, mihin järjestelmään käyttäjälle annetaan pääsy ja mitä hän voi tehdä järjestelmässä. IGA-järjestelmän tavoite on varmistaa IAM-järjestelmän määritysten pakottaminen käyttäjälle ja seurata vaatimusten täyttymistä. (Fryzel 2021.) Tässä opinnäytetyössä käytetään kumpaakin termiä ja niillä tarkoitetaan edellä kuvattuja järjestelmiä.

Tässä opinnäytetyössä identiteetillä viitataan henkilön sähköiseen identiteettiin. Identiteetti on tietojoukko erilaisista attribuuteista, kuten käyttäjätunnus, etunimi, sukunimi tai henkilönumero. Kaikki attribuutit yhdessä muodostavat sähköisen identiteetin. Yhdellä henkilöllä voi olla useita eri sähköisiä identiteettejä eri järjestelmissä (digital identity), mutta vain yksi henkilöllisyys (identity). Psykologian käsitteellä identiteetistä viitataan ihmisen yksilölliseen käsitykseen itsestään. Sähköisellä identiteetillä ei viitata psykologian käsitteeseen identiteetistä, vaan pelkästään digitaaliseen identiteettiin, joka on joukko attribuutteja. (Linden 2017, 10–12.)

Turvallisuuskomitea (2018) linjaa termistössään, että identiteetinhallinta on joukko toimenpiteitä, joilla käyttäjien tunnuksia, rooleja ja ryhmiä hallinnoidaan. Tyypillinen esimerkki tällaisesta toimenpiteestä on AD-tunnuksen muokkaaminen, nimen, yksikön muuttaminen tai käyttäjäryhmän lisääminen tai poistaminen.

Vaikka käyttövaltuustermiä ei tunneta turvallisuuskomitean (2018) kyberturvallisuuden sanastossa, viitataan esimerkiksi kuntaliiton (2013) kuntasektorin käyttövaltuushallinnan viitearkkitehtuurissa pelkästään käyttövaltuuksiin. Käyttövaltuus-termiä käytetään myös valtiovarainministeriön (2006) vahti-ohjeessa, mutta ohjeessa puhutaan myös käyttövaltuushallinnosta, joka sanastossa kerrotaan olevan käyttöoikeuksien ja käyttövaltuuksien ylläpitoa. Valtiovarainministeriö (2006, 20) edelleen kertoo, että käyttövaltuuksien määrittely on työroolien ja käyttöoikeuksien määrittelyä. Terveyden ja hyvinvoinnin laitoksen julkaisemassa käytönhallinnan sanastossa (THL 2021) avataan käyttöoikeus ja käyttövaltuus, jossa käyttöoikeus on yksittäinen luku-, luonti, kirjoitus- tai poisto-oikeus ja taas käyttövaltuus on enemmänkin kooste useasta käyttöoikeudesta. Tässä opinnäytetyössä käytetään käyttövaltuustermiä juuri yllä mainitussa tarkoituksessa. Efecten IGA-järjestelmällä annetaan käyttäjille käyttövaltuuksia ja käyttöoikeudet määritellään kohdejärjestelmässä. Käyttöoikeuden kuvaaminen on helpointa esittää seuraavan esimerkin kautta. Verkkolevyllä on kuvapankkikansio, johon käyttäjille pitää määritellä käyttöoikeuksia. Tähän tarpeeseen luodaan AD-ryhmä sg_kuvapankki_rwx, jolle vastaavasti määritellään luku-, kirjoitus ja suoritusoikeudet (Read, Write ja Execute*)* kansioon. IGA-järjestelmässä kyseiselle AD-ryhmälle määritellään tarvittavia lisätietoja ja se liitetään käyttövaltuutena eri työrooleihin ja mahdollisesti erikseen tilattavaksi. Tarkasti voitaisiin sanoa, että käyttövaltuuden kautta saa viidet eri käyttöoikeudet: luku-, luonti-, muokkaus-, suoritus- ja poisto-oikeudet.

ISO 27002 -standardissa (SFS-EN 27002: 2017) käytetään pääosin termiä pääsynhallinta, jolla tarkoitetaan menettelyä, minkä avulla toteutetaan käyttäjien, sovellusten ja laitteiden roolinmukainen pääsy järjestelmään, siinä missä käyttöoikeuksienhallinnalla tarkoitetaan prosessin mukaista tapaa huolehtia käyttöoikeuksiin liittyvien pyyntöjen asianmukainen käsittely. (Turvallisuuskomitea 2018.) Tässä opinnäytetyössä tutkitaan myös standardin vaatimuksia

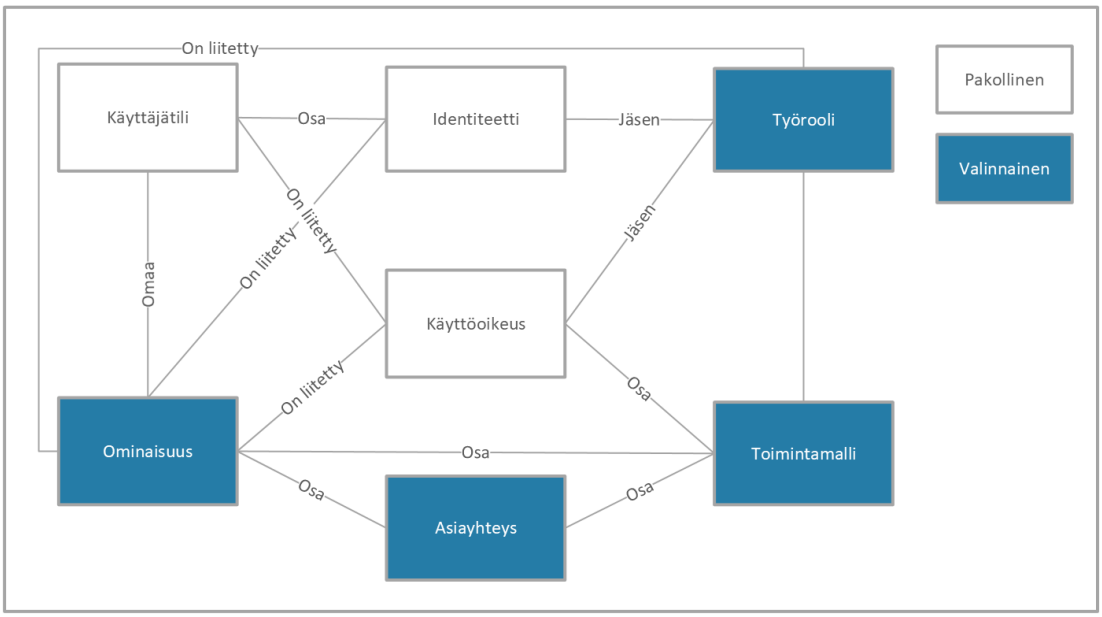
pääsynhallinnalle, koska se sisältää paljon myös identiteetin- ja käyttövaltuushallinnan vaatimuksia ja niiltä osin on tämän opinnäytetyön tutkimuksen kannalta oleellista.

On hyvä huomata, että puhekielessä käyttöoikeudella tyypillisesti tarkoitetaan käyttövaltuutta järjestelmään. Toisinaan käyttäjät saattavat puhua myös käyttäjätunnuksista, kun tarkoitetaan käyttövaltuutta. Käyttäjätunnuksella viitataan sähköiseen identiteettiin ja sillä olevaan käyttövaltuuteen. Joidenkin järjestelmien käyttäjähallinnassa käytetään myös rooleja sekä käyttäjäryhmiä, joilla viitataan käyttöoikeuksien kokoelmaan, jonka käyttäjä saa. Käyttäjällä voi samassa järjestelmässä olla yksi tai useampi rooli. Tämä järjestelmäkohtainen rooli tarkoittaa kuitenkin eri asiaa kuin Efecten IGA-järjestelmässä määritellyt roolit.

Tietojärjestelmien moninaisuuden vuoksi käyttöoikeushallintaa voidaan toteuttaa monella poikkeavalla tavalla ja jossain tapauksessa pelkkä käyttäjätunnus antaa ilman erillisiä käyttöoikeuksia pääsyn moneen tietoaineistoon. Yleisesti pelkkä AD-tunnus (työasematunnus) antaa pääsyn sähköpostiin, Teamsiin ja yrityksen intranetiin ja sitä kautta tietynlaisiin tietoaineistoihin. Näiden tietoaineistojen ei kuitenkaan lähtökohtaisesti tulisi sisältää sellaista tietoa, jonka käyttöoikeuksien hallinnasta pitäisi erikseen pitää järjestelmäkohtaista huolta.

Käyttöoikeuksien hallinnalla tarkoitetaan menettelyjä, joilla myönnetään, evätään tai käsitellään käyttöoikeuksia palveluissa ja järjestelmäresursseissa (Turvallisuuskomitea 2018). Käyttäjätunnuksilla viitataan yleisesti AD-tunnukseen, jolla työntekijälle mahdollistetaan työasemalla kirjautuminen ja esimerkiksi Microsoft-pilvipalvelujen käyttöoikeus. Käyttöoikeuksilla tarkoitetaan yleisesti AD-ryhmiä, mutta joissain tapauksissa myös yleensä legacy-järjestelmiä, joihin ei ole rakennettua kertakirjautumista tai AD-integraatiota.

Kunz ym. (2019) ovat havainnollistaneet Identity and Access Managementin (IAM), eli Identiteetin- ja käyttövaltuushallinnan kokonaisuuden käsitteellisessä mallissa (kuva 2), että käyttäjätili on vain osa identiteettiä ja käyttäjätili on liitetty yhteen tai useampaan käyttöoikeuteen. Käyttöoikeus voi olla erillinen tai osa työroolia. (Niemi 2020.)



Kuva 2. IAM-kokonaisuuden käsitteellinen malli (Kunz, ym. 2019, Niemen 2020, 9 mukaan)

Tutkimuksen aiherajauksen ja organisaation työkieleen vakiintuneen sanaston takia tässä tutkimuksessa päädyttiin termiin identiteetti- ja käyttövaltuushallinta. Tässä opinnäytetyössä käytetään termejä käyttövaltuus, käyttöoikeus tai pääsynhallinta aina sen mukaisesti, mihin asiaan se liittyy. Rooli- tai työrooli-termit tarkoittavat monesti samaa asiaa, ja tässä työssä termejä käytetään lähdeaineiston termistön mukaisesti.

2.4 Teoreettinen viitekehys

Opinnäytetyön teoreettinen viitekehys liittyy pitkälti lainsäädännön vaatimusten jälkeen kansallisiin ohjeisiin, suosituksiin sekä hyväksi havaittuihin käytäntöihin sekä standardeihin. Esimerkkinä voitaneen käyttää ISO 27001 -standardia, joka on yrityksen tapa todistaa noudattavansa vakioitua tietoturvallisuuden hallintajärjestelmää (SFS-EN 27001: 2017).

Tämä viitekehys valittiin, koska kunnan toimintaan vaikuttavat lait ovat ne keskeisimmät vaatimukset ja rajaukset, joiden mukaan on toimittava. Lait kuitenkin saattavat jättää paljon avoimia kysymyksiä varsinaiseen toteuttamistapaan, joihin kansallinen ohjeistus sekä aikaisemmin tutkittu tieto ja alan parhaat käytännöt tuovat tarvittavan toteutusnäkökulman. ISO 27001 -standardi on kansainvälisesti tunnustettu hyvä tapa toteuttaa tietoturvallisuuden hallintajärjestelmää. Kunnan identiteetin- ja käyttövaltuushallinnan toteutukseen sieltä

voi löytyä yksittäisiä erittäin hyödyllisiä ja hyväksi havaittuja tapoja, jotka halutaan adoptoida osaksi kunnan toimintaprosesseja ja käytäntöjä.

Aineistoa tutkimukseen kerättiin tutustumalla Suomen lainsäädäntöön, EU-direktiiveihin, kansallisiin ohjeisiin ja suosituksiin sekä yleisesti tunnettuun standardiin. Nämä yhdessä muodostavat laajan sekundääriaineiston tutkimukselle. Lisäksi tutkittiin aiheeseen liittyviä julkaisuja sekä tehtyjä opinnäytetöitä samasta aihepiiristä. Vaikka aikaisempien opinnäytetöiden aiheet ja tutkimuksen kohteet poikkesivat tämän opinnäytetyön aiheesta, tutkimuksilla oli väistämättä samoja yhteyskohtia. Tavoitteena oli löytää kansalliset lait, niiden reunaehdot ja niitä tukevat suositukset sekä tutkimukset tai julkaisut parhaiden käytäntöjen toteuttamiseen. Reunaehtojen lisäksi tavoitteena oli selvittää, miten identiteetin- ja käyttövaltuushallinnan toteuttaminen on kytköksissä tietoturvauhkiin tai kyberuhkiin.

Identiteetin- ja käyttövaltuushallintaan liittyy olennaisesti myös pääsynhallinta, tietosuoja ja tietoturva. Tästä aihepiiristä löytyi kattavasti tietoa tukemaan tätä tutkimusta. Primääriaineistona tutkimuksessa hyödynnettiin käyttövaltuushallinnan automatisoinnin projektin toteutuksessa tulleita teknisiä havaintoja, testitapauksia ja käyttäjien tai manuaalisen käyttöoikeusprovisioinnin tehtävien tekijöiden palautetta, jotka ovat Kanasen (2017, 43) mukaan interventiotutkimuksen aineistonkeruumenetelmiä. Interventiotutkimusta voidaan taas pitää yläkäsitteenä kehittämistutkimukselle (Jönsson & Lukka 2005, Kanasen 2017, 10, 18 mukaan).

3 LAINSÄÄDÄNTÖ

Lainsäädäntö muuttuu jatkuvasti ja tietosuojaan sekä tietoturvaan liittyvät asiat ovat monesti liitännäisiä muuttuneisiin lakeihin. Esimerkkinä tiedonhallintalaki (Laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906) asettaa reunaehtoja laadukkaaseen ja tietoturvalliseen viranomaisten tietoaineiston hallintaan ja lain yhden pykälän toteuttamisella käytännössä tarkoitetaan jopa vuosien toteutusprojektia viranomaisen organisaatiossa.

IT-alan yritykset seuraavat muuttuvaa tilannetta lainsäädännössä jatkuvasti ja reagoivat muuttuviin vaatimuksiin nopeasti ja tuotteistavat omia tuotteitaan

sen mukaisesti. Hyvänä ajankohtaisena esimerkkinä voidaan käyttää unionin oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta tehtyä direktiiviä (Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/1937), joka paremmin tunnetaan Whistleblower-direktiivinä. Vaikka kansallista lakia direktiivin käyttöönotosta ei vielä ole olemassa, yritykset ovat tuotteistaneet tämän palvelun osaksi omaa tuoteportfoliotaan (KPMG 2021; Efecte s.a.).

Viranomaisen tulisi aina ottaa itse selville, miten lainsäädäntö on muuttunut ja milloin sen velvoittavuus alkaa, eikä järjestelmätoimittajien tietoon viranomaista velvoittavasta laista tai sen tulkinnasta tulisi suoraan luottaa. Lain lausuntokierroksella muun muassa puolustusministeriö on lausunut, että lakiin tulisi lisätä siirtymäsäännös kaikille lain soveltamisalaan kuuluville organisaatioille (Puolustusministeriö 2021). Koska kansallinen laki ei ole vielä voimassa, ei voida varmuudella sanoa, milloin laki astuu voimaan ja suojelee ilmoittajaa sekä mikä on siirtymäaika lain velvoittavuudella. Oikeusministeriön tiedotteessa (Oikeusministeriö 2021) kerrotaan kansallisen lain valmistelun viivästymisestä ja todetaan selvästi, että ilmoituskanavia ei olisi tarkoituksenmukaista perustaa ennen lain voimaantuloa, koska ilmoittajansuojaa ei ennen tätä ole olemassa.

Whistleblower-direktiivin käyttöönotto kuvaa yhden esimerkin kautta valitettavaa tilannetta uusien lakien käyttöönoton prosessin aikana. Viranomaiselle muuttuva lainsäädäntö tarkoittaa aina lisää työtä ja selvitettävää lain vaikutuksista. Muutosten asianmukainen läpivienti toimintaprosesseihin ei tapahdu hetkessä ja voi tarkoittaa uuden palvelun tai tietojärjestelmän hankkimista, joka tulee suorittaa hankintalain (Laki julkisista hankinnoista ja käyttöoikeussopimuksista 1.1.2017/1397) mukaisesti. Täten onkin erityisen tärkeää olla tarkasti perehtynyt lainsäädäntöön ja sen todellisiin vaikutuksiin ennen muutosprojektin käynnistämistä.

Vaikka laki ei velvoittaisi tai viranomainen ei toiminnassaan tavoittele tiettyyn standardiin, on silti hyvä tarkastella lakia tai standardin vaatimuksia ja pyrkiä toimimaan sen suositusten mukaisesti niiltä osin, kun se viranomaisen toiminnalle on järkevää tai kustannustehokasta. Viranomaisille on tehty paljon myös ohjeita ja suosituksia, jotka eivät ole velvoittavia, mutta ohjeiden ja suositusten

hyöty on yhtenäiset toimintamallit, joista on hyötyä identiteetin- ja käyttöoikeushallinnan kokonaisuuden kannalta.

Tietoturvallisuus on johtamistoiminnan osa, josta jokaisen organisaation tulee huolehtia. Organisaation toiminnan ja siihen hankittujen palvelujen tietoturvallisuudesta tulee huolehtia sekä määritellä tarvittavat periaatteet ohjeistuksineen. Viranomaisen tehtävänä on määritellä ja hallinnoida käytössään olevien tietojärjestelmien ja henkilörekisterien käyttäjät tarkasti. Rekisterien käyttöön oikeutettujen henkilöiden käyttöoikeuksien laajuus ja käyttöoikeuksien voimassaoloaika tulee kirjata järjestelmään ja niitä tulee säännöllisesti, vähintään vuosittain, valvoa ja poistaa organisaation palveluksesta poistuneet käyttäjät sekä tarpeettomat roolit tai käyttöoikeudet tietojärjestelmästä. (Valtiovarainministeriö 2006.)

Identiteetin- ja käyttövaltuushallintaan vaikuttava lainsäädäntö rajoittuu pieneen määrään. Lait asettavat rajoituksia tiedon käsittelyyn ja luovat vaatimuksia, miten niitä pitää käsitellä. Käyttövaltuuksien osalta merkittävimmät lait ovat tietosuojalaki, joka määrittelee EU:n yleiseen tietosuoja-asetuksen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679) kansallisen käyttöönoton ja tiedonhallintalaki (Laki julkisen hallinnon tiedonhallinnasta).

Kummassakin laissa sekä tietosuoja-asetuksessa on olennaisia määrityksiä tai vaatimuksia, jotka toimivat ylimpänä ohjaavana kehyksenä identiteetin- ja käyttövaltuushallinnan toiminnassa.

Tietosuojalaki

Tietosuojalaki on laki, jolla on kansallisesti käyttöönotettu EU:n yleinen tietosuoja-asetus (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679) ja täsmennetty ja täydennetty henkilötietojen käsittelyä ja sen kansallista soveltamista. Identiteetin- ja käyttövaltuushallinnan näkökulmasta oleellista on, että laissa säädetään henkilötunnuksen käsittelystä. (Tietosuojavaltuutetun toimisto s.a.)

Identiteetin- ja käyttövaltuushallinnan järjestelmän automatisoinnin ja ongelmanselvitysten takia on tyypillistä käsitellä koko henkilöstöaineistoa, jossa mukana on myös henkilötunnus henkilön yksilöinnin takia. Tietosuojalain mukaan henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää. Henkilötunnusta ei tule kuitenkaan tarpeettomasti käyttää rekisterin perusteella laadituissa asiakirjoissa (Tietosuojalaki 29. §).

Julkisuuslaki

Julkisuuslaissa määritellään viranomaisen asiakirja, jossa asiakirjalla tarkoitetaan dokumenttia, jonka viranomainen on laatinut tai on vastaanottanut asiankäsittelyä varten. (Laki viranomaisten toiminnan julkisuudesta 5. § mom 2.) Tiedonhallintalain määritelmissä viitataan viranomaisen asiakirjaan, kun käsitellään tietovarantoja, tietoaineistoja ja tietojärjestelmiä (Laki julkisen hallinnon tiedonhallinnasta 2. §).

Työelämän tietosuojalaki

Tietosuojalaissa (Tietosuojalaki 30. §) viitataan työelämän tietosuojalakiin (Laki yksityisyyden suojasta työelämässä 13.8.2004/759), jonka mukaan henkilötietojen käsittely työsuhteen yhteydessä on sallittua vain välittömästi työsuhteen kannalta tarpeellisten henkilötietojen osalta, kun kyse on osapuolten oikeuksien ja velvollisuuksien hoitamisesta.

Henkilötunnuksen käsittely on kuvattu Sipoon kunnan henkilöstöpalvelujen tietosuojaselosteessa. Henkilötietojen käsittelyn tarkoitus on henkilöstöhallinnon ja palvelussuhdeasioiden hoitaminen. (Tietosuojaseloste / Henkilöstöpalvelut s.a.) Tietosuojalain ja tietosuojaselosteen perusteella henkilötietojen käsittely on siis perusteltua ja laillista.

Tiedonhallintalaki

Laki julkisen hallinnon tiedonhallinnasta, vakiintuneelta nimeltään tiedonhallintalaki, astui voimaan 1.1.2020 (Laki julkisen hallinnon tiedonhallinnasta). Lailla kumottiin aikaisemmin voimassa ollut tietohallintolaki (Laki julkisen hallinnon

tietohallinnon ohjauksesta (kumottu) 10.6.2011/634), joka keskittyi lähinnä tietohallinnon ohjaukseen, yhteentoimivuuteen ja kokonaisarkkitehtuuriin.

Uudessa laissa säädetään julkisen hallinnon yleisistä velvoitteista tiedonhallintaan, julkisen hallinnon tiedonhallinnan yleisestä ohjauksesta, tietoaineistojen muodostamisesta ja sähköisestä luovuttamisesta, julkisen hallinnon tietoturvallisuuden perusteista, teknisten rajapintojen hyödyntämisestä sekä asianhallinnasta ja tietoaineistojen säilyttämisestä. Käyttövaltuushallinnasta on säädetty lain 16. §:ssä. Viranomaisen tulee määritellä vastuullaan olevan tietojärjestelmänsä käyttöoikeudet ja ne tulee määritellä käyttäjän tehtävien mukaisesti ja käyttöoikeudet tulee pitää ajantasaisina. Laissa on myös § 12, joka vaatii, että tietohallinnon tulee tunnistaa erityistä luotettavuutta vaatimat tehtävät. Tietoturvallisuudesta, koskien tietojärjestelmiä ja tietoaineistoja, määritellään 13. §:ssä. (Laki julkisen hallinnon tiedonhallinnasta 12. §, 13. § ja 16. §.) Tiedonhallintalaissa tietojärjestelmillä käsitellään tietovarantoja, jotka koostuvat tietoaineistoista ja ne edelleen sisältävät viranomaisen asiakirjoja, kuten julkisuuslaissa on määritelty (Laki julkisen hallinnon tiedonhallinnasta 2. §). Viranomaisen asiakirja on keskeinen vaatimusten kohde.

Laki on ollut voimassa jo 1.1.2020 lähtien, mutta siihen on kirjattu siirtymäsäännöksiä. Pykälien 12–16 velvoittavuus astuu voimaan vasta 36 kuukauden kuluessa lain voimaantulosta. Käyttövaltuushallintaan liittyvän pykälän siirtymäsäännös loppuu siis kuntien osalta vasta 31.12.2022, johon mennessä toimenpiteet on saatettava valmiiksi.

4 EU:N YLEINEN TIETOSUOJA-ASETUS

EU:n yleinen tietosuoja-asetus, eli GDPR (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679) on henkilötietojen käsittelyä sääntelevä asetus, jonka täytäntöönpanosta on säädetty kansallinen laki. Lakia alettiin soveltaa EU-maissa keväällä 2018. (Tietosuojalaki.)

Yleisen tietosuoja-asetuksen keskeisin sisältö identiteetin- ja käyttövaltuushallintaan liittyen löytyy artikloista 5. henkilötietojen käsittelyä koskevat periaat-

teet, 24. rekisterinpitäjän vastuu, 25. sisäänrakennettu ja oletusarvoinen tietosuoja ja 32. käsittelyn turvallisuus. Yleisestä tietosuoja-asetuksesta puhuttaessa, tulee muistaa, että se koskettaa ainoastaan henkilötietojen käsittelyä.

Artikla 5 henkilötietojen käsittelyä koskevat periaatteet

Artiklassa 5 henkilötietojen käsittelyn koskevissa periaatteissa kohdassa 1 sanotaan, että henkilötietoja tulee käsitellä asianmukaisesti siten, että luvaton ja lainvastainen käsittely sekä vahingossa tapahtuva häviäminen, tuhoutuminen tai vahingoittuminen estetään. Alakohdassa mainitaan toimenpiteiksi asianmukaiset tekniset tai organisatoriset toimet (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 4 kohta 1 alakohta f; Linden 2017, 67). Linden (2017, 67) toteaa lisäksi, että juuri osoitusvelvollisuus, jolla henkilötietojen käsittelyä on noudatettu, on merkillepantavaa, koska sakot asetuksen rikkomisesta voivat olla yritykselle erittäin kovat.

Artikla 24 rekisterinpitäjän vastuu

Artiklassa 24 rekisterinpitäjän vastuusta sanotaan, että rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja voidaan osoittaa tietojenkäsittely tämän asetuksen mukaisesti. Lisäksi toimenpiteet tulee tarkistaa ja päivittää tarpeen mukaan. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 24 kohta 1.)

Lisäksi mainitaan, että rekisterinpitäjä voi halutessaan toteuttaa sertifioinnin, jolla osoitetaan, että rekisterinpitäjä noudattaa sille asetettuja velvollisuuksia (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 24 kohta 3 ja artikla 42 kohta 3). Lisäksi viitataan käytännesääntöihin, jossa mainitaan, että jäsenvaltioiden on edistettävä käytännesääntöjen laatimista, joilla tuetaan asetuksen asianmukaista soveltamista (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 40 kohta 1).

Artikla 25 sisäänrakennettu ja oletusarvoinen tietosuoja

Artiklassa 25 on sanottu, että asianmukainen tietojen käsittely edellyttää huomioimaan tiedonkäsittelyn luonteen, laajuuden, asiayhteyden sekä tarkoituksen. Lisäksi tulee huomioida tiedonkäsittelyn riskien todennäköisyys ja vakavuus. Asian keskiössä on koko ajan rekisteröidyn oikeudet. Toimenpiteinä mainitaan tietosuojaperiaatteiden mukainen tietojen minimointi sekä asianmukaiset tekniset ja organisatoriset toimet, jossa tulee ottaa huomioon uusin tekniikka ja toteuttamiskustannukset. Näillä toimilla varmistetaan, että käsitellään vain tarpeellisia rekisteröidyn henkilötietoja. Rekisterinpitäjän velvollisuus on huolehtia käsittelyn laajuudesta, säilytysajoista ja saatavilla olosta. Erityisesti mainitaan, että henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman, että luonnollinen henkilö on mukana käyttöoikeuksien myöntämisessä. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 25.)

Artikla 32 käsittelyn turvallisuus

Artiklassa 32 käsittelyn turvallisuudessa viitataan artiklassa 25 listattuihin tietojenkäsittelyyn liittyviin asioihin, tekniikkaan, kustannuksiin, käsittelyn luonteeseen, laajuuteen, asiayhteyteen ja tarkoituksiin sekä riskeihin. Toimenpiteinä turvalliseen käsittelyyn mainitaan mm. henkilötietojen pseudonymisointi ja salaus, järjestelmien ja palvelujen jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus, teknisistä vikatilanteista toipuminen ja tietojenkäsittelyn turvallisuuden varmistamisen menettelyt. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 32.)

5 OHJEET JA SUOSITUKSET

Viranomaisen työtä helpottaakseen on luotu runsas joukko erilaisia ohjeita. Valtiovarainministeriön asettama tietoturvallisuuden johtoryhmä (Vahti) on luonut runsaasti vahti-ohjeita, jotka ovat olleet vuosia käytössä ja tästä syystä erittäin tunnettuja (Valtiovarainministeriö 2006). Identiteetin- ja käyttövaltuushallinnan näkökulmasta vahti-ohjeistus on todella vanhaa. Vahti-ohjeisiin viitataan kuitenkin useasti tietohallinnon tietoturvatyöskentelyssä, joten ohjeistuksen käsitteleminen suppeasti on tältä osin perusteltua.

Puolustusministeriön laatima Katakri, eli kansallinen turvallisuusauditointikriteeristö, on alkujaan suunnattu valtionhallintoon, mutta nykyisin sen päivitetty versio pohjautuu lainsäädäntöön, joka velvoittaa myös kuntia, joten sen käsittely ja vaatimusten huomioiminen on järkevää. (Ulkoministeriö 2020, 2–6.) Pilvipalveluiden turvallisuuden arviointikriteeristö, eli PiTuKri, on Liikenne- ja viestintävirasto Traficomin alaisuudessa toimivan Kyberturvallisuuskeskuksen julkaisema työkalu pilvipalvelujen turvallisuuden arviointiin, joka antaa myös hyviä suosituksia pilvipalvelujen käyttövaltuushallinnan turvallisuuteen, ja viittaa muun muassa ISO 27001 -standardiin (SFS-EN 27001: 2017). (Kyberturvallisuuskeskus 2020b, 3.)

Suurimmassa roolissa kuntasektorin toimintaa ohjaavana ohjeena ja suosituksena toimii tiedonhallintolautakunnan (2021) tuottama suosituskokoelma ja kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri (Kuntaliitto 2013.)

5.1 Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta

Valtiovarainministeriö on laatinut suosituskokoelman tiedonhallintalain (Laki julkisen hallinnon tiedonhallinnasta) säädösten tarkemmasta toteuttamisesta. Identiteetin- ja käyttövaltuushallinnan osuus on laissa kirjattu hyvin lyhyesti. Suositusdokumentti avaa tarkemmin sen mitä lain laatija on tarkoittanut lakia säätäessään. Tiedonhallintolautakunnan (2021, 67–69) antama suosituskokoelma antaa viranomaiselle toimenpide-ehdotuksia tiedonhallintalain asettamien vaatimusten täyttämiseen. Tästä syystä suosituskokoelmaa voi pitää yhtenä tärkeimmistä identiteetin- ja käyttövaltuushallinnan toimintaa ohjaavista dokumenteista kuntasektorilla, koska lain yhtenä tarkoituksena on varmistaa yhdenmukainen ja laadukas tiedonhallinta tietoturvaa unohtamatta. Suosituskokoelma on myös hyvin ajantasainen, koska se on valmistunut vuonna 2021 (Tiedonhallintalautakunta 2021, 67–69).

Suosituskokoelmassa on selitetty toimenpiteet, joilla viranomainen voi toteuttaa toimet tiedonhallintalain (Laki julkisen hallinnon tiedonhallinnasta 16. §) vaatimusten mukaisesti. Käyttöoikeuksien hallinnan edellytyksistä on kerrottu hyödyllinen 14 kohdan luettelo konkreettisista toimista, miten käyttöoikeuksien

hallintaa tulee toteuttaa. Luettelon asiat jakaantuvat karkeasti prosessiin-, ohjeisiin, vastuuseen ja oikeuksiin liittyviin asioihin. (Tiedonhallintalautakunta 2021). Yhteenvetona luettelosta voi todeta, että yksikään käyttöoikeuksiin liittyvä asia ei ole vailla vastuuhenkilöitä tai dokumentoimaton, käyttövaltuushallintaan liittyvät asiat ovat tarkasti kuvattuja vakiomuotoisten prosessien mukaisia toimintoja, joissa ei ole mahdollisuutta vapaamuotoiselle toiminnalle.

Käyttöoikeuksien hallinta ja sen edellytykset

Suosituskokoelmassa on kirjattu käyttöoikeushallinnan edellytyksistä 14 kohdan lista, jossa otetaan kantaa, niin vastuuhenkilöihin tai omistajiin, ohjeistukseen, prosessiin ja oikeuksien myöntämisen perusteisiin ja poikkeuksiin. (Tiedonhallintalautakunta 2021, 67–68.)

Suosituskokoelman edellytyksinä on, että käyttöoikeuksien hallintaan tulee nimetä vastuuhenkilöt ja lisäksi jokaiselle käyttäjätunnukselle tulee nimetä omistaja, joka käsittää myös kone- tai palvelutunnukset, joita tyypillisesti tarvitaan teknisissä ratkaisuissa. Käyttäjätunnusten luomiseen, hyväksymiseen ja ylläpitoon, sekä poistamiseen tulee olla kuvattu prosessi ja vastuuhenkilöt tulee ohjeistaa ylläpitotehtäviin. Tunnuksien voimassaolo tulee perustua todelliseen ennalta sovittuun tarpeeseen. Organisaation ulkoisilla työntekijöillä tulee olla ostopalvelusopimus tai muu sopimus, joka perustelee tunnuksen voimassaolon. Ulkoisten käyttäjien tunnukset tulee myös erottaa sisäisten käyttäjien tunnuksista pelkän käyttäjätunnuksen perusteella. (Tiedonhallintalautakunta 2021, 67.)

Tunnuksen luonti automaattisesti työsuhteen alkaessa, perustuu juuri työsuhteen voimassaoloon. Samoin sen poistaminen työsuhteen päättyessä. Kunnalla käytetään etenkin sosiaali- ja terveysalalla, sekä sivistysalalla paljon lyhytaikaisia sijaisia, joista osa hankitaan kolmannen osapuolen yrityksestä.

Kaikista järjestelmiin annetuista käyttöoikeuksista tulee pitää ajantasaista tietoa yllä. Kaikista toimenpiteistä tulee jäädä asianmukaiset merkinnät, joista selviää koko prosessi ja siihen liittyvät vaiheet, tilaus, tilattu oikeus ja hyväksynnät. Käyttöoikeuksia tulee katselmoida säännöllisesti, vähintään kerran

vuodessa, jotta tarpeettomat käyttäjätilit ja oikeudet voidaan poistaa. Katselmointitapahtuma tulisi myös dokumentoida auditointia varten. (Tiedonhallintalautakunta 2021, 68.)

Järjestelmien käyttöoikeuksia myönnettäessä tulee noudattaa vähimpien käyttöoikeuksien periaatetta (Principle of Least Privilege). Vähimpien oikeuksien periaatteessa käyttäjälle annetaan vain ne oikeudet, joita hän tarvitsee. Lisäksi käyttöoikeuksia määriteltäessä tulisi erityisesti huomioida vaaralliset yhdistelmät sekä korkean riskin käyttäjäroolit, joita ovat esimerkiksi, ylläpitäjät, pääkäyttäjät tai muut erityistä luotettavuutta sisältävät roolit. Tällaisilla rooleilla tulisi lisäksi olla erityinen tilaus ja hyväksymisprosessi. Vaarallisten yhdistelmien osalta lisäksi todetaan, että ne tulee tunnistaa ja dokumentoida, mutta niiden hallitsemiseen riittää myös riskienhallinnan ratkaisut, jos rooleja ei voida eriyttää organisaatiossa. (Tiedonhallintalautakunta 2021, 67–68.)

Työssäni olen havainnut, että kuntasektorilla on monesti hyvin rajallinen määrä työntekijöitä hoitamassa tehtäviä ja moni korkean riskin rooli ja vaarallinen yhdistelmä kasautuu samojen henkilöiden tehtäviin.

Muutokset, seuranta ja hallinta

Käyttöoikeuksien muuttamisesta ja poistamisesta tulee vastaavasti olla kuvatut prosessit, jolla varmistetaan, että työtehtävien muuttuessa henkilön käyttövaltuudet muuttuvat uuden tehtävän mukaiseksi. (Tiedonhallintalautakunta 2021, 68–69.)

Kaikkia käyttäjätunnuksia ja käyttövaltuuksia tulee aktiivisesti seurata ja valvoa, jotta varmistutaan niiden asianmukaisuudesta. Havaituista poikkeamista tulee käynnistää ennalta sovittu prosessin mukainen toiminta. Valvonta takaa sen, että käyttäjätunnukset ja käyttövaltuudet ovat ajantasaiset ja ne noudattavat organisaation luomia käytäntöjä. Valvonnassa korostuu aikaisemminkin erityisasemaan nostetut vaaralliset yhdistelmät sekä korkean riskin käyttäjäroolit. (Tiedonhallintalautakunta 2021, 69.)

5.2 Käyttövaltuushallinnon periaatteet ja hyvät käytännöt

Vahti on valtiovarainministeriön asettama tietoturvallisuuden johtoryhmä, jonka päätavoitteena on muun muassa julkisen hallinnon toiminnan ja ICT-palvelujen turvaaminen sekä turvallisen uuden teknologian käyttöönoton mahdollistaminen. Vahti laatii selvityksiä, ohjeita ja käytänteitä ja pyrkii edistämään organisaatioiden digiturvakulttuuria sekä asennetta. (Digi- ja väestötietovirasto s.a.)

Vahti on laatinut ohjeen käyttövaltuushallinnon periaatteet ja hyvät käytännöt 9/2006 (Valtiovarainministeriö 2006). On kuitenkin todettava, että vahti-ohje on vuodelta 2006 ja se ei luonnollisesti huomioi tämän jälkeen tapahtunutta muutosta lainsäädännössä. Tiedonhallintalaki eli Laki julkisen hallinnon tiedonhallinnasta ja EU:n yleisen tietosuoja-asetusten vaatimukset puuttuvat vahti-ohjeesta.

Ohjeessa korostetaan johdon roolia ja sitoutumista, mutta se nostaa esiin myös valtiovarainministeriön suosituskokoelmassa (Tiedonhallintalautakunta 2021) esiin nostettuja asioita, kuten omistajuudet, hallintaprosessien kuvaaminen ja roolien määrittely (Valtiovarainministeriö 2006, 15–19).

Ohjeessa ei käsitellä sellaisia vaatimuksia, joita ei olisi jo huomioitu uudemmissa ohjeistuksissa, mutta se kuvaa hieman tarkemmin käyttövaltuushallintajärjestelmän käyttöönottoon liittyviä asioita kuten hallintajärjestelmän käyttöönottoon liittyvien järjestelmävalmiuksien suunnittelua ja toteutusta. Ohjeessa nostetaan esiin johdon roolia ja sitoutumista ja miten käyttövaltuushallinto liitetään osaksi riskienhallinnan prosessia. (Valtiovarainministeriö 2006, 15.)

5.3 Tietoturvallisuuden auditointityökalut

Puolustusministeriö on julkaissut Katakrin eli kansallisen turvallisuusauditointikriteeristön ensimmäisen kerran jo vuonna 2009. Nykyinen versio, Katakri 2020 - tietoturvallisuuden auditointityökalu viranomaisille, on jo neljäs päivitys Katakriin ja nykyisin sen päivitys ja hallinnointi on ulkoministeriön vastuulla. Viimeisimmässä päivityksessä on huomioitu viimeisin kansallinen lainsäädäntö ja huomioitu digitaalisen tietojenkäsittelyn kehitystä ja paranneltu ohjeistuksia. (Ulkoministeriö 2020, 2.)

PiTuKri, eli pilvipalveluiden turvallisuuden arviointikriteeristö on Liikenne- ja viestintävirasto Traficomin alaisuudessa toimivan Kyberturvallisuuskeskuksen tuottama ja sen tavoitteena on edistää viranomaisen käyttämien pilvipalvelujen ja niissä pidettävän salassa pidettävän tiedon turvallisuutta. PiTuKrin on tarkoitus olla työkalu pilvipalveluiden turvallisuuden arvioinnissa. (Kyberturvallisuuskeskus 2020b, 3.)

Vähimpien oikeuksien periaatetta on käsitelty sekä Katakrin tietojärjestelmäturvallisuuden luvussa, että PiTuKrin Identiteetin- ja pääsynhallinnan osa-alueessa (Ulkoministeriö 2020, 75–76; Kyberturvallisuuskeskus 2020b, 35). Kummassakin työkalussa on kerrottu samat vaatimukset ja toimenpiteet vähimpien oikeuksien periaatteen toteuttamiseen. Ensinnäkin käyttöoikeudet tulee määritellä, ja niiden myöntäminen voidaan antaa vain henkilölle, kenen käsittelyoikeudet on varmistettu. Näillä käsittelyoikeuksilla tarkoitetaan, että henkilö on organisaation työntekijä tai esimerkiksi toimittajan edustaja ja siten työtehtävän kautta oikeutettu kyseiseen käyttövaltuuteen. Lisäksi sanotaan, että käyttöoikeudet tulee pitää ajantasaisina ja käyttäjille ja automaattisille prosesseille annetaan vain ne oikeudet tai valtuudet, joita kyseisen tehtävän suorittaminen vaatii. Tämä on niin sanottu vähimpien oikeuksien periaate.

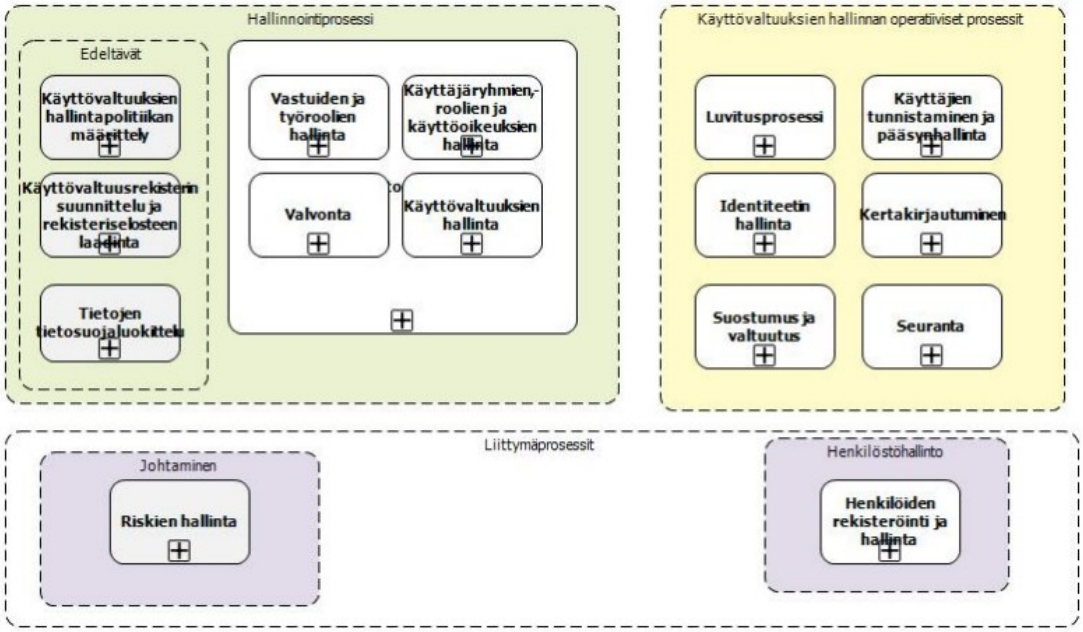
Vähimpien oikeuksien periaate (Principle of Least Privilege) on hyvin yleisesti tunnistettu tapa pienentää riskiä väärinkäytöksistä. Loppujen lopuksi tämä kytkeytyy tietoturvaloukkauksen riskiin tietojen tuhoutumisesta tai hävittämisestä. Perusajatus tässä periaatteessa on sallia käyttäjälle, ohjelmalle tai prosessille vain vähimmät oikeudet, mitä kyseisen asian toteuttamiseen tarvitaan. Esimerkiksi tietokannan varmistusten toteuttamiseen annetut admin-tasoiset oikeudet Edward Snowdenille mahdollistivat Yhdysvaltain kansallisen turvallisuuspalvelun (National Security Agency) tietojen vuotamisen. (Lord 2017.) Snowdenin tapauksen jälkeen 90 % NSA:n työntekijöiltä poistettiin korkeamman tason oikeuksia (Lord 2017; Allen 2013).

5.4 Käyttövaltuushallinnan viitearkkitehtuuri

Kuntaliiton julkaisema käyttövaltuushallinnan viitearkkitehtuuri käsittelee käyttövaltuushallintaa laajemmin. Käyttäjät jaotellaan aluksi viiteen eri ryhmään, joita ovat: henkilöasiakkaat ja organisaatioasiakkaat, kunnan työntekijät ja kumppanin työntekijät, jotka jaetaan kunnan sisäverkossa työskenteleviin

työntekijöihin ja kumppanin omassa verkossa työskenteleviin työntekijöihin. (Kuntaliitto 2013, 15.)

Käyttövaltuushallinnan viitearkkitehtuurissa hallinta on jaettu kahteen prosessiluokkaan, hallinnointiprosesseihin ja operatiivisiin prosesseihin (kuva 3). (Kuntaliitto 2013, 17.)



Kuva 3. Käyttövaltuushallinnan prosessikartta (Kuntaliitto 2013, 17)

Viitearkkitehtuurissa nostetaan esiin, että henkilöstöhallinnan prosessit linkittyvät tiukasti käyttövaltuushallinnan prosessien kanssa. Käyttövaltuuksien hallinnointi alkaa jo rekrytointiprosessin aikana ennen työsopimuksen allekirjoitusta ja päättyy lopulta, kun työntekijän työsuhde päättyy. (Kuntaliitto 2013, 17–18.)

Roolittamisesta mainitaan, että työroolit ovat käyttövaltuushallinnan perusta. Työntekijä tulisi liittää työrooleihin jo henkilön perustietoja luotaessa, käytännössä rekrytointivaiheessa. Rooleissa tuodaan esiin, että niillä tulee nimetä omistaja ja niillä tulisi olla henkilöstöhallinnon vastuuhenkilö, jonka tehtävänä on määritellä työroolit. Työroolien määrä tulisi pitää kohtuullisena, mieluiten noin sadassa, koska muutoin hallinta hankaloituu. (Kuntaliitto 2013, 18–19.)

Peussa ja Ruotsalainen (2013) kuvaavat vaarallisen työyhdistelmän syntymistä, kun työtehtäviä ei eriytetä tarpeeksi. Esimerkiksi sama henkilö ei saisi

hyväksyä ostoja ja vastata rahaliikenteestä tai ostotilausten tekijän ei tulisi hyväksyä laskua. Vaarallisten yhdistelmien välttämisellä ennalta ehkäistään väärinkäytöksiä.

Eriytettävät roolit ovat käytännössä käyttövaltuushallinnan viitekehyksessä kuvattuja työrooleja. Vaaralliset työyhdistelmät on mainittu viitekehyksessä ensimmäisen kerran esimiehen tehtävänä määräaikaista työsopimusta luotaessa, jolloin tulisi jo tunnistaa ennalta mahdolliset vaaralliset työyhdistelmät, joita ei saisi muodostua työntekijälle. Seuraava maininta vaarallisista työyhdistelmistä on valvonnan luvussa, jossa valvontaprosessin mukaisesti tulisi tarkistaa, onko työntekijöille myönnetty vaarallisia työyhdistelmiä. Tämän lisäksi luvitusprosessissa kuvataan käyttöoikeuspyynnön hyväksymisen tehtävänä arvioida vaarallinen yhdistelmä hyväksyntää tehdessä. Viimeinen maininta vaarallisista työyhdistelmistä nähdään viitekehyksessä identiteetinhallintapalvelun kuvauksessa, jossa kerrotaan vain vaarallisten työyhdistelmien raportoinnin helpottuvan järjestelmän avulla. (Kuntaliitto 2013, 6, 26, 30, 55.)

Käyttövaltuushallinnan viitearkkitehtuuri on laadittu ennen EU:n yleisen tietosuoja-asetuksen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679) ja tiedonhallintalain (Laki julkisen hallinnon tiedonhallinnasta) voimaantuloa ja niiltä osin viitteitä uusiin lakeihin ei ole. Viitearkkitehtuurissa viitataan laajalti vahti-ohjeisiin, jotka monin osin ovat vanhentuneita.

Hallinnointiprosessit

Ennen hallinnointiprosessien kuvaamista, tulisi viitearkkitehtuurin mukaan määritellä edeltävät tehtävät, jotka ovat edellytys onnistuneen käyttövaltuushallinnan luomiselle. Edeltäviin tehtäviin on listattu käyttövaltuuksien hallintapolitiikan määrittely, tietojen luokittelu ja käyttövaltuusrekisterin suunnittelu ja rekisteriselosteen laadinta (kuva 3). Tärkeänä lähtökohtana nostetaan esiin organisaation järjestelmäsalkun dokumentointi käyttövaltuushallinnan perspektiivistä. (Kuntaliitto 2013, 21.)

Varsinaiset hallinnointiprosessit ovat vastuiden ja työroolien hallinta, käyttäjäryhmien, -roolien ja käyttöoikeuksien hallinta, valvonta sekä käyttövaltuuksien

hallinta. Valtiovarainministeriön (2006) vahti-ohjeen tavoin, käyttövaltuushallinnan viitearkkitehtuuri korostaa johdon vastuuta, joiden tehtäviin kuuluvat vastuuhenkilöiden nimeäminen ja vastuiden määrittäminen. Muissa prosesseissa viitataan vastuun osalta pitkälti juuri tähän johdon asettamaan vastuuhenkilöön. (Kuntaliitto 2013, 23–28.)

Operatiiviset prosessit

Operatiiviset prosessit varmistavat onnistuneen käyttövaltuushallinnan. Operatiivisiin prosesseihin luetaan luvitusprosessi, identiteetinhallinnan prosessi, suostumukset ja valtuutukset, käyttäjien tunnistaminen ja pääsynhallinta, kertakirjautumisen sekä seurannan prosessit. Prosessit on kuvattu tarkasti ja pitää sisällään järjestäen myös useina prosessikaavioina sekä listattu erillisiksi tehtäviksi. (Kuntaliitto 2013, 28–43.)

Luvitusprosessissa mainitaan itsepalvelu käyttövaltuuksien hakemiseen, provisiointitehtävät kohdejärjestelmiin, jossa myös manuaalinen provisiointi on mainittu. Luvitusprosessissa on kuvattu toimintamalli ja tietovirrat sekä itsepalvelun ja käyttövaltuushakemiston hallinnan osaprosessit sekä näiden tehtävät. Itsepalvelun tehtävissä mainitaan, että esimiehen tulee hyväksyä käyttäjän tekemä hakemus, kun taas tiedonhallintalautakunnan (2021) suosituskokoelman mukaan riittää, että prosessi on kuvattu ja ohjeistettu. (Kuntaliitto 2013, 28–30.)

6 STANDARDIT JA PARHAAT KÄYTÄNNÖT

Seuraavassa kuvattujen standardien yhteydessä käytetään termiä pääsynhallinta, koska tätä termiä käytetään kyseisten standardien vaatimuksissa. Identiteetin ja käyttövaltuushallinnan osuus on kuvattu standardeissa, mutta terminologia poikkeaa tässä opinnäytetyössä käytetystä termistöstä.

ISO 27001 ja ISO 27002

ISO 27001- standardi (SFS-EN 27001: 2017) on erittäin tunnettu ja laajalti käytetty standardi tietoturvan hallintajärjestelmästä ja kontrolleista. DNV (s.a.)

mukaan ISO 27001 on kansainvälisesti tunnustetuin standardi tietoturvan hallintajärjestelmänä. Standardissa kerrotaan turvallisuuskontrollit, mutta ei kuitenkaan kerrota tarkemmin, miten niiden toteuttaminen olisi suositeltavaa tehdä. Sitä tukemaan on olemassa ISO 27002 -lisästandardi (SFS-EN 27002: 2017), joka antaa neuvoja ISO 27001 -standardin toteuttamiseen.

ISO 27002 -standardi (SFS-EN 27002: 2017) on erittäin hyvä täydentävä standardi, koska se käsittelee keskimäärin sivun mittaisella kuvauksella jokaisen tietoturvakontrollin. Standardi selittää kuinka jokainen kontrolli toimii, mikä niiden tarkoitus on ja miten organisaatio voi toteuttaa kyseisen kontrollin toteuttaakseen standardin vaatimuksia. (Irwin 2019.)

ISO 27002 -standardin (SFS-EN 27002: 2017) keskeisin identiteetin- ja käyttövaltuushallinnan osuutta koskeva sisältö liittyy pääsynhallintaosuuteen. Pääsynhallinta jakaantuu neljään alalukuun, joista pääsynhallinnan liiketoiminnalliset vaatimukset, pääsyoikeuksien hallinta ja järjestelmien ja sovellusten pääsynhallinta liittyvät tiukasti Identiteetin- ja käyttövaltuushallinnan osuuteen. Neljäs luku liittyy käyttäjän vastuisiin ja on siten löyhästi ohjeistuksen kautta linkitettävissä myös identiteetin- ja käyttövaltuushallinnan toteutukseen.

Organisaatiolla tulisi olla pääsynhallintapolitiikka laadittuna ja käytössä. Sillä tulisi määritellä miten pääsyä hallitaan ja kenelle pääsyoikeuksia annetaan. Tietovarantojen omistajien tulisi määritellä pääsynhallintasäännöt suojattavalle omaisuudelle ja näissä tulisi ottaa huomioon tietoturvariskit (Krapels 2018, SFS-EN 27002: 2017, 27).

Pääsy verkkoihin ja verkkopalveluihin tulisi rajoittaa vain niille, jotka tarvitsevat sitä työtehtävänsä suorittamiseen. Esimerkkinä voitaisiin mainita, että peruskäyttäjän ei tulisi päästä verkkoon, jossa on käytössä erikoiskoneita, ja työntekijät voisivat aiheuttaa tahatonta vahinkoa. (Krapels 2018.) ISO 27002 -standardissa (SFS-EN 27002: 2017, 28) nostetaan esiin verkkojen lisäksi VPN-yhteydet ja verkkojen palvelut.

Käyttäjien rekisteröinti ja poistaminen edellyttää, että jokaiselle käyttäjälle luodaan yksilöllinen tunnus, jonka avulla voidaan määrittää käyttöoikeudet eri resursseille ja verkoille yksityiskohtaisesti ja lisäksi valvoa tunnuksen käyttöä.

Käyttäjätunnus tulee poistaa tai jäädyttää välittömästi, kun työntekijä lähtee organisaatiosta. (Krapels 2018.) Jaettujen tunnusten käyttäminen tulisi olla sallittua vain, mikäli liiketoiminnalliset tai toiminnalliset tarpeet perustelevat ne ja tuolloinkin ne olisi erikseen hyväksytettävä ja dokumentoitava (SFS-EN 27002: 2017, 29).

Käyttäjien käyttöoikeuksien hallinta edellyttää prosessia käyttöoikeuksien myöntämistä ja poistamista varten. Suositeltavaa olisi luoda roolit samaa tehtävää tekeville työntekijöille ja antaa heille roolin mukaisesti samat peruskäyttöoikeudet. (Krapels 2018.) Prosessissa tulisi huomioida hyväksyntämenettelyt, pyynnön oikeellisuus pääsynhallintapolitiikan kanssa ja käyttäjien roolien tai työtehtävien muuttumisen yhteydessä pääsyoikeuksien välitön poistaminen. Pääsyoikeuksien säännöllinen katselmointi ohjeistetaan myös täällä. (SFS-EN 27002: 2017, 29.)

ISO 27002 -standardi (SFS-EN 27002: 2017, 30) toteaa ensinnäkin, että ylläpito-oikeuksien jakamista ja käyttöä tulisi rajoittaa ja valvoa. Krapels (2018) mainitsee, että joillakin työntekijöillä on oltava erityiset käyttöoikeudet tietovarantoihin tai järjestelmiin. Esimerkiksi järjestelmänvalvojat ovat tällaisia työntekijöitä, jotka tarvitsevat ylläpitotehtävissään kovimpia mahdollisia oikeuksia. Tämänkaltaisia oikeuksia tulisi käsitellä huolellisesti, koska väärinkäytöksen seuraukset voivat olla erittäin vakavia (Krapels 2018).

Käyttäjien tunnustautumistietoja, kuten salasanoja, salausavaimia ja varmennekortteja on hallittava muodollisesti. Tällaisia toimintoja ovat esimerkiksi käyttäjätunnuksen salasanan pakotettu vaihtaminen ensimmäisen kirjautumisen yhteydessä ja uuden salasanan vaihtamisen yhteydessä käyttäjän henkilöllisyyden varmistaminen. (Krapels 2018; SFS-EN 27002: 2017, 31.)

Pääsyoikeuksien uudelleen arvioinnista Krapels (2018) mainitsee, että organisaatiot ja niiden työntekijät eivät ole staattisia. Työntekijät vaihtavat työpaikkaa ja niiden roolit tai työtehtävät organisaation sisällä muuttuvat usein ja näin tarve käyttöoikeuksien muuttamiselle on jatkuvaa. Tietovarantojen omistajien tulisi säännöllisesti katselmoida heidän käyttöoikeuksiaan ja erityisesti kiinnittää huomiota ylläpitäjien oikeuksiin niiden arkaluonteisuuden takia. (Krapels 2018.)

Työntekijän työsopimuksen päättyessä, käyttöoikeuksien poistaminen tulisi tapahtua heti ja mikäli käyttöoikeuksia ei voida poistaa, niitä tulisi vähintään muuttaa. Jos työntekijän tiedossa on ollut käyttäjätunnuksia, jotka jäävät edelleen käyttöön, niiden salasanat tulisi vaihtaa välittömästi. Tämän toiminnan tulisi olla käytäntö, koska entisen työntekijän tai sopimusosapuolen luvaton tietojen käyttö voi tapahtua nopeasti ja sen vaikutukset voivat olla vakavia. (Krapels 2018.)

Pääsynhallintapolitiikan voi laatia täydelliseksi, mutta se ei yksistään riitä. Organisaation tulee varmistaa, että työntekijät noudattavat ohjeistusta. Tässä korostetaan työntekijän vastuuta. Salasanan muodostamiseen tulee olla ohjeet, joiden mukaan tulee toimia, jos järjestelmää ei voida pakottaa vaatimaan riittävän vahvaa salasanaa. Ohjeissa tulee myös huomioida tunnistetietojen, eli tunnuksen ja salasanan, jakamisen kieltäminen muille työntekijöille ja henkilökohtaisessa käytössä olevan salasanan kieltäminen yrityksen järjestelmissä. (Krapels 2018.) Pääsyn rajoittamisesta tietoihin, Krapels (2018) toteaa hyvin suppeasti, että rajoituksia tulee tehdä juuri pääsynhallintapolitiikan mukaisesti.

Turvallinen kirjautuminen nojaa pääsynhallintapolitiikan vaatimuksiin. Siinä missä Krapels (2018) toteaa vain, että pääsynhallintapolitiikan mukaisesti pääsyä tulee tietyissä järjestelmissä toteuttaa juuri tällä tavalla, ISO 27002 -standardissa (SFS-EN 27002: 2017, 33–34) turvallista kirjautumista käsitellään hyvin yksityiskohtaisesti. Toteutusohjeet lähtevät käyttäjän henkilöllisyyden tunnistamisesta, vahvan kirjautumismenetelmän käytöstä kattaen järjestelmän luvattoman käytön ennalta ehkäisevät toimenpiteet.

Parhaat käytännöt

Parhaiden käytäntöjen joukossa käsitellään myös sellaisia kokonaisuuksia, jotka eivät kuulu tämän opinnäytetyön rajattuun aiheeseen, mutta ovat kuitenkin käsitelty tiedonhallintalautakunnan (2021) toteuttamassa suosituskokoelmassa ja ovat siten linjassa tämän opinnäytetyön asiakokonaisuuden kanssa.

Identiteetin- ja pääsynhallinnan parhaita käytäntöjä on julkaistu paljon varsinkin IAM-ratkaisuja toteuttavien yritysten toimesta. Parhaat käytännöt pääsääntöisesti toteuttavat erilaista ideologiaa, mitä aikaisemmin kuvatut lait, asetukset, ohjeet, suositukset tai standardit ovat ohjeistaneet. Siinä missä edellä mainitut kuvaavat enemmän vaatimuksia, parhaat käytännöt ovat toteutustapoja.

SailPoint esittelee parhaiksi käytännöiksi seitsemän kohdan listan. IAM-työ tulisi aloittaa vasta, kun on tiedossa mitä ollaan tavoittelemassa tai mihin ollaan menossa. Ilman tavoitetilaa, on vaikea toteuttaa IAM-projektia. Korkean riskin järjestelmistä tulisi luopua kokonaan. Erityisesti mainitaan, että legacy-järjestelmistä tulisi luopua, koska pilvipalvelujen tarjoama turva on huomattavasti parempaa mm. tietoturvapäivitysten, segmentoinnin, salaamisen, integroinnin ja suojatun pääsyn vaatimuksien toteuttamiseen. (SailPoint 2021.)

Säännöllinen katselmointi ja orpotilien poistaminen, identiteetin hallinnan automatisointi työsopimuksen alkaessa ja päättyessä sekä monivaiheisen autentikoinnin käyttöönotto ovat tunnettuja tehtäviä IAM-järjestelmän keskittämisen lisäksi. Sen sijaan Zero Trust -ajattelun tuominen mukaan identiteetinhallinnan maailmaan ovat vähemmän tunnettuja kokonaisuuksia. Zero Trust -periaate perustuu lähtökohtaan, jossa keneenkään ei tule luottaa ja autentikointia tulee suorittaa jatkuvasti. Järjestelmien keskittämisellä taas tarkoitetaan nykyistä käyttäjien, sovellusten, tietokantojen ja portaalien monimuotoisuutta ja tämän kokonaisuuden hallintaan ehdotetaan yhtenä parhaana käytäntönä luoda keskitetty järjestelmä, jonka takana on kaikki organisaation identiteetit ja käyttövaltuudet. Tällä ratkaisulla organisaatio saa 360 asteen kuvan identiteettien turvallisuuteen ja nähdään, kenellä on pääsy ja mihin järjestelmiin pääsy on myönnetty. (SailPoint 2021.)

Soni (2020) listaa SailPoint (2021) lisäksi erityisten tilien tai käyttövaltuuksien välttämisen, vahvan salasanakäytännön sekä myös salasanattomuuden ja itsepalveluperiaatteet. Salasanattomuuden toteuttamisesta mainitaan sähköposti-, tekstiviesti-, biometriikkapohjainen kirjautuminen tai some-tilien hyödyntäminen kirjautumisessa. Itsepalvelussa viitataan työsopimuksen alkaessa

työntekijän itse käynnistämään identiteetin rekisteröintiin. Vahvan salasanakäytännön toteuttamisen suosittelee myös tiedonhallintalautakunnan (2021, 69) suosituskokoelma, jossa mainitaan, että politiikan tulisi olla pakotettu.

One Identity (s.a.) lähestyy parhaita käytäntöjä ensin sisäisten työntekijöiden ja ulkoisten työntekijöiden määrittämisellä ja erottamisella. Työntekijän organisaation tietämys helpottaa IAM-tehtävien toteuttamista, kun järjestelmä kasvaa käyttöönoton jälkeen. Identiteettien määrittelemisellä käytännössä tarkoitetaan yhtä tietokantaa, kuten LDAP-hakemistoa (Lightweight Directory Access Protocol), jossa kaikkien käyttäjien identiteetti on. Sähköposti- ja toiminnanohjausjärjestelmä (ERP) on myös mainittu, koska ne ovat keskeisiä organisaation toiminnan kannalta ja linkittyvät IAM-ratkaisuun vahvasti. Tavoitetilassa yhdellä ja samalla identiteetillä voitaisiin käyttää kaikkia järjestelmiä, mutta todellisuudessa, myös sähköposti ja ERP-järjestelmässä on omat sähköiset identiteetit ja ne mahdollisesti saadaan automaattisesti provisioitua IAM-ratkaisun avulla. (One Identity s.a.)

Yhtenä parhaana käytäntönä on tietouden ja kontrollien tuottaminen liiketoimintaomistajille. Tämän käytännön toteuttamiseen suositellaan itsepalvelupohjaista portaaliratkaisua, jossa ideana on, että liiketoimintaomistaja voi portaalista käydä tarkastamassa kuka pääsee hänen vastuullaan olevaan tietovarantoon tai järjestelmiin ja tarvittaessa muokata tai poistaa pääsy joltain työntekijältä. (One Identity s.a.)

Työnkulun toteuttaminen ja hallinnan automatisointi sekä katselmointi noudattaa samaa linjaa, mitä aikaisemmin mainituissa parhaissa käytännöissä on kerrottu. Yhtenä parhaana käytäntönä suositellaan luomaan mieluummin rooleja, kuin yksittäisiä käyttöoikeuksia. Roolien tulisi heijastua työtehtävistä ja tehtävänimikkeistä, joka on tehokas tapa hallita käyttövaltuuksia pitkässä juoksussa. Vaatimusten mukaisuudella viitataan lainsäädäntöön ja tietosuojaan ja siihen, miten IAM-ratkaisulla tulee määritellä selkeät työroolit, jotka saavat käsitellä henkilötietoja. (One Identity s.a.)

Katzin (2021) blogikirjoitus tiivistää identiteetin ja käyttövaltuushallinnan parhaat käytännöt vain viiteen kohtaan. Estä salaisuuksien, eli tunnuksen ja salasanan, vuotaminen kuulostaa itsestään selvältä asialta. Katz (2021) toteaa

kuitenkin, että niin tulee kuitenkin jossain vaiheessa tapahtumaan, vaikka käytössä olisi vahvimmatkin kontrollit tapahtuman estämiseen.

Kolmannen osapuolen työkaluja tulisi käyttää, mutta kuitenkin varoen. Ensinnäkin tulisi varmistua siitä, että kolmannen osapuolen työkalu IAM-hallinnassa on itsessään turvallinen. Monivaiheisen tunnistautumisen (MFA) ja kertakirjautumisen (SSO) käyttöä tulisi hyödyntää aina kuin mahdollista. Kertakirjautuminen helpottaa käyttäjien monitorointia huomattavasti, koska yhden tunnuksen takana on useampi järjestelmä ja sama identiteetti, mutta sillä on myös turvallisuusvaikutus, koska käyttäjän tarvitsee muistaa vain yksi tunnus ja salasana. (Katz 2021; Tiedonhallintalautakunta 2021, 69.)

Vähimpien oikeuksien periaatteen lisäksi kehotetaan valvomaan käyttäjien toimintaa suhteessa heidän käyttämiin resursseihin ja palveluihin ja niiden käyttöasteeseen. Ensimmäisenä mainintana nostetaan esiin myös lisenssien hallinta ja turhien lisenssien karsiminen, jolla voi olla taloudellisia vaikutuksia organisaatiossa. Jatkuvassa katselmoinnin ja vähimpien oikeuksien parhaassa käytännössä mainitaan esimerkki, että vaikka käyttäjällä on jossain vaiheessa tarve päästä järjestelmään, se ei tarkoita, että hänellä pitäisi olla koko ajan pääsy järjestelmään. Suosituksena on karsia oikeuksia, kun se on mahdollista, eikä häiritse ydintoimintaa tai heikennä tuottavuutta. (Katz 2021.)

Veritiksen (s.a.) kanssa yhtenevät parhaat käytännöt (kuva 4) ovat:

- Määrittele IAM-tavoitetila (SailPoint 2021).
- Tuota tietoutta omistajille (One Identity s.a.).
- Käytä rooleja (One Identity s.a.).
- Pakota MFA käyttöön (SailPoint 2021; Katz 2021; Soni 2020; Tiedonhallintalautakunta 2021, 69).
- Ota käyttöön SSO (Katz 2021; Tiedonhallintalautakunta 2021, 69).
- Noudata Zero Trust -periaatetta (SailPoint 2021; Soni 2020).
- Ota käyttöön vahva salasanapolitiikka (Soni 2020; Tiedonhallintalautakunta 2021, 69).
- Suojaa erityiset tilit (Soni 2020).
- Katselmoi käyttöoikeuksia säännöllisesti (SailPoint 2021; One Identity s.a.; Katz 2021).
- Ota käyttöön salasanaton kirjautuminen (Soni 2020).
- Noudata vähimpien oikeuksien periaatetta (Katz 2021).

Kuvassa 4 on esitelty 12 parasta IAM-käytäntöä (Veritis s.a), jotka ovat pääosin nostettu parhaiden käytäntöjen joukkoon SailPointin (2021), Sonin (2020), One Identityn (s.a.) tai Katzin (2021) julkaisemissa parhaissa käytännöissä.

Kuva 4. IAM-toteutuksen 12 parasta käytäntöä (Veritis. s.a.)

Parhaiden käytäntöjen joukossa on pääsynhallintaan liittyviä asioita, jotka nähdään IAM-toteutuksessa merkittäviksi. Tällaisia asioita ovat MFA:n tai SSO:n käyttöönotto.

7 IDENTITEETIN- JA KÄYTTÖVALTUUSHALLINNAN VAATIMUKSET

Käyttövaltuushallinnan tavoitteena on varmistua siitä, että tietoon pääsee käsiksi vain siihen oikeutetut henkilöt ja käyttäjätunnuksien elinkaaresta huolehditaan koko ajan säännöllisesti katselmoiden. Näin varmistutaan, että käyttäjillä on vain asianmukaisia voimassa olevia käyttövaltuuksia ja asiattomat käyttäjätunnukset poistetaan prosessin mukaisesti. (Ulkoministeriö 2020, 75.)

Hakalan ym. (2006, 4–5) mukaan tietoturvallisuus koostuu viidestä eri osatekijästä, joita ovat luottamuksellisuus, käytettävyys, eheys ja kiistämättömyys sekä pääsynvalvonta. Luottamuksellisuudella varmistetaan, että vain tietoon oikeutettu pääsee siihen käsiksi. Käytettävyydellä tai saatavuudella varmistetaan tiedon saatavuus aina kun sitä tarvitaan. Tiedon tulee olla eheää, eli paikkansa pitävää eikä se saa sisältää virheitä. Kiistämättömyydellä halutaan

varmistaa, että tiedon alkuperä on se, jonka sen kerrotaan olevan. Pääsynvalvonnan keinoiksi luetaan ICT-infrastruktuurin tekniset ja operatiiviset menetelmät. (Turunen 2018, 19.)

Nämä viisi tietoturvallisuuden perusmääritelmää ovat sidoksissa identiteetin- ja käyttövaltuushallinnan toteuttamiseen ja sitä kautta tietoturvallisuuteen. Luottamuksellisuus on yksi tärkeimmistä tietoturvan osatekijöistä, jotka linkittyvät identiteetin- ja käyttövaltuushallintaan, koska juuri IGA-ratkaisun avulla hallitaan käyttövaltuuksia ja sitä kautta varmistetaan, että vain oikeilla henkilöillä on oikeus oikeisiin tietoihin oikea-aikaisesti. Käytettävyyden yhteys IGA-ratkaisuun voidaan katsoa, esimerkiksi käyttäjälistan ylläpitämisen tai käyttöoikeuksien ajantasaisuuden tehtävien kautta. Käyttövaltuuksien muuttaminen hetkellä, jolloin nykyinen tieto oikeuksista ei ole saatavilla voi johtaa jopa myönnettyyn oikeuteen, jota ei saada kirjattua IAM-järjestelmään. Tämä voi johtaa hallitsemattomiin oikeuksiin. Säännöllisen katselmoinnin konstein pystytään hallitsemaan tähän liittyvää riskiä.

Eheyden merkitys käyttövaltuuksien tilaamisen prosessissa on ilmeinen. Käyttövaltuuksien määrämuotoinen tilaaminen tarkkaan määritellyllä lomakkeella on aina parempi tapa varmistaa kuka tilasi, milloin, minkä oikeuden, ja millä perusteilla, kuin että käyttäjä tekisi vapaamuotoisen tilauksen vajavaisilla tiedoilla. Kiistämättömyydellä ei ole suoranaista viitettä Identiteetin hallintaan tai käyttövaltuushallintaan, koska salausmenetelmät ja biometriikka on tässä vahvoja keinoja tunnistaa käyttäjä ja tehdä asia kiistämättömäksi. Tämä sisältö liittyy enemmän juuri pääsynhallintaan. (Hakala ym. 2006, Turusen 2018, 20 mukaan.)

Pääsynhallinnan osuus on osin rajattu tämän opinnäytetyön ulkopuolelle, mutta linkittyy kuitenkin vahvasti tietoturvallisuuteen. Pääsynhallinnan keinoin voidaan esimerkiksi teknisesti määritellä järjestelmään tietty mekanismi, jolla käyttäjä pääsee käyttämään sitä. Käyttövaltuushallinnan avulla pystytään mahdollistamaan määrämuotoinen tilaaminen tai rooliperusteinen automaattinen oikeus kyseiseen tietojärjestelmään. Yksinkertaisesti kuvattuna Järjestelmän pääsynhallinnassa voidaan määritellä tiettyyn rooliin AD-ryhmä, joka on määritelty käyttövaltuushallintaan automaattisesti provisioitavaksi käyttövaltuudeksi. Käyttäjän tilatessa IAM-järjestelmästä tämän oikeuden, hyväksytyn

tilauksen jälkeen hänelle provisioidaan käyttövaltuus automaattisesti ja käyttäjällä on pääsy järjestelmään. Pääsynhallinta aktivoituu siinä vaiheessa, kun käyttäjä kirjautuu järjestelmään ja hänen oikeutensa järjestelmän rooleihin tarkistetaan AD-tunnuksen ryhmäjäsenyyksistä.

Vastuuhenkilöiden nimeäminen

Tiedonhallintalaki (Laki julkisen hallinnon tiedonhallinnasta 16. §) ei mainitse mitään vastuuhenkilöiden nimeämisestä, mutta tiedonhallintalautakunta (2021, 67) edellyttää vastuuhenkilöiden nimeämistä käyttöoikeuksien hallintaan, kuitenkaan sen tarkemmin määrittelemättä tehtävän sisältöä.

Katakri nostaa toteutusesimerkin kautta, että järjestelmien käyttöoikeusien hallintaan on nimetty vastuuhenkilöt. Tämä suositus oli kaikista muista poiketen järjestelmäkohtainen vastuuhenkilö, eikä yleinen käyttövaltuushallinnan vastuuhenkilö. (Ulkoministeriö 2020, 76.)

Kuntaliiton (2013, 18) mukaan käyttövaltuuksien hallintaan tulee nimetä vastuuhenkilö tai vastuuhenkilöt. Vastuuhenkilö tulisi olla henkilöstöhallinnon nimeämä ja hänen tehtävänään tulisi olla työroolien ylläpitäminen, koska työroolit ovat keskeinen käyttövaltuushallinnan lähtökohta (Kuntaliitto 2013, 19).

Vahti-ohjeistus viittaa hyvään tiedonhallintatapaan ja sen edellyttämään vastuulliseen omistajaan. Omistajan tehtäviksi määritellään esimerkiksi käyttövaltuuksien määrittämiseen, hyväksyntään ja katselmointiin liittyvät tehtävät. (Valtiovarainministeriö 2006, 16.) Katakri kuitenkin toteaa, että käyttöoikeuksien hallintaan nimetyt vastuuhenkilöt riittävät, eikä sen tarvitse olla nimenomaisesti järjestelmän omistaja (Ulkoministeriö 2020, 76).

Vastuuhenkilön nimeämisestä voidaan edellisten perusteella päätellä että identiteetin- ja käyttövaltuushallinnan kokonaisuudelle tulee olla nimetty vastuuhenkilö ja tietojärjestelmille tulee nimetä vastuuhenkilö erikseen käyttöoikeuksien käsittelyyn, jos käyttöoikeuksien käsittely on hajautettu.

Prosessin kuvaaminen

Tiedonhallintalakiin (Laki julkisen hallinnon tiedonhallinnasta 16. §) nojaten, tiedonhallintalautakunta (2021, 67) edellyttää menettelyn kuvaamista käyttäjätilien hallintaan. Kuvauksessa tulee olla luonnin, hyväksymisen, ylläpidon ja poistamisen prosessi.

Katakri (Ulkoministeriö 2020, 76) jättää prosessin kuvaamisen hieman avoimeksi, mutta viittaa toteutusesimerkissä olemassa olevaan selkeään tapaan muutostilanteissa sekä kahden tai useamman henkilön (Two Man Rule) hyväksyntään, joka itsessään edellyttää toimintatavan kuvaamista. Toisaalta myös käyttöoikeuksien käsittelyn ja myöntämisen ohjeistus edellyttää jo prosessin kuvaamista. PiTukri (Kyberturvallisuuskeskus 2020b, 35) edellyttää täysin identtisiä toimenpiteitä.

ISO 27002 -standardissa edellytetään muodollista hallintaprosessia käyttäjien rekisteröintiin ja poistamiseen. Hallintaprosessin tulisi sisältää yksilöllisten tunnusten luomisen ohje sekä kuvaus miten jaettujen tunnusten käyttö tulee hyväksyttää ja dokumentoida. Lisäksi prosessin pitäisi kuvata tunnusten poistaminen tai jäädyttäminen. (SFS-EN 27002: 2017, 29.)

Kuntaliitto (2013, 5, 15–43) tarkastelee identiteetin- ja käyttövaltuushallinnan kokonaisuutta toiminnan näkökulmasta ja siinä ohjeistetaan kuvaamaan toimintamalli kokonaisuudessaan prosesseina. Vahti-ohjeen näkemys asiasta on samansuuntainen ja prosessikuvausten tulisi sisältää käyttövaltuuksien koko elinkaari ja prosessiin on kohdistettu myös turvallisuusvaatimus, joka pitää sisällään käyttövaltuuksien jäljittämiseen liittyvän vaatimuksen (Valtiovarainministeriö 2006, 16).

Ensinnäkin voidaan todeta, että prosessien kuvaaminen tulee tehdä. Prosessin kuvaamisen tehtäviksi voidaan katsoa seuraavat asiat:

- Käyttäjäidentiteettien luonti, hyväksyminen, ylläpito ja poistaminen koko elinkaari huomioiden.
- Tunnusten yksilöinnin menetelmä.
- Jaettujen tunnusten hyväksyminen ja dokumentointi.
- Ohjeista käyttäjät tunnusten henkilökohtaisuudesta.

- Kiellä tunnusten siirtäminen toiselle käyttäjälle.

Prosessikuvausten tulisi siis sisältää keskeisimmät työvaiheet sisäisten ja ulkoisten työntekijöiden kaikissa muutostilanteissa, joihin lukeutuvat koko työsuhteen elinkaaren aikaiset tapahtumat käyttäjätunnuksen luonnista sen poistoon.

Ohjeistuksen laatiminen

Ohjeistuksen laatimisen vaatimus perustuu tiedonhallintalakiin perustuvaan suosituskokoelmaan sekä Katakriin ja PiTuKriin. Kaikissa edellisissä todetaan, että käyttöoikeuksien käsittely ja myöntäminen on ohjeistettava. (Laki julkisen hallinnon tiedonhallinnasta 16. §; Tiedonhallintalautakunta 2021, 67; Ulkoministeriö 2020, 76; Kyberturvallisuuskeskus 2020b, 35.) Vahti-ohje edellyttää osana hallintaprosessien kuvaamista ajantasaisia ohjeistuksia (Valtiovarainministeriö 2006, 16).

Vähimpien oikeuksien periaate

Tiedonhallintalain mukaan käyttöoikeudet tulee perustua käyttäjän todellisiin käyttötarpeisiin. Suosituskokoelma tarkentaa tätä vaatimusta: työntekijälle saa antaa vain työtehtävien kannalta tarpeelliset tiedot, oikeudet tai valtuudet järjestelmiin vähimpien oikeuksien periaatetta noudattaen. (Laki julkisen hallinnon tiedonhallinnasta 16. §; Tiedonhallintalautakunta 2021, 67.)

Katakrissa viittaus vähimpiin oikeuksiin liittyy teknisemmin haittaohjelmiin liittyviin riskeihin, mutta myös tahallisiin ja tahattomiin tekoihin. Tarpeettoman laajat oikeudet antavat käyttäjälle, prosessille tai hyökkääjälle hyvät toimintaedellytykset väärinkäytöksiin. PiTuKri lähtee suoraan vaatimuksesta, että käyttöoikeuksien hallinta tulee toteuttaa vähimpien oikeuksien periaatteen mukaisesti. Taustalla on suojaukseen liittyvä tavoite, että käyttäjällä on pääsy vain välttämättömiin toimintoihin. (Ulkoministeriö 2020, 75; Kyberturvallisuuskeskus 2020b, 35.)

EU:n yleinen tietosuoja-asetus viittaa pääsääntöisesti vain luottamuksellisuuteen, joka itsessään tarkoittaa, että oikeilla henkilöillä on oikeus oikeisiin tietoihin oikea-aikaisesti. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 5 kohta 1 ja artikla 25 kohdat 1, 2). Tulee kuitenkin huomioida, että EU:n yleinen tietosuoja-asetus asettaa vaatimuksia vain henkilötietojen käsittelyyn.

ISO 27002 -standardissa käsitellään laajemmin tätä vaatimusta. Pääsyoikeuksien myöntämisen, verkkojen ja verkkopalvelujen sekä tietojen pääsyn rajoittamisessa viitataan pääsynhallintapolitiikkaan, jossa mainitaan hallintakeinona ja edellytyksenä, että kaikki tulisi olla lähtökohtaisesti kiellettyä, ellei sitä ole erikseen sallittu. Politiikassa kerrotaan myös kahdesta ohjaavasta periaatteesta: tarve tietää ja tarve käyttää, jotka ovat vain toisenlainen tapa ilmaista vähimpien oikeuksien periaatetta. (SFS-EN 27002: 2017, 27–29.)

Vähimpien oikeuksien periaate on yksi laajimmin mainittuja periaatteita tutkimuksen tuloksista. Myös Katz (2021) mainitsee vähimpien oikeuksien periaatteen noudattamisen parhaana käytäntönä. Tämän lisäksi kyberturvallisuuskeskuksen oppaassa tietomurtojen havaitsemiseen tietomurron estämisessä on mainittu käyttöoikeuksien hallinnasta, että peruskäyttäjillä ei tule olla ylläpito-oikeuksia. (Kyberturvallisuuskeskus 2020a.)

Apulaistietosuojavaltuutetun antaman huomautuksen mukaan POP Pankki rekisterinpitäjänä oli käyttänyt lomakejärjestelmää, jossa osalla henkilöstöstä on ollut tarpeettoman laajat pääsyoikeudet lomakkeiden sisältämiin tietoihin. Henkilöstöllä viitataan ulkoiseen tietojen käsittelijään eikä itse rekisterinpitäjään. Huomautuksessa viitataan EU:n yleiseen tietosuoja-asetukseen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 5, artikla 12, artikla 34 ja artikla 58). (Huomautus tietoturvaloukkauksesta ilmoittamisesta, kun rekisteröityjen yhteystiedot eivät ole rekisterinpitäjän tiedossa 3.1.2020.)

Yhteenvetona voidaan todeta, että käyttöoikeuksien rajaaminen tulee tehdä vähimpien oikeuksien periaatetta noudattaen, koska tarpeettoman laajat oikeudet mahdollistavat tarpeettoman laajat toimintamahdollisuudet mahdolliselle sisäiselle tai ulkoiselle hyökkääjälle. Tahallisten sekä tahattomien tekojen

riski pystytään minimoimaan noudattamalla asianmukaista käyttövaltuushallintaa ja tällä saavutetaan hyötyjä ja voidaan pienentää riskiä esimerkiksi haittaohjelmia vastaan (Ulkoministeriö 2020, 75–77, 83).

Tunnuksen vastuuhenkilö

Suosituskokoelmassa edellytetään, että jokaisella tunnuksella tulisi olla vastuuhenkilö, joka omistaa tunnuksen ja tietää sen käyttötarkoituksen (Tiedonhallintalautakunta 2021, 67). Muista vaatimuskehikoista ei vastaavaa mainintaa löydy, mutta periaate on hyvä ja sillä varmistutaan jokaisen tunnuksen tarpeellisuudesta ja pystytään rajaamaan sen käyttöoikeudet tarkasti.

Jaettujen tunnuksien välttäminen

Suosituskokoelma, joka perustuu tiedonhallintalakiin (Laki julkisen hallinnon tiedonhallinnasta 16. §), edellyttää yhteiskäyttötunnuksien käyttämiseen liittyen erikseen hyväksyttyä poikkeusmenettelyä (Tiedonhallintalautakunta 2021, 67).

Yksilöllisten sekä henkilökohtaisten tunnuksien käyttäminen kuvataan Katakrin toteutusesimerkissä, joka liittyy vaatimukseen, että tietojenkäsittely-ympäristöä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti (Ulkoministeriö 2020, 78). PiTuKrin käyttäjätunnistukseen liittyvässä vaatimuksessa todetaan, että käyttäjillä tulee olla yksilölliset henkilökohtaiset käyttäjätunnisteet (Kyberturvallisuuskeskus 2020b, 36).

ISO 27002 -standardin vaatimuksena luetellaan yksilölliset käyttäjätunnukset ja mainitaan, että vastuu voidaan yksilöllisesti kohdistaa henkilöön. Kuitenkin tätä seuraa maininta jaetuista käyttäjätunnuksista ja niiden sallimisesta. Salliminen edellyttää tällaisessa tilanteessa perusteltua liiketoiminnallista tai toiminnallista syytä. Lisäksi edellytetään erillistä hyväksyntämenettelyä sekä dokumentointia. Tämän lisäksi tunnistautumistietoihin, eli käyttäjätunnukseen ja salasanaan liittyen todetaan, että tunnukset ovat luottamuksellisia ja henkilökohtaisia sekä jaettujen tunnusten tiedot pidetään vain kyseistä palvelua käyttävän ryhmän tiedossa. (SFS-EN 27002: 2017, 29, 31.)

Johtopäätöksenä edellä kuvatuista vaatimuksista voidaan päätellä, seuraavaa:

- Jaettuja yhteiskäyttötunnuksia ei tulisi lähtökohtaisesti käyttää.
- Mikäli jaettuja tunnuksia kuitenkin on pakko käyttää, käytön tulee olla perusteltua.
- Käytön tulee sisältää erillinen hyväksyntäprosessi.
- Käyttö tulee dokumentoida ja tunnuksella tulee olla vastuuhenkilö.
- Ylläpitokäytössä olevia tunnuksia tulisi käsitellä erityisellä varovaisuudella.
- Käyttäjätunnusten salasanat tulisi vaihtaa säännöllisesti ja vähintään aina, kun ylläpitotehtäviä tekevä käyttäjä vaihtaa roolia tai lopettaa organisaatiossa.

Työssäni kokemani perusteella usein yhteiskäyttöisiä tunnuksia tavataan asiakaspalveluun tarkoitettujen ratkaisujen yhteydessä, jossa asiakkaalle on mahdollistettu kirjautuminen asiakaspäätteelle. Palvelutunnukset sekä ylläpitäjien root- ja admin-tunnukset ovat myös yhteiskäyttötunnuksia, joiden käsittelyssä ei usein ole huomioitu niihin kohdistuvaa ongelmaa. Näiden tunnusten dokumentaatiota ei usein ole olemassa ja vastuuhenkilö on myös määrittelemättä.

Käyttäjälistan ylläpitäminen

Tiedonhallintalakiin (Laki julkisen hallinnon tiedonhallinnasta 16. §) pohjautuvassa suosituskokoelmassa edellytetään käyttöoikeuksien ajantasaista tietoa, mutta erillisestä käyttäjälistauksesta ei varsinaisesti ole mainintaa (Tiedonhallintalautakunta 2021, 68). Käyttöoikeuksien tietoa on kuitenkin tarpeetonta ylläpitää ilman siihen liitettyä käyttäjäidentiteettiä.

Katakri sekä PiTuKri kummatkin edellyttävät vain käyttäjälistauksen olemassaoloa. (Ulkoministeriö 2020, 76; Kyberturvallisuuskeskus 2020b, 35.) Vaikka arviointityökalujen vaatimukset ovatkin vähäiset, on käyttäjälistan ylläpitäminen edellytys identiteetin- ja käyttövaltuushallinnan laadukkaaseen toteuttamiseen.

Oikeutuksen tarkastaminen

Käyttöoikeuksien myöntämisen yhteydessä pitää tarkistaa henkilön oikeutus sekä käyttäjän osaaminen tietojärjestelmän käyttämiseen. Työntekijän rekrytoinnin yhteydessä tulee myös varmistua työntekijän henkilöllisyydestä (Tiedonhallintalautakunta 2021, 68–69).

Katakrin ja PiTuKrin lähtökohtana on, että ilman vaitiolosopimusta ei käyttövaltuuksia anneta. Tämä lähtökohta pohjautuu työsuhteen aikaisiin muutosprosesseihin, kuten työsuhteen alkamiseen ja siihen liittyviin asioihin. Henkilöstön luotettavuuden arvioinnissa mainitaan keinoina henkilöllisyyden todentaminen, työhistorian varmentaminen sekä koulutustaustan tarkistus. Tehtävät ovat luonnollinen osa rekrytointiprosessia, mutta ulkoisilla työntekijöillä tai pilvipalvelun tarjoavalla toimittajalla ei vastaavaa rekrytointiprosessia ja sen tehtäviä toteuteta. Näin onkin syytä varmistaa, että ulkoisten työntekijöiden kanssa otetaan käyttöön salassapitomenettely ennen käyttöoikeuksien myöntämistä. Sopimuksessa tulee mainita mitkä tiedot ovat salassa pidettäviä, mitä ehtoja sopimukseen liittyy ja mitä toimia tehdään, kun sopimus päättyy. Lisäksi tietojen omistajuus, tietojen luovutus ja seuraamukset ehtojen rikkomisesta tulee kertoa. (Ulkoministeriö 2020, 17; Kyberturvallisuuskeskus 2020b, 25, 35.)

ISO 27002 -standardissa edellytetään edellisten tapaan henkilöllisyyden tarkastamista ennen käyttäjätunnuksien luovuttamista tai salasanan resetoinnin yhteydessä sekä ylläpito-oikeuksien kohdalla erityistä valtuutuksen prosessia, jossa käyttövaltuus voidaan myöntää vasta kun prosessi on suoritettu loppuun. (SFS-EN 27002: 2017, 30–31.)

Voidaankin siis todeta, että yksi merkittävä ennaltaehkäisevä toimintatapa on työsuhteen tai sopimussuhteen alkaessa solmia vaitiolosopimus ja varmistaa työntekijän henkilöllisyys. Tällä tavoin varmistutaan henkilön henkilöllisyydestä ja käydään läpi vaitiolosopimuksen sisältö ja sopimuksen päättyessä tehtävät toimet. Lisäksi joissain tapauksissa voi olla tarpeen edellyttää myös, että käyttäjän riittävä koulutus tai osaaminen tarkistetaan järjestelmän käyttöön.

Ulkoisten käyttäjien erottaminen

Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta edellyttää, että sisäiset ja ulkoiset käyttäjät tulee erotella pelkän käyttäjätunnuksen perusteella (Tiedonhallintalautakunta 2021, 68). Tämän perusteella on suositeltavaa käyttää esimerkiksi EXT-etuliitettä ulkoisten käyttäjien käyttäjätunnuksissa.

Käyttöoikeuksien ajantasaisuus

Tiedonhallintalaissa (Laki julkisen hallinnon tiedonhallinnasta 16. §) mainittu ajantasaisuus itsessään pitää sisällään jonkin rekisterin. Lakiin pohjautuvassa suosituskokoelmassa laajennetaan ja tarkennetaan vaatimusta. Jokaisesta järjestelmässä olevasta käyttöoikeudesta tulee olla ajantasainen tieto, joka käsittää myös oikeuksien muutokset (Tiedonhallintalautakunta 2021, 68).

Käyttöoikeuksien ajantasaisuus linkittyy tiukasti säännölliseen katselmointiin. Katakrin sekä PiTuKrin vaatimukset tältä osin ovat identtiset sisällöltään. (Ulkoministeriö 2020, 75–76; Kyberturvallisuuskeskus 2020b, 35.) ISO 27002 -standardissa, jossa kuvataan tietoturvallisuuden hallintakeinoja, käyttöoikeuksien ajantasaisuus linkittyy säännölliseen katselmointiin. Tämän lisäksi on kuitenkin kerrottu toteuttamisen tehtävinä käyttöoikeuksien välitön poistaminen, jos henkilö on vaihtanut roolia. Ylläpito-oikeuksien kohdalla luetellaan myös menettelyt, joilla käyttöoikeuksien vanheneminen määritellään. (SFS-EN 27002: 2017, 29, 31.)

Käyttövaltuushallinnan viitearkkitehtuurin valvonnan hallinnointiprosessin kautta kuvataan käyttöoikeuksien sekä valtuuksien ajantasaisuuden varmistaminen (Kuntaliitto 2013, 26.) Vahti-ohje mainitsee katselmoinnin keinona varmistaa, että käyttövaltuudet ovat ajantasaiset (Valtiovarainministeriö 2006, 21).

Käyttöoikeuksien ajantasaisuus on vahvasti yhteydessä säännölliseen katselmointiin ja sen toimenpiteisiin. Tehtäviksi edellisten perusteella voidaan määritellä, että perusteettomat käyttöoikeudet tulee poistaa ja erityisesti työntekijän roolin muuttuessa käyttöoikeudet tulee tarkistaa.

Muutosprosessin kuvaaminen

Tiedonhallintalain (Laki julkisen hallinnon tiedonhallinnasta 16. §) vaatima käyttöoikeuksien ajantasaisuus vaatii toimivan prosessin taustalle. Muutosprosessia edellytetään tiedonhallintalautakunnan (2021, 68–69) suosituskokoelmassa.

ISO 27002 -standardissa vaaditaan, että muutosprosessi kuvataan pääsyoikeuksien jakamisesta, muuttamisesta ja poistamisesta. Työsuhteen päättymisen yhteydessä tapahtuvaan käyttöoikeuksien poistamiseen vaikuttaa tapa, miten työntekijän työsuhde päättyy ja kenen aloitteesta. Huomioitava on, päättyykö työsuhde työntekijän vai työnantajan aloitteesta ja minkälaiseen tietoon työntekijällä on pääsy. Tietoturvariskinä mainitaan johdon aloitteesta päätetty työsuhde, jolloin työntekijä saattaa tahallaan sabotoida organisaation käytössä olevaa tietoa tai tehdä muita väärinkäytöksiä. Erityishuomio tulee kiinnittää ylläpito-oikeuksiin. (SFS-EN 27002: 2017, 29, 31–32).

Muutosprosessin sisällöstä voidaan edellisten vaatimusten kautta todeta seuraavaa:

- Kuvaa muutosprosessi, joka on selkeä.
- Muutosprosessin tulee sisältää käyttöoikeuksien muutostilanteet ja käyttöoikeuksien poistaminen.
- Työsuhteen päätösprosessi tulee kuvata käyttöoikeuksien näkökulmasta.
- Ylläpito-oikeuksien määrittäminen tulee kuvata tarkasti.
- Huomioi työsuhteen päätöksessä kenen aloitteesta työsuhde päättyy ja miten mahdollinen riski sabotoinnissa tai väärinkäytöksissä torjutaan.

Muutosprosessilla on yhteys prosessien kuvaamisen vaatimukseen. Siinä missä prosessien kuvaamisella tarkoitetaan enemmänkin identiteetin perustamista, muutosprosessi kuvaa myös käyttöoikeuksien myöntämiseen ja poistamiseen liittyvää toimintaa.

Säännöllinen katselmointi

Käyttöoikeudet tulee katselmoida säännöllisesti. Tähän tehtävään löytyy vaatimus tai suositus kaikista tutkituista vaatimuskehikoista. Tiedonhallintalaki edellyttää, että käyttöoikeudet tulee pitää ajantasaisina (Laki julkisen hallinnon tiedonhallinnasta 16. §). Tiedonhallintalautakunnan (2021, 68–69) suosituskokoelma edellyttää katselmointia ja vaatii sen dokumentoimista. Erityisesti tulee kiinnittää huomiota erityistä luotettavuutta edellyttäviin tehtäviin ja niihin liittyviin käyttövaltuuksiin. Aikamäärettä katselmoinnin toteuttamisen syklille ei kuitenkaan anneta.

Katakri ja PiTuKri noudattavat samaa linjaa keskenään. Kummassakin edellytetään katselmointia tehtäväksi esimerkiksi kuuden kuukauden välein sekä lisäksi työntekijän työsuhteen muuttuessa. Muutostilanteissa tulee olla selkeä prosessi käyttövaltuuksien uudelleen arviointiin. (Ulkoministeriö 2020, 75; Kyberturvallisuuskeskus 2020b, 35.)

EU:n yleisessä tietosuoja-asetuksessa katselmointiin liittyvät vaatimukset on kirjattu ylemmän tason vaatimuksina, eikä niinkään tarkkoina tehtävinä. Artiklan 5 mukaan henkilötietoja tulee käsitellä tavalla, jolla taataan tietojen eheys ja luottamuksellisuus. Artikla 24 rekisterinpitäjän vastuusta edellyttää, että rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet ja artikla 32:ssa viitataan edelleen luottamuksellisuuteen, eheyteen ja käytettävyyteen. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 5 kohta 1, artikla 24 kohta 1 ja artikla 32 kohta 1.)

ISO 27002 -standardin luvussa pääsyoikeuksien jakaminen edellytetään pääsyoikeuksien säännöllistä katselmointia. Pääsyoikeuksien uudelleenarvioinnin luvussa paikataan standardin muiden vaatimusten hallintakeinojen heikkouksia ja tarkennetaan, että katselmointi tulee tehdä työsuhteen muutostilanteissa ja erityisesti tarkastettava ylläpito-oikeudet tiheämmin kuin kuuden kuukauden välein. Ylläpito-oikeuksien hallinnoinnissa todetaan erikseen, että katselmoinnissa tulee selvittää ovatko työntekijät tehtäviensä tasalla. Ylläpito-oikeudet ovat vahvasti sidoksissa järjestelmän haavoittuvuuksiin ja häiriöihin. Tarkalla, kattavalla ja säännöllisellä katselmoinnilla on ennaltaehkäisevä vaikutus tietoturvauhkien syntymisessä. (SFS-EN 27002: 2017, 29–31.)

Käyttövaltuushallinnan viitearkkitehtuurissa valvonnalle on omistettu kokonainen luku, jossa kuvataan tarkemmalla tasolla katselmoinnissa huomioitavia tehtäviä. Vaatimuksina luetellaan mitä on muuttunut, koska on muuttunut, kuka on tehnyt muutoksen ja onko vaarallisia yhdistelmiä käytössä. (Kuntaliitto 2013, 26.)

Parhaissa käytännöissä myös SailPoint (2021), One Identity (s.a.) ja Katz (2021) suosittelevat tekemään säännöllistä katselmointia. Kähkönen (2020) mainitsee hyvin organisoidusta käyttövaltuushallinnosta, että sen tulee valvoa jatkuvasti sovittuja prosesseja ja käyttövaltuuksien ajantasaisuutta. Kähkönen (2020) toteaa lisäksi, että raportit ja säännölliset katselmoinnit ovat valvontavälineitä ja työroolien omistajat ovat velvollisia suorittamaan katselmointia.

Jatkuvalla valvonnalla varmistetaan määriteltyjen prosessien avulla hallinnoitujen käyttövaltuuksien hyvä ja organisoitu käyttövaltuushallinta. Valvontaa voidaan tehdä lokitietojen sekä järjestelmän käyttäjätietojen ja käyttövaltuuksien rekisterin perusteella. Valvontaa voidaan tehdä joko raportoimalla tai erillisiä katselmointeja toteuttamalla. Raportointi esitellään jatkuvan toiminnan välineeksi ja katselmointia, joka on myös työläämpi toteuttaa, esitetään kriittisempien järjestelmien valvonnan välineeksi ja toteutettavaksi vähintään vuosittain (Valtiovarainministeriö 2006, 21.) Valvonnan syklin osalta vaatimus on vanhentunut, koska Katakri sekä PiTuKri edellyttää katselmointiin kuuden kuukauden sykliä (Ulkoministeriö 2020, 75; Kyberturvallisuuskeskus 2020b, 35).

Katselmoinnin toteuttamisen tehtäviksi voidaan edeltävien perusteella todeta seuraavaa:

- Katselmoinnin järjestämisen vastuu kuuluu tiedon omistajalle.
- Katselmoi aina kun työsuhde muuttuu.
- Katselmoi aina kun työsuhde päättyy.
- Katselmoi kuuden kuukauden välein.
- Katselmoi ylläpito-oikeuksia useammin kuin kuuden kuukauden välein.
- Tarkastele erityisesti ylläpito-oikeuksia.
- Onko vaarallisia yhdistelmiä syntynyt.

Työtehtävieni kautta olen havainnut, että katselmointia ei usein suoriteta säännöllisesti ja katselmointitapahtumat syntyvät usein jonkin muun muutostarpeen

kautta, jolloin ne tulee samalla tehdyksi. Katselmointi vaatii myös paljon työaikaa, varsinkin ensimmäisen katselmoinnin tekeminen. Säännöllisyys yhdessä vakioitujen prossien kanssa keventää katselmoinnissa tarvittavaa työaikaa, koska poikkeamia ei juuri pitäisi päästä syntymään.

Vaaralliset yhdistelmät

Tiedonhallintalautakunnan (2021, 68) edellytykset käyttöoikeuksien hallinnalle määrittelee vaarallisten käyttöoikeusyhdistelmien tunnistamista sekä dokumentointia. Tällaiset käyttöoikeudet tulisi tunnistaa ja eriyttää mahdollisuuksien mukaan. Mikäli tehtäviä ei kyetä eriyttämään tulee vaarallisesta yhdistelmästä syntyvää riskiä hallita riskienhallintamenettelyllä.

Valvonnan toimenpiteinä käyttövaltuuksien katselmointiin liittyvänä toimenpiteenä luetellaan tehtävä, jossa vaaralliset yhdistelmät tulisi tunnistaa (Kuntaliitto 2013, 26; Kähkönen 2020). Identiteetinhallintapalvelun (IAM-järjestelmän) yhdeksi avuksi lasketaan juuri vaarallisten työyhdistelmien löytäminen (Kuntaliitto 2013, 55). Määräaikaisen työsuhteen yhteydessä luetellaan esimiehen tehtäväksi tunnistaa mahdolliset vaaralliset yhdistelmät (Kuntaliitto 2013, Liite 2, 6). Tämä kirjaus on puutteellinen, koska vastaavaa toimintoa ei edellytetä esimerkiksi normaalin työsuhteen alkaessa tai muissa muutostilanteissa. Lisäksi ohjeistus on vuodelta 2013 ja vaarallisten työyhdistelmien tunnistaminen kyetään nykyaikaisella identiteetin- ja käyttövaltuushallintajärjestelmän avulla tekemään automaattisesti ja ennalta ehkäisemään vaarallisen yhdistelmän syntyminen. Tämä luonnollisesti edellyttää vaarallisten yhdistelmien tunnistamista.

Vaarallisia käyttövaltuusyhdistelmiä ei saisi päästää syntymään, koska se on vahti-ohjeen mukaan riski, jota tulisi välttää työrooleja määritellessä. Kertaluonteinen käyttövaltuus on myös mahdollisuus pienentää riskiä kriittisten järjestelmien tai tietojen käytössä. Vaarallisten työroolien ja käyttövaltuusroolien tunnistaminen nostetaan esiin myös katselmointitehtävissä. (Valtiovarainministeriö 2006, 20–21.)

Pienessä organisaatiossa vaarallisen yhdistelmän ongelma on todellinen, koska tehtäviä ei ole välttämättä mahdollista eriyttää. Tällöin tästä syntyvää riskiä tulisikin hallita osana riskienhallintaa.

Korkeat riskiprofiilit

Tiedonhallintalautakunnan (2021, 11–12 ja 68) edellyttämällä tavalla korkeat riskiprofiilit eli erityiset oikeudet tulee huomioida omalla tilaus- ja poistoprosessilla. Erityisiin oikeuksiin lasketaan pääkäyttäjät, ylläpitäjät ja erityistä luotettavuutta edellyttävät tehtävät.

Standardissa korostetaan myös ylläpito-oikeuksien erillistä prosessia, kuten muutosprosessin kuvaamisessa on edellytetty. Katselmointiin viitaten ylläpito-oikeudet nostetaan säännönmukaisesti erityisasemaan ja niitä koskettaa erityiset toimenpiteet. (SFS-EN 27002: 2017, 30–31.)

Erityisiä oikeuksia tulisikin käsitellä aina erityisen tarkasti ja kaikissa tapauksissa arvioida oikeuksien tarpeellisuus suhteessa vaarallisiin yhdistelmiin ja riskienhallintaan.

Käyttöoikeuksien määritteleminen

Tiedonhallintalaissa (Laki julkisen hallinnon tiedonhallinnasta 16. §) sanotaan selkeästi, että viranomaisen on määriteltävä vastuullaan olevien tietojärjestelmien käyttöoikeudet. Katakrin vähimpien oikeuksien periaatteen ensimmäinen vaatimus lähtee siitä, että tietojärjestelmien käyttöoikeudet ovat määritelty (Ulkoministeriö 2020, 75). Tämän lisäksi myös Kuntaliitto (2013, 27) suosittaa käyttövaltuuksien määrittämistä. Käyttöoikeuksien määritteleminen on tietovarannon omistajan tehtävä. Määrittelytyössä tulee huomioida vahvan tunnistautumisen vaatimukset tai yleiseen pääsyyn liittyvät vaatimukset tietoverkon osalta. Käyttövaltuuksien määrittelyllä tarkoitetaan taas työroolien kytköstä käyttöoikeuksiin. (Valtiovarainministeriö 2006, 19–20.)

Pääsynhallintapolitiikka

Pääsynhallintapolitiikka on käytännössä kaiken identiteetin- ja käyttövaltuushallinnan keskiössä. Tiedonhallintalautakunta (2021, 68) suosittelee käyttöönottamaan käyttövaltuuksien hallintapolitiikan, joka perustuu riskienarviointiin. Politiikkaa luodessa tulee ottaa huomioon myös tietosuojalainsäädäntö, koska käyttövaltuuksien hallinta on itsessään henkilötietojen käsittelyä ja käyttövaltuuksien hallinta on lopulta yksi tärkeä toimenpide turvata henkilötietojen lainmukaista käsittelyä.

Standardin pääsynhallintaa käsittelevä kokonaisuus lähtee pääsynhallintapolitiikan luomisesta. Siinä ei pelkästään edellytetä politiikan laatimista vaan myös sen katselmointia sekä liiketoiminnallisten että tietoturvavaatimusten pohjalta. Turvallisuusvaatimusten lisäksi vaikuttava lainsäädäntö, vähimpien oikeuksien periaate, prosessit luomiseen, muutoksiin ja poistoon sekä valtuutuksiin tulisi kuvata. Politiikassa nostetaan erityishuomiona esiin, että lähtökohtana tulisi olla kaikkien oikeuksien kieltäminen ja salliminen vain tarpeeseen. Pääsynhallintaa ohjaavina periaatteina käytetäänkin usein tarve tietää, tarve käyttää -periaatetta. Myös roolipohjaisia käyttöoikeuksia suositaan, koska niillä voidaan helposti liittää työroolit käyttöoikeusrooleihin. (SFS-EN 27002: 2017, 27.)

Käyttövaltuuksien viitearkkitehtuurissa todetaan, että politiikkaa tulee luoda riskianalyysiin pohjautuen ja se on osa tietoturvapolitiikkaa (Kuntaliitto 2013, 21; Valtiovarainministeriö 2006, 16). Työroolien valtuuksien ylläpitäminen ja työroolien linkitys tietojärjestelmän käyttäjäryhmiin luetellaan käyttövaltuuksien hallintapolitiikan laatimisen tehtäviksi (Kuntaliitto 2013, 21, 27–28.)

Pääsynhallintapolitiikassa tulisi olla ainakin seuraavat asiat:

- Tietojärjestelmien vaatimukset riskiperusteisesti.
- Organisaatioon vaikuttava lainsäädäntö.
- Kaikkien hallintaprosessien kuvaukset.
- Hyväksymiseen liittyvät periaatteet.
- Ylläpito-oikeuksien käsittely.
- Vähimpien oikeuksien periaatteen mukainen toiminta.

Pääsynhallintapolitiikka tulisi luoda ensimmäisenä ja sen pitäisi kuulua osaksi tietoturvapolitiikkaa, koska ne ovat yhteydessä tietoturvan viiteen osa-alueeseen (luottamuksellisuus, käytettävyys, eheys, kiistämättömyys ja pääsynvalvonta).

Yksilölliset tunnukset

Yksilölliset ja muuttumattomat tunnukset ovat aukottoman lokivalvonnan perusta. Yksilöllisiä käyttäjätunnuksia edellytetään käytettäväksi sähköistä identiteettiä luodessa (Kyberturvallisuuskeskus 2020b, 35; SFS-EN 27002: 2017, 29; Kuntaliitto 2013, 34). Toteutustapaa yksilöllisten tunnusten toteuttamiseen ei kuitenkaan anneta, joten organisaation tehtäväksi jää itse määritellä millä tavalla tunnus yksilöidään. Työni kautta olen havainnut, että varsinkin lyhytaikaisia sijaisuuksia tekevien henkilöiden osalla yksilöllisen tunnuksen toteuttaminen on ollut haaste. Organisaation käytännön mukaisesti käyttäjätunnus voidaan luoda useampaan kertaan, koska tunnus poistetaan aina sijaisuusjakson jälkeen. Ainoaksi tunnisteeksi tunnuksessa määritelty nimi, ei ole riittävän yksilöivä ja AD-tunnuksen yksilöivät tiedot vaihtuvat joka kerta, kun tunnus poistetaan ja luodaan uudelleen. Aukottoman lokitiedon tarkasteleminen jälkikäteen tällaiseen käytäntöön perustuvalla tunnusten yksilöinnillä ei anna riittävää luotettavuutta tunnuksen käyttäjästä.

Roolien suosiminen

Roolien käyttäminen käsitellään suosituskokoelmassa poikkeuksellisesti luvussa elinkaaren huomioiminen tietojen käsittelyssä, joka kuuluu tiedonhallintalain 13. § vaatimukseen. Tietoaineistojen ja tietojärjestelmien tietoturvallisuuden pykälässä käsitellään tietojen käsittelyn turvallisuutta koko järjestelmän elinkaari huomioiden. Suosituksissa todetaan, että tietoaineistojen luvallisen käytön toteuttaminen tehdään henkilöiden työtehtäviin perustuvalla roolipohjaisella käyttöoikeuksien ja -valtuuksien hallinnalla. (Tiedonhallintalautakunta 2021, 13, 16.)

Standardi (SFS-EN 27002: 2017, 30) suosittaa harkitsemaan pääsyrooleja, koska käyttöoikeuksien hallinnointia on huomattavasti helpompi toteuttaa roo-

lien kuin yksittäisten oikeuksien kautta. Roolien määrää tulee tarkastella kriittisesti, sillä roolitus saattaa helposti paisua liian suureksi ja tekee hallinnoinnin jopa mahdottomaksi (Kuntaliitto 2013, 15–16, 19, 24–25).

Vahti-ohjeen mukainen roolien määrittely lähestyy asiaa käytännönläheisesti. Käyttäjien valtuuksia määriteltäessä tulisi pyrkiä eroon yksilötasosta ja suosia käyttäjäryhmiä. Konkreettisena esimerkkinä nostetaan esiin, että samaa tehtävää tekevillä työntekijöillä on samanlaiset tietotarpeet ja siten samanlainen työrooli. (Valtiovarainministeriö 2006, 17–18.) Tämä määritys on kuitenkin ristiriidassa vähimpien oikeuksien periaatteen kanssa.

Rooliperustainen käyttöoikeusmalli (Role Based Access Control, RBAC) on 2004 julkaistu standardiksi. Roolipohjaisen mallin vahvuutena on, että se on joustava ja ehkäisee vaarallisten työyhdistelmien syntymistä. (Sandhu ym. 1995, Kähkösen 2020, 19–20 mukaan.) Myös One Identity (s.a.) suosittelee parhaana käytäntöä käyttämään roolipohjaista käyttöoikeushallintaa, joten tästä voi todeta seuraavaa: roolien käyttämistä tulee suosia, roolit tulee kiinnittää työtehtävään tai tehtävänimikkeeseen, kiinnitä huomiota roolien rajalliseen määrään ja katselmoi roolit säännöllisesti.

8 TIETOTURVALLISUUSVAIKUTUKSET

Tietoturvan parantuminen mainitaan ensimmäisenä asiana IAM-järjestelmän hyödyissä. Käyttäjien käyttövaltuushallinta mahdollistaa organisaation paremman hallinnan ja ennaltaehkäisee identiteettivarkauksia ja luvatonta pääsyä arkaluonteisiin tietoihin. IAM-järjestelmän avulla on mahdollista suojautua hakkerointia, haittaohjelmia, kalastelua tai muunlaisia kyberhyökkäyksiä vastaan. (Rosencrance 2020.)

Ransomware

Ransomware on eräänlainen haitallinen hyökkäys, jossa organisaation tiedot salataan ja niiden vapauttamiseksi vaaditaan lunnaita. Ransomwareen liittyy myös tietojen varastaminen ja maksun vaatiminen siitä, että tietoja ei julkaista. (Barker ym. 2021, 1; Enisa 2021, 34.) Ransomware on voimakkaasti nousussa oleva haittaohjelman muoto. (Enisa 2021, 34.)

Suosituksena ransomware-uhkan mitigointiin Enisa (2021, 43) esittää toistakymmentä toimenpidettä, joista kolme liittyy identiteetin- ja käyttövaltuushallinnon kokonaisuuteen. IAM-järjestelmän käyttöönotto ja sen auditoiminen sisältäen vähimpien oikeuksien periaatteen ja vaarallisten yhdistelmien välttämisen. Käyttöoikeuksien ja -valtuuksien hallintaa tulisi tehdä vähimpien oikeuksien ja tehtävien erottamisen (Separation of Duties) periaatteiden mukaisesti. Luotettujen laitteiden, prosessien ja käyttäjien identiteettejä tulee hallita ja ne tulee tarkistaa. (Enisa 2021,43.)

Malware

Malware, eli haittaohjelma, on eräänlainen kattotermi luvattoman ja haitallisen koodin suorittamiseen, jolla on tarkoituksena aiheuttaa vahinkoa järjestelmän eheyteen, luottamuksellisuuteen tai saatavuuteen. Esimerkkejä malwaresta ovat muun muassa virukset tai troijalaiset. (Enisa 2021, 46.)

PiTuKri (Kyberturvallisuuskeskus 2020b, 3,42) käsittelee haittaohjelmasuojausta pilvipalvelujen osalta ja esittää, että haittaohjelmiin kohdistuvia riskejä voidaan pienentää myös käyttöoikeuksien rajauksilla. Myös Optimal IdM (s.a.) esittää IAM-järjestelmän etuna malwaren leviämisen estämisen. Enisa (2021, 49) ei nosta kuitenkaan yhtään suositeltua toimenpidettä malwaren mitigointiin, joka liittyisi identiteetin tai käyttöoikeuksien hallintaan.

Sähköpostiin liittyvät uhat

Tietojen kalastelu (phishing) on yksi verkkourkinnan tapa, jolla pyritään varastamaan sähköpostin kautta käyttäjän tärkeitä tietoja, kuten salasanoja tai luottokorttitietoja. Tietojen kalasteluun kuuluu myös hienostuneimpia muotoja, kuten keihäskalastelu (spear-phishing) ja valaanpyynti (whaling). Keihäskalastelu on suunnattu tietyille organisaatioille tai henkilöille, kun taas valaanpyynnillä pyritään saamaan kohteeksi mahdollisimman korkeassa asemassa oleva henkilö. (Enisa 2021, 56.)

Suositustoimenpiteitä sähköpostiin liittyviin uhkiin Enisa (2021, 58) mainitsee MFA:n käyttöönoton sekä tarve tietää -periaatteen käyttämisen. Mitä pienempi

pääsy käyttäjällä on tietoihin, sitä vähemmän tietoja voi varastaa tietojen kalastelulla. Myös pääsynhallintaan liittyvä vaatimus mahdollisimman vahvasta salasanasta esitetään ennaltaehkäisevänä keinona.

Tietoon kohdistuvat uhat

Tietoon kohdistuva uhka koostuu pääasiassa tietomurroista tai tietovuodoista, joissa kyse on arkaluonteisen tai luottamuksellisen tiedon luovuttamisesta epäluotettavalle taholle. Tavoitteena on saada luvaton pääsy, paljastaa tietoa, jakaa puutteellista tai väärää tietoa (misinformaatio) tai tietoisesti levittää väärää tietoa (disinformaatio). Tietomurto voi tapahtua sisäpiirissä olevan henkilön toimesta, kyberhyökkäyksen seurauksena tai tahattomasta tietojen katoamisesta. (Enisa 2021, 61.)

Enisa (2021, 64–65) on maininnut vähimpien oikeuksien periaatteen suositustoimenpiteenä tietoon kohdistuvien uhkien ehkäisemiseksi. Käyttöoikeudet tulee poistaa henkilöiltä, jotka eivät ole työntekijöitä. Suositus perustuu UC Berkeley (s.a.) julkaisemaan tarvitsee tietää -pääsynhallinnan ohjeeseen. Enisa (2021, 65) suosittelee lisäksi käyttöönottamaan MFA ja SSO sekä käyttämään vahvoja salasanoja.

Toimintatapaan liittyvät uhat

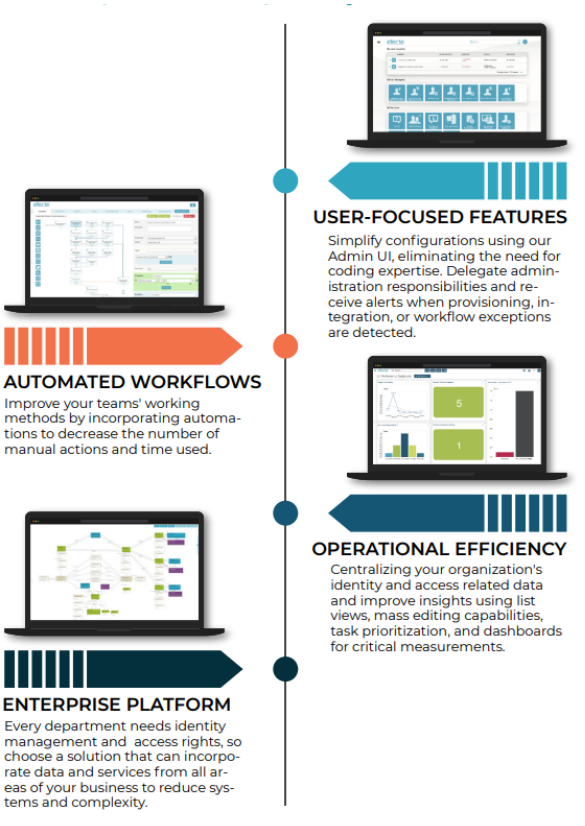
Kokonaan erilaisen uhan nostaa esiin Käck (2019), joka mainitsee, että käyttövaltuuksien haltuunotto on projekti ja toimintatapojen muutos tulee huomioida tai muuten uhkana on varjokulttuuri, joka rikkoo esimerkiksi pääsynhallintapolitiikan sääntöjä korotettujen käyttöoikeuksien käyttämisestä. Käckin (2019) keskeinen teema on, että ylläpitäjäkin on vain ihminen ja ihminen on laiska. Tietoturvakontrollien keskeinen teema on kiistämättömyyden todentaminen. Mikäli ylläpitäjä ei muuta toimintatapojaan ja käytä hänelle annettuja henkilökohtaisia käyttäjätunnuksia, vaan käyttää edelleen yhteiskäyttöisiä ylläpitotunnuksia, kiistämättömyyden todentaminen on huomattavasti vaikeampaa. Tämän lisäksi yhteiskäyttöisen tunnuksen käyttäminen lisää hyökkäyspinta-alaa. (Käck 2019.)

9 KEHITTÄMISPROJEKTI

Kehittämisprojektin tarkoituksena oli katselmoida IGA-järjestelmän käyttöönoton jälkeistä toteutusta identiteetin- ja käyttövaltuushallinnan vaatimuksia vasten. IGA-käyttöönottoprojektin jälkeisestä tilanteesta odotettiin löydettävän selkeitä havaintoja asioista, jotka ovat kunnossa ja asioista, jotka ovat puutteellisia. Osa löydöksistä oli osittain kunnossa, mutta edellyttää kehittämistä

9.1 Efecte IGA

IGA tulee englanninkielisistä sanoista Identity Governance and Administration, joka tarkoittaa identiteettien hallinnointia. IGA-järjestelmä on suomaisen ohjelmistoyhtiön, Efecte Oy:n, 2019 julkaisema tuote ja sillä voidaan hallinnoida Identiteettejä ja käyttövaltuuspyyntöjä itsepalveluportaalin kautta sekä automatisoimalla prosesseja. IGA voidaan liittää esimerkiksi osaksi uuden henkilön perehdytysprosessia, jossa se toimii automaattisesti prosessiin syötettyjen tietojen pohjalta. IGA-järjestelmällä voidaan varmistua siitä, että oikealla henkilöllä on oikeat oikeudet perustelluista syistä oikea-aikaisesti. Kuvassa 5 on esitetty pähkinänkuoressa IGA-järjestelmän toiminnallisuudet. (Efecte 2019).



Kuva 5. Efecte IGA factsheet (Efecte 2021)

Sipoon kunnalle Efecten IGA-järjestelmä valittiin, koska kunnassa oli jo aiemmin laajassa käytössä Efecten ITSM-järjestelmä (IT Service Management, eli IT palvelunhallinta) ja järjestelmän laajentaminen oli kustannustehokasta. Seuraavassa luvussa käsittelyt havainnut liittyvät osin IGA-järjestelmään ja siihen tehtäviin kehityskohteisiin.

9.2 Vaatimusten ja tehtävien havainnot

Jokainen vaatimus tai tehtävä on arvioitu objektiivisesti Sipoon kunnan nykytilannetta vasten ja tehty johtopäätöksenä jako kolmeen luokkaan: kehittämistä vaativat asiat, tarkennusta vaativat asiat ja vaatimusten mukaiset asiat.

Kehittämistä vaativat asiat

Opinnäytetyön tekijä oli nimetty IGA-järjestelmän vastaavaksi henkilöksi, mutta tutkimuksen tuloksena vastuuhenkilön nimittämisellä tarkoitetaan kuitenkin laajempaa vastuuta, joka ulottuu käytännössä kaikkeen käyttöoikeusmäärittelyyn ja provisiointitehtäviin (Ulkoministeriö 2020, 76). Vaikka IGA on määritelty Sipoon kunnassa identiteetin- ja käyttövaltuushallinnan järjestelmäksi, tehdään identiteettien ja käyttöoikeuksien provisiointityötä monessa järjestelmässä manuaalisesti ja tässä onkin yksi parannuskohde. Kaikkien tietojärjestelmien käyttöoikeuksista vastaavat henkilöt tulee nimetä.

Opinnäytetyön tutkimuksen mukaan, pääsynhallintapolitiikka on yksi peruselementti identiteetin- ja pääsynhallinnan toteutuksessa. Politiikan kautta luodaan perusta, jolla käyttövaltuushallintaa toteutetaan. Politiikka antaa myös selkeät rajaukset käyttövaltuuksien luomiseen, muutoksiin, poistamiseen sekä valtuutuksiin tai hyväksymisiin. Ilman asianmukaista politiikkaa käyttövaltuushallinnan toteuttaminen ei ole määrämuotoista. IGA-toteutusprojektissa ei luotu lainkaan tämän opinnäytetyön tutkimuksen tulosten mukaista pääsynhallintapolitiikkaa käyttövaltuushallinnan toteuttamiselle, mutta perusteet tunnusten luomiseen, yksilöintiin ja roolien määrittämiseen oli kuitenkin määritelty IGA-järjestelmään. Selkeänä parannuskohteena onkin pääsynhallintapolitiikan luominen.

IGA-toteutuksen aikana otettiin vahva näkökulma käyttöoikeuksien määrittelemiseen. Tämän opinnäytetyön toteutuksen ulkopuolella oli pääsynhallinta ja esimerkiksi kohdejärjestelmien käyttöoikeusmääritykset. Käyttöoikeuksien määrittämistä oli paikoin kuitenkin pakko tehdä, jotta käyttövaltuushallinnan määrittelyt olisivat vaatimusten mukaisesti toteutettu tarkasti ja yksityiskohtaisesti. AD-ryhmiin perustuvia käyttöoikeuksia määriteltiin uudestaan, jotta varmistuttiin kyseisen ryhmän antavan vain sen oikeuden, joka ryhmän nimen ja kuvauksen mukaan oli tarkoitettu. Tämän toteutuksen ulkopuolelle jäi kuitenkin kohdejärjestelmien käyttöoikeuksien määritys ja se on myös sidoksissa edelliseen ohjeistamisesta löydettyyn virheeseen. Tämä asia on selkeästi puute, johon tulee kiinnittää huomiota. Erillisten tietojärjestelmien käyttöoikeusmäärittelyt ja valtuutukset ovat hajautettu useille tekijöille, joilla ei ole ohjeistusta tai se ei vastaa pääsynhallintapolitiikan vaatimuksia, koska pääsynhallintapolitiikkaa ei ole laadittu.

Jaettujen tunnusten käyttäminen oli tavallinen käytäntö lyhyttä sijaisuutta tekevien opettajien tai sairaanhoitajien kesken. Tämä käytäntö lopetettiin jo IGA-toteutusprojektin aikana, mutta nyt tutkitun tiedon valossa myös perusteet ja vaatimukset ovat myös selvät ja toiminta tältä osin on täysin lainmukaista. Tarkemmassa tietojärjestelmien käyttöoikeustarkastelussa havaittiin, että osassa kriittisiäkin järjestelmiä oli ollut ylläpidolle jaettuja tunnuksia, jolloin tunnuksen käyttäjän yksilöiminen oli huomattavasti hankalampaa kuin, että tunnus olisi henkilökohtainen. Niin sanotun root- tai admin-tunnuksen poistaminen ei ollut aina mahdollista, mutta niiden salasana tulisi vaihtaa ja dokumentoida tunnus sekä rajata pääsy tunnukseen tiukasti. Kaikkia tällaisia tunnuksia ei ole kuitenkaan dokumentoitu, joten vaatimuksen mukaiseen tilaan pääseminen edellyttää kaikkien ylläpitotunnuksien dokumentointia ja niiden käyttäjien määrittämistä sekä salasanojen vaihtamista.

Yhtenä suurimpana löydöksenä toteutusprojektin puutteissa havaittiin toimintaprosessien tai muutosprosessin kuvaamisen puuttuminen. Projektissa tekemisen fokus oli pitkälti teknisessä ympäristössä ja sen toimintakuntoon saattamisessa ja käyttäjälähtöinen toimintaprosessi, varsinkin muutostilanteissa jäi tekemättä. Työntekijän rekrytointiin liittyvät toimet ovat toki henkilöstöosaston toimialaa ja kuvattu miten ne tehdään ja pelkästään sitä prosessia noudattamalla, työntekijälle syntyy palkkajärjestelmään sähköinen identiteetti ja sitä

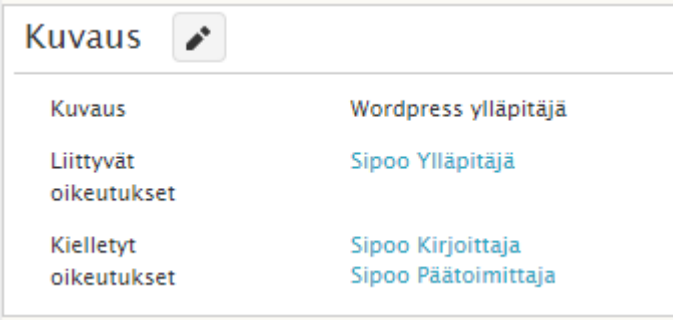
kautta työsuhteen alkaessa hänelle luodaan automaattisesti tunnus. Voisi ajatella, että onko erilliselle prosessin kuvaamiselle lainkaan tarvetta, koska se on niin vahvasti HR-lähtöinen. Tällöin kuitenkin käyttövaltuuksiin, rooleihin ja kolmansien osapuolien (tietojärjestelmien pääkäyttäjien) toteuttamaan käyttöoikeuksien määrittämisiin ei tule tällöin kiinnitettyä huomiota.

Esimerkiksi henkilöllisyyden tarkastamisen ja vaitiolosopimuksen hyväksymisen voisi olettaa olevan normaali osa prosessia rekrytointivaiheessa, mutta ilman, että tätä on kuvattu, prosessissa on vaikea osoittaa, että käyttövaltuushallintaa tehdään EU:n yleisen tietosuoja-asetuksen (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679) mukaisesti. Kokonaan vieras käytäntö on myös tarkistaa osaaminen ennen käyttöoikeuden antamista. Tämä voi olla perustelua varsinkin erityisissä korkeamman riskin profiileissa, kuten ylläpito-oikeuksissa. Toimintaprosessien kuvaaminen ja oikeutuksen tarkastamiseen liittyvät havainnot tulee organisaatiossa käsitellä ja huolehtia niiden osalta.

Käyttöoikeuksien ajantasaisuus sekä säännöllinen katselmointi on tutkimuksen mukaan erittäin tärkeä osa käyttövaltuushallintaa. Kaikissa tutkituissa viitekehyksissä oli vaatimuksia säännölliseen katselmointiin, joka avulla varmistutaan, että käyttöoikeudet ovat ajantasaiset. Teknisenä puutteena automaattisessa käyttövaltuushallinnassa oli toteutusprojektissa ulos rajattu käyttöoikeuksien poistamisen prosessi käyttövaltuuden määräajan päättyessä. Asiaa on pystytty kunnassa kuitenkin hallitsemaan henkilötietojen käsittelyohjeella, jossa todetaan, että käyttöoikeudet tulee poistaa, ellei niiden säilyttämiselle ole perustetta (Henkilötietojen käsittelyohje s.a.). Kirjaus on mielestäni puutteellinen, koska se koskettaa vain tietojärjestelmiä, joissa käsitellään henkilötietoja ja ohjeessa ei edellytetä säännöllistä katselmointia. Tässä asiassa on kunnalla tunnistettu kehittämistarve.

Käyttöoikeuksien tilauslomakkeelle (liite 1) rakennettiin pakollinen kenttä käyttöoikeuden voimassaolosta, jossa pisin arvo on 12 kuukautta. Tätä vasten ei kuitenkaan ole käytössä prosessia, jolla käyttövaltuudet uudelleen arvioidaan tai poistetaan. Nykymuodossaan tällaisen uudelleenarvioinnin toteuttaminen olisi äärimmäisen työllistävä, koska yksittäisiä käyttöoikeuskortteja on järjestelmään kirjattu jo yli 13 000 kappaletta.

Toteutusprojektissa huomioitiin valmius vaarallisten yhdistelmien määrittelemiseen, mutta vaarallisten yhdistelmien tunnistamista ei toteutettu. Myös teknisen käyttöönotto käyttöoikeuksien tilausprosessissa tai palkanmaksujärjestelmän tietojen mukaisessa automaattisessa tunnusten luonnissa on toteuttamatta. Tutkimuksen mukaan tiedonhallintalaki (Laki julkisen hallinnon tiedonhallinnasta 16. §) yhdessä tiedonhallintalautakunnan (2021) suosituskokoelman kanssa edellyttää vaarallisten yhdistelmien tunnistamista. Tästä huolimatta toteutusprojektin aikana ei tunnistettu tämän asian tärkeyttä identiteetin- ja käyttövaltuushallinnan toteuttamisessa. Kuvassa 6 on esitetty yksinkertaisen esimerkin kautta, miten vaarallinen yhdistelmä voidaan kuvata IGA-järjestelmään. Konfiguraatioon määritellään yksi liittyvä oikeus, ja vastaavasti sille kielletyt oikeudet, joita käyttäjällä ei saa olla samanaikaisesti. Teknisessä toteutuksessa tulee kuitenkin huomioida, että tämä määritys ei saa olla aina estävä, vaan poikkeuksia pitää kyetä hallitsemaan riskienhallinnan keinoin, kuten tiedonhallintalautakunta (2021, 68) on ohjeistanut.



Kuva 6. Vaarallinen yhdistelmä järjestelmässä konfiguroituna

Käytännönläheisenä esimerkkinä tällaisesta yhdistelmästä on ostolaskujen käsittelyjärjestelmässä laskun tarkastajan ja hyväksyjän rooli. Käyttövaltuushallinnan näkökulmasta työntekijällä voisi olla vain toinen rooleista. Perustyöntekijä ei saa koskaan hyväksyjän roolia, mutta kustannuspaikan vastaava, yleensä esihenkilö, saa hyväksyjän roolin. Hyväksyjän roolilla on kuitenkin mahdollista tehdä myös ostolaskujen tarkastamista. Tässä kohtaa käyttövaltuushallinta ei enää olekaan IAM-järjestelmän vaikutuspiirissä, vaan kohdejärjestelmän käyttöoikeusmäärittelyssä tulee tehdä tarkempi määrittely ja säännöt vaarallisen yhdistelmän estämiseksi. Esihenkilön tarkastama lasku tulisi ohjata organisaatiossa ylemmälle johdolle hyväksyttäväksi. Käyttöoikeuksien määritteleminen ei ollut tämän opinnäytetyön piirissä, joten se rajattiin pois.

Tarkennusta vaativat asiat

Teknisen ohjeistuksen osalta keskityttiin huolehtimaan, että IT-palvelujen tukihenkilöstö on riittävän hyvin ohjeistettu ja koulutettu uuden automaattisen identiteetin- ja käyttövaltuushallinnan käyttämiseen. Olennainen muutos työssä oli se, että ennen muutosprojektia AD:ssa voitiin tehdä paljon toimenpiteitä käyttäjätunnuksille ja ryhmäjäsenyyksille, mutta automaattisen tunnushallinnan käyttöönoton jälkeen näin ei voitu enää menetellä. Kaikki muutokset AD:lla eivät välittyneet IGA:n tietoon ja varsinkin käyttäjäryhmien liittäminen käyttäjätunnukselle kiellettiin.

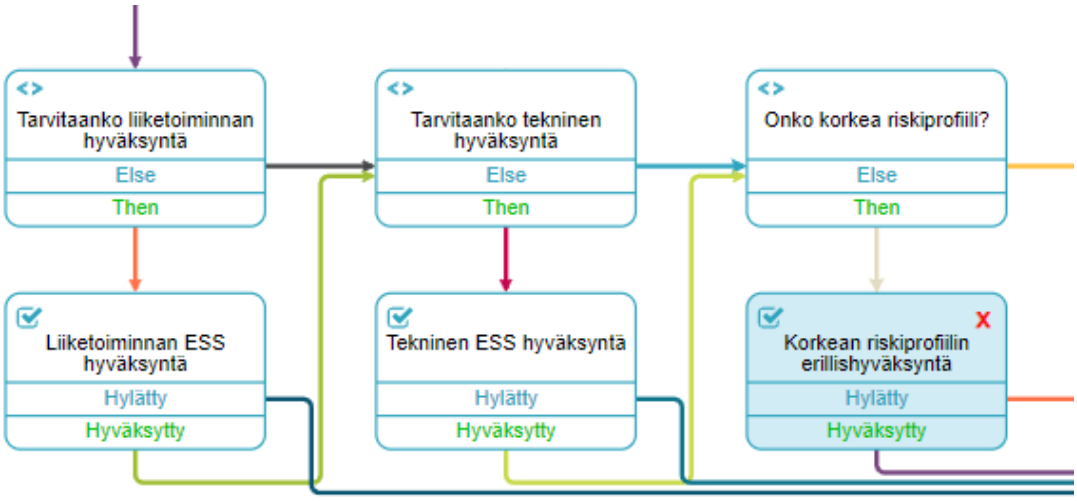
Käyttäjille ohjeistusta tehtiin hyvin minimaalisesti, koska vaikutus loppukäyttäjään oli viimekädessä hyvin pientä. Sen sijaan hyväksyntäroolia tekevien henkilöiden ohjeistus jätettiin huomiotta. Tämä oli nyt tutkitun tiedon valossa ollut väärä päätös ja hyväksyntäroolia tekevät henkilöt tulee ohjeistaa tarkasti hyväksyntärooliin liittyvistä asioista. Erityistä ongelmaa oli aiheuttanut IGA-järjestelmään konfiguroitu roolimuutoksen työnkulku, jossa työntekijän tehtävänimikkeen tai yksikön vaihtuessa, häneltä poistetaan kaikki käyttöoikeudet ja määritellään tilalle vain uuden työroolin mukaiset perusoikeudet. Toimintamalli on ISO 27002 -standardin (SFS-EN 27002: 2017, 29, 31–32) mukainen, mutta on käytännössä osoittautunut ongelmaksi manuaalista provisiointia vaativissa käyttövaltuuksissa, jossa hyväksyjä tai käyttöoikeuden toteuttaja ei ollut ymmärtänyt miksi näin menetellään.

Tunnuksen vastuuhenkilön määrittäminen jaetuille tunnuksille ja palvelutunnuksille ei ollut tapana ja tulee ottaa käytännöksi. Vastuuhenkilö pystytään määrittelemään IGA-järjestelmään tunnuskohtaisesti yhdessä tunnuksen käyttötarkoituksen kanssa. Henkilökohtaisten tunnuksien vastuuhenkilö oli ikään kuin sisäänrakennettuna oletusarvoisena tapana toimia, koska tunnuksen omistava henkilö on luonnollisesti myös vastuuhenkilö ja lisäksi hänelle on määritelty esihenkilö, joka tarpeen vaatiessa pystyy ottamaan kantaa tunnuksen elinkaareen. Ulkoisten käyttäjien tunnustilauslomakkeessa lähdettiin edellyttämään aina vastuuhenkilöä (liite 2 ja liite 3), vastuuhenkilö kirjattiin aina tunnuksen esimiestietoon AD-tunnuksessa. Tunnusten tilaamisen oikeus oli myös rajattu esihenkilöihin tai esimerkiksi koulusihteereihin. Uusi toimintatapa

jaettujen ja palvelutunnusten osalta täyttää käytännössä tiedonhallintalain vaatimukset (Tiedonhallintalautakunta 2021, 67).

Korkeiden riskiprofiilien suhteen kunnassa ei ollut tehty vaatimusten mukaista määrittelyä ennen automaattisen tunnushallinnan käyttöönottoa. IGA-käyttöönottoprojektin aikana ei myöskään tunnistettu erillistä tarvetta tehdä määrittelyä erityisoikeuksista. Pääosin korkean riskiprofiilin oikeudet määriteltiin suoraan nykyisten tehtävää tekevien henkilöiden hyväksynnän taakse. Tiedonhallintalautakunnan (2021, 68) mukaan korkeiden riskiprofiilien määritys tulee tehdä erillisenä prosessina ja päätös oikeuden saamisesta tulee huomioida. Tältä osin nykyinen tilaus- ja hyväksyntä prosessi edellyttää muutosta.

Nykyisessä toteutuksessa yksittäistä käyttöoikeutta voi tilata henkilö itse, esihenkilö tai vastuuhenkilö. Lomakkeiden toiminta on rajattu niin, että millään lomakkeella et voi tilata oikeutta itsellesi ilman hyväksyntää. Työntekijän tilaus menee aina vähintään esihenkilön hyväksyttäväksi ja siitä käyttöoikeudelle mahdollisesti määriteltyihin liiketoiminta- ja tekniseen hyväksyntään. Nykyisellä toteutuksella on mahdollistettu jopa kolmiportainen hyväksyntä. Korkeat riskiprofiilit voidaan, joko pakottaa käyttämään aina teknistä hyväksyntää tai rakentaa vielä erillinen hyväksyntäkierros, kuten kuvassa 7 on tehty. Hyväksyntä voidaan pakottaa tilauksen yhteydessä normaalin hyväksyntäkierroksen päätteeksi. Kuvassa 7 on liiketoiminta- ja teknisen hyväksynnän jälkeen määritelty erillinen päättely. Jos kyseinen oikeus on korkean riskiprofiilin oikeus, sen toteuttamiselle vaaditaan vielä yksi hyväksyntäkierros.



Kuva 7. Korkean riskiprofiilin erillishyväksyntä

Vaatimusten mukaiset asiat

Toteutusprojektissa oli myös asioita, jotka olivat täysin vaatimusten mukaisia. Järjestelmätoimittajan vahvasta suosituksesta päädyttiin erottamaan ulkoiset käyttäjät sisäisistä käyttäjistä pelkän tunnuksen avulla. Erottamiseen ja toisaalta käyttäjän identifiointiin käytettiin useita AD-attribuutteja.

SamAccountName määriteltiin aivan aluksi muuttumattomaksi ja tästä syystä haluttiin poistaa vanha määritys, jossa käyttäjätunnus muodostuu sukunimen ja etunimen kirjaimista. Uuden määrittelyn mukaisesti samAccountName määritellään henkilönumeroperusteisesti ja on täten identtinen palkkajärjestelmän ID:n kanssa. Ulkoisille käyttäjille ei voida käyttää henkilönumeroa, koska heidän sähköisiä identiteettejä ei perusteta palkkajärjestelmään, joten toteutuksessa päädyttiin käyttämään järjestelmän muodostamaa kuusinumeroista ID:ta IGAP-etuliitteellä, kuten kuvasta 8 voidaan havaita. UserPrincipalName ja sähköposti nimetään ulkoisten käyttäjien kohdalla myös EXT-etuliitteellä, kuten myös henkilön DisplayName ja näin henkilöt erottuvat helposti kaikissa yleisissä AD- tai Azure AD -hakemistoon perustuvissa käyttäjähakemistoissa, kuten O365-palvelussa.

GIVEN NAME	SURNAME (SN)	DISPLAY NAME	EMPLOYEEID
Testi	Henkilö-Ulkoinen	EXT-Henkilö-Ulkoinen Testi	IGAP-004404
Testi	Henkilö-Sisäinen	Henkilö-Sisäinen Testi	900051

SAM-ACCOUNT NAME	USER PRINCIPAL NAM...	MAIL
IGAP-004404	EXT-Testi.Henkilo-Ulkoinen@sipoo.fi	EXT-Testi.Henkilo-Ulkoinen@sipoo.fi
900051	Testi.Henkilo-Sisainen@sipoo.fi	Testi.Henkilo-Sisainen@sipoo.fi

Kuva 8. Internal ja External -käyttäjien eroavaisuudet nimeämisessä

Käyttäjien perustamisessa käytetään sisäisillä käyttäjillä uniikkina tietona henkilönumeroa. Koska tieto tulee syöttää prosessin käynnistämiseksi palkkajärjestelmään, niin henkilönumero on aina käytettävissä ja pysyy muuttumattomana. Ulkoisten käyttäjien osalla toteutuksen tekeminen vaati kaksi erilaista järjestelyä, koska henkilötunnuksen käyttäminen esimerkiksi toimittajien tunnuksien yksilöimisessä poistettiin tietosuojaselvitysten jälkeen. Käytäntö muutettiin siten, että toimittajilta ja ostopalvelutyöntekijöiltä vaaditaan syntymäaika,

joka yhdistetään etunimen ja sukunimen yhdistelmään ja tästä arvosta lasketaan käyttäjälle uniikki md5hash eli viestien tiivistelmäalgoritmilla luotu tiiviste (kuva 9).

Lyhytaikaisten sijaisten osalta tämä käytäntö on tiivisteen laskemisen osalta sama, mutta lähtötietona käytetään henkilötunnusta. Tämä perustuu toimintaprosessin vaatimaan seikkaan: lyhytaikaisten sijaisten työsuhteet kirjataan palkkajärjestelmään pääosin jälkikäteen, joten tätä tietoa ei voida hyödyntää samalla tavoin kuin sisäisten työntekijöiden kohdalla.

Tästä toteutuksen kokonaisuudesta rakentui kolmen eri yksilöllisen tiedon kokonaisuus: henkilönumero, henkilötunnus sekä syntymäajan ja nimitietojen tiiviste. Tämän takia on mahdollista, että samalla luonnollisella henkilöllä voi olla kolme eri sähköistä identiteettiä AD:ssa. Nykyinen järjestelmäarkkitehtuuri ja siihen liitetyt toimintaprosessit eivät kuitenkaan mahdollista tällä hetkellä parempaa ratkaisua.

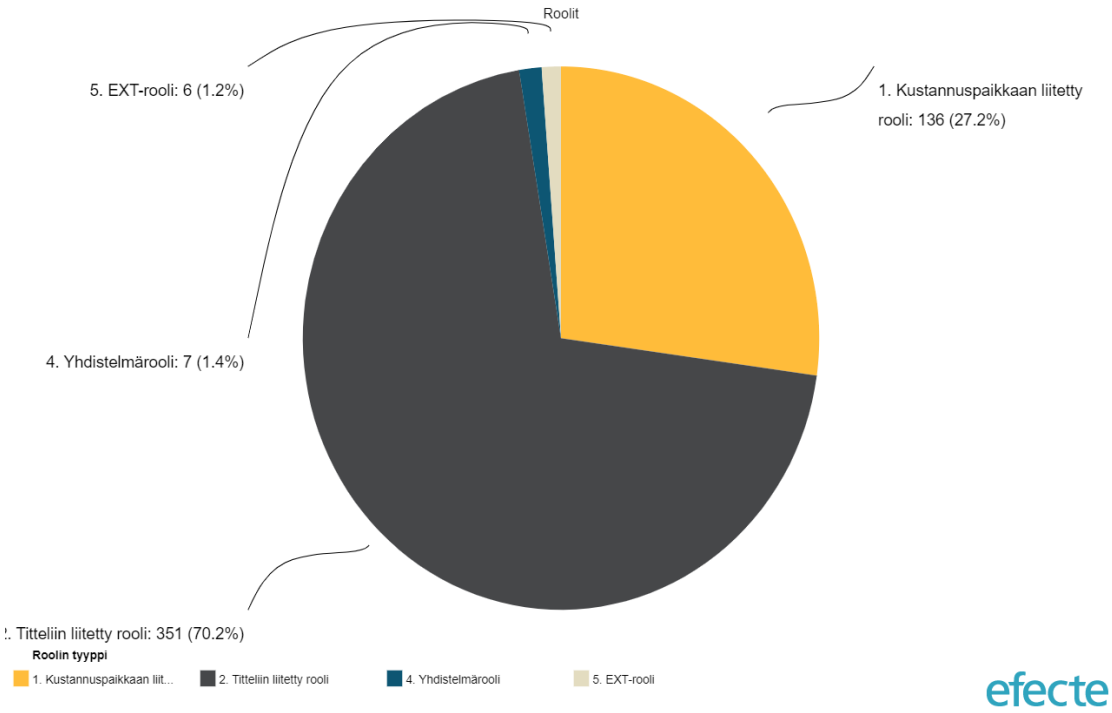
Run *

```
import hashlib
if social_security_number != None:
  _hetu = hashlib.md5(social_security_number.encode())
  this.set("social_security_number_hash", _hetu.hexdigest())
  this.set("social_security_number", None)
if birthday != None:
  _personid = birthday+first_name+surname
  _personhash = hashlib.md5(_personid.encode())
  this.set("social_security_number_hash", _personhash.hexdigest())
  this.set("birthday", None)
```

Kuva 9. Yksilöllisen hash-tiedon laskeminen ulkoisille työntekijöille

Toteutusprojektissa luotiin roolitusrakenne, joka perustuu kahteen palkanmaksujärjestelmässä määriteltävään perustietoon: tehtävänimikkeeseen ja kustannuspaikkaan. Lisäksi on mahdollista rakentaa myös näiden yhdistelmä, mutta tämä on toistaiseksi jätetty laajemmin käyttöönottamatta, koska rooleja syntyisi tämän roolitustavan myötä todella paljon. Kuntaliiton (2013, 19) mukaan roolien määrään tulee suhtautua kriittisesti ja ne tulisi pitää alle sadan, mutta kuitenkin todetaan, että roolit voidaan johtaa tehtävänkuvasta. Toteutuksessa

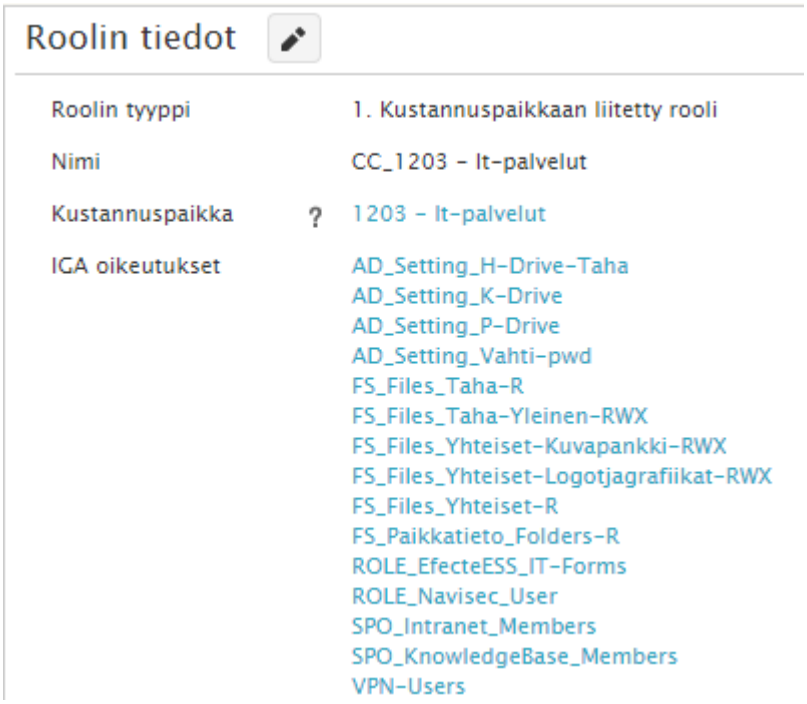
valittu toimintamalli on tässä tapauksessa perusteltu, vaikka rooleja on kokonaisuudessaan viisisataa, koska työroolien määritys tapahtuu palkkajärjestelmän tietojen pohjalta, eikä rooleja voi esihenkilö itse määrittää muuttamatta työntekijän tehtävänimikettä tai kustannuspaikkaa. Työroolit on esitetty kuvassa 10 tyypin mukaan. Työrooleja on tehtävänimikkeen ja kustannuspaikan lisäksi myös yhdistelmä- ja EXT-rooleja. Jälkimmäistä hyödynnetään ulkoisten työntekijöiden käyttöoikeuksien määrittämisessä.



Kuva 10. IGA-roolit tyypeittäin

Tutkitun tiedon valossa toteutettu roolitus oli pääosiltaan kunnossa, mutta käytännön havaintona hyvin pian tuli vastaan tapauksia, jossa jokin yksittäinen roolin määritelty oikeus ei voinutkaan olla osa roolia, koska rekrytoinnin kautta kuntaan tuli työntekijä samoilla roolimäärityksillä, mutta työntekijän tehtävänkuva oli kuitenkin sellainen, että jotain rooliin kuulunutta käyttöoikeutta ei voitukaan hänelle antaa. Tästä tehtiin nopeasti johtopäätöksenä uusi linjaus, että palkkajärjestelmän tietoihin pohjautuva rooli ei voi pitää sisällään järjestelmäkohtaisia käyttöoikeuksia. Tällaiset järjestelmäoikeudet tulee erikseen tilata ja samalla varmistaa käyttäjän riittävä osaaminen järjestelmän käyttöön. Kuvassa 11 on esitetty yhden roolin määritykset, josta voidaan todeta roolin sisältävän hyvin yleisiä oikeuksia kuten: verkkolevyjen käyttöoikeuksia, intranetin käyttöoikeus, ratkaisutietokannan käyttöoikeus, Efecten itsepalvelun IT-

lomakkeiden käyttöoikeus ja VPN-käyttöoikeus. Kaikki oikeudet ovat niin sanottuja perusoikeuksia, joissa ei tarvita hyväksyntämenettelyä tai käyttökoulutusta.



Kuva 11. Kustannuspaikkaroolin määritykset

Ensimmäisen vaiheen toteutusprojektiin ei sisältynyt roolien tilaamisen mahdollisuutta ja tässä onkin tunnistettu selvä parantamiskohde, joka helpottaa käyttöoikeuksien tilaamista niin työntekijöiden, esihenkilöiden tai myös käyttöoikeuksien toteuttajien osalta.

Yleiset havainnot

IGA-käyttöönoton jälkeen havaittiin, että käyttöoikeuksia on hyvin paljon erilaisia, ja vaikka kaikki oikeudet pystytään hallitsemaan IGA-järjestelmällä, ei kaikkiin oikeuksiin olisi tarpeen noudattaa täysin samaa hyväksyntäprosessia. Joidenkin oikeuksien avulla pääsee henkilötietoihin, erityisiin henkilötietoihin, rahaliikenteeseen tai muihin tärkeisiin tietoihin. Osa oikeuksista taas on vain yhtenäisen prosessin takia hyvä pitää yllä samassa järjestelmässä saman prosessin takana. Osaan vaikuttavat vuotuiset lisenssi- tai muut maksut, jonka takia säännöllinen validointi on hyvä tehdä. Ehkä selvimmin oikeudet ovat luokiteltavissa kahteen selkeään kategoriaan: järjestelmät, joissa on henkilötietoja ja järjestelmät, joissa ei ole henkilötietoja.

Jokin käyttövaltuus voi edellyttää oikeutta työasemasovellukseen asentamiseen, oikeutta ADFS-kirjautumiseen (Active Directory Federation Services) sekä oikeutta itse järjestelmään, joka on manuaalisesti provisioitava käyttöoikeus järjestelmään, jossa identiteetti linkitetään AD-tunnukseen. Joissakin järjestelmissä riittää pelkkä AD-ryhmäjäsenyys, jolloin oikeus on kokonaisuudessaan automaattisesti provisioitava. Jotkin oikeudet edellyttävät AD-ryhmäjäsenyyttä, mutta sen lisäksi vielä tarkempaa roolimääritystä kohdejärjestelmässä. Käyttöoikeuksien tarkka määrittely lisää turvallisuutta, mutta tuo mukanaan käytön hankaluutta. Loppukäyttäjän on luonnollisesti hankalaa ymmärtää, miksi yhden käyttöoikeuden saamiseen tarvitaan kolme erillistä tilausta. Tämän voisi laskea käyttöönottoprojektin ensimmäisen vaiheen ongelmaksi, joka vaatii jatkokehitystä, jotta roolien tilaaminen saadaan toteutettua identiteetin- ja käyttövaltuuksien hallintajärjestelmään.

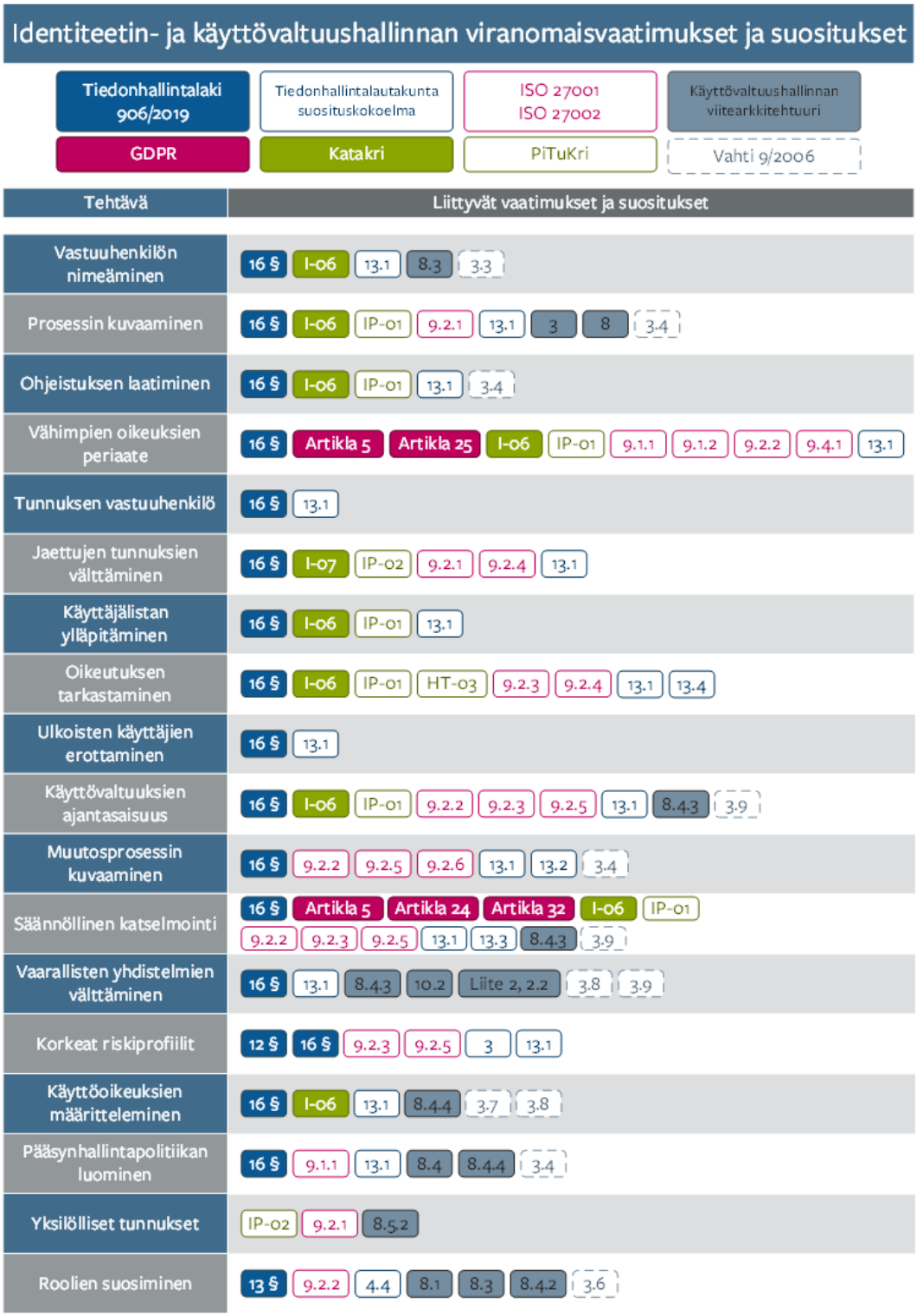
Käyttöoikeus termin määritys itsessään tuli vastaan hyvin pian IGA-järjestelmän käyttöönoton jälkeen. Koska IGA mahdollisti monenlaisen asian automatisoinnin pohdittavaksi tuli, onko esimerkiksi sovellusasennus käyttöoikeus. Toteutusprojektissa päädyttiin toteuttamaan IGA-järjestelmän avulla myös perussovellusten asennuksia AD-ryhmiin pohjautuen ja käyttövaltuutta tähän ryhmään hallittiin IGA-järjestelmällä. Vaikka sinänsä työasemasovelluksen käyttöönotto ei kaikissa tapauksissa vaadi erillisiä hyväksyntäkierroksia, päätettiin näin kuitenkin tehdä yhtenäisen määrittelyn ja käyttökokemuksen takia. Tässä yhteydessä ei nähty ongelmaksi, että esihenkilö hyväksyy lisäsovellusten käytön. Käyttöoikeuksia järjestelmän kautta oli myös mahdollista käsitellä esimerkiksi fyysisiä pääsyjä, kuten avainhallintaa, joka liittyy tilaturvallisuuteen. Toistaiseksi tästä osuudesta päätettiin luopua ja hallita avainhallinnan prosessia nykyisillä menetelmillä. Tämän osalta tilanne pitää arvioida uudelleen siinä yhteydessä, kun kulunvalvontajärjestelmää kehitetään.

10 TULOKSET

Kehitysprojektina oli tarkoitus saada käyttöön kunnalle automaattinen identiteetin- ja käyttövaltuushallinnan järjestelmä. Järjestelmän käyttöönoton jälkeen havaittuihin ongelmiin lähdettiin etsimään ratkaisua opinnäytetyön tutki-

musongelman kautta. Tutkimuskysymyksiin etsittiin vastauksia eri viitekehyksistä, joita tutkittiin yhteensä kahdeksaa erilaista, kansallista tai EU-tasoista. Erilaista näkemystä identiteetin- ja käyttövaltuushallinnan toteuttamiseen käsiteltiin tutkimalla IAM-hallintaan liittyviä parhaita käytäntöjä. Näistä tuotettiin kaikkiaan 18 eri vaatimusta identiteetin- ja käyttövaltuushallinnan toteuttamiseen liittyen, joita kutakin käsiteltiin ristiin kaikkien vaatimuskehysten kanssa. Tuloksia käsiteltiin lisäksi tietoturvaan peilaten ja etsittiin identiteetin ja käyttövaltuushallinnan työkaluilla tehtäviä toimenpiteitä kyberuhkien ehkäisemiseksi. Tutkimuksen tuloksena toteutettiin havainnollistava kuva vaatimuksista (kuva 12) ja tätä tukemaan erillinen tarkempi tehtävien kuvaus (liite 4), jonka avulla pystytään tarkistamaan, minkä viitekehyksen kautta vaatimus on perusteltu ja mitä vaatimukset ja tehtävät pitävät sisällään. Kaksi merkittävintä vaatimusta ovat vähimpien oikeuksien periaate ja säännöllinen katselmointi. Vastakkaisena havaintona on, että yksilölliset tunnukset, ulkoisten käyttäjien erottaminen ja tunnuksen vastuuhenkilö ovat taas asioita, joita ei useassakaan vaatimuskehyksessä mainita lainkaan.

Tiedonhallintalakiin eli Laki julkisen hallinnon tiedonhallinnasta, on määritelty erittäin yleisesti vain vaatimukset käyttövaltuushallinnan sisällöstä. Tätä tukemaan on kuitenkin olemassa tiedonhallintalautakunnan (2021) julkaisema suosituskokoelma, johon on kirjattu suositeltuja tehtäviä vaatimusten täyttämiseen. Kuvassa 12 esitellyt vaatimukset ja suositukset pohjautuvat suosituskokoelman luetteloon ja muihin vaatimuksiin ja tätä vaatimuslistaa on täydennetty kahdella muulla tutkimuksen kautta havaitulla vaatimuksella. Kuvassa 12 on esitetty kaikkien tutkittujen viitekehysten vaatimukset ja suositukset ja kirjattu ne havainnolliseen kuvaan helppolukuiseksi kokonaisuudeksi. Vahti-oheistuksen suositukset sisällytettiin kuvaan 12, vaikka ohjeen sisältö oli käytännössä käsitelty jo uudemmissa julkaisuissa tai ohjeissa. Vahti-ohjeesta löytyi kuitenkin hyödyllisiä tarkentavia tietoja eri vaatimuksiin. Myös Kuntaliiton (2013) julkaisema käyttövaltuushallinnan viitearkkitehtuuri on vaatimustensa puolesta käsitelty uudemmissa vaatimuskehyksissä, mutta sen sisältämiä prosessikuvauksia ja tarkempia tehtäväkuvauksia ei ole käsitelty muissa vaatimuskehyksissä.



Kuva 12. Identiteetin- ja käyttövaltuushallinnan viranomaisvaatimukset ja suositukset

Lakien ja asetuksien reunaehtojen selvittäminen käyttövaltuushallinnalle oli keskeisin tavoite, jotta identiteetin- ja käyttövaltuushallinnan toteuttamisella on jokin selkeä viitekehys, jota vasten toteutusta voidaan tehdä. Ylimpänä vaatimuskehyksenä kunnalle toimivat Suomen lait: tiedonhallintalaki (Laki julkisen hallinnon tiedonhallinnasta) ja tietosuojalaki (Tietosuojalaki), jolla käyttöönotetaan kansallisesti EU:n yleinen tietosuoja-asetus (Euroopan parlamentin ja

neuvoston asetus (EU) 2016/679). Tiedonhallintalain sisältö on erittäin lyhyesti kirjattu, mutta se sisältää tiiviistä vaatimusasettelusta huolimatta 17 eri vaatimusta 18 vaatimuksesta.

Tiedonhallintalautakunta (2021) määrittelee edellytyksiä lain vaatimusten soveltamiseen. Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta on lain tietoturvallisuutta käsittelevän neljännen luvun pykälien tarkempi läpikäynti (Tiedonhallintalautakunta 2021). Suosituskokoelman tarkoitus on opastaa lain vaatimusten täyttämisessä. Tätä julkaisua voidaan pitää reunaehtona käyttövaltuushallinnan toteuttamisessa.

Muista tutkituista viitekehyksistä voi tehdä päätelmän, että ne ovat kunnalle vain suosituksia ja parhaita käytäntöjä. Katakri on auditointityökalu, joka itsessään ei aseta mitään vaatimuksia käyttövaltuushallinnan toteuttamiseen. Katakrin avulla voidaan arvioida organisaation kyvykkyyttä suojata turvallisuusluokiteltua tietoa. PiTuKri on myös arviointityökalu ja sen tavoitteena on vain edistää salassa pidettävän tiedon turvallisuutta, kun palveluja tuotetaan pilvipalveluista. ISO 27001 -standardi (SFS-EN 27001: 2017) ja sitä tukemaan luotu ISO 27002 -lisästandardi (SFS-EN 27002: 2017) eivät ole kuntaa velvoittavia, koska kunta ei ole hakenut ISO 27001 -laatusertifiointia. ISO 27001 viitekehystä voidaan siis pitää vain hyvänä suosituksena identiteetin- ja käyttövaltuuden toteuttamisessa. Vahti-ohje, käyttövaltuushallinnon periaatteet ja hyvät käytännöt, on lähtökohtaisesti vain ohje, joka antaa hyviä periaatteita ja käytäntöjä, joita olisi suositeltava tehdä käyttövaltuushallinnassa (Valtiovarainministeriö 2006). Käyttövaltuushallinnan viitearkkitehtuurin lähtökohta on pelkästään IAM-ratkaisun käyttöönottoa helpottava ohje. Tavoitteena on antaa kunnalle käyttövaltuuksien hallintaan selkeä runko toteutusta helpottamaan. Kaikki edellä kuvatut viitekehykset antavat runsaasti samoja suosituksia, kuinka käyttövaltuushallintaa tulisi tehdä. Yksikään ei ole kaiken kattava, vaan kaikki jättävät osan vaatimuksista huomiotta.

Tiedonhallintalaki ja sitä tukemaan luotu suosituskokoelma ovat lopulta kattavin kokoelma vaatimuksia. Suosituskokoelmasta jää uupumaan vain vaatimus yksilöllisistä tunnuksista, joka on esitetty vaatimuksena PiTuKrissa, ISO 27002 -standardissa ja käyttövaltuushallinnan viitearkkitehtuurissa. Myös roolien suosiminen puuttuu lain 16. § käsittelystä, mutta on esitelty 13. § kautta. Muissa

viitekehyksissä on kuitenkin avattu yksittäisten vaatimusten sisältöä tarkemmin, joka antaa lukijalle paremman käsityksen kokonaisuudesta.

Kehitystoimenpiteiden löytäminen oli yksi tutkimuksen tavoite ja kehitystoimiksi löydettiin seuraavat tehtävät:

- Kaikkien tietojärjestelmien käyttöoikeuksista vastaavat henkilöt tulee nimetä.
- Kunnalle tulee luoda pääsynhallintapolitiikka.
- Hyväksyntäroolia tekevät käyttäjät tulee ohjeistaa.
- Kohdejärjestelmien käyttöoikeusmääritys vähimpien oikeuksien periaatteen mukaisesti tulee tehdä.
- Vastuuhenkilö tulee määrittää jaetuille tunnuksille.
- Jaettujen tunnusten välttäminen vaatii järjestelmäkohtaista katselmointia ja ohjeistusta.
- Prosessikuvaukset tulee laatia.
- Oikeutuksen tarkastamisen osalta tulee varmistaa, tarkistetaanko henkilöllisyys ja onko tarpeen vaatia osaamisen tarkistamista joissain järjestelmissä.

Identiteetin- ja käyttövaltuushallinnan asianmukainen toteuttaminen antaa organisaatiolle myös kyberuhkiin liittyviä ennaltaehkäiseviä toteutuskeinoja. Politiikan ja toimintaprosessien kautta vähimpien oikeuksien periaate sekä säännöllinen katselmointi yhdessä ennaltaehkäisevät tietoturvauhkien syntymistä. Ylläpito-oikeuksien tarkka määrittely on vaatimus turvalliseen hallintaan, koska korkean profiilin oikeuksilla on vahva side järjestelmän haavoittuvuuksiin ja häiriötilanteisiin. Ransomwareen, malwareen, sähköpostiin liittyviin- tai tietoon kohdistuviin uhkiin voidaan varautua käyttämällä IAM-järjestelmää. Vähimpien oikeuksien periaate tai tarve tietää -periaate rajaa myös mahdollisen hyökkääjän mahdollisuutta päästä tietoon käsiksi. Näiden lisäksi myös MFA ja SSO mainitaan toteutuskeinona, mutta näiden toteuttaminen liittyy enemmän pääsynhallinnan kuin identiteetin ja käyttövaltuushallinnan kokonaisuuteen. MFA, SSO ja Zero Trust -periaate tuodaan esiin myös kansainvälisten yritysten IAM-ratkaisujen parhaina käytäntöinä. MFA tekee kirjautumistapahtumasta turvallisemman ja SSO mahdollistaa vain yhden identiteetin käyttämisen, jolloin käyttöoikeuden poistaminen on mahdollista ilman erillistä kohdejärjestelmän käyttäjähallintaa. Zero Trust -periaatteessa autentikointia suoritetaan jatkuvasti ja lähtökohtaisesti keneenkään ei luoteta. Toimintatapojen muutoksen huomioi-

mista ei tule unohtaa identiteetin- ja käyttövaltuushallintajärjestelmän käyttöönotossa ja pääsynhallintapolitiikan vaatimusten mukaisessa muutoksessa. Mahdollinen varjokulttuuri voi synnyttää uhkia, jotka eivät ole organisaation hallinnassa, jos muutosta ei ole myös toimintatapojen osalta hallittu.

11 JOHTOPÄÄTÖKSET

Lainsäädännön muutokset tietosuojaan ja tietoturvaan liittyen aiheuttavat paljon vaatimuksia viranomaisen tehtäviin. Tiivistettynä voidaan todeta, että tiedonhallintalain 16. § lyhyesti kirjoitettu sisältö, on erittäin kattava ja voidaan purkaa useiksi tehtäviksi, joista osa vaatii suurta, koko organisaatiota koskevaa toimintatavan jalkauttamista. IGA-järjestelmän käyttöönottoprojekti oli loppujen lopuksi vain tekninen järjestelmän käyttöönotto ja tämän projektin kautta käyttöönotettu käyttövaltuushallinnan automatisointi tuotti vain teknisiä yksityiskohtia vaatimuksen mukaiselle tasolle. Tällaisia asioita olivat esimerkiksi ulkoisten käyttäjien erottaminen EXT-etuliitteellä, yksilölliset käyttäjätunnukset sekä roolien suosiminen. Nämä ovat asioita, joita pystytään teknisesti määrittelemään ja vaativat lopulta vähän ylläpitotyötä, kun ne ovat kerran määritelty oikein.

Opinnäytetyöprosessi onnistui ennakko-odotuksia paremmin. Tutkimusongelman tutkiminen vei lopulta mukanaan tärkeään aiheeseen ja tarkemman tutkimisen jälkeen sain luotua selkeät tavoitteet tutkimuksen tekemiseen ja pystyin noudattamaan aikataulua hyvin. Motivaattorina tutkimukselle toimi aiheen tärkeys omassa työssä ja hyödyt Sipoon kunnalle, oman ammattitaidon kehittyminen sekä myös kansallisesti tärkeän aiheen käsittely ja mahdollisuus, että myös muut kunnat voivat hyötyä tutkimuksen ohessa syntyneestä tuotoksesta (liite 4). Työ oli käytännössä täysin itsenäistä, eikä vuorovaikutusta toimeksiantajan puolelta ollut juuri saatavissa. Kriittistä tutkimuksen edetessä oli arvioida itse tekemäänsä kehitystyötä identiteetin- ja käyttövaltuushallinnan käyttöönoton suhteen ja löytää itse tekemiään virheitä ja kuitenkin pysyä objektiivisena löydösten suhteen. Kun työhön suhtautuu asenteella, että jokainen löydös on askel parempaan ja tietoturvallisempaan tilaan, ei ongelmaa omien virheiden myöntämisessä ollut.

Alun perin määriteltyä tutkimusongelmaa piti tarkentaa kesken tutkimuksen, koska tutkimuksen tuloksena tuotettu kuva 12, oli erittäin konkreettinen tuotos vaatimuksista ja tehty tutkimus avasi käytännössä identiteetin- ja käyttövaltuushallinnan perimmäisen tarkoituksen ja sen vaatimukset. Tämän jälkeen fokus opinnäytetyössä muuttui enemmän vaatimusten arviointiin, eikä niinkään IGA-järjestelmän käyttöönottoon ja teknisiin seikkoihin. Voidaan sanoa, että tässä suhteessa asennoituminen IGA-järjestelmän käyttöönottoon perustui väärään olettamukseen todellisista lain vaatimuksista. Tätä ongelmaa kuvasin ennen tutkimusta lainsäädännön haasteena ja tässä kehittämisprojektissa tämä asia konkretisoitui tavalla, jota en osannut odottaa. Jos nyt lähtisin tekemään uudelleen IAM- tai IGA-järjestelmän käyttöönottoprojektia, keskittyisin ensiksi toimintaprosesseihin ja pääsynhallintapolitiikkaan ja vasta sitten tekniseen järjestelmän käyttöönottoon.

Pelkästään käyttövaltuushallintaan liittyvä tiedonhallintalain vaatimuslista on erittäin suuri, se edellyttää koko organisaation osallistumista ja työtä tulee tehdä säännönmukaisesti luotujen prosessien mukaisesti. Muuttuva ja tietosuoja- ja tietoturvavaatimuksiltaan kiristyvä lainsäädäntö edellyttää paljon työtä kuntaorganisaatiolta ja työhön tulee resursoida riittävästi aikaa ja tekijöitä.

Yhtenä havaintona käyttövaltuushallinnan toteuttamisesta lain vaatimusten mukaisesti voidaan nostaa organisaation kulttuuri, johon muutosta ollaan tekemässä. Ilman koulutusta ja perehdytystä voidaan lainmukainenkin roolitettu käyttövaltuushallinta toteuttaa väärin, jos tilaamiseen ja hyväksymiseen osallistuvat henkilöt eivät ole ohjeistettu oikein. Oikein roolitettujen käyttöoikeuksien leväperäinen jakaminen johtaisi tilanteeseen, että oikeuksia ei olisi enää määritelty vähimpien oikeuksien periaatteen mukaisesti. Voitaisiin sanoa, että kaikki oikeudet kaikille -tyylisestä ympäristöstä siirtyminen vähimpien oikeuksien periaatteen mukaiseen toimintamalliin on iso toiminnallinen muutos ja se edellyttää pitkäjänteistä työskentelyä.

Tämän tutkimuksen yhteydessä havaittiin muutamissa vaatimuksissa yhteys riskienhallintaan. Vaarallisten yhdistelmien tunnistaminen ja toimenpiteet niiden välttämiseen, korkeat riskiprofiilit ja niiden käsittely sekä pääsynhallintapolitiikka ovat vahvasti yhteydessä riskienhallintaan ja tämän aiheen tarkempi

tutkiminen voisi avata enemmän, miten tietoturvariskeihin tulisi suhtautua ja toimia niiden suhteen ennaltaehkäisevästi käyttövaltuushallinnan osalta. Vähimpien oikeuksien periaate on myös aiheena suoraan johdettavissa riskien välttämisen toimenpiteenä. Vähimpien oikeuksien periaatteen vastainen tilanne olisi, kaikki oikeudet kaikille, joka toisi todella paljon riskejä lainmukaiseen tiedonhallintaan. Myös kommentointikierroksella olevan julkisen hallinnon tietoturvallisuuden arviointikriteeristö, eli Julkri, olisi hyvä katselmoida läpi käyttövaltuushallinnan näkökulmasta.

Erityisenä havaintona voidaan pitää myös tietynlaisten itsestäänselvyyksien puuttumista useista vaatimuskehyksistä. Tunnuksen vastuuhenkilöstä ei löytynyt mainintaa kuin tiedonhallintalautakunnan suosituskokoelmasta, ja yksilöllisten tunnusten vaatimus mainittiin vain PiTuKrissa ja ISO 27002 -standardissa. Muista vaatimuskehyksistä vastaavaa mainintaa ei löytynyt. Ulkoisten käyttäjien erottaminen työni kautta havaitulla, hyvin yleisellä, EXT-etuliitteellä ei ollut vaatimuksena kuin tiedonhallintalautakunnan suosituskokoelmassa. Aiheesta ei löytynyt tutkittua tietoa, vaikka olen havainnut käytännön olevan erittäin yleinen eri organisaatioissa. Roolien suosiminen puuttui suositustoimenpiteistä tiedonhallintalain 16. § käsittelyssä, mutta oli kuitenkin mainittu 13. § suosituksia käsittelevässä luvussa.

Pääsynhallintaan liittyvät havainnot nostettiin esiin, mutta niitä ei tätä enempää käsitelty. MFA ja SSO ovat kuitenkin mekanismeja, jotka parantavat tietoturvaa. Tutkimuksen mukaan SSO on tehokas tapa hallita pääsyä kohdejärjestelmään, koska sähköisen identiteetin kirjautumistiedot ovat samat. SSO:ta tulisikin ajatella ensiksi tietoturvan ja vasta sitten käyttäjälle näkyvän kertakirjautumisen asiana.

Opinnäytetyön tulokset ovat suoraan hyödynnettävissä kuntasektorilla identiteetin- ja käyttövaltuushallinnan työssä. Tuloksien kautta voidaan arvioida organisaation vaatimustenmukaista tilaa tai tuloksien avulla voidaan kehittää nykyistä tunnushallintaa vastaamaan paremmin lain vaatimuksia ja osin jopa ISO 27001 -standardin vaatimuskehystä.

Opinnäytetyön tekeminen opetti minulle uudenlaista osaamista lakien ja asetuksien käsittelystä ja niiden tulkitsemisesta. Kansallisesti kuntaorganisaatioille tuotetaan hyvää ohjeistusta ja suosituksia, mutta valitettavasti usean eri toimijan tuottamat ohjeet toistavat usein samaa asiaa hieman epätäydellisenä ja saavat aikaan epäselvän kuvan mitä vaatimukset lopulta ovat ja minkä mukaan kehittämistyötä tulee tai kannattaa tehdä. Omassa työssäni ei vastaaviin tutkimuksiin käytännössä ole mahdollisuuksia vastaavalla eri viitekehyksien läpikäynnillä ja tärkeää onkin osata tulkita ohjeistuksia ja niiden lähteitä sen mukaan mitä lait edellyttävät ja muodostaa niistä tarvittavat toimenpidesuositukset.

Tutkimus oli luonteeltaan tutkimuksellinen kehittämisprojekti, joka on yksi interventionistisen tutkimuksen muoto (Kananen 2017, 10). Tutkimuksessa käytiin tarkasti läpi identiteetinhallintaan ja käyttövaltuushallintaan liittyvä sisältö kahdeksasta eri viitekehyksestä, jotka antavat laajan kuvan saman asiakokonaisuuden käsittelystä. Tutkimusongelmasta johdetut tutkimuskysymykset olivat oleellisen tärkeät Sipoon kunnan käyttövaltuushallinnan kehittämistyölle ja tutkimuksen tuloksena löydetyt jatkokehitystehtävät antavat hyvät mahdollisuudet sen lainmukaiselle toteuttamiselle.

LÄHTEET

Allen, J. 2013. NSA to cut system administrators by 90 percent to limit data access. *Reuters*. Verkkolehti. Päivitetty 9.8.2013. Saatavissa: https://www.reuters.com/article/us-usa-security-nsa-leaks-idUSBRE97801020130809 [viitattu 9.3.2022].

Barker, W., Scarfone, K., Fisher, W. & Souppaya, M. 2021. Cybersecurity Framework Profile for Ransomware Risk Management. National Institute of Standards and Technology. Preliminary Draft NISTIR 8374. PDF-dokumentti. Saatavissa: https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf [viitattu 2.4.2022].

Contribyte. 2016. Tehokas Kanban vai kasa lappuja seinällä? WWW-dokumentti. Päivitetty 15.12.2016. Saatavissa: https://contribyte.fi/2016/12/15/tehokas-kanban-vai-kasa-lappuja-seinalla [viitattu 2.4.2022].

Digi- ja väestötietovirasto. s.a. VAHTI-verkosto kehittää digitaalista turvallisuutta. WWW-dokumentti. Saatavissa: https://dvv.fi/vahti [viitattu 28.2.2022].

DNV. s.a. ISO/IEC 27001 - tietoturvallisuuden hallintajärjestelmä. WWW-dokumentti. Saatavissa: https://www.dnv.fi/services/iso-iec-27001-tietoturvallisuuden-hallintajarjestelma-3327 [viitattu 28.3.2022].

Efecte 2019. Efecten IGA-ratkaisu nopeuttaa käyttövaltuuspyyntöjen hallintaa. WWW-dokumentti. Päivitetty 2.4.2019. Saatavissa: https://article.efecte.com/news/fi/efecten-iga-ratkaisu-lanseerattu [viitattu 13.3.2022].

Efecte 2021. Efecte IGA. PDF-dokumentti. Saatavissa: https://www.efecte.com/hubfs/Efecte-IGA-Factsheet-2021.4.pdf [viitattu 13.3.2022]

Efecte. s.a. Efecte Whistleblower - One Tool for Whistleblower and Beyond. WWW-dokumentti. Saatavissa: https://www.efecte.com/solutions/esm/whistleblower [viitattu 16.1.2022].

Enisa. 2021. Enisa Threat Landscape 2021. PDF-dokumentti. Päivitetty 27.10.2021. Saatavissa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 [viitattu 28.3.2022].

Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/1937.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.

Fryzel, C. 2021. Defining IAM and IGA. HumanID. WWW-dokumentti. Päivitetty 21.4.2021. Saatavissa: https://human-id.org/blog/defining-iam-and-iga/ [viitattu 30.3.2022].

Henkilötietojen käsittelyohje s.a. Sipoon kunta. PDF-dokumentti. Saatavissa: https://www.sipoo.fi/wp-content/uploads/2022/03/Henkilotietojen-kasittelyohje-Sipoon-kunta.pdf [viitattu 31.3.2022].

Huomautus tietoturvaloukkauksesta ilmoittamisesta, kun rekisteröityjen yhteystiedot eivät ole rekisterinpitäjän tiedossa 3.1.2020.

Hakala, H., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo

Irwin, L. 2019. ISO 27001 vs. ISO 27002: What's the difference? Blogi. Päivitetty 22.7.2021. Saatavissa: https://www.itgovernance.co.uk/blog/understanding-the-differences-between-iso-27001-and-iso-27002 [viitattu 21.2.2022].

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona: opas opinnäytetyön ja pro gradun kirjoittajalle. Jyväskylä. Jyväskylän ammattikorkeakoulun julkaisuja 232. E-kirja. Saatavissa: https://kaakkuri.finna.fi/ [viitattu 16.1.2022].

Katz, E. 2021. Top 5 Identity and Access Management Best Practices for DevSecOps. Spectral. WWW-dokumentti. Päivitetty 28.7.2021. Saatavissa: https://spectralops.io/blog/top-5-identity-and-access-management-best-practices-for-devsecops/ [viitattu 12.3.2022].

KPMG. 2021. Whistleblower-kanava. WWW-dokumentti. Saatavissa: https://home.kpmg/fi/fi/home/palvelut/neuvontapalvelut/riskienhallinta/whistleblowing.html [viitattu 16.1.2022].

Krapels, J. 2018. ISO27002 explained, part 2. ICT Institute. WWW-dokumentti. Päivitetty 22.6.2018. Saatavissa: https://ictinstitute.nl/iso27002-explained-part-2 [viitattu 2.3.2022].

Kuntaliitto. 2013. Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri. PDF-dokumentti. Saatavissa: https://www.kuntaliitto.fi/sites/default/files/media/file/Kuntasektorin%20k%C3%A4ytt%C3%B6valtuushallinnan%20viitearkkitehtuuri.pdf [viitattu 8.1. 2022].

Kyberturvallisuuskeskus. 2020a. Opas tietomurtojen havaitsemiseen. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Opas-tietomurtojen-havaitsemiseen.pdf [viitattu 27.1.2022].

Kyberturvallisuuskeskus. 2020b. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Liikenne- ja viestintävirasto Traficomin julkaisuja 13/2020. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf [viitattu 20.2.2022].

Käck, M. 2019. Ylläpitäjäkin on ihminen eikä täydellistä tietoturvaa ole - varaudu korotettujen käyttöoikeuksien riskeihin! *Tivi*. Verkkolehti. Päivitetty. 21.9.2020. Saatavissa: https://www.tivi.fi/kumppaniblogit/spellpoint/yllapitajakin-on-ihminen-eika-taydellista-tietoturvaa-ole-varaudu-korotettujen-kayttooikeuksien-riskeihin/044978ae-25e2-4520-8599-ed92e0b2b59b [viitattu 7.4.2022].

Kähkönen, L. 2020. Yksi yhtenäinen prosessi käyttäjätunnushallintaan. Case Savon ICT-palvelut Oy. Tampereen yliopisto. Informaatioteknologian ja viestinnän tiedekunta. Pro gradu -tutkielma. PDF-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi:tuni-202011168006 [viitattu 19.3.2022].

Linden, M. 2017. Identiteetin- ja pääsynhallinta. Tampereen teknillinen yliopisto. Tietotekniikan laboratorio. Raportti 7. PDF-dokumentti. Saatavissa: https://urn.fi/URN:ISBN:978-952-15-3992-3 [viitattu 15.1.2022].

Laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906.

Laki julkisen hallinnon tietohallinnon ohjauksesta (kumottu) 10.6.2011/634.

Laki julkisista hankinnoista ja käyttöoikeussopimuksista 1.1.2017/1397.

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.

Laki yksityisyyden suojasta työelämässä 13.8.2004/759.

Lord, N. 2017. What is the Principle of Least Privilege (POLP)? A Best Practice for Information Security and Compliance. Digital Guardian. WWW-dokumentti. Päivitetty 1.12.2020. Saatavissa: https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance [viitattu 9.3.2022].

Niemi, J. 2020. Case: Uuden käyttäjän identiteetti- ja käyttövaltuushallinnan kehittäminen organisaatiossa. Laurea-ammattikorkeakoulu. Turvallisuusjohtamisen koulutusohjelma. Opinnäytetyö. PDF-dokumentti. Saatavissa: http://urn.fi/URN:NBN:fi:amk-2020052614091 [viitattu 23.1.2022].

Oikeusministeriö. 2021. Hallituksen esitys ilmoittajansuojasta myöhästyy. WWW-dokumentti. Päivitetty 8.12.2021. Saatavissa: https://oikeusministerio.fi/-/hallituksen-esitys-ilmoittajansuojasta-myohastyy [viitattu 16.1.2022].

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. 3.–4. painos. Helsinki. Sanoma Pro.

One Identity s.a. 8 Best Practices for Identity and Access Management. PDF-dokumentti. Saatavissa: https://www.oneidentity.com/mx-es/whitepaper/8-best-practices-for-identity-and-access-management827122 [viitattu 12.3.2022].

Optimal IdM. s.a. Why identity access management is so important for data security. WWW-dokumentti. Saatavissa: https://optimalidm.com/resources/blog/importance-of-iam [viitattu 4.4.2022].

Peussa, T. & Ruotsalainen, T. 2013. Sisäinen valvonta ja vaaralliset työyhdistelmät. Kajaanin ammattikorkeakoulu. Yhteiskuntatieteiden, liiketalouden ja hallinnon ala. Opinnäytetyö. PDF-dokumentti. Saatavissa: http://urn.fi/URN:NBN:fi:amk-2013121220991 [viitattu 8.3.2022].

Puolustusministeriö. 2021. Lausunto luonnoksesta hallituksen esitykseksi eduskunnalle laiksi Euroopan unionin ja kansallisen

oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta sekä siihen liittyviksi laeiksi. PDF-dokumentti. Saatavissa: https://api.hankeikkuna.fi/asiakirjat/0b6fed29-b91b-4574-86c7-6b1354d8fc0d/15069150-f91e-44e0-80d1-fd9330f6098d/LAUSUNTO_20210903124434.PDF [viitattu 16.1.2022].

Rosencrance, L. 2020. 8 Reasons Identity and Access Management Is Important. TechTarget. WWW-dokumentti. Päivitetty 23.11.2020. Saatavissa: https://whatis.techtarget.com/8-Reasons-Identity-and-Access-Management-Is-Important [viitattu 4.4.2022].

SailPoint. 2021. 7 Best Practices for Identity Access Management. WWW-dokumentti. Päivitetty 2.2.2021. Saatavissa: https://www.sailpoint.com/identity-library/7-best-practices-for-identity-access-management [viitattu 12.3.2022].

SFS-EN ISO/IEC 27001. 2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

SFS-EN ISO/IEC 27002. 2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet.

Sipoon kunta. 2021. Tilinpäätös ja toimintakertomus 2020. PDF-dokumentti. Saatavissa: https://www.sipoo.fi/wp-content/uploads/2021/08/Liite-1-Tilinp%C3%A4%C3%A4t%C3%B6s-ja-toimintakertomus-2020-2.pdf [viitattu 6.1.2022].

Soni, R. 2020. 9 Identity and Access Management Best Practices for 2021. LoginRadius. WWW-dokumentti. Päivitetty 11.11.2020. Saatavissa: https://www.loginradius.com/blog/start-with-identity/identity-access-management-best-practices [viitattu 12.3.2022].

THL. 2021. Käytönhallinnan sanasto. Terveyden ja hyvinvoinnin laitos. WWW-dokumentti. Päivitetty 17.2.2021. Saatavissa: https://sotesanastot.thl.fi/termed-publish-server/vocabulary/74fec784-eaf6-441b-b60f-60ff8e3b1c32/concept/bbd36550-4586-47c8-af93-36860f0e7769 [viitattu 8.1.2022].

Tiedonhallintalautakunta. 2021. Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. julkaisut.valtioneuvosto.fi. PDF-dokumentti. Saatavissa: http://urn.fi/URN:ISBN:978-952-367-897-2 [viitattu 29.1.2022].

Tietosuojalaki 5.12.2018/1050.

Tietosuojaselosteet ja henkilötietojen käsittelyn asiakirjat s.a. Sipoon kunta. WWW-dokumentti. Saatavissa: https://www.sipoo.fi/organisaatio/digitaalinen-turvallisuus/tietosuojaselosteet [viitattu 31.3.2022].

Tietosuojaseloste / Henkilöstöpalvelut s.a. Sipoon kunta. WWW-dokumentti. Saatavissa: https://www.sipoo.fi/organisaatio/digitaalinen-turvallisuus/tietosuojaseloste-henkilostopalvelut [viitattu 31.3.2022].

Tietosuojavaltuutetun toimisto s.a. Tietosuojalaki. WWW-dokumentti. Saatavissa: https://tietosuoja.fi/tietosuojalaki [viitattu 6.2.2022].

Turunen, T. 2018. Kyberturvallisuuden hallintamallin kehittäminen. Kaakkois-Suomen ammattikorkeakoulu. Teknologiaosaamisen johtaminen. Opinnäytetyö. Saatavissa: https://urn.fi/URN:NBN:fi:amk-2018101616032 [viitattu 1.3.2022].

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. PDF-dokumentti. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyber-turvallisuuden-sanasto.pdf [viitattu 8.1.2022].

UC Berkeley. s.a. Need to Know Access Control Guideline. WWW-dokumentti. Saatavissa: https://security.berkeley.edu/need-know-access-control-guideline [viitattu 28.32022].

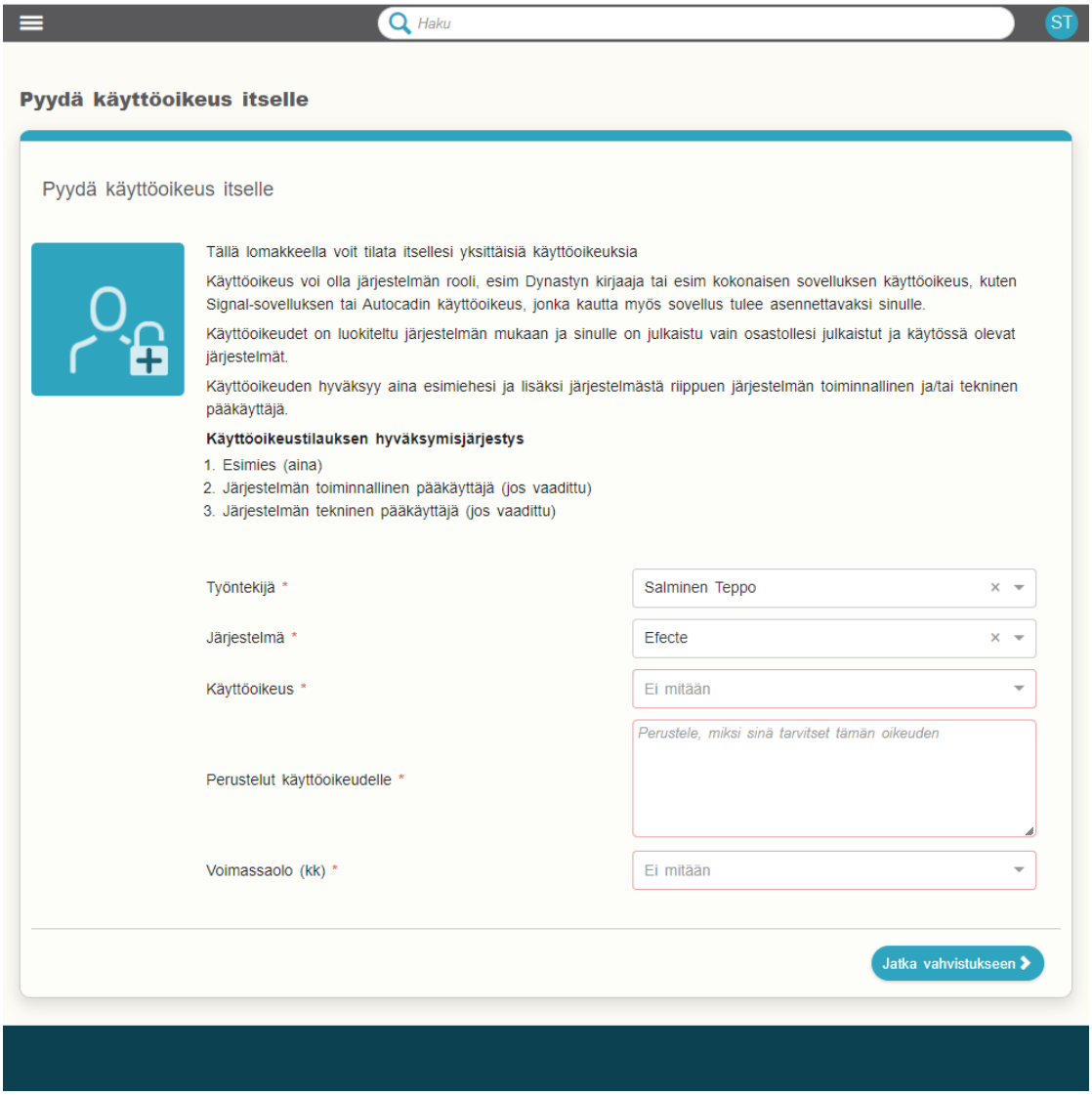
Ulkoministeriö. 2020. Katakri 2020. Tietoturvallisuuden auditointityökalu viranomaisille. Traficomin julkaisusarja 232/2020. PDF-dokumentti. Saatavissa: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf [viitattu 20.2.2022].

Valtiovarainministeriö. 2006. Käyttövaltuushallinnan periaatteet ja hyvät käytännöt. PDF-dokumentti. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_9_2006.pdf [viitattu 15.1.2022].

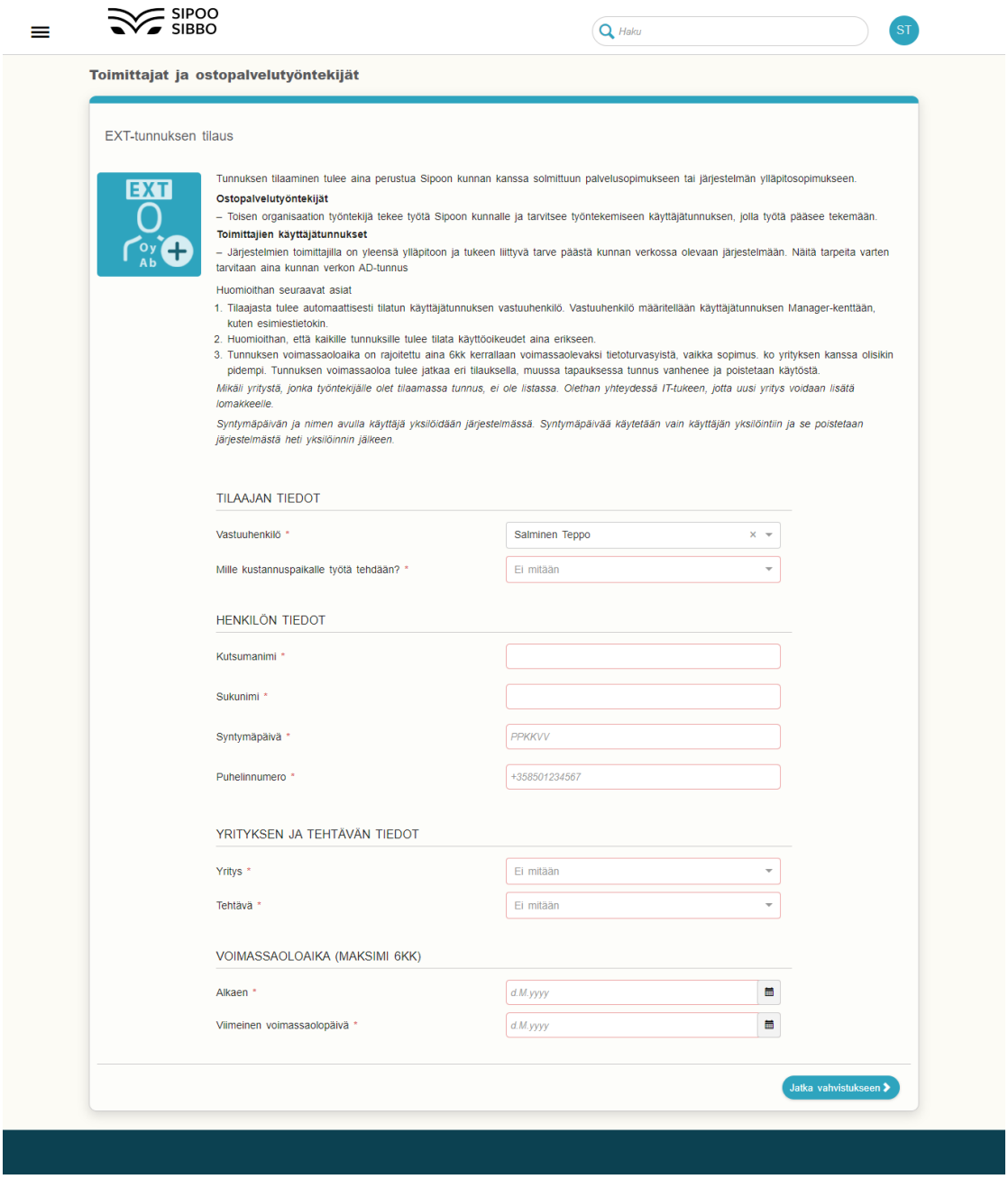
Veritis. s.a. Best Practices for Effective ‘Identity and Access Management (IAM)’ Implementation. Blogi. Saatavissa: https://www.veritis.com/blog/best-practices-for-identity-and-access-management-iam-implementation [viitattu 13.3.2022].

TILAUSLOMAKE – PYYDÄ KÄYTTÖOIKEUS ITSELLE

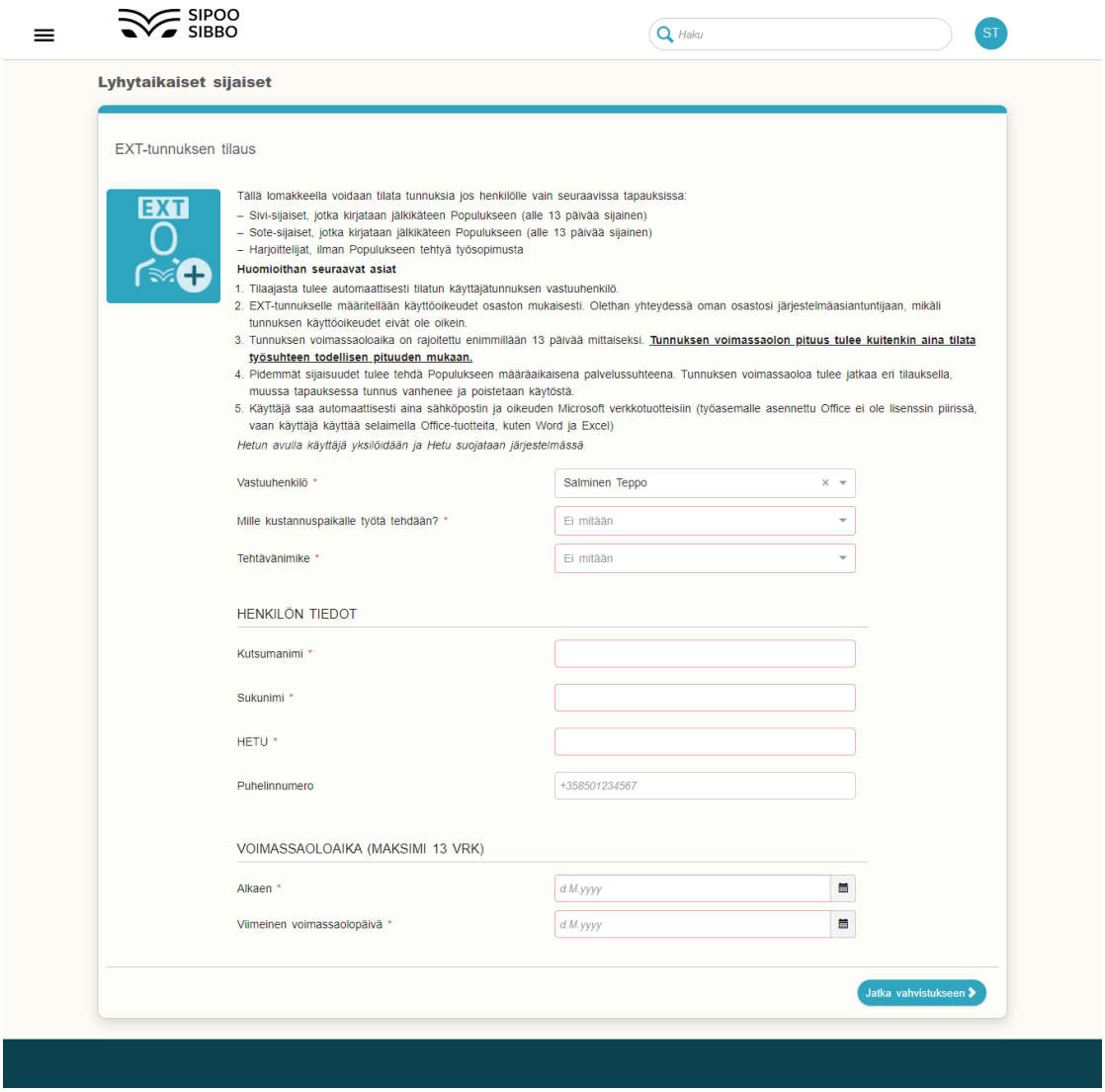
SIPOO
SIBBO



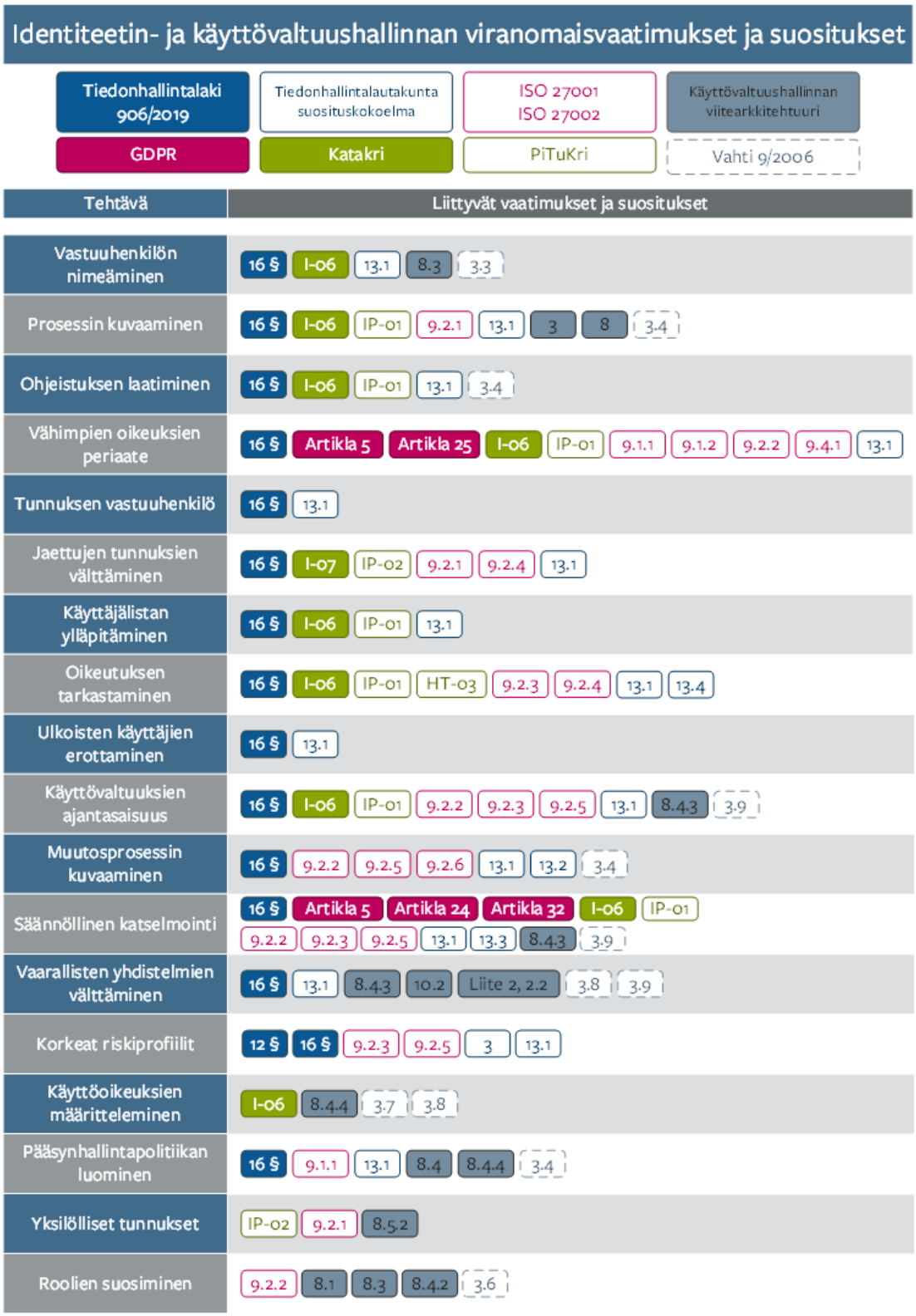
TILAUSLOMAKE – TOIMITTAJAT JA OSTOPALVELUTYÖNTEKIJÄT



TILAUSLOMAKE – LYHYTAIKAISET SIJAISET



IDENTITEETIN- JA KÄYTTÖVALTUUSHALLINNAN VIRANOMAISVASTUUS JA SUOSITUKSET



Identiteetin- ja käyttövaltuushallinnan viranomaisvaatimukset ja suositukset

Tiedonhallintalaki 906/2019
EU:n yleinen tietosuoja-asetus (GDPR)
Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta - http://urn.fi/URN:ISBN:978-952-367-897-2
Katakri - https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille
PiTuKri - https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri
SFS-EN ISO/IEC 27001:2017 ja SFS-EN ISO/IEC 27002:2017
Käyttövaltuushallinnan viitearkkitehtuuri - https://www.kuntaliitto.fi/file/15588/download?token=ARa_OdrJ

Tehtävä	Tarkempi tehtävän kuvaus
Vastuuhenkilön nimeäminen	Käyttöoikeuksien hallintaan tulee nimetä vastuuhenkilö(t).
Prosessin kuvaaminen	Käyttäjätilien luontiin, hyväksymiseen, ylläpitoon ja poistamiseen tulee olla kuvattu menettely ja käyttöoikeuden tulee perustua tunnuksen saajan kanssa tehtyyn sopimukseen (esim. työsopimus, ostopalvelusopimus).
Ohjeistuksen laatiminen	Käyttöoikeuksien käsittely ja myöntäminen tulee ohjeistaa.
Vähimpien oikeuksien periaate	Järjestelmien käyttäjille annetaan vain ne tiedot, oikeudet tai valtuudet, jotka ovat työtehtävien kannalta tarpeellisia. Käyttöoikeudet on määriteltävä kullekin tietojärjestelmän käyttäjälle hänen tyypillisten työtehtäviensä perusteella ja vähimpien oikeuksien periaatetta noudattaen (Principle of Least Privilege).
Tunnuksen vastuuhenkilö	Jokaiselle käyttäjätunnukselle tulee olla nimetty vastuuhenkilö eli omistaja. Tunnuksen omistajuus on määriteltävä erikseen, jos myönnetään tunnuksia kone- tai palvelutileille, kuten esim. ohjelmistorobotiikan käyttöön.
Jaettujen tunnuksien välttäminen	Yhteiskäyttötunnuksia tulee käyttää vain erikseen hyväksytyissä poikkeustapauksissa. Jaettujen tunnuksien käyttö tulee dokumentoida.
Käyttäjälistan ylläpitäminen	Järjestelmään myönnetyistä käyttöoikeuksista tulee olla saatavilla ajantasainen tieto. Jokaisesta myönnetystä käyttöoikeudesta ja siihen tehdyistä muutoksista tulee jäädä merkintä lokiin (paperi tai sähköinen).
Oikeutuksen tarkastaminen	Käyttöoikeuden myöntämisen yhteydessä tulee tarkistaa, että henkilöllä on oikeutus käyttöoikeuden saamiselle sekä riittävä koulutus kyseisen järjestelmän käyttöön. Uudelta henkilöltä tulee tarkistaa henkilöllisyys rekrytointiprosessissa. Salassapito- tai vaitiolositoumusmenettely tulee olla käytössä.
Ulkoisten käyttäjien erottaminen	Organisaation ulkoiset ja sisäiset käyttäjät tulee olla eroteltavissa käyttäjätunnuksen perusteella, esim. EXT-etuliitteellä.
Käyttövaltuuksien ajantasaisuus	Tarpeettomat käyttäjätilit ja käyttöoikeudet tulee poistaa, kun niitä ei enää tarvita. Esimerkiksi käyttäjän lähtiessä organisaatiosta, vaihtaessa työtehtäviään tai, kun käyttäjätiliä ei ole käytetty ennalta määritellyn ajanjakson aikana.
Muutosprosessin kuvaaminen	Organisaatiolla on oltava selkeät ja toimivat menettelyt käyttäjien tehtävien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä niistä aiheutuvien toimenpiteiden tekemiseen.
Säännöllinen katselmointi	Käyttöoikeudet tulee katselmoida säännöllisesti, esim. 6kk välein, mutta vähintään 12kk välein. Katselmointi tulee dokumentoida.
Vaarallisten yhdistelmien välttäminen	Vaaralliset käyttöoikeusyhdistelmät on tunnistettava, dokumentoitava ja eriytettävä mahdollisuuksien mukaan. Mikäli tehtäviä ei voida eriyttää, tulee niistä syntyviä riskejä hallita riskienhallinnan keinoin. Vaarallinen yhdistelmä on kyseessä, jos henkilö käsittelee yksin väärinkäytös tai virhealttiissa prosessissa kaikkia tai useita tapahtumaketjun osia.
Korkeat riskiprofiilit	Käyttöoikeuksien hallinnassa tulee kiinnittää huomiota etenkin korkeamman riskiprofiilin rooleihin (kuten pääkäyttäjät, ylläpitäjät ja muut erityistä luotettavuutta edellyttävät työtehtävät) ja niihin liitettyihin käyttöoikeuksiin. Erityisrooleilla tulee olla erillinen haku- ja päätösprosessi.
Käyttöoikeuksien määritteleminen	Tietojärjestelmien käyttöoikeudet tulee olla määritelty.
Pääsynhallintapolitiikan luominen	Pääsynhallintapolitiikka on laadittava, dokumentoitava ja katselmoitava liiketoiminnallisten vaatimusten ja tietoturvavaatimusten perusteella. Politiikkaa luodessa on suositeltavaa käyttää riskienarviointia.
Yksilölliset tunnukset	Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet, jotka eivät muutu elinkaarensa aikana.
Roolien suosiminen	Käyttövaltuusroolien toteuttaminen tulee tehdä perustuen tehtäviin ja tehtävänimikkeisiin. Käyttövaltuuksien pyytämistä ja katselmointia on helpompi hallita tällaisten roolien tasolla kuin yksittäisten oikeuksien tasolla.