Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Samuli Virtanen

Kulunvalvontasovelluksen prototyyppi

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

28.4.2021

Tekijä Otsikko Sivumäärä Aika	Samuli Virtanen Kulunvalvontasovelluksen prototyyppi 32 sivua + 2 liitettä 28.4.2021
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ammatillinen pääaine	Mobile Solutions
Ohjaajat	Yliopettaja Kari Salo Turvallisuusupseeri Tomi Jauho

Insinöörityön tavoitteena oli kehittää ja tehostaa asiakasorganisaation lupahallintoprosessia ja kulunvalvontaprosessia tuottamalla kulunvalvontasovelluksen prototyyppi osana nykyaikaisen ja tietoturvallisen lupahallintosovelluskokonaisuuden suunnittelutyötä. Insinöörityössä muodostettiin lupahallinnon ja kulunvalvonnan kokonaisprosessikuvaus sovelluskokonaisuuden suunnittelu- ja toteuttamistyön tueksi. Insinöörityössä tutkittiin sovelluskokonaisuuden suunnittelun ja loppukäyttöliittymien kannalta olennaisia, soveltuvia pääsyoikeuden varmentamismenetelmiä ja henkilöllisyyden tunnistamismenetelmiä, joita ovat esimerkiksi erilaiset henkilötodistukset ja etäluettavat tunnisteet.

Kulunvalvontasovelluksen prototyypin toteutukseen valittiin Electron-hybridikehitystyökalu ja JavaScript-teknologia. Prototyyppi suunniteltiin huomioiden asiakkaan vaatimusmäärittelyt ja loppukäyttöympäristön erityispiirteet. Taustapalvelinjärjestelmä kehitettiin taustapalvelinohjelmiston, ohjelmointirajapinnan ja tietokannan osalta niin, että se palvelee kulunvalvontasovelluksen prototyypin välttämättömiä toimintoja. Kulunvalvontasovelluksen prototyyppiä testattiin erillisessä testausympäristössä, ja testauksesta kerättiin palautetta ja havaintoja jatkokehitystä varten.

Lopputuloksena valmistui tavoitteiden ja asiakkaan vaatimusmäärittelyiden mukainen, moderneja ja tietoturvallisia teknologioita käyttävä sovellus ja erillinen suunnitelma sovelluskokonaisuudesta. Insinöörityössä toteutettua sovellusta ja sovelluskokonaisuuden suunnitelmaa on mahdollista jatkokehittää tehdyn työn aineiston perusteella.

Avainsanat	kulunvalvonta, lupahallinto

Author	Samuli Virtanen
Title	Visit control application prototype for checkpoint
Number of Pages	32 pages + 2 appendices
Date	28 April 2021
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Professional Major	Mobile Solutions
Instructors	Kari Salo, Principal Lecturer Tomi Jauho, Security Officer

The purpose of this bachelor thesis was to improve and streamline the customer's permission administration and visit control processes by producing a prototype of visit control checkpoint application as a part of the design work for a modern and secure permission administration software. A comprehensive description of the customer's permission administration and access control process was made to support the designing and creation work of the entire permission administration software. The methods of verifying the access rights and person identification which are essential in terms of software design and end-user interfaces were examined in the work. Previously mentioned essential methods include for example various identity cards and remotely readable contactless tags.

Electron hybrid development tool and JavaScript programming language were chosen to build the visit control checkpoint application prototype. The prototype was designed considering the customer's requirement specification and the characteristics of the end-use location. Regarding the back-end services, a back-end server software, application programming interface and database were developed to only meet the essential functions required by the visit control checkpoint application. The prototype was tested in a separate testing environment and feedback was gathered for the further software development.

As a result, based on the set targets and customer's requirement specifications, a working software application was developed using modern and secure technologies. A separate plan of the permission administration software product family was also prepared. Checkpoint application prototype and software product family plan can be developed further based on this thesis.

Keywords	Access control, visit control, permission administration

Sisällys

Lyhenteet

API	Application programming interface. Ohjelmointirajapinta.
DNA	Deoksiribonukleiinihappo on nukleiinihappo, joka sisältää kaikkien eliöiden solujen ja joidenkin virusten geneettisen materiaalin.
GDPR	General Data Protection Regulation. Euroopan unionin yleinen tietosuoja-asetus, 2016/679.
HTML	Hypertext Markup Language. Avoimesti standardoitu kuvauskieli, jolla voidaan kuvata hyperlinkkejä sisältävää tekstiä eli hypertekstiä.
HTTP	Hypertext Transfer Protocol. Protokolla, jota mm. selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
JSON	JavaScript Object Notation. Avoimen standardin tiedostomuoto.
LAN	Local Area Network. Rajoitetulla maantieteellisellä alueella toimiva tietoliikenneverkko.
MVC	Model-View-Controller. Ohjelmistoarkkitehtuurimalli.
NFC	Near-field communication. Lyhyen kantaman tunnistautumis- ja tiedonsiirtoprotokolla.
PHP	PHP: Hypertext Preprocessor. Tulkattava komentosarjaohjelmointikieli.
PIN	Personal identification number. Tunnusluku tai PIN-koodi.
REST	Representational State Transfer. HTTP-protokollaan perustuva arkkitehtuurimalli ohjelmointirajapintojen toteuttamiseen.
RFID	Radio Frequency Identification. Radiotaajuudella toimiva etätunnistusmenetelmä.

SMS	Short Message Service. Lyhyt viesti, joka lähetetään matkapuhelinverkossa.
SQL	Structured Query Language. IBM:n relaatiotietokannoille kehittämä standardoitu kyselykieli.
SSL	Secure Sockets Layer. Tietoverkkosalausprotokolla.
QR	Quick Response, QR-koodi eli ruutukoodi on kaksiulotteinen kuviokoodi, johon on koodattu informaatiota.

1 Johdanto

Insinöörityön tavoitteena on kehittää ja tehostaa asiakasorganisaation lupahallintoprosessia ja kulunvalvontaprosessia tuottamalla kulunvalvontasovelluksen prototyyppi osana modernin ja nykyaikaisen lupahallintosovelluskokonaisuuden suunnittelutyötä, joka valmistuessaan soveltuu minkä tahansa yrityksen tai organisaation käyttöön. Käytännössä tavoitteet ovat lupahallintoon käytetyn työmäärän vähentäminen, tietoturvan parantaminen, kulkuluvan hakuprosessin nopeuttaminen, tiedonvälityksen automatisointi, lupahallintoon liittyvien muiden prosessien yhdistäminen yhteen sovelluskokonaisuuteen ja ekologisuuden tehostaminen vähentämällä paperipohjaisen aineiston käytön tarvetta.

Turvallisuusalaan ja turvallisuuteen liittyvät ohjelmistot ovat haastava tutkimuksen ja kehittämisen kohde. Alan vakiintunut ja mielestäni osin vanhanaikainen ajatus vaikuttaa olevan, että tiedon kokonaisvaltainen salaaminen on aina osa turvallisuutta, vaikka tämä ei kaikilta osin pidä paikkaansa. Kaupallisista turvallisuusalan ohjelmistoista ja sovelluksista on likipitäen mahdotonta löytää esittelymateriaalia tarkempaa tietoa julkisista lähteistä. Ohjelmistojen valmistajat eivät yleensä edes julkaise järjestelmiensä käyttöohjeita julkisesti internetissä. Kaikkien tutkittujen sovelluskokonaisuuksien loppukäyttöliittymät oli toteutettu joko Microsoft Windows -sovelluksina, selainversioina tai Android-loppukäyttöliittyminä. Pääkäyttöliittymien osalta korostui Windows-rajapinta: lähes jokainen pääkäyttöliittymä oli Windows-sovellus. Tähän voi olla syynä Windows-alustan vahva historia teollisuudessa ja teollisuuden käyttämissä sovelluksissa (Why are Windows PCs So Popular in Industrial Automation? 2016). Poikkeuksena olivat kosketusnäytölliset loppukäyttöliittymät, joissa oli mahdollisuus pääkäyttäjätoiminnallisuuksiin. Tutkitut, kosketusnäytölliset loppukäyttöliittymät oli toteutettu aina käyttäen Android-laitteita. Androidin suurimpia vahvuuksia on erittäin laaja laitteistovalikoima, kustannustehokkuus sekä nopea ja ketterä ohjelmoitavuus.

Sovelluskokonaisuuden suunnittelutyön tavoitteena on tuottaa suunnittelutyön ja toteuttamisen tukimateriaalia kaupallisen sovelluskokonaisuuden tuottamiseen liittyen. Sovelluskokonaisuus on suunniteltu yleiseen käyttöön liittyviä vaatimuksia noudattaen, ja se on sovellettavissa minkä tahansa yrityksen tai yhteisön toimintaan.

Kulkulupahallinnon tehostaminen koskee monia erilaisia organisaatioita ja käyttöympäristöjä. Pääsyoikeuksien haku tulee olla järjestetty mahdollisimman helppokäyttöiseksi. On myös tärkeää, että ne henkilöt, joilla on pääsyoikeus, pääsevät liikkumaan pääsyoikeusrajoitetuissa kohteissa, vaikka he kadottaisivatkin yleensä käyttämänsä kulkutunnisteen tai -välineen. On myös tärkeämpää, että henkilöt, joilla ei ole pääsyoikeutta pääsyoikeusrajoitettuun kohteeseen, eivät pääse valvotulle vyöhykkeelle tai kohteeseen lainkaan. Tämän insinöörityön tavoitteena on myös herättää ajatuksia pääsyoikeuksien hallinnasta ja valvonnasta minkä tahansa organisaation toimintaan liittyen.

2 Kulkulupahallinto- ja kulunvalvontaprosessi

2.1 Kokonaisprosessi

Kulkulupahallinnon ja kulunvalvonnan kokonaisprosessi käsittää henkilöiden pääsyoikeuksien määrittämisen erilaisiin kulunvalvottuihin kohteisiin, kuten esimerkiksi kulunvalvottuihin alueisiin, kiinteistöihin ja vyöhykkeisiin sekä myös tarvittaessa kulunvalvonnan kohteissa vierailuihin ja kohteisiin pääsyyn. Kokonaisprosessi onkin loogista jakaa kahteen pääosa-alueeseen: kulkulupahallintoprosessiin, ts. lupahallintoprosessiin ja kulunvalvontaprosessiin. Lupahallintoa ja kulunvalvontaa suorittavat yritykset ja muut tahot sellaisissa kohteissa joihin pääsyä halutaan rajoittaa ja tarvittaessa myös valvoa.

Kokonaisprosessin eri osa-alueissa tarvitaan erilaisia pääsyoikeuden tunnistamis- ja varmentamismenetelmiä. Näitä menetelmiä ovat mm. erilaiset henkilötodistukset, ajokortti, passi, etäluettavat tunnisteet, biometriset tunnistusmenetelmät ja salasanat. Kokonaisprosessin kannalta tärkeimmiksi oletettuja pääsyoikeuden tunnistamis- ja varmentamismenetelmiä on selvitetty osana tätä insinöörityötä.

2.2 Pääsyoikeuden tunnistamis- ja varmentamismenetelmät

Lupahallintoprosessin eri vaiheissa tarvitaan erilaisia henkilöllisyyden ja pääsyoikeuden varmentamismenetelmiä. Esimerkiksi pääsyoikeutta haettaessa ja erityisvalvottuun kohteeseen pyrittäessä tarvitaan usein henkilötodistusta ja vahvaa henkilöllisyyden tunnistamismenetelmää, kun taas pääsyoikeuden myöntämisen jälkeen tunnistamiseen voidaan monissa sovelluksissa käyttää etäluettavaa tunnistetta tai jotain muuta vastaavaa menetelmää.

Pienemmissä organisaatioissa työntekijät yleensä tuntevat toisensa ja päivittäinen kulunvalvonta toimii avain- ja kulkutunnistehallinnan (etäluettavat tunnisteet) lisäksi osittain myös työntekijöiden tekemänä heidän tunnistaessaan muut kohteessa liikkuvat henkilöt. Työntekijöiden omatoimisesti suorittamaa alueella liikkuvien henkilöiden tunnistamista ja valvontaa ei voida kuitenkaan pitää varsinaisena valvontamekanismina jo pelkästään juridisesta näkökulmasta tarkasteltuna, koska tällöin syntyy vastuukysymyksiä ja niihin liittyviä ongelmakohtia. Lisäksi henkilöiden aktiivisuuden omatoimisesti suoritettavassa valvonnassa määrittää pääosin henkilöiden oma motivaatio ja intressit valvonnan suorittamista kohtaan. Vaikuttamalla yrityksen tai organisaation yleiseen turvallisuuskulttuuriin voidaan omatoimisen valvonnan suorituskykyä parantaa jonkin verran, mutta mikäli valvontaan tarvitaan luotettava valvontamekanismi, on se määritettävä erikseen.

Pienemmissäkin kohteissa keskitetty, henkilötiedot ja pääsyoikeudet sisältävä pääsyoikeusrekisteri mahdollistaa myös kolmansille osapuolille, kuten esimerkiksi vartiointiliikkeille, luotettavan ja helposti ylläpidettävän rekisterin luvallisista kohteissa vierailevista henkilöistä esimerkiksi hälytyksen tarkastustehtävällä tai muuhun valvontaan liittyen. Tämänkaltainen, keskitetty pääsyoikeusrekisteri voisi mahdollistaa esimerkiksi asunto-osakeyhtiön käyttämälle huolto- ja kunnossapito-organisaatiolle luotettavan tavan varmistaa henkilön pääsyoikeus kiinteistöön tai asunto-osakkeeseen tilanteessa, jossa asukas on unohtanut omat avaimensa sisälle kiinteistöön ja tarvitsee ulkopuolisen tahon apua sisäänpääsyn mahdollistamiseksi.

Henkilötodistukset

Henkilöllisyyden todentamiseen on useita eri asiakirjoja. Suomen kansalaisten osalta passi, henkilökortti ja osittain myös ajokortti ovat voimassaoloajan puitteissa yleisesti käytössä olevia, poliisin myöntämiä asiakirjoja henkilöllisyyden todentamiseen Suomessa. Lisäksi eri organisaatioilla on omia, sisäisessä käytössä hyväksyttäviä henkilötodistuksia, joita ovat esimerkiksi yritysten omat, kuvalliset henkilötodistukset tai -kortit, viranomaisten osalta virkamerkit, henkilökortit ja mahdollisesti myös muut kortit ja todistukset.

Ulkomaalaisten henkilöiden henkilöllisyyden todentamiseen yleisimmin käytettäneen muiden valtioiden myöntämää passia. Muut valtiot myöntävät myös muita asiakirjoja, joista henkilöllisyys voidaan todentaa, mikäli henkilöllisyyden tarkastaja pitää tällaista asiakirjaa riittävän luotettavana. Tällaisia asiakirjoja ovat esimerkiksi Euroopan unionin myöntämä ajokortti tai vieraan valtion myöntämä muu henkilötodistus.

Jokainen organisaatio määrittää itse, minkälaisia asiakirjoja voidaan käyttää henkilöllisyyden todistamiseen. Ajokortin asema henkilöllisyyden todistamiseen soveltuvana asiakirjana on viime aikoina heikentynyt (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta 1009/2018). Euroopan unionin alueella yleisesti hyväksytään kuitenkin EU-alueen jäsenmaan myöntämä passi sekä henkilökortti tai -todistus. Julkisen sektorin osalta näitä todistuksia on määritelty laein: Henkilökorttilaki 663/2016; Ajokorttilaki 386/2011; Laki puolustusvoimista 551/2007; Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009; Puolustusministeriön asetus oleskelu- ja vierailuluvista, kieltotauluista, vartio- ja päivystystehtävää suorittavan virkamiehen koulutuksesta sekä ammattisotilaan perustaidoista ja kunnosta 1253/14.12.2007

Etäluettavat tunnisteet

Etäluettavat tunnisteet ovat yleensä radiotaajuudella toimivia etäluettavia tunnisteita, joissa käyttöoikeuden tai henkilöllisyyden tunnistaminen perustuu yksilöiviin, langattomasti luettaviin mikropiireihin. Hyvin yleisiä teknologioita ovat mm. RFID (Radio Frequency Identification) ja NFC (Near-field communication). RFID on käytössä yleisesti

mm. sähköisissä kulkutunnisteissa, julkisen liikenteen matkakorteissa ja teollisuudessa. NFC:n yleisesti tunnetuin sovellus on todennäköisesti pankkikorttien ja puhelimien lähimaksuominaisuus (Nieminen 2017; Sonali ym. 2017).

Viivakoodia ja nykyisin yleisimmin käytössä olevaa QR-koodia (Quick Response) voidaan pitää myös etäluettavina tunnisteina (ISO/IEC 15417:2007, ISO/IEC 18004:2015). Nämä koodit voi mieltää myös salasanoiksi, koska ne ovat visuaalisesti nähtynä yhtä helposti kopioitavissa kuin paperille kirjoitetut salasanatkin. Käyttäjät eivät yleensä tiedosta, että viivakoodien ja QR-koodien kopiointiin ei vaadita yksinkertaisimmillaan mitään muuta kuin matkapuhelimen kamera. Tämän havainnon voi jokainen helposti todeta hieman tarkkailemalla ihmisten käyttämiä asiakirjoja, laitteita ja kortteja esimerkiksi julkisessa liikenteessä, julkisissa paikoissa tai lentokentillä. Harva edes suojaa PIN-koodiaan näppäillessään sitä maksupäätteeseen tai muuhun vastaavaan laitteeseen maksutapahtuman tai tunnistautumisen yhteydessä. Viivakoodien ja QR-koodien sisältämä data voi usein sisältää henkilötietoja. Esimerkiksi valokuva suomalaisen ajokortin etupuolelta, jossa on peitetty ainoastaan tekstimuodossa oleva henkilötunnus, sisältää edelleen henkilötunnuksen helposti luettavassa muodossa viivakoodina.

Etäluettavien tunnisteiden käyttöä ainoana tunnistamismenetelmänä ei voida pitää kovinkaan luotettavana henkilöllisyyden tunnistamismenetelmänä, koska niitä voidaan aina kopioida ja myös käyttää luvattomasti. Pelkästään etäluettavaan tunnisteeseen perustuva pääsyoikeus kohteeseen on täysin verrattavissa mekaaniseen avaimeen, joka kadotettuna, kopioituna tai luvattomasti käytettynä on kenen tahansa käyttäjän käytettävissä ja täten mahdollistaa pääsyn kohteeseen mekaanisen avaimen tapaan.

Henkilöllisyyden tunnistamista etäluettavien tunnisteiden käytön avulla voidaan parantaa käyttämällä yhtä tai useampaa tunnistamismenetelmää etäluettavan tunnisteen käytön yhteydessä. Sopivia lisämenetelmiä ovat esimerkiksi PIN-koodin (Personal Identification Number) näppäileminen etäluettavan tunnisteen lukijalaitteeseen, erillisen salasanan tai biometristen tunnistamismenetelmien käyttö ja kaksivaiheisen tunnistamisen muut menetelmät.

Biometriset tunnisteet ja tunnistamismenetelmät

Todennäköisesti yleisin käytössä oleva biometrinen tunnistamismenetelmä henkilön tunnistamiseen on valokuva. Valokuvaa käytetään lähes jokaisessa henkilön tunnistamismenetelmässä, ml. henkilöllisyystodistukset ja kaikki muut vastaavat asiakirjat. Muita yleisiä biometrisen tunnistuksen sovellutuksia ovat esimerkiksi useissa laitteissa käytössä olevat sormenjälkien- ja kasvojentunnistusmenetelmät. Lisäksi hieman harvinaisemmat tunnistusmenetelmät, kuten esimerkiksi käsialanäyte, verkkokalvojen tunnistus ja DNA-tunniste (deoksiribonukleiinihappo), soveltuvat joko tunnistamismenetelmiksi tai ainakin varmennusmenetelmiksi joissakin sovellutuksissa.

Hyvin yleinen, yksinkertainen biometrinen tunniste on myös ihmisen fyysinen koko. Tätä menetelmää käytetään mm. kuntosalien, lentokenttien ja metrojen henkilöannostelijoissa, joissa henkilöannostelijan läpi kulkeminen on rakennettu niin, että siitä on hankala kulkea kaksi henkilöä kerrallaan esimerkiksi sähköisen, etäluettavan tunnisteen tarkastamisen jälkeen mahdollistetun yhden kiertosyklin aikana. Painoa ja pituutta voidaan myös käyttää biometrisenä tunnisteena teknisemmissä kulkuannostelijoissa vaa'an ja pituusmitta-anturin avulla (Nopeat henkilöannostelijat 2020).

Salasanat

Yksi vanhimmista ja yleisimmin käytetyistä pääsyoikeuden tai käyttöoikeuden varmentamismenetelmistä on salasana tai pääsykoodi, jota sovelletaan edelleen lähes jokaisessa järjestelmässä. Nykyaikaisempi, paranneltu versio tästä on kertakäyttöinen, vaihtuva salasana tai tunniste, joka on voimassa vain yhden käyttökerran ja yleensä myös vain rajoitetun ajan. Käytännön esimerkkeinä mainittakoon RSA SecurID® (Identity and Access Management – SecurID Suite 2021) ja kaikki muut kaksivaiheista tunnistamista käyttävät menetelmät, jotka toimittavat yksinkertaisen salasanan loppukäyttäjälle käyttämällä jotain erillistä tiedonvälitysprotokollaa, kuten esimerkiksi tekstiviestiä eli SMS-viestiä (Short Message Service), sähköpostiviestiä tai erillistä tunnuslukusovellusta, jossa tämän yksinkertaisen salasanan perille toimittamiseen käytetään jo olemassa olevaa, luotettavaa tiedonvälitysprotokollaa ainoastaan haluttua kohdehenkilöä varten.

Salasanaa tai pääsykoodia voidaan melko turvallisesti käyttää hyödyksi tilapäisissä kulkuoikeustunnisteissa, jotka tulostetaan tai toimitetaan sähköisesti vain yhtä tai lyhyttä käyttökertaa varten. Käytännön esimerkkeinä voidaan mainita mm. lentolipuissa oleva QR- tai viivakoodi, lentomatkatavaroihin kiinnitettävä QR-koodin sisältävä tarra, laivaliikenteen QR-koodin sisältävä maihinnousukortti ja Helsingin Seudun Liikenteen käytössä oleva QR-koodin sisältävä matkustusasiakirja, joka toimitetaan asiakkaalle yleisimmin sähköisesti. Näissä sovellutuksissa on huomioitava, että koodin kopioiminen on erittäin helppoa, mikäli se on visuaalisesti nähtävissä, ja siten pelkän etäluettavan viivakoodin tai vastaavan tunnisteen käyttö ei ole riittävä henkilöllisyyden luotettavaan tunnistamiseen, vaan siihen on käytettävä jotain muuta, vahvempaa tunnistamismenetelmää.

Salasanaa voidaan kuitenkin pitää käyttökelpoisena ja kustannustehokkaana lisävarmenteena pääsyoikeuden todentamiseen esimerkiksi pelkän etäluettavan tunnisteen tarkastamisen yhteydessä. Joskus myös pelkkä salasana tai PIN-koodi voi olla riittävä pääsyoikeus tiettyihin kohteisiin, kuten esimerkiksi kerrostalojen rappukäytäviin ja postipakettien noutoautomaatteihin. Näissäkin sovellutuksissa tulee huomioida ja arvioida salasanojen vaihtamisen ja uusimisen tiheyden tarve sekä estää mahdollisten väsytyshyökkäysten mahdollisuus, joissa järjestelmällisesti kokeillaan jokainen mahdollinen salasanayhdistelmä pääsyoikeuden mahdollistamiseksi.

2.3 Lupahallintoprosessi

Lupahallintoprosessi on kokonaisuus, joka käsittää haku- ja käsittelyprosessin lisäksi pääsyoikeustietokannan hallinnan, ylläpidon ja kausittaisen valvonnan toimenpiteineen. Yksittäisiä kulkuoikeuksia voidaan joutua käsittelemään, myöntämään ja peruuttamaan päivittäin.

Lupien hakemisen ja päivittämisen osalta on tärkeää huomioida kaikki mahdolliset, erilaiset toimintatapamallit ja toimintaympäristöt, joissa lupahallintoprosessia suoritetaan, jotta sovelluskokonaisuudesta saadaan mahdollisimman tehokas ja toimiva. Lupia voidaan hakea, päivittää, uusia ja poistaa monin eri tavoin. Sovelluskokonaisuuden tulee tarjota toimivat rajapinnat monia erilaisia loppukäyttötilanteita varten.

Lupahakemus tai lupien uusimishakemus voidaan toimittaa lupahallintoprosessin käsittelyyn esimerkiksi paperista lupahakemuslomaketta käyttäen, puhelimitse, paikan päällä asioiden, sähköpostitse, sähköistä lomaketta käyttämällä tai muulla vastaavalla tavalla. Lupahakemus voi myös vaatia erillisen, tunnistetun varmentajan käsittelyn suorittamiseksi. Käytettävyyden ja lupahallintoprosessin tehostamisen näkökulmasta on tärkeää, että hakemukset toimitetaan käsittelyyn pääasiassa sähköisessä muodossa tai tavalla, joka on helposti automatisoitavissa luettavaksi sähköiseen muotoon. Lisäksi lupahakemuksen varmentajan luotettavuus tulisi olla automaattisesti todennettavissa ilman erillistä tarkastamista varmentajalta. Varmentajalla tarkoitetaan tässä yhteydessä henkilöä tai tahoa, joka validoi lupahakemuksen kohteena olevien henkilöiden lupahakemusten oikeuden ja varmentaa lupahakemuksen käsittelyn jatkamismahdollisuuden.

Lupien epääminen, poistaminen tai tilapäinen mitätöinti voi myös tulla kyseeseen hyvinkin nopeasti ja yllättävinä ajankohtina. Käytännön esimerkkejä ovat mm. tilanteet, joissa luvan haltija on kadottanut lupatodistuksensa, kulkutunnisteensa, henkilötodistuksensa tai minkä tahansa muun vastaavan pääsyoikeuteen tai henkilöllisyyden varmentamiseen liittyvän asiakirjan tai siihen soveltuvan tunnisteen, laitteen tai välineen. Tämänkaltaisessa tilanteessa on tärkeää, että järjestelmään saadaan nopeasti päivitettyä tieto henkilön kulkuoikeuden, asiakirjan, salasanan, kulkutunnisteen tai muun vastaavan, pääsyoikeuteen tai lupaan oikeuttavan pääsyoikeus- tai lupamenetelmän mitätöinnistä.

2.4 Kulunvalvontaprosessi

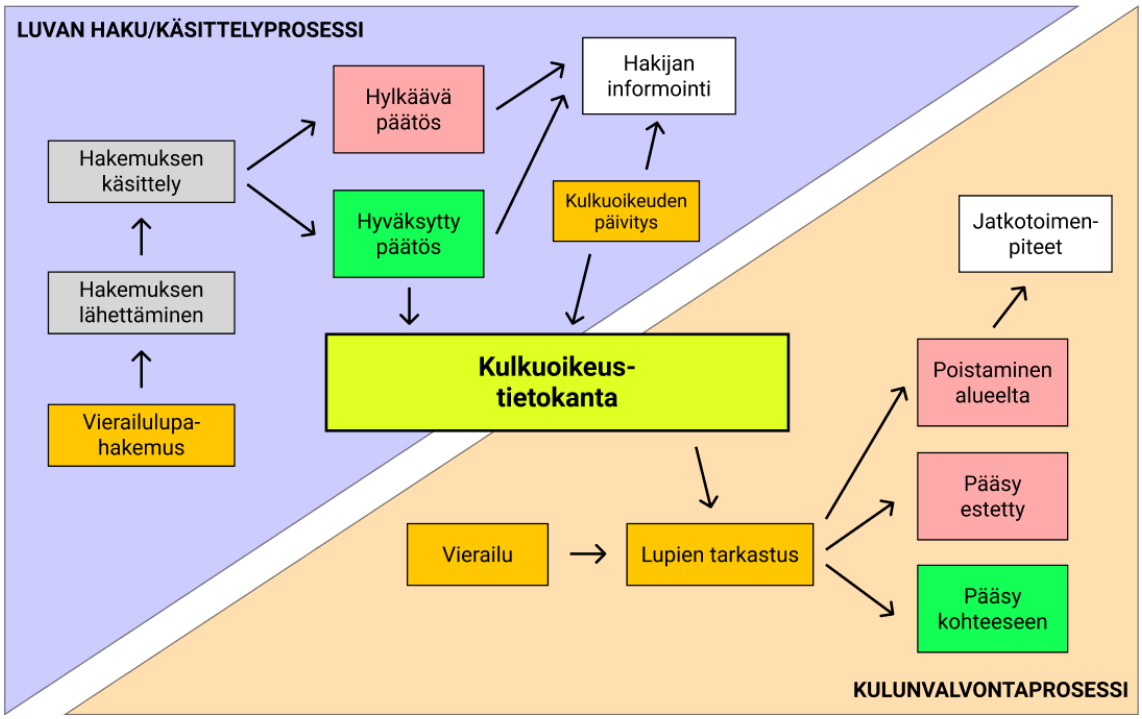
Pääsyoikeusvalvonnassa tai kulunvalvontapisteessä tarkastetaan, onko lupahallintoprosessin mukainen lupa myönnetty. Voimassa oleva lupa pääsyoikeusrekisterissä mahdollistaa pääsyn erikseen määritettyihin kohteisiin. Käytännön esimerkkinä voidaan mainita poliisin suorittama liikenteen ajo-oikeusvalvonta, joka toimii samanlaisella rakenteella käänteisesti. Puuttuva ajo-oikeus (ajokortti) aiheuttaa toimenpiteitä, kun taas kuljettaja, jolla on voimassa oleva ajo-oikeus, saa jatkaa matkaansa ilman seuraamuksia (Ajokorttilaki 386/29.4.2011).

Kulunvalvontaprosessia voidaan suorittaa myös poliisin suorittaman ajo-oikeusvalvonnan kaltaisesti tarkastamalla alueella tai tiloissa jo olevia ihmisiä ja tarkastamalla heidän oikeuksiaan oleskella valvotuissa tiloissa. Mikäli valvotulla ja pääsyoikeuksien osalta rajoitetulla alueella tavataan henkilö, jolla ei ole oikeutta oleskella kyseisissä tiloissa, hänet poistetaan alueelta ja häneen tarvittaessa kohdistetaan myös muita lakien määrittelemiä ja mahdollistamia toimenpiteitä.

Väärinkäyttötapausten ja rikosepäilyiden selvittämisessä voi myös olla tarpeellista pystyä tarkastelemaan sähköisten kulkutunnisteiden ja muiden pääsyoikeuteen mahdollistavien laitteiden, asiakirjojen ja välineiden käytön kirjausmerkintöjä. Tietokantaan tallennetut kirjausmerkinnät muodostavat vierailurekisterin ja kulkutunnisteiden käyttörekisterin. Näistä rekistereistä voidaan tarkastella milloin henkilö, jonka henkilöllisyys on tunnistettu tai jolla on pääsyyn oikeuttava tunniste, on kulkenut sisään tai ulos valvotulta vyöhykkeeltä. Tämänkin ominaisuuden osalta sähköisiä, etäluettavia kulkutunnisteita voidaan pitää mekaanisia avaimia turvallisempina. Sähköisten kulkutunnisteiden käyttö tallentuu yleensä automaattisesti tietokantaan ja jokainen kulkutunnisteen käyttötapahtuma esimerkiksi ovien aukaisuun on tarkasteltavissa tietojärjestelmien käyttölokeista. Tavallisten mekaanisten avaimien käytöstä tämänkaltaista raporttia on mahdoton muodostaa. Poikkeuksen mekaanisten avaimien osalta muodostavat uuden sukupolven digitaaliset lukitusratkaisut, kuten esimerkiksi iLOQ Oy:n älyavaimet (Asuinkiinteistöjen lukitusratkaisu – iLOQ, 2021), jotka yhdistelevät mekaanisen avaimen ja NFC-tekniikan ominaisuuksia.

2.5 Lupahallinnon kokonaisprosessi

Muodostin yksinkertaistetun lupahallinnon kokonaisprosessin kuvauksen (kuva 1 lupahallinnon ja kulunvalvonnan prosessi) haastattelemalla insinöörityön asiakasorganisaation yhteyshenkilöitä (Jauho 2020; Kallio 2020) sekä muutamia muita ulkopuolisten organisaatioiden kulkulupahallinnon parissa työskenteleviä henkilöitä. Kokonaisprosessi voidaan jakaa pääpiirteissään kahteen eri osa-alueeseen, luvan haku- ja käsittelyprosessiin sekä valvontaprosessiin (vierailun valvonta). Jos lupahallinto koskee kulkua tai liikkumista kohteessa, voidaan puhua kulkulupien hakemisesta ja käsittelystä ja valvonnan osalta kulunvalvonnasta tai vierailun valvonnasta.



Kuva 1. Lupahallinnon ja kulunvalvonnan prosessi.

Käsittelyprosessissa luvan hakija hakee kulku- tai vierailulupaa (pääsyoikeus) itselleen tai ilmoittamilleen henkilöille. Vierailulupahakemuksessa määritellään henkilötiedot loppukäyttäjän tarvitsemalla tarkkuudella ja kuvataan pääsyoikeusvaatimukset tarvittaviin kulunvalvottuihin kohteisiin. Kohdeorganisaation suorittaman varsinaisen käsittelyprosessin jälkeen (luvan hyväksyminen tai hylkääminen) luvan hakijaa informoidaan päätöksestä.

Kulunvalvontaprosessissa vierailijan kulkua valvova taho varmentaa henkilön tai henkilöiden kulkuoikeuden kohteisiin tarkastamalla henkilöllisyyden joko manuaalisesti tai sähköisesti esimerkiksi kulkutunnisteella, biometrisellä tunnisteella tai muulla vastaavalla tavalla.

Lupahallintoprosessi ja kulunvalvontaprosessi linkittyvät toisiinsa pääsyoikeusrekisterin kautta, joka on koko prosessin keskiössä. Käsittelyprosessi käyttää tätä tietokantaa vierailulupien lisäämiseen, muokkaamiseen ja poistamiseen. Kulunvalvontaprosessi käyttää samaa tietokantaa pääsyoikeuksien tarkastamiseen ja vierailujen kirjaamiseen.

3 Sovelluskokonaisuus

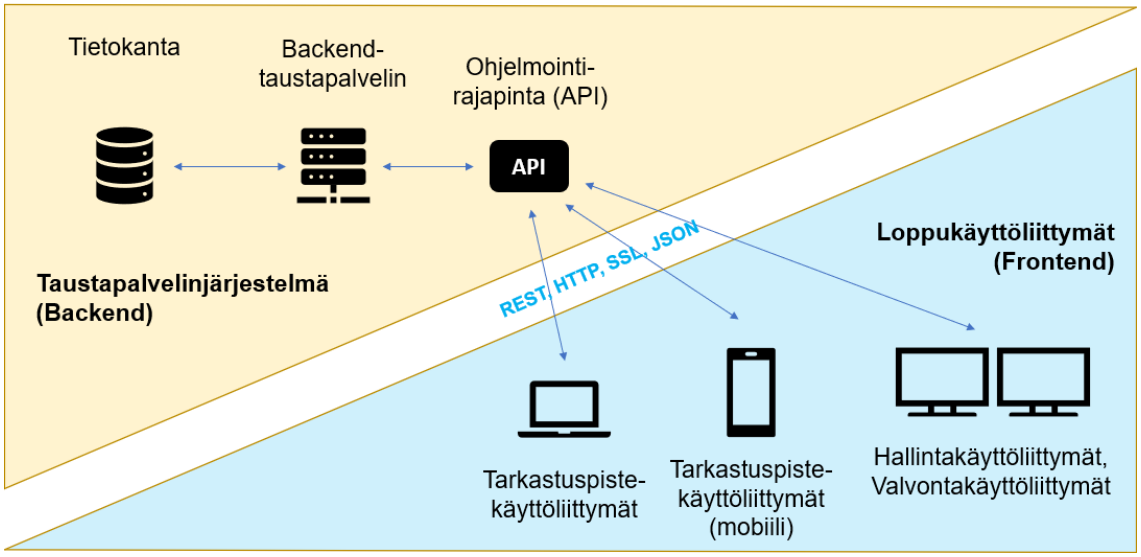
Insinöörityönä tehtiin suunnitelma sovelluskokonaisuudesta jatkokehitystä ja kaupallistamista varten. Kulunvalvontasovelluksen prototyyppi, tietokanta ja tiedonsiirtorajapinnat ovat sen eri osia. Sovelluskokonaisuus koostuu tietokantapalvelimesta, taustapalvelinjärjestelmästä sekä erilaisista loppukäyttösovelluksista, joista yksi on tarkastuspisteen loppukäyttöliittymä eli kulunvalvontasovelluksen prototyyppi. Lisäksi taustapalvelinjärjestelmään voidaan liittää erillinen viestinvälityspalvelu, joka mahdollistaa henkilöiden informoinnin lupahallintoprosessin lupien käsittelytilanteen muutoksista esimerkiksi sähköpostitse tai tekstiviestitse.

3.1 Vaatimusmäärittely

Sovelluskokonaisuuden vaatimusmäärittely toteutettiin haastattelemalla asiakasorganisaation useita eri yhteyshenkilöitä. Haastatteluista muodostettiin vaatimusmäärittely (liite 1), jossa vaatimukset luokiteltiin ohjelmistokokonaisuuden eri osa-alueiden osiksi. Vaatimusmäärittelyn perusteella muodostettiin määritelmät sovelluskokonaisuuden toteuttamiseksi sovellusarkkitehtuurin, tiedonsiirtomenetelmien, käytettävien rajapintojen, tietokannan, taustapalvelinjärjestelmän ja loppukäyttöliittymien osalta.

3.2 Arkkitehtuuri

Sovellusarkkitehtuurin vaatimusmäärittelyssä korostui kaksi tärkeää asiaa arkkitehtuurin suunnittelua varten: modernien ja kustannustehokkaiden kehitysympäristöiden käyttö sekä tietoliikenteen riittävän suojauksen toteuttamisen mahdollistaminen. Muodostin sovelluskokonaisuuden arkkitehtuurista graafisen suunnitelman vaatimusmäärittelyn perusteella osana sovelluskokonaisuuden suunnittelutyötä (kuva 2).



Kuva 2. Sovellusarkkitehtuurimallin suunnitelma.

Lupahallintosovelluksen arkkitehtuuri suunniteltiin niin, että jokainen sovelluskokonaisuuden osa-alue on täysin itsenäinen ja riippumaton toisistaan. Tämä mahdollistaa käyttöjärjestelmä-, sovellus- ja laitteistoriippumattomuuden, kun valitaan tai vaihdetaan taustapalvelinjärjestelmän eri osien toteutukseen käytettäviä laiteratkaisuita ja tekniikoita. Minkään yksittäisen palvelimen tekniikan vaihtaminen tai korvaaminen täysin eri käyttöjärjestelmällä ja ohjelmistolla ei vaikuta sovelluskokonaisuuden muihin osiin. Loppukäyttöliittymät ovat täysin eriytettyjä taustapalvelinjärjestelmästä, ja ne keskustelevat API-rajapinnan kautta erikseen sovitulla tiedonvälitysmuodolla.

3.3 Tietokanta

Tietokannan toteutusmalliksi valittiin SQL-kyselykielimallia (Structured Query Language) tukevat relaatiotietokannat, ja tietokantojen yhteysrajapinnat kehitettiin niin, että ne tukevat yleisesti kaikkia SQL-kyselykielimallia tukevia tietokantoja. Prototyypin testauksessa käytettiin avoimeen lähdekoodiin perustuvaa MariaDB-tietokantaa. Loppukäytössä voidaan käyttää mitä tahansa muuta SQL-kyselykielimallia tukevaa tietokantaa, joita ovat esimerkiksi Oracle 12c, Microsoft SQL Server, MySQL ja PostgreSQL.

Muunlaisten tietokantojen käyttö sovelluskokonaisuudessa on myös mahdollista. Tämä kuitenkin vaatii erillisen tietokantakommunikaatioprotokollan määrittämistä, mikäli SQL-kyselykielimallia ei voida noudattaa.

Kulunvalvontasovelluksen prototyypin tietokannan keskeisiä osa-alueita ovat henkilörekisteri, kohderekisteri, aikataulurekisteri, pääsyoikeusrekisteri, vierailurekisteri ja tapahtumaloki. Nämä osa-alueet kuvataan seuraavaksi tarkemmin. Kirjautumisessa ja istunnon ylläpidossa käytetään myös useita muita tietokannan tauluja.

Henkilörekisteri

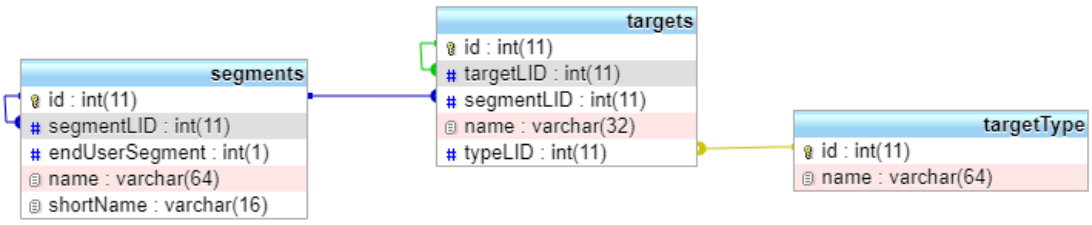
Henkilörekisteri sisältää tiedot yksittäisistä henkilöistä henkilötietoineen tarvittavilta osin pääsyoikeuksia varten. Henkilörekisterin tietue liittyy muutamaa poikkeustilannetta lukuun ottamatta aina johonkin pääsyoikeuteen. Henkilörekisteri sisältää laajan valmiuden erilaisiin henkilötietoihin, joista käyttäjäorganisaatio voi itse valita, mitä tietoja järjestelmässä haluaa käyttää. Näitä tietoja ovat esimerkiksi henkilön nimi, syntymäaika, puhelinnumero, henkilötunnus, passin numero, sähköpostiosoite, valokuva ja muut vastaavat tiedot.

Henkilörekisterin käytössä on tärkeää huomioida Euroopan unionin määrittelemä, tietosuojaa koskeva tietosuoja-asetus GDPR (General Data Protection Regulation), joka määrittää henkilörekisterin pitäjälle tiettyjä vastuita ja velvollisuuksia henkilötietojen käsittelyyn, tallentamiseen ja sääntelyyn. GDPR-asetuksen kannalta on tärkeää tiedostaa rekisteriin kirjattujen henkilöiden oikeudet omiin henkilötietoihinsa ja käytännössä huomioida, että rekisteriin tallennetaan vain niitä tietoja, jotka ovat välttämättömiä rekisterin ja muun sovelluskokonaisuuden käytettävyyden kannalta. GDPR-asetus tulee myös huomioida sovelluskokonaisuuden suunnittelussa varsinkin tietokannan ja käyttöoikeusrajausten määritysten mahdollisuuden osalta. On tärkeää, että järjestelmässä on mahdollista määrittää tiedon käsittelyn käyttöoikeudet joustavasti niin, että ne soveltuvat kaikkien erilaisten loppukäyttäjäorganisaatioiden käyttöön niin, että GDPR-asetusta noudatetaan. Myös valmius asetuksen vaatimuksien mahdolliseen muutokseen tulee ottaa huomioon jo suunnitteluvaiheessa.

GDPR-asetuksen määritelmistä voi helposti muodostaa ajatuksen, että henkilötietoja tulisi tallentaa tietojärjestelmiin mahdollisimman vähän. Pitää kuitenkin huomioida, että nämä tiedot osaltaan myös parantavat organisaatioturvallisuutta mm. henkilöllisyyden varmentamisessa vierailun tai kulkuoikeuden tarkastamisen yhteydessä. Lisäksi tilanteessa, jossa henkilö pyytää rekisterinpitäjältä tarkasteltavakseen hänestä tallennettuja henkilötietoja, on tärkeää pystyä varmistumaan siitä, että pyynnön esittäjä voidaan luotettavasti tunnistaa ja hänelle toimitetaan vain häntä itseään koskevaa aineistoa. Esimerkiksi pelkkään nimeen ja syntymäaikaan perustuva varmistus voi olla varsin epäluotettava, sillä nämä tiedot ovat monessa tapauksessa yleisesti useiden muiden henkilöidenkin tiedossa. Luotettavampaa onkin, että henkilötietoja toimitetaan esimerkiksi vain henkilörekisteriin määritettyyn sähköpostiosoitteeseen, puhelinnumeroon tai osoitteeseen. Mikäli tietoja toimitetaan tämänkaltaisessa tilanteessa jollain muulla tavalla tai edellä mainittuja tietoja ei ole saatavilla, on henkilöllisyyden varmistaminen luotettavampaa käyttämällä virallista tai muuta hyväksyttävää henkilöllisyystodistusta ja vertaamalla sitä henkilörekisteriin tallennettuun henkilötunnukseen. Myös tallennettua valokuvaa voidaan käyttää tämänkaltaisessa varmentamisessa ilman henkilöllisyystodistusta ja järjestelmään tallennettua henkilötunnusta.

Kohteet

Kohderekisteri on vierekkäisyysmallia noudattava tietokantarakennetta (Mäenpää 2015) noudattava taulu, joka sisältää kaikki kulunvalvonnan piirissä olevat kohteet kattaen niiden osat ja osakokonaisuudet sekä määrittää yksittäisen kohteen käyttöoikeushallinnan segmentointimääreellä. Kohderekisterillä on relaatioita segmenttirekisterin ja kohteen tyyppirekisterin kanssa (kuva 3).



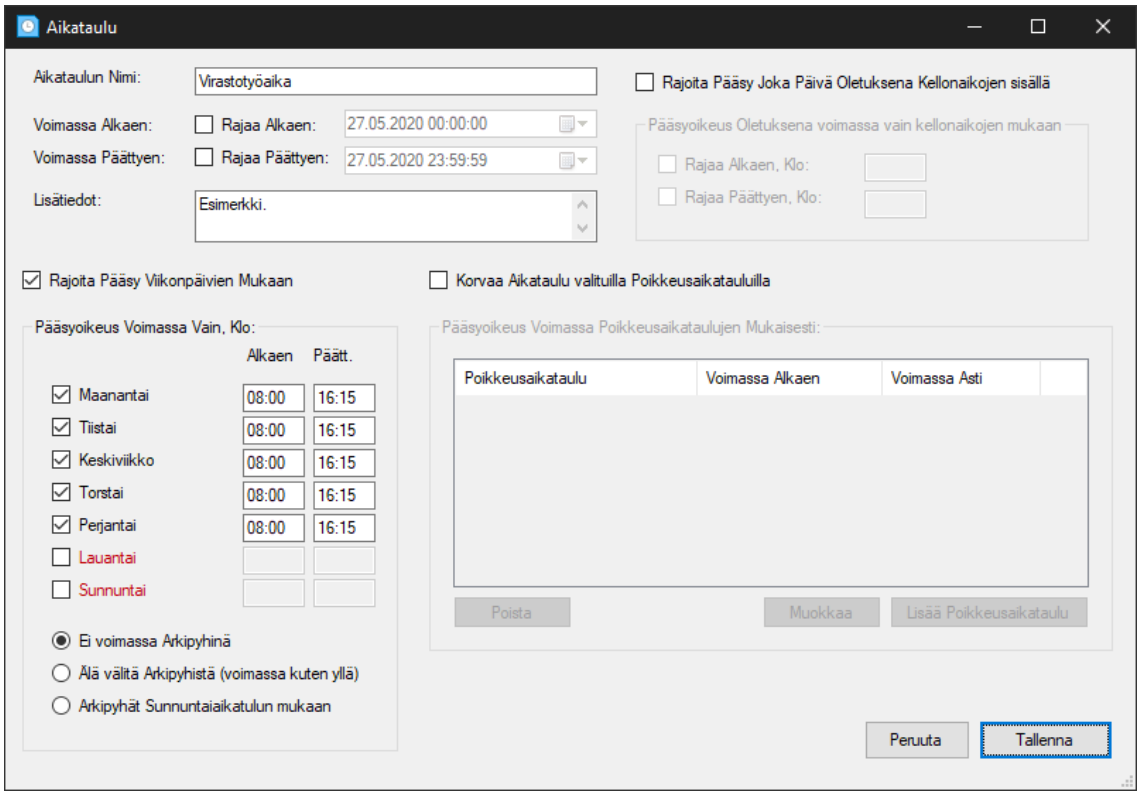
Kuva 3. Tietokannan kohteet-tauluun liittyvät taulut ja niiden väliset relaatiot.

Kohde (kohteen tyyppi) voi olla esimerkiksi rakennus, rakennuksen osa tai osio, vyöhyke, aidattu alue tai muu alue, suoja-alue, kaupunki tai lähiö, joukko-osasto, vastuualue, valvottu vyöhyke ja myös mikä tahansa muu vastaava määre. Kohde voi olla aina jonkin toisen kohteen alikohde ja periä osan isäntäkohteen määreistä. Kohteella voi olla myös määritettynä segmentti, johon kohde kuuluu. Kohteen segmentti periytyy isäntäkohteen mukaan, mutta se voi olla myös erikseen määritetty alikohteessa.

Vierekkäisyysmallin käyttäminen tietokantataulun rakenteessa mahdollistaa eri rivien keskinäisten relaatioiden määrittämisen halutulla tavalla. Rivejä voidaan lisätä ilman relaatiota tai niille voidaan määrittää haluttu isäntärivi. Näitä relaatioita voidaan käyttää hyödyksi pääsyoikeuksia määritettäessä.

Aikataulut

Aikataulurekisteri on vierekkäisyysmallia noudattava taulu, joka sisältää erikseen määritellyt tarkennetut aikataulut kulkulupaa varten. Aikataulurekisteri määrittää tarvittaessa sallitut kulkuaikataulut yleisellä aikarajauksella, eri viikonpäivinä ja arkipyhinä halutun voimassaoloajan mukaisesti. Aikataulurekisteri on pääsyoikeutta rajaava määre, jota voidaan käyttää, mikäli halutaan rajata pääsyoikeutta tiettyinä viikonpäivinä ja kellonaikoina. Luonnos graafisesta aikataulurekisterin muokkausnäkymästä on esitetty kuvassa 4.

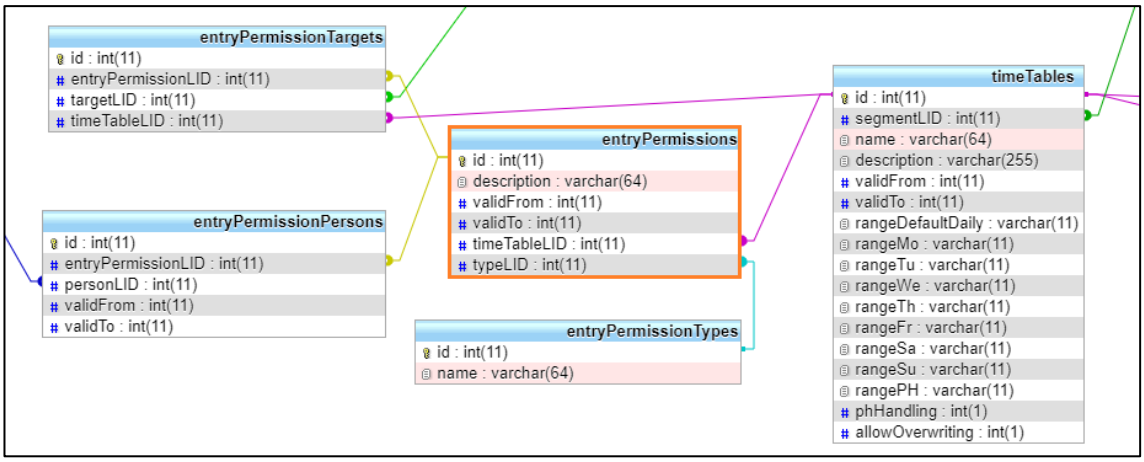


Kuva 4. Esimerkki aikataulun muokkausnäkymästä hallintakäyttöliittymässä.

Aikataulun voi korvata toisella aikataululla (poikkeusaikataululla), joka on voimassa erikseen määritetyn ajan. Poikkeusaikataulua voidaan käyttää tilapäisissä muutoksissa, kun varsinaista aikataulua ei haluta muuttaa.

Pääsyoikeudet

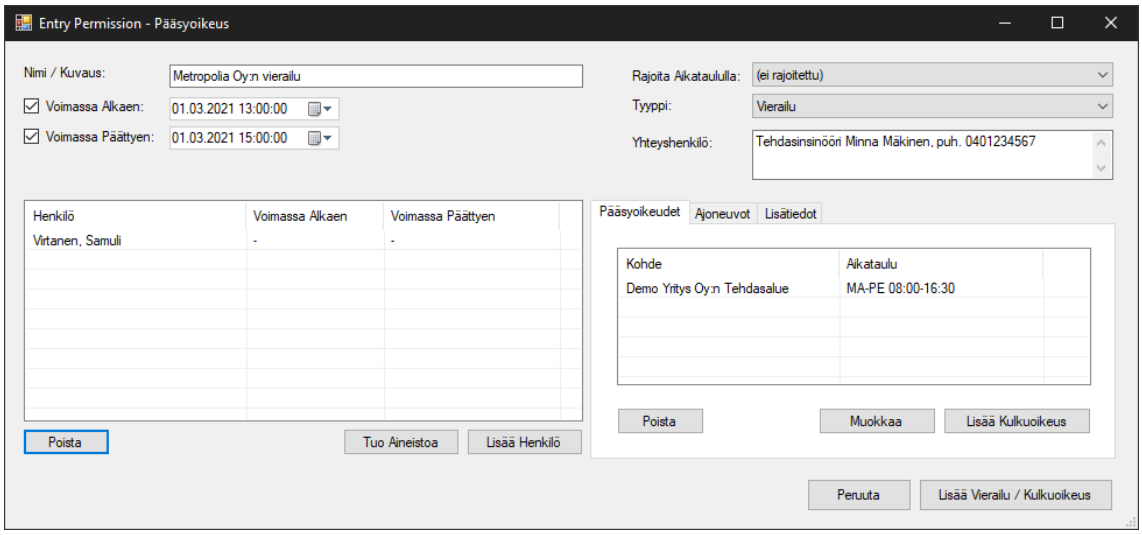
Pääsyoikeusrekisteri määrittää henkilöiden kulkuoikeudet valittuihin kohteisiin tarvittaessa rajattuna voimassaoloajan ja määritettyjen aikataulujen puitteissa. Pääsyoikeusrekisteri koostuu yhdestä päätaulusta (entryPermissions) ja muutamasta alitaulusta, jotka määrittävät pääsyoikeuteen liittyvät kohteet, henkilöt ja aikataulun sekä pääsyoikeuden tyypin (kuva 5).



Kuva 5. Pääsyoikeusrekisterin tietokantataulu ja sen lähimmät relaatiot muihin tietokannan tauluihin.

Pääsyoikeuden aikataulu- ja voimassaolorajaukset on toteutettu mahdollisimman monipuoliseksi loppukäyttöä ajatellen, mutta kuitenkin niin, että pääsyoikeuden aikataulun määrittäminen olisi mahdollisimman helppoa, yksinkertaista ja nopeaa. Jokainen aikataulu- ja voimassaolorajaus on erillinen rajaava määre, jonka voi ottaa käyttöön missä tahansa pääsyoikeuden aikataulurajauksen määrittämiseen liittyvässä osiossa, mikäli se koetaan tarkoituksenmukaiseksi.

Pääsyoikeuden lisääminen, muokkaaminen ja poistaminen tehdään erikseen toteutettavassa hallintakäyttöliittymässä. Luonnostelma pääsyoikeuden muokkausnäkymästä hallintakäyttöliittymässä (kuva 6) on toteutettu käyttämällä Microsoft Visual Studio 2019 -ohjelmistoa. Tietosisällöltään vastaava lomake toteutetaan myös toiseen erikseen toteutettavaan loppukäyttöliittymään, jossa pääsyoikeuslupahakemuksia voidaan lähettää käsittelyyn joko vierailijan itsensä tai vierailun varmentavan tahon puolesta. Pääsyoikeushakemusten lähettäminen suoraan järjestelmän loppukäyttöliittymän kautta tehostaa pääsyoikeuden haku- ja käsittelyprosessia, kun tietoja ei tarvitse kirjata sähköiseen järjestelmään hallintakäyttöliittymässä ja hakija voi tehdä pääsyoikeushakemuksen ajasta ja paikasta riippumatta.



Kuva 6. Esimerkki pääsyoikeuden muokkausnäkymästä hallintakäyttöliittymässä.

Vierailurekisteri

Vierailurekisteriin tallennetaan yksittäisten tarkastuspisteiden suorittamat vierailuiden aloittamiset (alueelle saapuminen) ja vierailujen päättämiset (alueelta poistumiset) henkilön tarkkuudella. Vierailut kohdistuvat aina yhteen kohteeseen, joka voi olla esimerkiksi valvottu vyöhyke, rakennus, rakennuksen osa tai mikä tahansa muu vastaava määre. Vierailurekisterin tarkoitus on pitää yllä tietoa yksittäisten henkilöiden vierailuiden alkamis- ja päättymisajoista halutuilla valvontavyöhykkeillä.

Vierailurekisteri on yksinkertainen rivimuotoinen tietokantataulu, jonka rivit ovat yksittäisiä yksittäisten henkilöiden vierailuita tietyissä kohteissa. Vierailurekisterin tietoja säilytetään tietokannassa sovelluskokonaisuuden asetusmäärittelyjen mukaisen säilytysajan verran, ja tämän jälkeen tiedot poistetaan kokonaan järjestelmästä.

Tapahtumaloki

Tapahtumalokiin kirjataan kaikki tapahtumat, joita järjestelmässä halutaan seurata. Näitä tapahtumia voivat olla mm. kulkulupatietokantajärjestelmään suoritetut hakukyselyt, onnistuneet ja epäonnistuneet kirjautumisyritykset järjestelmään, tietueisiin tehdyt muutokset sekä henkilötietojen katselumerkinnät. Pääkäyttäjän tulee voida määrittää, mitä tietoja järjestelmä kirjaa tapahtumalokiin. Käyttäjäorganisaation tulee käyttää

huolellista harkintaa päättäessään, mitä tietoja tapahtumalokiin valitaan kirjattavaksi, ja määrittää tietojen säilytysaika. Järjestelmä voidaan määrittää hävittämään tietokantaan tallennetut tiedot, joiden säilytysaika on umpeutunut ja säilyttämisen tarve on päättynyt.

Käyttöoikeusrekisteri ja segmentointi

Käyttöoikeusrekisteri määrittää järjestelmän käyttäjien käyttöoikeudet järjestelmän kaikkien toimintojen osalta. Pääkäyttäjät voivat luoda, tarkastella, muokata ja poistaa käyttöoikeusrekisterin määrityksiä käyttämällä hallintakäyttöliittymäsovellusta. Pääkäyttäjät voivat tehdä muutoksia vain niihin segmentteihin, joihin heillä on määritetty käyttöoikeus. Käyttöoikeusrekisteriin voidaan lisätä myös käyttöoikeuksia oman organisaation tai segmentin sisällä, mikäli siihen on lisätty oikeus pääkäyttäjätasolla. Käyttöoikeusrekisterin määreet määrittävät käyttöoikeudet sovelluksen eri osa-alueiden käyttöön. Yksittäisiä käyttöoikeusrekisterin käyttöoikeusmääreitä ovat mm. oikeus pääsyoikeustietokannan hallinnointiin ja lokitietojen tarkasteluun oman segmentin tai organisaation käyttäjien osalta.

Segmenttirekisteri määrittää segmenttien sisäiset käyttöoikeudet järjestelmän käyttöoikeustunnuksille. Yksittäiselle järjestelmän käyttäjälle voidaan määrittää erilaisia käyttöoikeuksia eri segmentteihin. Segmentoinnin ideana on mahdollistaa monipuolisempi ja monitasoisempi käyttöoikeuksien määritys- ja rajausmahdollisuus. Segmentointi on sovelluskokonaisuuden käyttöoikeushallintaa täydentävä lisätyökalu, jonka voi ottaa käyttöön sovelluskokonaisuuden käyttöoikeushallinnan lisäosana, mikäli se koetaan tarpeelliseksi.

3.4 Taustapalvelinjärjestelmä ja ohjelmointirajapinta (API-rajapinta)

Taustapalvelinjärjestelmä palvelee loppukäyttöliittymiä tarjoamalla ohjelmointirajapinnan eli API:n (Application Programming Interface), hoitaa järjestelmän sovelluskokonaisuuden taustalla tapahtuvia ydintoimintoja ja on yhteydessä järjestelmän käyttämiin tietokantoihin sekä ulkopuolisiin palveluihin. Insinöörityön prototyypissä taustapalvelinjärjestelmässä käytetään kolmikerrosmallia (What is Three-Tier Architecture 2020).

Loppukäyttäjä tai loppukäyttöliittymä käyttää taustapalvelinkokonaisuutta ohjelmointirajapinnan avulla. Insinöörityön prototyypissä viestintään käytetään kaikissa rajapintakutsuissa REST-arkkitehtuurimallia (Representational State Transfer). Rajapintakyselyt lähetetään käyttämällä HTTP-protokollaa (Hypertext Transfer Protocol) ja sisältötyyppiä application/x-www-form-urlencoded (esimerkkikoodi 1). Rajapintakyselyn voi toteuttaa helposti lähes kaikilla ohjelmointikielillä, kuten esimerkiksi käyttämällä C#-ohjelmointikieltä (esimerkkikoodi 2). Rajapintakysely palauttaa vastauksen JSON-muotoisena (JavaScript Object Notation) tekstitietona (esimerkkikoodi 3).

```
POST /KVSP/permissions/list HTTP/1.1
Host: 127.0.0.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 49

checkpoint=14&surname=Virtanen&birthdate=19870101
```

Esimerkkikoodi 1. HTTP-muotoinen rajapintakysely.

```
var client = new RestClient("127.0.0.1/KVSP/permissions/list");
client.Timeout = -1;
var request = new RestRequest(Method.POST);
request.AddHeader("Content-Type", "application/x-www-form-urlencoded");
request.AddParameter("checkpoint", "14");
request.AddParameter("surname", "Virtanen");
request.AddParameter("birthdate", "19870101");
IRestResponse response = client.Execute(request);
Console.WriteLine(response.Content);
```

Esimerkkikoodi 2. Rajapintakysely käyttäen C#-ohjelmointikieltä.

```
{
  persons: [
    {
    surname: "Virtanen",
    firstname: "Samuli",
    birthdate: "19870101",
    organization: "Metropolia Oy",
    permissions: [
        {
          id: 10,
          title: "Takuukorjaukset",
          contact_person: {
            name: "Minna Mäkinen",
            tel: "+358401234567"
          },
        validity: {
          from: "2009-03-12T00:00:00+02:00",
          to: "2021-12-15T23:59:59+02:00"
          }
        }
      ]
    }
  ]
}
```

Esimerkkikoodi 3. Ohjelmointirajapinnan esimerkkivastaus pääsyoikeushakukyselyyn JSON-muodossa.

Yleiset toiminnallisuudet

Taustapalvelinjärjestelmän yleisiä toiminnallisuuksia ovat mm. kirjautuminen järjestelmään, kirjautuminen ulos järjestelmästä sekä aktiivisen istunnon validointi. Nämä toiminnallisuudet ovat olennainen osa mitä tahansa nykyaikaista taustapalvelinjärjestelmää, ja niiden toteuttamiseen on olemassa useita erilaisia tapoja ja valmiita kaupallisia ratkaisuja.

Tietoturvan kannalta on tärkeää kiinnittää huomiota varsinkin salausalgoritmeihin, joita käytetään salasanojen tiivisteiden muodostamiseen ja mahdollisesti myös tiedon salaamiseen. Lisäksi tulee huomioida, että taustapalvelinjärjestelmän yleisiin toiminnallisuuksiin käytettävän ratkaisun tulee sisältää riittävät valvonta- ja estomekanismit väsytyshyökkäyksiä ja muita vastaavia tietoturvariskejä vastaan.

Pääsyoikeuksien hakukysely

Pääsyoikeuksien hakukysely palauttaa hakuehtojen mukaiset pääsyoikeudet, joihin kirjautuneella käyttäjällä on luku- tai muokkausoikeus. Pääsyoikeuksien hakuehtoina

voidaan käyttää mitä tahansa pääsyoikeusrekisterin määreistä, joita ovat mm. etunimi, sukunimi, syntymäaika, henkilötunnus, puhelinnumero, organisaatio, vierailun nimi, yhteyshenkilö, ajankohta ja ajoneuvon rekisterinumero. Hakukysely palauttaa vain ne tiedot, joihin kirjautuneella loppukäyttäjällä on käyttöoikeusmäärein määritellyt luku- ja tarkasteluoikeudet.

Pääsyoikeuksien hakukyselyt voidaan tallentaa myös tapahtumalokiin. Tämä tallentaminen mahdollistaa järjestelmän käytön valvonnan ja voi siten paljastaa tietojen aiheettoman tarkastelun, vaikka tietojen tarkastelijalla olisikin käyttöoikeus tietojen tarkasteluun. Pääsyoikeuksien hakukyselyiden ja henkilötietojen tarkastelun tallentaminen tapahtumalokiin mahdollistaa GDPR-asetuksen mukaisen henkilötietojen tarkasteluiden seurannan ja valvonnan jälkikäteen.

Vierailun kirjaaminen ja päättäminen

Vierailun kirjaaminen luo vierailurekisteriin uuden merkinnän, johon kirjataan saapunut henkilö, saapumisaika, vierailun kirjaaja, vierailun numero ja tarvittaessa vierailijakortin tiedot sekä muut lisätiedot. Vierailun päättäminen lisää vierailurekisterissä olevaan vierailun päättämiseen liittyvät merkinnät, joita on ainakin vierailun päättämisen ajankohta.

Vierailun voi kirjata vain järjestelmään sisäänkirjautunut käyttäjä, jolla on oikeus tarkastella alueelle saapuvan henkilön tietoja tarkastuspisteen vyöhykemäärityksen ja omien henkilökohtaisten käyttöoikeusmäärityksien perusteella. Pääsyoikeudettoman henkilön vierailun kirjaaminen on mahdollista, mikäli loppukäyttäjällä on käyttöoikeus kirjata vierailuita myös henkilöille, joilla ei ole pääsyoikeutta alueelle pääsyoikeusrekisterin mukaisesti. Tämä käyttöoikeus voidaan määrittää loppukäyttäjille tai tarkastuspisteille hallintakäyttöliittymässä.

3.5 Loppukäyttösovellukset (Frontend)

Loppukäyttösovellukset ovat lupahallintosovelluskokonaisuuden eri laitteille ja erilaisia käyttöympäristöjä varten suunniteltuja, erilaisia käyttötarkoituksia varten optimoituja loppukäyttöliittymiä. Insinöörityössä toteutettiin yksi loppukäyttösovellus, joka noudattaa

kulunvalvontakäyttöliittymän loppukäyttösovelluskuvausta ja on siten täysin soveltuva vyöhykkeen rajalla toimivan tarkastuspisteen käyttöön. Insinöörityössä suunnitellun sovelluskokonaisuuden erilaiset, loppukäyttöä varten suunnitellut ja optimoidut loppukäyttösovellukset on kuvattu seuraavaksi.

Kulunvalvontakäyttöliittymä voi olla työpöytäsovellus, mobiilisovellus tai sulautetun järjestelmän sovellus. Kulunvalvontakäyttöliittymällä tarkastetaan henkilön pääsyoikeus tarkastuspisteellä ja tehdään vierailun aloittamis- ja päättämismerkinnät. Kulunvalvontakäyttöliittymä on tarkoitettu tarkastuspisteiden käyttöön ja mobilisoituihin ympäristöihin, joissa on tarve tarkastaa pääsyoikeuden voimassaolotietoja.

Hallintakäyttöliittymä on työpöytäsovellus, jonka keskeisimmät toiminnallisuudet ovat vierailu- ja kulkulupahakemusten (pääsyoikeudet) käsittely, järjestelmän käyttäjien käyttöoikeuksien määrittely; pääsyoikeuksien lisääminen, muokkaaminen ja poistaminen; segmentin mukaisten parametrien määrittäminen ja raporttien tulostus. Insinöörityön loppukäyttöliittymän suunnittelussa käytetään MVC-mallia (Model View Controller). Hallintakäyttöliittymä on tarkoitettu lupahallinnon käsittelytyökaluksi ja palvelun pääkäyttäjien loppukäyttöliittymäksi.

Vierailuilmoituskäyttöliittymä on verkkoselainohjelmisto vierailu- ja kulkulupien (pääsyoikeus) hakemiseen. Vierailuilmoitus-sovelluksella autentikoitu henkilö ilmoittaa tulevasta vierailusta tai hakee pääsyoikeutta ilmoittamilleen henkilöille hakemuksen mukaisesti. Vierailuilmoituskäyttöliittymä on tarkoitettu pääsyoikeuden hakijoiden työkaluksi, ja se voidaan tarjota loppukäyttäjille verkkoselaimen palvelun Internetin tai yrityksen omien sisäisten verkkojen välityksellä.

Valvontakäyttöliittymä on työpöytäsovellus, jota voidaan käyttää valvomoissa aktiivisten ja päättyneiden vierailujen tilannekuvan muodostamiseen. Valvontakäyttöliittymä voidaan myös toteuttaa kulunvalvontakäyttöliittymän erilaisella näkymällä. Valvontakäyttöliittymä on suunniteltu vierailujen seurantaan ja tilannekuvan tarkastelua ja muodostamista varten.

Loppukäyttöliittymien eriyttäminen useaan eri sovellukseen mahdollistaa käytettävyyden erityispiirteiden huomioimisen jokaisessa erilaisessa loppukäyttöpisteessä. Tässä

insinöörityössä toteutettiin loppukäyttöliittymistä vain kulunvalvontakäyttöliittymän prototyyppi eli kulunvalvontasovelluksen prototyyppi.

4 Kulunvalvontasovellus

Kulunvalvontasovellus toteutettiin noudattamalla sovelluskokonaisuuden yleisiä vaatimusmäärittelyitä ja kulunvalvontasovelluksen loppukäyttöliittymän teknisiä ja muita vaatimusmäärittelyitä. Kulunvalvontasovellus toteutettiin käyttämällä Electron-hybridikehitystyökalua ja JavaScript-ohjelmointikieltä.

Suurin osa kulunvalvontasovelluksen toiminnallisuuksista tapahtuu taustapalvelimella. Sovelluksen toiminnan edellytyksenä on toimiva taustapalvelinjärjestelmä, joka tuottaa tietoaineiston käsittelyyn ja tallentamiseen soveltuvat tietokannat ja API-rajapintakuvaukset. Kulunvalvontasovelluksen vaatimusmäärittely, käyttöliittymäsuunnittelu ja toteutus kuvataan seuraavaksi.

4.1 Vaatimusmäärittely

Kulunvalvontasovellus on kohteen rajalla sijaitsevalla tarkastuspisteellä käytettävä sovelluskokonaisuuden loppukäyttöliittymä. Sovelluksen tulee toimia 64-bittisessä Windows-ympäristössä. Sovellusta käytetään tietokoneella käyttäen näyttöä, näppäimistöä ja tarvittaessa hiirtä. Sovelluksen tulee lisäksi tukea erikseen määritettyjä lisälaitteita, kuten esimerkiksi erillistä viivakoodinlukijaa.

Sovelluksella tulee voida tarkastaa kohteeseen pyrkivän henkilön pääsyoikeus kohteeseen ja tehdä vierailun aloittamis- ja päättämismerkinnät. Sovelluksen tulee toimia myös tilanteessa, jossa verkkoyhteys on tilapäisesti poissa käytöstä. Kulunvalvontasovelluksen tulee myös mahdollisesti tukea erillisiä tai integroituja lisälaitteita, kuten esimerkiksi viivakoodinlukijaa, tarratulostinta ja dokumenttiskanneria. Asiakkaan määrittämä tarkempi vaatimusmäärittely on esitetty liitteessä 1.

4.2 Käyttöliittymäsuunnittelu

Käyttöliittymän suunnittelu toteutettiin asiakkaan vaatimusmäärittelyjen (liite 1) mukaisesti. Tärkeimpiä huomioon otettavia asioita olivat käyttöympäristön erityispiirteet ja vaatimukset sekä lisälaitteiden käytön tuki. Vaatimusmäärittelyssä korostui myös selkeys ja yksinkertaisuus varsinkin loppukäyttöä tarkastuspisteellä ajatellen. Tarkastuspisteellä operoivan loppukäyttäjän tulee voida todeta pääsyoikeuden voimassaolo kulunvalvontasovelluksesta selkeästi ja mahdollisimman nopeasti henkilöllisyyden tarkastamisen yhteydessä.

Ohjelmistoa tulee voida käyttää mahdollisimman helposti ja nopeasti lisälaitteiden, näppäimistön pikanäppäimien ja ohjelmiston käyttöliittymän painikkeiden avulla tarvittaessa myös ilman hiirtä. Ohjelmiston näkymän tulee olla luettavissa tavallista työpöytäkäyttöä etäämmältä. Ohjelmiston käyttöliittymäsuunnittelussa tulee huomioida myös, että loppukäyttöliittymää käytetään sekä valoisassa että pimeässä toimintaympäristössä.

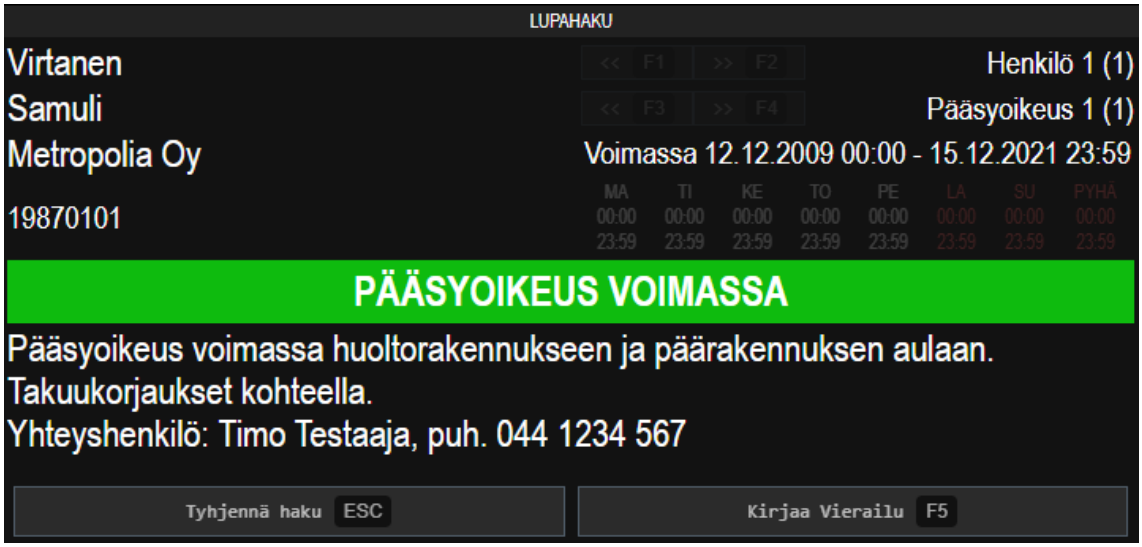
Vaatimusmäärittelyissä korostui myös pääsyoikeuden voimassaolon selkeä esittämistapa. Pääsyoikeuden tilan tulee olla visuaalisesti helposti ymmärrettävä pääsyoikeuden tarkastamisen yhteydessä.

4.3 Toteutus

Insinöörityön kulunvalvontasovelluksen prototyypin vaatimuksena on 64-bittisessä Windows-käyttöjärjestelmässä toimiva työpöytäsovellus. Prototyypistä toteutettiin suunnitteluvaiheessa kaksi eri versiota. Ensimmäinen prototyyppi toteutettiin käyttämällä Microsoft Visual Studio 2019 -ohjelmistoa ja C#-ohjelmointikieltä. Toinen prototyyppi toteutettiin käyttämällä Electron-hybridikehitystyökalua ohjelmointikielenä JavaScript. Insinöörityön kulunvalvontasovelluksen prototyypin kehitystyökaluksi valittiin lopulta Electron pääosin siksi, että se mahdollisti riittävän nopean ohjelmiston kehitystyön, kun käytössä oli rajattu aikaresurssi kehitystyötä varten. Jatkokehitystä varten on tärkeää valita kulunvalvontasovelluksen loppukäyttöliittymän varsinainen kehitystyökalu

tarkastelemalla eri kehitystyökalujen soveltuvuutta loppukäyttöä ajatellen, huomioiden varsinkin tietoturvaan ja jatkokehitettävyyteen liittyvät asiat.

Prototyypin pääsyoikeushaun jälkeinen näkymä (kuva 7) esittää pääsyoikeushaun palauttamat tulokset selkeästi luettavassa ja selattavassa muodossa. Hakutulosnäkymässä näytettävien tietojen laajuus voidaan määrittää sovelluskokonaisuuden asetuksissa.



Kuva 7. Kulunvalvontasovelluksen prototyypin hakutulosnäkymä pääsyoikeushaun jälkeen.

Pääsyoikeuden voimassaolo pyrittiin toteuttamaan loppukäyttäjille mahdollisimman selkeäksi. Pääsyoikeuden voimassaolon tila esitetään tekstuaalisesti hakutulosnäkymän keskellä, ja tilaa indikoidaan lisäksi käyttämällä joko vihreää tai punaista väriä. Voimassa oleva pääsyoikeus esitetään oletuksena vihreällä värillä. Tilanteissa, joissa pääsyoikeutta ei löydy tai pääsyoikeus ei tarkasteluhetkellä ole voimassa, vihreän värin tilalla käytetään oletuksena punaista. Loppukäyttöliittymän asetukset mahdollistavat myös täysin vapaat värimääritykset ja kielikäännöksen sanavalinnat.

Kulunvalvontasovelluksen prototyypin suunnittelussa huomioitiin erillisen viivakoodinlukijan käyttö osana sovelluksen perustoiminnallisuuksia. Viivakoodinlukijan käyttö luettaessa viivakoodimuotoista henkilötunnusta toteuttaa henkilötunnukseen tai syntymäaikaan perustuvan hakukyselyn riippuen loppukäyttöliittymän ja sovelluskokonaisuuden asetusmäärittelyistä.

Peruskäytössä oletettavasti usein käytettäviin toiminnallisuuksiin määriteltiin erillinen pikanäppäin tai näppäinyhdistelmä käytön helpottamiseksi ja nopeuttamiseksi sovellusta näppäimistöllä käytettäessä. Oletuspikanäppäimet määritettiin Windows-käyttöjärjestelmässä tapahtuvaa loppukäyttöä ajatellen, mutta kaikki pikanäppäimet ja näppäinyhdistelmät voidaan korvata kulunvalvontasovelluksen prototyypin asetuksissa millä tahansa pikanäppäimellä tai näppäinyhdistelmällä.

5 Loppukäyttäjätestaus

Prototyypin loppukäyttäjätestaus toteutettiin rakentamalla testausympäristöksi erillinen lähiverkko eli LAN (Local Area Network) kahden työaseman välille. Molempiin työasemiin valittiin käyttöjärjestelmäksi Windows 10. Taustapalvelinjärjestelmän käytettäviksi tekniikoiksi valittiin Apache HTTP -palvelin MySQL-tietokanta ja PHP-ohjelmointikieli (PHP: Hypertext Preprocessor). Loppukäyttäjätestausta suoritettiin kahden viikon ajan.

Ensimmäisessä työasemassa käytettiin ainoastaan kulunvalvontasovelluksen prototyyppiä loppukäyttökohteessa. Tässä työasemassa loppukäyttäjätestauksen osalta arvioitiin sovelluksen toiminnallisuuksia, käytettävyyttä ja toimintavarmuutta.

Toinen työasema toimi kaikkien sovelluskokonaisuuden vaatimien taustapalvelinjärjestelmien suoritusympäristönä. Tässä työasemassa loppukäyttäjätestauksessa arvioitiin sovelluskokonaisuuden taustapalvelinjärjestelmän eri osien toimivuutta ja toimintavarmuutta sekä testattiin toista kulunvalvontasovelluksen prototyyppiä lukutilassa ja arvioitiin sen tiedonsiirron nopeutta, luotettavuutta ja ohjelmiston toisen instanssin toimintavarmuutta samassa ympäristössä.

Loppukäyttäjätestauksen palaute kerättiin loppukäyttäjiltä kahden viikon testauskäytön jälkeen. Kyselyssä (liite 2) arvioitiin kulunvalvontasovelluksen prototyypin käytettävyyttä ja toimintavarmuutta. Palautekyselyyn vastasi yhdeksän järjestelmän testaukseen osallistunutta henkilöä.

5.1 Käytettävyys

Kyselylomakkeella kerättiin tietoa sovelluksen käytön helppoudesta ja nopeudesta, sovelluksen käyttöliittymän väriteeman soveltuvuudesta sovelluksen käyttöön valoisassa ja pimeässä ympäristössä, lisälaitteiden käytön helppoudesta sekä loppukäyttösovelluksen tekstin ja näkymän lukemisen helppoudesta kauempaa tarkasteltaessa. Palautteesta pyrittiin selvittämään käytettävyyden jatkokehitystarpeet.

Palautteen mukaan loppukäyttösovelluksen käytettävyydessä ei ilmennyt varsinaisia ongelmakohtia. Palautteesta saatiin muodostettua muutamia havaintoja ja jatkokehitystarpeita käytettävyyteen liittyen. Hiiren käyttötarve on loppukäyttösovelluksessa pyritty optimoimaan olemattomaksi pikanäppäimiä ja näppäinyhdistelmiä hyödyntämällä, mutta hiirtä kuitenkin käytettiin palautteen mukaan jonkin verran oletettua enemmän. Haettujen tietojen automaattinen piilottaminen, kun toimenpiteitä ei suoriteta, osoittautui myös muutamissa tapauksissa liian nopeasti tapahtuvaksi: havaittiin muutamia tilanteita, joissa haetut tiedot hävisivät loppukäyttöliittymän näkymästä (automaattinen haettujen tietojen tyhjennys, kun tietoja ei käytetä määritellyn ajan sisällä) liian nopeasti, kun vierailun todentamiseen kului tavallista enemmän aikaa. Lisäksi ilmeni tarve kirjata vierailuja ilman erillistä vierailijakorttia tai kortin numeroa.

5.2 Toimintavarmuus

Kyselylomakkeella kerättiin tietoa sovelluksen vikatilanteiden ja virheiden määrästä, palvelinyhteyden katkoksien määrästä ja katkoksien kestosta sekä vikatilanteista, jolloin ohjelmistoa ei voinut lainkaan käyttää loppukäyttötestauksen aikana. Palautteesta pyrittiin selvittämään sovelluksen toimintavarmuuden ja sovelluskokonaisuuden infrastruktuurin toimintavarmuuden jatkokehitystarpeet. Loppukäyttötestauksen aikana ei ilmennyt sähkökatkoja tai muita vastaavia verkkoliikenteen häiriötilanteita.

Taustapalvelinjärjestelmäkokonaisuuden toimintavarmuus todettiin vakaaksi ja luotettavaksi testauskäytön perusteella. Taustapalvelinjärjestelmä tai mikään sen osa ei vaatinut ylläpitotoimia tai uudelleenkäynnistyksiä testauskäytön aikana.

Taustapalvelinjärjestelmäkokonaisuus todettiin luotettavaksi loppukäyttäjätestauksen aikana.

Verkkoyhteyden toimintavarmuus todettiin vakaaksi ja luotettavaksi testauskäytön perusteella. Verkkoyhteys oli koko testauskäytön ajan käytettävissä ilman katkoksia ja ylläpitotoimia.

Loppukäyttöliittymän toimintavarmuus todettiin vakaaksi ja luotettavaksi testauskäytön perusteella. Loppukäyttöliittymä toimi luotettavasti koko testausajanjakson ajan.

Tulee kuitenkin huomioida, että testaus suoritettiin täysin erillisessä lähiverkossa. Lopullinen toimintaympäristö sisältää hyvin todennäköisesti myös muuta dataliikennettä ja on verkkoratkaisultaan erilainen. Toimintavarmuus on tärkeää testata myös tuotantokäyttöjärjestelmässä ennen sovelluksen käyttöönottoa.

6 Yhteenveto ja jatkokehitys

Insinöörityössä tutkittiin kulkulupahallintoa ja kulunvalvontaprosessia pääosin insinöörityön asiakasorganisaation kannalta sekä soveltuvin osin myös muiden organisaatioiden käyttötarpeita ajatellen. Tutkimuksella pyrittiin tuottamaan kokonaisvaltainen lupahallinnon prosessikuvaus, jossa asiakasorganisaation ja muiden loppukäyttäjäorganisaatioiden tarpeet otetaan huomioon mahdollisimman kattavasti. Asiakasorganisaation toimintaa säätelevät lait selvitettiin ja ne otettiin huomioon kulunvalvontasovellusta sekä sovelluskokonaisuutta suunniteltaessa.

Insinöörityön tavoitteet saavutettiin hyvin kulunvalvontasovelluksen prototyypin testauksen ja siitä kerätyn palautteen perusteella. Insinöörityön tavoitteina oli kehittää ja tehostaa asiakasorganisaation lupahallintoprosessia ja kulunvalvontaprosessia tuottamalla kulunvalvontasovelluksen prototyyppi osana modernin ja nykyaikaisen lupahallintosovelluskokonaisuuden suunnittelutyötä.

Kulunvalvontasovelluksen testaus onnistui hyvin, ja siitä saatiin kerättyä kehitysideoita ja -tarpeita jatkokehitystä varten. Kulunvalvontasovelluksen prototyyppi ja

taustapalvelinjärjestelmä toimivat erittäin vakaasti koko testauksen ajan. Testaukseen valitut taustapalvelinjärjestelmän ratkaisut osoittautuivat luotettaviksi ja toimiviksi.

Loppukäyttäjätestauksen perusteella muodostetun yhteenvedon mukaan kulunvalvontasovelluksen prototyypin jatkokehitystarpeita ovat yleisen pääsyoikeushaun hakutermien laajentaminen, hakutietojen näkymisajan pidentäminen tai näkymisajan määrittäminen pääsyoikeushaun jälkeen, vierailun kirjaaminen ilman vierailijakorttia tai erillistä vierailijakortin numeroa ja hiiren käyttötarpeen vähentäminen.

Sovelluskokonaisuuden muita, olennaisia jatkokehitystarpeita ovat tietokannan viimeistely, taustapalvelinjärjestelmän eri toimintojen kehittäminen, API-rajapinnan jatkokehitys ja hallintakäyttöliittymän kehittäminen. Näiden olennaisten jatkokehitystarpeiden toteuttamisella saadaan aikaiseksi toimiva lopputuote, mutta käytettävyyden kannalta tulee kehittää myös erikseen kuvatut, erilliset loppukäyttöliittymät eri käyttökohteita ja käyttöympäristöjä varten.

Lähteet

Ajokorttilaki. 2011. 386/29.4.2011.

Asuinkiinteistöjen lukitusratkaisu – iLOQ. 2021. Verkkoaineisto. iLOQ. <https://www.iloq.com/fi/ratkaisut/asuinkiinteistot>. Luettu 14.4.2021.

Henkilökorttilaki. 2016. 663/25.8.2016.

Identity and Access Management – SecurID Suite. 2021. Verkkoaineisto. RSA Security. <https://www.rsa.com/en-us/products/rsa-securid-suite>. Luettu 6.4.2021.

Jauho, Tomi. 2020. Turvallisuusupseeri, Puolustusvoimat, Lappeenranta. Keskustelu 23.9.2020.

Kallio, Kalle. 2020. Turvallisuuspäällikkö, Puolustusvoimat, Helsinki. Keskustelu 21.4.2020.

Laki puolustusvoimista. 2007. 551/11.5.2007.

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta. 2018. 1009/2018.

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista. 2009. 617/7.8.2009.

Mäenpää, Teemu. 2015. Utilization of adjacency model in graph analysis. Verkkoaineisto. Vaasan yliopisto. <https://osuva.uwasa.fi/bitstream/handle/10024/7669/isbn_978-952-476-643-2.pdf>. Luettu 9.3.2021.

Nieminen, Joni. 2017. Digitreenit: Perehdy lähimaksamiseen maksukortilla ja puhelimella. Verkkoaineisto. Yleisradio. <https://yle.fi/aihe/artikkeli/2017/09/20/digitreenitlahimaksaminen-yleistyy-vauhdilla-joko-sina-kaytat-sita>. Luettu 6.10.2020.

Nopeat henkilöannostelijat. 2020. Verkkoaineisto. IDcontrol. <https://www.idcontrol.fi/osasto/kulkuportit/nopeat-portit/>. Luettu 1.11.2020.

Puolustusministeriön asetus oleskelu- ja vierailuluvista, kieltotauluista, vartio- ja päivystystehtävää suorittavan virkamiehen koulutuksesta sekä ammattisotilaan perustaidoista ja kunnosta. 2007. 1253/14.12.2007.

Sonali, Patil; Priyanka, Dhumal; Shweta, Lokhande & Trishala, Kamble. 2017. Design and Implementation of Secure Biometric Based Authentication System using RFID and Secret Sharing. Verkkoaineisto. IEEE. <https://ieeexplore.ieee.org/abstract/document/8226175>. Luettu 28.9.2020.

What is Three-Tier Architecture. 2020. Verkkoaineisto. IBM. <https://www.ibm.com/cloud/learn/three-tier-architecture>. Luettu 9.3.2021.

Why are Windows PCs So Popular in Industrial Automation. 2016. Verkkoaineisto. IntervalZero. <https://www.intervalzero.com/software/why-are-windows-pcs-so-popularin-industrial-automation/>. Luettu 5.10.2020.

Asiakkaan vaatimusmäärittely ohjelmistokokonaisuudesta

Taustapalvelinjärjestelmä (Backend)

- API-ohjelmointirajapinta
  - HTTP/REST
  - JSON
- Käyttöoikeusrajaukset järjestelmän käyttäjille
  - Segmentointi

Viestinvälityspalvelu **(optio)**

- Mahdollisuus käyttää ulkoista viestinvälityspalvelua **(optio)**
  - Pääsyoikeuden käsittelyprosessin tilanteen muutosten ilmoittaminen kulkuluvan hakijalle
    - Pääsyoikeushakemus (tai vierailuanomus) vastaanotettu.
    - Pääsyoikeushakemus (tai vierailuanomus) käsitelty (hyväksytty, hylätty).
  - Viestinvälitysmenetelmät
    - Sähköposti
    - Tekstiviesti

Tietokantapalvelin

- SQL-yhteensopiva tietokantapalvelin (MySQL, MariaDB, tms.)

Hallintajärjestelmä (Frontend)

- Windows 64-bit työpöytäsovellus
- Kulkulupahallinto
  - Hakemusten käsittely järjestelmässä
  - Kulkulupien lisääminen, poistaminen ja muokkaaminen
- Raportit
  - Raporttien ja lokien tarkastelu ja tulostus
- Järjestelmän konfiguraatio
  - Tarkastuspisteet
  - Järjestelmän käyttöoikeudet
  - Kohteiden hallinta

Tarkastuspiste (Frontend) – kulunvalvontasovelluksen prototyyppi

- Windows 64-bit työpöytäsovellus
- Kulkuoikeuden tarkastaminen
  - Haku
  - Henkilötiedot
  - Kuva **(optio)**
  - Ajoneuvon rekisterinumerot **(optio)**
  - Näytettävät tiedot pitää voida määrittää erikseen

- Vierailun kirjaaminen (alueelle/alkanut - alueelta pois/päättynyt)
  - Vierailija, alkuaika, syy, kohde
  - Vierailun numero / muut tiedot
- Offline -tuki
  - Tietojen synkronointi offline-käyttöä varten mahdollisten tietokatkojen varalle
- Tuki lisälaitteille
  - Viivakoodinlukija
  - Skanneri (henkilötodistusten, passien, yms. skannaus ja tallennus järjestelmään) **(optio)**

Loppukäyttäjätestauksen palautelomake

Käytettävyys		**Täysin eri mieltä**				**Täysin samaa mieltä**
1	Sovellusta on helppo käyttää.	**1**	**2**	**3**	**4**	**5**
2	Sovellusta on nopea käyttää.	**1**	**2**	**3**	**4**	**5**
3	Sovelluksen näkymä on selkeästi luettavissa päivänvalossa / kirkkaassa ympäristössä.	**1**	**2**	**3**	**4**	**5**
4	Sovelluksen näkymä on selkeästi luettavissa yöllä / pimeässä ympäristössä.	**1**	**2**	**3**	**4**	**5**
5	Sovelluksen näkymää on helppo lukea myös kauempaa.	**1**	**2**	**3**	**4**	**5**
6	Lisälaitteen (viivakoodinlukija) käyttö sovelluksen yhteydessä on helppoa.	**1**	**2**	**3**	**4**	**5**
7	Sovelluksessa on kaikki tarvittavat toiminnallisuudet	**1**	**2**	**3**	**4**	**5**
Toimintavarmuus		**Ei yhtään**				**Todella usein**
8	Kuinka paljon sovelluksen käytössä aiheutui vikatilanteita, sovelluksen virheitä tai sovelluksen kaatumisia?	**1**	**2**	**3**	**4**	**5**
9	Kuinka usein järjestelmä ei ollut yhteydessä palvelimeen vaan toimi ns. Offline-tilassa?	**1**	**2**	**3**	**4**	**5**
10	Kuinka usein järjestelmä ei ollut ollenkaan käytettävissä?	**1**	**2**	**3**	**4**	**5**
Muu		**En ollenkaan**				**Todella usein**
11	Kuinka usein käytit hiirtä, kun käytit sovellusta?	**1**	**2**	**3**	**4**	**5**
Vapaa palaute						
12	Mitä kehitettävää sovelluksessa tai sen toiminnallisuuksissa on? Onko siinä jotain tarpeetonta, puuttuuko jotain tai pitäisikö jotain muuttaa?					
13	Mikä sovelluksessa toimii hyvin?					
14	Mikä sovelluksessa toimii huonosti?					
15	Vapaa palaute					