Olli Hönö

Kulkutunnisteiden personointi- ja hallintaohjelmiston asennus ja konfigurointi

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

13.09.2017

Metropolia

Tekijä Otsikko Sivumäärä Aika	Olli Hönö Kulkutunnisteiden personointi- ja hallintaohjelmiston asennus ja konfigurointi 40 sivua 13.09.2018
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Ammatillinen pääaine	Tietoverkot ja tietoliikenne
Ohjaajat	Teknologiajohtaja, Aventra, Jan Sjöblom Lehtori, Marko Uusitalo

Insinöörityön tavoitteena oli suorittaa asiakasorganisaatiolle toimitetun järjestelmän päivityksen testaus, asennus ja konfiguraatio sekä dokumentoida prosessi. Asiakasorganisaationa oli suuri suomalainen yritys. Insinöörityö tehtiin järjestelmäasiantuntijan roolissa Aventra Oy:ssä keväällä 2018. Järjestelmäasiantuntijan roolissa tavoitteena oli olla tärkeänä osana projektia, suorittaa asennukset, testaukset, konfiguraatiot sekä kirjoittaa tarvittavat dokumentit. Asiakasorganisaatiolle toimitettu järjestelmä oli ollut jo projektin alkuvaiheessa käytössä useamman vuoden useammassa toimipisteessä ympäri Suomea sekä yhdessä muussa maassa.

Asiakasorganisaatiolle asennettu järjestelmä hallitsee siellä käytettäviä kulkutunnisteita, kulkuoikeuksia sekä kaikkia niihin liittyviä tietoja. Projektissa päivitettävä ohjelmisto on yksi oleellinen osa tätä järjestelmää. Ohjelmisto asennettiin insinöörityön aikana yhteen asiakkaan Suomen toimipisteeseen ja se asennettiin siellä asiakkaan toimittamiin työasemiin.

Insinöörityössä käytiin läpi järjestelmän käyttämät tekniikat sekä teknologiat, niihin liittyvä teoria ja kuvataan järjestelmän toiminta, sen eri osat sekä varsinainen projektin toteutus. Projektin lopputuloksena oli onnistunut asennus, uutta dokumentaatiota ja opettavainen kokemus projektista. Asennettu päivitys on parantanut ohjelman vikasietoisuutta sekä nopeuttanut ja yksinkertaistanut sen käyttöä. Projektin aikataulutus oli yksi selkeästi parannettava asia ja siihen pitää jatkossa kiinnittää enemmän huomiota. Varsinainen asennus oli kuitenkin onnistunut.

Avainsanat	RSA, RFID, Kulkutunnisteet, Henkilökortit, Älykortit

Author Title Number of Pages Date	Olli Hönö Installation and configuration of access control token personalization and management software 40 pages 13 September 2018
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Professional Major	Communication Networks and Applications
Instructors	Jan Sjöblom, Chief Technology Officer, Aventra Oy Marko Uusitalo, Senior Lecturer

The aim of the thesis was to test, install and configure an update into a customer's system and document the process. The customer organization was a large Finnish company. The project was done in the role of a systems specialist at Aventra Oy in the spring of 2018. The role of the systems specialist was to be in an important part of the project, to carry out the installations, tests, configuration and to write the necessary documentation. The system had been previously running for many years in the customers environment in multiple locations throughout Finland and in one other country.

The system installed in the client organizations environment manages the access control tokens, access control areas and all the related information for the client. The software updated in the project is one essential component of this system. During the project described in this thesis the software was installed at one of the customers offices in Finland. It was installed there on workstations provided by the customer.

The thesis explains the techniques used by the system, as well as the technologies, related theory, describes the operation of the system, its various components and the practical work done in the project. The result of the project was a successful installation, new documentation and a valuable learning experience on working in projects. The installed update has improved the fault tolerance of the software as well as speeding up and simplifying its use. The scheduling of the project was one of the things that should be improved upon and it should be paid more attention to in future projects, but the actual installation was successful.

Keywords	RSA, RFID, Access control tokens, ID-cards, Smartcards

Sisällys

Lyhenteet

RFID	Radio Frequency Identification on teknologia, jota käytetään tiedon etäluku-un ja -kirjoittamiseen.
PKI	Public key infrastructure on tapa hallita digitaalisia varmenteita ja salausavaimia.
APM	ActivePerso Manager on Aventran kehittämä ohjelma, jota käytetään muun muassa henkilökorttien personointiin.
ACR	Admission Control Registry on Aventran tarjoaman järjestelmäkokonaisuuden kutsumanimi, jota käytetään projektin asiakkaan toimistoilla ja tehtailla henkilökorttien ja muiden tunnisteiden hallintaan ja tuotantoon.
RSA	RSA on salausalgoritmi, jota käytetään avainten salaamisessa.
MIFARE	MIFARE on standardi, joka määrittelee etäluettavan muistikortin. Tässä tapauksessa muistikortti on henkilökortin sirulla.
DESFIRE	Desfire on Mifare standardin mukainen henkilökorttien tuoteperhe.
CA	Certificate Authority on PKI-ympäristön luotettu osa joka jakaa, säilyttää ja allekirjoittaa digitaalisia varmenteita.
ACMS	ACMS eli ActiveCMS on Aventran kehittämän järjestelmä, jolla hallitaan tunnisteita ja henkilöitä selainkäyttöliittymän kautta.
HR	Human Resources tarkoittaa yleisimmin henkilöstötietojen tai asioista vastaavaa henkilöä tai osastoa.
AD	Active Directory on Microsoftin Windows pohjainen palvelu, jolla hallitaan käyttäjiä ja ryhmiä.
REST	REST eli Representational State Transfer on arkkitehtuurimalli ohjelmointirajapintojen ja verkkopalveluiden kehittämiseen.

API	Application programming interface eli ohjelmointirajapinta on tapa, jolla ohjelmat ja järjestelmät voivat lähettää tietoja toisilleen.

1 Johdanto

Tämän insinöörityön tarkoituksena oli päivittää jo käytössä olevaa ohjelmaa, uudistaa sen konfiguraatiota, suorittaa päivityksien ja muutosten testausta sekä dokumentoida prosessia. Ohjelmalla suoritetaan henkilökorttien ja muiden tunnisteiden visuaalista personointia sekä RFID-sirun ohjelmointia ja hallintaa. Uudistuksen tarkoituksena on helpottaa ohjelman käyttöä, parantaa sen vikasietoisuutta, parantaa ylläpidettävyyttä, tuoda lisäominaisuuksia ja helpottaa vikatilanteiden selvittämistä. Projektissa kuvataan asiakasorganisaatiolle toimitettu järjestelmä tietyin rajauksin; ulkoisten urakoitsijoiden hallintaan luotua järjestelmää ei kuvata. Muuten projektissa esitetty järjestelmäkuvaus vastaa todellisuutta. Projektin asiakasorganisaatiota ei mainita tässä insinöörityössä nimeltä, se on piilotettu kaikista kuvista ja dokumentaatiosta.

Insinöörityö tehtiin Aventra Oy:lle keväällä 2018, jossa olin osana asiakasprojektia järjestelmäasiantuntijan roolissa. Järjestelmäasiantuntijana tehtävänäni oli suorittaa ohjelman uuden version ja konfiguraation testausta, dokumentointia, konfigurointia sekä lopullista asennusta asiakkaan tiloihin. Lopulliset asennukset suoritettiin 19.2.2018 asiakkaan toimipisteellä, asennukset suoritettiin kahden henkilön työparina.

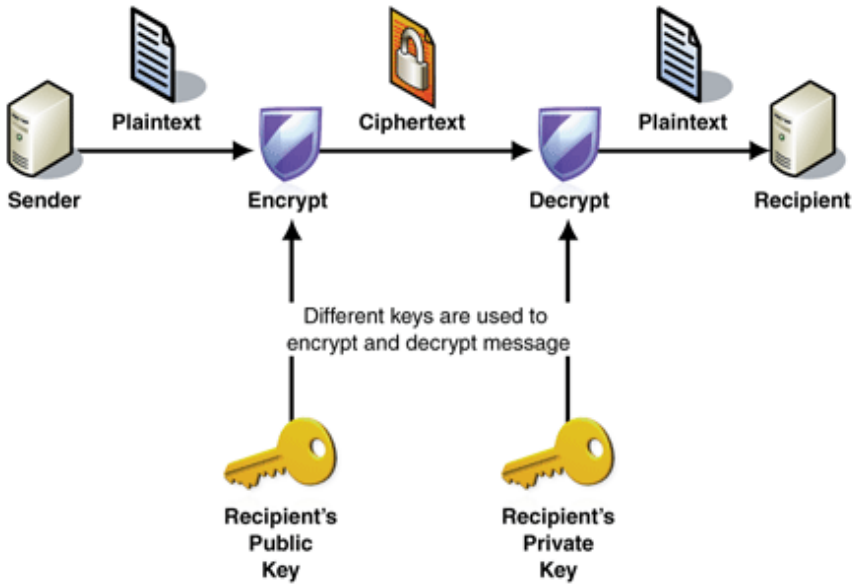
Tämä insinöörityö kuvaa järjestelmän toimintaa, sen käyttämiä teknologioita ja tekniikoita, projektin vaiheita, projektin lopputulosta ja opittuja asioita.

2 Järjestelmässä käytetyt teknologiat sekä tekniikat

2.1 Salaus

Salauksen tarkoituksena on salata tietoja niin, että vain siihen oikeutetut henkilöt voivat sen lukea. Salausmenetelmät jaetaan kahteen ryhmään: symmetrisiin ja asymmetrisiin. Symmetrisessä salauksessa sekä salaus että purku tehdään samalla avaimella. Asymmetrisessä salauksessa salaus ja purkaminen tehdään eri avaimilla. Nämä avaimet muodostavat avainparin. Tässä projektissa käytetään lähinnä asymmetristä salausta ja keskitytään siihen.

Asymmetrisessä salauksessa käytetään avainparia. Avainparissa on julkinen ja salainen avain. Julkisen avaimen voi halutessaan paljastaa kenelle vain vaarantamatta järjestelmän turvallisuutta. Salainen avain taas tulee pitää nimensä mukaisesti salassa. Julkisella avaimella kuka tahansa muu voi halutessaan salata esimerkiksi tekstiä, jonka voi avata vain ainoastaan saman avainparin salaisella avaimella. Julkisen avaimen avulla voidaan myös esimerkiksi todentaa, että saman avainparin salaisen avaimen haltija on lähettänyt viestin. Kuvassa 1 esitetään tyypillinen käyttötapaus asymmetrisestä salauksesta.



Kuva 1. PKI:n rakenteen kuvaus (1).

Projektissa käytettävä RSA-salausalgoritmi kuvailtiin julkisesti ensimmäistä kertaa vuonna 1978. RSA-lyhenne tulee sen kehittäjien sukunimien etukirjaimista, Ron Rivest, Adi Shamir ja Leonard Adleman. Myös Iso-Britannian tiedustelupalvelu GCHQ oli kehittänyt vastaavan järjestelmän vuonna 1973, mutta se oli luokiteltu salaiseksi vuoteen 1997 asti (2). RSA on suhteellisen hidas algoritmi, eikä sitä tästä syystä yleisesti käytetä koko datan salaamiseen. Projektissa sitä käytetään kulunvalvontatunnisteiden symmetristen avainten salaukseen.

RSA-salausalgoritmin turvallisuus perustuu siihen, että suurten alkulukujen tulon tekijöiden selvittäminen laskennallisesti on erittäin vaikeaa ja ennen kaikkea aikaa vievää.

RSA:n matemaattinen todistus perustuu Fermatin pieneen lauseeseen, jonka mukaan kaikilla alkuluvuilla p ja kokonaisluvuilla a on voimassa $a^p \equiv a\ (mod\ p)$, eli a^p on kongruentti a:n kanssa modulo p (3). Esimerkiksi jos $a = 2$ ja $p = 7,\ 2^7 = 128$, ja $128 - 2 = 7 \times 18$, joka on jaollinen 7:llä.

RSA-algoritmin käyttöön tarvitaan julkinen avain, yksityinen avain ja koodausavain k. Ensiksi valitaan kaksi (yleensä erittäin suurta, mutta tässä esimerkissä pientä) alkulukua, esimerkiksi $P = 13, Q = 19$. Niistä lasketaan $n = pq$ eli $13 \times 19 = 247$ ja $d = (p-1)(q-1)$ eli $12\ x\ 18 = 216$. Lasketaan luku e siten, että $syt(e, d) = 1$. Eli suurin yhteinen tekijä d:llä ja e:llä on 1 eli ne ovat keskenään jaottomia, yksi tällainen jaoton luku on esimerkiksi 7. Purkuavain k saadaan, kun lasketaan e :n käänteisalkio, $k \times e\ mod\ d = 1$. Eli $31 \times 7\ mod\ 216 = 1$.

Näillä tiedoilla voimme koota julkisen ja yksityisen avaimen, joilla voimme salata tietoa ja purkaa salauksen. Julkinen avain koostuu kahdesta luvusta, $n = 247$ ja $e = 7$. Selkokielisen viestin t salaaminen salattuun muotoon s onnistuu salausfunktiolla $s(t) = t^7\ mod\ 247$ eli siihen käytetään julkista avainta. Yksityinen avain koostuu luvuista $n = 247$ ja $d = 31$. Salatun viestin s muuttaminen selkokieliseen muotoon t onnistuu purku funktiolla $t(s) = s^{31}\ mod\ 247$, tähän siis käytettiin yksityistä avainta.

Voidaan esimerkiksi salata tieto siitä, että $t = 96$. Käytetään julkista avainta, salattu viesti on $s = 96^7\ mod\ 247$ eli $s = 229$. Tämä salattu viesti voidaan taas purkaa käyttämällä yksityistä avainta, selkokieliseksi purettu viesti $t = 229^{31}\ mod\ 247$ eli $t = 96$. Kuten aiemmin todettua oikeassa RSA-implementaatiossa käytetään erittäin suuria lukuja. Tällä hetkellä vuoteen 2030 turvalliseksi arvioidut RSA-avaimet ovat vähintään 2048 bittiä pitkiä. Myös usein käytetään julkista eksponenttia $e = 65537$, joka on alkuluku ja täten mahdollistaa nopean salauksen, mutta silti tarpeeksi iso tarjotakseen hyvän turvallisuuden.

2.2 PKI

“Public key infrastructure” eli PKI on periaate, johon henkilökorttien digitaaliset varmenteet ja niiden turvallisuus perustuvat. PKI:llä pystytään luomaan järjestelmä, jonka avulla luodaan, säilytetään, tarvittaessa perutaan ja jaetaan varmenteita (4). Vaikka työssä kuvattu järjestelmä ei ole täysi PKI-implementaatio, on työssä kuitenkin seurattu useita

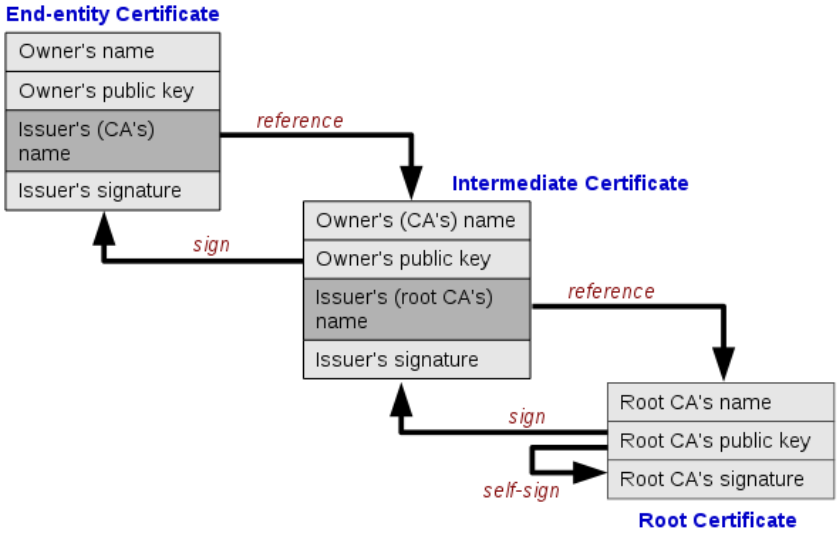
PKI:n periaatteita. Tässä työssä käytettävän järjestelmän tärkeimmät ja työlle oleellisimmat osat ovat itse varmenne, Certificate Authority (CA), eli varmentaja ja Registration Authority (RA), eli varmenteiden rekisteröijä.

2.2.1 Varmenne

Varmennetyyppi, johon tässä työssä keskitytään, on eräänlainen elektroninen henkilöllisyystodistus. Varmenteeseen on koottuna tietoja esimerkiksi varmenteen julkisesta avaimesta, varmenteen saajan nimestä, varmenteen voimassaoloajasta ja varmenteen myöntäjästä. Muita varmennetyyppejä on monia. Yksi esimerkki laajasti käytössä olevasta varmenteesta on TLS/SSL-palvelinvarmenne, jolla palvelin todentaa olevansa se palvelin, johon käyttäjä yrittää yhdistää. Kaikki projektissa käytettävät palvelimet käyttävät myös TLS/SSL-tyyppisiä palvelinvarmenteita suojaamaan kommunikaatiota.

2.2.2 Varmentaja

PKI perustuu kaikkien järjestelmän käyttäjien yhteisesti luotettuun tahoon, Certificate Authorityyn (CA), joka jakaa varmennepyynnöstä varmenteita (5). Certificate Authority eli varmentaja myöntää varmenteita käyttäjille sekä takaa varmenteiden aitouden ja niissä olevien tietojen oikeellisuuden. Kun jokin ohjelma vastaanottaa varmenteen, se tarkistaa varmenteesta, kuka sen on allekirjoittanut ja mistä sen allekirjoittajan varmenne on noudettavissa. Seuraavaksi ohjelma hakee tämän varmenteen ja taas tekee samat toiminnot, kunnes varmenne on itse allekirjoitettu eli juurivarmenne. Varmentaja itse varmentaa oman juurivarmenteensa (Root Certificate). Tästä juurivarmenteesta lähdetään rakentamaan varmenteiden hierarkiaa ylöspäin, kuten kuvasta 2 näkyy. Varmentajan oma varmenne ja sen salainen avain ovat erittäin tärkeä pitää turvassa. Jos ne pääsevät vääriin käsiin, on koko varmenneketju hyödytön.



Kuva 2. Varmenteiden hierarkia (6).

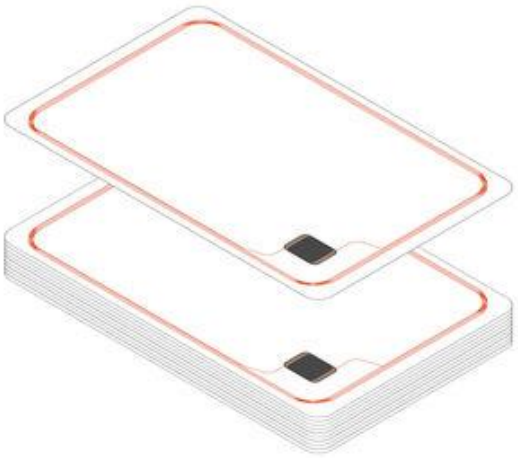
2.2.3 Rekisteröijä

Projektissa keskitytään hyvin laajalti rekisteröintipisteen toimintaan. Registration authority (RA) eli rekisteröijä on PKI-järjestelmässä osa, joka pystyy pyytämään varmenteita CA:lta (5). Rekisteröijä varmistaa varmenteiden hakijan henkilöllisyyden ja tarkistaa sekä kerää varmenteisiin tulevat tiedot. Tässä projektissa rekisteröijän roolia pitää henkilökorttien personointi- ja hallintapiste tai tarkemmin sen käyttäjänä toimiva henkilö.

2.3 Kulkutunnisteet

Projektissa oleellisena osana on personoitava ID-kortti tai muu kulkutunniste. Kaikki projektin asiakkaalla käytettävät kortit ja muut kulkutunnisteet käyttävät RFID-teknologiaa. Tunnisteisiin on upotettu pieni siru sisälle, joka on teoriassa täysi tietokone. Joissain projektissa käytettävissä tunnisteissa on useampia siruja, mutta kortille ei voi käytännössä laittaa useampaa samalla taajuudella toimivaa sirua, vaikka se teknisesti olisi mahdollista. Projektin ympäristössä on mahdollista käyttää hyvin montaa erilaista tunnistetta, osa näistä on id-kortteja, joihin tulostetaan henkilön kuva ja tietoja, ja osa myös erilaisia tageja eli kuvattomia kortteja tai avaimenperiä. Näiden tunnisteiden sisällä olevissa siruissa on oma CPU, RAM-muistia, EEPROM-muistia, ROM-muistia sekä RFID-antenniin tarvittavat yhteydet. Myös varsinaisiin krypto-operaatioihin on oma prosessori. Siruilla on monimutkaiset turvamekanismit, joilla pystytään turvaamaan sirulla olevat salausavai-

met. Turvamekanismit seuraavat muutoksia esimerkiksi sen käyttöolosuhteissa, jännitteessä, lämpötilassa ja kellotaajuudessa, jos muutoksia huomataan, on avaimet sirulta mahdollista tuhota (7). Koska kortin siruilla tehdään salaustoimintoja ja siihen liittyvää laskentaa, on sen suojaaminen fyysiseltä hakkeroinnilta tärkeää. Kortin RFID-antenni koostuu usein n. 5 kierroksesta kuparinauhaa, joka on kierretty kortin sisään. Kuvassa 3 havainnollisestaan RFID-antennin ja RFID-tunnisteen tyypillistä sijaintia tunnistekortin sisällä.



Kuva 3. Havainnekuva RFID-antennista ja RFID-tunnisteesta kortin sisällä (8).

Kun kortinlukija kommunikoi kortin kanssa, se lähettää radiotaajuista perussignaalia eli kantoaaltoa, jonka taajuus tälle antennille on 13,56 MHz. Tämä taajuus mahdollistaa kortille lukuetäisyyden, mikä on noin 2-5 cm riippuen lukijasta. Kortti saa kortinlukijan luomasta elektromagneettisesta kentästä sen tarvitseman virran. Tämä kortin ja lukijan välinen liikenne on salattua. ID-kortit personoidaan visuaalisesti, sekä koodaamalla kortti. Korteille usein tulostetaan henkilön nimi, hänen kuvansa, yrityksen nimi, logo tai muuta vastaavaa visuaalista tulostusta. ID-korteille on myös mahdollista laminoida päälle ohut muovikerros, jonka tarkoituksena on suojata kortin pintaa kulumiselta.

Projektissa käytettävien kulkutunnisteiden turvallisuus perustuu osaksi joidenkin PKI:n periaatteiden ja tunnisteiden fyysisen turvallisuuden lisäksi myös tunnisteiden tiedostorakenteeseen ja avainten käyttöön. Tunnisteilla olevilla siruilla on 2-4kB muistia. Tätä

muistia käytetään hyväksi asettamalla sinne sovellus, jonka tiedostoihin kirjoitetaan tunnisteen personointivaiheessa sen tietoja. Tunnisteella olevalle sovellukselle kirjoitetaan muun muassa tunnisteen numero, tunnisteen saavan henkilön ID, vaihtoehtoinen tunnisteen ID sekä muutama datatiedosto. Nämä ylimääräiset datatiedostot ovat siellä lähinnä tulevaisuutta varten. Jälkikäteen on helpompi kirjoittaa olemassa oleviin tiedostoihin dataa kuin luoda myös tiedostot.

Sovellukselle varattu muisti on jaettu kolmeen osaan: jokaisesta tiedostosta on A-, B- ja C-versiot. Jokaisella versiolla on myös oma sarja luku- ja kirjoitusavaimia. Tällä saavutetaan kyky vaihtaa järjestelmässä käytettävät avaimet uusimatta kaikkia tunnisteita. Jos esimerkiksi A-sarjan luku- ja kirjoitusavainten havaittaisiin olevan uhattuna, voidaan melko helposti siirtyä käyttämään B-sarjan avaimia järjestelmässä. Näillä avaimilla myös estetään tunnisteilla olevien tietojen luvaton lukeminen. Kaikille lukijoille, joilla on lupa lukea tarvittavat tiedot tunnisteelta, on ”opetettu” käytettävän avainsarjan lukuavain eräänlaisella ”opetuskortilla”. Tämä on yleinen tapa kulunvalvontajärjestelmissä, ja avaimet tallennetaan turvalliseen muistiin lukijan sisälle.

2.4 RFID

Projektin kortit sekä muut tunnisteet käyttävät erilaisten lukijoiden kanssa kommunikointiin RFID-teknologiaa. RFID:n avulla voidaan tietoa lukea sekä kirjoittaa etänä. RFID:ssä on usein kolme komponenttia, ”tag” eli tunniste, antenni ja lukija (9). Tunniste ja antenni ovat tässä tapauksessa kortissa sekä muissa tunnistetyypeissä yhdessä. Tunniste voi tyypiltään olla täysin passiivinen, aktiivinen tai puoliaktiivinen.

Passiivinen tunniste on täysin ilman omaa virtalähdettä ja odottaa lukijalta lähetettyä radioteitse saatavaa energiaa. Lukija generoi jatkuvasti radiotaajuista kantoaaltoa, ja kun passiivinen tunniste tulee sen alueelle, se saa käyttövirtansa tästä kantoaallosta. Kaikki korteissa olevat RFID-tunnisteet ovat passiivisia. Aktiivinen tunniste taas sisältää oman virtalähteen ja lähettää usein jatkuvasti ja automaattisesti tunnistenumeroansa ulkomaailmaan. Puoliaktiivinen tunniste taas lähettää tunnistenumeronsa oman virtalähteen avulla, kun se huomaa RFID-lukijan sen läheisyydessä. Yleisesti käytetyt RFID-lukijat ovat suhteellisen pieniä (kuva 4).

Kuva 4. Idesco 8, eräs yleisesti käytetty RFID-lukija (10).

RFID-järjestelmissä olennaisena osana ovat niissä käytettävät taajuudet. Taajuudet muuttavat lukuetäisyyksiä, häiriösietoisuutta, lukunopeuksia ja muita ominaisuuksia. Suomessa taajuusalueita ja niiden käyttöä valvoo ja säätelee Viestintävirasto. Tällä hetkellä yleisesti käytössä olevia taajuuksia on neljä, matala taajuusalue (LF), korkea taajuus (HF), erittäin korkea taajuusalue (UHF) ja mikroaaltotaajuusalue (11). Vaikka eri taajuuksilla on erilaisia lukuetäisyyksiä, saadaan kaikkien lukuetäisyyksiä parannettua moninkertaiseksi suurentamalla antenneja. Projektissa käytettävät antennit ovat kuitenkin niin pieniä, että etäisyydet jäävät pienemmiksi.

Matalaan taajuusalueeseen kuuluu 125-134 KHz. Matalan taajuusalueen tunnisteita käytetään esimerkiksi eläinten tunnistukseen ja autojen varkaudenestojärjestelmiin. Niiden ominaisuuksiin kuuluvat heikompi lukuetäisyys, pienempi lukunopeus ja parempi häiriönsietokyky. Isommilla antenneilla voidaan saavuttaa tietyissä olosuhteissa jopa metrin lukuetäisyyksiä (12).

Korkean taajuuden tunnisteet toimivat 13,56 MHz:n taajuudella. Tämä on kaikkien projektin erilaisten RFID-tunnisteiden käyttämä taajuus. Sen ominaisuuksiin kuuluu parempi lukuetäisyys, noin 0,6 – 1,5m, tunnisteiden halpa hinta sekä ei-metallisten aineiden hyvä läpäisykyky ja häiriönsietokyky. Projektissa käytettävien lukijoiden kanssa lukuetäisyys jää kuitenkin käytännössä vain muutamaan senttiin. Kulunvalvonnan lisäksi sitä käytetään esimerkiksi kirjojen seuraamiseen kirjastoissa sekä vaatteiden jäljittämiseen (11).

Erittäin korkean taajuusalueen tunnisteet toimivat 300 – 956 MHz alueella, niistä tyypillisiä käytettäviä taajuuksia ovat 433 MHz ja 865 MHz – 956 MHz. Sen ominaisuuksiin

kuuluvat muun muassa monen tunnisteen lukeminen samanaikaisesti sekä nopeasti, kohtalainen häiriösietokyky sekä pitkät lukuetäisyydet. Passiivisilla UHF-tunnisteilla voidaan päästä noin 6-8 metrin lukuetäisyyksiin ja aktiivisilla yli 100 metrin lukuetäisyyksiin. UHF-taajuusalueen tunnisteita käytetään eniten logistiikassa, esimerkiksi konttien, laatikoiden ja kuorma-autojen seurantaan satama- tai varastoalueilla. (11).

Mikroaaltotaajuusalueeseen kuuluvat kaikki 2-30 GHz alueelta, joista tyypillisiä käytettäviä taajuuksia ovat 2,45 GHz sekä 5,8 GHz. Mikroaaltotaajuusalueen ominaisuuksiin kuuluvat nopea tiedonsiirto, nopea lukunopeus ja pitkä lukuetäisyys. Mikroaaltotaajuudella toimivia tunnisteita käytetään samoissa paikoissa kuin UHF-tunnisteita. (11).

3 Järjestelmän arkkitehtuuri

3.1 ACR

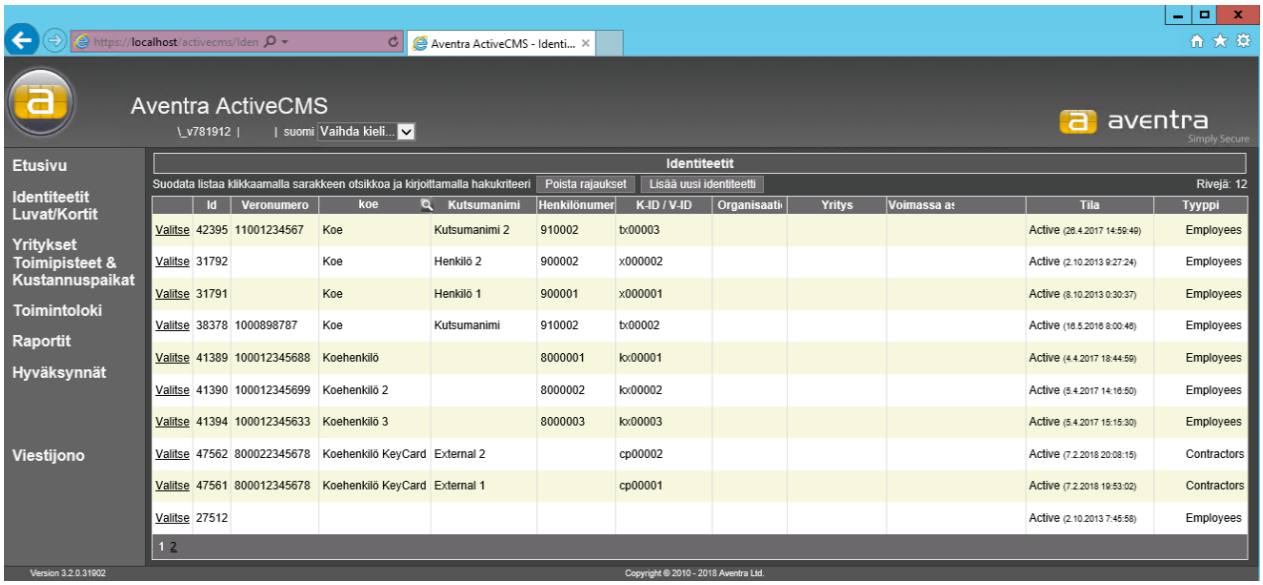
ACR on Aventran asiakasorganisaatiolle kehittämä järjestelmäkokonaisuus, jolla hallinnoidaan tietoja henkilöistä, heidän korteistaan, heille määritellyistä kulkuneuvoistaan ja kulkuoikeuksista. ACR kuvaa kokonaisuutta, johon kaikki pienemmät järjestelmän osat ja osakokonaisuudet kuuluvat.

ACR tulee sanoista Access Control Registry, eli vapaasti suomennettuna kulkuoikeusrekisteri. Tämä nimi kuvaa hyvin ACR:n päätehtävää, joka on hallinnoida pääsyoikeuksia ja siihen liittyviä kokonaisuuksia. ACR on yhteydessä moneen asiakkaan tietojärjestelmään ja hakee näistä järjestelmistä tietoa, jota se sitten pystyy käyttämään. Esimerkiksi ACR saa joka aamu asiakkaan HR-järjestelmästä muuttuneet tai uudet tiedot, joiden perusteella tehdään automaattisia muutoksia henkilöiden kulkuoikeuksiin.

3.2 ActiveCMS

Koko ACR järjestelmäkokonaisuus pohjautuu ActiveCMS:ään ja sillä on erittäin keskeinen osa. ActiveCMS on Aventran kehittämä tunnisteiden ja niihin liittyvien tietojen hallintajärjestelmä. ActiveCMS:n oleellisimpina osina ovat sen oma palvelin sekä helppokäyttöinen selaimella toimiva käyttöliittymä (kuva 5). ActiveCMS:n web-käyttöliittymällä voi-

daan helposti tarkastella ja muokata esimerkiksi henkilön tietoja, kortin tietoja sekä tarvittaessa vaikka peruuttaa eli revokoida henkilön kulkutunnisteen kulkuoikeus. ActiveCMS:llä on asiakasorganisaatiossa monia käyttäjiä. Sitä käyttävät esimerkiksi vartijat, HR-henkilöt, kulunvalvonnasta vastaavat henkilöt sekä myös tietyissä tapauksissa Aventran henkilökunta.



Kuva 5. Aventra ActiveCMS:n -selainkäyttöliittymä.

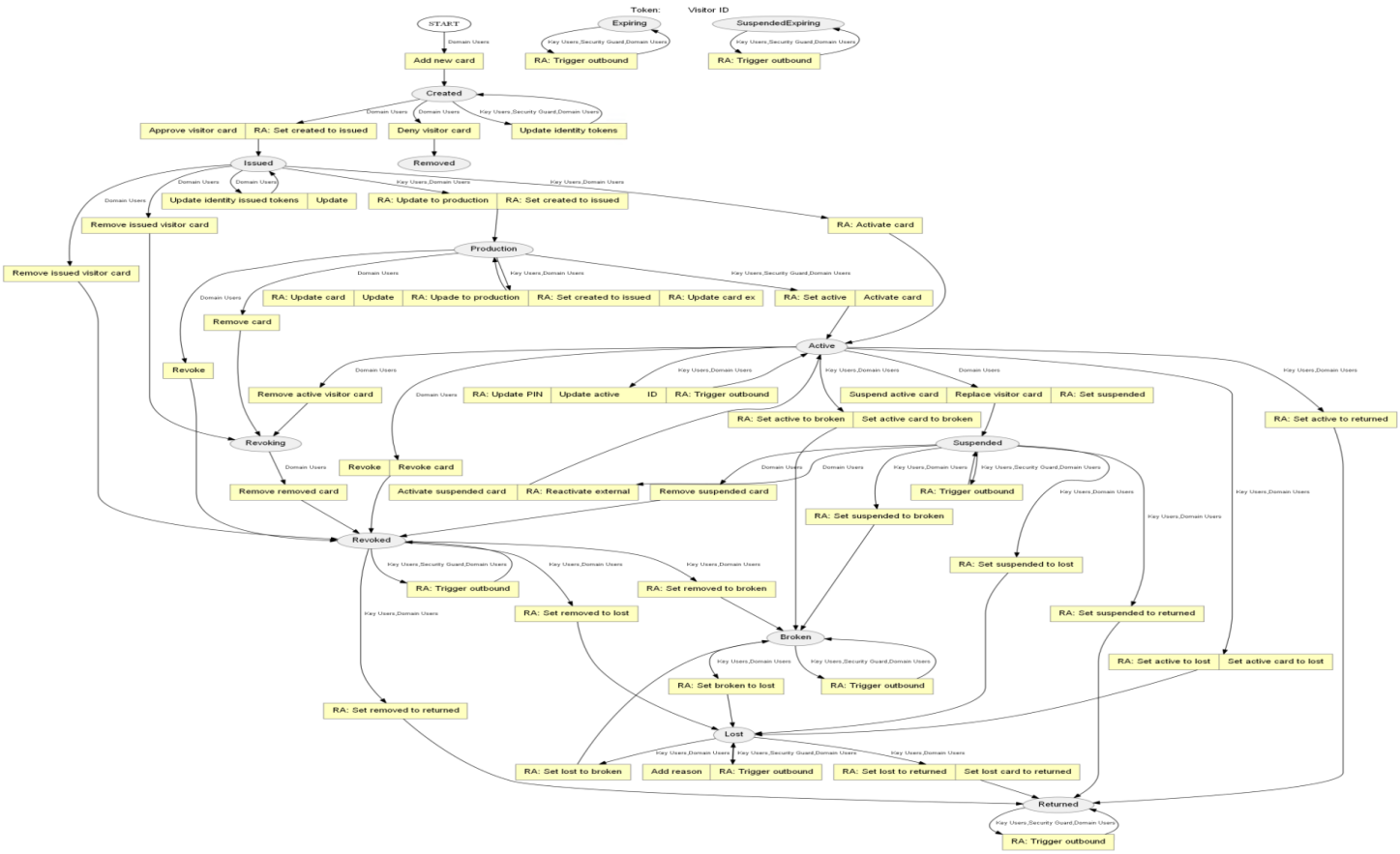
3.2.1 ActiveCMS toimintaperiaate

ActiveCMS:n kaikki toiminta perustuu erilaisiin entiteetteihin, niiden tiloihin, niitä muuttaviin operaatioihin sekä niitä määrääviin sääntöihin. ActiveCMS on siis monipuolisesti muokattaviin sääntöihin perustuva tilamoottori. Sen tärkein tehtävä on automatisoida kulunvalvontaan liittyviä prosesseja mahdollisimman paljon. Se lisää myös turvallisuutta ja mahdollisia virheitä poistamalla kaikki turhat ja vanhentuneet kulkuoikeudet automaattisesti. ActiveCMS:n avulla siis pystytään käsittelemään kaikkia entiteettejä ja niiden muutoksia.

Näitä entiteettejä on esimerkiksi kaikki kortit, henkilöt, yritykset tai sopimukset. Kaikilla näillä voi olla hyvin monia eri tiloja. Esimerkiksi tunnisteella voi asiakkaan järjestelmässä olla 15 erilaista tilaa. Näitä tiloja muuttamalla voidaan henkilön tilannetta muokata, esimerkiksi, jos henkilö on siirretty blocked-tilaan, otetaan häneltä automaattisesti samalla kaikki kulkuoikeudet pois. Tai jos henkilön tiedoissa on tietty toimipiste merkittynä, saa

hän automaattisesti tietyt kulkuoikeudet ja niiden kautta sopivat tunnisteet. Tällä tavalla pystytään automatisoimaan kulkuoikeuksiin liittyviä prosesseja.

Tunnisteiden tiloja, henkilöiden tiloja tai tietoja muuttamalla voidaan siis hallita henkilöiden kulkuoikeuksia. Kuvassa 6 näkyvät kaikki eräälle vierailijakorttityypille konfiguroidut tilat sekä niitä muuttavat operaatiot. Osaa tiloista tai operaatioista ei ole konfiguroitu kaikille korttityypeille, koska tilat ovat kaikille korttityypeille yhteisiä riippumatta siitä, käytetäänkö niitä vai ei.

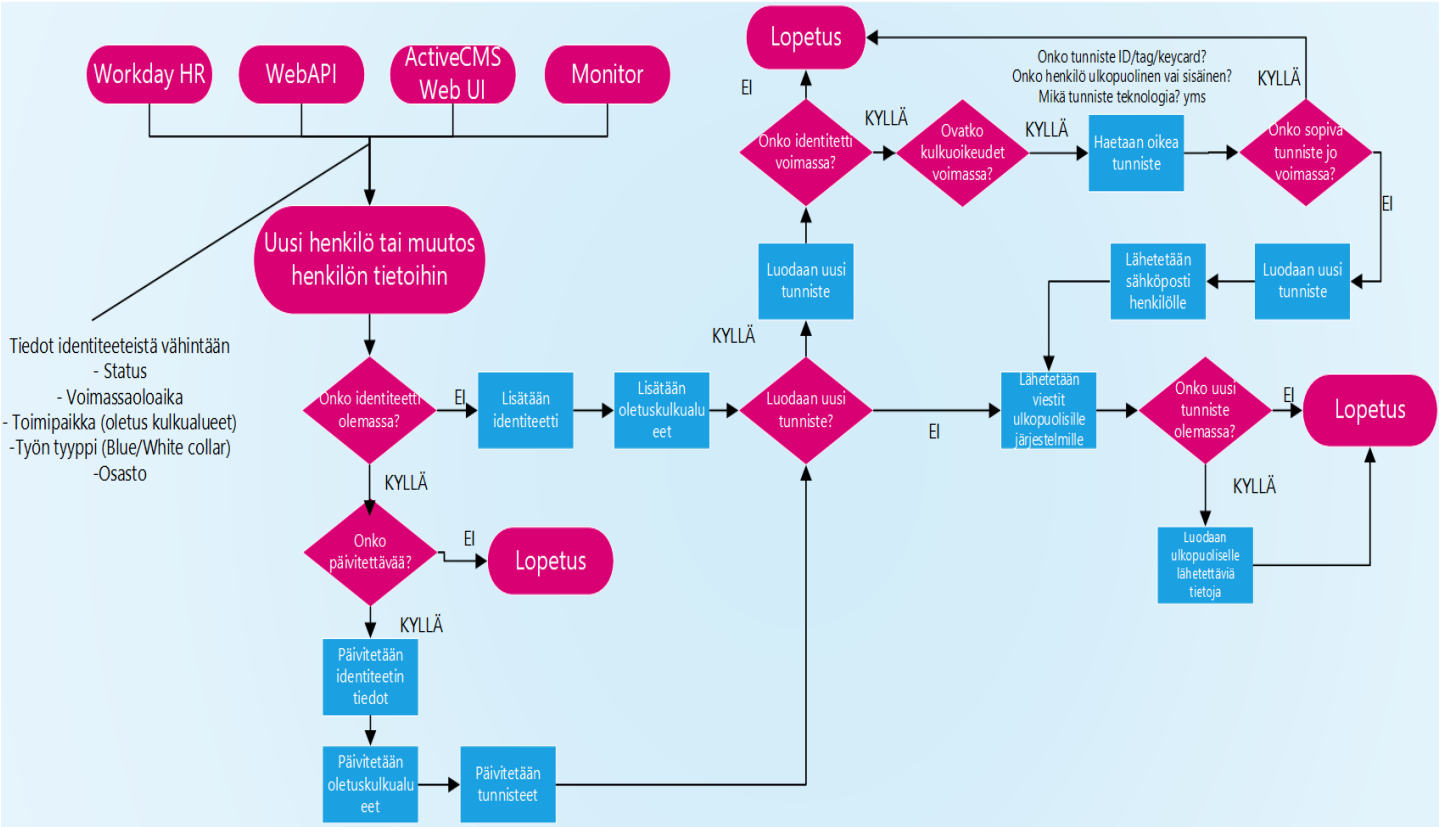


Kuva 6. Asiakkaan järjestelmässä yhden vierailijakorttityypin mahdolliset tilat ja niitä muuttavat operaatiot.

Osa näistä operaatoista voidaan suorittaa esimerkiksi Aventran kehittämällä Active Perso Manager -ohjelmalla, osa taas selaimella käytettävän käyttöliittymän kautta ja osa taas suoritetaan automaattisesti tietyissä tilanteissa. Operaatioilla voi myös olla niihin linkitettyjä ns. ”before-operaatoita” tai ”after-operaatioita”. Nämä operaatiot suoritetaan aina ennen tai jälkeen, kun niihin linkattu operaatio on suoritettu. Eri toiminnot vaativat

myös erilaiset oikeudet. Näitä oikeuksia jaetaan asiakkaan hallitseman käyttäjähakemiston, Actice Directoryn ryhmien avulla. Lähes kaikissa operaatioissa kuitenkin muutetaan jonkun entiteetin tilaa johonkin, joten kaikki tosiaan perustuu entiteetteihin ja niiden tiloihin.

ActiveCMS-järjestelmä voi vastaanottaa uusia tietoja henkilöistä, heidän korteistaan ja kulkuoikeuksista monella eri tavalla, mutta kaikki nämä tiedot käsitellään saman logiikan mukaa riippumatta siitä mistä tieto varsinaiseti tulee. Kuvassa näkyy koko tarkistusketju, kun uutta tietoa tulee ActiveCMS-järjestelmään sisään.

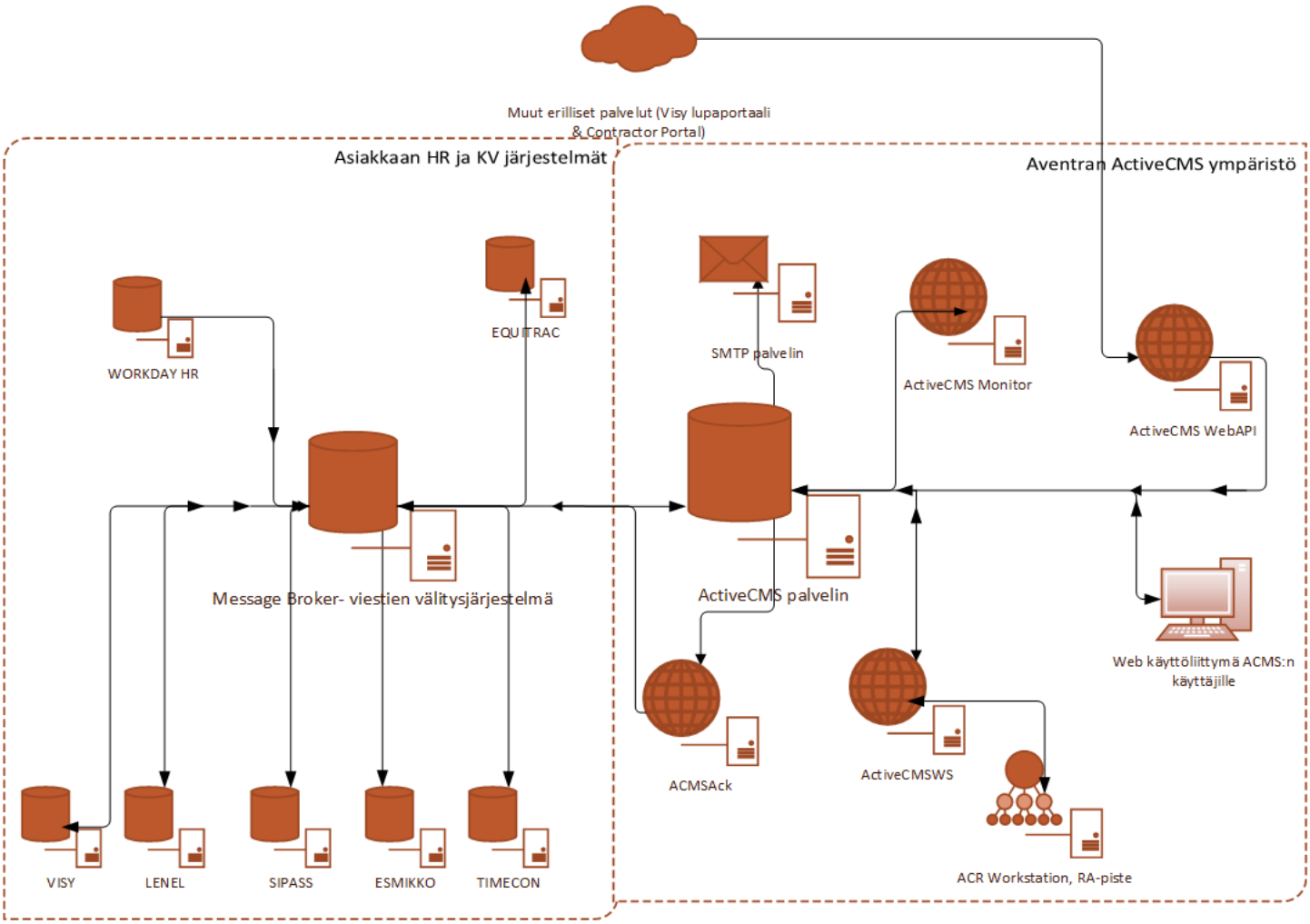


Kuva 7. Uuden henkilön tai päivitetyn tiedon tuominen järjestelmään

Kun luodaan uusi henkilö tai olemassa olevan henkilön tietoja päivitetään, käydään läpi sama logiikka ja samat tarkistukset. Tässä tarkistusketjussa annetaan oletuskulkualueet sekä niitä vastaavat tunnisteet. Suurin osa kaikista kulkuoikeuksista on oletuskulkualueita, ja ne annetaan henkilön tiedoissa olevan toimipaikan mukaan. Jos henkilön toimipaikka vaihtuu, menevät henkilön aiemmat kulkuoikeudet ”Expiring”-tilaan, jossa ne poistuvat 14 päivässä. Henkilöt voivat myös hakea kulkuoikeuksia lisää tarvittaessa, mutta ne vaativat ylimääräisen hyväksynnän.

3.2.2 ActiveCMS dataliikenne

ActiveCMS:ään haetaan ja tuodaan tietoja monesta eri asiakkaan järjestelmästä. Näihin kuuluvat muun muassa erilaiset kulunvalvonta- sekä HR-järjestelmät. Kuvassa 8 näkyvät erilaiset asiakkaan järjestelmät, joista tulee tietoja ActiveCMS:ään ja joihin tietoja myös lähetetään ActiveCMS:stä. Tässä kuvassa myös eritellään kaikki eri ActiveCMS:n osat, joissa tietoja käsitellään, jotka itse lähettävät, vastaanottavat tai hyödyntävät näitä tietoja. Kuvassa nuolet tarkoittavat viestien kulkusuuntaa, osa järjestelmistä tai niiden osista vain vastaanottaa tai lähettää tietoja.



Kuva 8. ActiveCMS-järjestelmän osat, asiakkaan ympäristön järjestelmät sekä niiden tiedonkulku ActiveCMS:n kanssa.

Workday HR on asiakkaan HR-järjestelmä, josta tuodaan ActiveCMS:ään uusia henkilöitä sekä erilaisia muutoksia näiden henkilöiden tietoihin. Equitrac on järjestelmä, jolla hallitaan tunnistautumista vaativaa tulostusjärjestelmää.

Asiakkaan eri toimipisteillä käytössä olevat kulunvalvontajärjestelmät (VISY, LENEL, SIPASS, ESMIKKO ja TIMECON) vastaanottavat kaikki viestejä ActiveCMS:stä. Viesteillä välitetään tietoja henkilöstä sekä hänen kulkuoikeuksiin liittyviä tietoja. Viestit ovat kaikki XML-formaatissa ja näin myös melko helposti luettavissa. Kaikilla järjestelmillä on omat pienet muutokset viestiformaattiin. Tässä esimerkkinä yhden järjestelmän esimerkkiviesti.

```
<record xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" target="Timecon" mes-
sageid="934168">
  <internal_id>3032030253</internal_id>
  <person_number>k123456</person_number>
  <person_id>241138</person_id>
  <employee_number>k123456</employee_number>
  <last_name>Example</last_name>
  <first_name>Evan</first_name>
  <title>Manager, production planning</title>
  <company_number>77282</company_number>
  <company>Example Oyj</company>
  <department_number>533</department_number>
  <department />
  <card_number>3032030253</card_number>
  <card_number2>5861887</card_number2>
  <card_type>16</card_type>
  <email>evan.example@example.com</email>
  <phone>+358(40)5426717</phone>
  <tax_number>100098713687</tax_number>
  <supervisor>235657</supervisor>
  <personnel_group>533</personnel_group>
  <dinner_group />
  <timeplan_group>LIUKUVA SALDO 40</timeplan_group>
  <timeplan_name>LIUKUVA 6-19</timeplan_name>
  <lang>en</lang>
  <cost_center />
  <pin protection_scheme="AES"
transport_encoding="base64">DVvCbfN/vYr9qtuZoFMbTYnTyWl3YXM40t6ahHlpQzo=</pin>
  <valid_from>2017-06-12T00:00:00</valid_from>
  <valid_until>2117-05-19T23:59:59</valid_until>
  <status>Active</status>
  <picture />
  <city>Lappeenranta</city>
  <access_group>Example</access_group>
  <temp_access_group />
  <info />
  <licenseplates />
  <accessLevels>
    <access id="193" from="2017-11-25T00:00:00" to="2117-05-
19T23:59:59">102</access>
    <access id="194" from="2017-11-25T00:00:00" to="2117-05-
19T23:59:59">103</access>
    <access id="195" from="2017-11-25T00:00:00" to="2117-05-
19T23:59:59">104</access>
```

```
  </accessLevels>
</record><
```

Esimerkkikoodi 1. Timecon kulunvalvontajärjestelmään lähettävä viesti henkilön kulkuoikeuksista ja muista tiedoista.

Viestissä näkyy esimerkiksi tiedot henkilöstä, hänen tunnisteestaan, työhön liittyviä tietoja sekä kulkuoikeudet. Viesteistä voidaan tarvittaessa vikatilanteissa tarkistaa, onko henkilölle laitettu oikeat tiedot.

Kaikki viestit asiakkaan eri järjestelmien sekä ActiveCMS-järjestelmän välillä kulkevat asiakkaan Message Broker -viestien välitysjärjestelmä kautta. Sen käytöllä halutaan tilastoida tietoja näistä viesteistä sekä hallita muun muassa viestien uudelleenlähettämistä.

3.2.3 ActiveCMS Monitor

ActiveCMS Monitor on Windows-palvelu, joka valvoo ActiveCMS-palvelimelle sisääntulevia tiedostoja, prosessoi, parsii näitä tiedostoja, lähettää sähköposteja ja pystyy lähettämään tekstiviestejä, sekä muita viestejä ulospäin esimerkiksi asiakkaan erilaisille kulunvalvontajärjestelmille. Monitor pystyy myös lähettämään XML-ja JSON-dataa REST web service -menetelmillä tai esimerkiksi luoda tarvittaessa tiedostoja. Se on asennettuna ActiveCMS-palvelimelle ja sitä suoritetaan siellä. Monitorilla suoritetaan ACR:n yhteydessä monenlaisia tehtäviä. Sillä suoritetaan ajoittain niin sanottuja massalatauksia, joissa järjestelmään lisätään isoja tietokokonaisuuksia. Näin tehdään, kun esimerkiksi asiakkaalla otetaan käyttöön uusi toimipiste ja siihen liittyvät tiedot pitää saada järjestelmään. Monitorilla suoritetaan myös erilaisia ajoitettua tehtäviä, esimerkiksi lokitiedostojen kirjoitusta.

Yksi toinen tärkeä ajoitettu tehtävä ActiveCMS-Monitorille on joka aamu ActiveCMS-palvelimelle asiakkaan HR-järjestelmästä tulevan tiedoston prosessointi. Näissä tiedostoissa on kaikki edellisen päivän aikana muuttunut HR data eli nimet, henkilötunnus, sähköpostiosoite, puhelinnumero, osasto ja niin edelleen. Tällä saadaan oleellisimmat muutokset sekä kaikki uudet henkilöt kirjattua järjestelmään. ActiveCMS Monitor käy

nämä tiedostot läpi rivi riviltä, vertaa niitä ActiveCMS:n tietoihin. Aina kun muutoksia havaitaan, se muuttaa tarvittavat tiedot, ja jokaisen muutoksen kohdalla käydään aiemmin kuvattu uusien tietojen tarkistusketju.

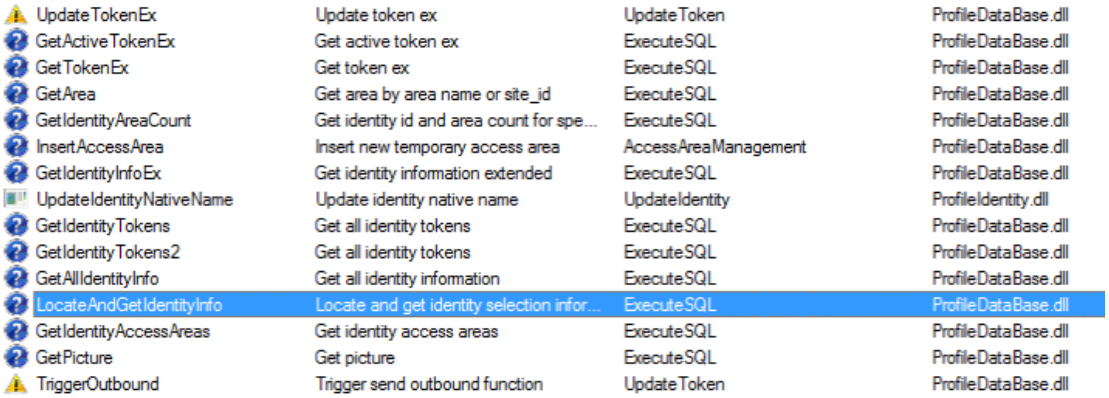
Tiedostossa on jokaisella rivillä ensimmäisenä asiakasorganisaatiossa käytetty henkilöstönumero, jolla jokainen henkilö on yksilöity. Sillä tunnistetaan käyttäjä ja löydetään oikeat tiedot. Jos henkilöä ei löydy, luodaan hänet tätä kautta.

```
k123456$Example$Evan$CallingName$011275-0000$200476$Manager, Application &
Prod. Development$1107$Example Company OyJ$50370924$Application and Product
Development$00000$$9030$TEST$$3$20080915$00000000$US02$HELSINKI 9$Esimerk-
kikatu $00100$Helsinki$US03$TAMPERE 5$Esimerkkitie 101$33100$Tampere$evan.ex-
ample@example.com
```

Esimerkkikoodi 2. Yksi rivi esimerkkidataa asiakkaan järjestelmästä, jota ActiveCMS Monitor prosessoi.

3.2.4 ActiveCMS CPI

ActiveCMS:n CPI (Command Profile Interface) on tapa APM:lle hakea tietoa ActiveCMS:stä. CPI on Aventran kehittämä standardi rajapinta ActiveCMS:n ja APM:n välillä. ActiveCMS:n tarjoamat CPI:t toimivat siis APM:lle eräänlaisina muokattavina rajapintoina, joilla voidaan APM:n kautta hakea, päivittää tai lisätä tietoa ActiveCMS-palvelimelle. Monelle toiminnolla on tehty oma muokattu CPI tätä tarkoitusta varten. Esimerkiksi joka kerta, kun APM hakee henkilöstä tietoa ActiveCMS:stä nimen perusteella, käytetään CPI:tä ”LocateAndGetIdentityInfo” (kuva 9). APM kutsuu tätä CPI:tä ja CPI ottaa annetun henkilön nimen muuttujana sisään ja suorittaa tiedon hakuun tarvittavan SQL-lauseen. Lauseeseen kuuluu esimerkiksi laajoja tarkistuksia sekä datan muokkaamista sopivanlaiseen muotoon. Tämä haettu ja muokattu data annetaan APM:lle, joka sitten voi näyttää käyttäjälle datan haetusta henkilöstä tai käyttää datan itse sen päätöksentekoprosesseihin. Erilaisia CPI:tä ovat esimerkiksi erilaiset tietojen haut, tietojen päivittämiset ja lisäämiset.



UpdateTokenEx	Update token ex	UpdateToken	ProfileDataBase.dll
GetActiveTokenEx	Get active token ex	ExecuteSQL	ProfileDataBase.dll
GetTokenEx	Get token ex	ExecuteSQL	ProfileDataBase.dll
GetArea	Get area by area name or site_id	ExecuteSQL	ProfileDataBase.dll
GetIdentityAreaCount	Get identity id and area count for spe...	ExecuteSQL	ProfileDataBase.dll
InsertAccessArea	Insert new temporary access area	AccessAreaManagement	ProfileDataBase.dll
GetIdentityInfoEx	Get identity information extended	ExecuteSQL	ProfileDataBase.dll
UpdateIdentityNativeName	Update identity native name	UpdateIdentity	ProfileIdentity.dll
GetIdentityTokens	Get all identity tokens	ExecuteSQL	ProfileDataBase.dll
GetIdentityTokens2	Get all identity tokens	ExecuteSQL	ProfileDataBase.dll
GetAllIdentityInfo	Get all identity information	ExecuteSQL	ProfileDataBase.dll
LocateAndGetIdentityInfo	Locate and get identity selection infor...	ExecuteSQL	ProfileDataBase.dll
GetIdentityAccessAreas	Get identity access areas	ExecuteSQL	ProfileDataBase.dll
GetPicture	Get picture	ExecuteSQL	ProfileDataBase.dll
TriggerOutbound	Trigger send outbound function	UpdateToken	ProfileDataBase.dll

Kuva 9. Listassa useampi tuotantokäytössä oleva CPI.

Suurin osa CPI:stä on SQL-lauseiden suorittamista, mutta myös esimerkiksi tunnisteiden tilan muuttamiset sekä erilaiset avainten hallintaan tarvittavat toiminnot suoritetaan oman tyyppisillä CPI:llä.

```
-- Kaikki Contractorit jolla kortti joka on Issued (Waiting for photo)
SELECT ROW_NUMBER() OVER (ORDER BY dealer_site, dealer, emp_type, name) AS
[row], *
FROM (SELECT f.name AS dealer_site,
        '' AS dealer_site2,
        f.id AS dealer_id,
        f.nbr AS dealer_upn,
        f.name AS dealer,
        0 AS emp_count,
        'contractor' AS emp_type,
        CONCAT(c.lastname, ' ', c.firstname) AS name,
        c.id AS id,
        ISNULL(c.phone, '') AS upn,
        c.type AS "type",
        ISNULL(i.unid, '') AS tax_nbr,
        ISNULL(c.assignment, '') AS site1,
        '' AS site2
FROM [card] c
JOIN [state] s ON s.id = c.state
JOIN [identity] i ON i.id = c.identity_id
LEFT JOIN [company] f ON f.id = c.company_id
LEFT JOIN [identity_type] it ON it.id = i.type
WHERE c.type = 17
AND s.name IN ('Issued', 'Production')
) rw
WHERE rw.tax_nbr <> ''
ORDER BY rw.dealer_site, rw.dealer, rw.emp_type, rw.name;
```

Esimerkkikoodi 3. Tämä SQL-lause suoritetaan, kun haetaan asiakasorganisaatiossa toimivia urakoitsijoita, joilla on tunniste ”Issued” -tilassa eli odottamassa sen luovuttamista.

3.2.5 ActiveCMSWS

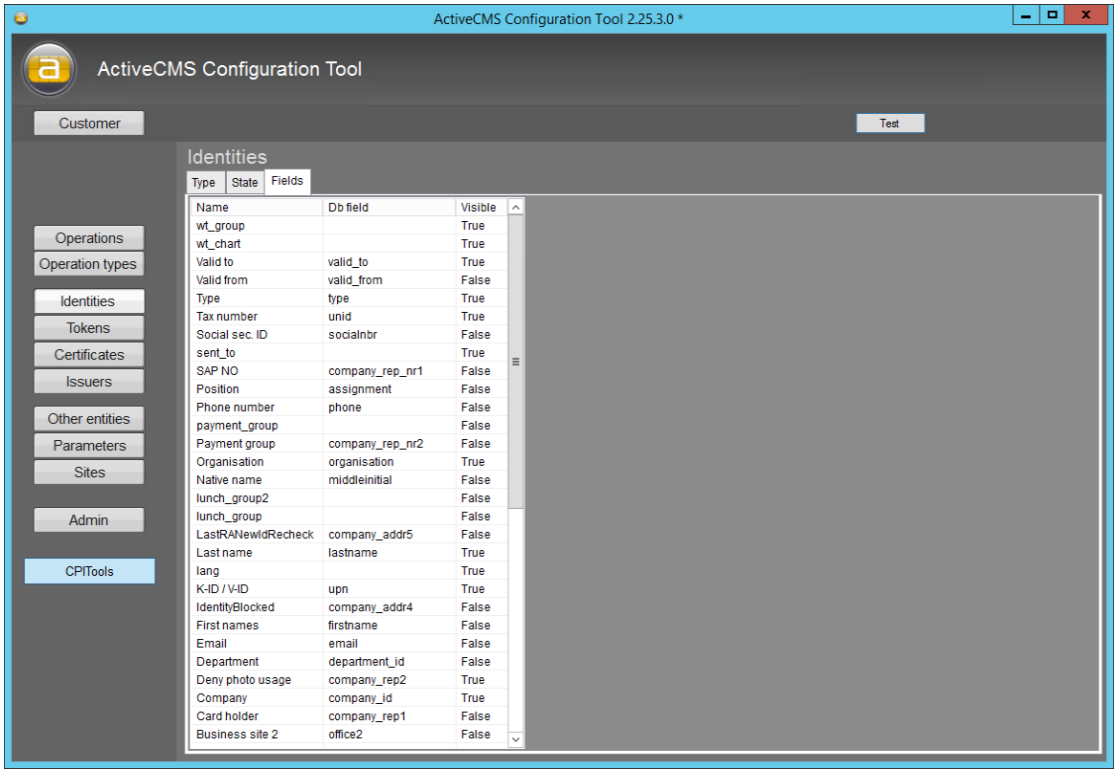
ActiveCMSWS eli ActiveCMS WebService on ActiveCMS-palvelimella pyörivä web-palvelu, jonka kautta APM pystyy kutsumaan sekä käyttämään aiemmin kuvattuja CPI:tä. Niiden avulla APM pystyy hakemaan tietoja ActiveCMS:stä sekä päivittämään siellä olevia tietoja.

3.2.6 ActiveCMS WebAPI

ActiveCMS WebAPI on REST-rajapinta, jolla ActiveCMS voi vastaanottaa tietoja muista ulkoisista järjestelmistä. Näitä järjestelmiä on esimerkiksi Visyn lupaportaali sekä Aventran erillinen Contractor Portal -järjestelmä, joka on rajattu tämän insinöörityön ulkopuolelle.

3.2.7 ActiveCMS Configuration tool

ActiveCMS configuration tool on ActiveCMS-järjestelmän hallintaan suunniteltu työkalu, jolla voidaan helposti muokata ActiveCMS-järjestelmän erilaisia osa-alueita. Sillä voidaan muun muassa muokata, lisätä tai poistaa järjestelmässä käytettäviä korttityyppejä, operaatioita, identiteettityyppejä, varmenteita, eri toimipisteiden pohjapiirustuksia, alueita, alueiden valvojia ja kontakti- sekä vastuuhenkilöitä, alueryhmiä sekä esimerkiksi järjestelmän lähettämien sähköpostien formaattia. Toisin sanoen sillä siis hallitaan ja muokataan järjestelmän työnkulkua. Sen avulla voidaan muuttaa koko järjestelmän toimintalogiikkaa. ActiveCMS configuration tool on hyvin monipuolinen, mutta myös monimutkainen työkalu (kuva 10).



Kuva 10. Tässä näkymässä voidaan muokata identiteettien ominaisuuksien syöttökenttiä sekä niiden ominaisuuksia.

3.3 ActivePerso Manager

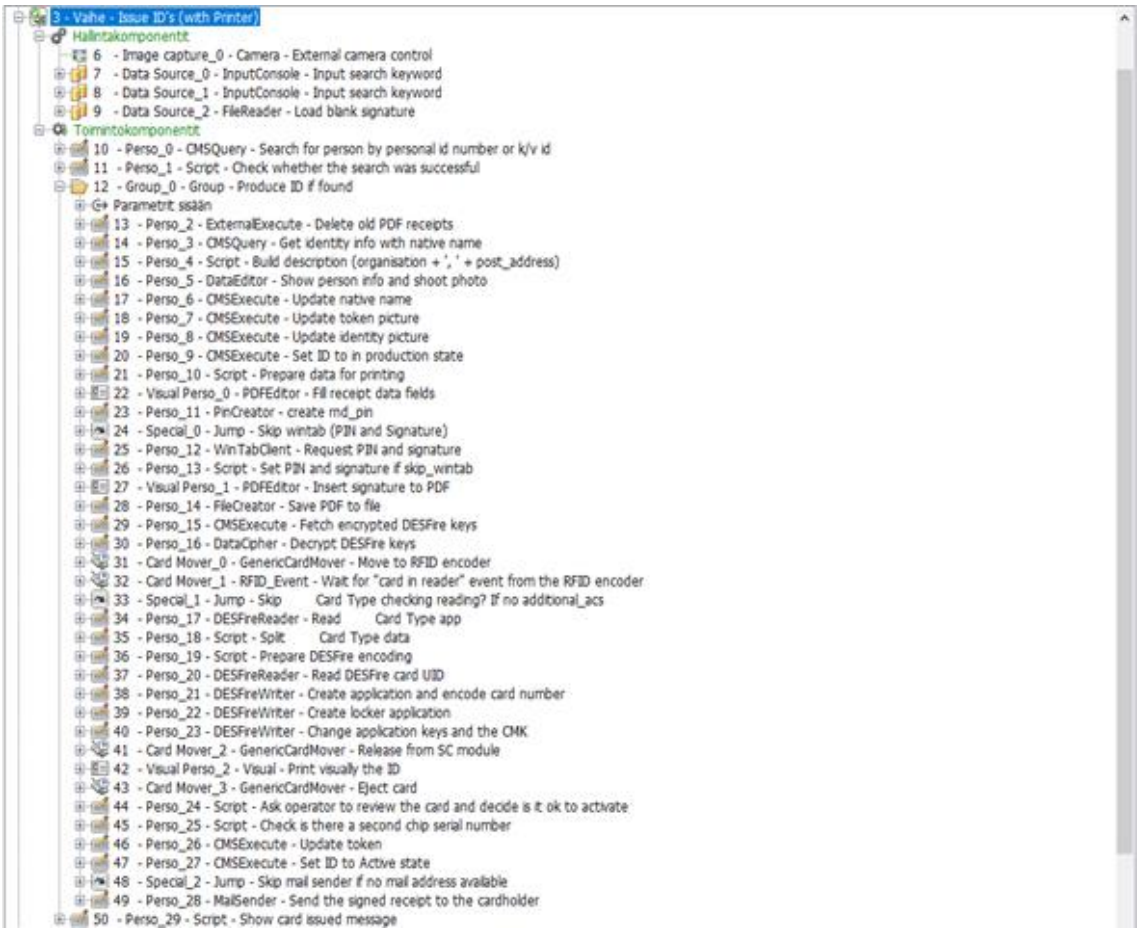
ActivePerso Manager (APM) on Aventran kehittämä ohjelma, jonka konfiguraation päivitys, sen testaaminen ja uuden version asennus sekä testaus ovat projektin varsinaisena aiheena. APM suorittaa asiakasorganisaatiossa lähes kaikkia henkilökorttien ja tunnisteiden personointiin ja hallintaan liittyviä toimintoja. APM:n tärkeimpiä toimintoja asiakasorganisaatiossa ovat esimerkiksi uusien kulkukorttien ja tunnisteiden myöntäminen, korttien tulostaminen, kadonneiden tunnisteiden palauttaminen ja tunnisteiden PIN-koodin vaihtaminen. APM:n yleisimmät käyttäjät ovat vartijoita, lupatoimistojen henkilökuntaa tai esimerkiksi aulahenkilökuntaa. APM suunniteltiin alun perin älykorttien personointiin, mutta sitä on laajennettu tekemään erittäin monia muitakin toimintoja. Tässä hieman esimerkkejä, mihin sitä on eri asiakasorganisaatioissa käytetty:

- henkilökorttien visuaalinen personointi
- hontaktisirun, RFID tunnisteen ja magneettiraidan personointi
- salausavainten generointi

- varmennepyynnöt ja varmenteiden revokointi
- erilaisten lomakkeiden tulostaminen
- datan siirto, muokkaus ja prosessointi tietokantojen ja tiedostojen välillä
- tietojen pyytäminen käyttäjältä, esimerkiksi allekirjoitustabletin avulla
- Active Directoryn kanssa toimiminen, sieltä datan siirto ja sen lukeminen
- valokuvien ottaminen, muokkaaminen ja siirto tietokantoihin
- tunnisteiden aktivointi ja deaktivointi kulunvalvontajärjestelmien kautta
- viranomaisten myöntämien PKI-henkilökorttien itseaktivointi
- erilaisten tietojärjestelmien välisiin tarkistuksiin, esim. viranomaistietojen tarkistuksiin.

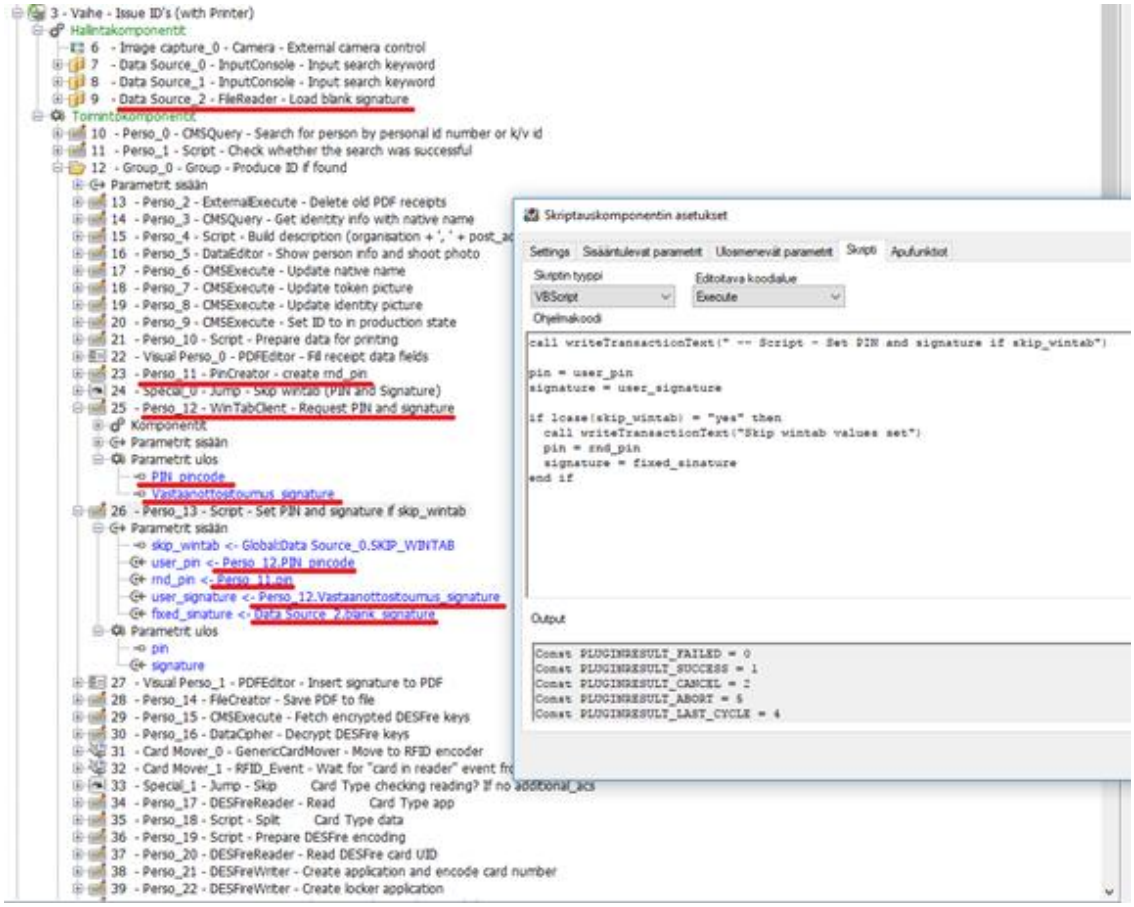
APM suorittaa toimintoja ohjaamalla erilaisia komponentteja tai ”plugineita”, jotka suorittavat erilaisia tarkoin määriteltyjä, mutta hyvin laajasti muokattavia, toimintoja. Komponentteja voidaan muokata APM:n käyttöliittymästä ja niille voidaan määritellä erilaisia parametreja, ehtoja, asetuksia ja sääntöjä. Nämä kaikki komponentit, niiden asetukset, parametrit ja sisäiset skriptit kootaan yhteen kokonaisuuteen, jota kutsutaan tuttavallisemmin APM-”työksi”. Tätä työtä suoritetaan ohjelman kautta. APM-työ on teoriassa selkokuluista XML-formaatissa olevaa dataa. APM-työt voidaan tarvittaessa myös sekä salata, että suojata salasanalla. APM-töiden muokkaamiseen ja lukemiseen on yleisesti helpompaa ja kätevämpää APM:ää käyttäen. Esimerkiksi uudempi APM-työ on kehitysvaiheessa yli 42 000 riviä pitkä XML-tiedostona, joten sen muokkaaminen tekstitiedostona vaatii erityistä tarkkuutta ja osaamista. APM:n kautta työtä muokatessa käytetään yleisesti hyväksi helppoa, sitä varten luotua, visuaalista käyttöliittymää.

APM:ssä suoritettavat komponentit lajitellaan ohjelman sisällä kahteen eri kategoriaan, hallinta- ja toimintokomponentteihin. Hallintakomponenteilla nimensä mukaisesti hallitaan yleensä käyttäjältä tai ulkopuolelta tulevaan dataan tarvittavia yhteyksiä, esimerkiksi kameraan, tietokantaan tai kortinlukijaan. Toimintokomponenteille taas käytetään näitä yhteyksiä ja yhdistettyjä laitteita. Kaikki nämä toiminnot voivat olla erittäin monipuolisia, esimerkiksi datan hakeminen tietokannasta, kameralla kuvan ottaminen, datan manipulointi erilaisilla skripteillä tai vaikka kortin liikuttaminen korttitulostimen sisällä tiettyyn haluttuun paikkaan. Komponenteille voidaan asettaa erilaisia asetuksia, kuten toimintaa virhetilanteessa tai suorituskertojen lukumäärän. Komponentteja voidaan myös lajitella ryhmiin kokonaisuuksien hahmottamisen ja muokattavuuden helpottamiseksi.



Kuva 11. Yhden askeleen komponentit asiakkaan poistuvasta APM-työstä.

Kuvassa näkyvät tarvittavat askeleet uuden henkilökortin myöntämiselle ja tulostamiselle vanhemmalla, nyt jo poistuvalla konfiguraatiolla. Tämä vaihe alkaa asiakkaan henkilönumeron, henkilöstönumeron tai veronumeron antamisella. Sen perusteella etsitään henkilön tiedot. Jos henkilölle tietojen perusteella löytyy sopiva henkilökortti tulostettavasta tilasta, voidaan edetä tulostamaan. Uuden kortin luomiseen tarvittavat askeleet on lajiteltu ryhmään ”Produce ID if found”, jonka alta ne kaikki saadaan näkyviin. Askeleissa edetään oletuksena ylhäältä alas, mutta tästäkin voidaan poiketa niin haluttaessa. APM:ssä voidaan ajaa työn sisällä erilaisia skriptejä eli komentosarjoja. Niillä voidaan helposti automatisoida monia erilaisia tehtäviä, esimerkiksi muokata ja siirtää dataa eri komponenttien välillä tai muokata työn sisäistä logiikkaa. APM:ssä ajettavat skriptit on lähes poikkeuksetta kirjoitettu VBScriptillä.



Kuva 12. APM-työssä oleva skripti ja siihen käytettävät parametrit.

Tässä näytetään yksinkertainen työssä käytettävä skripti, jossa jätetään allekirjoituspääte (Wintab), jos sellaiseen vaativa arvo on asetettu. Tämä voidaan asettaa käyttöön esimerkiksi, pisteellä ei ole allekirjoitus tablettia käytössä. Kun tämä osa jätetään välistä, haetaan tälle komponentille ”Parametrit sisään”-kohdassa aiemmin luodut satunnaisesti generoitu PIN(Perso_11) ja tyhjä allekirjoitusdata (Data_source_2). Sisään tulevien parametrien perässä näkyy nuolen jälkeen tarkemmin sen askeleen nimi, josta parametrien arvot haetaan. Eli yhden askeleen ulos tulevat parametrit ovat yleensä toisen askeleen sisään tulevia parametrejä. Nämä parametrit ovat siis näin linkitettyjä. Jos allekirjoitusta ei jätetä välistä, siirretään edellisestä askeleesta (Perso_12) saadut asiakkaalta kysytty allekirjoitus ja PIN eteenpäin.

3.4 ACR Workstation

ACR Workstation on uuden APM-pisteen työnimi. Siinä uudistetaan tapa, jolla APM toimii sekä tapa jolla APM työ on konfiguroitu. Uudella APM-työllä haluttiin tehdä sen käyttämisestä yksikertaisempaa, parantaa sen vikasietoisuutta, tuoda lisää toivottuja ominaisuuksia, helpottaa ylläpitämistä sekä helpottaa vianselvitystä ja tukea erilaisia kokoonpanoja.

3.4.1 Olennaisimmat APM:n versiouudistukset

APM:n versiopäivityksessä siirryttiin käyttämään kaikilla asiakasorganisaation toimipisteiden APM-pisteillä uutta 3.3.0-versiota. Aiemmin APM-pisteillä on ollut 3.1.7 – 3.2.2 -versiota. Näiden asennuksien yksi päätarkoituksista oli juuri asennettujen pisteiden yhtenäinen lopputulos, samat APM:n versiot sekä samat APM-työn versiot.

APM:n oleellisimmat versiouudistukset 3.3.0 versiossa olivat:

- substepit
- resultAction
- pluginien ryhmittäminen toisen ryhmän sisään
- Desfire tuoteperheen tunnisteiden koodauksen nopeuttaminen.

Substepit tarkoittavat eri toimintojen (steppien) kutsumista toisten toimintojen sisältä. Tällä mahdollistetaan tiettyjen toimintojen keskittäminen samaan kohtaan, eikä monessa kohdassa tarvittavaa toiminnallisuutta tarvitse kopioida vaan sitä voidaan käyttää kaikkialta.

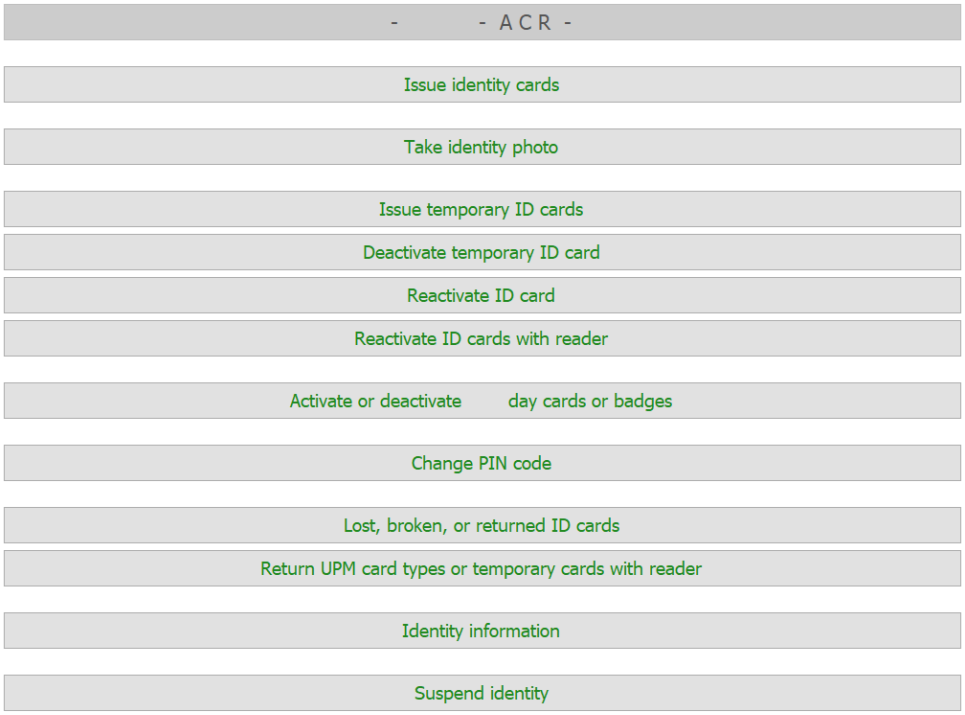
ResultAction on APM:n uusi toiminnallisuus, jolla voidaan APM:n työtä ohjata eri tavalla riippuen edellisen toiminnon lopputuloksesta. Esimerkiksi jos tunnisteen koodaaminen keskeytyy virheeseen, voidaan siitä palata takaisin edelliseen kohtaan tai yrittää helposti uudelleen. Aiemmin tällainen virhetilanne aiheutti koko APM-työn pysähtymisen.

Pluginien ryhmittäminen sisäkkäin mahdollistaa helpon tavan valita, suoritetaanko ryhmän sisäisen ryhmän alla olevat komponentit vai ei. Aiemmin ryhmien sisällä ei pystynyt tekemään ryhmiä jolloin tämä ei ollut mahdollista. Tämä helpottaa APM-töiden konfigurointia ja lukemista.

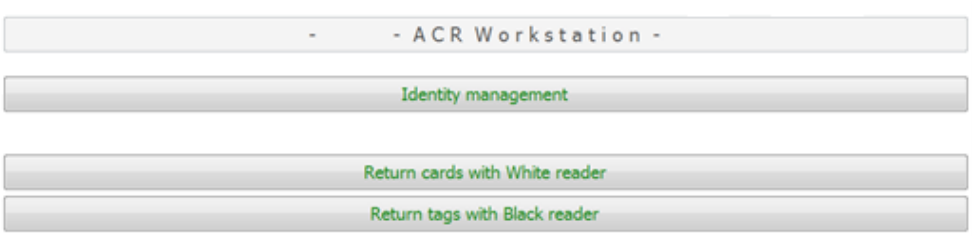
Myös Desfire-tuoteperheen tunnisteiden koodaamiseen tehtiin parannuksia, koodauskomponentti toimii nyt nopeammin ja varmemmin.

3.4.2 APM-työn parannukset

Aikaisemmassa APM-työssä virheistä ei juurikaan pystynyt palautumaan, tiettyjä toimintoja ei voinut tehdä APM:n kautta ollenkaan ja sitä oli myös vaikeampi käyttää. Vanha APM-työ toimi ylhäältä alas yksi toiminto kerrallaan. Sen alkuvalikossa oli kaikki saatavilla olevat toiminnot heti valittavissa (kuva 13). Tämä selkeästi vaikeutti pisteen toimintaa. Asiakas tai häntä palveleva henkilö ei usein tiedä, minkälainen kortti asiakkaalle kuuluu ja toiminnoissa näkyvät tiedot olivat hyvin rajalliset. Jos haluttua toimintoa ei voinut tehdä henkilölle, piti toiminto aloittaa uudelleen sekä hakea henkilö uudelleen.

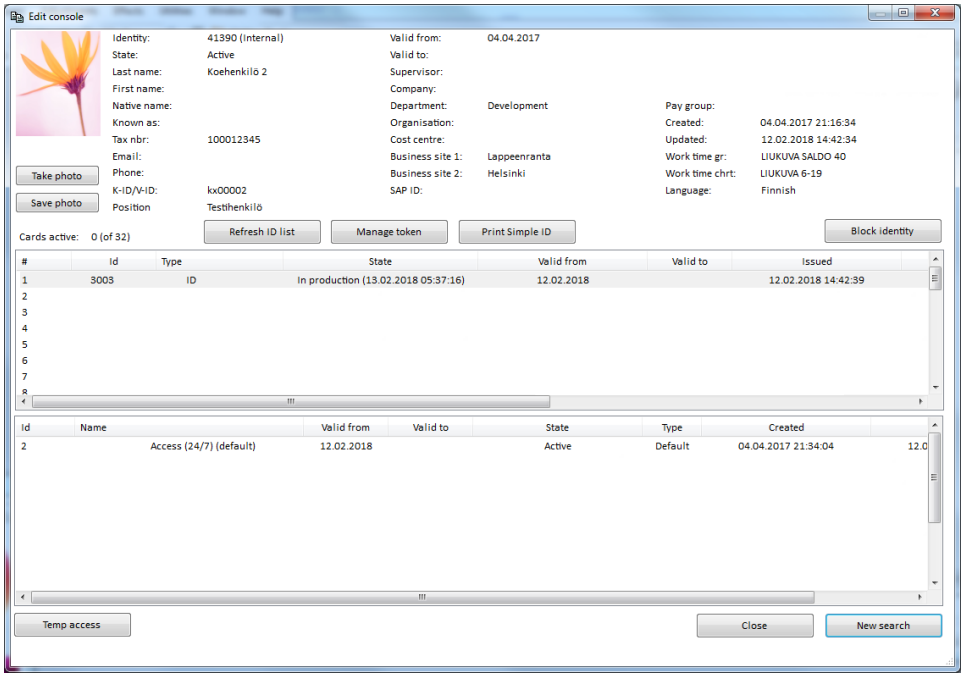


Kuva 13. Vanhan APM-työn aloitusikkuna.



Kuva 14. Uuden APM-työn aloitusikkuna.

Uudessa APM-työssä on aloitusikkunaa yksinkertaistettu (kuva 14) ja aluksi käytettäviä toimintoja on rajoitettu paljon. APM:n käyttö on haluttu tehdä mahdollisimman yksinkertaiseksi ja suoraviivaiseksi. Lähes kaikki uuden APM-työn toiminnot alkavat ”Identity management” -napista. Sillä haetaan pisteen asiakkaana olevan henkilön tiedot, siitä voidaan hakea henkilöitä heidän nimellä, veronumerolla, jo olemassa olevalla tunnisteella sekä asiakasyrityksessä henkilön yksilöivällä id:llä. Tällä halutaan helpottaa pisteen käyttäjän työtä, hänen ei pidä arvailla, mikä kortti tai toiminto henkilölle pitää tai edes voi tehdä. Pisteen käyttäjä voi vain pyytää henkilön nimeä tai muuta yksilöivää tietoa, ja hän saa näkyviin henkilön tiedot (kuva 15), josta voi helpommin päätellä tarvittavat toimenpiteet.

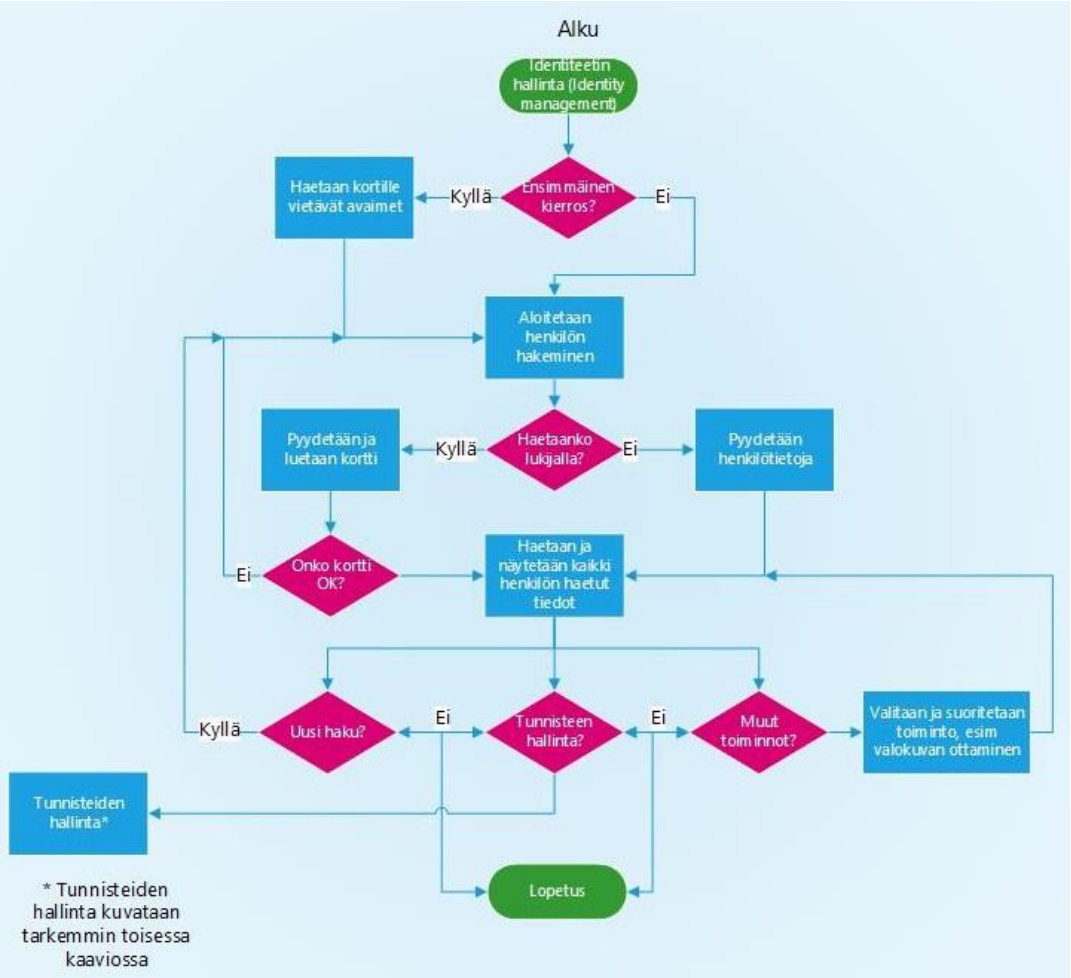


Kuva 15. Testihenkilön tiedot, lista korteista sekä kulkuoikeuksista.

Uusi APM-työ muokkaa käyttäjälle näkyviä nappeja ja näkymiä sen mukaan, mikä toimipiste on kyseessä, mitä ulkoisia laitteita pisteellä on käytössä ja minkälaisia toimintoja asiakkaalle tai hänen tunnisteelleen voi tehdä. Esimerkiksi, jos käyttäjällä on järjestelmään merkitty sähköposti, näkyy henkilön kuvan alapuolella ”Send photo” -nappi, jolla voidaan lähettää käyttäjän sähköpostiosoitteeseen tämä kuva. Jos käyttäjällä taas ei ole sähköpostiosoitetta näkyy ”Send photo” -napin tilalla ”Save photo”. Sillä kuva voidaan tallentaa paikallisesti ja esimerkiksi siirtää USB-tikulle. Myös esimerkiksi toimipisteillä, missä ei ole korttitulostimia ei voida ollenkaan kuvallisia ID-kortteja tulostaa ja se on ohjelmallisesti estetty.

3.4.3 Uuden APM-työn toimintaperiaate

Uudessa APM-työssä poiketaan hieman periaatteesta, jossa APM-töiden toiminnot lähes poikkeuksetta suoritetaan ylhäältä alas. Eli uudessa työssä palataan useasti takaisin eri pisteisiin työtä, tällä on tarkoituksena nopeuttaa APM:n käyttöä huomattavasti. Esimerkiksi jos henkilö on väärä, palataan hakemaan henkilöä, tai jos valitulle kortille ei pystynytkään tekemään haluttua toimintoa, voidaan palata takaisin ja valita oikea kortti eikä APM-työtä joudu käynnistämään uudelleen. Tällä yritetään vähentää APM-työn uudelleenkäynnistämistä sekä turhia yhteyksien luomista ja sulkemista. Tämä uusi toimintaperiaate (kuva 16) mahdollistaa erilaisten toimintojen helpomman käytön sekä nopeuttaa työn käyttöä huomattavasti, mutta myös monimutkaistaa työn konfigurointi sekä lisää mahdollisia ongelmia konfiguroinnissa.



Kuva 16. Uuden APM-työn toimintaperiaate vuokaaviossa

Vuokaaviosta huomataan, että siinä on tietojen tarkistuksia ja lähes jokaisesta pisteestä voidaan palata askel taaksepäin aloittamatta kokonaan alusta. Tämä nopeuttaa ja helpottaa pisteen toimintaa huomattavasti.

3.4.4 Avainten hallinta APM:ssä

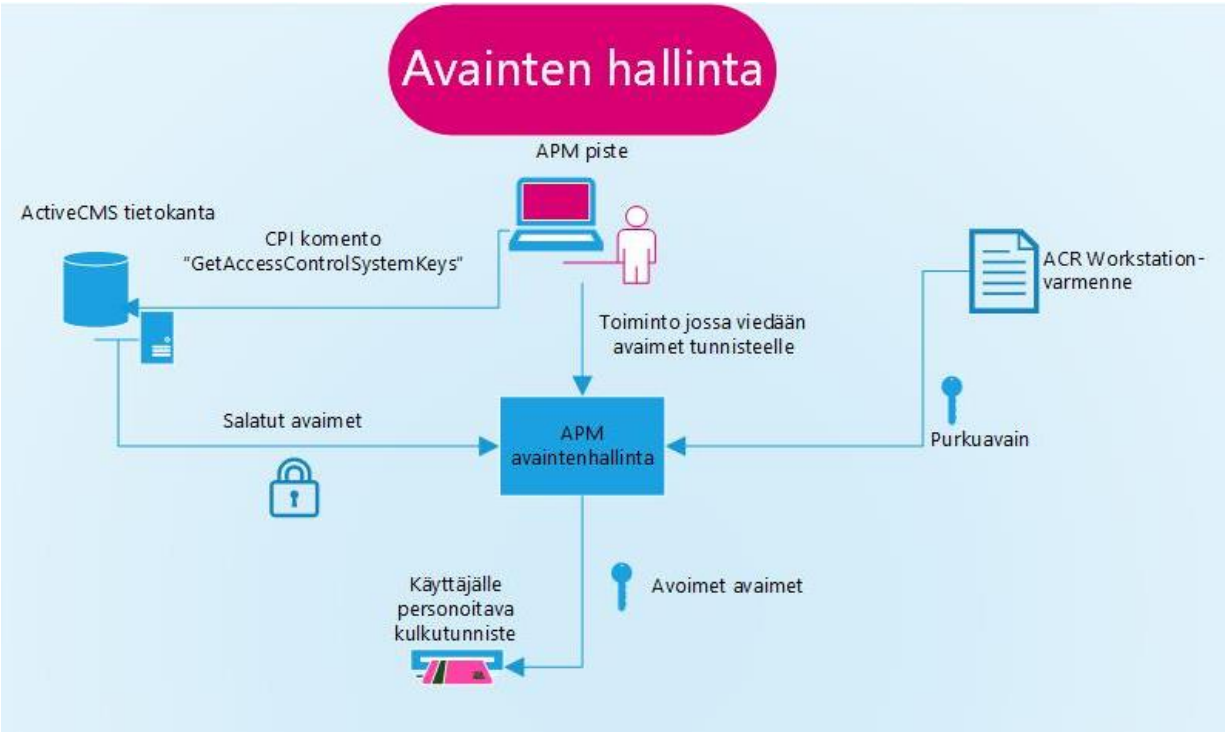
APM-työssä eräs oleellinen osa sen tarjoamaa turvallisuutta on avainten hallinta ja salauksen toteutus. APM:n avulla luodaan tunnisteille niissä käytettävä tiedostorakenne sekä viedään tunnisteille niiden avaimet. Näillä avaimilla pystytään helposti ja turvallisesti todentamaan henkilöllisyys. Avainten hallinta APM:n kautta suoritetaan seuraavalla tavalla:

Koko järjestelmän pystytyksen yhteydessä vietiin ActiveCMS-tietokantaan kaikille tunnisteille vietävät avaimet. Avaimet pidetään tietokannassa salattuna. Näitä avaimia on

kolme sarjaa: A, B ja C. Jos ensimmäinen sarja avaimia paljastuu, voidaan siirtyä käyttämään seuraavaa sarjaa uusimatta tunnisteita.

Avainten vienti tunnisteille lähtee APM-työn käynnistämisestä. Sen yhteydessä APM:n avulla tarkistetaan, löytyykö APM:ää suorittavalla työpisteellä ”ACR Workstation” -varmenne. Tällä varmenteella pystytään avaamaan tunnisteille vietävät avaimet. Nämä avaimet ovat salattuna ActiveCMS-tietokannassa, ja ne saadaan auki vain tässä varmenteessa olevalla yksityisellä avaimella. Kun varmenne on tarkistettu, haetaan CPI:n avulla ActiveCMS-tietokannasta salatut avaimet. Nämä avaimet sitten avataan varmenteen avulla ja lähdetään suorittamaan kaikkia APM:n toimintoja normaalisti. Tunnisteiden myöntämisessä käytetään näitä avaimia ja ne viedään APM:n avulla tunnisteille, josta niitä voidaan lukea vain tietyillä lukuavaimilla, jotka on järjestelmän lukijoille ”opetettu”.

Kuvassa 17 havainnollistetaan tapa, jolla kulunvalvontajärjestelmän avaimia käytetään järjestelmässä.



Kuva 17. Avainten hallinta APM-työssä

4 Projektin toteutus

Projektin käytännön osuutena oli uuden ohjelmistoversion sekä sen konfiguraation eli työn testaaminen, dokumentaation tekeminen ja lopullinen tuotantoon asennus. Asennukset suoritettiin asiakkaan tiloissa, ja asennuksien jälkeen asennettu ohjelmisto siirtyi normaaliin tuotantokäyttöön.

4.1 Testaaminen

APM:n uuden ohjelmistoversion, sekä uudemman työn testaaminen oli projektin yksi tärkeimmistä osa-alueista. APM-työ oli erittäin laaja, monimutkainen ja erilainen kuin vanhempi työ. APM-työn monimutkaisuus toi esiin monia ongelmia, sekä uuden ohjelmistoversion tuomat muutokset lisäsivät virheitä ja vaikeuttivat joidenkin virheiden korjaamista. Projektin testit suoritettiin testaamista varten tehdyssä testiympäristössä, joka vastasi teknisesti tuotantoympäristöä. Vain tietokannat ovat erilliset.

4.1.1 Testiympäristö

Testiympäristö koostuu seuraavista osista:

- kannettavasta tietokoneesta
- tietokantapalvelimesta
- IIS-palvelimesta
- korttitulostimesta
- korttilukijoista
- allekirjoitustabletista
- VPN tunnelista asiakkaan verkkoon.

Testiympäristö on perustettu tuotannon rinnalle toimimaan erillisellä palvelimella. Testiympäristön laitteistolla voidaan siis myös tarvittaessa yhdistää tuotannon puolelle ja tehdä sinne muutoksia tai korttituotantoa.

Asiakkaan tarjoamasta kannettavasta tietokoneesta on VPN-tunnelin kautta mahdollisuus yhdistää asiakkaan verkkoon. Asiakkaan APM-työtä ei pystytä käyttämään ilman VPN-yhteyttä ja pääsyä asiakkaan verkossa toimiviin palvelimiin. VPN-tunnelin käyttö

sekä kannettavalle tietokoneelle kirjautuminen onnistuu vain henkilökohtaisilla käyttäjätunnuksilla sekä salasanoilla. Kannettavan tietokoneen kovalevy on myös kryptattu ja erillisellä salasanalla avattava.

IIS-palvelin ja tietokantapalvelin on käytännössä sama, ne toimivat fyysisesti samalla palvelimella. Palvelin on asiakkaan toimittama ja lähes identtisesti konfiguroitu kuin tuotannon palvelin. Palvelimelle on pääsy rajoitettu vain asiakkaan verkosta, ja siihen vaaditaan erilliset palvelimen käyttöön tarkoitetut käyttäjätunnukset ja käyttöoikeudet.

Korttitulostin, kortinlukijat sekä allekirjoituspääte ovat Aventran säilyttämiä laitteita, jotka toimivat samalla varalaitteina asiakkaalle. Korttitulostimena on Fargo HDP5000, allekirjoituspääte on Elcom Secure Sign II ja kortinlukijana on ACR 122.

4.1.2 Käytännön testaaminen

Käytännön testaaminen oli yksinkertaisesti kaikkien toimintojen käyttämistä, sekä oikein että kaikilla mahdollisilla tavoilla väärin. Testaamista varten oli luotu jokaista korttityyppiä varten omat testikäyttäjät. Jokaisella korttityypillä sekä asiakkaan toimipisteellä on erilaisia toimintoja käytettävissä. Näistä syistä on kaikki mahdolliset yhdistelmät kokeiltava. Kaikista testattavista toiminnoista, toimipisteistä, korttityypeistä ja niiden yhdistelmistä on tehty omat kohtansa testauspöytäkirjaan (kuva 18). Siihen on lisätty myös useampia tapoja käyttää ohjelmaa väärin.

Identity management					
	Function	**Test case**	**Data**	**Expected result**	**Result**
	Search with keyword:				
		k/v id	"kx00001"	Show identity	ok
		empty		Return to search	ok
		last name		Show identity	ok
		multiresult search	"koe"	Show select identity	ok
		too long data	larger than 50	Not possible, return to search	ok
		sql injection	Select/Insert **ONLY IN TEST**	Not possible, return to search	ok
		Non existing search value	"xxxxxxxxxx"	Return to search	ok
		tax number		Show identity	ok
		Esc			ok
		Enter			ok
		Enter (after enterin e.g. kx00001		Should show identity kx00001	ok
		Multi result search -> single search	"koe", "kx00003"	Should show identity kx00003	ok
		Search with special characters	"-- ^' ¨'1230+942987´´ ´98£@£@€"		ok
		Search with empty field (space)			ok
		Search with hyphen '			ok

Kuva 18. Pieni osa testauspöytäkirjaa.

Tästä kuvasta näkee, miten esimerkiksi henkilön hakemista on testattu, minkälaista dataa käytetään testiin, minkälaista käyttäytymistä odotetaan ohjelmalta ja onko testi onnistunut. Testipöytäkirjaan on myös merkitty, onko jokin aikaisemmin toimimaton osa tai bugi korjattu, miten korjaus on tehty ja mahdollisia muita kommentteja.

4.2 Dokumentointi

Toinen tärkeä osa projektissa oli testaukseen, koulutukseen, asennukseen liittyvän dokumentaation kirjoittaminen. Projektista on tarkoituksena saada hyödyllistä dokumentaatiota sekä asiakkaalle sekä Aventralle itselleen. Dokumentaation tavoitteena on avustaa jatkossa testauksessa, uusissa asennuksissa, vianselvityksessä sekä uusien käyttäjien kouluttamisessa.

4.2.1 Testauspöytäkirja

Aiemmassa osiossa olevasta kuvasta (kuva 18) näkee hyvin, mitä tietoja testauspöytäkirjassa on. Testauspöytäkirjasta selviää kaikki mahdolliset testatut ja testattavat korttityypit, mahdolliset toimipisteet ja näiden kaikkien yhdistelmien tarjoamat mahdollisuudet sekä näiden testauksien tulokset, korjaukset, mahdolliset kommentit testausta tai korjausta varten.

Testauspöytäkirjaa tullaan käyttämään jatkossa uusien versioiden testaamisessa sekä asennettavien pisteiden testaamiseen.

4.2.2 Koulutusmateriaali

Projektin varsinaisen käytännön asennusten yhteydessä pidettiin myös koulutus ohjelman tuleville käyttäjille. Tätä koulutusta varten tarvittiin koulutusmateriaali, jonka kirjoittaminen oli osa projektin työtä. Koulutusmateriaaliksi tuli noin 50-sivuinen Powerpoint-esitelmä. Sama esitelmä tehtiin suomeksi ja englanniksi. Esitelmässä käydään läpi kaikki ohjelman toiminnot, uusi toimintalogiikka, mahdolliset korttityypit, kaikkien pisteeseen kuuluvien laitteiden toiminta sekä mahdollisia virhetilanteita ja niihin toimintaohjeita. Ensimmäisen asennuksen yhteydessä esitelmä käytiin läpi 5 henkilön ryhmälle samalla esittäen ohjelman sekä laitteiden toimintaa.

4.2.3 Asennussuunnitelma

Asennussuunnitelma on dokumentti, jossa kuvataan kokonaan uuden pisteen asennukseen ja vanhaan pisteen päivittämiseen vaadittavat toimenpiteet. Asennusdokumentin on tarkoitus toimia ohjeena jatkossa asennettavilla tai päivitettävillä pisteillä. Siinä esitellään kaikki tarvittavat tiedostot, kansiorakenne sekä asennettavat ohjelmistot ja ajurit. Dokumentissa käydään myös läpi kaikki asennuksessa tehtävät toimenpiteet sekä mahdollisten ongelmien korjaamiset.

4.2.4 Järjestelmäkuva

Järjestelmäkuva on dokumentti, jossa kuvataan Aventran asiakkaalle tarjoama järjestelmä ja kaikki sen osat mahdollisimman tarkasti. Järjestelmäkuvan on tarkoitus toimia pohjana dokumentaatiolle, jolla voidaan mahdollisesti opettaa uusille henkilöille järjestelmän toimintaa tai muuten ottaa selvää järjestelmän toiminnasta. Yksi dokumentoinnin aikana tehty järjestelmäkuva on osana insinöörityötä osassa 3.

4.3 Asennus

Projektin käytännön osuutena ollut varsinainen asennus tehtiin 19.2.2018 asiakkaan toimipisteellä. Tällä toimipisteellä oli käytössä vanha APM versio kahdella työasemalla. Toinen työasema oli toimipisteen portilla, jota käyttivät siellä toimivat vartijat. Tällä pisteellä APM:ää käytettiin enimmäkseen myöntämään tarvittavia kuvattomia kulkutunnisteita sekä avustamaan vikatilanteissa. Toinen toiminnassa ollut työasema oli toimistorakennuksessa. Tällä APM:llä suoritettiin tulostettavien kulkutunnisteiden tulostusta ja myöntämistä. Tämän lisäksi suoritettiin asennus myös kolmannelle, uudelle työasemalle. Tämä uusi työasema oli myös toimipisteen portilla, jossa oli jo asennuksen alussa toiminnassa ollut vanha APM-piste.

Näillä uusilla pisteillä oli jatkossa tarkoitus tehdä samoja toimintoja kuin ennen, mutta erityisen tärkeä uudistus portilla käytettävillä pisteillä oli henkilöiden tunnistaminen kulkutunnisteen avulla. Toimistolla oleva piste on ns. täysi piste, eli siinä on kaikki oheislaitteet (kamera, allekirjoitustabletti, korttitulostin, kortinlukijat) ja toiminnot käytössä. Molemmat portilla olevat pisteet ovat ns. kevyitä pisteitä, eikä niissä ole ollenkaan kuvauslaitteita eikä korttitulostinta.

Uusi APM-ohjelmistoversio sekä APM-työ tuli asentaa, konfiguroida ja todeta toimivaksi näille kolmelle eri työasemalle samassa toimipisteessä. Asennusten yhteydessä pidettiin myös koulutus ohjelmaa käyttäville henkilöille. Koulutuksessa käytiin läpi kaikki pisteen toiminnot, pisteeseen kuuluvien laitteiden käyttö, yleisimpiä virhetilanteita ja muuta yleistä tietoa. Käytännön asennus suoritettiin kahden henkilön työparina. Asennuksissa olevilla työasemilla oli käytössä Windows 7 -käyttöjärjestelmä. Taulukossa 1 kuvataan projektin aikana asennettujen APM-pisteiden tietoja.

Taulukko 1. Asennetut APM-pisteet

Pisteen nimi	**Pisteen sijainti**	**Pisteen kokoonpano**	**Pisteen käyttötarkoitus**
"_OFFICE"	Toimistorakennus	Täysi piste.	Kaikkien toimipisteellä käytettävien tunnisteiden myöntäminen ja henkilöiden kuvaaminen.
"_SEC_GATE"	Pääportti	Kevyt piste.	Henkilöiden tunnistaminen tunnisteiden avulla sekä tiettyjen kuvattomien tunnisteiden myöntäminen.
"_SEC_GATE2"	Pääportti	Kevyt piste.	Henkilöiden tunnistaminen tunnisteiden avulla sekä tiettyjen kuvattomien tunnisteiden myöntäminen

Asennusprosessi aloitettiin toimiston täyden pisteen päivityksellä. Ensimmäinen toimenpide kaikissa asennuksissa on kaiken vanhempien tiedostojen, APM-työn, asiakaskansion ja ohjelmien varmuuskopiointi. Näin voidaan palata tarvittaessa takaisin varmasti toimivaan vanhaan APM-työhön ja versioon. Tiedostot varmuuskopioitiin paikallisesti sekä myös USB-tikuille. Varmuuskopioinnin jälkeen tehtiin vanhalle APM:lle oma pikakuvake. Vanha APM-työ konfiguroitiin käynnistymään uuden APM-ohjelmistoversion kanssa käyttämällä pikakuvakeparametreja. Eli ohjelmalle tehtiin uusi pikakuvake, jonka ”target” -kohtaan, jossa määritellään avattavan ohjelman polku, lisättiin load -käsky. Tällä saataisiin vanha APM-työ ajettua vain tätä pikakuvaketta käytettäessä, mutta muulloin käytettäisiin uutta versiota. Näin voi ohjelman operaattori halutessaan palata takaisin varmasti toimivaan versioon.

Asennusta jatkettiin tuomalla uusi APM-versio ensimmäiselle työasemalle. Uuden version asennustiedostot kopioitiin vanhan version tiedostojen päälle. Näin korvattiin kaikki vanhat tiedostot ja tuotiin muutamia uusia tiedostoja. Jatkossa tämä asennuksen osa suoritetaan oikeaoppisella asennuspaketilla, joka tekisi kaiken tämän automaattisesti. Ensimmäiseen asennukseen tätä ei kuitenkaan vielä saatu valmiiksi.

Uusi APM-työ vaatii myös toimiakseen asiakaskansioon hieman uusia tiedostoja. Ohjelman asiakaskansioissa on yleensä asiakkaasta riippuen erilaisia taustoja ja logoja tulostuksia varten, asetustiedostoja, testikonfiguraatioita ja esimerkiksi lokitiedostoja. Uuden APM-työn mukana tänne oli tarpeen tuoda erillinen ”settings” -kansio, johon kaikki asetukset tulee laittaa. Toinen muutos oli myös ”pdf” -kansio, mihin siirrettiin kaikki .pdf-tiedostot, esimerkiksi jokaisen uuden tunnisteen saavan henkilön allekirjoitettava vastaanottositoumus. Nämä uudet tiedostot sekä tarvittava kansiorakenne kopioitiin vanhan asiakaskansion päälle. Näistä uusista tiedostoista ”alias”-tiedosto piti yksilöidä jokaiselle pisteelle erikseen. Aiemmin ”alias”-tiedostoa on käytetty vain toimipisteen nimen asettamiseen, nyt uudessa alias-tiedostossa määritellään paljon enemmän asetuksia. Tämä ”alias”-tiedosto on ”.apa”-tiedosto, jossa xml-formaatilla listataan pisteelle ominaisia asetuksia. Näillä asetuksilla vaikutetaan pisteen toimintaan sekä pisteellä käytettävissä oleviin ominaisuuksiin. Esimerkiksi jos pisteellä ei ole korttitulostinta kytkettynä, ei pisteellä ole käytössä ”Issue”-toiminto tulostettavien korttien yhteydessä.

Alias-tiedostossa valitaan seuraavat tiedot:

Taulukko 2. Alias-tiedoston sisältämät asetukset

Asetuksen nimi	**Asetuksen sisältö**	**Esimerkki asetus**
"apm_location"	Tämä asetu kertoo APM-pisteen sijainnin vanhalla formaatilla	”1. HELSINKI_1”
"apm_location_new"	Tämä alias kertoo APM-pisteen sijainnin uudella formaatilla	”HELSINKI_1”
"prod_file_prefix"	Tätä aliasta käytetään APM-piteen tuotannossa Aventran tiloissa.	”/Test_”
"printer_connected"	Tämä asetus kertoo, käytetäänkö pisteessä korttitulostinta	”YES/NO”
"camera_connected"	Tämä asetus kertoo, käytetäänkö pisteessä kameraa.	”YES/NO”

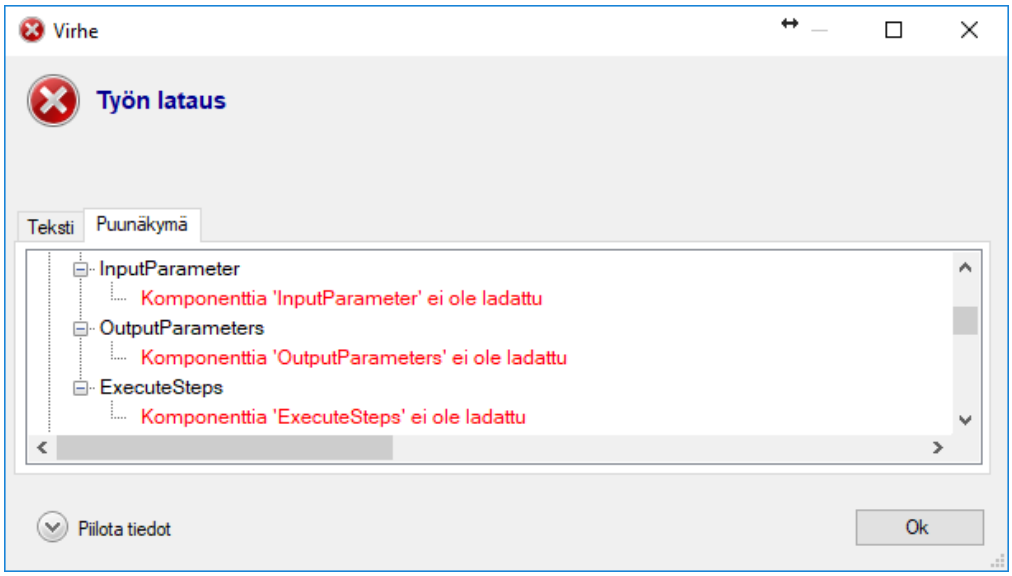
”ask_pin_visible”	Tämä asetus kertoo, onko PIN:n kysely näkyvillä.	”YES/NO”
”ask_pin_default”	Tämä asetus kertoo, onko PIN:n kysely oletuksena päällä.	”YES/NO”
”pdf_lang_default”	Tämä asetus kertoo allekirjoitettavan vastaanottositoumuksen oletuskielen.	”FI/SE/UK”
”default_card_type”	Tämä asetus kertoo oletuksena käytettävän korttityypin.	”Visitor ID”
”print_taxnbr_default”	Tämä asetus kertoo, tulostetaanko veronumero oletuksena.	”YES/NO”
”request_signature”	Tämä asetus kertoo, kysytäänkö allekirjoitusta.	”YES/NO”
”testing_frontend”	Tämä asetus kertoonäytettäänkö TESTING varoitus	”YES/NO”
”apm_exec_env”	Tämä asetus kertoo ympäristön, jossa ohjelma suoritetaan.	”Production/Testing”
”testing_email”	Tämä asetus kertoo testisähköpostiosoitteen.	”esimerkki@aventra.fi”
”black_reader_acs”	Tämä asetus kertoo mustan lukijan kulunvalvontajärjestelmän.	”Timecon”
”issue_id_types”	Tämä asetus kertoo pisteellä sallittujen korttityyppien nimet	”Visitor ID, External ID”
”card_printer”	Tämä asetus kertoo pisteellä käytettävän korttitulostimen	”HDP5000 Card printer”
"allow_temp_access”	Tämä asetus kertoo sallitaanko pisteellä ”temporary access” toiminnon käyttäminen vai ei.	”YES/NO”

aliases.apa

```
<?xml version="1.0" encoding="utf-8"?>
<AliasNames xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" ExecuteMode="Production">
  <Alias Type="URL" Name="acme" Production=                                    Testing=
  <Alias Type="VALUE" Name="apm_location" Production=                  Testing=                    />
  <Alias Type="VALUE" Name="apm_location_new" Production=               Testing=                  />
  <Alias Type="FILE" Name="prod_file_prefix" Production="" Testing="Test_" />
  <Alias Type="VALUE" Name="printer_connected" Production="YES" Testing="YES" />
  <Alias Type="VALUE" Name="camera_connected" Production="YES" Testing="YES" />
  <Alias Type="VALUE" Name="ask_pin_default" Production="YES" Testing="YES" />
  <Alias Type="VALUE" Name="ask_pin_visible" Production="Show=True" Testing="Show=True" />
  <Alias Type="VALUE" Name="pdf_lang_default" Production="UK" Testing="UK" />
  <Alias Type="VALUE" Name="default_card_type" Production=         Testing=         />
  <Alias Type="VALUE" Name="print_taxnbr_default" Production="NO" Testing="NO" />
  <Alias Type="VALUE" Name="request_signature" Production="YES" Testing="YES" />
  <Alias Type="VALUE" Name="testing_frontend" Production="PROD" Testing="TESTING" />
  <Alias Type="VALUE" Name="apm_exec_env" Production="Production" Testing="Testing" />
  <Alias Type="VALUE" Name="testing_email" Production="" Testing="          @aventra.fi" />
  <Alias Type="VALUE" Name="black_reader_acs" Production="       " Testing="       " />
  <Alias Type="VALUE" Name="issue_   _id_types" Production="" Testing="" />
  <Alias Type="PRINTER" Name="card_printer" Production="HDP5000 Card Printer" Testing="HDP5000 Card Printer" />
</AliasNames>
```

Kuva 19. Asiakkaan ”alias.apa”-tiedosto.

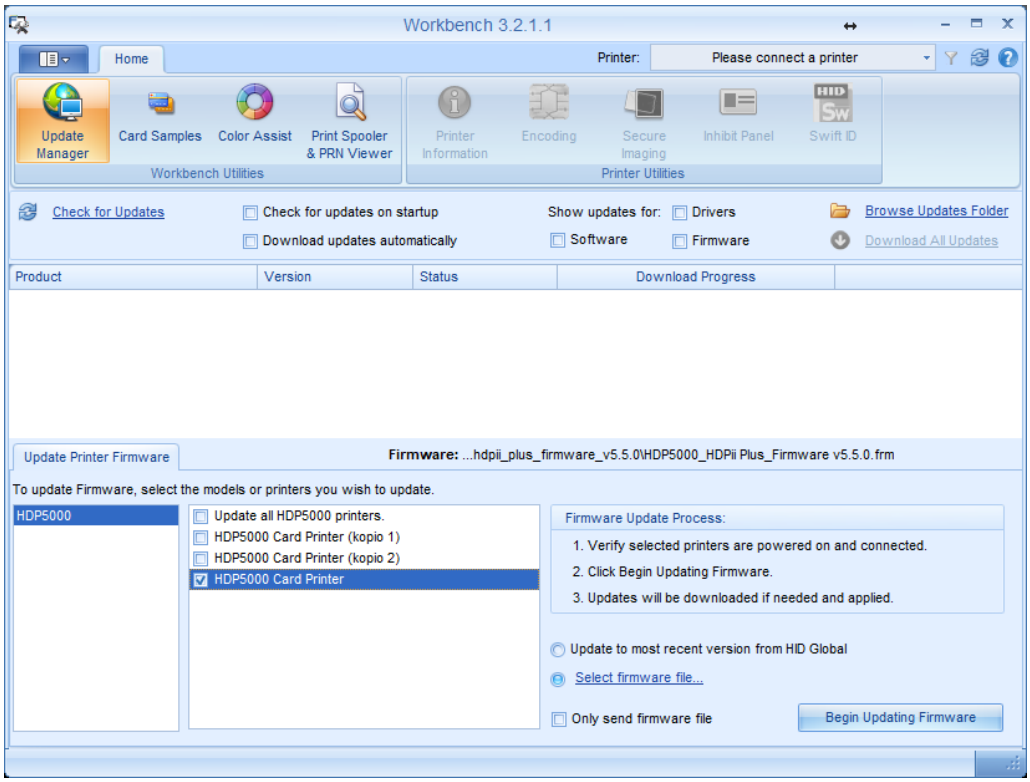
Tarvittavien tiedostojen lisäämisen jälkeen yritettiin käynnistää uusi APM-työ uudella APM-versiolla, mutta törmättiin seuraavaan ongelmaan (kuva 20).



Kuva 20. Komponenttien lataus ei onnistu.

Tämä ongelma ilmeni, kun asiakkaan lisenssistä virheellisesti puuttui näiden 3 komponentin käyttöoikeus. Uusi lisenssitiedosto tuli luoda ja asentaa. Uusi lisenssi generoitiin ja lisenssin varsinainen asennus onnistui yksinkertaisesti tuplaklikkaamalla lisenssitiedostoa. Uuden lisenssin asentamisen jälkeen voitiin siirtyä APM:n osalta testaamiseen.

Pisteellä ajettiin olennaisien toimintojen testejä ja niissä löytyneitä virheitä korjattiin. Esimerkiksi siruttoman kortin tulostuksen yhteydessä annettiin tulostimelle turhia komentoja, jotka saivat sen jumiutumaan lähes joka kerralla. Tulostimeen piti myös asentaa firmware-päivitys, jolla saatiin korjattua toinen ongelma, mikä aiheutti tulostimen satunnaisen jumiutumisen. Firmwaren päivitys onnistui tulostimen ajuriohjelmalla, siitä valittiin firmwaren asennustiedosto ja valittiin tulostin. Tulostimen ajuriohjelman (kuva 21) oma automaatio hoiti lopun asennuksesta.

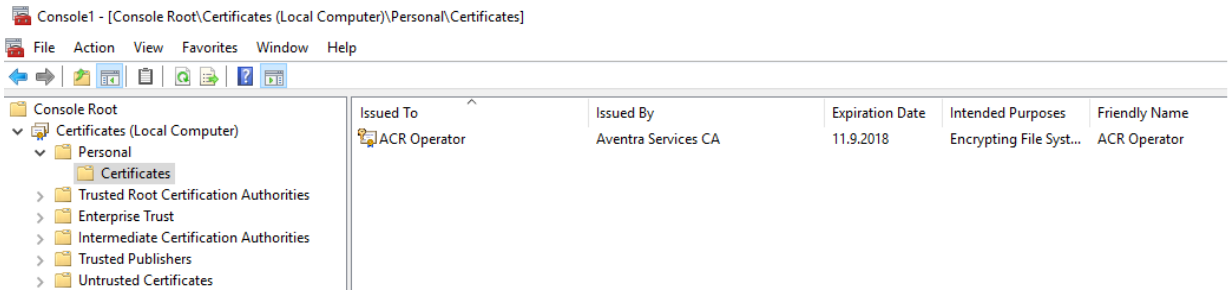


Kuva 21. Tulostimen firmwaren päivitys

Kun virheet oli korjattu, firmware päivitetty, koulutus pidetty ja ohjelma sekä sen konfiguraatio oli saatu toimimaan luotettavasti, siirryttiin suorittamaan asennus saman toimipisteen kahdelle kevyelle pisteelle.

Näillä kahdella pisteellä ainoa oheislaite oli allekirjoitustabletti, joten asennus oli helpompi ja lyhyempi, myös virheiden korjaukset oli tehty suoraan APM-työhön. Niitä ei siis tarvinnut tehdä enää uudelleen. Toinen näistä pisteistä oli kokonaan uusi, siihen ei ollut asennettu ollenkaan APM:n vanhempaa versiota. Tällä pisteellä APM:stä piti asentaa vanhempi versio, 3.2.2, ja tämän päälle tuotiin nämä uuden APM:n asennustiedostot.

Ainoa ongelma asennuksen aikana oli operaattorivarmenteen kanssa. Se oli ennakkoon asennettuna näihin kahteen pisteeseen väärään paikkaan. Operaattorivarmennetta käytettiin vanhassa APM-työssä eri tavalla. Se oli myös asennettu eri pisteillä eri paikkoihin, koska asennuksia suoritti useampi henkilö eikä yhtenäistä ohjetta tai käytäntöä ollut. Operaattorivarmennetta käytetään tunnisteille tuotavien avainten avaamiseen. Operaattorivarmenne tulee tässä tapauksessa asentaa työaseman ”My computer” varastoon (kuva 22), eikä jokaiselle pisteen käyttäjälle erikseen. Näin säästytään ongelmilta, jos pisteelle esimerkiksi tulee uusia käyttäjiä.



Kuva 22. Operaattorivarmenne oikeaoppisesti asennettuna.

Asennuksien lopputuloksena oli kolme toimivaa pistettä, joille asennettiin uusin APM-versio sekä uusin APM-työ. Kaksi näistä pisteistä oli ns. kevyitä ja yksi täysi piste. Pisteitä testattiin ja todettiin kaikki toiminnot toimiviksi ja jätettiin vanha APM-työ toimivaksi varalle kaikkiin pisteisiin, joissa se oli asennettuna. Uuden APM:n tuotantokäyttö alkoi toimipisteellä heti asennuksien jälkeen.

5 Yhteenveto

5.1 Suunnittelu, dokumentointi ja testaaminen

Projektin aikataulutus sekä suunnittelu alkoi jo marraskuussa 2017. Projekti oli alun perin tarkoitus suorittaa vuoden loppuun mennessä, mutta ennakoimattomien ongelmien takia jouduttiin asennusta siirtämään myöhemmälle testauksien ja korjauksien jatkuessa odotettua pidemmälle. Ensimmäiset testaukset uuden APM-version kanssa tehtiin 7.12, mutta tästä löytyneiden virheiden korjausten jälkeistä versiota päästiin testaamaan vasta 16.1.

Yksi iso ongelma oli APM-työssä käytettyjen ”Jump”-komponenttien kanssa havaittu ohjelmistobugi. Näillä komponenteilla nimen mukaisesti hypitään APM-työssä eri kohtien välillä. Komponenteissa havaittu bugi rikkoi niiden toiminnallisuuden kokonaan, kun APM-työtä editoitiin ja tallennettiin. Tämä vaati ison määrän manuaalista työtä, kun AMP-työtä konfiguroitiin. Jokainen ”Jump”-komponentti piti asettaa uudelleen jokaisen pienenkin muutoksen jälkeen, kunnes tämä bugi saatiin korjattua.

Alkuperäisen aikataulutuksen epäonnistumisen suurimpana syynä erittäin laajojen muutosten vaatiman testauksen, isompien muutosten tuomat bugit ja virheet sekä niiden vaikutusten aliarviointi. Projektiin olisi pitänyt varata merkittävästi lisää aikaa muutosten tekemiseen, testaukseen, konfigurointiin ja muutosten implementointiin. Projektiin tehtiin uusi aikataulutus helmikuun alussa, kun korjausten ja testausten tulokset alkoivat vaikuttaa kelvolliselta. Tässä uudessa aikataulussa merkitty asennuspäivämäärä piti loppuun asti, joten sen kannalta onnistuttiin.

5.2 Asennus

Asennus onnistui melko hyvin. Muutamia ongelmia osattiin odottaa, mutta osa tuli täysin yllätyksenä. Esimerkiksi joitain ongelmia tulostimen kanssa osattiin odottaa, ja niihin osattiin varata aikaa. Asennukseen oli varattu tarvittaessa 2 päivää, mutta asennus onnistui yhdessä pidemmässä työpäivässä. Lopputuloksena asennuksesta oli kolme toimivaa pistettä, kaikissa lähes identtinen konfiguraatio, uusimmat APM-versiot sekä vanha konfiguraatio tallella niissä pisteissä, missä se oli asennettuna aikaisemmin.

Lähteet

1 X.509 Certificates – Explained. Verkkoaineisto <https://techblognow.files.wordpress.com/2015/02/x509-1.gif?w=300&h=200>. Luettu 29.12.2017.

2 RSA (cryptosystem). Verkkoaineisto <https://en.wikipedia.org/wiki/RSA_(cryptosystem)>. Luettu 21.12.2017.

3 Fermat'n pieni lause. Verkkoaineisto. <https://fi.wikipedia.org/wiki/Fermat%E2%80%99n_pieni_lause.> Luettu 3.1.2018

4 Public key infrastructure. Verkkoaineisto. <https://en.wikipedia.org/wiki/Public_key_infrastructure>. Luettu 21.12.2017

5 Certificate authority. Verkkoaineisto. <https://en.wikipedia.org/wiki/Certificate_authority>. Luettu 29.12.2017.

6 Root certificate. Verkkoaineisto. <https://en.wikipedia.org/wiki/Root_certificate>. Luettu 11.1.2018.

7 Smart Card Technology and Security. Verkkoaineisto. <https://people.cs.uchicago.edu/~dinoj/smartcard/security.html>. Luettu 11.1.2018

8 Havainnekuva. Verkkoaineisto. < http://p.globalsources.com/IMAGES/PDT/B0600187397/RFID-chip-inside-transparent-card.jpg> Luettu 11.1.2018.

9 Radio-frequency identification. Verkkoaineisto. <https://en.wikipedia.org/wiki/Radio-frequency_identification> Luettu 29.12.2017.

10 Havainnekuva. Verkkoaineisto. < https://idesco.fi/wp-content/uploads/2016/08/Basic-transparent-web-and-screen-1-435x341.png> Luettu 17.1.2018.

11 Weis, Stephen A. RFID (Radio Frequency Identification): Principles and Applications. Verkkoaineisto <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.182.5224> Luettu 07.08.2018.

12 Sjöblom, Jan. 2018. Teknologiajohtaja, Aventra Oy, Espoo. Keskustelu.