Valtteri Rauhala

Tietokantojen pääsynhallinnan uudistus Mehiläisessä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto ja viestintätekniikka

Insinöörityö

15.11.2021

Tiivistelmä

Tekijä:	Valtteri Rauhala
Otsikko:	Tietokantojen pääsynhallinnan uudistus Mehiläisessä
Sivumäärä:	32 sivua
Aika:	15.11.2021
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto ja viestintätekniikka
Ammatillinen pääaine:	Hyvinvointi ja terveysteknologia
Ohjaajat:	Sakari Lukkarinen, lehtori Metropolia AMK Tommi Ruoste, Tietokanta-Asiantuntija Mehiläinen Digitaaliset palvelut

---

Tämän työn tarkoituksena on luoda malli, jonka pohjalta tulevaisuudessa tehdään kohdeyrityksen tietokantojen pääsynhallintaa. Kohdeyritykselle syntyi tarve pääsynhallinnan uudistukselle, kun nykyinen tapa toimia ei enää toimi yrityksen näkökulmasta.

Tulevaisuuden mallin tavoitteena on olla aikaa kestävä, ylläpidettävä ja kestää organisaatiollisia muutoksia. Mallin tarkoituksena on olla ylätason raakapohja-ajatus siitä, miten pääsynhallintaa tulevaisuudessa tehdään yrityksessä.

Kohdeyrityksellä on käytössään Microsoftin tuoteperheen tuotteet, ja niiden avulla tulevaisuudessa pääsynhallintaa tullaan tekemään yrityksessä.

Tämän opinnäytetyön aikana esitellään tietokantoja, pääsynhallintaa yleisesti sekä syvennytään Microsoft SQL palvelimen oikeuksien jako prosessiin. Työssä esitellään myös itse tulevaisuuden mallia, niiden tuloksia sekä pohdintaa siitä, miten tämä työ vastasi kohdeyrityksen tarpeita.

Avainsanat: Microsoft SQL server, Active Directory, Pääsynhallinta,Tietokannat

Abstract

Author:	Valtteri Rauhala
Title:	Modernization of IAM for Databases, Case Mehiläinen
Number of Pages:	32 pages
Date:	15th of October 2021
Degree:	Bachelor of Engineering
Degree Programme:	Information and communication Technology
Professional Major:	Health Technology
Supervisors:	Tommi Ruoste, Database Administrator Mehiläinen Oy, Digital services Sakari Lukkarinen, Senior Lecture Metropolia UAS

The aim of the study to build a new model of database identity access management for the client Mehiläinen Oy. Currently Mehiläinen has no controlled way to control identity access management for databases.

The aim for the future model is that it should stand time, be easy to maintain and to be able to stand future organizational changes. The new model will be an upper-level raw model of how identity access management should be done in the future.

The thesis presents databases, identity access management broadly and goes deeper into the way identity access management is done in Microsoft SQL Server. Also, the thesis presents the future model and how Mehiläinen should implement the IAM process in the future. The thesis includes presentation of the future model, the results, and considerations as to how the model fulfilled the needs of Mehiläinen.

Keywords: Microsoft SQL Server, Active Directory, IAM, Databases

Sisällys

Lyhenteet

1 Johdanto 1

2 Tietokanta-alustat 3

2.1 Tietokannat 3
2.2 Tietokanta-alustojen toiminta 4
2.3 Tietokanta-alustojen vertailu 6
2.3.1 RDBMS vs. Columnar 6
2.3.2 SQL vs. No SQL 8
2.3.3 Tietokanta-alustojen vertailu 9

3 Microsoft SQL Server 11

3.1 Historia 11
3.2 Relaatiotietokanta 11
3.3 MSSQL-pääsynhallinta 13
3.4 Tietokantakäyttäjät 15
3.5 Tietokannan käyttövaltuudet 17

4 Pääsynhallinta 21

4.1 Perusteet 21
4.1.1 Käyttövaltuudet 22
4.1.2 Pääsynhallinta 22
4.2 Identiteettien ja käyttövaltuuksien hallintaprosessi 23
4.2.1 Uuden työntekijän luonti 23
4.2.2 Työntekijän poisto 24

5 Pääsynhallinnan malli 25

5.1 Nykytilanteen kartoitus 25
5.2 Kehitetty malli 26
5.3 Oikeuksien jakaminen tietokantoihin 27
5.4 Mallin validointi 29

6 Yhteenveto 29

Lähteet 31

Lyhenteet

AD	Active Directory, Microsoftin tarjoama palvelu, jonka avulla luodaan käyttäjätilejä yrityksen ympäristöön.
IAM	Identity and Access Management. Identiteetin ja pääsynhallinta.
IdM	Identity Management. Identiteetin hallinta.
MSSQL	Microsoft SQL Server. Microsoftin tuottama tietokanta-alusta.
NoSQL	Not only SQL on kieli, joilla kuvataan relaatiomallista poikkeavia tietokantoja.
OLAP	Online Analytical Processing (OLAP) on tekniikka, jolla järjestetään suuria yritystietokantoja ja tuetaan liiketoimintatietojen.
OLTP	Online transaction processing on tekniika, joka tukee transaktio orientoituneita sovelluksia ja järjestelee päivittäisiä organisaation transaktioita.
RDMBMS	Relation Database Management Systems on yksi vanhimmista tietokantajärjestelmistä.
SQL	Structured Query Language on standardoitu ohjelmointikieli, jota käytettään relaatiotietokantojen kanssa.
T-SQL	Transact SQL. Microsoft SQL -palvelimeen käyttämä tietostruktuuri sekä kyselykieli.

1 Johdanto

Työn tarkoituksena on luoda uusi malli tietokantojen pääsynhallinnan toteuttamiseksi. Mallin pohjana tuli olla mahdollisimman hyvä muutoksen kesto, ylläpidettävyys sekä tietoturvallisuus. Työn kontekstissa malli tarkoittaa ylätason kaaviota sekä ajatusta, miten tulevaisuudessa luodaan pääsynhallintaa enemmänkin, kuin puhdasta nimilistaa ja pääsyoikeuksia.

Työn tilaajana toimii Mehiläinen Oy, ja työ on tehty yhteistyössä heidän digitaalisten palveluidensa kanssa. Mehiläinen on Suomen suurimpia yksityisiä terveyspalveluita tuottava yritys. Mehiläisellä on yli 540 toimipistettä ympäri Suomea, ja he työllistävät yli 22 300 henkilöä ja heidän toimipisteissänsä asioi vuosittain jopa yli 1 000 000 henkilöä. [1.]

Pääsynhallinnan tarkoituksena on rajata pääsyjä eri tietoihin tai toimintoihin. Työssä pääsynhallintaa tehdään lähtökohtaisesti Microsoftin tarjoamaan Active Directory (AD) -tunnuksien sekä AD-ryhmien avulla. AD:n avulla pystytään luomaan täysin kustomoituja ryhmiä, joihin voidaan liittää monien eri liiketoimintojen ihmisiä helposti. Tämän toimintatavan vahvuutena on myös se, kun henkilö lähtee yrityksen palveluksesta, poistuu hänen AD-tunnuksensa myös automaattisesti. Tällöin hänelle ei jää mitään pääsyjä yrityksen järjestelmiin.

Mehiläisellä on käytössä Windows AD -palvelin, jonka avulla ylläpidetään yrityksen tunnuksia. Nykyään Mehiläisessä pääsynhallintaa suoritetaan ilman mitään yhtenäisiä prosesseja, mutta kohdeyrityksen toiveenaan olisi luoda malli, joka mahdollistaa selkeämmän ja ylläpidettävämmän pääsynhallinnan. Tulevaisuudessa myös yrityksen aggressiivinen kasvu sekä kotimarkkinoilla että kansainvälisesti luo haasteita pääsynhallinnan osalta.

Mehiläisellä on tietokanta-alustana käytössä Microsoftin tarjoama Microsoft SQL Server, jonka pääsynhallintaa voidaan suorittaa joko SQL-kirjautumistunnuksien tai AD-tunnusten avulla. Tulevaisuuden tahtotilana olisi siirtää kaikki pääsyoikeudet ryhmien taakse, ja yksittäisiä käyttäjäoikeuksia jaettaisiin vain erityistarpeiden mukaisesti kuten potilastietojen osalta.

Tässä työssä tullaan esittelemään tarkemmin pääsynhallinnan perusperiaatteita, teknisempää kuvausta siitä, miten AD-ryhmät toimivat ja miten niitä luodaan sekä MSSQL-pääsynhallintamekanismeja ja eri tietokantarooleja.

2 Tietokanta-alustat

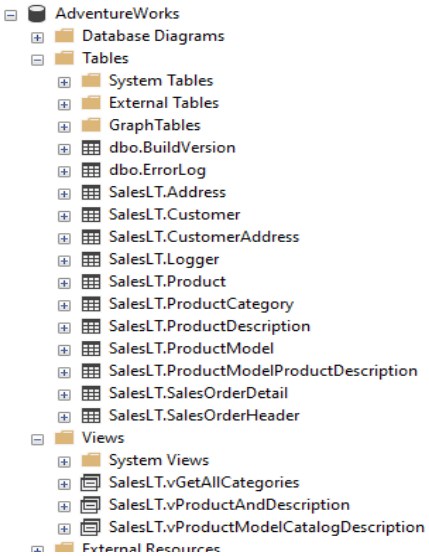
Tässä osiossa käydään läpi tietokantojen perusteita, eri alustoja sekä vertaillaan niiden toimintoja ja soveltuvuutta eri tarkoituksiin. Tietokannat ovat järjestelmiä, jossa voidaan säilyttää suuria määriä tietoja järjestelmällisesti.

2.1 Tietokannat

Yksinkertaistettuna tietokanta on lista erinäistä tietoa. Niiden tarpeellisuus ei välttämättä näy ihmisen päivittäisessä elämässä, mutta suurin osa kaikesta tiedosta, mitä tuotetaan, säilytetään erinäisissä tietokannoissa.

Tietokannoissa tiedot tallentuvat erinäisiin tauluihin, jotta tiedot olisivat helpommin nähtävissä ja ne olisivat jäsenneltävissä järkeviksi kokonaisuuksiksi. Tietokanta sisältää aina vähintään yhden taulun.

Kuvassa 1 esitetään esimerkki tietokannasta. Kyseinen tietokanta on Microsoftin palveluista löytyvä AdventureWorks, joka on oletuksena Microsoft SQL (MSSQL) -palvelimilla, kun käyttäjä ottaa sen käyttöön. Microsoft SQL on siis Microsoftin tuottama ohjelmisto, joissa tietokantoja voidaan ylläpitää.



Kuva 1: MSSQL löytyvä AdventureWorks -tietokanta esiteltynä. [2.]

Kuvassa 1 nähdään tietokannan nimi AdventureWorks. Nimen alapuolella olevat kansiot ovat automaattisesti tuotettuja kansioita, joihin voidaan tallentaa eri tietoja tietokantaan liittyen.

Ylimpänä ovat tietokantataulukot, joihin voidaan tallentaa kuva tietokannan suunnittelumallista tai muita haluttuja teknisiä dokumentaatioita.

Seuraavana listassa on itse tietokannan sydän eli taulut. Tämä sisältää kaikki tietokantaan tallennetut taulut, jotka sisältävät tietoa. MSQL luo automaattisesti alikansiot ja käyttäjä voi lisätä tauluja tarpeiden mukaan.

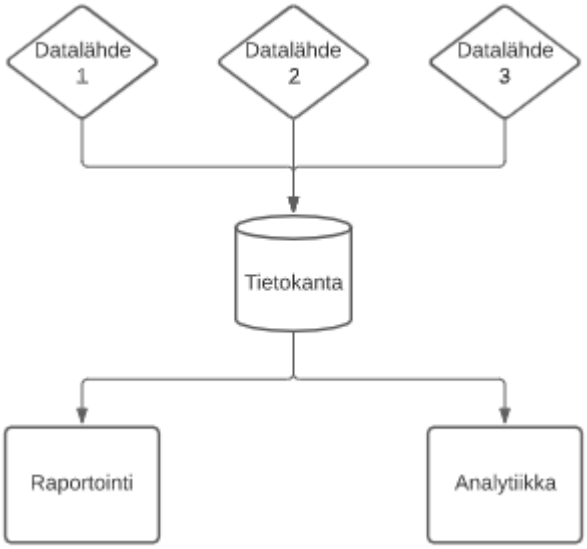
Alimpana kansiona näkyvät näkymät. Nämä ovat käyttäjien itseluomia tauluja, joita voidaan muokata käyttäen SQL-ohjelmointikieltä. Näkymät sisältävät aina tietoa tauluista, ja ne muodostuvat käyttäjän kyselyn perusteella.

2.2 Tietokanta-alustojen toiminta

Tietokanta-alustojen tarkoituksena on olla ratkaisu, jonka avulla analysoidaan, prosessoidaan sekä ylläpidetään tietoa. Nykypäivänä tietoa syntyy lähes jokaisesta liiketoiminnan alueesta, eri järjestelmistä sekä prosesseista. Kaikki tämä tieto päätyy tietokantojen eri tauluihin, joissa ne ovat sitten käyttäjien käytettävissä. [3.]

Tietoa, jota on tietokannoissa, voidaan jalostaa moneen eri tarkoitukseen, jotta eri käyttäjien tarpeet voidaan täyttää. Tietokantoja voidaan käyttää vain tietojen varastoimiseen, mutta ne mahdollistavat myös erinäisiä muita mahdollisuuksia. Tärkeänä osana on myös se, että varmistetaan tietojen turvallisuus, näkyvyyden rajaus sekä suorituskyky. [3.]

Kuva 2 on yksinkertaistettu esimerkki tietokanta-alustojen toimintaperiaatteesta.



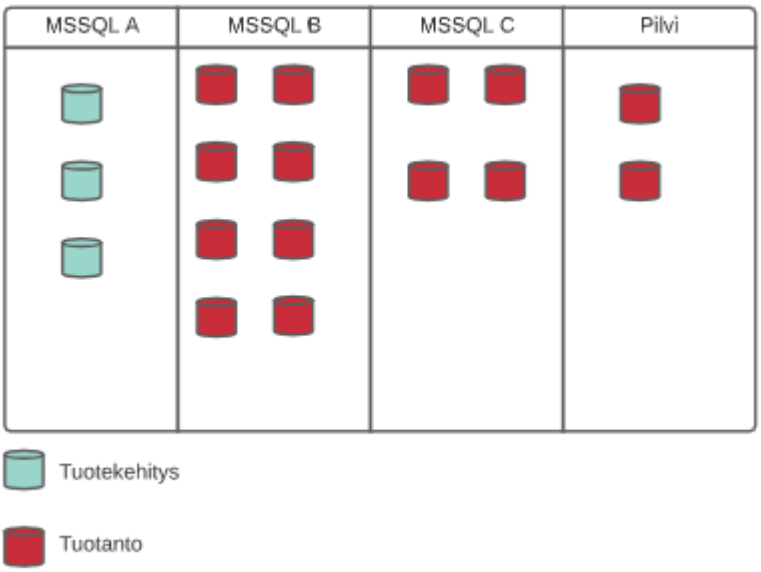
Kuva 2: Yksinkertaistettu tietokanta-alustan toimintaperiaate.

Kuva 2 on yksinkertaistettu esimerkki, miten tietokanta toimii. Tietokannoissa tulee aina olla tietolähteitä, joista tiedot saadaan. Tietolähteinä voi toimia esimerkiksi sovellus tai muu järjestelmä, joka kerää tietoja. Näiden lähteiden kautta tulleet tiedot tallennetaan tietokantaan.

Kohdeyrityksen osalta suurin osa tiedoista syntyy lääkärikäynneistä syntyvän tiedon pohjalta. Käynnin pohjalta syntyvät eri tietopisteet ovat muun muassa sairauskertomukseen liittyvät tiedot kuten diagnoosit, hoitosuunnitelma sekä myös kaikki tiedot ajanvarauksesta maksusuoritukseen.

Yhtiöllä on monia eri tietokanta palvelimia, jotka sisältävät useita tietokantoja. Haasteena on, että palvelimilla on eri vuosien MSSQL-järjestelmiä ja osa on jo nykyään pilvialustoilla.

Kuvassa 3 on yleistason kuvaus Mehiläisen tietokantajärjestelmien versioista. Jokainen laatikko kuvaa yhtä tietokantapalvelinta, ja eriteltynä on myös kehitykseen tarkoitetut palvelimet.



Kuva 3:Yleistason kuvaus kohdeyrityksen tietokantapalvelimista.

Kuva 3 osoittaa, miten kohdeyrityksen tietokantojen versiot voivat olla täysin eriäviä. Nykyaikana myös useammin mukaan ovat tulleet pilvipalvelut ja niiden tarjoajien vahvuutena voidaan pitää suhteellista edullisuutta varsinkin tallennustilan osalta, sekä palveluvarmuutta, kun palvelimet eivät enää sijaitse tietyissä paikoissa vaan voivat olla hajautettuna ympäri palveluntarjoajan infrastruktuuria.

2.3 Tietokanta-alustojen vertailu

Nykyään erinäisiä alustoja on satoja, ja niiden käyttötarkoitus vaihtelee paljolti tarpeiden mukaan. Tässä Luvussa esitetään eri tietokanta-alustoita ja niiden eroavaisuuksia.

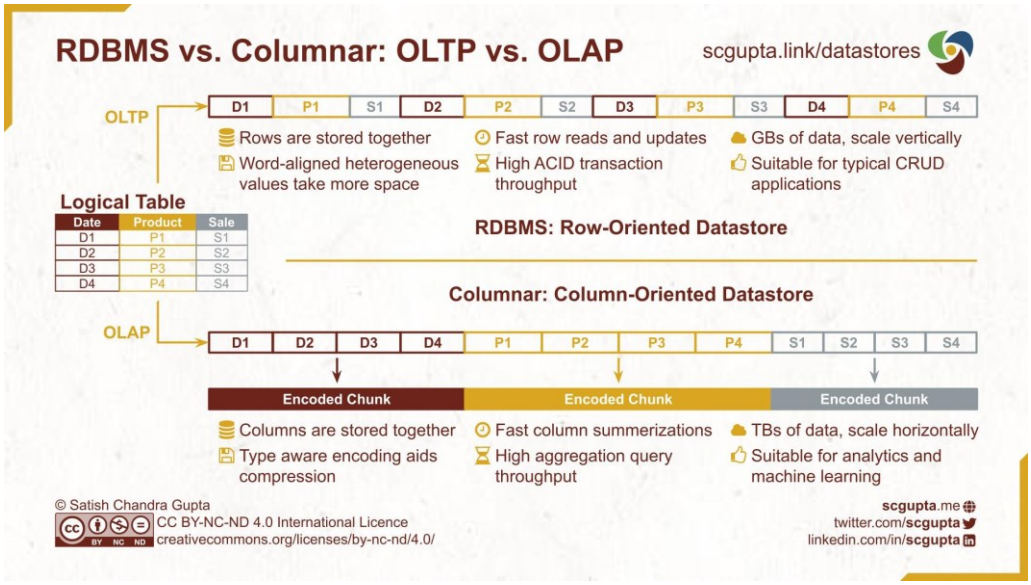
2.3.1 RDBMS vs. Columnar

Relaatiotietokantahallintajärjestelmä (RDBMS) on yksi varhaisimmista tiedon tallennusjärjestelmistä. Tällaisissa järjestelmissä tieto on organisoitu tauluihin.

Taulut ovat normalisoituja, jotta tietojen yhtenäisyys voitaisiin taata mahdollisimman laadukkaasti. Nämä taulut ovat myös rivi orientoituneita eli muutoksia ja kyselyitä tehdään rivi kerallaan. [4.]

Columnar eli sarakepohjainen järjestelmä on uudempi versio, jonka suurimpana muutoksena on, että vaikka muutokset tapahtuvat rivitasolla Kyselyitä pystytään tuottamaan myös yksittäisen sarakkeen tasolla.

Kuva 4 esittää RDBMS sekä Columnar-järjestelmien suurimpia eroavaisuuksia sekä vertailee niiden soveltuvuutta eri käyttötarkoituksiin.



Kuva 4: RDBMS- sekä Columnar-tietokantaratkaisuiden toiminnallisuuksien eroavaisuudet [4.].

Kuva 4 kuvastaa sitä, miten kyselyn prosessointi tapahtuu eri tietokantamalleissa.

RDBMS taulujen kysely tapahtuu rivikohtaisesti kuten kuvan ylemmässä osuudessa näkyy. Tämän vahvuutena on nopeat luku-sekä-kirjoitusoperaatiot, joita tietokannoissa tehdään.

Columnar taulujen kysely tapahtuu sarakekohtaisesti. Tämä mahdollistaa esimerkiksi nopeampaa analytiikan tekoa sekä muita operaatioita, joita voidaan tehdä sarake kerrallaan. Sarakepohjainen järjestelmä toimii myös palasissa eli kuten kuvassa nähdään, eli paloittelee kyselyn jokaista saraketta kohden ja suorittaa niitä järjestyksessä.

2.3.2 SQL vs. No SQL

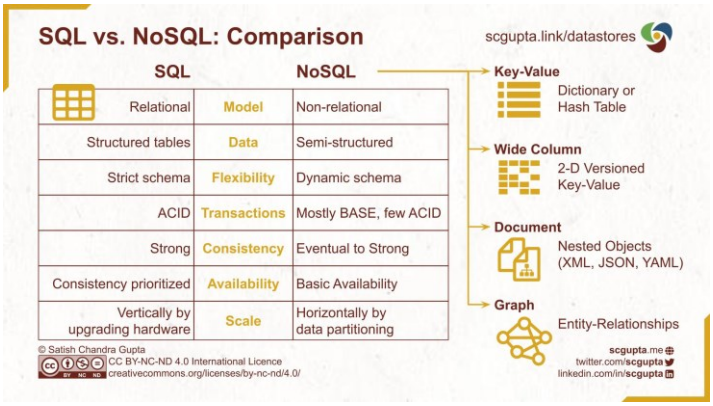
SQL eli Structured Query Language on standardoitu ohjelmointikieli, jota käytettään relaatiotietokantojen kanssa. Tietokannoissa puhuessa SQL-tietokanta on relaatiotietokanta.

NoSQL eli Not only SQL on kieli, joilla kuvataan relaatiomallista poikkeavia tietokantoja. Tämä poikkeama tarkoittaa sitä, että tietokantoihin siirrettävä tieto ei tarvitse olla missään tietyssä muodossa ja tiedostotyyppi voi olla mikä tahansa.

Suurin ero näiden kahden teknologian välillä on tietokantoihin tallennettavien tietojen tietotyyppien osalta. NoSQL tukee myös puolistrukturoitua tietoa, joka mahdollistaa sen, että tiedon ei tarvitse olla standardoidussa muodossa, kun tietoja viedään tietokantaan. [4.]

NoSQL:n suurimpana vahvuutena voidaan pitää sen skaalautuvuutta ilman, että tarvitsee ostaa lisää tietokonekapasiteettia. Viime aikoina NoSQL-alustat ovat yleistyneet vauhdilla myös yrityskäytössä. [4.]

Kuvassa 5 esitellään SQL- sekä NoSQL-erovaisuuksia ja verrataan niiden ominaisuuksia.



Kuva 5: SQL-sekä NoSQL-vertailu tietokantaratkaisuiden ominaisuuksien osalta. [4.]

Kuten kuvassa 5 esitetään, SQL-tietokanta on relaatiokanta, jonka tiedot ovat strukturoidussa muodossa. Tietokannassa vahvuutena voidaan pitää sen tasalaatuisuutta. Haasteena SQL-tietokantojen osalta on niiden skaalautuvuus, joka tarkoitta lähes aina suuremman prosessointitehon tarvetta, joka voidaan toteuttaa usein vain ostamalla tehokkaampia palvelimia.

NoSQL:n osalta voidaan todeta, että se on osittain SQL:n vastakohta. Isoimpana erona ovat jo yllä esitellyt asiat eli puolistrukturoidun tiedon käsittely.

2.3.3 Tietokanta-alustojen vertailu

Tietokantajärjestelmien käyttötarkoituksia on useita ja myös eri valmistajien tekemiä järjestelmiä on useita. Perusperiaatteena voidaan kuitenkin pitää sitä, että mitä suurempi valmistaja, sen parempi dokumentaatio ja usein myös haastavampi käyttöönotto. Tätä voidaan perustella sillä, että niiden hinnat sekä käyttötarkoitus ovat usein suurien yrityksien tarpeisiin sopivia, kun taas uudet edulliset ja ketterät toimijat ovat pienempien yrityksien suosiossa [5.].

Kuvassa 6 on vertailtu 9-järjestelmää, niiden tietostruktuuria, hinnoittelua, dokumentaatiota, skaalautuvuutta, muiden tietotyyppien sietoa sekä oppimisen haasteellisuutta.

Tietokantaalustojen vertailu

Tietokanta järjestelmä	Tietostruktuuri	Lisenssointi	Dokumentaation Laatu sekä saatavuus	Skaalautuvuus	Muut tietostruktuurit	Oppimiskäyrä
MySQL	SQL	GNU, Yleinen lisenssi	Hyvä	Vertikaalinen, Kompleksi	-	Helppo
Maria DB	SQL	GNU, Yleinen lisenssi	Erinomainen	Vertikaalinen	SQL,NoSQL	Helppo
Oracle	Monimallinen, SQL	Lisenssipohjainen	Erinomainen	Vertikaalinen	NoSQL	Vaikea/ Monimutkainen
PostrgeSQL	Objekti Orientoitunut, SQL	Avoin Lähdekoodi	Hyvä	Vertikaalinen	NoSQL	Vaikea/ Monimutkainen
MSSQL server	T-SQL	Lisenssipohjainen	Erinomainen	Vertikaalinen, Kompleksi	SQL,NoSQL	Vaikea/ Monimutkainen
MongoDB	NoSQL, Dokumentaatio orientoitunut	Palvelinpuolen yleinen lisenssi	Erinomainen	Horisonttaalinen	SQL,NoSQL	Helppo
Redis	NoSQL, avainarvot	Avoin Lähdekoodi	Erinomainen	Horisonttaalinen	-	Helppo
Cassandra	NoSQL, sarake orientoitunut	Avoin Lähdekoodi	Erinomainen	Horisonttaalinen	-	Vaikea/ Monimutkainen
Elasticsearch	NoSQL, Dokumentaatio orientoitunut	Avoin Lähdekoodi	Erinomainen	Horisonttaalinen	-	Vaikea/ Monimutkainen

Kuva 6: Tietokanta-alustoiden vertailua [5.].

Kuva 6 vertailee yhdeksää eri tietokantajärjestelmää, niiden ominaisuuksia sekä oppimiskäyrää.

Kuten huomataan yleisimpinä tietostruktuureina ja tietokanta kielinä, ovat SQL sekä NoSQL. Huomiota herättävää oli MSSQL:n osalta Transact SQL-eli T-SQL- kieli, joka on ainoastaan MSSQL:ssä käytössä. Nykyaikana ero T-SQL sekä SQL:n välillä ei ole enää niin suuri vaan voidaan sanoa, että T-SQL on vain murre SQL:stä.

Oppimiskäyrä määriteltiin järjestelmän yleisyyden sekä saatavilla olevan dokumentaation perusteella. Kuten kuvasta 6 huomataan, helpoimpia järjestelmiä oppia on yleisen lisenssin alla olevat MySQL sekä Maria DB. Nämä järjestelmät ovat myös yleisimpiä tietokantajärjestelmiä.

Skaalautuvuudesta puhuttaessa on tärkeä ymmärtää horisontaalisen sekä vertikaalisen skaalautuvuuden erot. Skaalautuvuus on tärkeä osa-alue, kun pohditaan tietokantojen ylläpidettävyyttä sekä sopivuutta yritystoimintaan. Skaalautuvuudella tarkoitetaan sitä, miten tietokantoja tulee päivittää, jotta ne kestävät suuremman tieto- tai käyttömäärän.

Vertikaalinen skaalautuminen on yksinkertaistettuna sitä, että aina, kun tarvitaan lisää kapasiteettia, joudutaan ostamaan tehokkaampia tietokoneita sekä

järjestelmiä. Vertikaalinen skaalautuvuus tarkoittaa siis sitä, että kasvatetaan olemassa olevan kokoa suuremmaksi.

Horisontaalinen skaalautuvuus tarkoittaa sitä, että skaalautuvuus tapahtuu ostamalla lisää samankokoisia tietokoneita.

Yksinkertaistettuna vertikaalinen skaalautuvuus tapahtuu kasvattamalla nykyisten tietokoneiden kokoa. Horisontaalinen skaalautuvuus tarkoittaa tietokoneiden määrän kasvattamista.

Kuvassa 6 huomataan, että SQL-tietostruktuuria käyttävät järjestelmät skaalautuvat pääsääntöisesti vertikaalisesti, kun taas NoSQL-tietostruktuuria käyttävät skaalautuvat horisontaalisesti.

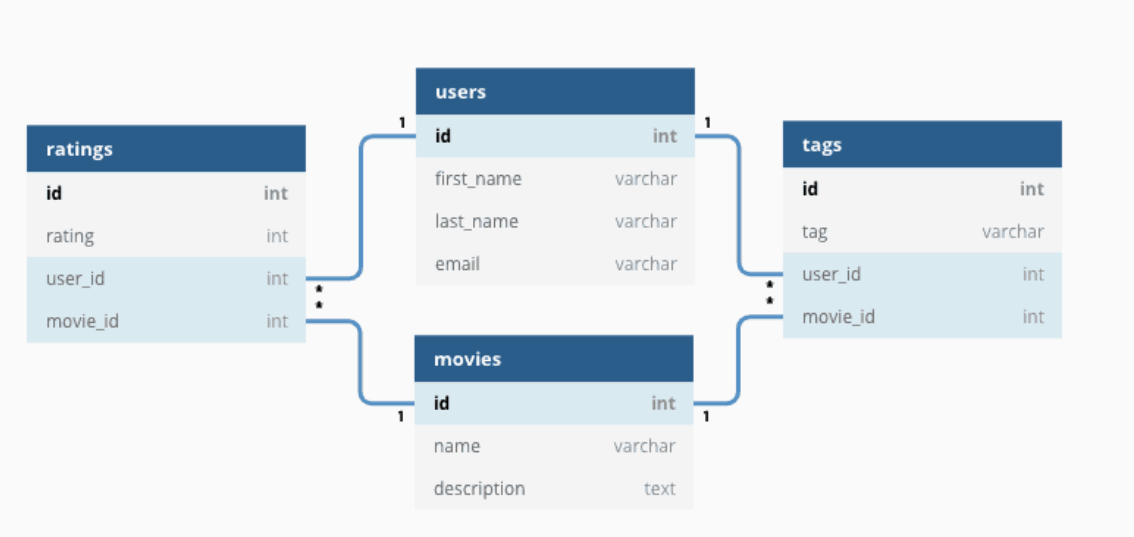
3 Microsoft SQL Server

3.1 Historia

MSSQL-ohjelmiston julkaistiin ensi kerran 1989. Ohjelmiston historiana on, kun 80-luvun lopulla Microsoft ja Sysbase aloittivat yhteistyön, jonka tarkoituksena oli luoda kilpaileva ohjelmisto siihen asti markkinaa hallinnoineen IBM db2 -järjestelmää sekä Oraclen tietokantajärjestelmä vastaan. [6.]

3.2 Relaatiotietokanta

Tässä työssä käytettävä MSSQL on relaatio tietokanta, joka tarkoittaa sitä, että tietokanta sisältää monia eri tauluja, jotka ovat relaation avulla yhdistetty toisiinsa. Kuvassa 7 on esimerkki tietokantojen välisestä relaatiosta [7.].



Kuva 7: Esimerkki tietokannoista löytyviin relaatioihin. [7]

Yllä oleva kuva esittää yksinkertaistetun esimerkin siitä, millainen yksinkertainen relaatiotietokanta voisi olla. Kuvassa nähdään keskellä käyttäjät-(users) sekä elokuvat-(movies) taulut. Näissä tauluissa on molemmissa id-sarakkeet sekä muita tietoja. Kuvan vasemmassa reunassa on arvostelut (ratings) taulu. Kuten kuvassa nähdään, tähän tauluun on luotu relaatio käyttäjät sekä elokuvat taulusta. Tämä mahdollistaa sen, että käyttäjä voi helposti poimimalla arvostelut taulusta Movies_id-numeron löytää kyseisen elokuvan tiedot.

Relaatiotietokannan vahvuutena voidaan pitää sen helppoa skaalautuvuutta, joka mahdollistaa tiedon lisäämisen niin, että ne ovat täysin itsenäisinä muusta tiedosta niin pitkään, kunnes relaatio on toteutettu. Toisena vahvuutena voidaan pitää relaatiokantojen yksinkertaisuutta loppukäyttäjälle. Tämä esiintyy usein siinä, että vaikka tiedot itse tietokannoissa voi olla hyvin kompleksisia itse tiedon haku on usein helppoa [7].

Turvallisuutta voidaan myös pitää relaatiotietokantojen vahvuutena. Tämä perustuu siihen, että koska eri tiedot tulisi periaatteessa olla eri tauluissa. Tällöin eri taulujen näkyvyyttä voidaan rajata eri tavoin ja vain halutut tiedot voidaan

saada näkyville. Viimeisempänä relaatiotietokannat mahdollistavat yhteiskäytön, eli samaa taulua on mahdollista käyttää monen käyttäjän toimista samanaikaisesti [7.].

3.3 MSSQL-pääsynhallinta

MSSQL käyttää kahta eri pääsynhallinta menettelemää, Windows ja SQL-palvelin [8]. Pääsynhallinnalla varmistetaan, että vain tarvittavilla henkilöillä on pääsy MSSQL-palvelimelle.

Windows pääsynhallinta vaatii sitä, että käyttäjä ensin tunnistautuu Windowsiin heidän tunnuksellansa + -salasanalla. Kun käyttäjä on tunnistautunut Windowsiin, he voivat yhdistää itsensä MSSQL:lään. Tämä koko prosessi tapahtuu periaatteessa AD-tunnuksien päällä, ja jotta käyttäjä voi yhdistää itsensä MSSQL-palvelimelle, tulee hänen tunnuksensa olla määritelty pääsy palvelemille. [8.]

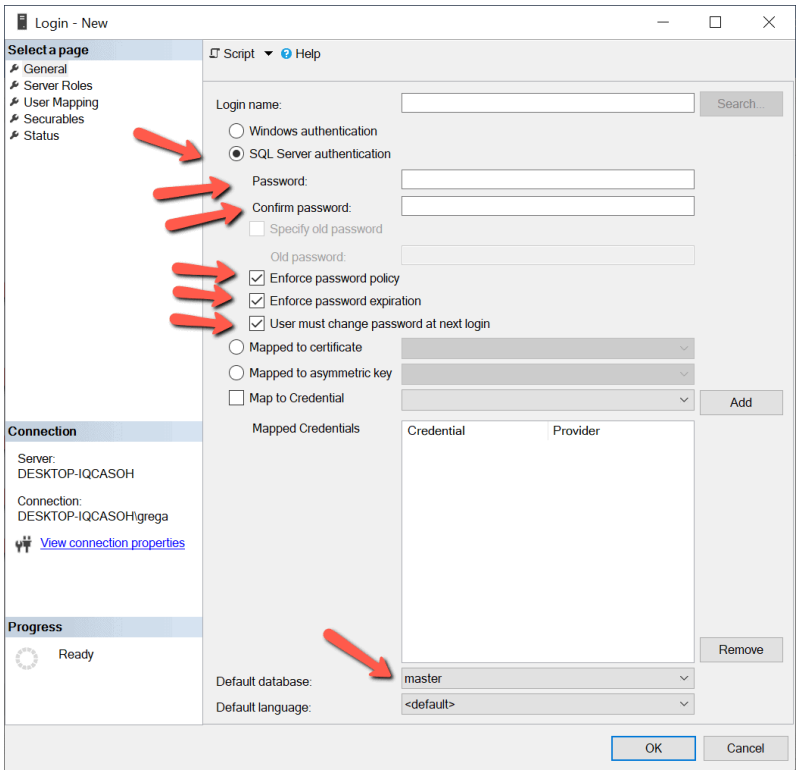
Windows-pääsynhallinta on mahdollista tehdä myös AD-ryhmille, jolloin sisään pääsy vaatii, että on osana määriteltyä AD-ryhmää. AD-ryhmä on vain periaatteessa lista AD-tunnuksia.

Toinen mahdollinen pääsynhallintamenetelmä on SQL- pääsynhallinta. Tämän menetelmän käyttö perustuu pääsääntöisesti siitä, että on olemassa tilanteita, joissa käyttäjällä ei välttämättä ole tarvittavaa AD-tunnusta tai käyttäjä ei ole henkilö vaan esimerkiksi integraatiotyökalu [8]. SQL-pääsynhallinta tarkoittaa yksinkertaistettuna sitä, että luodaan manuaalisesti käyttäjälle tunnus sekä salasana, jotka toimivat pelkästään SQL-Palvelimeen kirjautuessa.

SQL-pääsynhallinta on tietoturvan kannalta hieman heikompi vaihtoehto perustuen siihen, että tunnukset ovat aina käsin luotuja ja elinkaaren hallinta on hankalampaa verrattuna Windows-pääsynhallintaan, joka on sidoksissa käyttäjän Windows-tiliin- [8.]

Kuva 8 esittää, miten SQL pääsynhallintatunnus luodaan MSSQL järjestelmissä ja mitä erinäisiä tietoja siihen tarvitaan. Tietoturvan näkökulmasta on tärkeää

valita nuolella esitetyt kohdat päälle, jotta luodaan mahdollisimman tietoturvallinen ympäristö. [8.]



Kuva 8: SQL-pääsynhallinnan luomisikkuna, jossa punaiset nuolet korostavat kriittisimpiä kohtia.

Kuten kuvassa 8 nähdään, MSSQL antaa mahdollisuuden valita joko Windows-pääsynhallinnan tai SQL-palvelinpääsynhallinnan välillä.

Toisena nuolena on salasananasettaminen. Tähän kohtaan käyttäjän tulee kirjata haluttu salasana ja seuraavaan kohtaan kirjataan salasana uudestaan.

Seuraavana osuutena tulee salasanavaatimuksien eli MSSQL:n määrittelemä salasanavaatimuksen päälle asettaminen. Nämä kaikki kolme kannattaa jättää päälle, koska se mahdollistaa mahdollisimman hyvän tietoturvan. Kolme valintaa on salasana politiikka eli salasanan tulee tiettyjen kriteerien mukainen. Seuraavana on salasanan vanhentuminen eli salasana tulee vaihtaa tietyn ajan välein. Viimeisimpänä on ehkä jopa tärkein kohta eli salasanan vaihto seuraavan

kirjautumisen yhteydessä. Tämä mahdollistaa sen, että pystytään tekemään salasana ja lähettämään salasana käyttäjälle turvallisesti, koska käyttäjän tulee vaihtaa se heti seuraavalla kerralla. Viimeisin nuoli esittää, mihin tietokantaan pääsynhallinta halutaan antaa.

Käytännössä lähes kaikissa yritys ympäristöissä käytetään molempia pääsynhallintamenetelmiä. Tämä perustuu puhtaasti siihen, että kaikkia tarvittavia tunnuksia ei saada/haluta tehdä AD-tilin kautta. Näistä suurimpia ovat erinäiset ulkoiset järjestelmät kuten integraatiotyökalut sekä ulkopuolisten konsulttien tunnukset, joille ei haluta luoda asiakasyrityksen AD-tiliä. [8.]

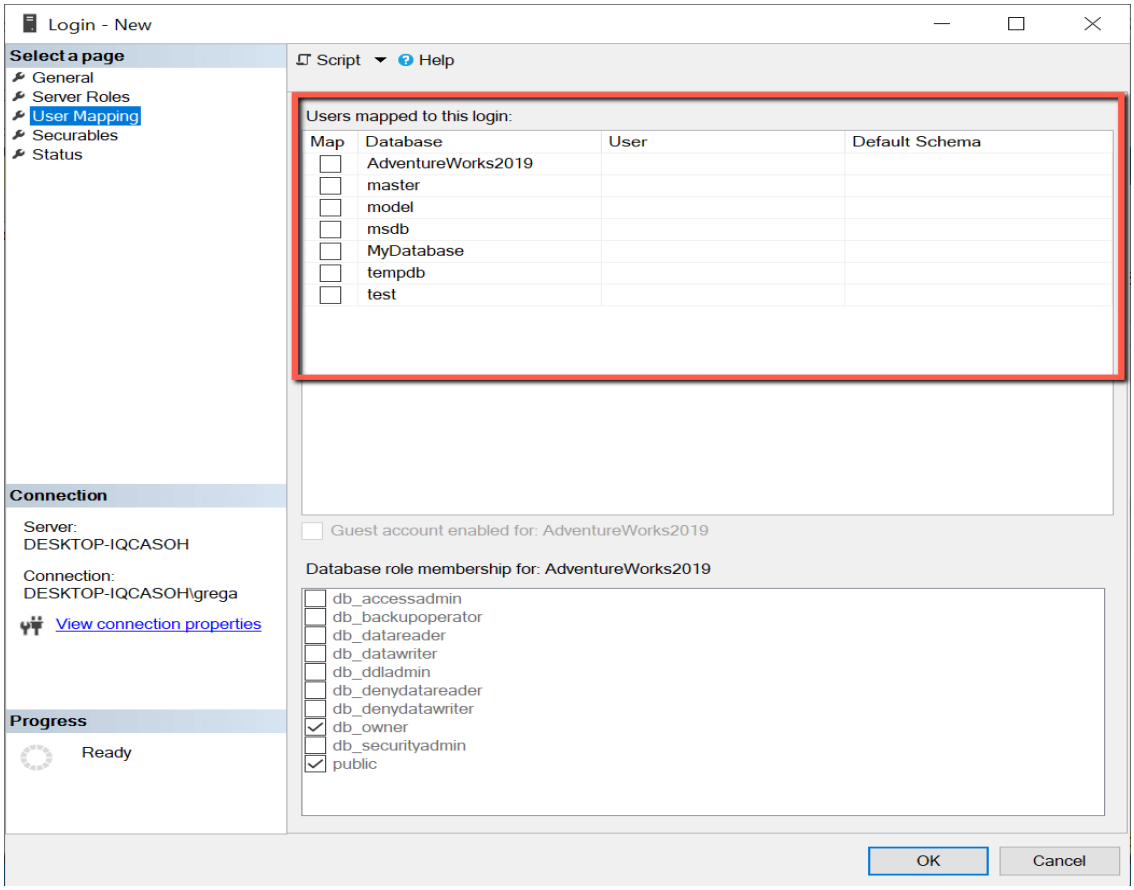
Näitä kutsutaan sisäänkirjautumisiksi, jotka mahdollistavat pääsyn tietokantapalvelimelle. Kaikki uudet sisäänkirjautumistunnukset antavat lähtökohtaisesti oikeudet ainoastaan master-tietokantaan, mutta ei muihin tietokantoihin.

3.4 Tietokantakäyttäjät

Tietokanta palvelemille kirjaudutaan aina joko Windows - tai SQL-pääsynhallinnan avulla. Nämä eivät kuitenkaan mahdollista näkyvyyttä palvelimella oleviin tietokantoihin. Tämä toteutetaan tietokantakäyttäjien avulla.

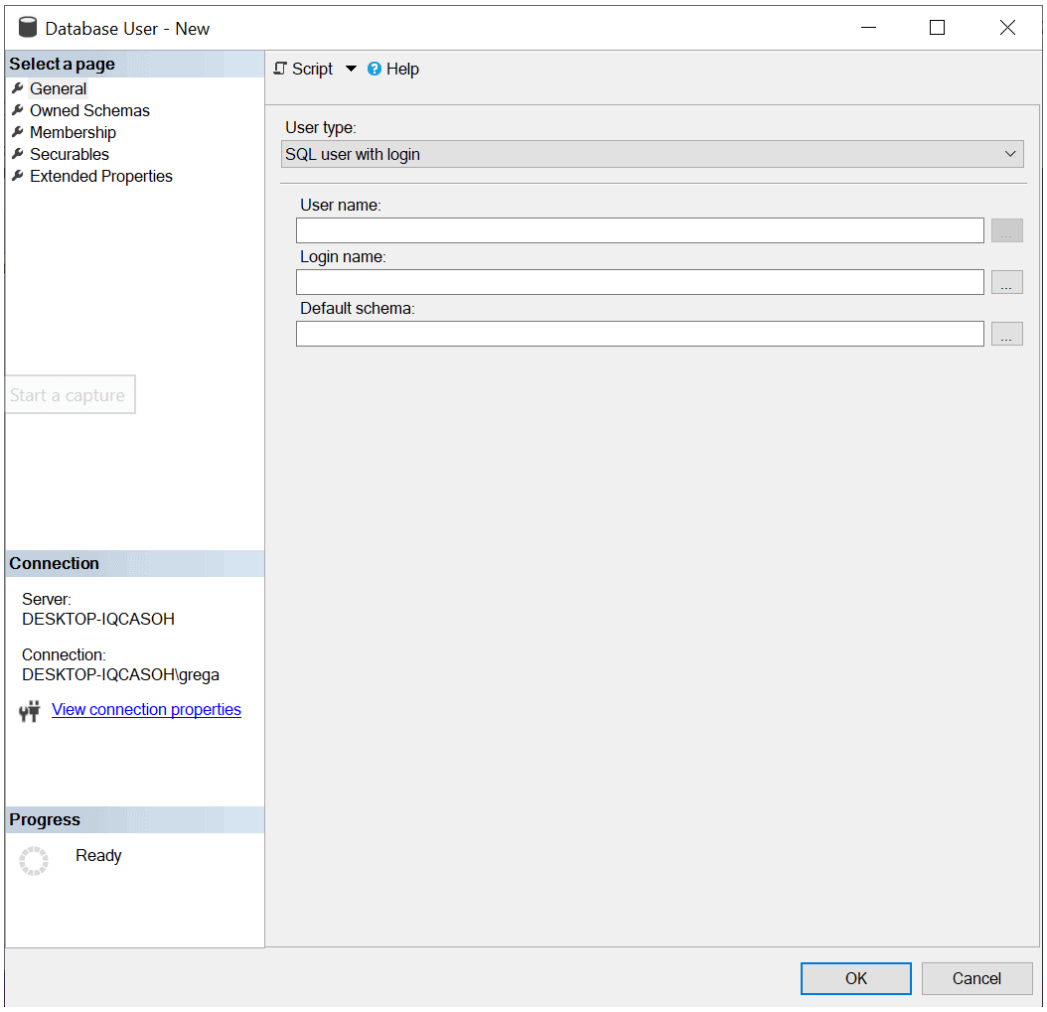
Nämä ovat aina yhteydessä tiettyyn sisäänkirjautumistunnukseen, ja näiden avulla annetaan luvat halutuille tietokannoille. Tätä yhteyttä kutsutaan käyttäjäkartoitukseksi. Tämä voidaan joko toteuttaa tietokantapääsyn luontivaiheessa tai myöhemmin olemassa olevan kirjautumistunnuksen päälle.

Kuvassa 9 esitetään toteutus MSSQL-palvelimella, kun uusi kirjautumistunnus luodaan. Punaisen laatikon sisällä näkyvät kaikki mahdolliset tietokannat, mihin voidaan käyttäjä luoda. Kun laatikkoon User kirjoitetaan nimi, yhdistyy kyseinen kirjautumistunnus ja käyttäjä yhteen. Tällöin käyttäjä saa oikeudet haluttuun tietokantaan.



Kuva 9: Käyttäjäkartoitus, kun luodaan uusi kirjautumistunnus

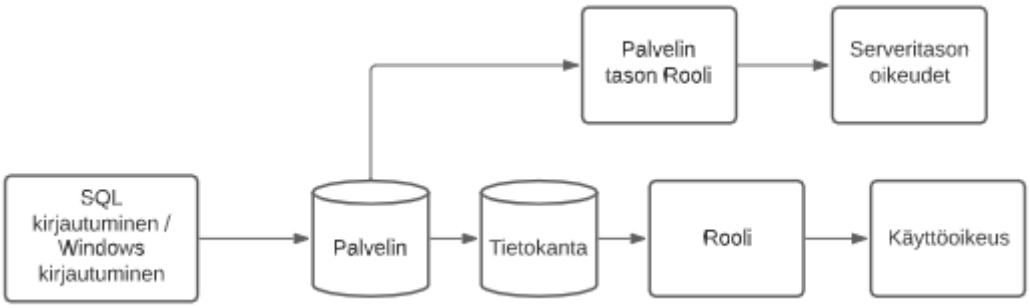
Kun tiettyyn tietokantaan halutaan luoda käyttäjä, joka käyttää jo olemassa olevaa kirjautumistunnusta, valikko on hieman erinäköinen. Tässä on tärkeä varmistua siitä, että valitsee oikean käyttäjätyypin sekä varmistaa, että kirjautumistunnus on varmasti oikea.



Kuva 10: Tietokantakäyttäjän luonti olemassa olevan kirjautumistunnuksen päälle

3.5 Tietokannan käyttövaltuudet

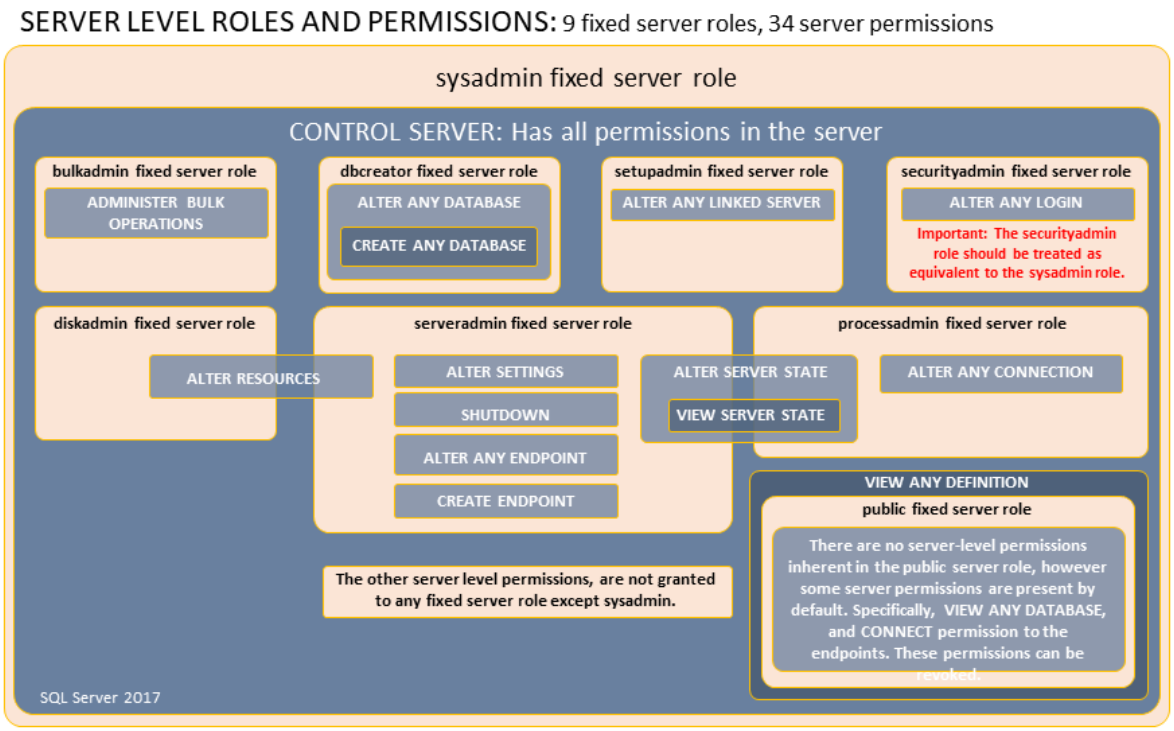
MSSQL-tietokannoissa tietokannan käyttäjä saa erinäisiä oikeuksia, joiden avulla käyttäjä pystyy tekemään haluttuja asioita tietokantaympäristössä. Näitä oikeuksia hallitaan roolien avulla. Kuvassa 12 on esitetty perusprosessi siitä, miten tietokantaoikeuksien prosessi menee.



Kuva 11: Tietokantaoikeuksien antamisen perusprosessi.

Prosessi alkaa siitä, että on luotuna kirjautumistunnus, jolla on oikeus päästä tietokantapalvelimelle. Tämän jälkeen voidaan antaa joko palvelintason tai tietokantatason rooleja. Käyttäjälle annetaan halutut oikeudet, jonka jälkeen hänellä on roolin mukaiset käyttöoikeudet.

On olemassa niin sanottuja palvelintason rooleja, jotka mahdollistavat muutoksien teon sekä muut toimenpiteet itse palvelimella, missä MSSQL on asennettuna Palvelintason roolit sisältävät oikeuksia, joilla voidaan ylläpitää tietokanta palvelimen toimintaa. MSSQL sisältää 9 valmiiksi jaettua roolia sekä 34 oikeutta, joiden avulla toimintoja tehdään palvelimella. Lähtökohtaisesti palvelin oikeuksia ei tulisi jakaa muille, kuin tietokantoja ylläpitäville henkilöille. Tärkeä on huomata roolit järjestelmien ylläpitäjä oikeudet (Sysadmin) sekä turvallisuusylläpitäjäoikeudet (securityadmin), koska nämä kaksi roolia mahdollistavat lähes kaikkien muutoksien teon tietokantapalvelimella. [9.]



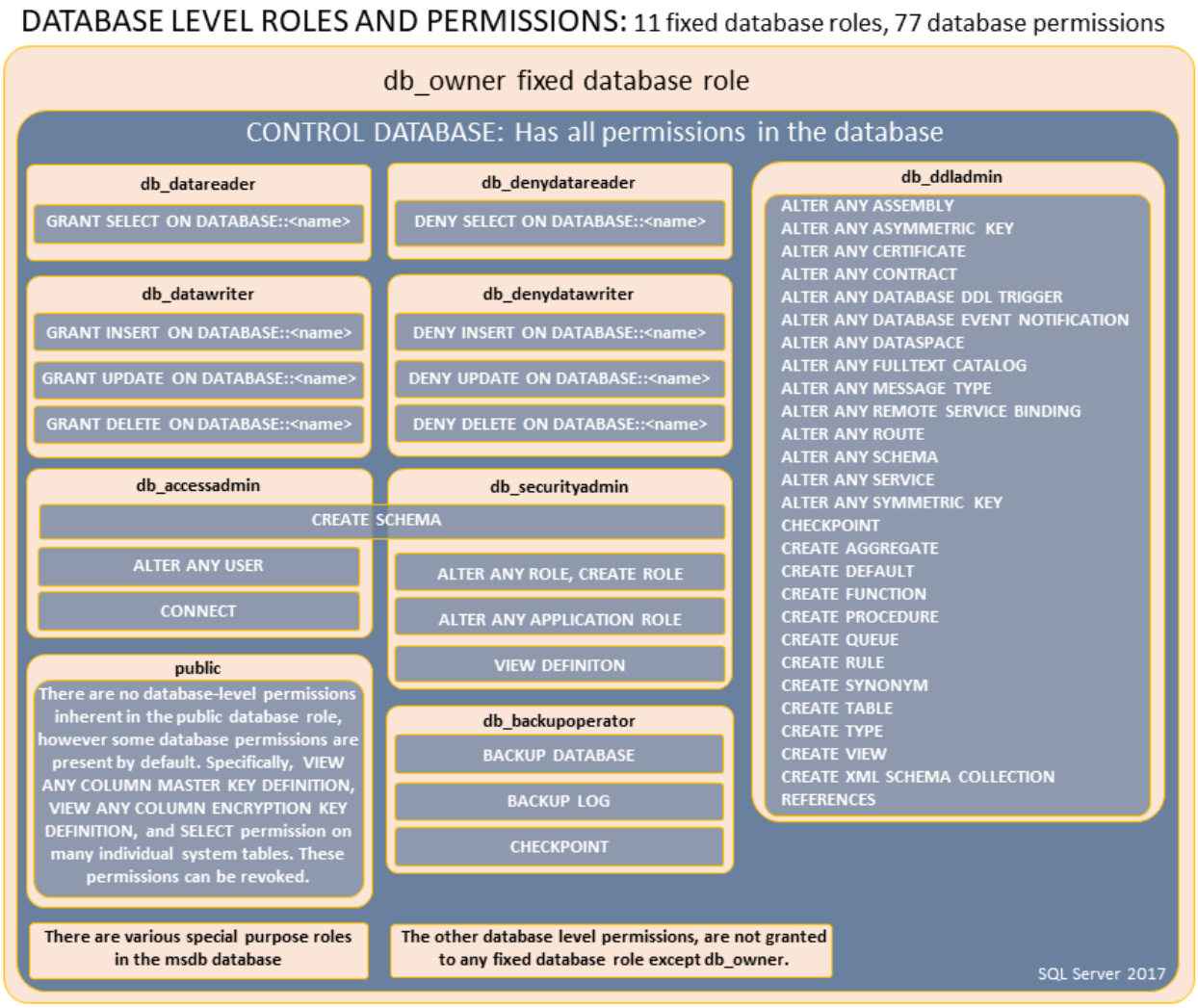
Kuva 12: Tietokantapalvelin tason oikeudet [9]

Kuvassa 12 on esiteltynä valmiit palvelintason roolit, jotka löytyvät MSSQL:sta. Suurimpana roolina ovat sysadmin-oikeudet, jotka mahdollistavat kaikkien muutoksien teon koko palvelimen tasolla. Kuvassa keltaisen laatikoiden yläreunassa oleva teksti on aina kyseisen roolin nimi.Laatikon sisällä olevat siniset laatikot ovat eri oikeuksia, joita kyseisellä roolilla on.

Kuvassa esiintyvät käsitteet ALTER, CREATE, VIEW ovat tiettyjä toimintoja, joita käyttäjä pystyy suorittamaan. ALTER tarkoittaa muutoksien tekemistä, CREATE uuden luomista ja VIEW antaa mahdollisuuden tarkastella eri asioita.

Toisena ryhmänä ovat tietokantatason oikeudet. Näiden oikeuksien tarkoituksena on rajata, mitä käyttäjä voi tehdä tietyn tietokannan sisällä. Tämä työ keskittyy pääsääntöisesti näiden oikeuksien jakoon ja hallintaan. Tämä johtuu siitä, että valtaosa tietokantoihin liittyvistä oikeuksista ovat tämän kaltaisia.

MSSQL sisältää valmiina 11 eri roolia, jotka sisältävät 77 eri oikeutta. Näistä on tärkeä huomata tietokantojen omistajan (db_owner) oikeudet, jotka mahdollistavat kaikki muutokset tiettyyn tietokantaan. [10.]



Kuva 13: Tietokantojen oikeudet [10]

Kuva 13 on hyvin samanlailla kerätty kuin kuva 12. Kuvassa on siis esitettynä Microsoftin valmiit tietokantaroolit ja niihin liittyvät tietokantaoikeudet. Yleisimpinä näistä rooleista voidaan pitää tietokantojen lukuroolia (db_datareader) roolia, joka antaa oikeudet tehdä valintakyselyitä (select) tietokannoissa. Valintakyselyt ovat periaatteessa lukuoperaatioita tietokannoissa, joiden avulla tauluja voidaan lukea.

Näiden valmiina olevien oikeuksien lisäksi MSSQL:n on mahdollista tehdä itse erinäisiä räätälöityjä rooleja. Näille rooleille voidaan lisätä ihan mitä tahansa oikeuksia. Esimerkkikoodissa on näytetty peruspohja SQL-kielellä kirjoitettu ohjelmakoodi, jonka perusteella voidaan luoda uusia rooleja.

```
declare @RoleName varchar(50) = 'RoleName'

declare @Script varchar(max) = 'CREATE ROLE ' + @RoleName + char(13)
select @script = @script + 'GRANT ' + prm.permission_name + ' ON ' + OBJECT_NAME(major_id) + '
TO ' + rol.name + char(13) COLLATE Latin1_General_CI_AS
from sys.database_permissions prm
   join sys.database_principals rol on
      prm.grantee_principal_id = rol.principal_id
where rol.name = @RoleName
```

Esimerkkikoodi 1. Mukautetun tietokantaroolin luomiseen tarvittava ohjelmakoodi

4 Pääsynhallinta

Tässä luvussa käydään läpi pääsynhallinnan perusteita sekä kuvaillaan tulevaisuuden prosesseja, joita niiden hallinnassa tulevaisuudessa tehdään.

4.1 Perusteet

Pääsynhallintaa sekä käyttövaltuushallintaa ohjaa lainsäädäntö sekä mahdolliset yrityksen sisäiset ohjeet sekä toimintamallit. Valtiovarainministeriön Valtiohallinnon tietoturvallisuuden johtoryhmän julkaisemassa ”Käyttövaltuushallinnon periaatteet ja hyvät käytännöt” –ohjeistuksessa suositellaan, että jokaisen organisaation tulisi huolehtia käyttöoikeuksien hallinnoinnista ja määritellä organisaation sisäiset käyttövaltuushallinnan perusteet. [11.]

Organisaatioiden tulisi määritellä ja luoda prosessi, jolla voidaan hallinnoida henkilörekistereitä, tietojärjestelmiä sekä sovellusten käyttöoikeuksia sekä käyttöoikeuksien laajuutta että niiden kestoa.

4.1.1 Käyttövaltuudet

Käyttövaltuushallinnalla tarkoitetaan käyttäjän eli mehiläisen tilanteessa AD-tunnukseen perustuvia käyttöoikeuksiin eri järjestelmissä. Rooleihin perustuva käyttövaltuuden hallinta tarkoittaa sitä, että käyttäjille annetaan erinäisiä rooleja, jotka mahdollistivat tietyt käyttöoikeudet. Perinteisesti eri IT-järjestelmissä käyttöoikeudet jaetaan usein työnkuvan eli roolin pohjalta. Nämä mahdollistavat tiettyjä oikeuksia. On kuitenkin tärkeä ymmärtää, että henkilöllä voi olla useita eri rooleja, jolloin hänellä voi olla myös useita eri oikeuksia. [12.]

Yrityksen tasolla on myös tärkeä eriyttää ulkopuolisten tunnukset ja oikeudet sisäisistä työntekijöistä. Tämä voidaan toteuttaa esimerkiksi luomalla nimeämissäännöt, joilla ulkopuolisille laitetaan aina nimen eteen jonkin tietty lyhenne.

Tärkeä osa käyttövaltuuksien antoa on niin sanottu ”Vähimmän käyttövaltuuden periaate”. Tämä tarkoittaa sitä, että on tarkoituksenmukaista antaa vain niin laajat oikeudet kuin työntekijän työtehtävä vaatii. Ongelmaksi käyttöoikeuksien hallinta muuttuu, jos työntekijöiden oikeuksia joudutaan äkillisesti pienentämään. Tällöin työtapojen muutos on suurempi verrattuna siihen, kun annetaan alusta asti pienin mahdollinen määrä oikeuksia. [12.]

4.1.2 Pääsynhallinta

Pääsynhallinta tarkoittaa lähes samaa kuin käyttöoikeuksien hallinta, mutta sillä tarkoitetaan vain osaa koko siitä prosessista. Pääsynhallinta toteutetaan Mehiläisessä AD-tunnuksen avulla.

Tämä käytännössä tarkoittaa sitä, että oikeudet annetaan lähtökohtaisesti aina joko AD-tunnukselle tai AD-tunnukseen kautta syntyneeseen Office 365-käyttäjälle. On toki ulkopuolisia palveluita sekä muita järjestelmiä, joille pääsynhallinta on toteutettu muilla tavoin. Ongelma täılaisissa tapauksissa on heidän heikompi ylläpidettävyytensä sekä näkyvyys eri alustojen läpi.

Pääsynhallinta siis yksinkertaistettuna mahdollistaa pääsyn järjestelmään, ja käyttöoikeudet antavat mahdollisuuden tehdä siellä järjestelmässä erinäisiä asioita. Nämä kaksi eri asiaa liikkuvat siis aina käsikädessä, eikä työtä voida tehdä laadukkaasti sekä turvallisesti ilman, että molemmat ovat kunnossa.

4.2 Identiteettien ja käyttövaltuuksien hallintaprosessi

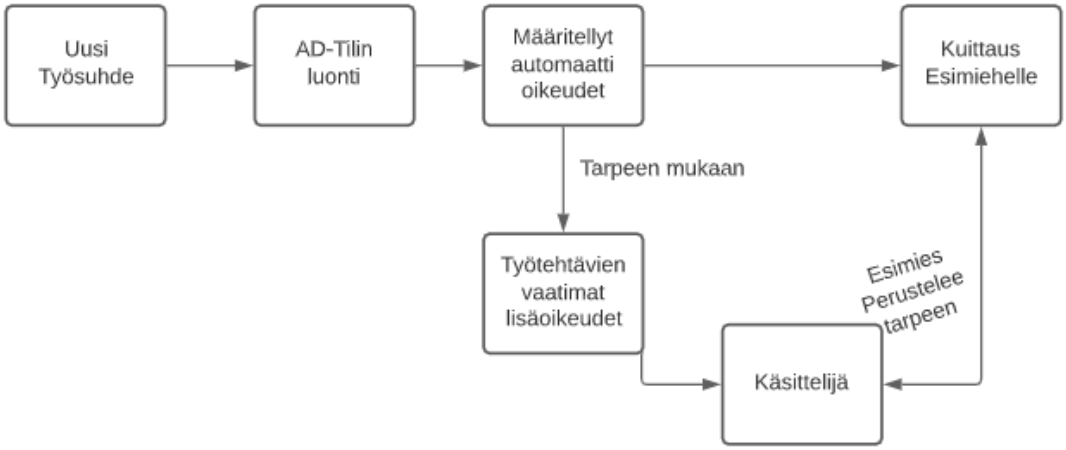
Kun puhutaan Identiteetin ja pääsynhallinnan hallinnasta (IAM) on myös tärkeä korostaa sitä, että se koostuu kahdesta eri osasta. Puhutaan identiteetin hallinnasta (idM) sekä käyttövaltuuksien hallinnasta (AM). [12.]

Identiteetinhallinnalla (Identity Management, IdM) tarkoitetaan prosessia, jossa käyttäjä esitetään digitaalisena identiteettinä tietojärjestelmissä. Muillakin kuin ihmisillä voi olla identiteetti, kuten organisaatioilla tai verkkoon kytketyillä tietokoneilla, mutta tavallisesti identiteetin- ja pääsynhallinnassa keskitytään kuitenkin ihmisten identiteetteihin. Identiteetinhallinta on usein käyttäjän kannalta näkymättömissä tapahtuvaa käyttäjätiedon hallintaa. [12.]

4.2.1 Uuden työntekijän luonti

Tärkeä osa identiteetinhallinta prosessia on luoda järkevä prosessi siihen, miten uusia työtekijöitä luodaan ja miten se prosessi saadaan mahdollisimman sujuvaksi. Tämä mahdollistaa turvallisen ja standardoidun tavan, joilla henkilöiden identiteettiä sekä peruskäyttöoikeuksia voidaan hallita.

Kuva 14 uuden työntekijän luonnista. Tärkeänä on huomata ”Työtehtävien vaatimat lisäoikeudet” jotka vaativat käsittelijää. Tämmöisiä käyttövaltuuksia ovat juuri esimerkiksi tietokanta sekä muiden palveluiden käyttöön vaadittavat oikeudet. Jos näitä tarvitaan, on tärkeä luoda raamit siihen, millä tavalla näitä jaetaan ja dokumentoida tarpeet laadukkaasti, jotta tulevaisuudessa näihin voidaan palata ja on näkyvyyttä siihen, mitä eri iAM-oikeuksia henkilöillä on.



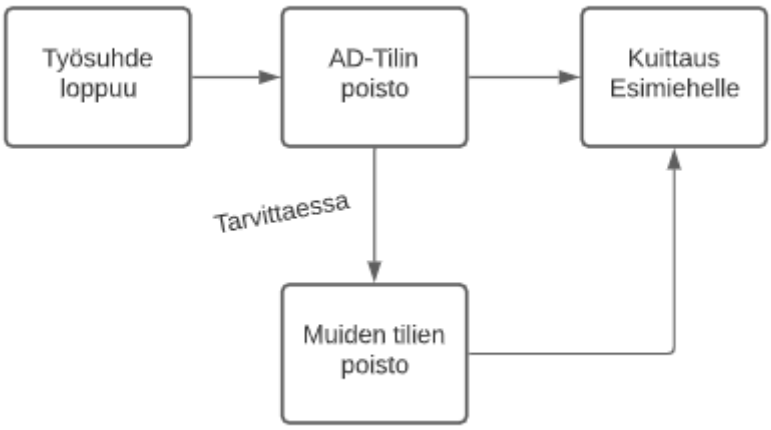
Kuva 14: Uuden työntekijän käyttövaltuuksien hallintaprosessi.

4.2.2 Työntekijän poisto

Kriittisempi osa käyttövaltuuksien hallintaprosessia on oikeuksien poisto työn päättyessä. Työntekijän poistuessa yrityksen palveluksesta tulisi olla luotuna prosessi, joka mahdollistaa työntekijän mahdollisien käyttövaltuuksien mitätöinnin niin, että hänelle ei jää enää käyttövaltuuksia yrityksen järjestelmiin.

Prosessin tärkeimpänä osana on AD-tilin poisto, joka katkaisee pääsyn kaikkiin yrityksen sisäisiin palveluihin sekä muihin paikkoihin, jotka käyttävät AD:ta tunnistautumisessa.

Onnistuneen prosessin mahdollistaa se, että on selkeästi dokumentoituna kaikki ulkoiset järjestelmät, joihin poistuvalla työntekijällä on tunnuksia niin, että ne eivät ole AD:hen linkitettynä. Näiden tunnuksien poisto tapahtuu manuaalisesti, tai jos mahdollista, palvelun hallintoportaallista.



Kuva 15: IAM-prosessi, työsuhteen loppuminen.

5 Pääsynhallinnan malli

5.1 Nykytilanteen kartoitus

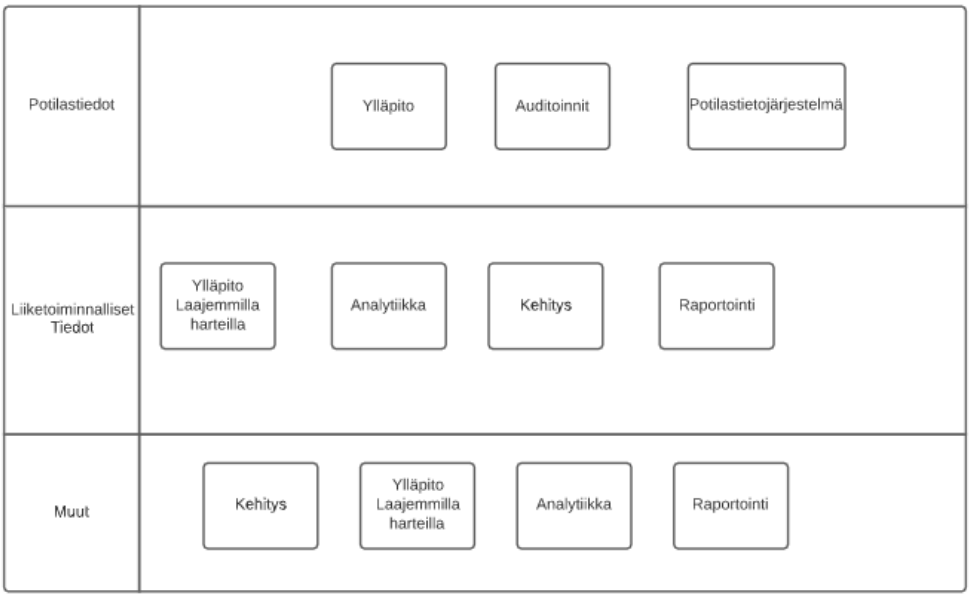
Työ aloitettiin selvittämällä tämänhetkinen tilanne. Tilanne selvitettiin katsomalla kaikki kirjautumistunnukset sekä tietokantojen käyttäjät. Nämä tiedot jaoteltiin palvelintasolla sekä tietokantatasolla eri roolien perusteella. Alun selvitystyön perusteella pystyttiin selkeämmin näkemään tarpeet sekä nykytilanne.

Tämä työ mahdollisti uuden pohjan luomisen sekä prosessin käynnistämisen. Tällä nähtiin myös nykytilanne ja voitiin aloittaa keskustelut siitä, miten tulevaisuudessa pääsynhallintaa halutaan toteuttaa.

Osana tätä prosessia oli myös luoda ymmärrys siihen, mitä muiden tiimien tarpeet tulevaisuudessa olisi, sekä se, miten ne pystyttäisiin toteuttamaan niin, että samalla kyetään ylläpitämään tietoturvaa sekä tietosuojaa.

5.2 Kehitetty malli

Tämän koko prosessin lopputuloksena oli alla oleva kaavio. joka kuvainnollista sitä, mitä eri tietoja meillä on ja mitä toimintoja niiden päällä tulevaisuudessa tulee tapahtumaan.



Kuva 16: Pohjamalli tulevaisuuden mallista, jossa esiintyvät eri tehtävät eri tietokategorioiden välillä

Ylimpänä olevassa laatikossa ovat potilastiedot, jotka ovat Mehiläisen tiedoista arkaluontoisimpia. Niiden näkyvyyttä tulee rajata mahdollisimman pienelle joukolle. Näiden tietoja ei tulisi tulevaisuudessa tapahtumaan muuta kuin aivan välttämätön ylläpito, johon kuuluu erinäisiä tiedonsiirtoja sekä tietokannoissa olevien tietojen ylläpitoa. Toisena osana ovat auditoinnit, joita joudutaan tekemään esimerkiksi luovuttamalla tiedot siitä, keillä kaikilla on näkyvyys tiettyihin tietoihin.

Toki potilastietoihin tulee myös tulevaisuudessa päästä käsiksi myös potilastyössä olevat henkilöt sekä muut siihen oikeutetut henkilöt. Nämä eivät kuitenkaan tapahdu tietokantaympäristössä vaan potilastietojärjestelmän kautta jolloin

heillä ei ole tarvetta saada mitään käyttöoikeuksia tietokantapuolelle potilastietoihin.

Seuraavana ovat liiketoiminnalliset tiedot. Näitä voivat olla esimerkiksi laskutustiedot sekä kaikki muut tiedot, joita kohdeyrityksen kaikki erinäiset järjestelmät synnyttävät. Näiden päälle voidaan luoda jo huomattavasti enemmän toimintoja ja suurena muutoksena se, että ylläpito voidaan siirtää pieneltä ryhmältä hieman suuremman joukon tehtäväksi. Tämä on myös se taso, missä raportointia voidaan aloittaa tekemään.

Viimeisenä tasona ovat ”Muut”, joka sisältää eri järjestelmien tuottamaa tietoa sekä muuta tietoa, jota yritykselle syntyy. Näiden toiminnot ovat lähes identtisiä liiketoimintatietojen kanssa, eikä suurta eroa niiden käsittelyssä synny.

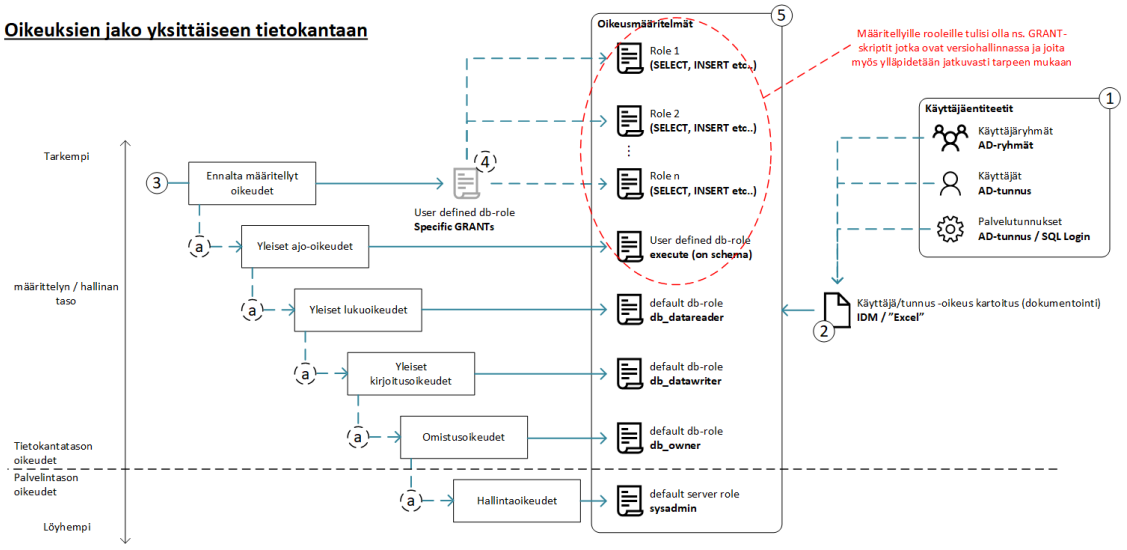
Näitä eri toimintoja varten on luotu tietty määrä AD-ryhmiä, jotka perustuvat rooleihin, jotka tekevät näitä toimintoja. Kuvassa 17 perusrooleja ,joita identifioitiin prosessin aikana.

Kuva 17:AD-ryhmien rooleja. Roolit kuvaavat tulevaisuuden tehtäviä.

5.3 Oikeuksien jakaminen tietokantoihin

Osana työtä luotiin prosessikuvaus, joka on pohjadokumentaatio siitä, miten tulevaisuudessa oikeuksia tulisi jakaa eri tietokantoihin. Tämä tehtiin sen takia, että on tärkeä luoda peruspohja sille, miten tulevaisuudessa toimitaan tämän prosessin aikana.

Kuvassa 18 on tehty kaavio siitä, miten tulevaisuudessa pääsynhallintaa suoritetaan yksittäisen tietokannan osalta.



Kuva 18: Oikeuksien jakamisen prosessikuvaus.

Prosessi on luotu seuraavien askelmien päälle;

1. Onko käyttäjäidentiteetti yhdistettynä tietokantoihin joko AD:n tai SQL kirjautumistunnuksen avulla?

    a. Löytyessä käytetään aina sitä hyväksi.

    b. Jos tunnusta ei vielä löydy, tehdään tunnus joko AD- tai SQL- kirjautumisen avulla.

2. Kirjataan uudet oikeudet haluttuun järjestelmään. Tulevaisuudessa identiteetin hallinnan työkalu tällä hetkellä ”Excel” tai muu taulukkotyökalu.

3. Annetaan Tietokanta tason oikeuksia.

    a. Pyritään aina aloittamaan rooliin valmiiksi luoduilla oikeuksilla.

    b. Mitä syvemmälle kaaviota edetään sen suuremmat oikeudet ovat ja niiden dokumentointi sekä tarpeiden arviointi korostuvat.

Kokonaisuutena tällainen prosessi on askel kohti standardoidumpaa pääsynhallintaa, jolloin kaikilla on selkeä näkyvyys siihen, miten tätä toteutetaan.

5.4 Mallin validointi

Osana työtä suoritettiin myös mallin validointia. Validoiminen tapahtui eri sidosryhmien kanssa käytyjen keskusteluiden avulla.

Keskustelut olivat hyvin vapaamuotoisia, ja ne henkilöt niihin valittiin mahdollisimman laajalta osalta eri liiketoimintoja. Henkilöitä oli niin laatutiimistä, hallinnosta sekä tukipalveluiden toiminnoista. Tämä tehtiin siksi, että kyettäisiin luomaan mahdollisimman laaja näkemys uudistuksen tarpeesta, ymmärrys erinäisistä toimintatavoista sekä eri ryhmien työtehtävistä.

Keskusteluiden pohjilta tehtiin muutoksia lopputuloksena syntyneeseen malliin. Muutoksia oli muun muassa prosessin kehitystä sekä osittain tiukennuksia pääsynhallinnan kriteereihin.

6 Yhteenveto

Eräs suurimmista työn anneista oli yrityksen sisällä syntynyt sisäinen keskustelu ja kommunikaatio aiheen ympärillä. Myös nykyhetken kartoituksella sekä työtehtävien ymmärtämisen tärkeys korostuvat myös tulevaisuudessa, kun organisaatio jatkaa kasvuaan.

Voidaan todeta, että kehitetty malli vaikuttaa hyvin onnistuneelta. Tämä siksi että mallin pohjalta saadaan tulevaisuudessa vähennettyä turhan laajoja käyttövaltuuksia. Työ ja aikaansaatu malli aloittivat keskustelun ja uusien prosessien luonnin kohdeyrityksen työtavoista, jotka koskevat käyttövaltuuksien hallintaa.

Itse mallin kestävyyden osalta on mahdotonta sanoa, miten mallin ylläpidettävyys pystytty toteuttamaan. Tämä johtuu siitä, että kestävyyttä ei voida vielä mitata, kun muutoksesta mennyt aika on niin lyhyt. Kestävyyden osalta asiaa tulee

tarkastella muutaman vuoden päästä uudestaan, jolloin nähdään, miten hyvin malli on toiminut ja kuinka paljon muutoksia malliin on tarvinnut tehdä

Suurimpana kehityskohteena voidaan pitää sitä, että työ ei ota kantaa siihen, miten suurta organisaatioallista sekä asennemuutosta tämmöisen muutoksen läpivienti vaatii yrityksen tasolla. Kuitenkin kun tehdään näin laajaa muutosta, niin myös organisaatio ja tietyt avainhenkilöt pitäisi saada mukaan paremmin muutokseen, jotta muutos saataisiin vietyä läpi organisaation. Tältä osin tulevaisuudessa tällaisia muutoksia tehdessä ottaisin vielä vahvemmin muita mukaan projektin tekoon.

Pääsynhallinnan osalta voidaan todeta, että vaikka on olemassa yleismaailmallisia ohjeita siitä, miten sitä tulisi organisaatiossa ylläpitää, on kuitenkin jokaisen yrityksen löydettävä omiin tarpeisiinsa toimiva malli.

Itse opinnäytetyön osalta huomataan, että työltä puuttui vahva tutkimuksellinen teoriapohja, sekä siitä osittain johtuva struktuurin sekä teoriapohjan puute. Esimerkiksi konstruktiivinen tutkimus olisi voinut selventää työn tekoa huomattavasti ja luoda sille teorian, jota vasten on helpompaa tehdä.

Lähteet

1. Mehiläinen OY. Mehiläinen yrityksenä. Verkkoaineisto. < https://www.mehilainen.fi/yritysinfo/mehilainen-yrityksena> Luettu 20.9.2021.

2. SQL server central. Verkkoaineisto. < https://www.sqlservercentral.com/wp-content/uploads/2013/05/2020-12-02-14_15_42-SQLQuery11.sql-sqlservercentralpublic.database.windows.net_.AdventureWorks-ssc.png>. Luettu 20.9.2021.

3. Splunk. What is a data platform. Verkkoaineisto. < https://www.splunk.com/en_us/data-insider/what-is-a-data-platform.html#overview>. Luettu 20.9.2021.

4. Satish Chandra Gupta . SQL vs. NoSQL Database: When to Use, How to Choose. Verkkoaineisto. < https://towardsdatascience.com/datastore-choices-sql-vs-nosql-database-ebec24d56106>.Luettu 20.9.2021.

5. Altexsoft. Comparing Database Management Systems: MySQL, PostgreSQL, MSSQL Server, MongoDB, Elasticsearch and others. Verkkoaineisto. < https://www.altexsoft.com/blog/business/comparing-database-management-systems-mysql-postgresql-mssql-server-mongodb-elasticsearch-and-others/>. Luettu 20.9.2021.

6. 2008 R. Mohan T K Nithin. Evolution of SQL Server from SQL 2000 to SQL Server. Verkkoaineisto. < https://www.nitrix-reloaded.com/2010/05/09/evolution-of-sql-server-from-sql-2000-to-sql-server-2008-r2/ >. Luettu 20.9.2021.

7. OMNI-SCI. Relational Database. Verkkoaineisto. < https://www.omnisci.com/technical-glossary/relational-database>. Luettu 22.9.2021

8. Greg Larsen.SQL Server authentication methods, logins, and database users. Verkkoaineisto. <https://www.red-gate.com/simple-talk/home-page/sql-server-authentication-methods/>. Luettu 20.9.2021.

9. Microsoft.Server-Level Roles. Verkkoaineisto. <https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/server-level-roles?view=sql-server-ver15>.Luettu 23.9.2021.

10. Microsoft. Database-Level Roles. Verkkoaineisto. < https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver15 >. Luettu 23.9.2021.

11. Valtiovarainministeriö. VAHTI. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt. 2006. Verkkoaineisto < https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_9_2006.pdf>. Luettu 20.9.2021.

12. Linden, Mikael. 2015. Identiteetin- ja pääsynhallinta. Tampereen teknillinen yliopisto. < https://trepo.tuni.fi/bitstream/handle/10024/116698/linden_identitee-tin_ja_paasynhallinta.pdf?sequence=1&isAllowed=y>. Luettu 23.09.2021.