Toni Soini

IAM-sovelluksen Okta integraatio

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Mobile Solutions

Insinöörityö

1.3.2023

Tiivistelmä

Tekijä:	Toni Soini
Otsikko:	IAM-sovelluksen Okta integraatio
Sivumäärä:	22 sivua
Aika:	1.3.2023
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikan tutkinto-ohjelma
Ammatillinen pääaine:	Mobile Solutions
Ohjaajat:	Osaamisaluepäällikkö Janne Salonen Teknologiajohtaja Lauri Reunanen

---

Tässä projektissa rakennetaan integraatio ServiceNow-alustalla olevalle IAM-sovelluksen ja Okta-järjestelmän väliin. Insinöörityössä hyödynnetään ServiceNow:n sekä työn tilaajan IAM-sovelluksen jo olemassa olevia toimintoja ja työkaluja. Ohjelmointikielenä toimii JavaScript ja järjestelmien välinen kommunikointi suoritetaan REST-rajapintaa hyödyntäen.

Lopputuloksena saamme identiteetin- ja pääsynhallintasovellukselle kyvykkyydet tilata, poistaa ja ylläpitää käyttöoikeuksia Okta-järjestelmään.

Avainsanat: IAM, ServiceNow, Okta, integraatio, pääsynhallinta

---

Abstract

Author:	Toni Soini
Title:	Okta integration for an IAM-application
Number of Pages:	22 pages
Date:	1 March 2023
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Mobile Solutions
Supervisors:	Janne Salonen, Responsible Supervisor Lauri Reunamäki, Chief Technical Officer

---

In this thesis we will be creating an integration between ServiceNow and Okta plaforms. This will be built for an existing IAM application.

The result should create the capabilities for the existing IAM application to manage and control identities and access rights in the Okta-platform.

Keywords: IAM, ServiceNow, Okta, integration, access management

Sisällys

Lyhenteet

PaaS: Platform as a service

OOB: Out of the box, eli vakiotoiminnallisuus järjestelmässä.

REST: Representational state transfer

API: Application programming interface, eli ohjelmointirajapinta

JSON: JavaScript Object Notation

IAM: Identity and Access Management, eli identiteetin ja pääsynhallinta

OAuth: Open Authorization, pääsyoikeuksien välittämiseen tarkoitettu protokolla.

GDPR: General Data Protection Regulation

1 Johdanto

Tämän insinöörityön on tilannut Appmore Oy, joka on perustettu vuonna 2012. Yrityksen tavoitteena on auttaa organisaatioita saamaan arvoa digitaalisesta alustasta nimeltä ServiceNow. Viimeisen kymmenen vuoden aikana he ovat implementoineet useita erilaisia liiketoiminta ratkaisuja, esimerkiksi identiteetinhallintaan ja häiriönhallintaan. Yritys toimi vuoteen 2022 asti nimellä Lempinen & Partners Oy. Yrityksellä on toimipisteet Espoossa ja Tampereella. [1.]

Projektissa laajennetaan olemassa olevaa IAM-sovellusta, joka on rakennettu ServiceNow-alustalle. Tavoitteena on mahdollistaa informaation kulku ja identiteettien hallinta ServiceNow-alustalla olevan IAM-sovelluksen ja Okta-järjestelmän välillä. Tämä mahdollistaa sen, että käyttäjä voi IAM-sovelluksen avulla tilata esimerkiksi käyttäjätunnuksen tai käyttöoikeuden Okta-järjestelmään.

Projektin tavoitteena on, että käyttöoikeustilauksen jälkeen tieto siirtyy kohdejärjestelmään, eli Okta:aan automaattisesti hyödyntäen tässä työssä luotuja työnkulkuja. Tiedon täytyy kulkea myös toiseen suuntaan, eli Okta:sta täytyy olla mahdollista täsmäyttää dataa ServiceNow ympäristössä olevaan IAM-sovellukseen. Tietoja voidaan lähettää ja noutaa REST-rajapintaa hyödyntäen.

Projektin tekninen toteutus hyödyntää ServiceNow:n toimintoja kuten esimerkiksi Workflow:ta. Ohjelmointikielenä käytetään alustalla pääsääntöisesti käytössä olevaa JavaScriptiä.

Insinöörityössä esitellään projektissa käytettävät teknologiat, luodaan integraatio sovellusten välille, sekä lopuksi käydään läpi toteutuksen tulokset ja johtopäätökset.

2 ServiceNow

ServiceNow on pilvipohjainen IT-palvelunhallintajärjestelmä. Alusta tarjoaa erilaisten IT-hallinta työnkulkujen automaatiota ja sen erikoisosa-alueisiin kuuluu IT-käyttöpalvelun hallinta sekä IT-palvelunhallinta.

ServiceNow integroituu helposti eri työkalujen kanssa, mahdollistaen sen hyödyntämisen monenlaisiin eri käyttötarkoituksiin.

Yrityksen on perustanut Fred Luddy vuonna 2003 ja sen pääkonttori sijaitsee nykyään Santa Clarassa, Kaliforniassa.

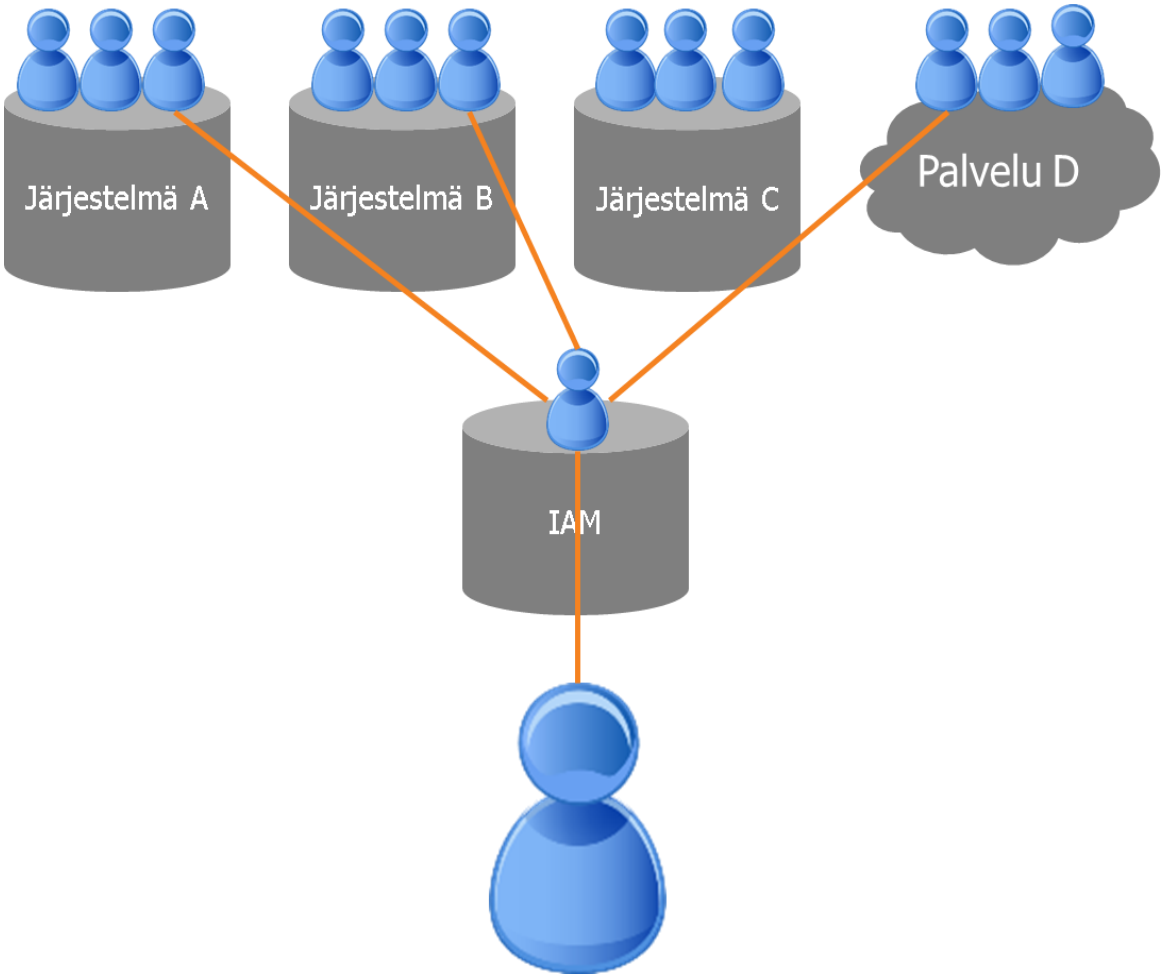
Yleisiä käyttötarkoituksia ServiceNow tuotteille ovat esimerkiksi tiketöintijärjestelmät suurten projektien hallintaan ja vertailuanalyysi edistysten seuraamiseen. [2.]

ServiceNow tarjoaa erikoistuneita palvelunhallinta kyvykkyyksiä esimerkiksi seuraaville aloille:

- Teknologiateollisuus
- Telekommunikaatio
- Teollisuusala
- Finanssiala
- Julkinen sektori

3 IAM

Identiteetin- ja pääsynhallinta on kokoelma prosesseja, työkaluja ja käytäntöjä roolien ja käyttöoikeuksien hallintaan ja määrittämiseen. Tämä voi koskea sekä käyttäjiä että laitteita. Käyttöoikeuksia voidaan hallita useampaan eri järjestelmään yhdestä keskitetystä paikasta.



Kuva 1: Identiteetti yksinkertaistettuna. [3.]

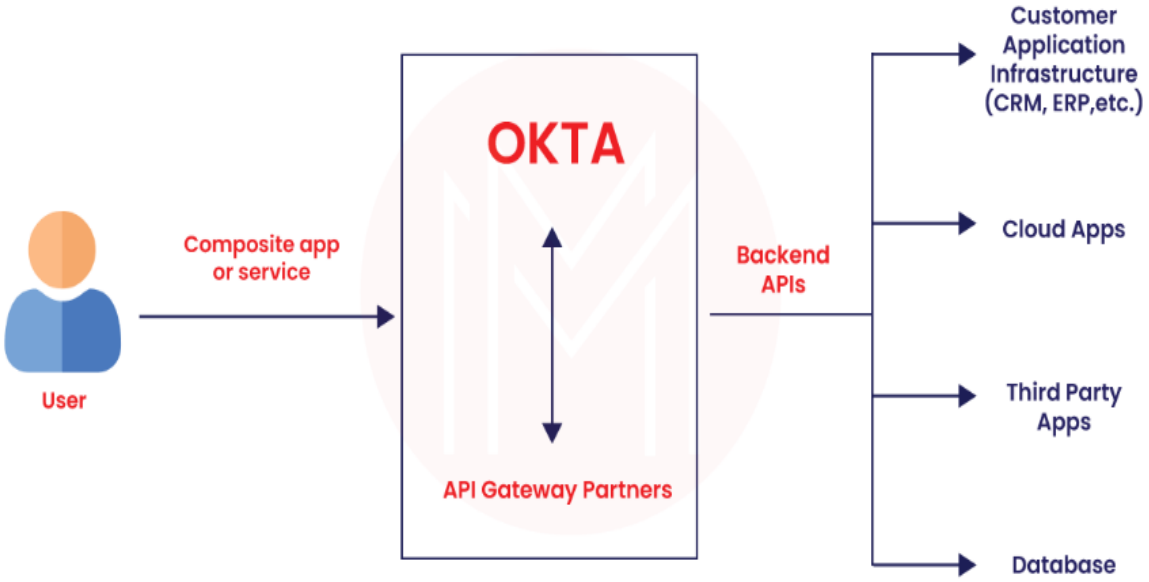
Käyttäjänä voi toimia esimerkiksi asiakas tai työntekijä. Laitteena voi olla esimerkiksi serveri, puhelin tai tietokone. IAM-järjestelmien keskeinen päämäärä on yksi digitaalinen identiteetti, joka vastaa käyttäjää tai laitetta. Tämän jälkeen kyseistä digitaalista identiteettiä voidaan hallinnoidaan ja tarkkailla IAM-sovelluksen avulla.

Tavoitteena IAM:ssa on, että identiteetiltä löytyy informaatio kaikista käyttäjän (tai laitteen) käyttöoikeuksista niiden koko elinkaaren ajan. [4.]

Appmoren identiteetinhallinta ratkaisu on sovellus nimeltään IGAmore. Tässä projektissa rakennamme tähän ServiceNow-alustalla olevalle sovellukselle integraation, joka mahdollistaa identiteetinhallinnan asiakasorganisaation Okta-järjestelmään.

4 Okta

Okta on pilvipohjainen identiteetinhallinta ratkaisu. Järjestelmän avulla voidaan hallinnoida työntekijöiden pääsyä heidän sovelluksiin sekä laitteisiin. Järjestelmän keskinäisiin ominaisuuksiin kuuluuvat esimerkiksi provisiointi, SSO, AD, LDAP integraatio, keskitetty deprovisointi ja kaksivaiheinen tunnistautuminen. [6.]



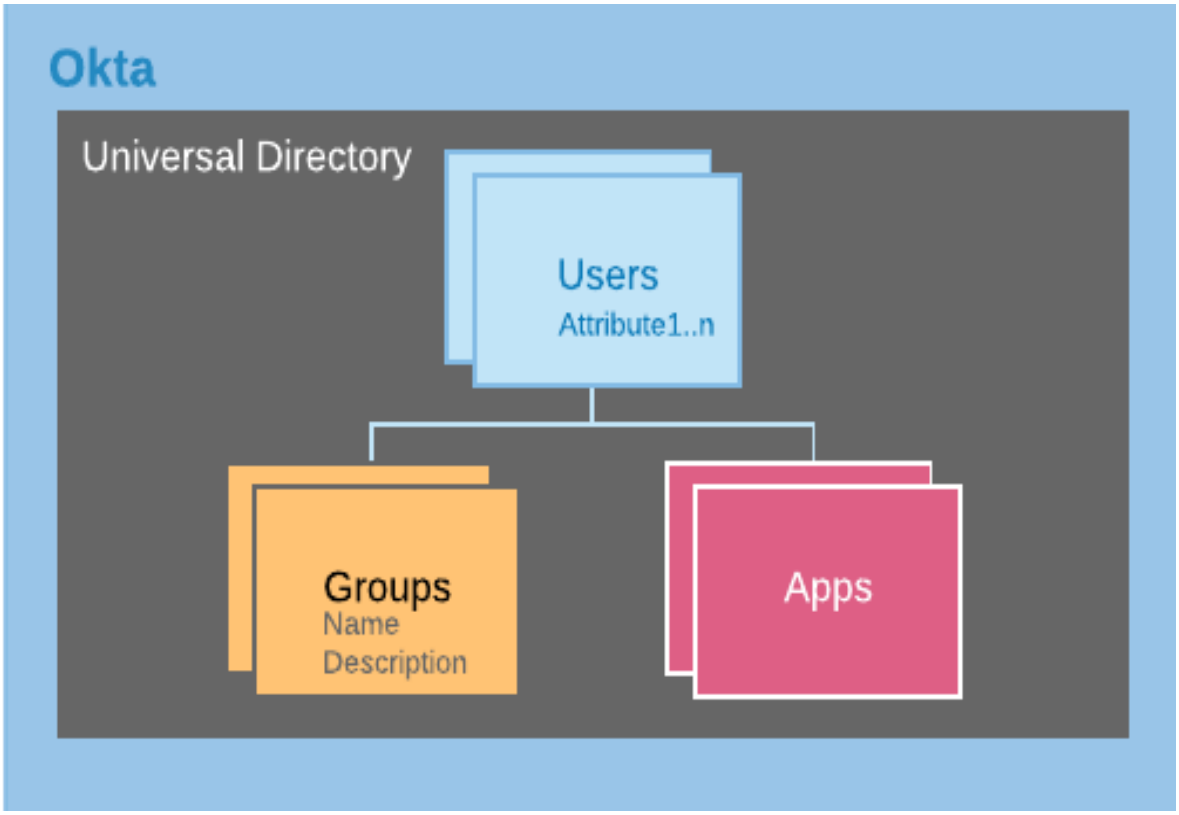
Kuva 2: Okta diagrammi. [7.]

4.1 Resurssit

Kohdejärjestelmästä löytyy laaja kokoelma erilaisia resursseja, joita meidän on mahdollista katsella ja hallita REST-rajapinnan kautta. Seuraavassa kappaleessa käymme läpi identiteetin hallinnan näkökulmasta tärkeimmät resurssit, joiden selkeän hallinnoinnin aiomme mahdollistaa tämän projektin myötä.

Tässä projektissa käytettävät resurssit ovat:

1. Käyttäjät
2. Ryhmät
3. Sovellukset



Kuva 3: Okta arkkitehtuuri. [8.]

4.1.1 Käyttäjät

Käyttäjät ovat tunnuksia, jotka mahdollistavat järjestelmään kirjautumisen. Käyttäjät voivat kuulua ryhmiin sekä sovelluksiin. Käyttäjätietue sisältää paljon dataa verrattuna muihin resursseihin, esimerkiksi nimi, puhelinnumero ja sähköposti. Käyttäjältä löytyy yhteensä kymmeniä eri tietoja, joista aiomme hallinnoida vain osaa. Kaikki kohdejärjestelmässä oleva data ei meidän identiteetinhallintamme näkökulmasta ole tarpeellista.

4.1.2 Ryhmät

Ryhmät ovat kokoelma järjestelmässä olevia käyttäjiä. Näiden tarkoitus on suoraviivaistaa oikeuksien antamista ja hallinnointia. Käyttöoikeuksia on mahdollista antaa ryhmille, jolloin kaikki ryhmään kuuluvat käyttäjät perivät kyseiset oikeudet. Ryhmätiedoissa olevat tiedot, jotka aiomme tuoda ja hallinnoida ovat nimet, kuvaukset ja ryhmän jäsenet.

4.1.3 Sovellukset

Sovellukset ovat järjestelmään luotuja integraatioita, joihin on mahdollista antaa oikeuksia liittämällä niihin käyttäjiä. Sovelluksien osalta aiomme tuoda järjestelmästä tämän projektin myötä vain sovelluksen nimen sekä siihen kuuluvat käyttäjät, koska muu tieto ei ole oleellista identiteetinhallinnan näkökulmasta.

5 Integraation rakentaminen

5.1 Käyttötapaukset

Projektin ohjenuorana toimivat työn tilaajan asettamat käyttötapaukset. Suunnittelu ja toteutus tehdään näitä ajatellen. Toteutusta voidaan myös jälkikäteen arvioida sen mukaan, ollaanko nämä käyttötapaukset saatu toteutettua.

Seuraavat käyttötapaukset toteutetaan tässä projektissa:

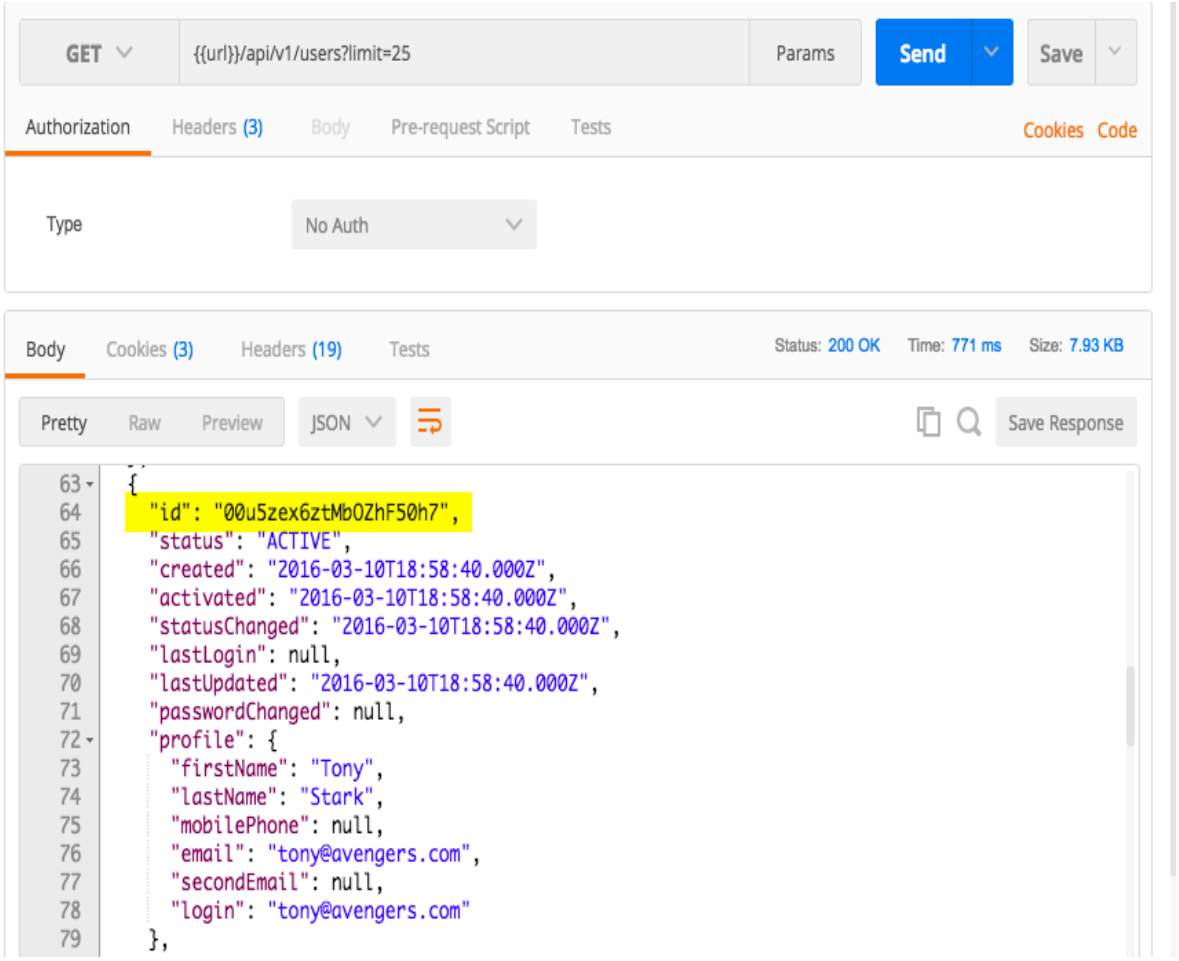
- Tunnuksen hallinta
    - Tunnuksen päivittäminen
    - Tunnuksen päivittäminen
    - Tunnuksen deaktivointi
    - Tunnuksen poistaminen
- Ryhmäoikeuksien hallinta
    - Ryhmäoikeuksien tilaaminen
    - Ryhmäoikeuksien poistaminen
- Applikaatio-oikeuksien hallinta
    - Applikaatio-oikeuksien tilaaminen
    - Applikaatio-oikeuksien poistaminen
- Täsmäytys

- Käyttäjätietojen täsmäytys
- Ryhmien täsmäytys
    - Ryhmäjäsenyyksien täsmäytys
- Applikaatioiden täsmätys
    - Applikaatiojäsenyyksien täsmäytys

5.2 Suunnittelu

Ensimmäiseksi täytyy suunnitella työn tekemisen teon vaiheet, jotta edellä mainitut käyttötapaukset saadaan toteutettua. Tämä alkaa Okta-järjestelmään kehitysympäristön avaamisesta. Ympäristöön perehtyminen tekee suunnittelusta ketterämpää.

Järjestelmän REST-rajapintaan löytyy hyvä dokumentaatio, josta käy ilmi kuinka REST-rajapintaa pystyy hyödyntämään. Kehitysympäristöä käyttäen todensin, kuinka voin noutaa tietoa järjestelmästä, sekä minkälaisia kriteerejä rajapinta asettaa työn toteuttamiselle.



Kuva 3: Esimerkki Okta API pyynnöstä ja sisällöstä [10.]

Rajapintakutsujen selvityksessä ja kehityksessä hyödynnettiin Postman-sovellusta.

Ensimmäinen askel oli kehitysympäristössä REST-rajapinnan autentikoiminen ja sanomien luominen jokaiselle käyttötapaukselle. Tämän jälkeen täytyi pohtia, kuinka nämä autentikoinnit ja sanomien luonnit rakennetaan ServiceNow-alustalla.

Kun sanomat olivat selkeät, siirryimme tilauslomakkeen suunnittelemiseen. Lomakkeella käytetään käyttäjien perustietoja, sekä mahdollistetaan oikeuksien tilaaminen. Tämän jälkeen rakennettiin eri käyttötapauksille logiikkaa. Esimerkkinä jos tilataan uusi tunnus, täytyi tämä yhdistää uuden käyttäjän työnkulkuun, jotta osaamme lähettää oikean sanoman kohdejärjestelmään.

5.3 Sovelluksen työnkulku

Sovelluksessa käyttöoikeuksien hallinta perustuu siihen, että käyttäjällä on yksi identiteetti. Tähän identiteettiin lisätään tämän jälkeen käyttöoikeustilausten pohjalta tunnuksia ja käyttöoikeuksia.

Ennen sovelluksen käyttöönottoa ensimmäinen askel on täsmäyttää olemassaoleva data kohdejärjestelmästä.

Uuden identiteetin työnkulku lähtee liikkeelle, kun käyttäjä tekee tilauksen ServiceNow-portaalissa. Tässä vaiheessa tilauksesta riippuen luodaan hyväksyntäpyyntö tästä tilauksesta. Tilauksen hyväksymisen jälkeen luodaan käyttäjälle tarvittavat tunnukset. Uudelle käyttäjälle luodaan esimerkiksi identiteetti ja tälle identiteetille pyydetyt tunnukset ja oikeudet.

Hyväksyntöjen sekä identiteetin luominen eivät kuulu tämän projektin laajuuteen. Tarkoituksena on mahdollistaa identiteetille Okta-tunnuksen ja käyttöoikeuksien tilaaminen ja hallinnointi.

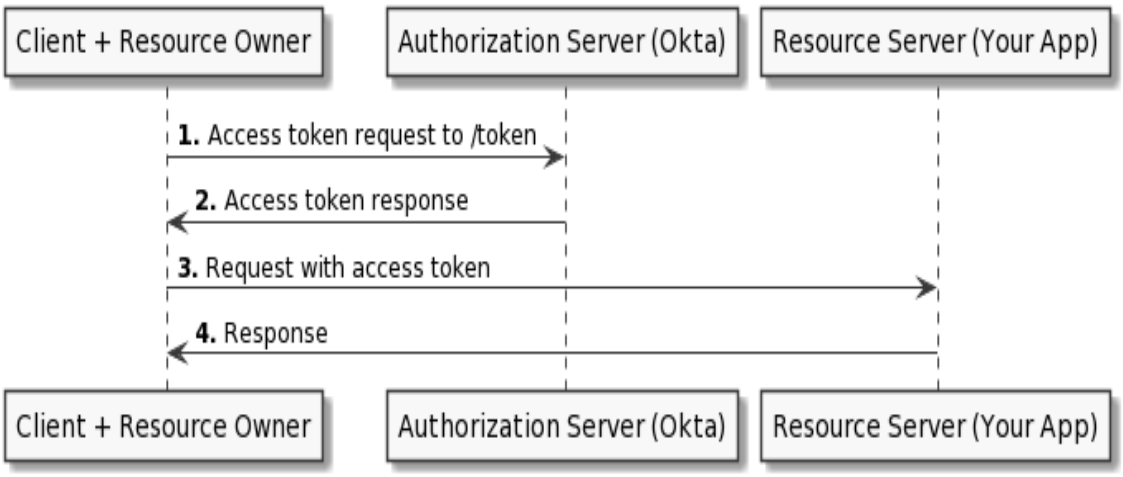
5.4 Autentikointi

Ensimmäisenä askeleena projektissa on autentikoimisen konfigurointi käyttäen OAuth-protokollaa. OAuth mahdollistaa pääsyn verkkopalveluihin identiteetillä ilman salasanaa. Salasanan sijaan OAuth hoitaa verifioinnin autentikointitokenilla. [9.]

Protokollassa on määriteltynä neljä erilaista roolia:

- Resource owner (resurssin omistaja)
- Resource server (resurssipalvelin)
- Client (asiakasohjelma)
- Authorization server (valtuutuspalvelin)

Resource owner eli resurssin omistaja projektin yhteydessä on henkilö, joka voi myöntää pääsyn resurssiin eli Okta järjestelmään. Resource server eli resurssipalvelin on tietojen omaava palvelin. Client eli asiakasohjelma on pyynnön lähettävä sovellus. Projektin yhteydessä se on IAM-sovellus. Authorization server eli valtuutuspalvelin on palvelin, joka luovuttaa käyttöoikeustietueen (engl. Access token) asiakasohjelmalle onnistuneen autentikoinnin jälkeen. [11.]



Kuva 3: Client Credentials-tyypisen tapahtuman kulku [12.]

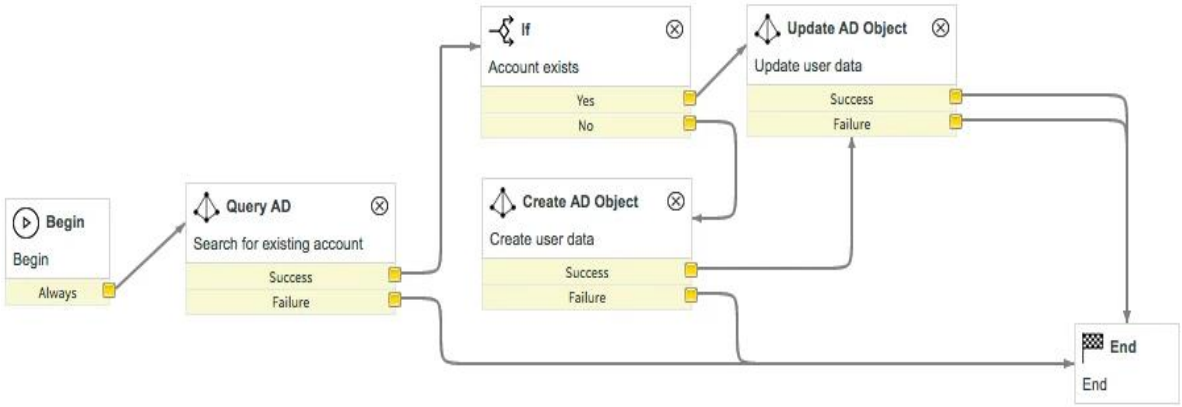
5.5 Täsmäytysajo

Kun yhteys on saatu muodostettua kohdejärjestelmään voimme jatkaa olemassa olevien tunnuksien, ryhmien ja applikaatioiden täsmäytystä kohdejärjestelmästä. Tämä alkaa työnkulun tekemisellä, joka suoritetaan ServiceNow:n Workflow toiminnallisuutta käyttämällä.

Työkalu on raahaa ja pudota toiminnolla käytettävä graafinen käyttöliittymä. Työnkulussa suoritetaan askel askeleelta tarvittavien täsmäytysten tekeminen. Jokaista täsmäytettävää resurssia kohden luodaan oma aktiviteetti työnkulkuun. JavaScriptiä käyttäen, aktiviteeteissa hoidetaan täsmäytystehtävien luonti sekä mahdollisten virhetilanteiden hallinta.

Täsmäytystehtävien tarkoitus on muodostaa REST-rajapintaan lähtevät pyynnöt, sekä vastaanottaa ja jäsennellä saapuva JSON-formaattinen objekti olemassa olevaan dataan.

Täsmäytystyönkuluissa on tärkeä muistaa eritellä kaikki täsmäytettävät resurssit erikseen ja hoitaa mahdolliset virhetilanteet. Aktiviteettien eritteleminen ja työnkulun pilkkominen mahdollisimman pieniin aktiviteetteihin mahdollistaa nopean ja tehokkaan virhetilanteen selvittämisen.



Kuva 4: ServiceNow Workflow esimerkki. [13.]

5.5.1 Käyttäjien täsmäytys

Käyttäjien täsmäytys on työnkuluista yksinkertaisin, koska se sisältää vain käyttäjätietoja. Käyttäjätietojen sisältö on kuitenkin määrältään suuri, joten näiden täsmäyttäminen oikeisiin kenttiin lähdejärjestelmässä vaatii tarkkuutta.

5.5.2 Ryhmien täsmäytys

Ryhmien täsmäytyksessä isoin ero käyttäjiin on ryhmäjäsenyystieto, jotka ovat referenssejä käyttäjätietoihin. Tämä tarkoittaa sitä, että ryhmien täsmäytyksessä meidän täytyy samanaikaisesti lisätä käyttäjiä täsmäytettäviin ryhmiin.

5.5.3 Sovelluksien täsmäytys

Sovellukset eivät sisällöltään eroa ryhmistä lähes ollenkaan. Ne täsmäytetään järjestelmään käyttöoikeuksina samalla tavalla kuin ryhmät. Näiden täsmäytyksessä jouduimme myös lisäämään käyttäjille oikeuksia sovelluksiin sovellusjäsenyyksien perusteella.

5.6 IAM definition

IAM definition on IAM-sovelluksesta löytyvä tietuetyyppi. Se on tärkein osa sovellusta, koska sinne määritellään mistä kohdejärjestelmästä on kyse. Tähän projektiin kuului Okta-järjestelmälle oman IAM definitionin luonti.

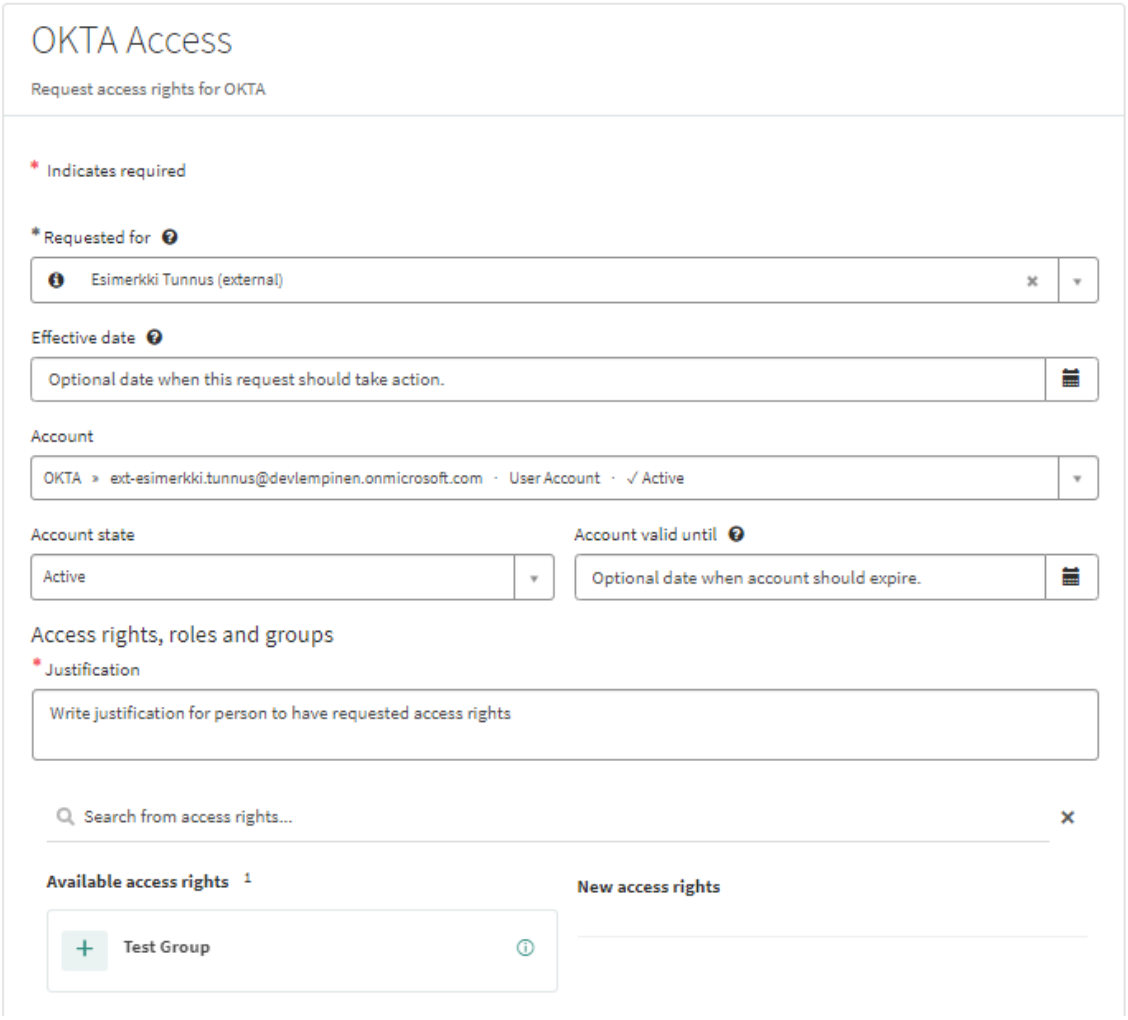
IAM definitioniin määritellään myös kohdejärjestelmästä lisäksi mitä työnkulkuja ja ominaisuuksia siitä löytyy. Sinne määritellään esimerkiksi kaikki työnkulut, milloin niitä käytetään, millä toiminnolla täsmäytys toteutetaan ja kuinka erotellaan eri käyttötapaukset.

Käyttöoikeuksien tilauslomake on linkitetty IAM definitionille, joten tilauksen jälkeen tiedämme mihin kohdejärjestelmään tilaus on tehty. Tämän jälkeen tilaukselle täytetyt tiedot käydään läpi, jotta tiedämme tarkalleen mitä tehtäviä meidän täytyy tehdä. Näille eri tehtäville on rakennettu omat logiikkansa, jotka löytyvät IAM definitionilta. Esimerkki tapauksia ovat tunnuksen luonti tai tunnuksen poistaminen.

5.7 Käyttöoikeustilaus

Käyttöoikeustilauksia varten loimme uuden lomakkeen IAM-sovellukseen. Tällä lomakkeella on tarkoitus suorittaa käyttäjien tilaus, päivitys, deaktivointi ja poisto. Kaikki nämä käyttötapaukset suoritetaan samalla työnkululla, mutta työnkulku osaa suorittaa oikean toimenpiteen lomakevalintojen sekä olemassa olevan datan perusteella.

Lomakkeella voi myös tilata ryhmä- ja sovellusoikeuksia siinä olevasta luettelosta. Lomakkeelta löytyy yksi luettelo, joka sisältää kaikki tilattavat oikeudet. Vierestä löytyy toinen luettelo, joka mahdollistaa oikeuksien poistamisen.



Lomake-esimerkki 1: Ryhmäoikeuksien tilaaminen olemassa olevalle tunnukselle.

Tilauksen jälkeen työnkulku lähtee käyntiin ja luo järjestyksessä IAM-pyynnön, IAM-tehtävän ja IAM-connector tehtävän. Kaikilla näillä on oma tarkoituksensa, ja ne löytyvät omista taulukoistaan järjestelmästä. Nämä eivät ole OOB-taulukoita ServiceNow alustalla, vaan kuuluvat IAM-sovelluksesta löytyviin kustomoituihuin taulukoihin.

5.7.1 IAM-pyynnöt

Kun käyttäjä on suorittanut tilauksen lomakkeelta luodaan tästä IAM-pyyntötietue järjestelmään. Nämä tietueet kuuluvut IAM-sovelluksen kustoimoituun tauluun, eivätkä ole vakio-ominaisuuksia ServiceNow-alustalla.

Pyynnölle tallennetaan kaikki tarvittavat tiedot tilauksesta. Tähän kuuluu esimerkiksi: kuka on tilannut, kenelle tilataan, mahdolliset olemassa olevat tunnukset ja identiteetit, tilatut ja/tai poistetut käyttöoikeudet sekä tilauksen syy. Tämän jälkeen pyynnön työnkulussa olevat määritelmät päättävät mitä IAM-tehtäviä tästä luodaan sekä IAM-tehtävät linkitetään pyynnölle.

5.7.2 IAM-tehtävät

IAM-tehtävät kuuluvat myös kustomoituun tauluun, joka ei kuulu ServiceNow:n vakio-ominaisuuksiin. IAM-tehtävät ovat yksittäisiä toimenpiteitä, mitä järjestelmän täytyy suorittaa. Tehtävät ovat linkitettyina IAM-pyyntöihin ja pyyntö voi sisältää useamman tehtävän. Tehtäviin voi kuulua esimerkiksi: uuden tunnuksen luominen, käyttöoikeuden lisääminen tunnukselle, käyttöoikeuden poistaminen tunnukselta tai tunnuksen deaktivointi.

Tehtäviä kohden löytyy omat ServiceNow Workflowit, joihin on rakennettu logiikka jokaisen tapauksen käsittelyä varten. Tehtävät suorittavat datan luomisen ja hallitsemisen IAM-sovelluksessa. Tämän jälkeen tehtävät luovat IAM-connector tehtäviä, jotka yhdistetään tehtävälle.

5.7.3 IAM-connector tehtävät

IAM-connector tehtävät ovat IAM-tehtäville linkitettyjä toimenpiteitä, joiden tarkoitus on muodostaa kohdejärjestelmään lähtevät sanomat REST-rajapintaa hyödyntäen.

Näiden luominen tapahtuu IAM-tehtävillä ajautuvissa työnkuluissa. Työnkulussa oleville aktiviteeteille on JavaScriptillä kirjoitettu logiikka, jonka tarkoitus on luoda IAM-connector tehtävä hyödyntäen sinne asetettua dataa.

Kun IAM-connector tehtävä on luotu se muodostaa lähtevän sanoman. Tämän jälkeen odotamme, että kohdejärjestelmä palauttaa vastauksen. Tässä vaiheessa muodostamme mahdollisen virheviestin, jos sellainen tulee. Onnistuneen sanoman lähetyksen jälkeen tehtävälle täyttyy kohdejärjestelmästä tullut sanoma. Tämä JSON-objektina saapunut sanoma käydään läpi ja siellä olevat kentät kohdennetaan IAM-sovelluksesta löytyviin kenttiin käyttäen projektissa luotuja kenttämäärityksiä.

Kenttämääritykset ovat rakennettu kaikille käyttötapauksille erikseen ja näitä hyödyntäen saamme kohdejärjestelmässä olevan datan siirrettyä oikeaan tietueeseen sekä oikeaan kenttään.

5.8 Testaaminen

Toteutuksen jälkeen täytyi testata ja varmistaa kaikkien käyttötapauksien toiminta. Aluksi loimme Okta:n kehitysympäristöön dataa, eli käyttäjiä, ryhmiä ja applikaatioita. Käyttäjiä täytyi myös lisätä ryhmien ja applikaatioiden jäseniksi.

Tämän jälkeen suoritimme IAM-sovelluksessa täsmäytyksen. Täsmäytysajo on mahdollista konfiguroida ajautumaan säännöllisesti, mutta testausta varten pystyimme suorittamaan täsmäytysajon manuaalisesti. Tietojen pitäisi tulla ServiceNow-järjestelmään ja tietojen täsmäytyä oikeisiin kenttiin. Kun data saapui virheittä järjestelmään ja olimme validoineet, että se saapui oikeaan paikkaan, pystyimme toteamaan täsmäytyksen toimivan.

Mahdollisia virhetilanteita oli mahdollista tarkkailla täsmäytystehtäviltä, jos sellaisia tuli. Näitä saattoi aiheuttaa esimerkiksi virheellinen data tai täsmäytyslogiikka.

Seuraavaksi testasimme käyttäjän ja oikeuksien luvittamista. Tilauslomaketta hyödyntäen saimme tilattua käyttäjiä sekä oikeuksia. Nämä pystyimme validoimaan ensiksi ServiceNow:ssa, että näimme datan muodostuneen virheittä. Tämän jälkeen teimme validoinnin kohdejärjestelmässä. Data oli molemmissa järjestelmissä identtistä, joten pystyimme toteamaan sen toimivan.

Lomaketta hyödyntäen pystyimme seuraavaksi poistamaan käyttäjältä oikeuksia ja tämä heijastui myös kohdejärjestelmään. Oli hyvä myös varmistaa, että käyttäjän oikeudet inaktivoituivat ServiceNow-järjestelmässä.

Käyttäjän inaktivoiminen onnistui myös lomakkeelta. Tässäkin tapauksessa validoimme, että käyttäjä inaktivoitui sekä ServiceNow-järjestelmässä, että myös kohdejärjestelmässä.

6 Tulokset

6.1 Lopputulos

Projektissa saavutettiin sovellukselle kyvykkyydet tehdä ennalta määritetyt toimenpiteet kohdejärjestelmään. Autentikointi, täsmäytys ja käyttöoikeuksien hallinta IAM-sovelluksella toimii odotetusti.

IAM-sovelluksen käyttäjä voi mennä tilaamaan käyttöoikeuksia kohdejärjestelmään ja liittymään tai poistumaan ryhmistä sekä applikaatioista. Työnkulut ajautuvat sujuvasti ilman virheitä, sekä data on yhdenmukaista molemmissa järjestelmissä. Näin ollen voimme todeta projektin toteutuneen onnistuneesti.

6.2 Jatkokehitys

Integraatiota on mahdollista jatkaa tarpeiden mukaan. Prosessiin on mahdollista lisätä esimerkiksi laitteiden täsmäytys ja hallinnointi samalla tavalla kuin ryhmien ja applikaatioidenkin kohdalla. Okta-järjestelmä tarjoaa laajat mahdollisuudet REST-rajapinnan kautta datan hallinnointiin, joten jatkokehityksen mahdollisuuksia löytyy todella paljon.

Integraatioita on myös mahdollista räätälöidä erilaisiin tarpeisiin. Kaikkea dataa ei ole tarpeellista täsmäyttää, eikä kaikkia tässä projektissa rakennettuja käyttötapauksia hyödyntää.

7 Yhteenveto

Projekti alkoi IAM-sovellukseen tutustumalla. Sovelluksesta löytyi paljon työkaluja, joita hyödyntämällä on mahdollista rakentaa integraatio toiseen kohdejärjestelmään helposti. Itse ServiceNow-järjestelmä taipuu myös hyvin integraatioiden luomiseen. Tilaajalta löytyi myös laajat tekniset dokumentaatiot sekä ohjeet, kuinka kehitys kannattaa suorittaa.

Projektin toteutus sujui suoraviivaisesti. Olemassa olevat työkalut ja työnkulut helpottivat toteutusta, mutta vaati suunnittelussa enemmän aikaa. Tämä johtui siitä, että olemassa oleviin komponentteihin täytyi ensin perehtyä ja tämän jälkeen tarvittaessa muokata tähän käyttöön sopivaksi. Hyvä suunnittelu kuitenkin teki kehityksestä helpompaa ja johdonmukaista.

Seuraava askel oli kohdejärjestelmään tutustuminen. Tähän kuului kehitysympäristön pystyttäminen ja sen toimintoihin perehtyminen. Tämän jälkeen täytyi tarkemmin ymmärtää, miten IAM-sovelluksen näkökulmasta tärkeää dataa hallinnoidaan kohdejärjestelmässä. Viimeisenä kohtana oli vielä REST-rajapinnan ja resurssien datastruktuurin tutkiminen. Nämä vaativat selvitystä ja tutkimista, koska esimerkiksi ryhmäjäsenyyksien noutaminen ei ollut itsestäänselvää. Nämä eivät löytynee omasta sijainnistaan, vaan täytyi tulkita ryhmien datasta.

Okta-järjestelmän REST-rajapintaan löytyi erityisen laajat dokumentaatiot, jotka tekivät kehityksestä erittäin mieluisaa. Teknisesti haastavin osuus oli OAuth-protokollan käyttöönotto, sekä REST-rajapinnan kutsujen rakentaminen jokaiseen eri käyttötarkoitukseen. Täsmäytysajojen skriptit olivat myös ajoittain todella monimutkaisia ja teknisiä. Näistä huolimatta toteutus oli pääsääntöisesti sujuvaa.

Eniten aikaa vievä osuus oli tilauksien työnkulun rakentaminen. Työnkulku haarautuu tilauksesta riippuen useisiin eri polkuihin ja näiden kehittäminen, testaaminen sekä validointi vaati aikansa.

Lopputuloksena saimme rakennettua toimivan integraation kahden eri järjestelmän välille. Sovellus mahdollistaa olemassa olevien käyttäjien, ryhmien, ryhmäjäsenyyksien, sovellusten ja sovellusjäsenyyksien täsmäyttämisen IAM-sovellukseen. Tämän jälkeen on mahdollista ylläpitää kaikkia edellä mainittuja resursseja sovelluksesta käsin. Kaikki tilaukset onnistuvat tilauslomakkeelta käsin ja data siirtyy kohdejärjestelmään niin kuin suunniteltu, sekä vastaa lähdejärjestelmään muodostunutta dataa.

Lähteet

1. About Us – Appmore. Verkkoaineisto. 2023. <https://appmore.com/about-us/>. Luettu 1.4.2023.

2. ServiceNow. Verkkoaineisto. 2023. <https://www.techtarget.com/searchitoperations/definition/ServiceNow>. Luettu 8.4.2023.

3. Niemi, Kalle. Identiteetin ja pääsynhallinta (IAM). <https://www.itewiki.fi/opas/kayttajahallinta-iam/>. Luettu 11.4.2023.

4. Strom, David. What is IAM? Identity and access management explained. Verkkoaineisto. 2021. <https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html>. Luettu 11.4.2023

5. Security Benefits of Identity and Access Management (IAM). Verkkoaineisto. <https://cybriant.com/security-benefits-of-identity-and-access-management-iam/>. Luettu 12.4.2023

6. What is Okta and What Does Okta Do?. Verkkoaineisto. 2023. <https://support.okta.com/help/s/article/what-is-okta?language=en_US>. Luettu 21.4.2023.

7. What is Okta?. Verkkoaineisto. <https://mindmajix.com/what-is-okta>. Luettu 21.4.2023.

8. Architechture. Verkkoaineisto. <https://docs.idp.rocks/guide/architecture.html#okta-basics-users-groups-apps>. Luettu 24.4.2023.

9. Fioretti, Marco. OAuth 2.0: What is it, and how does it work?. 2022. <https://www.techrepublic.com/article/oauth-2-0-what-is-it/>. Luettu 28.4.2023.

10. Test the Okta REST APIs using Postman. Verkkoaineisto. <https://developer.okta.com/code/rest/#send-a-request>. Luettu 15.5.2023.

11. OAuth 2.0 Authorization Framework. 2012. Verkkoaineisto. <https://data-tracker.ietf.org/doc/rfc6749/>. Luettu 29.4.2023.

12. Implement authorization by grant type. Verkkoaineisto. <https://developer.okta.com/docs/guides/implement-grant-type/clientcreds/main/#about-the-client-credentials-grant>. Luettu 5.5.2023.

13. How ServiceNow Workflow Ensures End-to-End Automation. Verkkoaineisto. <https://vsoftdigital.com/blog/how-servicenow-workflow-ensures-end-to-end-automation>. Luettu 6.5.2023.