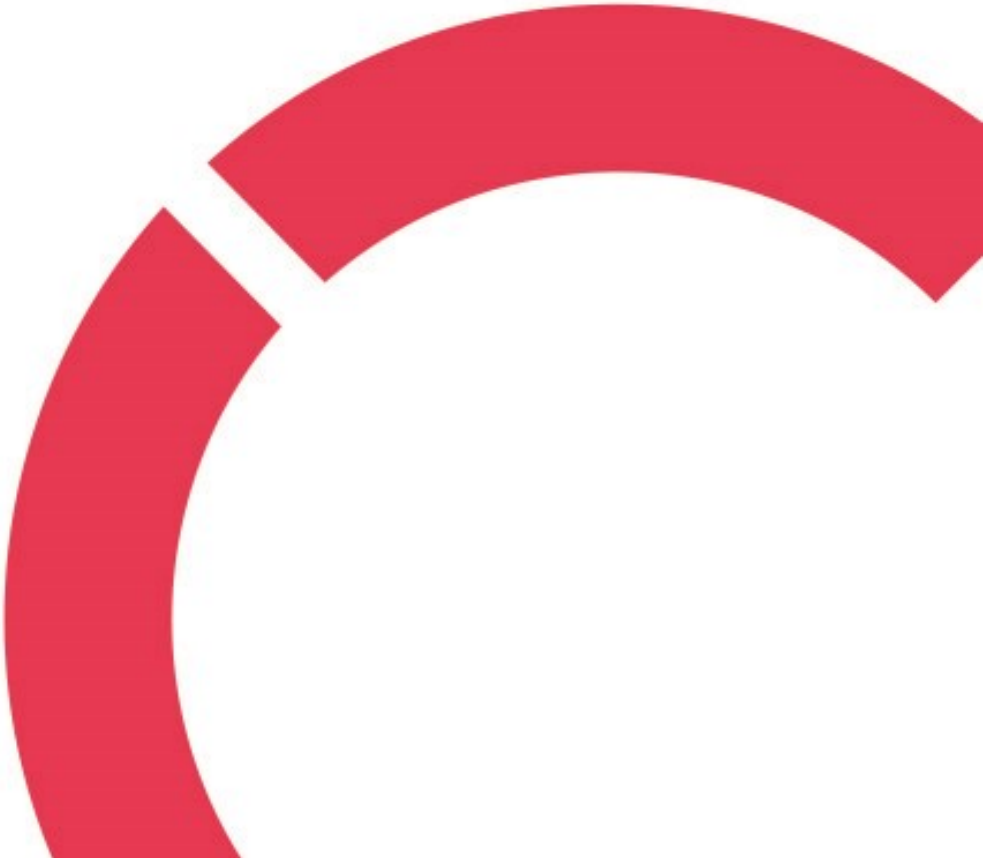
Roy Utter

BIOMETRINEN KIRJAUTUMINEN TIETOKONEISIIN PALVELINYMPÄRISTÖSSÄ

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutus
Kesäkuu 2022



TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Kesäkuu 2022	**Tekijä/tekijät** Roy Utter
Koulutus Tieto- ja viestintätekniikka		☒ AMK ☐ YAMK
Työn nimi Biometrinen kirjautuminen tietokoneisiin palvelinympäristössä		
Työn ohjaaja Jari Isohanni		**Sivumäärä** 38 + 32
Työelämäohjaaja		

Tämän opinnäytetyön tavoitteena oli kartoittaa ja testata mahdollisuutta käyttää biometristä tunnistautumistapaa palvelinympäristössä keskittyen erityisesti oppilaskäytössä oleviin tietokoneisiin ensimmäisen asteen opetuksessa. Työssä käydään myös lyhyesti läpi, miten Euroopan GDPR-laki vaikuttaa biometriikkaan. Opinnäytetyössä kuvataan tunnetuimpia erilaisia biometrisiä tunnistautumistapoja ja valitaan niistä sopivin testauslaitteistoa huomioon ottaen.

Tämän jälkeen opinnäytetyössä käytiin läpi palvelinympäristön ja muun testilaitteiston asennus ja tarvittava konfigurointi. Seuraavaksi suoritettiin itse testi, joka onnistui ilman ongelmia.

Lopuksi opinnäytetyössä pohditaan moraalisuutta ja oikeutta alaikäisten datankeruuseen ja rakennetun ympäristön turvallisuuteen, mikäli opinnäytetyössä tehty kokonaisuus olisi jossakin käytössä.

Asiasanat
Biometriikka, GDPR, Kirjautuminen, Palvelinympäristö

ABSTRACT

Centria University of Applied Sciences	**Date** June 2022	**Author** Roy Utter
Degree programme Information and communication technologies		
Name of thesis Biometric login in domain-environment		
Centria supervisor Jari Isohanni		**Pages** 38 + 32
Instructor representing commissioning institution or company		

The goal of this thesis is to map and assess the possibility of using biometric identification in a domain environment, focusing especially in the area where first degree students are using computers. The thesis will also briefly touch the relevant parts of European GDPR-law and how it affects biometrics. The most common biometric authentication methods are explained and then a suitable method is chosen dependant on the testing hardware.

The thesis will then go through the domain and other infrastructure needed for the test, also the configuration of the infrastructure is shown and explained. After that is the test itself, which was a resounding success.

Lastly in the thesis is some pondering on the morality and legality of collecting biometric data on minors and the overall security of the testing environment, if it really were in use.

Key words
Biometrics, Domain environment, GDPR, Login

KÄSITTEIDEN MÄÄRITTELY

Ankkuripiste: Ankkuripisteet ovat biometriikassa hyödynnettäviä ihmisen kasvoissa ja muualla kehossa sijaitsevia kiinteitä pisteitä, joiden muodostama kokonaisuus ei muutu, vaikka ihmisen paino muuttuu tai kun vanhenee.

Safe Boot/Secure Boot:
Secure boot tai safe boot on PC-yhteisön luoma turvallisuusstandardi, jonka avulla voidaan varmistaa, että sertifikaatit ja tiedostojen yksilölliset ”allekirjoitukset” ovat aitoja ja turvallisia käynnistettäväksi tietokoneella.

UEFI:
UEFI on käytännössä päivitys vanhanaikaiseen BIOS-käynnistykseen, BIOS tulee sanoista Basic Input-Output System, jonka avulla tietokonetta ohjattiin ennen kuin käyttöjärjestelmä on ladattu levyltä. BIOS-sin valikoista pystyi valitsemaan, miltä levyltä kone käynnistetään, toimiiko wifi ja paljon muuta vaativampaa.

USB:
Universal Serial Bus on ollut tietokoneissa jo todella kauan. Tätä liitäntää hyödyntäen voi tietokoneeseen liittää melkein mitä tahansa, oli se sitten kamera, hiiri, sormenjälkiskanneri, kaiuttimet tai vaikka ratti.

DOMAIN:
Domain on tietyllä palvelimella asennettu alue, jossa tietyn kohteen laitteet sijaitsevat, myös muut palvelimet. Huomaa että yhdellä kohteellakin voi olla useampi domain, jos niin tarvitaan.

FOREST:
Forest on alue, jolla palvelimet sijaitsevat. On helpompi ajatella jokaista palvelinta yhtenä puuna metsässä, jossa jokaisella puulla on oma tehtävänsä.

PALVELIN:
Jokaisella palvelimella Forestissa on omat tehtävänsä, esimerkiksi on olemassa palvelimia, joilla on useita eri tehtäviä. Vastaavasti löytyy myös palvelimia, joilla on yksi tietty tehtävä. Tehtävät voivat vaihdella aina tietokonekannan ylläpidosta IP-osoitteiden jakeluun ja tulostimien hallintaan. Voi olla

myös palvelimia, joilla on sama tehtävä kuin toisella palvelimella. Näin estetään kokonaisjärjestelmän toimimattomuus, mikäli jokin palvelin lakkaa vastaamasta tai menee rikki.

GROUP POLICY:

Group policy eli suomeksi ryhmäkäytäntö on laaja lista sääntöjä, joita palvelin lähettää käyttäjien profiileihin, mutta myös tietokoneisiin. erilaisia sääntöjä ovat muun muassa mihin verkkoon voi yhdistää, mitä tapahtuu, jos tietty henkilö kirjautu sisään johonkin tiettyyn koneeseen tai jopa milloin tietokone käynnistetään uudelleen riippumatta siitä, mitä mahdollinen käyttäjä koneella silloin tekee.

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

KUVAT

1 JOHDANTO

Tämän työn tavoitteen on kuvata ja testata biometristä kirjautumisjärjestelmää, joka soveltuu käyttöönotettavaksi kouluissa, erityisesti alakoululaisten keskuudessa. Vaikeus tulee esiin varsinkin 1–2 luokkalaisten kanssa, joilla voi tuottaa ongelmia omien nimiensä ja salasanojensa muistamisessa ja näiden oikeinkirjoituksessa, jolloin usein opettajan apua tarvitaan. Opettajathan eivät saisi tietää luokkalaistensa salasanoja. Pitää siis löytää helpompi tapa tunnistautua. Ratkaisuna toimisi esimerkiksi biometrinen kirjautuminen. Biometrinen kirjautuminen antaa henkilön kirjautua tietokoneeseen käyttämällä esimerkiksi sormenjälkitunnistautumista.

Tässä työssä avataan myös hieman EU:n GDPR-lain vaikutusta oppilaan yksityisyyden suojaamiseen. Päivitetty EU-yksityisyyssuojaus estää yhteistunnusten käytön, mitkä olivat yleisessä käytössä kouluissa. Oppilaat ja opettajat joutuvat käyttämään nykyään omia tunnuksiaan, jotka välillä tuottavat ongelmia erityisesti nuorempien lasten keskuudessa. EU-yksityisyyssuojaus eli toisin sanoen GDPR-laki on EU:ssa voimaan tullut lainsäädäntö, joka rajoittaa datan keruuta.

Tämä työ toteutetaan testiympäristössä pienellä määrällä tietokoneita, jotta projektin toimivuus voidaan todeta. Haastateltujen opettajien keskuudessa ilmapiiri on yleisesti ollut positiivinen, parilla on myös ollut jopa halukkuutta olla mukana testiryhmässä.

Ongelmana tulee todennäköisesti olemaan ensimmäinen kirjautuminen koneelle kuin koneelle, tämä täytyy suorittaa käyttämällä henkilön käyttäjänimeä ja salasanaa. Biometriset tiedot eivät myöskään oletuksena tallennu mihinkään verkossa olevaan tietokantaan vaan pysyvät tietoturvan nimissä vain ja ainoastaan paikallisesti tietokoneessa, jota henkilö käyttää. Tämä tarkoittaa siis uutta kirjautumista ilman biometrisiä toimintoja jokaisella kerralla, kun henkilö käyttää uutta tietokonetta.

2 TIETOSUOJAN LAIT JA MÄÄRÄYKSET

Nykyään kaiken datan kerääminen on hyvin tarkkaa puuha, varsinkin jos kyseessä on henkilökohtaista ja arkaluontoista dataa, jota voi hyödyntää tunnistamaan henkilöitä. Tämä tuottaa tietenkin haasteita silloin kun puhutaan biometriikasta, sillä se jos mikä on arkaluontoista dataa. Tietosuojan lait voidaan jakaa pääpiirteittäin kahteen pääryhmään: Europanlaajuiseen ”General Data Protection Regulation” lakiin eli jokaisen netissä liikkuvaa vastaan tulleet GDPR-ponnahdusikkunat ja Suomen oma tieto-suoja-laki, joka täydentää ja täsmentää tätä aikaisemmin mainittua GDPR-lakia. (Lexia 2018).

2.1 General Data Protection Regulation (GDPR)

GDPR-laki hyväksyttiin EU-parlamentissa huhtikuussa 2016 kahden vuoden käyttöönotto ajalla, jonka jälkeen laki muuttui pakolliseksi 25.5.2018.

GDPR-laki vahvistaa EU-kansalaisen yksityissuojaa ja muuttaa miten kansalaisten dataa hallitaan aina terveydenhuollosta pankkiasioihin. (*EU:n tietosuoja-asetuksen velvoitteet johdolle.*)

Tämä opinnäytetyö ei ole GDPR-tutkielma, joten tässä työssä ei erityisen syvälle sukelleta GDPR-lain syövereihin, vaan käydään vähän yleisesti läpi tarvittavia alueita.

2.1.1 GDPR vaikutusalue

Lyhyesti sanottuna GDPR-laki vaikuttaa melkein kaikkeen missä käsitellään dataa.

Jokainen meistä on varmasti huomannut netissä liikkuessamme eri sivustojen evästekyselyt, joihin pitää vastata ennen. Kyseisellä sivustolla on mahdollista jatkaa, mikäli vastasi myöntävästi vähintään pakollisiin evästeisiin. Tämä on suora esimerkki siitä, kuinka laajasta vaikutusalueesta GDPR-laissa on kyse.

Tarkemmin sanottuna GDPR-laki vaikuttaa kaikkiin organisaatioihin, yrityksiin ja julkisiin sektoreihin EU:n sisällä tai sen ulkopuolella, jotka joko varastoivat tai käyttävät EU-kansalaisten henkilökohtaista tai arkaluontoista dataa, riippumatta siitä missä kyseinen organisaatio, yritys tai julkinen sektori fyysisesti sijaitsee. (*Miten asetus muuttaa henkilötietojen käsittelyä?.*)

Henkilökohtaisella datalla tarkoitetaan kaikkea sitä dataa, jotka voidaan yhdistää johonkin tiettyyn henkilöön. Näitä ovat mm. henkilökohtainen sähköpostiosoite, käyttäjänimet, IP-osoitteet, ja mahdollinen data, joka paljastaa henkilön fyysistä sijaintia, toisin sanoen, hyvin laaja alue.

Arkaluontoisella datalla tarkoitetaan uskonnollista suuntautumista, poliittista suuntautumista, terveystietoja, biometristä dataa, geneettistä dataa, nimeä, mutta myöskin rotua ja etnisyyttä. (HAMK 2020.)

2.1.2 GDPR-toiminnan varmistus ja rangaistukset

Jotta GDPR-laki toimii yrityksissä, organisaatioissa ja julkisilla sektoreilla, nimetään vähintään yksi tietosuojavaltuutettu. Tämän henkilön on työnään, tai muun työn ohessa on varmistettava, että yritys tms. noudattaa GDPR-lakia onnistuneesti. (Europa.eu 2021a).

Jos GDPR-lakia ei noudateta, saa rangaistuksen. Rangaistus on useimmiten sakkojen muodossa 2–4 % koko yrityksen liikevaihdosta, riippuen rikkeen vakavuudesta. Viranomainen voi myös määrätä korjaavia toimenpiteitä tai henkilötietojen käsittelyn lopettamista kokonaan. (Europa.eu 2021b).

Pääpiirteiltään GDPR-laki antaa käyttäjälle oikeuden nähdä, mitä tietoja kyseinen organisaatio on hänestä tallentanut, mahdollisuuden poistaa nämä tai estää organisaatiota lähettämästä tietoja eteenpäin. Tietojen pitää olla myös hyvin suojattu niin kutsutulla Privacy by Design -tavalla, eli käyttäjän turvallisuus pitää olla keskeinen teema jo järjestelmän suunnitteluvaiheessa. Mahdolliset tietomurrot on ilmoitettava tietosuojavaltuutetulle 72 tunnin kuluessa siitä, kun murto on havaittu. Esimerkki tieto-turvaloukkauksesta voi olla niinkin yksinkertainen, kuin hävinnyt usb-muistitikku tai vakavampana esimerkkinä kyberhyökkäys. (European Commission; Tietosuojavaltuutetun toimisto. *Tietoturvaloukkaukset*).

Yritys tms. pitää myös hyvin näkyvästi ja selkeällä kielellä ilmoittaa mitä tietoja säilytetään käyttäjästä ja miten niitä säilytetään. Esimerkiksi internet-sivustojen evästeet, jotka vaativat sivuston keksien hyväksymistä, ovat viime aikoina yleistyneet hyvinkin paljon internetissä johtuen juuri GDPR-laista. (Tietosuojavaltuutetun toimisto. *Kun haluat tarkastaa tietosi*).

2.2 Kansallinen tietosuoja

Suomen kansallinen tietosuojalaki soveltaa EU:n GDPR-lakia laajentaen ja täydentäen sitä, jotta se soveltuisi paremmin Suomen lainsäädäntöön.

Keskeisimmät muutokset, joita kansallinen tietosuoja tarkentaa, ovat erityistilanteissa sovellettavaa tietojen käsittelyä esimerkiksi tieteellisessä tutkimuksissa, tilastoinnissa ja arkistoinnissa. Pieniä muutoksia esiintyy myöskin liittyen alaikäisiin ja ikärajoihin, koska Pohjoismaissa ikärajat ovat yleisesti ottaen alhaisemmat kuin muualla Euroopassa. (*Tietoyhteiskunnan palvelujen tarjoamiseen lapselle sovellettava ikäraja.*)

2.3 Alaikäiset tietosuojassa

Alaikäisten huomioon ottaminen kaikessa tässä tuottaa myös omat haasteensa. Tietosuojan näkökulmasta katsoen alaikäisyyden raja on Suomen kansallisessa tietosuojalaissa 13 vuotta. Näin ollen, jos henkilö on alle 13-vuotias, pitää lapsen huoltajan antaa suostumus. 13 vuotta vanhemmille voi palveluita tarjota ilman huolitsijan suostumusta. Kannattaa tosin muistaa, että tämä ikäraja vaihtelee eri jäsenvaltioissa 13–16 ikävuoden välillä. Nämä erot pitää siis ottaa huomioon silloin kun palveluiden tarjonta ulottuu muihin EU-maihin. (Lexia 2018).

3 BIOMETRIIKKA

Biometrisessä kirjautumisessa käytetään hyväksi henkilön uniikkeja bioloogisia eroja, kuten sormenjälkeä ja silmän iiristä. Biometristä tunnistautumista on käytetty jo jonkin aikaa esimerkiksi turvaovien kanssa. Näin ollen esimerkiksi vain lukijalle määritetyt sormenjäljet voivat avata ovessa olevan lukon. Biometrinen kirjautuminen on ollut myös mahdollista jo jonkin aikaa puhelimissa ja tietokoneissakin, mutta Windows Hellon käyttöönoton jälkeen, on tämä yleistynyt räjähdysmäisesti myöskin yksityisille käyttäjille. (Parmar 2020).

3.1 Tunnistautumistapoja

Tunnistautuminen tapahtuu käyttämällä hyväksi erilaisia henkilön yksilöllisiä biologisia eroja, kuten hammaskarttaa, sormenjälkeä, silmän iiristä tai dna:ta. Ihmisistä löytyy monia biologisia eroja, jopa identtisistä kaksosista.

Useimmiten käytettävissä olevat tunnistustavat ovat sormenjälki, iiris, kämmenjälki, ääni ja kasvot. (Jirik 2021).

Biometrisiä tunnistautumistapoja löytyy kuitenkin hyvinkin paljon. Pitäen opinnäytetyön järkevän pituisena, mainitsen vain tunnetuimmat tunnistautumismuodot.

3.1.1 Sormenjälki

Sormenjäljen tunnistaminen on yleisin ja tunnetuin biometrinen tunnistautumistapa yhdessä kasvojen skannauksen kanssa, lähinnä puhelimissa käytettävien tunnistautumistapojen takia. Sormenjälkiskannereita löytyy kirjoitushetkellä kolmea eri tyyppiä.

Optinen skanneri toimii käyttämällä hyödykseen valoa luomalla digitaalisen kopion sormesta, samantyylisellä tavalla, kuin perinteinen skanneri tai kopiokone. Sormi sijoitetaan linssille, joka on esimerkiksi lasia tai muovia. Linssin läpi johdetaan valoa ja sormesta heijastunut valo otetaan vastaan sensorin

avulla. Tämän jälkeen algoritmien avulla kuva varmistetaan hyvälaatuiseksi, minkä jälkeen siitä muodostetaan pätkä koodia. Koodi perustuu sormenjäljen eri piirteisiin, kuvion muotoon, reunojen paksuuteen ja niin edelleen, joten koodista tulee yksilöllinen. Sama tulos saadaan, jos sormi laitetaan skanneriin uudelleen, vaikka hieman eri asennossakin. (Woodford 2022.)

Kuva 1. Kapasitiivinen skanneri. (Pixabay 2019).

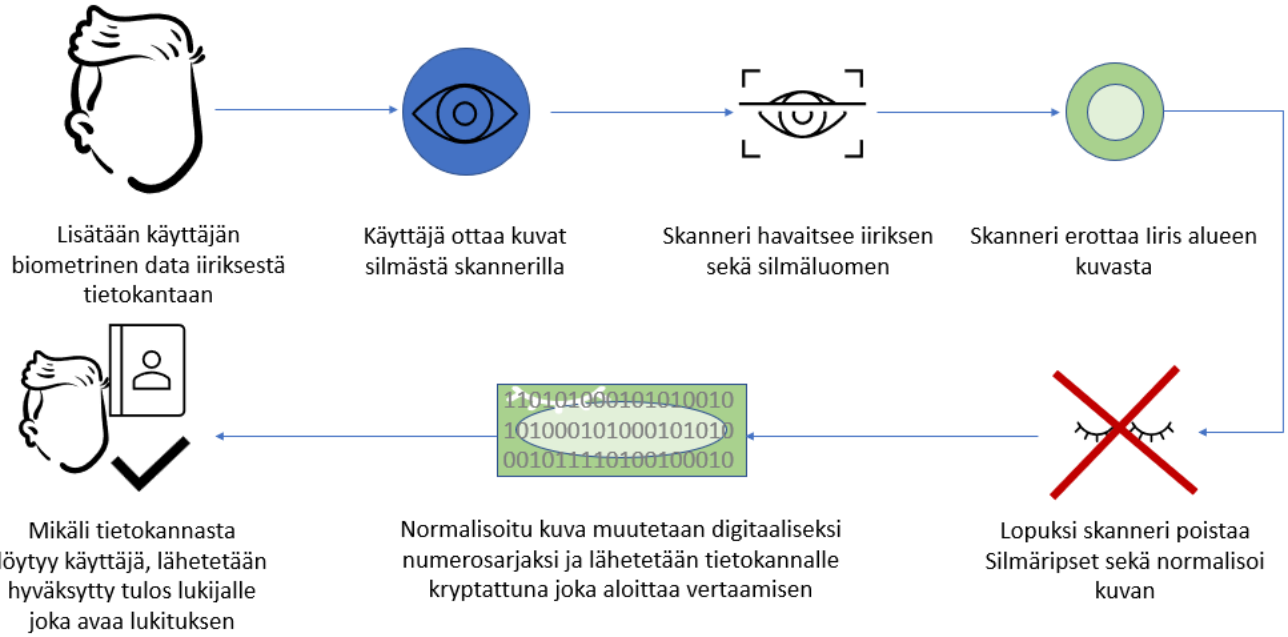
Kapasitiivinen skanneri toimii mittaamalla sormessa syntyvää vastusta, kun se laitetaan sensorilevyn päälle. Skanneri toimii parhaiten silloin kun sormi laitetaan levyn päälle, kuitenkaan painamatta liikaa. Silloin sormenjäljessä esiintyvät urat ovat helpommin havaittavissa ja niiden leveys laskettavissa. Kuten huomata saattaa, kapasitiivinen skanneri on tuvallisempi kuin optinen skanneri. Optista skanneria voi huijata pelkällä hyvälaatuisella kuvalla sormesta, mutta kapasitiivisessa skannerissa tarvitaan jo uria ja vastaavaa epätasaisuutta, jotka johtavat sähköä. Kapasitiivinen skanneri on nopeampi ja turvallisempi kuin optinen skanneri, mutta kapasitiivinen skanneri toimii huonosti, jos skannausvaiheessa sormi on märkä, skanneri saattaa jopa vioittua staattisesta sähköstä.

Ultraääni-skanneri on näistä kolmesta se turvallisin, mutta myös hitain sormenjälkitunnistin, riippuen siitä minkälaisessa valotetussa tilassa aiemmin mainittu optinen skanneri sijaitsee. Ultraääni-skanneri

toimii tekemällä ultraäänen avulla 3-ulotteisen kuvan sormenjäljestä, näitä tunnistimia löytyy useimmiten puhelimen näytön takaa, mikäli kyseisessä puhelimessa on sormenjälkitunnistin. Sormesta siis luodaan 3-ulotteinen objekti, josta algoritmi mittaa nämä aikaisemmin mainitut urat ja muut kohokkeet ja syvennykset, joita sormenjäljessä esiintyy. Tämä tieto muutetaan koodinpätkäksi, joka sitten lähetetään eteenpäin autentikoivalle osapuolelle, joka vertaa omassa tietokannassa olevia koodinpätkiä ja varmistaakseen, saako kyseinen sormi pääsyn, oli se sitten koneelle kirjautuminen tai ovesta sisään pääseminen. (Woodford 2022.)

3.1.2 Iiris-skanneri

Yksi myös hyvin tunnettu biometrinen tunnistautumistapa on silmän iiristä hyödyntävä skanneri. Skannerin avulla tunnistetaan henkilö toisesta hyödyntämällä ihmisen silmän iiristä. Iiris on niin monimutkainen, että algoritmit nykypäivänä hyödyntävät noin 260 eri ankkuripistettä, verrattuna sormenjälkeen, jotka käyttävät 60–70 pistettä laitteesta ja menetelmästä riippuen. (Refaces 2020).



KUVA 2. Visualisointi iiris skannerin toiminnasta.

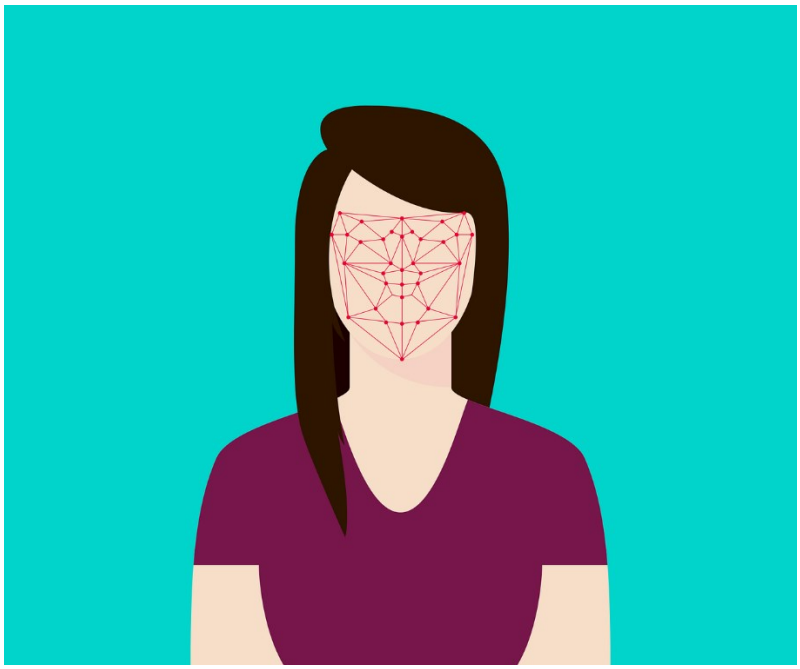
Iiris-skanneri toimii ottamalla kaksi kuvaa iiriksestä, josta toinen on infrapunakuva. Laitteesta riippuen nämä kuvat otetaan 10 cm – 1 metrin etäisyydeltä. Tämän jälkeen kuvista poistetaan ylimääräiset osat, kuten esimerkiksi silmäripset. Seuraavaksi kuvat muokataan, jotta silmän yksityiskohdat näkyvät mahdollisimman selkeästi. Lopuksi kuvista haetaan ankkuripisteiden kautta tarvittavat tiedot, jotka muutetaan digitaaliseksi numerosarjaksi, joka vastaa kyseistä silmää. Digitaalisessa muodossa olevaa silmää verrataan tietokannassa oleviin numerosarjoihin.

Iiris-skannerin selvä etu sormenjälkeen on sen muuttumattomuus, se ei muutu henkilön vanhetessa tai käyttäessä piilolinssejä. Silmän vahingoittuminen on myös harvinaisempaa kuin sormen vahingoittuminen. Myös sokeat ihmiset voivat käyttää iiriskanneria, mikäli silmässä on iiris.
(Refaces 2020.)

3.1.3 Kasvontunnistus

Kasvojen tunnistus on toinen hyvin yleisellä käytöllä olevista biometrisistä tunnistautumistavoista, lähinnä puhelimien takia, mutta myöskin kannettavien tietokoneiden takia. Tässä tunnistautumismenetelmässä hyödynnetään tunnistettavan henkilön kasvoja, jotta henkilön identiteetti voidaan varmistaa.

Tunnistamisessa hyödynnetään kasvoissa esiintyviä uniikkeja piirteitä, niin kutsuttuja kasvojen maamerkkejä, niin kutsuttuja ankkuripisteitä. Nämä maamerkit ovat muun muassa silmien etäisyys toisistaan ja otsan ja leuan etäisyys toisistaan, mutta myös silmien, nenän ja suun muoto. Siksi kasvomaskien yleistyessä tämänhetkisen tilanteen takia kasvotunnistusta hyödyntävät laitteet eivät ole toimineet kunnolla viime aikoina ilman kasvomaskin poistamista. (Symanovich 2021).



KUVA 3. Visualisointi kasvojen ankkurpisiteistä. (Pixabay 2021).

Henkilön tunnistus tapahtuu joko kaksi- tai kolmiulotteisella kuvalla, josta algoritmien avulla otetaan henkilöstä kasvojentunnistusta varten tarvittava data.

Dataa verrataan laitteen käytössä olevaan tietokantaan ja positiivinen tulos löytyy, mikäli kyseisen henkilön kasvot on jo lisätty laitteen tietokantaan. (Recogtech 2021.)

Kasvojen tunnistus ei tosin ole ilman omia haasteitaan. Täydellisissä oloissa virhemarginaali voi olla jopa niin alhainen kuin 0,08 %, mutta jos valaistus on huono tai kyseessä on liikkeessä otettu video, tai yksinkertaisesti henkilö on vanhentunut merkittävästi, voi virhemarginaali nousta roimasti. (Refaces 2020)

3.1.4 Äänitunnistus

Ääntä hyödyntävässä biometrisessä tunnistautumisessa käytetään yksilöllisiä äänikuvioita, joista luodaan digitaalinen koodi, jota verrataan jo järjestelmässä olevaan koodiin, joilla henkilö tunnistetaan.

Tunnistautumisessa hyödynnetään muun muassa henkilön tavutusta, painotusta, puheen nopeutta ja aksenttia. Tunnistautumisessa käytetään myös hyväksi kehon biologisia eroja, joiden takia ääni muuttuu. Ääntä muokkaavat biologisella tasolla pääasiassa äänihuulten muoto, suu ja nenäkäytävä. (Nice.)

Tästä syystä biometrinen äänitunnistautuminen on yksi tarkimpia tunnistautumistapoja, mutta on samalla myös valitettavasti herkkä hyökkäyksille ja väärille negatiivisille, jos esimerkiksi käyttäjällä on paha nuha, voi ääni muuttua niin paljon, ettei järjestelmä enää tunnista henkilöä.

Hyökkäykset äänen tunnistautumista vastaan voivat olla helpompia, kuin muita biometrisiä tunnistautumistapoja vastaan. Mikäli järjestelmässä luonnin yhteydessä ei ole ollut mukana niin sanottua vahvaa Liveness Detection -mentaliteettia, jonka avulla järjestelmä voi päätellä, onko ääni orgaanisesti vai tietokoneellisesti luotu. Jos kyseistä metodia ei ole käytetty, niin järjestelmää voi mahdollisesti huijata pelkällä personoitavan henkilön äänitetyllä viestillä. (Pinto 2021.)

Opinnäytetyön kirjoitushetkellä äänen biometrinen tunnistus on ehkä parhaiten käytössä kaksivaiheisessa tunnistuksessa eikä omana yksilöllisenä tunnistautumisena. Muun muassa Yhdysvalloissa biometrinen äänentunnistus on käytössä puhelin- ja pankkiasioissa asioitaessa puhelimen välityksellä. Tunnistusmenetelmää on myös hieman huvittavasti hyödynnetty Yhdysvaltojen Yellowstonen kansallispuistossa ilmenevien susien yksilöllisessä tunnistamisessa. (Monster 2021).

3.1.5 Kämmentunnistus

Kämmentunnistuksessa hyödynnetään käden yksilöllistä kolmiulotteista muotoa, jonka avulla henkilö todennetaan sellaiseksi, jolla joko on tai ei ole pääsyä, minne hän yrittääkään päästä. Järjestelmä hyödyntää kämmenen eri mittasuhteita nämä ovat; kämmenen pituus, leveys, paksuus ja pinta-ala.

Nämä tiedot saadaan asettelemalla kämmen erilliselle alustalle, niin että kämmen asettuu tiettyyn asentoon ja kuvat otetaan, kun kämmen on oikeassa asennossa. Kuvassa on mukana ja kämmenen yläpuoli, ja peilien avulla myös kämmenen sivut. Näiden avulla kuvasta luodaan siluetti, josta otetaan 31 000 pistettä, ja 90 eri mittausta. Informaatio mahtuu 9 bittiin, joka on erittäin alhainen luku, verrattuna muihin biometrisiin tunnistautumistapoihin.

Kämmenestä yleensä otetaan kolme kuvaa, joiden pisteiden sekä mittauksien keskiarvoa hyödynnetään tunnistamisessa. Tietoja verrataan tietokannassa oleviin tietoihin ja riippuen järjestelmän herkkyydestä on kämmen joko hyväksytty tai hylätty. (Mayhew 2012.)

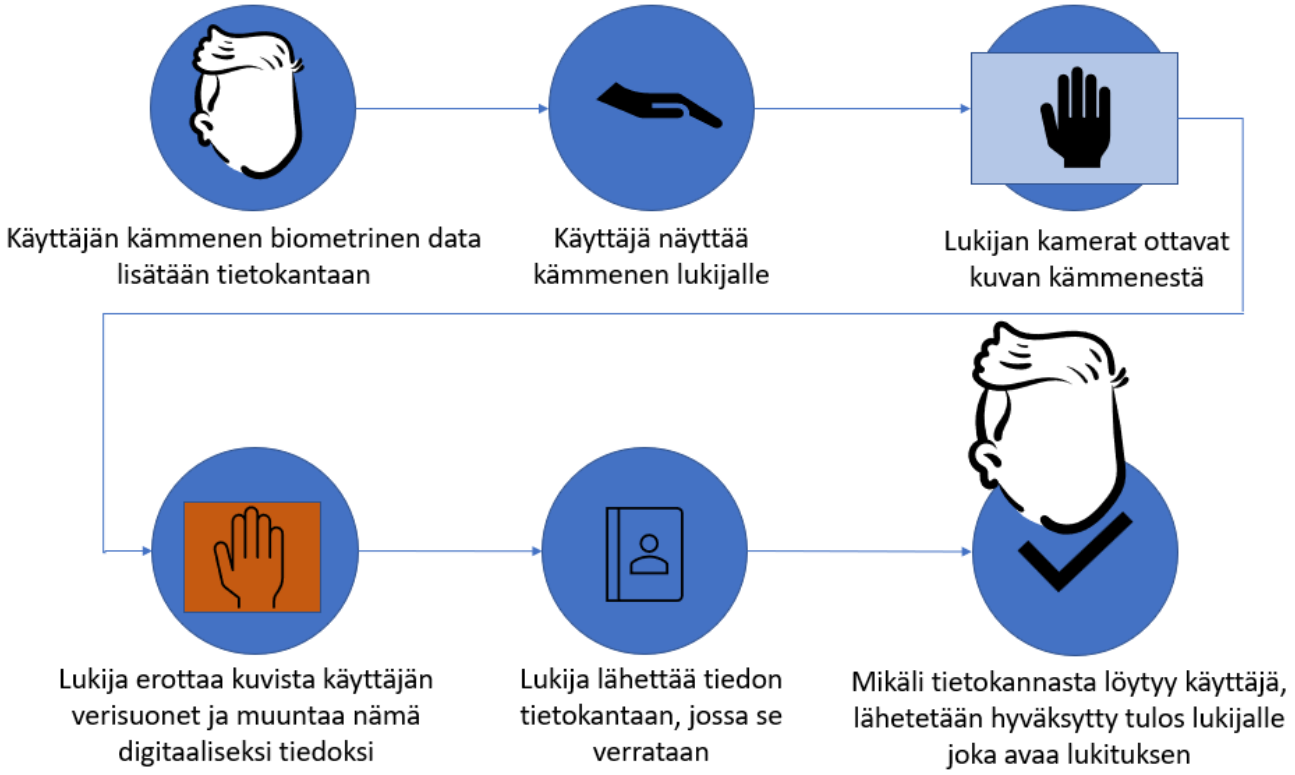
KUVA 4. Kämmen asetettuna lukijaan. (Flickr 2022).

Kämmentunnistuksen huonoja puolia on se, ettei kämmen ole kovin uniikki. Kämmen voi myöskin vaurioitua helpommin ja myös muuttuu herkemmin ikääntyessä ja painon muuttuessa, jolloin kämmenkuvasta voi tulla hyvinkin erilainen. (Mayhew 2012).

3.1.6 Verisuonien tunnistus

Verisioninen tunnistus kämmenestä on tällä hetkellä todennäköisesti sekä turvallisin ja uusin vaihtoehto, mutta myös kallis ja tilaa vievä tunnistautumisjärjestelmä.

Tunnistautumisessa käytetään kämmenessä esiintyviä yksilöllisiä suonia. Kämmenen suonista otetaan infrapunan avulla kuva, joka muutetaan digitaaliseksi, jota sitten verrataan tietokannassa olevaan dataan. Mikäli data täsmää, on henkilöllä pääsy eteenpäin. (Santolalla 2021).



KUVA 5: Visualisointi kämmenlukijan toiminnasta.

Kuvassa esitetään esimerkki, kuinka suonien biometrinen tunnistus kämmenestä voi toimia. Käyttäjän biometrinen data kämmenen suonista tallennetaan tietokantaan. Myöhemmässä vaiheessa käyttäjä yrit-

tää avata lukituksen, johon vaaditaan biometrinen tunnistautuminen. Käyttäjä näyttää lukijalle kämmenensä ja lukija ottaa niistä tarvittavat kuvat. Lukija muuttaa kuvat sopivaan muotoon ja lähettää ne eteenpäin tietokantaan, jossa niitä verrataan tietokannasta löytyviin kämmenen suoniin perustuvaan dataan. Mikäli tietokannasta löytyy tarpeeksi lähellä oleva tulos, avataan lukitus. Kyseinen toimintaperiaate on pääpiiretiltään hyvin pitkälle samanlainen myös muissa mainituissa biometrisissä tunnistautumistavoissa.

Kämmensuonien tunnistustavan turvallisuus tulee pitkälti siitä, että tunnistustapa on kehon sisällä, kun taas muissa mainituissa biometrisissä tunnistustavoissa tunnistettava kohde on kehon ulkopuolella tai tunnistustapaa käytetään koko ajan, esimerkiksi sormenpäissä olevat sormenjäljet mutta myöskin äänen ja lauseen tunnistus. Tämä tekee suonien väärentämisen vaikeaksi, varsinkin kun jotkin tunnistimet vaativat, että suonissa virtaa veri, jotta tunnistus ylipäätänsä edes onnistuisi. (Findbiometrics.)

Verisuonten tunnistus kämmenestä tosin on altis osittain samoille vaaroille kuin niin sanottu normaalimpi kämmenen tunnistus. Näistä vaaroista on ehkä yleisin kämmenen vaurio, joka muuttaa verisuonien sijaintia tai katkaisee kokonaan. Esimerkiksi koiran puraisu voi tällaista aiheuttaa.

3.2 Standardisointi

Opinnäytetyön kirjoitushetkellä kolme edellä mainittua biometrisistä tunnistautumistapaa ovat internationaalisesti standardisoituja tunnistautumismenetelmiä. Nämä ovat sormi, iiris ja kasvot. Esimerkiksi sormi tuottaa saman koodinpätkä, riippumatta siitä kuka on lukijan valmistanut, kunhan valmistaja on noudattanut standardisointia. (icao).

4 WINDOWS HELLO

Windows Hello on Microsoftin kehittämä järjestelmä, joka helpottaa tietokoneeseen tunnistautumisessa. Windows Hello -sovelluksen avulla voidaan käyttää joko yksinkertaista PIN-koodia, tai tietokoneen laitteistosta riippuen erilaisia biometrisiä tunnistautumistapoja, kuten sormenjälkeä tai kasvojen tunnistusta. Tässä opinnäytetyössä hyödynnetään Windows Hello -sovellusta sillä, jokaisesta Windows 8 ja sitä uudemmasta Windows-käyttöjärjestelmästä kyseinen järjestelmä löytyy.

Käyttäjäkohtaisesti Windows Hello on myös helppo ottaa käyttöön, sillä kyseinen järjestelmä on valmiiksi asennettuna laitteissa, ellei sitä ole yrityksen, koulun tai vastaavan atk-tuen puolesta poistettu tai deaktivoitu.
(Kapko & Finnegan 2021.)

Jotta Windows Hello -sovelluksen biometriset ominaisuudet voivat toimia, pitää laitteessa olla kytkettynä biometrinen laite, joko sisäisesti tai esimerkiksi USB-laitteen välityksellä. Kyseisen biometrisen laitteen pitää myös olla niin tarkka, että muun muassa sormenjälkisensoreissa virhemarginaali pitää olla vähemmän kuin 0,002 prosenttia, kun taas kasvojen tunnistuksessa virhemarginaali pitää olla vähemmän kuin 0,001 prosenttia.

Lukuja voidaan verrata Applen Face ID:hen, jossa virhemarginaali on vain yksi suhde miljoonaan, kun taas Applen Touch ID:llä virhemarginaali on 1:50 000, eli suurin piirtein yhtä tarkka kuin Windowsin kasvojen tunnistus. (Kapko & Finnegan 2021.)

5 TESTILAITTEISTON ASENNUS

Testiympäristönä käytetään yhtä kannettavaa tietokonetta, josta löytyy sormenjälkitunnistin. Ympäristössä on myös käytössä yksi palvelin.

Windows Hello tallentaa yksilöllisen biometrisen datan tietokoneen muistiin, ei palvelimen. Näin ollen, jos yhdellä tietokoneella voi käyttää sormea kirjautumiseen, toisessa ei voi, ellei Windows Hello -sovellusta määrittele erikseen myös toiseen tietokoneeseen.
(Microsoft Docs 2022).

Palvelimena toimii Fujitsun pöytäkone, johon on asennettu Windows Server 2016 uusimmilla tämänhetkisillä päivityksillä, jotka viimeksi tarkistettiin 15.2.2022.

Testikoneena toimi Dellin Ultrabook kannettava tietokone mallia LATITUDE E7250. Koneessa myös pyörii viimeisin versio Windows-10 käyttöjärjestelmästä uusimmilla päivityksillä, jotka viimeksi tarkistettiin 15.2.2022.

Kaikissa koneissa on käytetty asennusvaiheessa Safe-boot ja UEFI-tilaa. Ilman näitä Windows Hello ei joko toimi kunnolla tai ollenkaan.

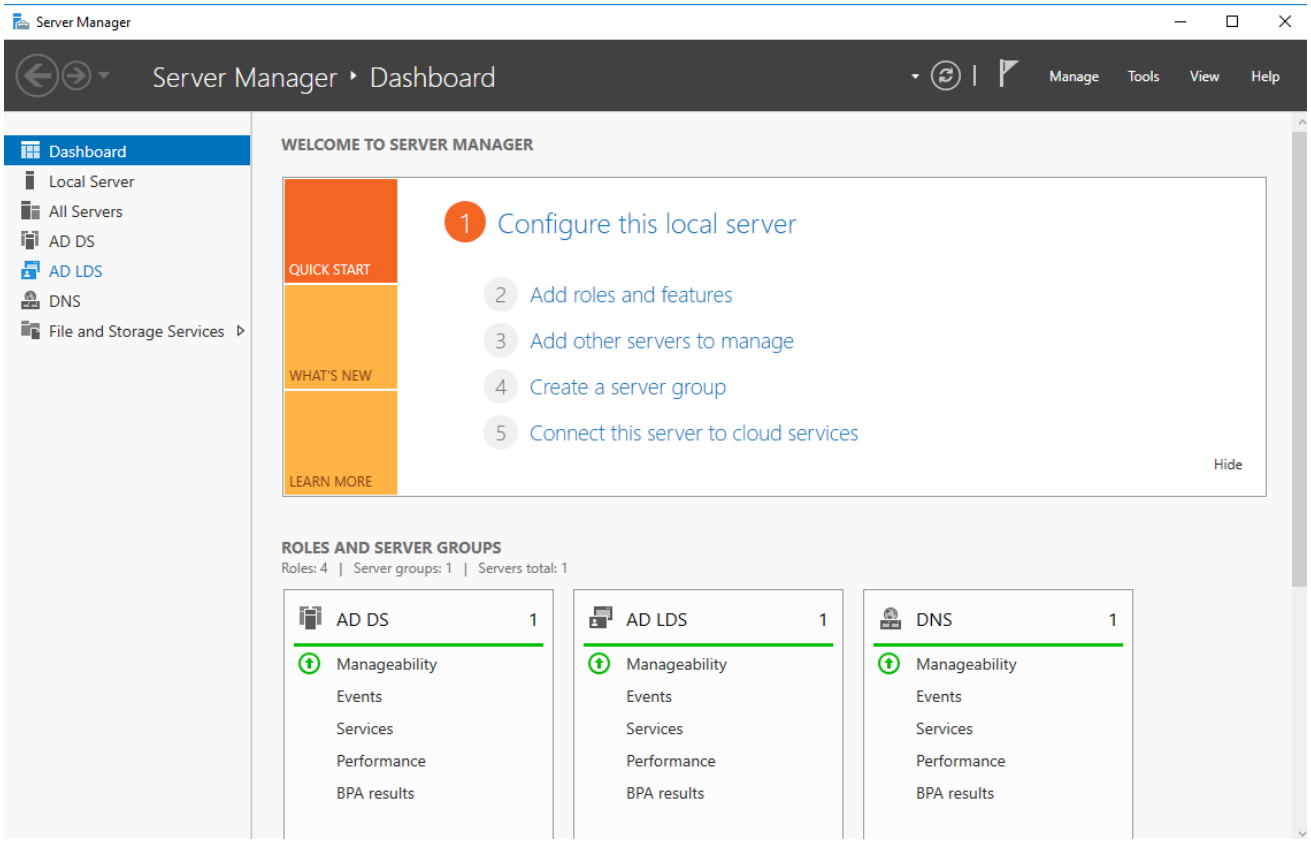
5.1 Palvelimen asennus

Testausympäristön palvelin asennetaan ensin. Asennusvaiheessa käytetään perusasetuksia ilman mitään suurempia muutoksia. Asennuksen jälkeen varmistetaan, että palvelimessa on uusimmat päivitykset.
Asennuksen jälkeen palvelimelle luodaan ensin Forest jonka jälkeen domain. Forestin nimenä toimii BIO ja domain-nimenä toimii bio.local.

Toimintaperiaatteeltaan serverin alkuasennus on hyvinkin samanlainen kuin minkä tahansa muun Windows-laitteen asennus. Ensin tietokone tai serveri käynnistetään avautumaan asennusmedialle. Konemallien mukaan tämä voi tapahtua usealla eri tavalla. Käytössäni olevassa Fujitsun serverissä, tämä tapahtui painamalla del-näppäintä käynnistyksen yhteydessä ja valitsemalla sitten asennusmedia, joka minun tapauksessani oli USB-tikku käynnistysvalikosta. Asennusmediassa oli hyvin selkokieliset ohjeet ja

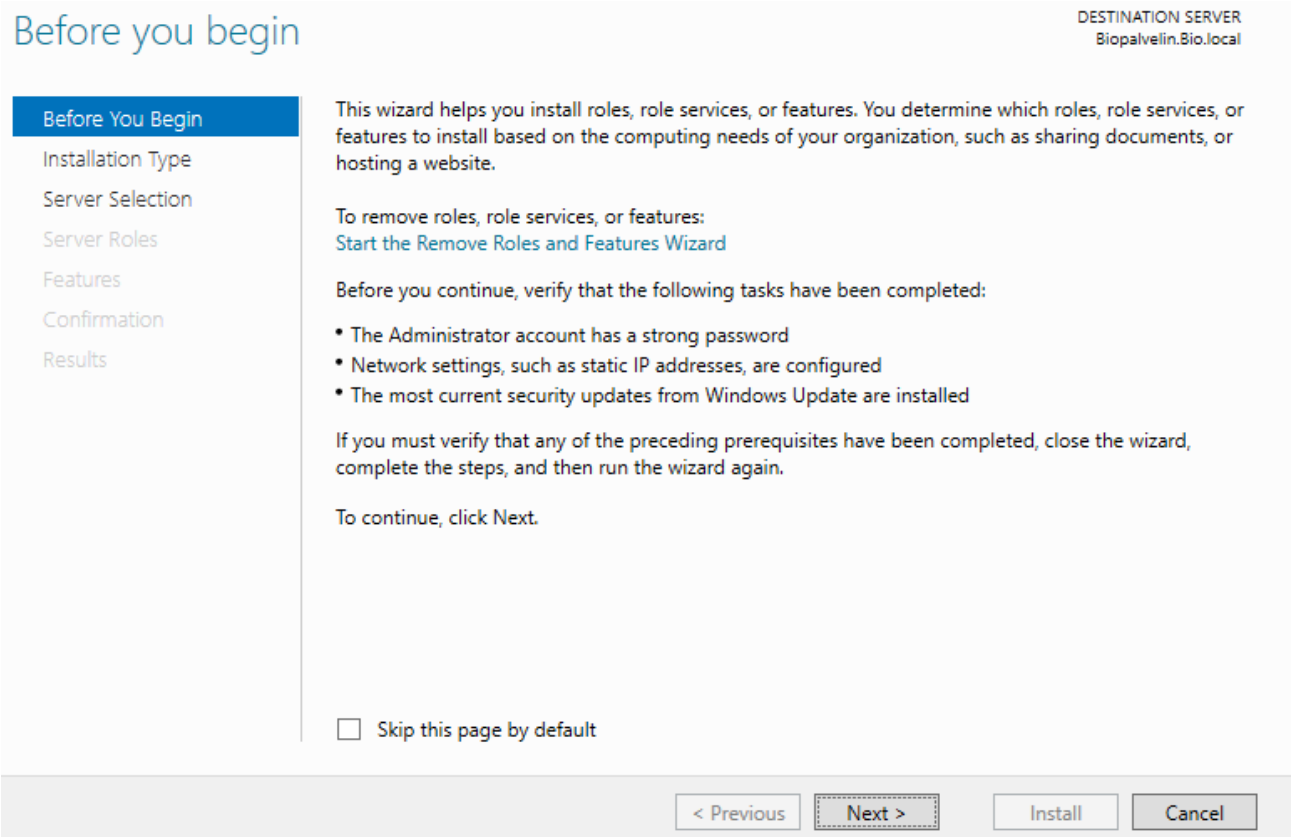
niitä kun seurasi niin oli serveri valmis käytettäväksi hyvinkin vaivattomasti ja nopeasti. Uudelleenkäynnistyksen jälkeen syötetään järjestelmänvalvojalle salasana ja varmistetaan, että järjestelmässä on uusimmat päivitykset ja korjaukset sisällä.

Tämän jälkeen päästään sitten itse varsinaisen serverin rakenteluun. Jokaisesta serveristä löytyy Server Manager-niminen sovellus, jonka avulla voi asentaa erinäisiä rooleja ja ominaisuuksia serverille, kuten esimerkiksi AD DS ja AD LDS roolit.



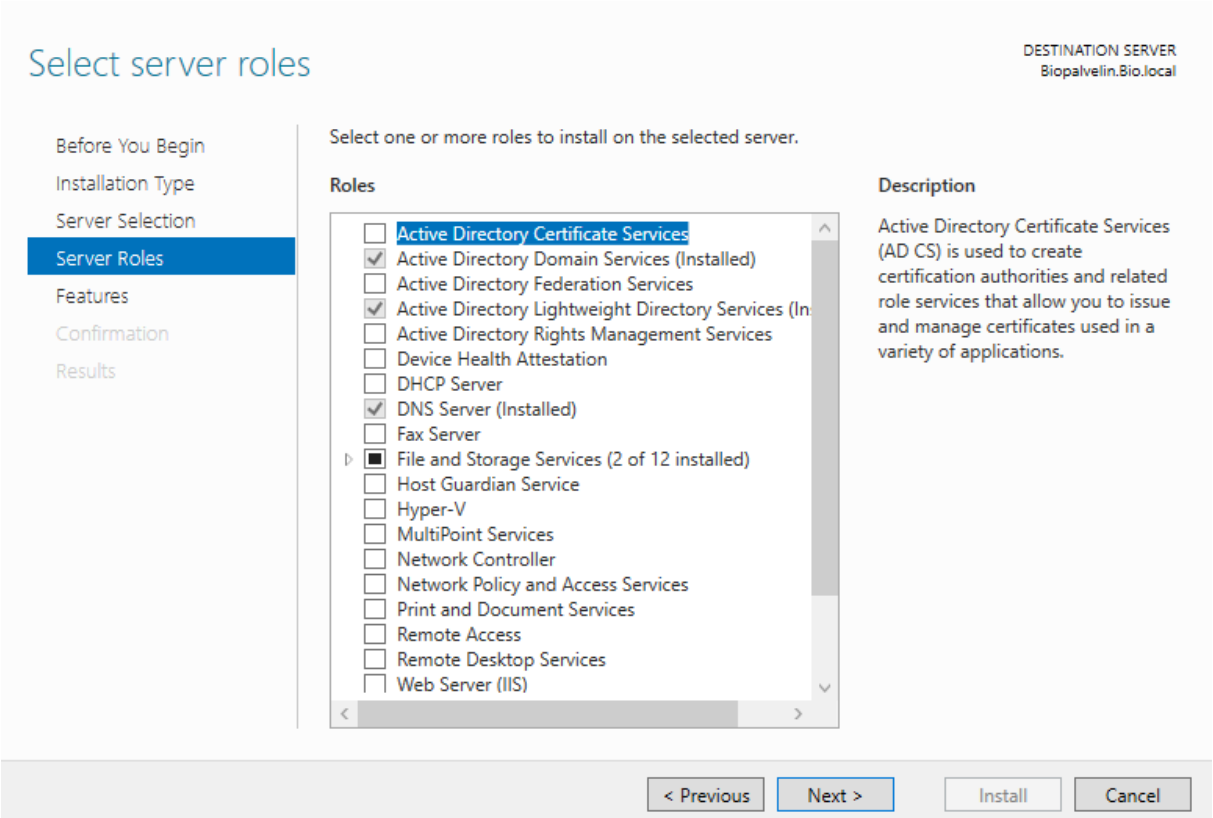
KUVA 6. Server Manager aloitusnäkymä.

Server manager-sovelluksen Dashboard -näkymästä päästään rakentamaan serveriä omien tarpeiden mukaan. Dashboardin sisältä löytyvillä ohjatuilla työkaluilla on helpohkoa pystyttää sellainen serveri, jota tarvitaan. Opinnäytetyötä ajatellen tämä ei kumminkaan ole se tärkein osa, siksi tulen käymään läpi vain oleelliset asiat opinnäytetyötä ajatellen.



KUVA 7. Add Roles and Features-asentajan aloitusnäkymä.

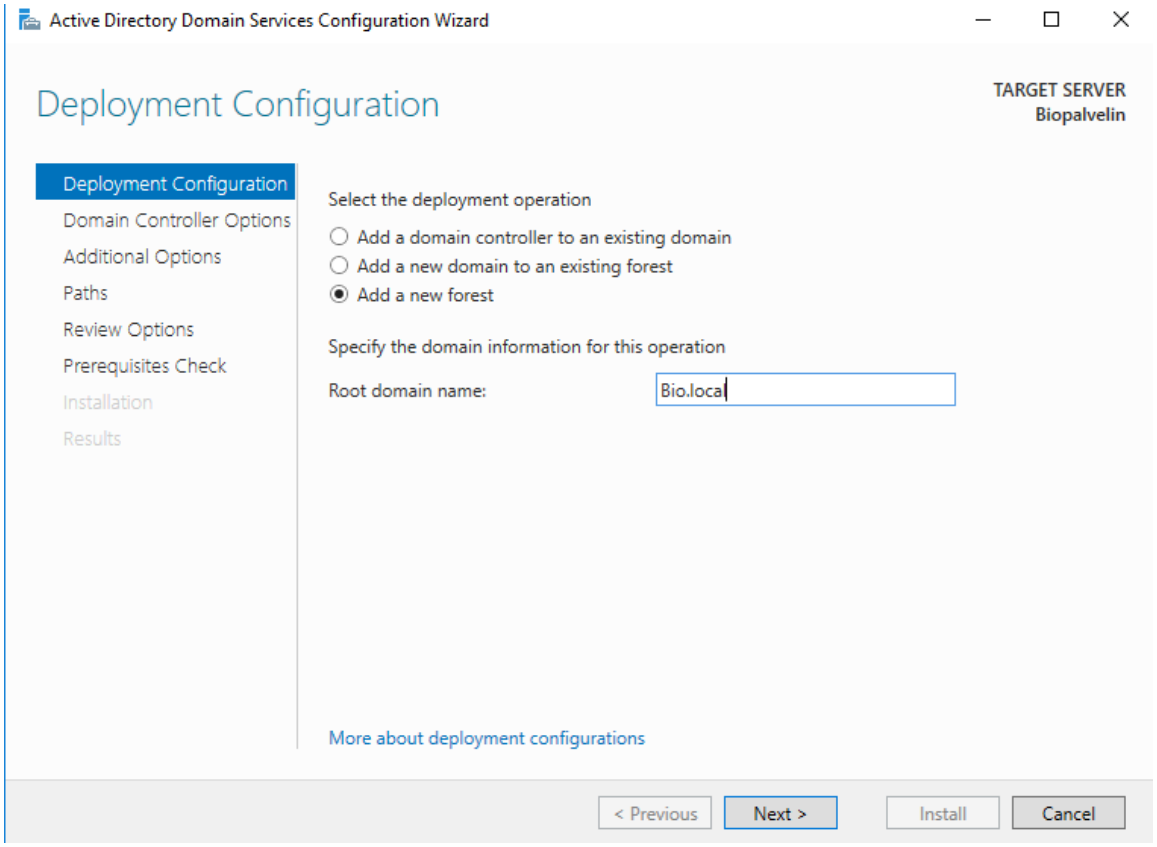
Server manager Dashboard -sovelluksen toinen osio on opinnäytetyön kannalta tärkein osa Server manageria. Sen tarjoaman ohjeistetun asennuksen avulla asennetaan tarvittavat roolit ja ominaisuudet opinnäytetyötä ajatellen. Ennen niiden asentamista pitää tosin määrittää se, mille serverille ne asennetaan. Opinnäytetyössä on tosin vain yksi serveri käytössä, joten valinta on sinänsä itsestään selvä.



KUVA 8. Roolien valinta.

Seuraavaksi valitaan mille serverille rooleja ja ominaisuuksia asennetaan. Tämä on oleellista silloin, jos verkosta löytyy useampi serveri. Normaalissa tilanteessa servereille yleensä asennetaan vain pari roolia, jotta kokonaisuus pysyy stabiilina ja eikä kaadu kokonaan, mikäli yksi serveri lakkaisi toimimasta.

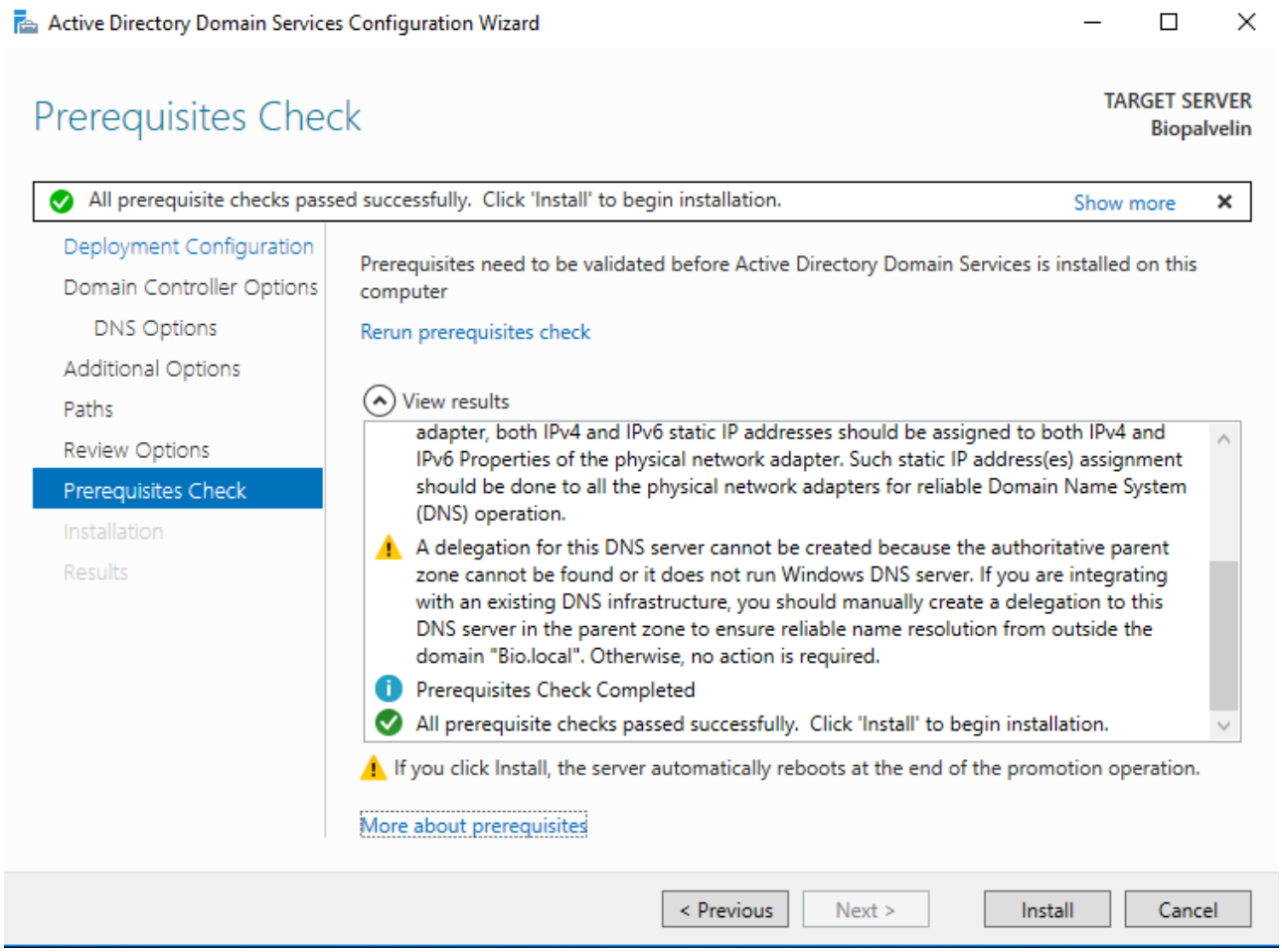
Tässä opinnäytetyössä tosin tämä ei ole tarpeellista. Opinnäytetyötä ajatellen serverille asennetaan seuraavat roolit ja ominaisuudet: Active Directory Domain Services, Active Directory Lightweight Directory Services ja DNS Server. Features-puolelta valitaan vielä biometrinen vaihtoehto.



KUVA 9. Forest-nimen luonti.

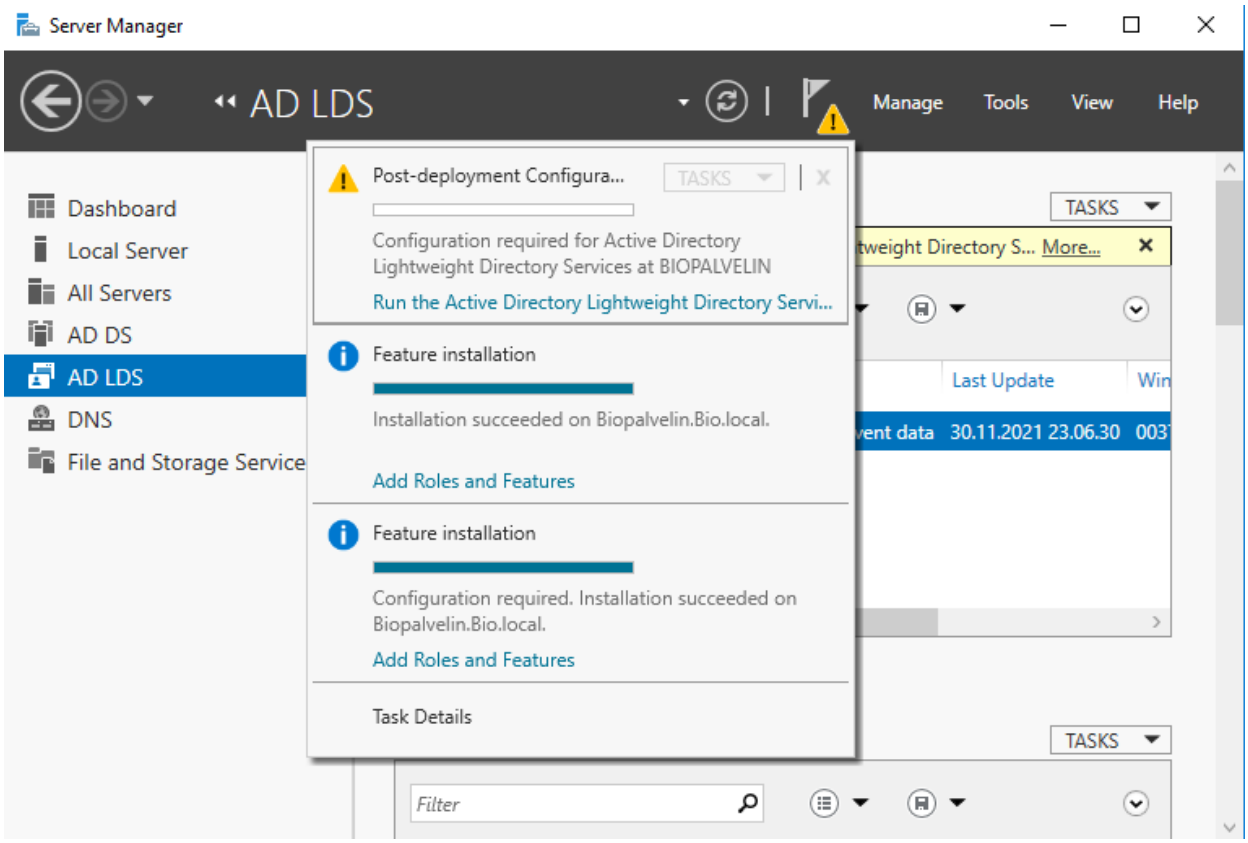
Roolien ja ominaisuuksien valinnan jälkeen määritellään niiden tehtävät. Ensimmäisenä vuorossa ovat AD DS- ja AD DSL-roolit.

Näiden roolien asennus on alussa tärkeää Forestin nimeämisen aikana ja pääsalasanan luonnissa. Muuten asennus viedään läpi perusasetuksilla, joihin kuuluu muun muassa lokitiedostojen tallennuspaikka.



KUVA 10. Asennuksen yhteenveto.

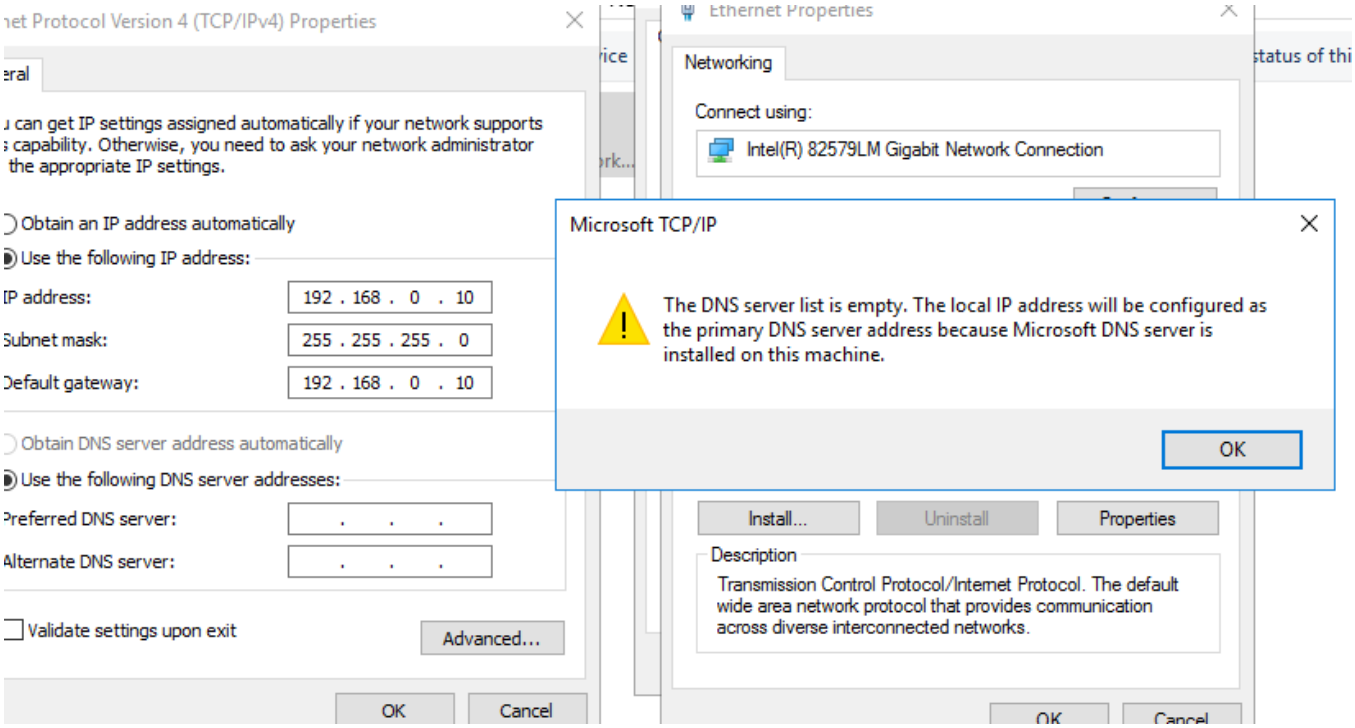
Määrittelyiden jälkeen on viimeinen tarkistus, jossa opastava asennus käy läpi, tuleeko asennus onnistumaan, mikäli asennus ei onnistuisi niin asentaja osaa yleensä kertoa myös miksi näin kävi.



KUVA 11. AD LDS jälkiasennus Server Manager-sovelluksessa.

Sitten tarvitaan vielä AD LDS, jonka avulla voidaan ohjata Domain services-moduuli.

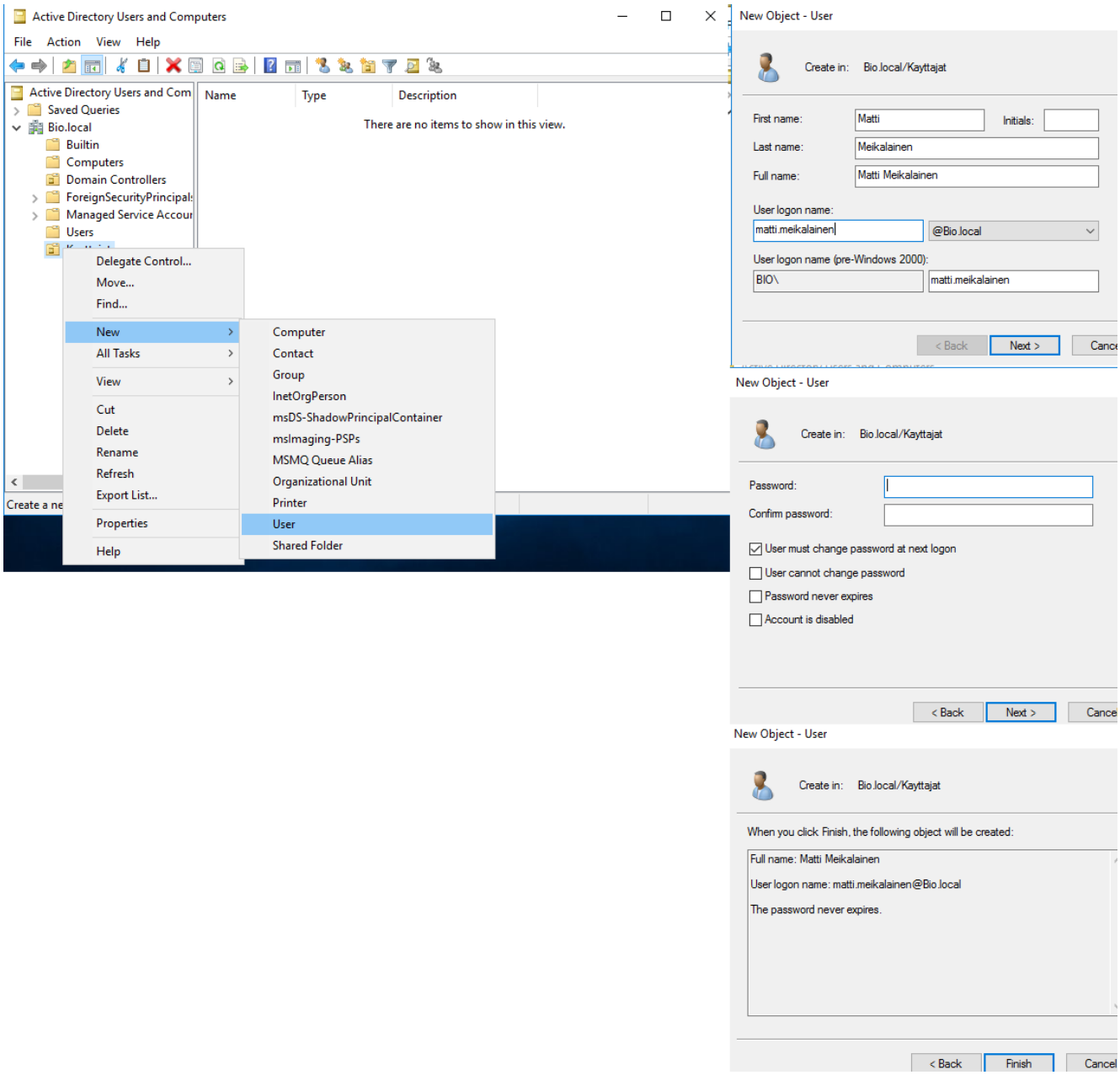
Asennuksen jälkeen osa rooleista tarvitsee vielä jälkiasennuksen. Opinnäytetyössä ainut rooli, joka tarvitsee jälkiasennuksen, on AD LDS-rooli. Tosin sekin viedään läpi perusasetuksia käyttäen opinnäytetyötä ajatellen.



KUVA 12. IP asetuksien määritys palvelimella.

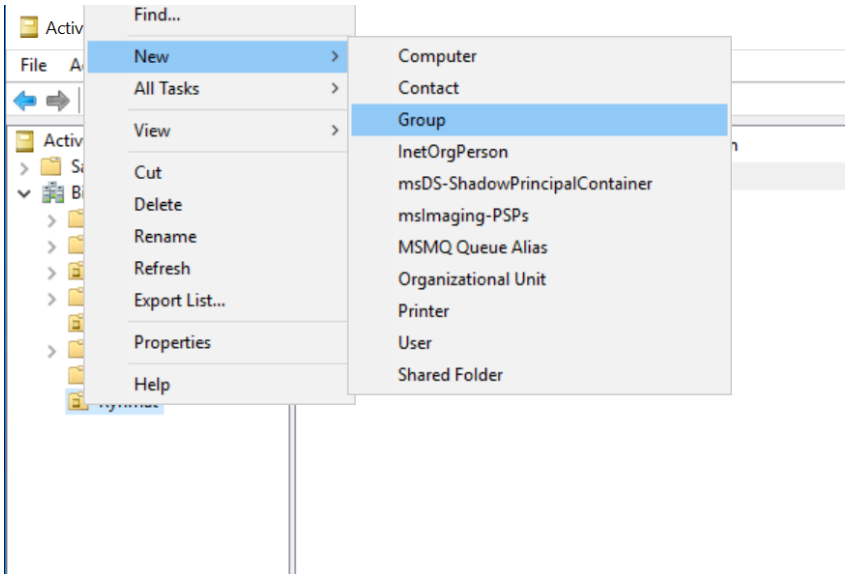
Lopuksi palvelimelle laitetaan vielä IP-asetukset kuntoon. Normaalisti IP asetukset ovat ensimmäisiä, jotka laitetaan kuntoon, mutta ne voidaan myös jälkikäteen laittaa ilman suurempaa ylimääräistä työtä, joka koostuu lähinnä ylimääräisestä uudelleenkäynnistyksestä.

Nyt kun palvelimen puolelta on alustavasti kaikki valmiina, voidaan ryhtyä itse testausta koskeviin toimenpiteisiin.



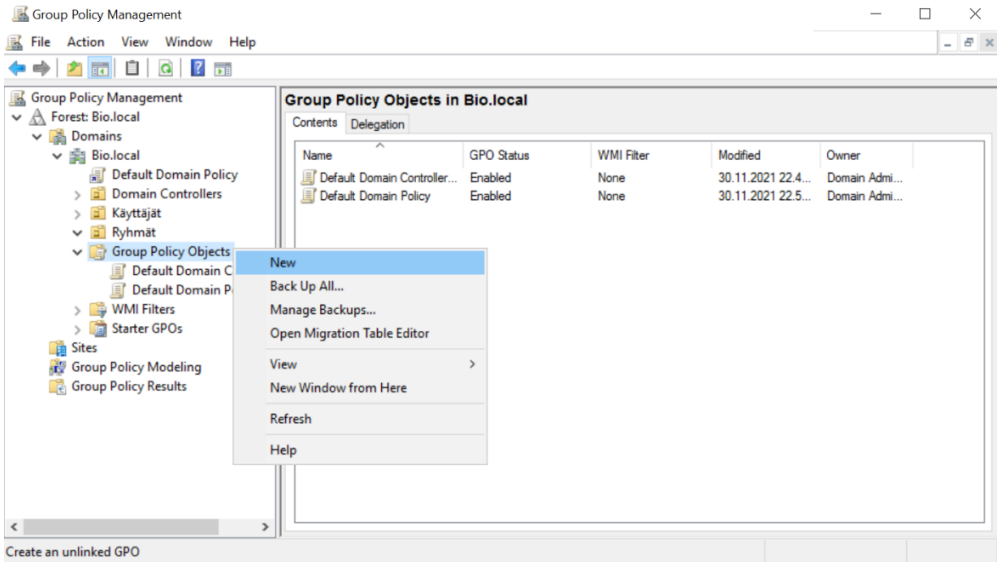
KUVA 13. Käyttäjän luonti.

Palvelimelle luodaan ensin peruskäyttäjä Active Directory Lightweight Domain Sercices-roolin Active Directory Users and computers-ohjelmalla. Käyttäjänä toimii Matti Meikäläinen.



KUVA 14. Ryhmän luonti.

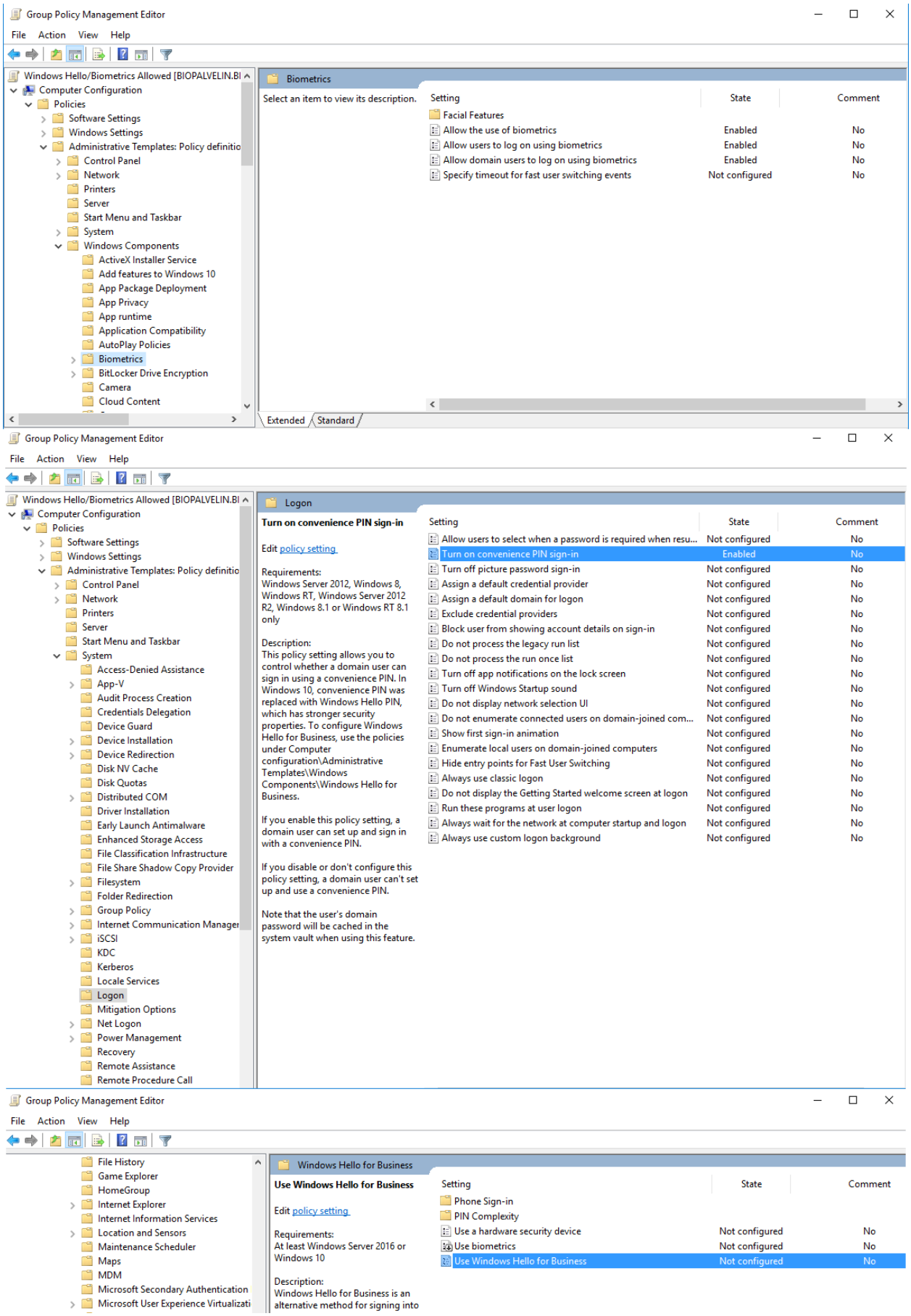
Kun käyttäjät on luotu, luodaan seuraavaksi ryhmä, johon biometriikan käytön sallivat asetukset liitetään. Opinnäytetyössä voisi periaatteessa jättää kokonaan ryhmien luonnin tekemättä, koska testitilejä on vain yksi. Toiminta ei olisi kuitenkaan järkevää, jos käyttäjiä on enemmän, sillä ryhmien käyttö on paljon kätevämpää organisoinnin kannalta.



KUVA 15. Group Policy-objektin luonti.

Ryhmän luonnin jälkeen rakennetaan vielä ryhmäkäytäntöön oikeat asetukset kuntoon, jotta Windows Hello voidaan aktivoida ja ottaa käyttöön käyttäjän puolella group policy management-ohjelmalla, joka on osa AD LDS-roolia. Group policyn, eli ryhmäkäytännön toimeenpano aloitetaan luomalla ensin group policy-objekti, jonka sisälle rakennetaan ne asetukset, joita kyseinen objekti tulee tekemään, oli

se sitten webbiselaimen kotisivun asettaminen tai tässä tapauksessa biometriikan kannalta tarvittavien asetuksien muutto.

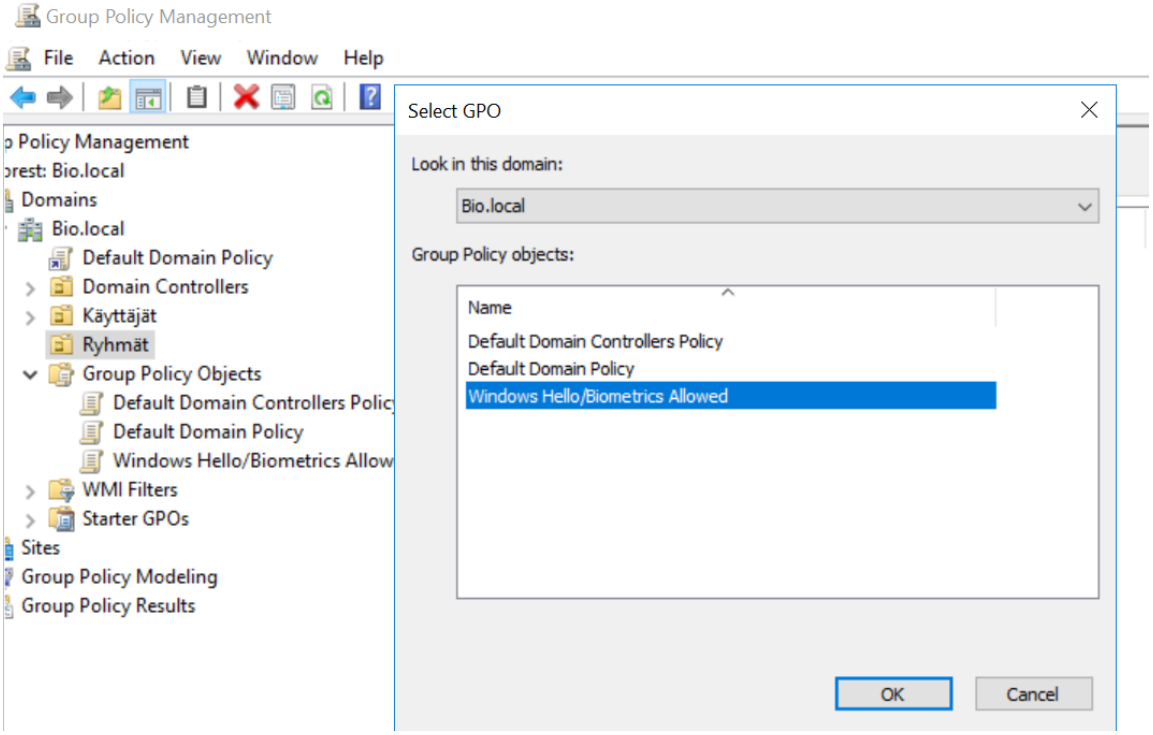


KUVA 16. Biometriikan asetukset.

Luodussa group policy-objektissa valitaan kuvassa 16 näkyvät asetukset kuvan mukaan.

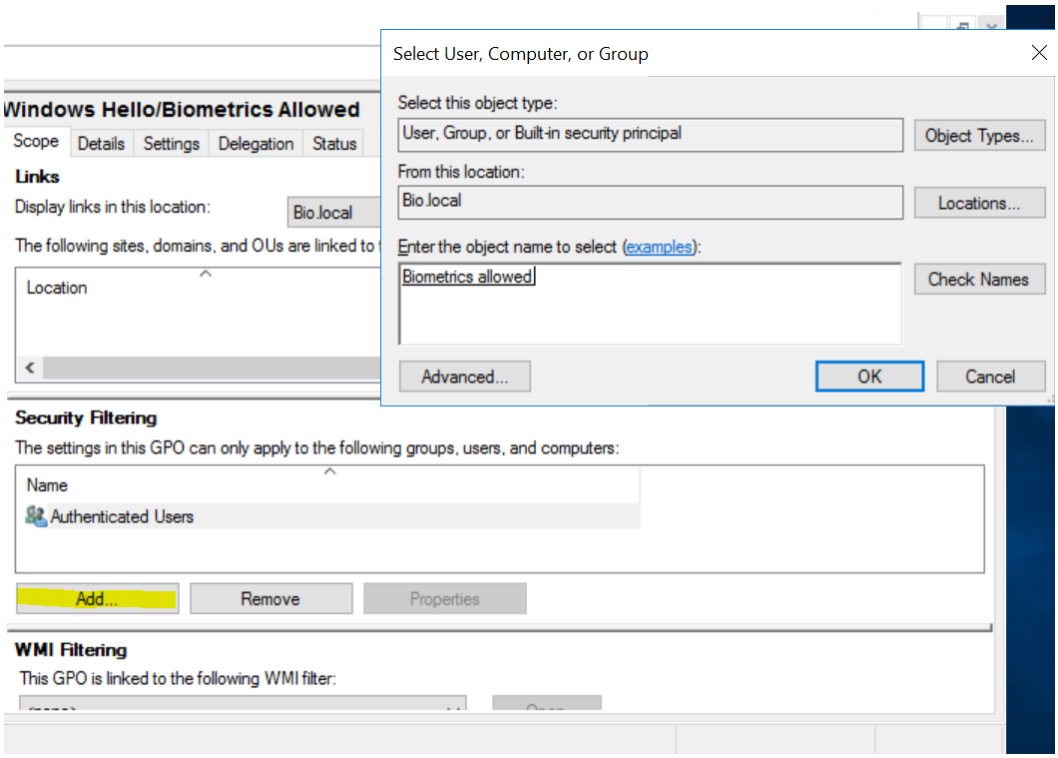
Yllä oleva kuva 16 esittää seuraavat neljä toimintoa järjestyksessä ylhäältä alas. Sallitaan biometrinen tunnistautuminen koneelle kirjauduttuessa. Sallitaan biometrinen kirjautuminen domainalueella.

Sallitaan PIN koodin käyttö kirjautumiseen, mikä on välttämätön Windows Hello -sovelluksen toiminalle. Viimeiseksi määritellään, että biometrisiä toimintoja ei ole pakko käyttää, mikäli ei halua. Tämä osio on kriittinen biometrian toiminnan varmistamiseksi kohteena olevassa tietokoneessa, sillä jos toiminto olisi aktivoitu koneella, siihen ei voisi kirjautua muuta kuin biometrisellä tavalla mikä tietysti estäisi käyttäjää aktivoimasta biometristä tunnistautumista, koska ei pysty koneelle kirjautumaan.



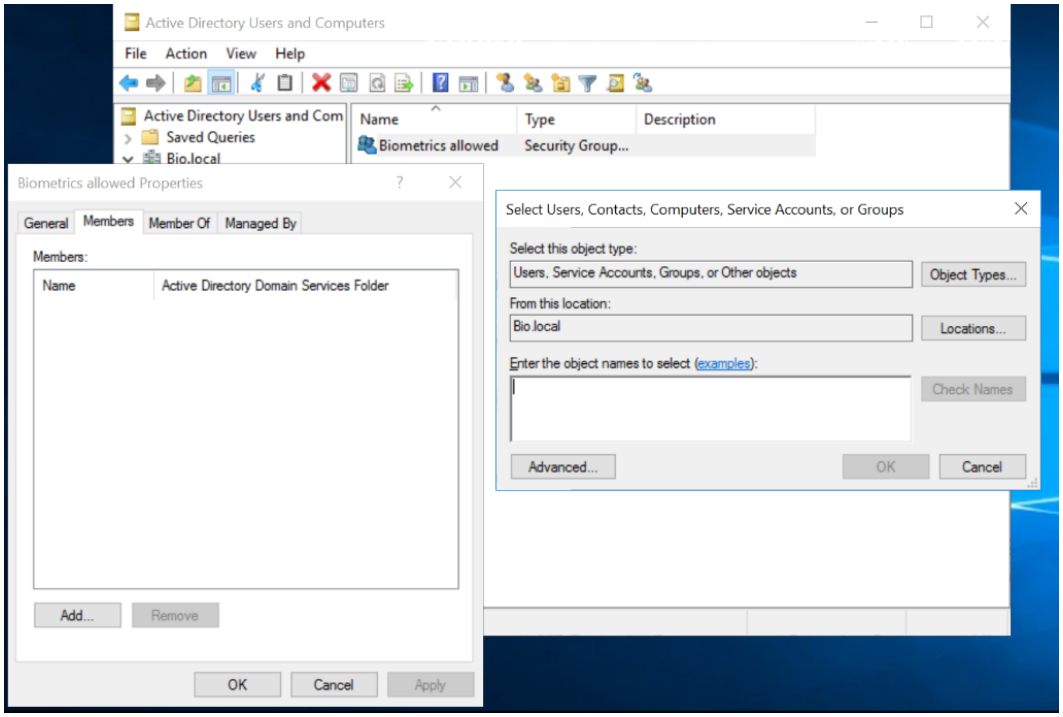
KUVA 17. Linkitetään Tehty GPO

Nyt kun käytettävä policy on valmis, on aika linkittää se tarvittaviin ryhmiin. Tämä aloitetaan linkittämällä tehty group policy ryhmät kansioon. Näin ollen kaikilla ryhmät kansion alla olevilla kohteilla on mahdollisuus käyttää kyseistä group policyä, mikäli se heille määritetään.



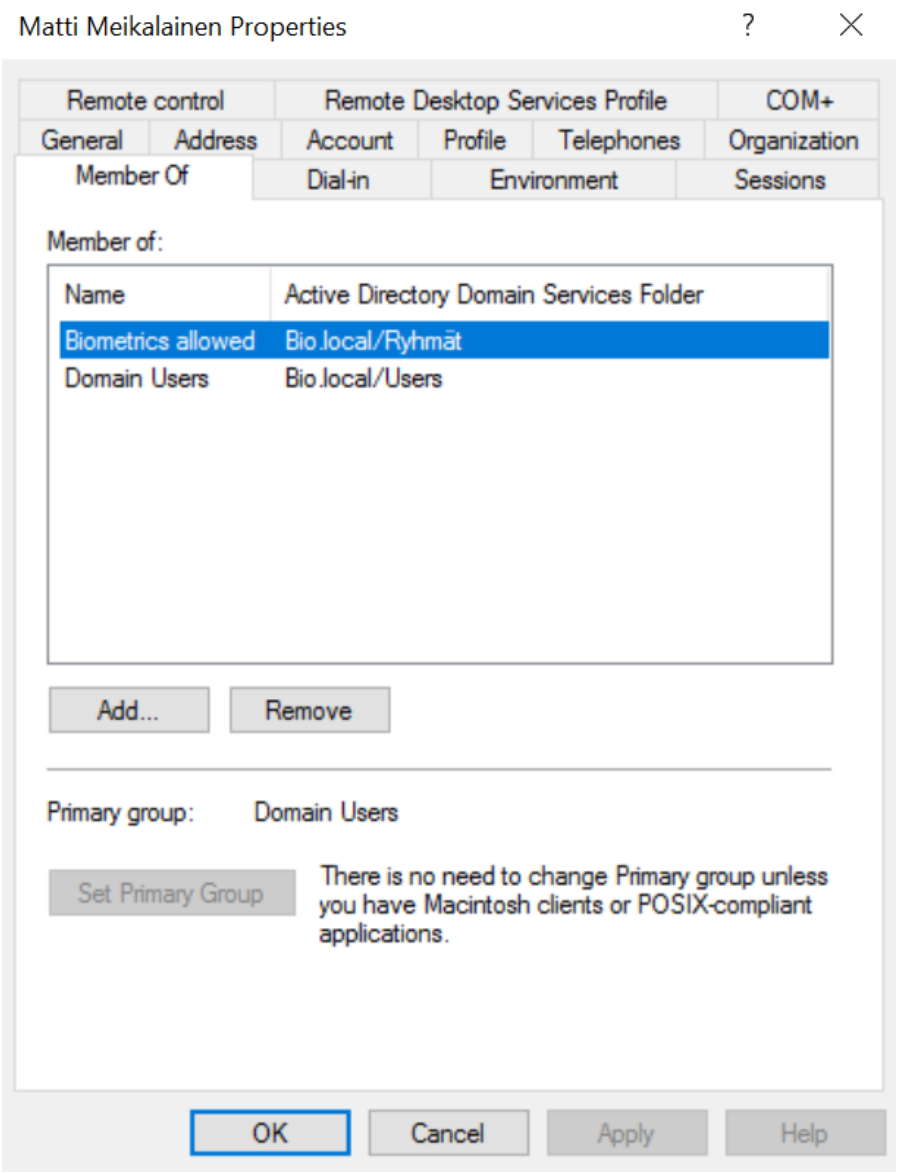
KUVA 18. GPOn linkitys itse käyttäjäryhmään

Lopuksi linkitetään vielä luotu GPO-käyttäjäryhmälle.



KUVA 19. Käyttäjien lisäys Biometrics allowed -käyttäjäryhmään.

Group policy on luotu ja nyt myös linkitetty Biometrics allowed -ryhmään, nyt palvelimen puolelta puuttuu vain käyttäjien yhdistäminen kyseiseen ryhmään, jonka jälkeen palvelin on valmis testiä varten.



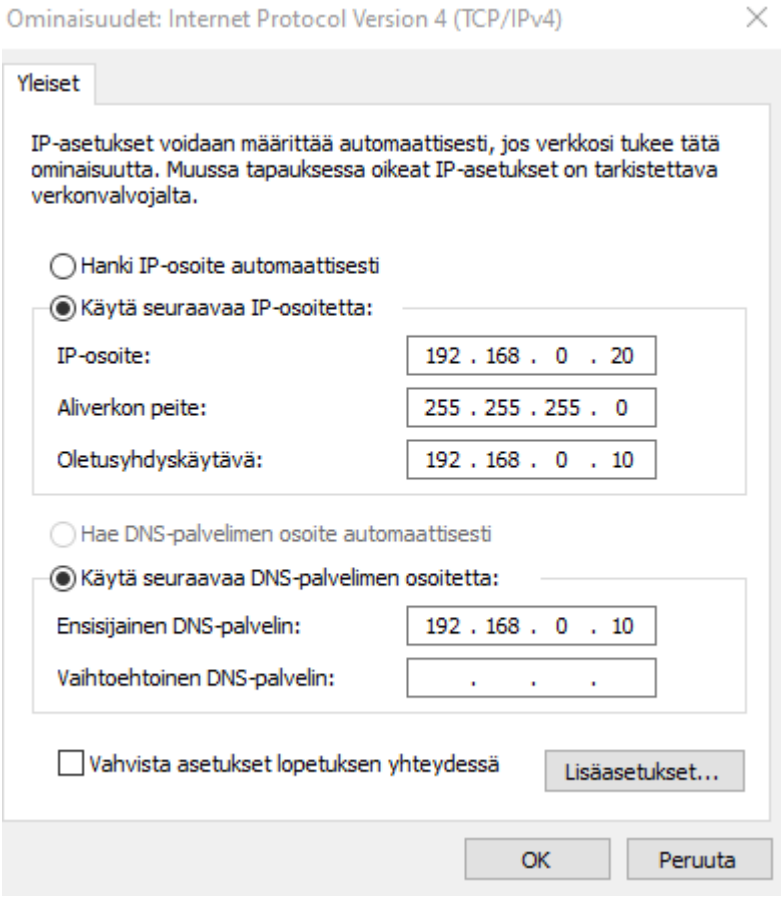
KUVA 20. Käyttäjä Matti Meikäläisen ryhmät

Kun käyttäjät on lisätty ryhmään, varmistetaan vielä yhdeltä käyttäjältä, että määritetty ryhmä löytyy. Lopuksi käynnistetään palvelin vielä varmuuden vuoksi uudelleen ja varmistetaan viimeisimmät päivitykset. Mahdollisten päivityksien jälkeen käynnistetään vielä kertaalleen uudelleen.

5.2 Clientin valmistaminen

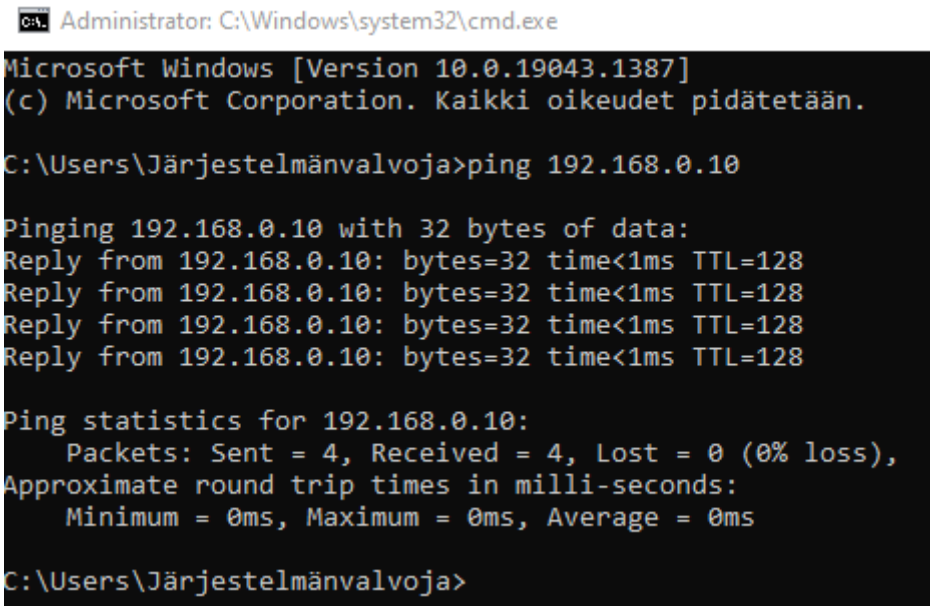
Client-laitteen valmistelussa ei tarvitse ottaa paljon asioita huomioon. Asiat mitkä pitää huomioida ovat, että laitteessa on jokin toimivista biometrisistä tunnestautumisjärjestelmistä. Käytettävässä testilaitteessa tunnistautumistapana toimii sormenjälkitunnistin.

Kannattaa myös varmistaa, että laitteessa on uusin Windows-versio. Testiä helpottamaan luodaan laitteisiin myös paikallinen järjestelmänvalvojan tunnus mahdollisten ongelmien ratkontaan.



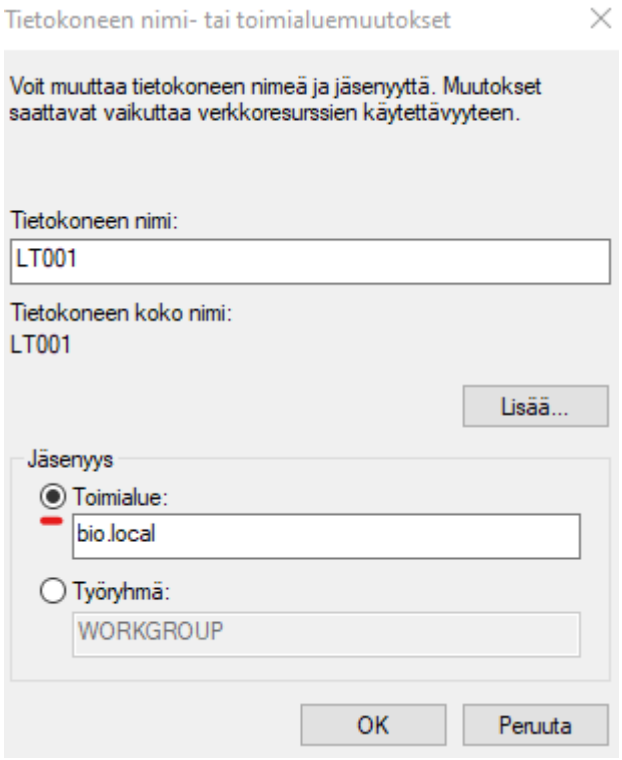
KUVA 21. IP-Asetuksien määritys

Aloitetaan liittämällä tietokone samaan verkkoon, jossa palvelin on. Sitten vielä IP-asetukset vastaamaan palvelimen IP-asetuksia, jotta tietokone kykenee ylipäätänsä kommunikoimaan palvelimen kanssa.



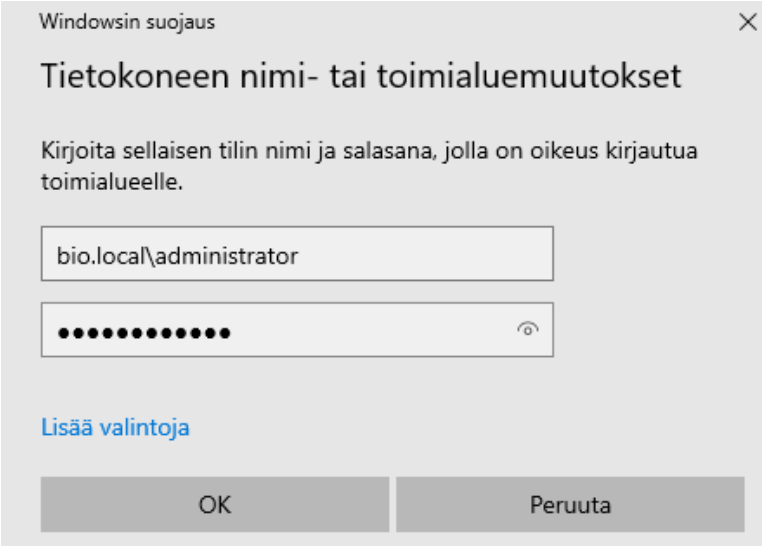
KUVA 22. Ping testaus Bio palvelimeen

Määrityksen jälkeen tehdään vielä nopea ping-testi palvelimelle ja varmistetaan että kommunikaatio toimii koneen ja palvelimen välillä.



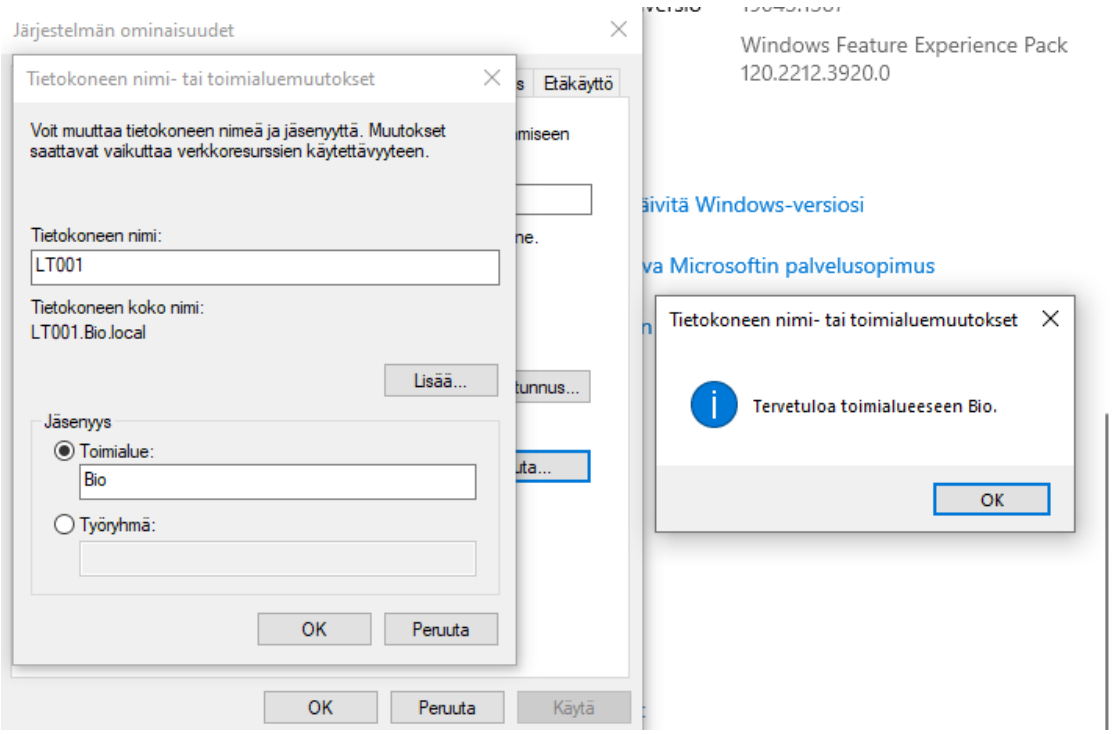
KUVA 23. Toimialueelle nosto.

Onnistuneen Ping testauksen jälkeen nostetaan tietokone Bio.local domainiin. Nosto tapahtuu käyttämällä palvelimella olevia toimintaan tarkoitetulla tilillä.



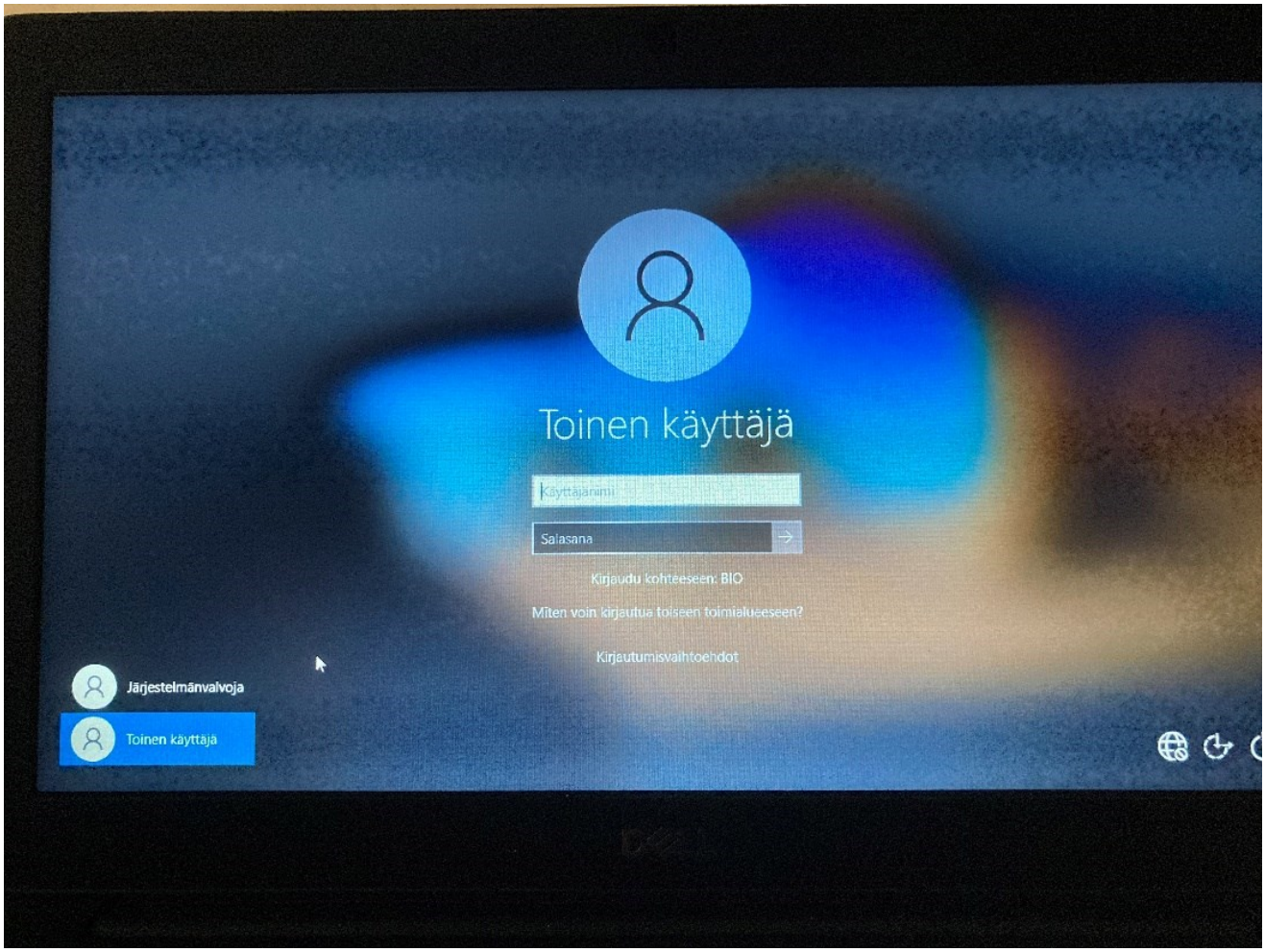
KUVA 24. Toimialueen nostoprosessi.

Opinnäytetyössä käytin palvelimen järjestelmänvalvojan tiliä. Tämä on turvallisuuden kannalta huono tapa, mutta merkitystä opinnäytetyölle tällä toiminnalla ei ole.



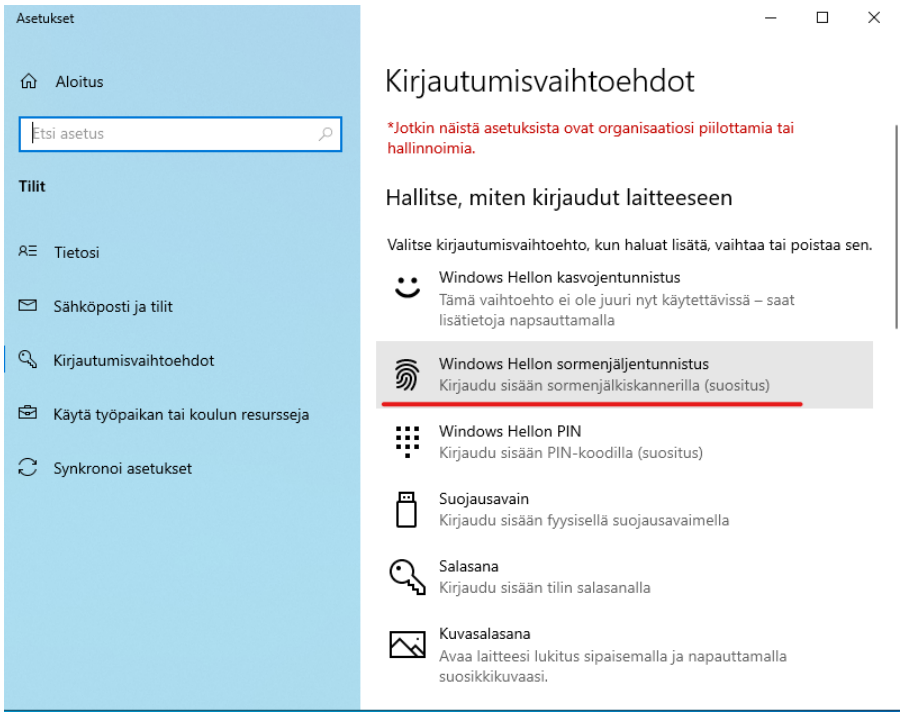
KUVA 25. Tervetuloa toimialueelle.

Kun tiedot on syötetty oikein, tuodaan tietokone toimialueelle onnistuneesti. Tietokone pitää vaan käynnistää uudelleen viimeistelyä varten.



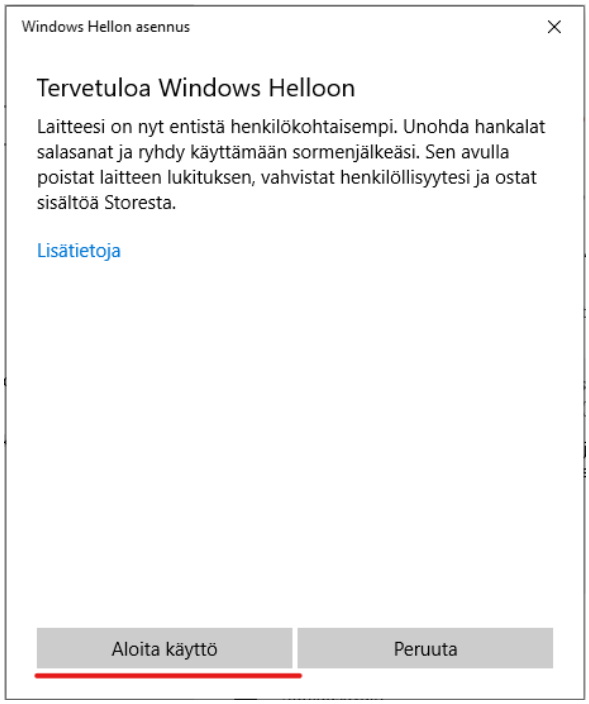
KUVA 26. Kirjautuminen domaintilillä

Tietokoneen uudelleen käynnistyksen jälkeen on mahdollista kirjautua sisään Matti Meikäläisen tilillä. Onnistuneen kirjautumisen jälkeen voidaan aloittaa määrittämisen viimeinen vaihe ennen testausta, biometrisen kirjautumisen aktivointi.



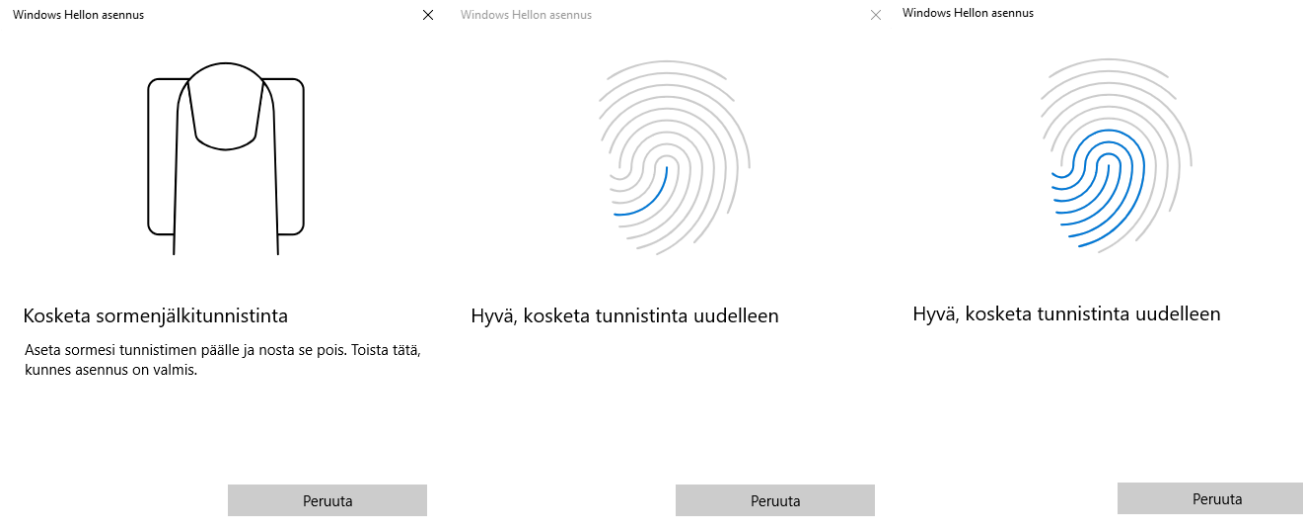
KUVA 27. Windows Hello-sormenjälkitunnistus

Aktivointi tapahtuu menemällä tietokoneen asetuksiin ja testauslaitteisto huomioon ottaen otetaan käyttöön sormenjälkikirjautuminen, sillä kyseisessä tietokoneessa ei ollut muita biometrisiä kirjautumisvaihtoehtoja.



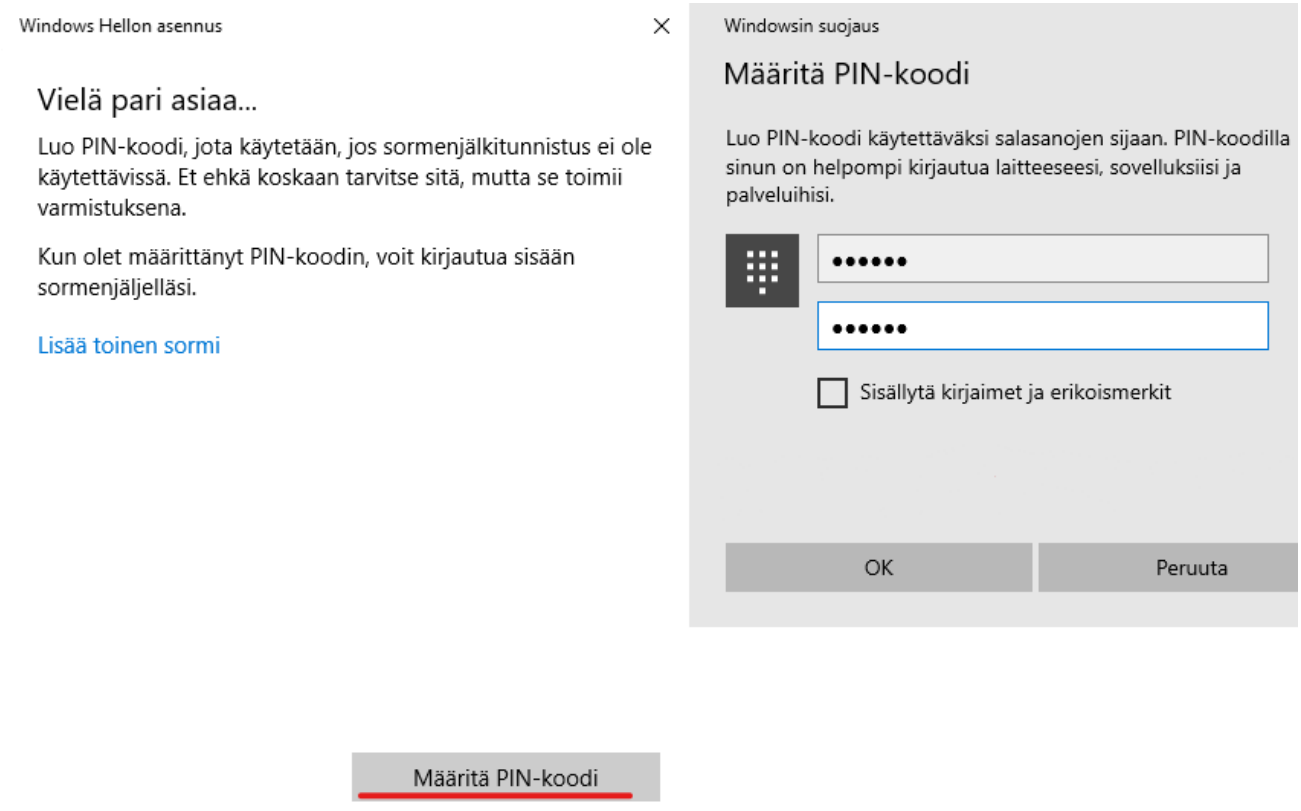
KUVA 28. Sormenjäljen määritys.

Windows Hellon-asennusavustaja avustaa hyvin selkeällä kielellä mitä tulee milloinkin tehdä, jotta määritys onnistuu.



KUVA 29. Sormenjäljen rekisteröinti sisään kirjautuneelle tunnukselle

Käyttö aloitetaan valitsemalla sormi, jota halutaan käyttää tietokoneen avaamisen ja asettamalla tämä sormi sitten tietokoneen anturiin ja seuraamalla näytöllä näkyviä ohjeita.

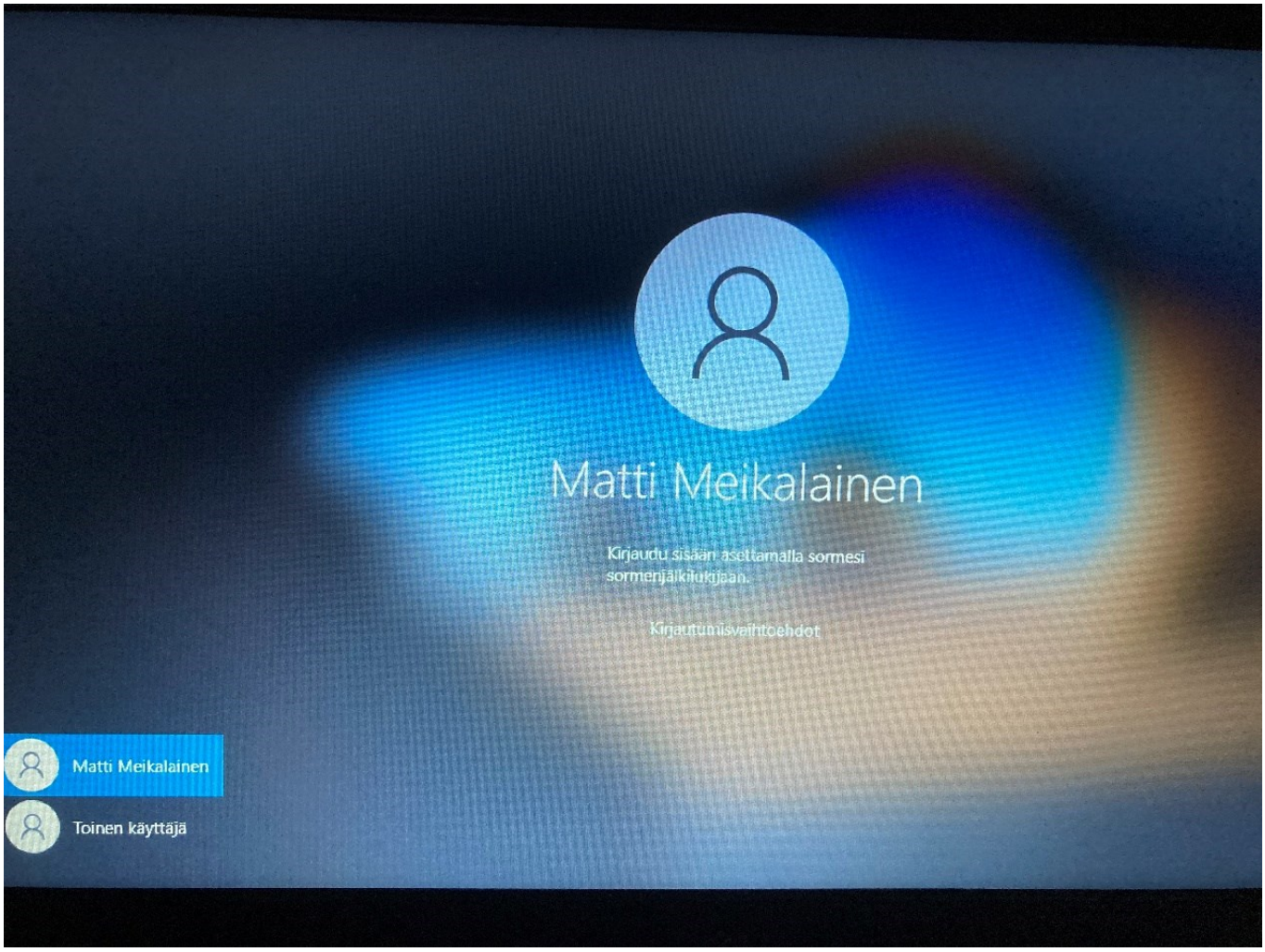


KUVA 30. PIN-koodin määritys

Kun sormenjälki on tarpeeksi kattavalla tarkkuudella annettu laitteelle pitää vielä tilille linkittää PIN-koodi.

Lopuksi tietokone käynnistetään uudelleen. Sen jälkeen kaiken pitäisi olla valmista testausta varten.

5.3 Biometrisen kirjautumisen testaus



KUVA 31. Kirjautuminen.

Testaus toimivuuden varmistamiseksi ei tässä tilanteessa nyt siis muuta tarvitse kuin että tietokone on takaisin käynnistysruudussa ja varmistetaan että tietokone pyytää sormenjälkeä kirjautumiseen.

KUVA 32. Onnistunut testi.

Sormi painetaan anturiin ja tietokone tunnistaa tämän sormen kuuluvan Matti Meikäläisen tilille ja kirjaa hänet sisään domaintunnuksilla. Testi siis onnistui.

6 LOPPUPÄÄTELMÄT

Työn suunnitteluvaihe vaati paljon aikaa, mutta itse toteutus onnistui lopulta suhteellisen helposti ilman suurempia ongelmia.

Windows Hello-järjestelmä on helppo liittää jo olemassa oleviin käyttäjätietokantoihin, sikäli mikäli tietokannat ovat perustasolla, eikä sieltä löydy kolmannen osapuolen järjestelmiä, jotka sekoittaisivat Windows Hello-järjestelmän toimintaa.

Moraaliselta näkökulmalta ajatellen biometristen tietojen kerääminen alaikäisiltä on ehkä hieman kyseenalaista, mutta kirjautuminen käyttäen näitä tietoja on paljon nopeampaa ja helpompaa. Tietojen joutuminen vääriin käsiin on myöskin huomattavan vaikeaa sillä varkaan pitäisi ensin saada laite fyysisesti omaan hallintaansa, sen jälkeen kirjautua vähintään järjestelmänvalvoja tasoisilla tunnuksilla sisään laitteeseen. Vasta tämän jälkeen olisi hänellä mahdollisuus saada biometriset tiedot haltuunsa, jotka ovat vahvasti kryptattuja. Jos tunkeutuja haluaa usealta henkilöltä kryptatut tiedot, joutuu hän tekemään saman asian jokaisella laitteella erikseen.

Laillisesti on oikeus kerätä biometrisiä tietoja alaikäisiltä (alle 12–13-vuotias) huoltajan kirjallisella suostumuksella. (Europa.eu 2021c).

Käyttäjän biometriset tiedot pysyvät paikallisesti kryptattuina vain ainoastaan kyseisessä laitteessa, jossa käyttäjä on ottanut järjestelmän käyttöönsä.

Alun perin käytössä oli kaksi testikonetta, mutta toisessa testikoneista sormenjälkianturi oli epävarma, joten käytössä oli vain yksi testikone. Muita ongelmia ei esiintynyt opinnäytetyötä tehdessä.

Jos käyttäjä haluaa käyttää ominaisuutta useissa laitteissa, joutuu hän aktivoimaan ominaisuuden aina uudelleen joka laitteelle. On myös mahdollista, että käyttäjän informaatio katoaa tietokoneesta, jota hän on käyttänyt, useimmiten näihin tilanteisiin päädytään laitteen tilan puutteen, uudelleen asennuksen tai jonkin muun ongelmatilanteen vuoksi, jolloin korjaaminen johtaa käyttäjän tietojen katoamiseen kyseisetä laitteesta.

LÄHTEET

Europa.eu. 2021a. *Milloin tietojenkäsittely on sallittua?* Saatavissa: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm#shortcut-7. Viitattu 21.3.2022

Europa.eu. 2021b. *Avoin tiedotus tietojen käsittelystä*. Saatavissa: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm#shortcut-9. Viitattu 21.3.2022

Europa.eu. 2021c. *Tietojenkäsittelyyn suostuminen*, Saatavissa: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm#shortcut-8. Viitattu 8.3.2022

European Commission. *What does data protection 'by design' and 'by default' mean?* Saatavissa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en. Viitattu 21.3.2022

Findbiometrics. *Vein Recognition* Saatavissa: https://findbiometrics.com/solutions/vein-recognition/. Viitattu 15.11.2021

Finlex. *1050/2018 Tietoyhteiskunnan palvelujen tarjoamiseen lapselle sovellettava ikäraja.* Saatavissa: https://finlex.fi/fi/laki/alkup/2018/20181050. Viitattu 21.3.2022

HAMK. 2020. *digipediaohjeet* Saatavissa: https://digipedaohjeet.hamk.fi/ohje/mita-ovat-henkilotiedot-ja-erityiset-arkaluonteiset-henkilotiedot/. Viitattu 21.3.2022

icao. Doc 9303, *kappale 3.1 sivu 4* Saatavissa: https://www.icao.int/publications/Documents/9303_p9_cons_en.pdf. Viitattu 2.11.2021

Jirik, P. Phonexia. 2021. *5 Popular Types of Biometric Authentication: Pros and Cons* Saatavissa: https://www.phonexia.com/en/blog/5-popular-types-of-biometric-authentication-pros-and-cons/#:~:text=The%20five%20most%20common%20types,palm%20or%20finger%20vein%20patterns. Viitattu 4.4.2022

Kapko, M & Finnegan, M. Computerworld. 2021. *What is Windows Hello? Microsofts's biometrics security system explained* Saatavissa: https://www.computerworld.com/article/3244347/what-is-windows-hello-microsofts-biometrics-security-system-explained.html. Viitattu 23.11.2021

Lexia. 2018. *Uusi kansallinen tietosuojalaki tarkentaa henkilötietojen käsittelyyn liittyviä velvoitteita*. Saatavissa: https://www.lexia.fi/fi/uusi-kansallinen-tietosuojalaki/. Viitattu: 30.11.2021

Mayhew, S. Biometricupdate. 2012. *Explainer: Hand Geometry Recognition* Saatavissa: https://www.biometricupdate.com/201206/explainer-hand-geometry-recognition. Viitattu 11.11.2021

Microsoft Docs. 2022. *Windows Hello for Business Deployment Prerequisite Overview* Saatavissa: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification. Viitattu 17.11.2021

Monster, B. Plumvoice. *What is voice biometrics* Saatavissa: https://www.plumvoice.com/resources/blog/voice-biometrics/. Viitattu 10.11.2021

Nice. *Voice biometrics* Saatavissa: https://web.archive.org/web/20211204184115/https://www.nice.com/engage/real-time-technology/voice-biometrics/. Viitattu 10.11.2021

Opi Tietosuojaa. *EU:n tietosuoja-asetuksen velvoitteet johdolle* Saatavissa: https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus/. Viitattu: 21.3.2022

Opi Tietosuojaa. *Miten asetus muuttaa henkilötietojen käsittelyä?* Saatavissa: https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus/. Viitattu 21.3.2022

Parmar, M. Bleepingcomputer. 2020. *Windows Hello is now being used by 84% of Windows 10 users*- Saatavissa: https://www.bleepingcomputer.com/news/microsoft/windows-hello-is-now-being-used-by-84-percent-of-windows-10-users/. Viitattu 21.3.2022

Pinto, R. 1kosmos. 2021. *Voice Authentication: How It Works & Is It Secure?* Saatavissa: https://www.1kosmos.com/biometric-authentication/voice-authentication/. Viitattu 10.11.2021

Recogtech. 2021. *Facial Recognition* Saatavissa: https://www.recogtech.com/en/knowledge-base/5-common-biometric-techniques-compared. Viitattu 4.11.2021

Refaces. 2020. *How Facial Recognition works* Saatavissa: https://recfaces.com/articles/how-facial-recognition-works. Viitatttu 4.11.2021

Refaces. 2022. *What are iris and retina scanners* Saatavissa: https://recfaces.com/articles/iris-scanner. Viitattu 2.11.2021

Santolalla, O. Ubisecure. 2021. *The ultimate guide to finger vein biometrics* Saatavissa: https://www.ubisecure.com/authentication/finger-vein-biometrics/. Viitattu 15.11.2021

Steve Symanovich. Norton. 2021. *What is facial recognition? How facial recognition works* Saatavissa: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html. Viitattu 4.11.2021

THL. 2019. *Alaikäisten puolesta asiointi on toteutettava potilastietojärjestelmiin* Saatavissa: https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/-/alaikaisen-puolesta-asiointi-on-toteutettava-potilastietojarjestelmiin. Viitattu 4.4.2022

Tietosuojavaltuutetun Toimisto. *Kun haluat tarkastaa tietosi* Saatavissa: https://tietosuoja.fi/kun-haluat-tarkastaa-tietosi. Viitattu 21.3.2022

Tietosuojavaltuutetun Toimisto. *Tietoturvaloukkaukset* Saatavissa: https://tietosuoja.fi/tietoturvaloukkaukset. Viitattu 21.3.2022

Woodford, C. Explainthatstuff. 2022. *Biometric fingerprint scanners* Saatavissa: https://www.explainthatstuff.com/fingerprintscanners.html. Viitattu 1.11.2021

KUVAT

KUVA 1. Kapasitiivinen skanneri.
Planka, S. 2019 Pixabay, Saatavissa: https://pixabay.com/fi/photos/sormenj%c3%a4lki-sensori-4703841/. Viitattu 19.5.2022

KUVA 3: Visualisointi kasvojen ankkurpisiteistä.
Saatavissa: https://pixabay.com/fi/vectors/tasainen-tunnustamista-kasvohoito-3252983/. Viitattu 19.5.2022

KUVA 4: Kämmen asetettuna lukijaan.
2013, Nuclear Plant Security - Hand Scanner, Flickr,
Saatavissa: https://www.flickr.com/photos/nrcgov/9680484108/in/photostream/. Viitattu 19.5.2022