Heidi Lehtonen

Roolipohjainen käyttövaltuushallinta

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tieto- ja viestintätekniikka
Insinöörityö
20.3.2023

Tiivistelmä

Tekijä:	Heidi Lehtonen
Otsikko:	Roolipohjainen käyttövaltuushallinta
Sivumäärä:	39 sivua
Aika:	20.3.2023
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Monimuoto
Ohjaajat:	Osaamisaluepäällikkö Janne Salonen

Tässä opinnäytetyössä tarkastellaan roolipohjaista käyttövaltuushallintaa sekä teoriatasolla että käytännön tutkimuksen keinoin. Käyttövaltuudella yleisesti, tarkoitetaan henkilön tarvitsemaa tietojärjestelmää, fyysistä laitetta tai pääsyä rajoitettuun tilaan, joita ei voi käyttää ilman erillistä lupaa - käyttövaltuutta.

Opinnäytetyössä käsitellään ensiksi käyttövaltuushallintaa yleisellä tasolla, minkä avulla voidaan ymmärtää paremmin roolipohjaisen käyttövaltuushallinnan käsitettä. Tutkimusosuus rajoittuu toimeksiantajayrityksen ICT-ympäristöön, missä käyttövaltuuden tarve perustellaan aina henkilön työtehtävien hoitamisella. Opinnäytetyössä ei käsitellä henkilön vapaa-ajallaan käyttämiä laitteita tai tietojärjestelmiä, eikä muiden yritysten tapaa toteuttaa käyttövaltuushallintaa.

Roolipohjaisen käyttövaltuushallinnan perusperiaate on käyttövaltuusjoukon myöntäminen tai poistaminen henkilön tai useamman henkilön senhetkisiin työtehtäviin perustuen, sen sijaan että käyttövaltuudet myönnettäisiin ja poistettaisiin esim. järjestelmä tai laite kerrallaan.

Opinnäytetyön toimeksiantona on saada suunniteltua toimeksiantajayrityksen käyttövaltuushallintajärjestelmään kaksi käyttövaltuusroolia, jotka karkeasti jaoteltuna ovat tietoliikenneasiantuntija ja konesaliasiantuntija. Tutkimusosassa kartoitetaan em. roolien vaatimia käyttövaltuuksia, tilausprosessin nykytilaa, sekä vastataan roolien määrittelyyn liittyviin tietoturvakysymyksiin hyväksytysti.

Opinnäytetyön konkreettisena lopputuloksena syntyy ehdotelma tulevista käyttövaltuusrooleista.

Pohdinnassa analysoidaan tutkimuksen lopputulosta, sekä saavutettuja hyötyjä toimeksiantajayritykselle. Analysoidaan lopputulos myös käytettyjen työmenetelmien ja oman henkilökohtaisen oppimisen kautta.

Avainsanat: IAM, käyttövaltuushallinta, tietoturva, RBAC, rooli

Abstract

Author:	Heidi Lehtonen
Title:	Role Based Access Control
Number of Pages:	39 pages
Date:	20 March 2023
Degree:	Bachelor of Engineering
Degree Programme:	Information technology
Professional Major:	Blended learning
Supervisors:	Janne Salonen, Head of School (ICT)

In this thesis, role-based access control is examined both on a theoretical level and with the means of practical research. Identity and access management in general means an information system, physical device, or access to a restricted space that a person needs, which cannot be used without a separate permit - authorization.

The thesis first deals with identity and access management at a general level, which helps to better understand the concept of role-based access control. The research part is limited to the ICT environment of the commissioning company, where the need for authorization is always justified by the performance of the person's work tasks. The thesis does not deal with devices or information systems used by a person in their free time, nor with the way other companies implement identity and access management.

The basic principle of role-based access control is to grant or remove a set of user authorizations based on the current work tasks of a person or several persons, instead of granting and removing user authorizations e.g., system or device at a time.

The assignment of the thesis is to have two expert roles created in the user authorization management system of the commissioning company, which roughly divided are ICT expert and data center expert. In the research part, the user authorizations required by the roles are mapped, the current state of the order process, and the information security questions related to the definition of the roles are answered with approval.

The result of the thesis creates the necessary user authorization roles. Alternatively, the result is a theoretical explanation of the requirements of the roles.

In the reflection, the result of the research is analyzed, as well as the achieved benefits for the commissioning company. The result will also be analyzed through the working methods used and one's own personal learning.

Keywords: IAM, Identity and Access Management, Information security, RBAC, role

Sisällys

Lyhenteet ja käsitteet

ICT: Information and communication technology. (Suom. tieto- ja viestintätekniikka

IT: Information Technology. (Suom. tietotekniikka)

RBAC: Role Based Access Control. (Suom. roolipohjainen käyttövaltuushallinta)

ARBAC: Attribute-Enabled Role Based Access Control Model. (Suom. Attribuuttipohjainen käyttövaltuushallintamalli

IDM: Identity Management. (Suom. identiteetinhallinta)

IAM: Identity and Access Management. (Suom. käyttövaltuushallinta)

HVA: High value assets. (Suom. arvokas tieto.)

SSO: Single sign-on. (Suom. kertakirjautuminen)

MFA: Multifactor authentication. (Suom. monivaiheinen tunnistautuminen)

GDPR: General Data Protection Regulation. (Suom. yleinen tietosuoja-asetus)

Zero Trust: Nollaluottamusmalli

SOX: Sarbanex-Oxley. Käytetään lyhenteenä Sarbanex-Oxleyn laista

SEC The Securities and Exchange Commission. Yhdysvaltain arvopaperimarkkinoita valvova elin.

NDA: Non-disclosure agreement. (Suom. salassapitosopimus)

OIKEUS: Puhekielen lyhenne sanasta käyttöoikeus, josta käytetään myös termiä käyttövaltuus. Esim. ”antaa oikeudet”, on sama kuin ”myöntää käyttövaltuus)

SUPO: Suojelupoliisi

EU: Euroopan unioni

OTO: Oman toimen ohella

TURSEL: Turvallisuusselvitys

KÄYTTÖOIKEUS: Sama kuin käyttövaltuus

1 Johdanto

Opinnäytetyössä tarkastellaan käyttövaltuushallintaa (IAM), sekä roolipohjaista käyttövaltuushallintaa (RBAC). Roolipohjaisen käyttövaltuushallinnan osalta tarkastellaan sekä RBAC malleja ja standardeja, että roolipohjaista käyttövaltuushallintaa yleisesti.

Tietolähteinä tutkimuksessa käytetään omaa ICT-alan työkokemusta, internetistä löytyviä lähteitä, toimeksiantajayrityksen olemassa olevaa dokumentaatiota ja prosessikuvauksia, sekä työpaikalla suoritettavia henkilöhaastatteluita. Tutkimuksen kohteena on ICT-ala, tarkemmin toimeksiantajayrityksen ICT-ympäristö.

Käyttövaltuuksia tarvitsevat yritysten ja organisaatioiden työntekijät, jotta he pystyvät suoriutumaan työtehtävistään. Järjestelmät, laitteet tai kulun salliminen tiettyyn tilaan, joiden käyttämiseen tarvitaan perusteltu lupa – käyttövaltuus, ovat esimerkkejä modernin työelämän työkaluista, joita ilman työtehtävien suorittaminen ei ole mahdollista.

1.1 Opinnäytetyön tavoitteet

Opinnäytetyön tavoitteena on saavuttaa ymmärrys käyttövaltuushallinnasta yleisesti, sekä roolipohjaisesta käyttövaltuushallinnasta niin yleisesti kuin mallien ja standardien kautta. Opinnäytetyössä tarkastellaan myös käyttövaltuuksien hallintaan liittyviä lakeja ja säädöksiä osana käyttövaltuushallintaan liittyviä tietoturvakysymyksiä.

Opinnäytetyön aihe valikoitui tarpeesta selkeyttää toimeksiantajayrityksessä aloittavien, tai yrityksen sisällä tiettyihin asiantuntijatehtäviin siirtyvien uusien asiantuntijoiden käyttövaltuuksiin liittyvää tilausprosessia, luomalla käyttövaltuushallintajärjestelmään kaksi asiantuntijaroolia, jotka ovat karkean

ylätasoisesti jaoteltuna tietoliikenneasiantuntija ja konesaliasiantuntija. Tällä hetkellä prosessi koetaan haasteelliseksi ja ajankäytön näkökulmasta liialliseksi.

Tutkimusosiossa vastataan tunnistettuihin haasteisiin etsimällä niihin ratkaisua roolipohjaisen käyttövaltuushallinnan keinoin, jolloin lopputuloksena syntyy ehdotelma toivotuista käyttövaltuusrooleista.

Opinnäytetyön tekemisessä käytettävät työmenetelmät ovat osana tutkimusta. Työmenetelmiä analysoimalla saavutetaan ymmärrys mm. käyttövaltuusroolien luomiseen sisältyvistä työvaiheista, työvaiheisiin kuluneesta ajasta, oleellisista tietoturvakysymyksistä, ajankäytön järkevyydestä, sekä tuotetun dokumentaation laadusta.

1.2 Toimeksiantajayrityksen esittely

Yrityksessä on noin 400 työntekijää ja yritys on osa isompaa konsernia. Yritys tuottaa asiakkailleen monipuolisia ICT-palveluita.

Yrityksen asiakkaita ovat mm. yritykset, julkishallinto, rahoituslaitokset ja teollisuussektori.

1.3 Opinnäytetyön rakenne

Opinnäytetyö jakautuu kolmeen pääosaan:

- teoriaosuus
- tutkimusosuus
- pohdinta.

Teoriaosuus aloitetaan käsittelemällä käyttövaltuushallintaa yleisesti, sekä tutustutaan aiheen kannalta oleellisiin lakeihin ja säädöksiin. Tämän jälkeen pohditaan roolipohjaisen käyttövaltuushallinnan olemassaoloa sekä RBAC mallien ja standardien kautta, että yleisenä käsitteenä.

Tutkimusosassa kuvataan tarkemmin toimeksiantajayrityksen ilmaisema tarve määritellä käyttövaltuushallintajärjestelmään kaksi käyttövaltuusroolia erilaisille asiantuntijatehtäville. Tarkastellaan, voidaanko pitäytyä kahdessa roolissa, vai onko rooleille tarve luoda erilaisia tasoja ja variaatioita ja mitkä ovat niiden perusteet? Pureudutaan aiheen kannalta oleellisiin tietoturvakysymyksiin sekä yleisellä tasolla, että asiakasyritysten tietoturvavaatimusten erityispiirteiden kautta.

Viimeisessä, eli pohdintaosassa käsitellään tutkimusosuutta, tutkimuksessa käytettyjä työmenetelmiä ja tutkimuksen lopputulosta. Analysoidaan tutkimuksen lopputulosta saavutetulla konkreettisella hyödyllä, käytettyjen työmenetelmien kautta, sekä kokemuspohjaisesti – mitä opin, mitä tunsin?

2 Käyttövaltuushallinta

Käyttövaltuushallinnan perusperiaate on yksikertainen. Sen avulla hallitaan pääsyä tietojärjestelmiin, tietoon, laitteeseen tai fyysiseen tilaan.

Pääsyn rajoittamisesta fyysiseen tilaan käytetään nimitystä kulunvalvonta (Göös, J, 2018). Tässä opinnäytetyössä ei erikseen käsitellä kulunvalvontaa, vaan keskitytään enemmän tietojärjestelmiä koskevaan käyttövaltuushallintaan.

Käyttövaltuushallinta (IAM) on liiketoimintaprosessien, käytäntöjen ja teknologioiden kehys, joka helpottaa sähköisten tai digitaalisten identiteettien hallintaa. Kun IAM-kehys on käytössä, voidaan organisaatioissa hallita käyttäjien pääsyä kriittisiin tietoihin. (Gittlen, Rosengrance, 2021)

Tarkasteltaessa käyttövaltuuksia työntekijän tarvitsemina työkaluina, on käyttövaltuuksien tarve aina pystyttävä perustelemaan henkilön senhetkisillä työtehtävillä. Työntekijän näkökulmasta pitäisi kuitenkin olla mahdollisimman selkeää, miten ja mistä käyttövaltuuksia voi saada ja millä perusteella.

> Työntekijän näkökulmasta käyttövaltuudet kuuluvat jokaiselle, koska kaikki tarvitsevat niitä. Työntekijälle pitäisi myös olla selvää,

> miten käyttövaltuuksia voi saada. Lisäksi prosessin pitää olla turvallinen. Ennen kaikkea on siis kyse prosesseista ja tavoitteista kuten automaatio, jäljitettävyys sekä helppous. (Nykänen. H, 2021)

Kuten Nykänen kirjoittaa artikkelissaan Telia Finlandin verkkosivuilla, työntekijälle pitäisi olla selviö, mitä käyttövaltuuksia hän tarvitsee ja kuinka hänen tulee toimia saadakseen ne käyttöönsä. Työntekijän itsensä ei pitäisi joutua selvittämään käyttövaltuuksien tilaamiseen liittyviä ongelmakohtia, vaan hänellä tulisi olla helposti saavutettavissa oleva, ajantasainen, ymmärrettävä ja luotettava ohjeistus.

Nykäsen mainitsema jäljitettävyys on tietoturvan kannalta oleellinen tekijä. Tilanteessa, jossa epäillään tapahtuneen tietoturvapoikkeama, täytyy pystyä nopeasti ja luotettavasti selvittämään, kenellä kaikilla on pääsy suojattuun tietoon, ja kuka tietoa on käsitellyt ja milloin. Tietoturvapoikkeaman käsitettä avataan tarkemmin kappaleessa 3.3.

2.1 Identiteetin elinkaari

Edellisessä kappaleessa todettiin, että käyttövaltuushallinta tarkoittaa sähköisten tai digitaalisten identiteettien hallintaa.

> Digitaalinen identiteetti on kokoelma henkilöön liittyviä ominaisuuksia. (Laakkonen, 2019)

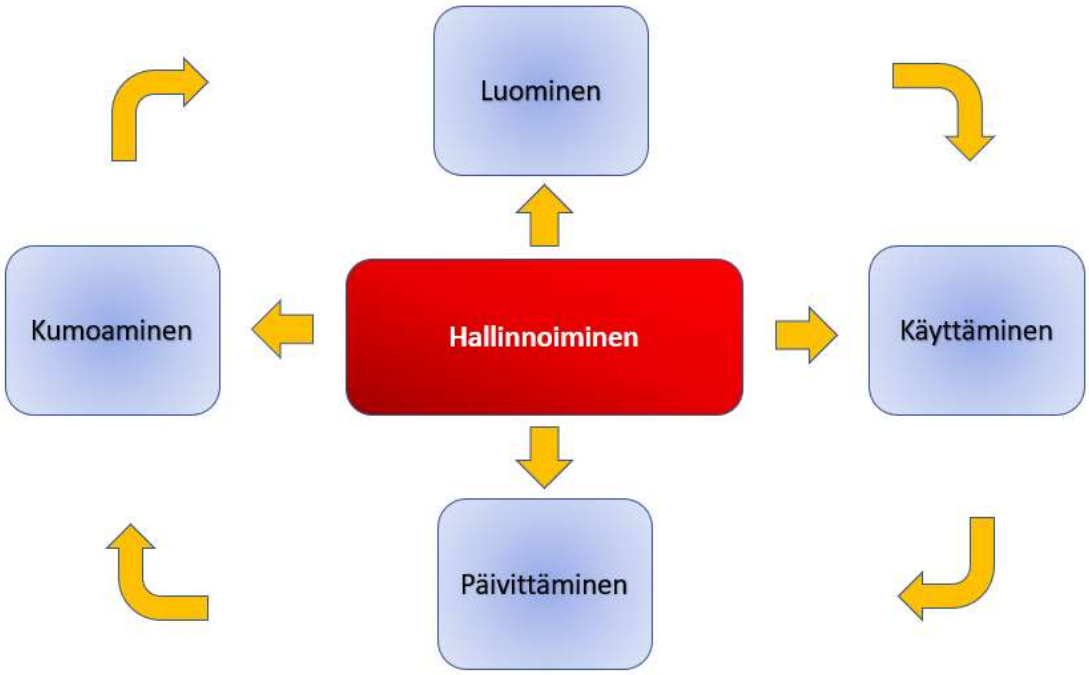
Digitaalisia identiteettejä voi henkilöllä olla yksi tai useampia ja ne voivat liittyä yhteen tai useampaan palveluun. Digitaalinen identiteetti löytyy usein myös vainajalta, koska internetissä julkaistut asiat säilyvät siellä käytännössä ikuisesti. (Laakkonen, 2019)

Kuvattaessa identiteetin elinkaarta (Bertino, E. Takahashi, K. 2010), havaitaan että kaiken keskiössä on hallinnoiminen. Käyttövaltuushallinnan yksi tärkeimpiä kulmakiviä onkin sujuva ja luotettava hallittavuus.

Tarkasteltaessa identiteetin elinkaarta kuvassa 1. myötäpäivään, ensiksi identiteetti luodaan. Kun identiteetti on luotu, sitä voidaan käyttää. Tärkeä osa identiteetin elinkaarta on ymmärtää, ettei elinkaari pääty identiteetin käyttämiseen, vaan kaikkea ohjaa keskiössä oleva hallinnoiminen.

Jatkettaessa elinkaarta edelleen myötäpäivään, havaitaan että käytössä olevaa identiteettiä tulee päivittää, kun havaitaan tarpeita muutoksille. Päivittäminen voi tarkoittaa paitsi käyttövaltuuksien laajentamista myös niiden supistamista tai muuttamista.

Viimeisenä, muttei vähäisimpänä, on elinkaarelle kuvattu kumoaminen. Jos henkilö poistuu organisaation palveluksesta kokonaan, tai vaihtaa tehtäviä, tulee organisaatiolla olla luotettava prosessi tarpeettomiksi jääneiden käyttövaltuuksien poistamiselle. Tarpeettomien käyttövaltuuksien voimassaolo voi olla huomattava tietoturvariski.



Kuva 1. Identiteetin elinkaari (Bertino, E & Takahashi, K. 2010)

Käyttövaltuuksien hallinnointiin liittyy elinkaaren lisäksi useita tietoturvakysymyksiä, sekä ohjaavia lakeja ja säädöksiä. Esimerkkeinä työelämän tietosuojalaki, eli laki yksityisyyden suojasta työelämässä (759/2004) ja EU:n yleinen tietosuoja-asetus GDPR (eng. General Data Protection Regulation).

Kappaleissa 3.4.1. ja 3.4.2. käsitellään tarkemmin lakia yksityisyyden suojasta työelämässä sekä EU:n yleistä tietosuoja-asetusta GDPR:ää.

3 Käyttövaltuushallinta ja tietoturva

Käyttövaltuuksien hallintaan liittyy monia tietoturvaan liittyviä huomioita. Niitä ei voi jättää käsittelemättä asian vaatimalla vakavuudella, kun mietitään toimintamalleja. Kappale 3 käsittelee kokonaisuudessaan oleellisia tietoturvaan liittyviä huomioita parhaiden käytäntöjen, sekä lakien ja asetusten kautta.

3.1 Käyttövaltuushallinnan parhaita käytäntöjä

3.1.1 Zero Trust toimintamalli

Lähtökohtana voidaan pitää Zero Trust toimintamallia (suom. nollaluottamusmalli), jonka perusperiaate on, että henkilöllisyyden tulee aina perustua todennukseen, ei luottamukseen.

Magnusson kutsuu implisiittiseksi luottamusominaisuudeksi tilannetta, missä järjestelmä ”muistaa” käyttäjänsä, eikä käyttäjän henkilöllisyyttä todenneta erikseen jokaisella kirjautumisella. Kyseessä on huomattava tietoturvariski, koska tilanne mahdollistaa luvattoman tahon pääsyn järjestelmiin helposti, muistettujen käyttövaltuustietojen avulla. Zero Trust toimintamalli kumoaa implisiittiseen luottamukseen perustuvan toimintatavan, koska sen avulla voidaan taata järjestelmää käyttävän henkilön todella olevan se, jonka tunnuksia käytetään kirjautumiseen. Zero Trust tukee parhaita käytäntöjä ja tietoturvaa, paitsi estämällä tahallisen luvattoman kirjautumisen, myös estämällä tahattomasti kirjautuvien luvattomien käyttäjien pääsyn yrityksen resursseihin. (Magnusson, A. 2023, 1.)

3.1.2 Arvokkaan tiedon (HVA) tunnistaminen ja suojaus

Yksi tietoturvan avaintekijä on arvokkaan tiedon eli HVA:n (eng. High Value Assets) suojaaminen. Jotta arvokas tieto voidaan suojata, täytyy se ensiksi tunnistaa. Tunnistamiseen liittyvät mm. seuraavat tekijät. Mitä on arvokas tieto? Mihin se on tallennettu? Miten sitä käytetään? Millä sovelluksilla ja/tai työkaluilla tietoon pääsee käsiksi? Yritykset määrittelevät arvokkaan tiedon yleensä sen perusteella, mikä aiheuttaisi isoimman uhan yritykselle kadotessaan tai joutuessaan vääriin käsiin. Esimerkkinä arvokkaasta tiedosta voidaan käyttää arkaluontoisia tietoja, kuten liikesalaisuuksia tai asiakkaiden ja työntekijöiden henkilökohtaisia tunnistetietoja. (Magnusson, A. 2023, 2.)

3.1.3 Vahvojen salasanojen käytäntö

Käyttövaltuushallinnan teknologioiden voidaan ajatella olevan yhtä vahvoja, kuin niitä tukevat parhaat käytännöt. Esimerkkinä vahvojen salasanojen käytänteet. Erityisesti jos yrityksellä on käytössään SSO-työkaluja, on tärkeää varmistaa, että käyttäjät eivät aseta helposti arvattavia tai muuten turhan yksinkertaisia salasanoja. Helposti arvattavia salasanoja voivat olla esimerkiksi lemmikkien tai perheenjäsenten nimet, tai henkilön omat ja hänen lähipiirinsä merkkipäivät. Salasanavaatimusten tulee olla riittävän monimutkaisia, jotta vahvojen salasanojen avulla voidaan paremmin ehkäistä kyberhyökkäyksiä. Vaikka salasana täyttäisi vahvan salasanan määritelmän ja olisi lisäksi riittävän uniikki, se täytyy vaihtaa riittävän usein. Tarpeeksi tiheä salasanan vaihtoväli ei luotettavasti toteudu kehotuksin ja ohjeistuksin, vaan salasanan vaihdon tulee olla pakotettu riittävän usein. Jos käytössä on MFA-todennus, sen käyttö ei poista tarvetta salasanan vahvuudesta ja tarpeeksi tiheästä vaihtovälistä. (Magnusson, A. 2023, 3.)

3.1.4 MFA-työkalut

MFA-työkalut (eng. Multi Factor Authentication) yksinkertaistavat todennusprosessia ja vahvistavat käyttäjän henkilöllisyyden. Pelkät kirjautumistiedot eivät riitä varmistamaan kirjautujan henkilöllisyyttä, erityisesti jos on olemassa riski,

että järjestelmä ”muistaa” kirjautumistiedot. MFA työkalut käyttävät todentamiseen yleensä jotain seuraavista menetelmistä:

- Biometrinen todennus (esim. sormenjäljet tai kasvojentunnistus)
- Hallussapitotodennus (esim. kertaluonteisen salasanan lähettäminen käyttäjän henkilökohtaiseen laitteeseen, kuten älypuhelin)
- Tietojen todennus (esim. turvakysymyksiin vastaaminen)
- Käyttäjän sijainti- tai aikatiedot.

(Magnusson, A. 2023, 4.)

3.1.5 Vähimmän pääsyn periaate

Vähimmän pääsyn periaate (eng. Least Priviledge) on roolien ja käyttövaltuuksien kannalta yksi parhaista käytännöistä. Vähimmän pääsyn periaate auttaa rajoittamaan pääsyä ja käyttöoikeuksia mahdollisimman paljon, mutta siten etteivät rajoitukset häiritse päivittäistä työnkulkua. (Magnusson, A. 2023, 6.)

3.1.6 Säännölliset auditoinnit

Säännöllisen auditoinnin tulisi aina olla osa yrityksen turvallista ja toimivaa käyttövaltuushallinnan prosessia. Esimerkiksi tarkastelemalla käyttölokeja ja käyttövaltuuksia säännöllisesti, voidaan turhia käyttövaltuuksia poistaa ja siten minimoida kyberhyökkäyksille alttiina olevaa hyökkäyspintaa. Yrityksissä ja organisaatioissa saatetaan tämän tästä ottaa käyttöön uusia sovelluksia ja työkaluja ja työntekijät saattavat haluta päästä niihin heti käsiksi. Käyttövaltuuksien ja niiden tason tulisi kuitenkin olla aina perustella henkilön työtehtävillä, ei sillä mihin ”olisi kiva” päästä käsiksi. (Magnusson, A. 2023, 9.)

3.2 Turvallisuusselvitykset

Kappaleessa 3.1.2. tutustuimme arvokkaan tiedon käsitteeseen. Kun arvokas tieto on tunnistettu, se täytyy suojata. Yksi suojaukseen käytetyistä menetelmistä on turvallisuusselvitys.

Turvallisuusselvitys voidaan tehdä yrityksestä tai henkilöstä.

Turvallisuusselvityksen yrityksestä suorittaa suojelupoliisi, ellei kyseessä ole puolustusvoimien antama tehtävä tai puolustusvoimiin liittyvä hankinta. Jälkimmäisessä tapauksessa yritysturvallisuusselvityksen laatii pääesikunta.

Turvallisuusselvityksen tarkoitus on suojella Suomen turvallisuutta. Turvallisuusselvityksistä säädetään turvallisuusselvityslaissa (19.9.2014/726). (Finlex, 2023)

Suojelupoliisin verkkosivuilla kuvataan turvallisuusselvityksen käsitettä seuraavasti:

> Suojelupoliisi voi tehdä yritysturvallisuusselvityksen suomalaisesta yrityksestä, joka toimii viranomaisen sopimuskumppanina ja tarvitsee oikeuden käsitellä turvallisuusluokiteltuja kansallisia tai kansainvälisiä viranomaistietoja. Jos yrityksen on tarkoitus hoitaa puolustusvoimien antamaa tehtävää tai yritys liittyy puolustusvoimien hankintoihin, yritysturvallisuusselvityksen laatii pääesikunta. (Suojelupoliisi, 2023)
>
> Suomen tärkeimpiä tuotantotekijöitä on osaamiseen liittyvä tieto. Se löytyy yhä useammin tietojärjestelmistä, jotka ovat kiinni verkossa. (Suojelupoliisi, 2023)
>
> Kun yhteiskunnan kriittiset toimet siirtyvät yhä enemmän verkkomaailmaan, järjestelmien riski joutua laittoman tiedustelun kohteeksi kasvaa. Vaikka vakoilua tapahtuu edelleen myös perinteisin menetelmin, internet on laajentanut keinovalikoimaa. (Suojelupoliisi, 2023)
>
> Talouden digitalisaatio on monimuotoistanut kansallisen turvallisuuden uhkakuvia. Uusi ilmiö ovat esimerkiksi ulkoistettuihin alihankinta- tai palveluntuottajaketjuihin kohdistuvat hyökkäykset, joiden kautta voi päästä varsinaisen tiedustelun kohteen järjestelmiin. (Suojelupoliisi, 2023)

3.3 Tietoturvapoikkeama

Tietoturvapoikkeama tarkoittaa esimerkiksi tietojen kalastelua, tietomurtoja, palvelunestohyökkäyksiä tai näiden yrityksiä. (Kyberturvallisuuskeskus, 2023)

Tietoturvapoikkeama voi olla myös tahaton, mutta sen seurauksena yrityksen tai organisaation vastuulla olevien tietojen luottamuksellisuus tai palveluiden käytettävyystaso voi olla vaarantunut. (Kyberturvallisuuskeskus, 2023)

Tietoturvapoikkeamasta voi ilmoittaa kuka tahansa ja yrityksillä tulisi aina olla ajantasainen ohjeistus tietoturvapoikkeamasta ilmoittamiselle, jotta henkilöstöllä on tarvittava ymmärrys tietoturvapoikkeaman käsitteestä, ilmoittamisvelvollisuudesta ja käytännön ilmoittamistavoista. (Kyberturvallisuuskeskus, 2023)

3.4 Lainsäädäntö ja asetukset

3.4.1 EU:n yleinen tietosuoja-asetus - GDPR

Vielä joitain vuosia sitten, oli voimassa henkilötietolaki, puhekielessä myös ”laki henkilötietojen käsittelystä” (Laki 523/1999). Henkilötietolaki on sittemmin kumottu ja korvattu 1.1.2019 voimaan astuneella tietosuojalailla (1050/2018). (Finlex, 2018)

> Tietosuojalaki (1050/2018) täsmentää ja täydentää EU:n yleistä tietosuoja-asetusta ja sen kansallista soveltamista. Laissa säädetään muun muassa tietosuoja-asioita valvovan viranomaisen nimittämisestä ja organisaatiosta sekä sen toimivaltuuksista. (Tietosuojalaki.fi, 2023)

GDPR, eli EU:n yleinen tietosuoja-asetus on lyhenne englanninkielisestä termistä General Data Protection Regulation (suom. yleinen tietosuoja-asetus). Kyseessä on laki, joka säätelee henkilötietojen käsittelyä ja sen soveltaminen aloitettiin EU-maissa vuonna 2018. GDPR antaa paremman suojan henkilötiedoilla ja tarjoaa keinoja henkilötietojen käsittelyn hallintaan.

Lainsäädännön uudistuksen tavoitteena oli:

- Parantaa tietosuojaoikeuksia ja henkilötietojen suojaamista
- Vastata tietosuojakysymyksiin, jotka ovat seurausta digitalisaatiosta ja globalisaatiosta
- Yhtenäistää EU-maiden tietosuojasääntelyä

- Edistää digitaalisten sisämarkkinoiden kehittymistä.

(Tietosuojavaltuutetun toimisto, 2023)

Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Seuraava luetelma on suora lainaus Tietosuojavaltuutetun toimiston verkkosivuilta ja se käsittää oleelliset kohdat siitä mitä on henkilötieto:

- nimi
- kotiosoite
- sähköpostiosoite, kuten etunimi.sukunimi@yritys.com
- puhelinnumero
- henkilökortin numero
- auton rekisterinumero
- paikannustiedot
- IP-osoite
- potilastiedot
- isovanhempien perinnöllisiä sairauksia koskevat tiedot.

(Tietosuojavaltuutetun toimisto, 2023)

GDPR:n mukaisesti henkilöllä on mm. oikeus tietää millaisia henkilötietoja organisaatiolla on henkilöstä ja mihin tarkoitukseen henkilötietoja käytetään. Henkilö voi pyytää virheellisten henkilötietojen korjaamista, henkilötietojen rajoittamista tai poistamista kokonaan. Henkilöllä on oikeus olla joutumatta automaattisen päätöksenteon kohteeksi yrityksen hallussa olevien henkilötietojensa perusteella. Jos korjauspyyntö tehdään, organisaation on vastattava siihen kuukauden kuluessa. Henkilötietojen poistoon liittyvissä pyynnöissä yrityksen täytyy poistaa ne, ellei säilyttämiseen tai käsittelyyn ole laillista perustetta. (Tietosuojavaltuutetun toimisto, 2023)

Organisaation täytyy pyydettäessä toimittaa tieto, onko heillä pyytäjän henkilötietoja, sekä vahvistaa ettei henkilötietoja käsitellä. Tiedot tulee toimittaa yleisesti käytetyssä sähköisessä muodossa, ellei toisin pyydetä. Tarkkaa

jäljennöstä ei kuitenkaan tarvitse toimittaa, ellei se vaikuta haitallisesti muiden oikeuksiin. (Tietosuojavaltuutetun toimisto, 2023)

Organisaatio saa käsitellä henkilötietoja laissa määrättyjen perusteiden mukaisesti. Perusteita voivat olla mm. sopimus, rekisteröidyn suostumus, yleinen etu, elintärkeiden tietojen suojaaminen tai rekisterinpitäjän lakisääteinen velvoite. (Tietosuojavaltuutetun toimisto, 2023)

Tietosuojavaltuutetun nimeäminen organisaatiossa tulee kyseeseen, jos yritys laajamittaisesti käsittelee arkaluonteista tietoa, seuraa ihmisiä säännöllisesti ja järjestelmällisesti, tai organisaatio luetaan julkishallinnon toimijaksi (muu kuin tuomioistuin). (Tietosuojavaltuutetun toimisto, 2023)

Organisaation työntekijöiden määrän ylittäessä 250, on sen laadittava seloste henkilötietojen käsittelytoiminnasta. Alle 250 henkilön organisaatiossa selosteen laatiminen tulee kyseeseen, kun henkilötietojen käsittely on jatkuvaa, henkilötietojen käsittelystä aiheutuu riski rekisteröidyn oikeuksille tai organisaatio käsittelee arkaluontoisia tietoja. (Tietosuojavaltuutetun toimisto, 2023)

Tietosuojaperiaatteita tulee noudattaa kaikissa henkilötietojen käsittelyn vaiheissa ja organisaation on pystyttävä osoittamaan, että se noudattaa tietosuojaperiaatteita. (Tietosuojavaltuutetun toimisto, 2023)

3.4.2 Työelämän tietosuojalaki, eli laki yksityisyyden suojasta työelämässä (759/2004)

Palataan ajassa muutama vuosi taaksepäin ja tarkastetaan tilannetta hieman lisää ennen GDPR:n aikakautta. Anunti avaa tilannetta artikkelissaan seuraavasti:

> Aivan tyhjästä ei lähdetty liikkeelle, sillä tietosuojasta oli säännelty aiemmin kansallisessa henkilötietolaissa. Lisäksi Suomessa työntekijöiden henkilötietojen käsittelyä ohjaa jo yli 10 vuotta ennen GDPR:ää voimaantullut työelämän tietosuojalaki eli laki yksityisyyden suojasta työelämässä (759/2004). Viime kädessä yksityisyyden

suojasta on säädetty myös perustuslaissa (731/1999). (Anunti, T. 2022)

Vaikka GDPR toi mukanaan paljon uusia säädöksiä, ei sitä ennen oltu tyhjän päällä ensinkään.

3.4.3 Tietosuoja käyttövaltuushallinnassa

Kappaleessa 3 on tietoturvakysymyksissä tähän mennessä sivuttu mm. EU:n yleistä tietosuoja-asetusta GDPR:ää ja työelämän tietosuojalakia (759/2004).

Nykypäivän työelämän yleisimpiä sähköisiä työkaluja ovat erilaiset viestintävälineet, joita lisäksi voivat koskea omat säädöksensä. Käytetään esimerkkinä sähköpostia.

Viestintävälineiden, kuten sähköpostin käyttöä varten vaaditaan aina erillinen käyttövaltuus, joka on yleensä henkilökohtainen ja näin ollen sidoksissa luonnolliseen henkilöön. On siis huomionarvoista nostaa käsittelyyn myös perustuslaissa säädetty kirjesalaisuus ja sähköisen viestinnän tietosuojalaki (7.11.2014/917). (Finlex, 2023)

3.4.4 Sähköisen viestinnän tietosuojalaki (7.11.2014/917) ja kirjesalaisuus

Tämän päivän viestintä on muuttunut entistä enemmän sähköiseksi ja yritysten ja organisaatioiden käytössä on paljon tietojärjestelmiä ja sovelluksia, joita voidaan käyttää viestintään. Käyttövaltuushallinnan keinoin mahdollistetaan työntekijöille henkilökohtaisten viestintävälineiden käyttö, esimerkkinä sähköpostin käyttäminen.

Sähköpostia koskee kirjesalaisuus. Kirje tarkoittaa kirjallista viestiä joko luonnolliselta- tai juridiselta henkilöltä toiselle. (Wikipedia, 2022)

Kirjesalaisuudesta säädetään perustuslaissa ja se koskee kaikkia kirjeitä, riippumatta kirjoitus- tai lähetystavasta. Näin ollen laki koskee myös sähköpostia. (Laki24, 2023)

Kirjesalaisuus turvaa kirjeen lähettäjän oikeuden saattaa kirje vastaanottajalle luottamuksellisesti, ilman että muu kuin vastaanottaja avaa kirjeen tai muulla tavoin saa tietää kirjeen sisällöstä. Kirjesalaisuudesta voi luopua ainoastaan henkilö, jota salaisuus suojaa, eli lähettäjä tai vastaanottaja. Esimerkiksi vastaanottajan ei tarvitse pitää kirjeen sisältöä salassa, vaan hän voi vapaasti päättää mitä tekee kirjeelle, esim. säästää, tuhoaa tai näyttää/kertoo kolmannelle osapuolelle. Jos vastaanottaja päättää toimia edellä mainitulla tavalla, kyseessä ei ole kirjesalaisuuden rikkominen, koska vastaanottajalla on oikeus luopua kirjesalaisuudesta kirjeen vastaanotettuaan. Poikkeuksen kirjesalaisuuteen muodostaa vainaja, koska nykykäsityksen mukaan ihmisen perusoikeudet eivät koske vainajaa. (Laki24, 2023)

Sähköisen viestinnän tietosuojalain (516/2004) tarkoituksena on turvata sähköisen viestinnän luottamuksellisuus ja yksityisyyden suojan toteutuminen. Laissa säädetään tarkemmin nimenomaan sähköiseen viestintään liittyen. (Finlex, 2023)

3.4.5 Sarbanes-Oxley (SOX) -laki

2000-luvun alkupuolella Yhdysvalloissa tapahtuneiden isojen yrityspetosten seurauksena astui vuonna 2002 voimaan Sarbanes-Oxleyn laki, jota kutsutaan myös SOX-laiksi.

SOX-lakiin sisältyi joukko tiukkoja vaatimuksia, joiden tarkoituksena oli pyrkiä estämään talouspetoksia, joiden tekemiseen voitiin käyttää hyväksi yrityksen tietojärjestelmiä.

SOX-lain säätämisen seurauksena yritykset alkoivat panostaa käyttövaltuuksien hallinnan parantamiseen erilaisten hallintajärjestelmien avulla. SOX-lain

vaatimuksiin perustuen yrityksillä oli velvollisuus olla tietoisia kuka heidän tietojärjestelmiään käyttää ja milloin järjestelmiin on kirjauduttu sisään tai niistä on kirjauduttu ulos. Kirjautumisaikaleimojen lisäksi yrityksillä tuli olla tiedossaan mitä heidän tietojärjestelmissään on tehty, millaisilla valtuuksilla ja mitä muutoksia on tehty. (Bednarz 2005; Snellman 2010.)

Vaikka Ferraiolo ja Kuhn esittelivät ensimmäisen RBAC-mallin Baltimoressa jo vuonna 1992, suunniteltiin roolipohjaisen käyttövaltuushallinnan standardi erityisesti vastaamaan vuonna 2002 voimaantulleen SOX-lain vaatimuksiin, jotka voidaan tiivistää seuraavasti:

- Tietojärjestelmien käyttövaltuuksien hallintaan ja valvontaan tulee olla kattava prosessi
- Prosessin tulee olla tehokas ja tietoturvallinen ja siinä tulee huomioida sekä käyttövaltuuksien myöntäminen että poistaminen
- Arkaluontoisen tiedon osalta yrityksen täytyy pystyä varmistamaan, että vain valtuutetuilla henkilöillä on tietoon pääsy.

(Snellman, K. 2010.)

Sarbanes-Oxley laki koskee ainoastaan tiettyjä yrityksiä. Sellaisia ovat mm. SEC:in alaiseen pörssiin (Eng. The Securities and Exchange Commission) listautuneet yritykset. SEC on Yhdysvaltain arvopaperimarkkinoita valvova elin. Vastaavanlaisia lakeja on laadittu myös muissa maissa. (Snellman, K. 2010.)

4 Roolipohjainen käyttövaltuushallinta

Käyttövaltuuksien hallinnan selkeyttämiseksi on luotu roolipohjaisen käyttövaltuushallinnan malli.

Roolipohjainen käyttövaltuushallinta perustuu siihen, ettei käyttövaltuuksia enää myönnetä henkilölle järjestelmäkohtaisesti ja ns. yksitellen, vaan työtehtävään liittyvän työroolin kautta. Käyttövaltuushallinnan kannalta työroolilla tarkoitetaan joukkoa käyttövaltuuksia, joita henkilö tarvitsee suoriutuakseen työtehtävistään.

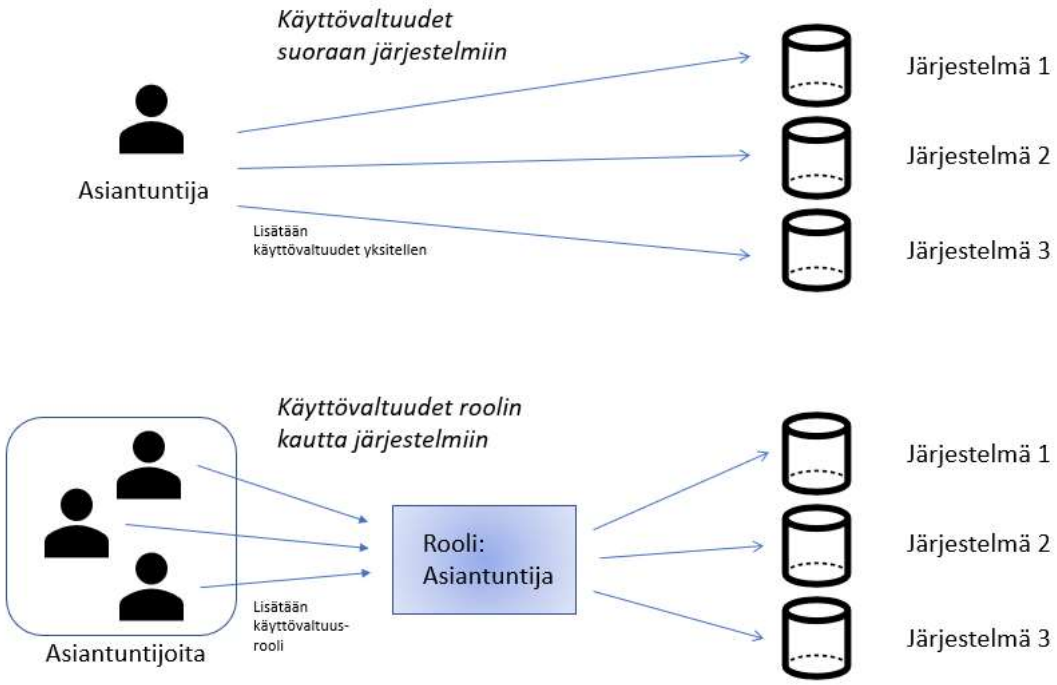
Työtehtävällä tarkoitetaan tässä organisatorista roolia, joka määrittelee työntekijän työtehtävät. Tällöin käyttövaltuuksien kannalta ajatellaan työroolin sallimaa ja velvoittavaa pääsyä järjestelmiin. Toisaalta työrooli voi toimia myös rajoittavana tekijänä, eli tulee ymmärtää ero työntekijän kompetenssin ja organisatorisen roolin välillä. Vaikka työntekijä pystyisi osaamisensa puitteissa tekemään enemmän kuin työnkuva sallii, hänen ei ole hyväksyttävää sitä tehdä. (Sandhu et al. 1996)

Käyttövaltuusroolien avulla voidaan hallita myös pääsynhallintaa yksittäisen järjestelmän osalta, jolloin käyttövaltuusroolilla tarkoitetaan RBAC-standardin mukaisia järjestelmän sisäisiä rooleja. Järjestelmäkohtaista RBAC-mallia avataan esimerkin myötä tarkemmin kappaleessa 5.2.

Kuten jo aiemmin todettiin, Ferraiolo ja Kuhn esittelivät ensimmäisen RBAC-mallin Baltimoressa vuonna 1992. Malliin on sittemmin tehty useita laajennoksia.

RBAC-mallien laajennoksia käsitellään tarkemmin kappaleessa 5. Roolipohjainen käyttövaltuushallinta vastaa myös Yhdysvalloissa vuonna 2002 voimaan tulleen Sabarnes-Oxley (SOX) lain vaatimuksiin. SOX-laki kehitettiin estämään taloudellisia petoksia, joihin voitiin käyttää hyväksi yritysten tietojärjestelmiä.

Roolit ovat ryhmälähtöisiä, jolloin jokaiselle roolille allokoidaan joukko käyttövaltuuksia ja roolia ylläpidetään. Jokaisella roolilla puolestaan on joukko yksittäisiä jäseniä. Menettely tarjoaa tavan nimetä ja kuvaa monesta moneen -suhteita yksilöiden ja käyttövaltuuksien välillä. (Ferraiolo & Kuhn 1992, 4.)



Kuva 1. Roolin kautta lisättävien käyttövaltuuksien käsitemalli verrattuna yksittäin lisättäviin käyttövaltuuksiin.

Ensimmäisessä RBAC –mallissa esiteltiin kaksi roolipohjaisen käyttövaltuushallinnan tärkeää periaatetta, jotka ovat käytössä myös RBAC-mallin myöhemmissä versioissa.

- Vähimmän pääsyn periaate
- Vastuiden rajaamisen periaate.

Vähimmän pääsyn periaate (eng. Least Priviledge) tarkoittaa, että henkilöllä ei tule olla enempää käyttövaltuuksia, kuin työtehtävien suorittamisen kannalta on oleellista. Työtehtäviin liittymättömien käyttövaltuuksien käyttäminen tulee estää.

Vastuiden rajaamisen periaate (eng. Separation of Duties), toiselta nimeltään tehtävien eriyttäminen, on sääntökokoelma, jonka avulla vastuita rajataan. Tähän liittyy oleellisesti termi kielletyt yhdistelmät. Kiellettyjen yhdistelmien avulla varmistetaan, ettei samalle henkilölle anneta oikeuksia, jotka tarjoavat

tilaisuuden tehdä petoksia. Esimerkiksi sama henkilö ei voi sekä asettaa että hyväksyä palkkoja. (Ferraiolo & Kuhn 1992, 9.)

Vähimmän pääsyn periaate ja vastuiden rajaamisen periaate ovat paitsi roolipohjaisen käyttövaltuushallinnan kulmakiviä, myös käyttövaltuushallinnan kulmakiviä yleisesti.

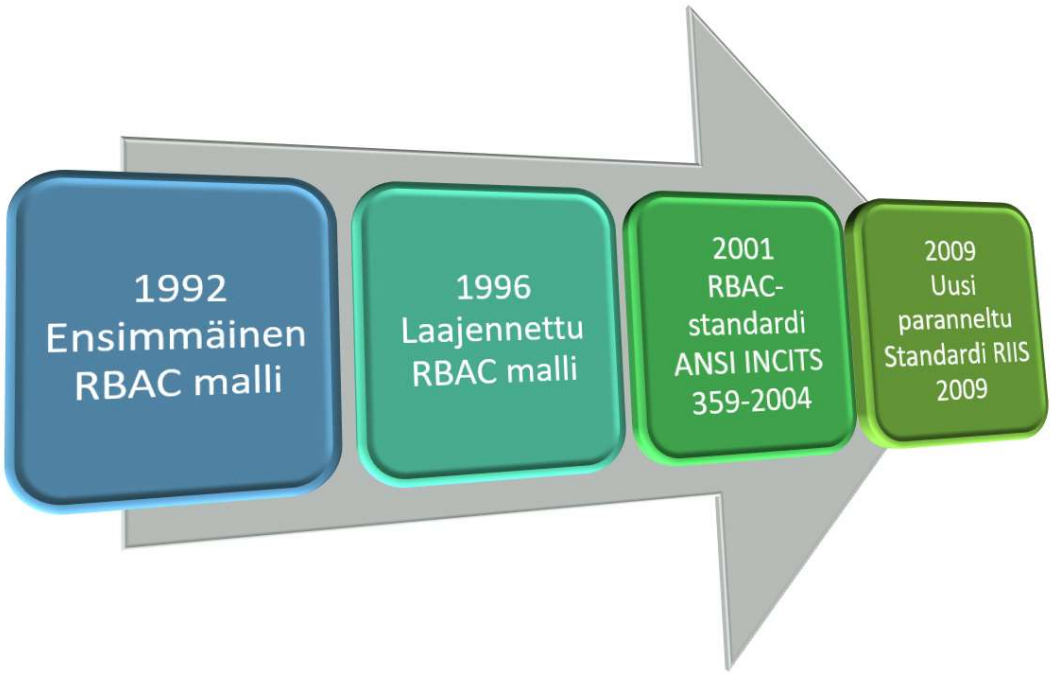
5 RBAC malleja ja standardeja

Roolipohjaisesta käyttövaltuushallinnasta puhuttaessa käytetään usein yleisenä nimityksenä lyhennettä RBAC (Role-based Access Control). Lyhenne esiintyy yleisesti myös keskusteltaessa RBAC-standardeista.

RBAC standardit sopivat sekä organisatoristen että järjestelmätasoisten roolien käyttöön. Standardeihin on tehty useita muunnoksia ja laajennoksia.

RBAC standardit voivat koskea myös yksittäisiä järjestelmiä, esimerkkinä Azure. Azureen on määritelty tarkat, järjestelmänsisäiset roolit, jotka on suunniteltu ainoastaan Azuren toimintaa varten.

RBAC-malli esiteltiin ensimmäisen kerran vuonna 1992 ja mallia on sittemmin kehitetty ja siihen on tehty useita laajennoksia. Kuvassa 2 on karkeasti kuvattu RBAC-mallin kehitystä.



Kuva 2. RBAC-mallin kehityskaari

RBAC-mallin laajennoksista muutamia esimerkkejä ovat ARBAC ja komposiittimalli.

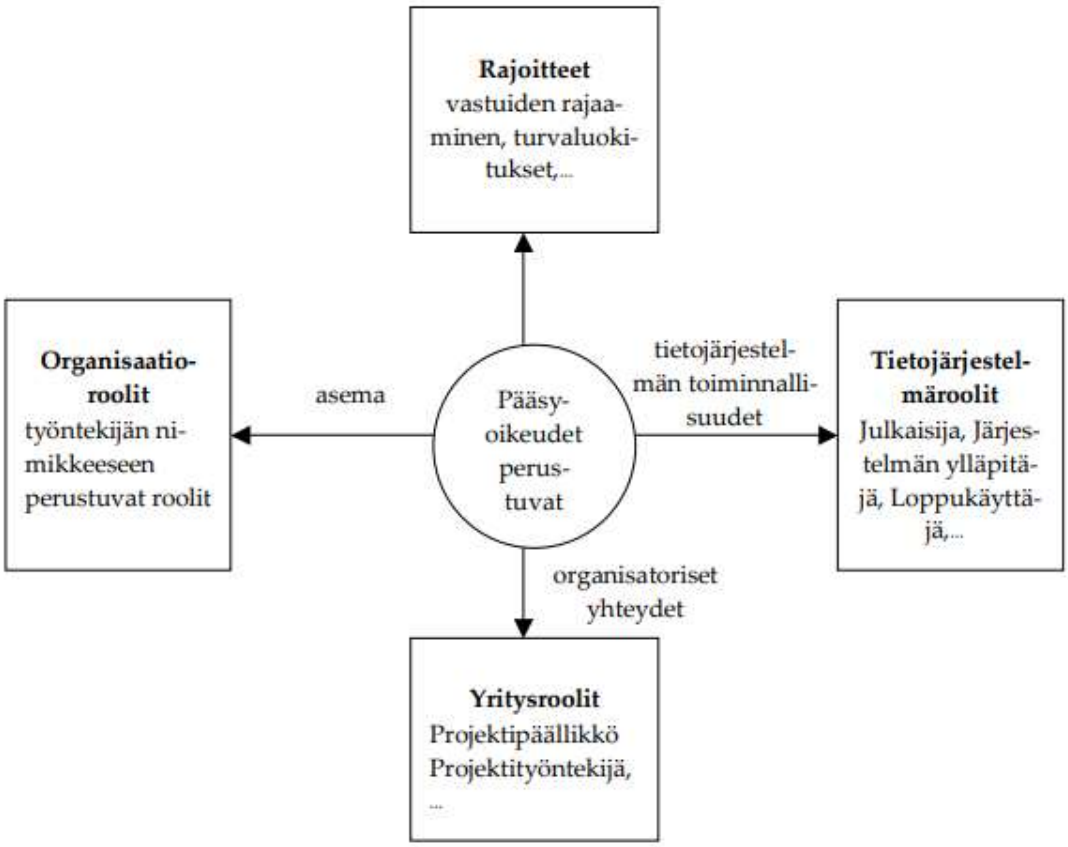
RBAC-mallin perustana on ollut käyttövaltuuksien hallinnan helpottaminen, mutta perus RBAC-malli ei täysin vastaa tarpeisiin, kun kyseessä on laaja organisaatio tai jokin todella suuri järjestelmäkokonaisuus. RBAC-mallia on pitänyt kehittää vastaamaan isojen ympäristöjen ja organisaatioiden tarpeita. Suurten kokonaisuuksien hallintaan kehitettiin roolien ryhmittelyihin perustuva komposiittimalli, jota käsitellään tarkemmin kappaleessa 5.1.

5.1 Komposiittimalli

Komposiittimalli on suunniteltu erityisesti laajoja kokonaisuuksia varten. Laajalla kokonaisuudella voidaan tarkoittaa järjestelmäkokonaisuutta, organisaatiota tai molempia.

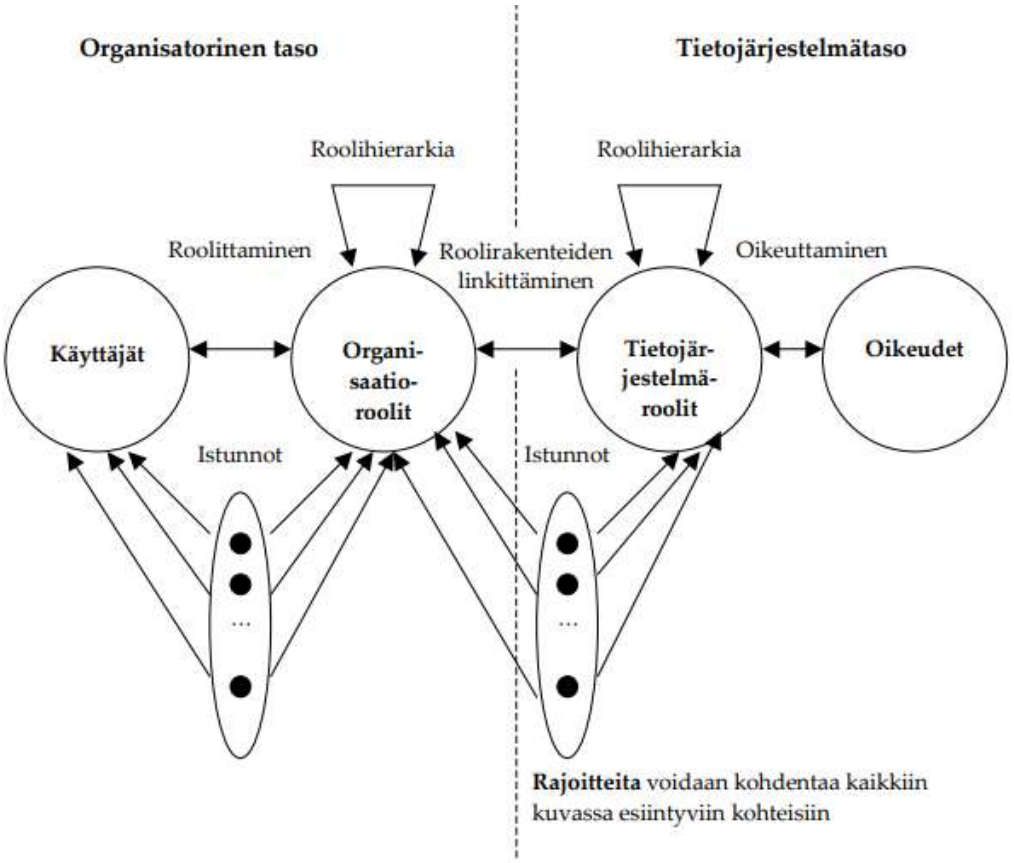
Komposiittimallissa roolit määritetään organisaatiokaavioiden perusteella. Komposiittimallin perusperiaatteena on roolien ryhmittely kolmeen pääluokkaan: tietojärjestelmäroolit, yritysroolit ja organisaatioroolit. Malli perustuu organisatoristen roolien erottamiseen järjestelmätason rooleista, mutta luoden yhtymäkohdan niiden välille.

Kuvassa 3 esitetään komposiittimallin luokittelu kolmeen pääluokkaan, eli organisatoriset roolit, tietojärjestelmäroolit ja yritysroolit.



Kuva 3. Komposiittimallin kolmeen pääluokkaan perustuva rooliryhmittely (Mäkelä, N. 2008, 34–35.)

RBAC-malli voidaan erottaa tietojärjestelmä- ja organisaatiotasoiksi komposiittilaajennoksella. Kuvassa 4 on havainnollistettu tätä erotusta ja niiden välistä linkitystä. Koska komposiittimalli on kehitetty erityisesti laajoja kokonaisuuksia silmällä pitäen, helpottaa se roolien rakenteellista hallintaa merkittävästi.



Kuva 4. Komposiittimallin organisatorisen ja järjestelmätason kuvaus (Mäkelä, N. 2008)

5.2 Järjestelmäkohtaiset RBAC standardit

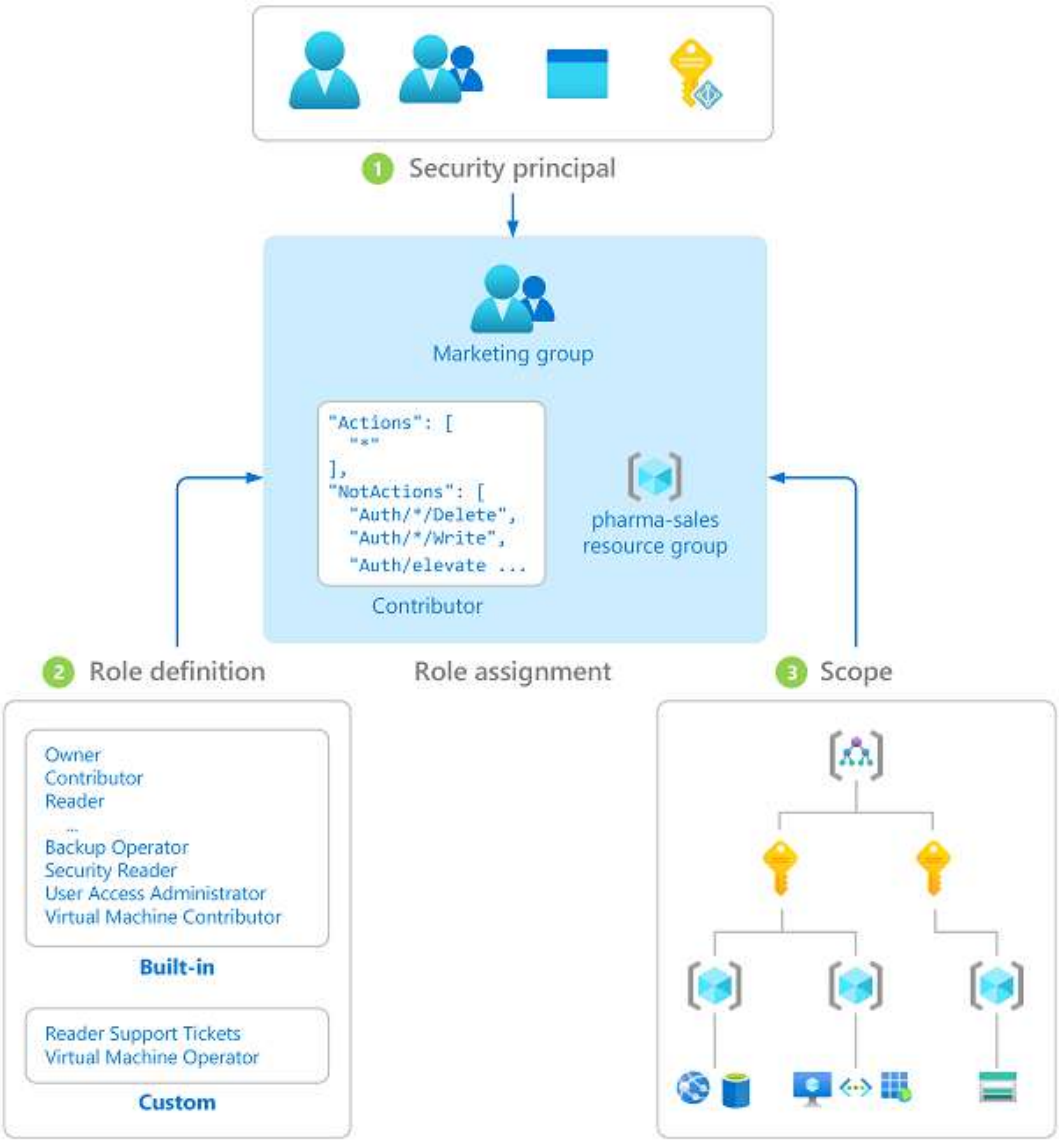
RBAC-standardi voi koskea myös yksittäistä järjestelmää. Käytetään esimerkkinä Microsoftin Azurea ja Azuren omaa RBACia.

Roolimääritys liitetään esim. käyttäjälle, ryhmälle, palvelun pääkäyttäjälle käyttöoikeuden myöntämistä varten. Käyttöoikeus myönnetään luomalla roolimääritys ja vastaavasti peruutetaan poistamalla se.

Seuraavassa kaaviossa on esimerkki roolimäärityksestä.

Esimerkissä markkinointiryhmälle on määritetty lääkemyyntiresurssiryhmän avustajarooli. Tämä tarkoittaa, että markkinointiryhmän käyttäjät voivat luoda tai hallita mitä tahansa Azure-resurssia lääkemyyntiresurssiryhmässä.

Markkinoinnin käyttäjillä ei ole pääsyä lääkemyyntiresurssiryhmän ulkopuolisiin resursseihin, elleivät he ole osa toista roolijakoa. (Microsoft, 2022)



Kuva 5. Esimerkki Azuren roolimäärityksistä (Microsoft, 2022).

6 Asiantuntijaroolien suunnittelu ja toteutus toimeksiantajayrityksen käyttövaltuushallintajärjestelmään

Opinnäytetyön tavoitteisiin kuului mm. selkeyttää asiantuntijoiden käyttövaltuuksiin liittyvää tilausprosessia ja kartoittaa sen nykytilaa.

Tutkimuksen alkuperäisenä tavoitteena oli saada luotua ehdotelma kahta uutta käyttövaltuusroolia varten, jotka olivat tietoliikenneasiantuntija ja konesaliasiantuntija.

6.1 Käyttövaltuusroolien määrittäminen ja tilausprosessin nykytila

Roolien suunnittelu aloitettiin tarkastelemalla vastaako kaksi käyttövaltuusroolia tunnistettuun tarpeeseen.

Pohdinnoissa vaihteli tarve käyttövaltuusroolien määrästä 2–3 roolin välillä, eikä niiden välisestä jaottelusta tullut täyttä varmuutta. Vaikka karkea jaottelu asiantuntijoiden välillä voidaan ajatella olevan tietoliikenneasiantuntija vs. konesaliasiantuntija, on erilaisia variaatioita todellisuudessa enemmän. Esimerkiksi osa tekee työtä 24/7 vuoroissa, osa pelkässä päivävuorossa. Tämän lisäksi voidaan ajatella asiantuntijatekemisessä olevan erilaisia vaativuustasoja, sekä mahdollisia asiakaskohtaisia vastuita.

Edellä mainittujen syiden vuoksi oli olemassa riski, että vähimmän pääsyn periaate ei toteudu, jos roolien jaottelua ja niihin liittyvien oikeuksien tarkastelua ei tehdä huolellisesti.

Epävarmuus jaottelusta roolien välillä asetti haasteita käytännön toteutukselle, joten toteutuksen lähestymiskulmaa jouduttiin miettimään uudelleen.

Aloin miettiä toteutusta konkreettisen lopputuloksen sijaan sekä vähimmän pääsyn periaatteen, että työmenetelmien ja niihin liittyvän ajankäytön kautta.

6.1.1 Tilausprosessin nykytila

Käyttövaltuuksien tilausprosessin nykytila havaittiin haastavaksi. Ei ole yksiselitteistä ohjetta sille, mitä käyttövaltuuksia uusi asiantuntija tarvitsee työssään ja mikä puolestaan olisi liikaa.

Vähimmän pääsyn periaatteetta noudattamalla, ei ole mahdollista tilata uudelle asiantuntijalle varmuuden vuoksi samoja käyttövaltuuksia kuin esim. useamman vuoden talossa olleella asiantuntijalla on. Pidempään työskennellyt on saattanut osallistua erilaisiin projekteihin ja hänellä voi olla OTO-tehtäviä, jolloin laajemmille käyttövaltuuksille on työtehtäviin perustuva pätevä syy.

Tilausprosessi on hidas ja aikaa vievä, kun käyttövaltuudet täytyy tarkastella yksitellen, kun niille ilmenee tarvetta, sekä varmistaa jokaisen käyttövaltuuden kohdalla, että vähimmän pääsyn periaate toteutuu.

6.2 Työmenetelmät

Opinnäytetyössä tutkimuksenalaisena olivat myös roolien määrittämiseen ja suunnitteluun käytettävät työmenetelmät.

Lähestyin roolien määrittämistä hetkellisesti pelkästään työmenetelmien tarkastelun kautta. Asetin tavoitteeksi löytää työtapoja, jotka tukevat järkevää ajankäyttöä ja joita noudattamalla vähimmän pääsyn periaate toteutuu, ja tilausprosessi helpottuu tulevaisuudessa.

Koska roolien jakautumisesta eri asiantuntijaryhmien välille oli edelleen epävarmuutta, tein päätelmän, että alkuperäistä tavoitetta kahden tai jopa useamman roolin suunnittelusta kerralla ei kannata yrittää viedä läpi sellaisenaan.

Päätin luopua alkuperäisestä tavoitteesta suunnitella kaikki tietoliikenne- ja konesaliasiantuntijoiden tarvitsemat käyttövaltuusroolit ja keskittyä sen sijaan laatimaan mallin käyttövaltuusroolien luomista varten ja pilotoimaan lopputulosta

vain yhdellä roolilla. Mallin avulla asiantuntijaroolit voidaan tulevaisuudessa määrittää helposti, tehokkaasti ja luotettavasti.

Mallin luominen aloitettiin pilottiroolin valinnalla, joksi valikoitui tietoliikenneasiantuntijan käyttövaltuusrooli ja sen myötä 1–2 esihenkilöä, joiden kanssa tarkempi määrittely aloitettiin.

Tietoliikenneasiantuntijan käyttövaltuusrooli palvelee akuuteinta tarvetta ja toimii hyvänä esimerkkinä tuleville käyttövaltuusrooleille.

6.3 Käyttövaltuusroolin pilotointi

Jotta pilottiroolin suunnittelu voitiin aloittaa, tarvittiin speksit käyttövaltuushallintajärjestelmän näkökulmasta. Kartoitettiin kohdat, jotka täytyy olla selvitettynä ennen kuin käyttövaltuusrooli voidaan luoda käyttövaltuushallintajärjestelmään teknisessä mielessä.

6.3.1 Päällekkäisten käyttövaltuuksien välttäminen

Käyttövaltuushallintajärjestelmässä on tulevien asiantuntijaroolien lisäksi olemassa ns. peruskäyttäjärooli, joka antaa tietyt perustason käyttövaltuudet kaikille toimeksiantajayrityksen työntekijöille.

On tärkeää osata erottaa toisistaan peruskäyttäjärooli ja asiantuntijatekemiseen liittyvä(t) rooli(t), jotta voidaan välttää päällekkäisyyksiä ja ymmärtää mitä käyttövaltuuksia minkäkin roolin kautta myönnetään.

Toimeksiantajayrityksen tapauksessa mikään ei teknisessä mielessä mene rikki, jos päällekkäisiä oikeuksia annetaan eri roolien kautta. Tällainen ei kuitenkaan ole laadukasta toimintaa ja saattaa häiritä vähimmän pääsyn periaatetta, joten päällekkäisyydet tulee eliminoida.

6.3.2 Turvallisuusselvitykset ja käyttövaltuushallintajärjestelmä

Toimeksiantajayrityksessä työskentelevistä henkilöistä tehdään aina turvallisuusselvitys, jonka periaatetta käsiteltiin teoriatasolla kappaleessa 8.

Toimeksiantajayrityksen asiakkaissa on yrityksiä, jotka vaativat lisäksi erillisen asiakaskohtaisen turvallisuusselvityksen, ennen kuin ko. asiakkaaseen liittyvään tietoon voi henkilö työtehtäviensä edellyttämällä tasolla päästä käsiksi. Mainittuihin asiakasyrityksiin liittyvään tietoon ei voi päästä käsiksi ns. varmuuden vuoksi, vaan pääsyn tarve tietoon tulee perustella henkilön työtehtävillä, minkä lisäksi vaaditaan hyväksytysti läpäisty turvallisuusselvitys.

Jos turvallisuusselvitys ei mene läpi, henkilö ei tule pääsemään käsiksi tietoon, jonka perusteella turvallisuusselvitys tehtiin.

Pilottiroolin suunnittelussa huomioitiin turvallisuusselvitysten vaatimukset.

6.3.3 Hyväksyntäketju ja hyväksyjäryhmät

Käyttövaltuusrooleja suunniteltaessa täytyy ottaa huomioon, että jokaisella erillisellä käyttövaltuudella on yleensä omistaja. Kun suunnitellaan hyväksyntäketjuja, on käytännön toimivuuden kannalta oleellista suunnitella toimivat hyväksyntäketjut ja mahdollisesti suosia hyväksyntäryhmiä, ettei esimerkiksi lomalla oleva yksittäinen henkilö jää pullonkaulaksi hyväksyntäketjussa.

Toteutustapoina voidaan käyttää yksittäisten tuotteiden hyväksyjiä, tai luoda roolille erillinen hyväksyntäryhmä.

Pilottiroolin suunnittelussa huomioitiin hyväksyntäketju.

6.4 Pilottiroolin suunnittelu

Pilottiroolin suunnittelussa pohdittiin mm seuraavia aiheita, joiden ympärille rooli suunniteltiin.

- Roolien nimeämiskäytännöt
- Roolien kuvaukset
- Roolien sijainti käyttövaltuushallintajärjestelmän kansiorakenteessa
- Hyväksyntäketju/hyväksyntäryhmät
- Erityisturvallisuusselvitettävät asiakkaat
- Vähimmän pääsyn periaate.

Pilottirooliin liitettävät käyttövaltuudet käytiin läpi yksitellen ja kirjoitettiin jokaisesta lyhyt kuvaus tietoliikenneasiantuntijan työtehtävän näkökulmasta. Kuvauksiin ei kirjattu ympäripyöreästi ”mahdollistaa työtehtävien hoidon”, vaan esimerkiksi ”mahdollistaa verkkolaitteiden konfiguraatioiden palauttamisen”, mikä on selkeästi perusteltu työtehtävien hoitamisella.

Rooliehdotelmaan ei tullut yhtäkään sellaista käyttövaltuutta, jota ei olisi katsottu huolellisesti läpi ja perusteltu työtehtävien edellyttämällä tarpeella.

6.4.1 Vähimmän pääsyn periaate pilottiroolissa

Pilottiroolin suunnittelussa tunnistettiin aluksi muutamia käyttövaltuuksia, joiden osalta ei ollut täyttä varmuutta tarvitseeko jokainen tietoliikenneasiantuntija niitä vai ei. Vähimmän pääsyn periaatetta noudattaen asia käytiin epäselvät oikeudet läpi ja poistettiin pilottiroolista ylimääräiset.

6.5 Toimintasuunnitelma pilottiroolista eteenpäin

Opinnäytetyön puitteissa laadittiin ehdotelma yhdestä käyttövaltuusroolista, joka valittiin pilottirooliksi.

Pilottiroolia suunniteltaessa selvitettiin roolin suunnitteluun ja toteutukseen liittyvät työvaiheet, sekä tunnistettiin mahdolliset haasteet ja pullonkaulat.

Tulevaisuudessa pilottiroolin avulla voidaan laajentaa roolipohjaista käyttövaltuushallintaa koskemaan myös muita asiantuntijarooleja, sekä mahdollisesti myös muunlaisia työrooleja.

7 Pohdinta

7.1 Saavutettiinko tavoite?

Opinnäytetyön alkuperäinen tavoite oli kaksiosainen. Ensimmäinen tavoite oli saavuttaa ymmärrys roolipohjaisesta käyttövaltuushallinnasta. Toinen tavoite oli luoda ehdotelma kahdesta asiantuntijaroolista käyttövaltuushallintajärjestelmään.

Ensimmäinen tavoite saavutettiin sellaisenaan. Tämän myötä ymmärrettiin, ettei ole kannattavaa puskea toista tavoitetta maaliin sellaisenaan, vaan ajatella kriittisesti ja muokata tavoitetta realistisemmaksi havaintojen perusteella.

Tutkimuksen edetessä kävi ilmi, ettei ole kannattavaa lähteä määrittämään kahta tai useampaa käyttövaltuusroolia kerralla ns. tyhjästä. Sen sijaan oli järkevämpää laatia ensiksi pilottirooli, jolloin voidaan minimoida sekä tietoturvariskit että hallitsematon ajankäyttö, kun keskitytään pilotoimaan sekä käyttövaltuusroolin suunnittelua, että sen laatimiseen vaadittavia työvaiheita.

Pidän opinnäytetyön kokonaistavoitetta saavutettuna, koska ymmärrys roolipohjaisesta käyttövaltuushallinnasta kasvoi, mikä itsessään edesauttoi ymmärtämään alkuperäistä tavoiteasetantaa ja muokkaamaan sitä järkevämpään suuntaan.

Yllä mainituin perusteluin katson opinnäytetyön tutkimustuloksen olevan onnistunut ja toimeksiantajayritykselle tavoitellun hyödyn saavutetun.

7.2 Työmenetelmät

Käyttövaltuusroolien luomiseen käytetyt työmenetelmät olivat osana tutkimusta.

Työmenetelmiä ja niihin liittyvää ajankäytön järkevyyttä tarkastelemalla, saavutettiin nopeasti ymmärrys käyttövaltuusroolien suunnittelun vaatimuksista. Kun

vaatimukset olivat selvillä, pystyttiin esittämään täsmällisempiä kysymyksiä epäselvien asioiden selventämiseksi ja laatimaan selkeää dokumentaatiota.

Ymmärtämällä millainen prosessi on luoda käyttövaltuusrooli tietylle asiantuntijatehtävälle, voidaan tulevaisuudessa laajentaa roolipohjaista käyttövaltuushallintaa koskemaan useampia työrooleja.

Pidän työmenetelmiin kohdistuvaa kriittistä analysointia yhtenä suurimpana avaintekijänä lopputuloksen onnistumiselle.

7.3 Mitä opin, mitä tunsin?

Opinnäytetyön tekeminen oli minulle kasvun ja oppimisen prosessi. Vaikka minulla on työelämää takanani jo pari vuosikymmentä, löysin opinnäyteprosessista paljon uutta. Vaikka pidän lopputulosta onnistuneena, oli itse opinnäytetyön tekeminen, oman tekemisen ymmärtäminen ja kriittinen tarkastelu minulle suurin anti.

Opiskelemalla ensin teoriaa ja jäsentämällä sitä tekstiksi opinnäytetyön teoriaosuuteen, saavutin maksimaalisen hyödyn oppimisessa.

Jos olisin alkanut tehdä varsinaista tutkimusta jo ennen kuin teoria oli opiskeltu ja opinnäytetyön teoriaosuus kirjoitettu valmiiksi, en esimerkiksi olisi pystynyt sujuvasti keskustelemaan tiettyjen sidosryhmien kanssa aiheesta, puutteellisen substanssiosaamisen vuoksi.

Teoriaosuuden kirjoittaminen toimi minulle erinomaisena oppimismenetelmänä, koska en voinut tuottaa tekstiä ymmärtämättä kirjoittamaani.

Opinnäytetyön edetessä tunsin ensiksi riittämättömyyden tunnetta, mutta kirjoittamisen edetessä aloin kokea enenevissä määrin onnistumisen tunnetta. Onnistumisen kokemus nousi paitsi opitusta teoriasta, myös käytännön oivalluksista. Suurin oivallus oli päätös luopua alkuperäisestä tavoitteesta kahdesta valmiista käyttövaltuusroolista ja luoda sen sijaan malli pilotoinnin avulla.

Kokonaisuudessaan pidän opinnäytetyön tavoitteita saavutettuina niin substanssiosaamisen kasvun, toimeksiantajayritykselle saavutetun hyödyn, kuin oppimiskokemuksen perusteella.

Lähteet

1 Gittlen, S. Rosengrance, L. 2021 What is identity and access management? Guide to IAM. Saatavissa: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

2 Göös, J, 2018. Miksi yrityksen kannattaa kiinnostua kulunvalvonnasta? Saatavissa: https://optima.fi/blogi/miksi-yrityksen-kannattaa-kiinnostua-kulunvalvonnasta/

3 Nykänen, Henrik. 2021. IAM - Kenelle käyttövaltuudet kuuluvat? Saatavissa: https://www.telia.fi/yrityksille/artikkelit/artikkeli/mita-tarkoittaa-iam-eli-identiteetin-ja-paasynhallinta

4 Laakkonen, Miska. 2019. Digitaaliset identiteetit keltanokille - 10 termiä, jotka sinun tulisi jo tietää. Saatavissa: https://www.nixu.com/fi/blog/digitaaliset-identiteetit-keltanokille-10-termia-jotka-sinun-tulisi-jo-tietaa

5 Bertino, Elisa & Takahashi, Kenji 2010. Identity Management: Concepts, Technologies, and Systems. Artech House. [Viitattu 2023]

6 What Is Role-Based Access Control (RBAC)? A Complete Guide. [Viitattu 13.03.2023] Saatavissa: https://frontegg.com/guides/rbac

7 Magnusson, A. 2023. Identity and Access Management (IAM) Best Practices. Saatavissa: https://www.strongdm.com/blog/iam-best-practices

8 Finlex. Turvallisuusselvityslaki 19.9.2014/726. [Viitattu 2023]. Saatavissa: https://www.finlex.fi/fi/laki/ajantasa/2014/20140726

9 Suojelupoliisi. Turvallisuusselvitykset. [Viitattu 2023]. Saatavissa: https://supo.fi/turvallisuusselvitykset

10 Kyberturvallisuuskeskus, 2020. Tietoturvapoikkeama. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toimi-nain-jos-havaitset-tietoturvapoikkeaman

11 Tietosuojalaki (1050/2018) Tietosuojavaltuutetun toimisto, Usein kysyttyä EU:n tietosuoja-asetuksesta. [Viitattu 2023]. Saatavissa: https://tietosuoja.fi/gdpr

12 Tietosuojavaltuutetun toimisto. Mitä on henkilötieto? [Viitattu 2023). Saatavissa: https://tietosuoja.fi/mika-on-henkilotieto

13 Anunti, T. 2022. Tietosuojan kertauskurssi – mitä henkilötietojen keräämisestä ja käsittelystä on kerrottava? Saatavissa: https://tilisanomat.fi/palkka-ja-henkilostohallinto/tietosuojan-kertauskurssi-mita-henkilotietojen-keraamisesta-ja-kasittelysta-on-kerrottava

14 Tietosuojavaltuutetun toimisto, työelämän tietosuojalaki. Muutettu /247/2019) 1.4.2019. [Viitattu 2023]. Saatavissa: https://tietosuoja.fi/tyoelaman-tietosuojalaki

15 Finlex. Sähköisen viestinnän tietosuojalaki (7.11.2014/917) [Viitattu 2023]. Saatavissa: https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

16 Wikipedia, 2022. Kirje. Saatavissa: https://fi.wikipedia.org/wiki/Kirje

17 Laki24. Mikä on kirjesalaisuus? [Viitattu 2023]. Saatavissa: https://laki24.fi/mika-on-kirjesalaisuus/

18 Snellman, K. 2010. Tutkiva kirjoittaja ammattikorkeakoulussa. Opinnäytetyö. Lahden ammattikorkeakoulu. Theseus-tietokanta.

19 Sandhu, R.S., Coynek,E.J., Feinsteink, H.L. & Youmank, C.E. 1996. Role-Based Access Control Models. IEEE Computer [Viitattu 13.03.2023]. Saatavissa: http://csrc.nist.gov/rbac/sandhu96.pdf

20 Mäkelä, N. 2008. Tutkiva kirjoittaja yliopistossa. Pro Gradu -tutkielma. Tampereen yliopisto. Theseus-tietokanta.

21 Bednarz, A. 2005. Compliance: Thinking outside the Sarbox. Networkworld [Viitattu 2023]. Saatavissa: http://www.networkworld.com/research/2005/020705sox.html

22 Microsoft, 2022. What is Azure role-based access control (Azure RBAC)? Saatavissa: https://learn.microsoft.com/en-us/azure/role-based-access-control/overview