Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2021

Aleksi Teerisalo

IDENTITEETIN- JA PÄÄSYNHALLINNAN HYÖDYNTÄMINEN ORGANISAATIOISSA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2021 | 54 sivua

Aleksi Teerisalo

IDENTITEETIN- JA PÄÄSYNHALLINNAN HYÖDYNTÄMINEN ORGANISAATIOISSA

Opinnäytetyössä käsitellään identiteetin- ja pääsynhallinnan ratkaisuja sekä perehdytään niiden hyödynnettävyyteen osana organisaatioiden käyttövaltuushallintaa. Nykyaikaiset identiteetin- ja pääsynhallinnan järjestelmät sisältävätkin monia hyödyllisiä toimintoja, joilla voidaan kehittää organisaatioiden tietoturvaa ja operatiivista tehokkuutta sekä varmistaa lainsäädännön ja yritysten omien käytäntöjen noudattaminen. Identiteetin- ja pääsynhallinnan tärkeys korostuu erityisesti isommissa yrityksissä, joissa hallitaan satojen tai jopa tuhansien työntekijöiden ja yhteistyökumppaneiden käyttöoikeuksia. Järjestelmät tuovat tällöin merkittäviä hyötyjä niin organisaation johdolle, IT-osastolle kuin käyttäjillekin.

Opinnäytetyön tärkeimpänä tavoitteena oli löytää toimeksiantajaorganisaation tarpeita vastaava identiteetinhallintajärjestelmä, jolla korjattaisiin nykyisiin menettelyihin liittyviä haasteita sekä vähennettäisiin käyttäjienhallintaan kuluvaa työaikaa. Työssä tutustutaan myös identiteetin- ja pääsynhallinnan termeihin, toimintoihin ja vaiheisiin, jotta saadaan monipuolinen käsitys järjestelmien toiminnasta. Opinnäytetyö käsittelee identiteetin- ja pääsynhallinnan tehtäviä, erityyppisiä todennus- ja valtuutusmekanismeja sekä sähköisen identiteetin elinkaaren vaiheita. Työn loppupuolella tutustutaan myös neljään erilaiseen identiteetin- ja pääsynhallinnan tuotteeseen sekä perehdytään hankittavan järjestelmän käyttöönottoon liittyviin valmisteluihin ja testaamiseen.

Toimeksiantajan tarpeisiin soveltuva identiteetinhallinnan ratkaisu löydettiin ja sen toimivuutta varmistettiin testaamisen kautta. Järjestelmä otettaisiin myöhemmässä vaiheessa laajemmin käyttöön, jolloin sen avulla automatisoitaisiin verkkotunnusten luomista, päivittämistä ja sulkemista sekä hallinnoitaisiin pilvipalveluihin liittyvien käyttöoikeuksien voimassaoloa. Organisaatiossa tapahtuva identiteetin- ja pääsynhallinta olisi uuden järjestelmän ansiosta entistä tehokkaampaa ja johdonmukaisempaa.

ASIASANAT:

identiteetinhallinta, pääsynhallinta, todennus, valtuutus, sähköinen identiteetti

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2021 | 54 pages

Aleksi Teerisalo

UTILIZATION OF IDENTITY AND ACCESS MANAGEMENT IN ORGANIZATIONS

The thesis handles identity and access management solutions and examines their usability as a part of user account management of organizations. The main objective of the thesis was to find an identity management system that meets the needs of the commissioning organization. This identity management system would be intended to fix the challenges associated with the current procedures and reduce the work time spent on the user account management.

In order to achieve the objective of this thesis, the terms, functions and stages of identity and access management were examined, in order to gain a comprehensive understanding of how these solutions work. This work presents, inter alia, the tasks of identity and access management, the different types of authentication and authorization mechanisms, and the steps of the digital identity lifecycle. The thesis also introduces four different identity and access management products and focuses on the testing of the chosen system.

As a result of the thesis, the suitable identity management system was found, and its functionality has been verified through the testing. The chosen system will facilitate identity and access management in the assignment organization in many ways. The system would be more widely deployed at a later stage, allowing creation, updating and closing employee domain accounts and managing access rights for the cloud services in a more consistent way than previously.

Identity and access management is becoming increasingly important in larger companies that manage access rights for hundreds or even thousands of employees and partners. In these kinds of companies identity and access management systems bring significant benefits to the organization management, IT department as well as to the users. The modern systems also contain many useful features that improve the information security and operational efficiency of organizations. In addition, they contain features that help to ensure adherence both to legislation and the companies' own policies.

KEYWORDS:

identity management, access management, authentication, authorization, digital identity

SISÄLTÖ

1 JOHDANTO **7**

2 IDENTITEETIN- JA PÄÄSYNHALLINTA **9**

2.1 Sähköinen identiteetti 10

2.2 Identiteetinhallinta (IdM) 10

2.3 Pääsynhallinta (AM) 11

2.4 Kertakirjautuminen (SSO) 11

2.4.1 Selainpohjainen kertakirjautuminen (Web SSO) 12

2.4.2 Asiakasohjelmaan perustuva kertakirjautuminen (eSSO) 12

2.5 Yhdistetty identiteetinhallinta (FIM) 13

2.6 Itsepalveluportaali 13

3 IDENTITEETIN- JA PÄÄSYNHALLINNAN TEHTÄVÄT **15**

3.1 Tunnistus 15

3.2 Todennus 16

3.3 Valtuutus 17

3.4 Tilastointi 17

4 TODENNUS- JA VALTUUTUSMEKANISMIT **18**

4.1 Todennusmekanismit 18

4.1.1 Fyysiset suojausmekanismit 18

4.1.2 Digitaaliset suojausmekanismit 18

4.2 Valtuutusmekanismit 22

4.2.1 Roolipohjainen pääsynvalvonta (RBAC) 23

4.2.2 Attribuuttipohjainen pääsynvalvonta (ABAC) 23

4.2.3 Pakollinen pääsynvalvonta (MAC) 24

4.2.4 Harkinnanvarainen pääsynvalvonta (DAC) 24

4.2.5 Käyttöoikeus-/tehtäväpohjainen pääsynvalvonta 25

5 IDENTITEETIN ELINKAARI **26**

5.1 Luominen 26

5.2 Provisiointi 27

5.3 Käyttö 28

5.4 Päivittäminen 29

5.5 Sulkeminen 29

5.6 Deprovisiointi 29
5.7 Hallinnointi 30

6 IDENTITEETIN- JA PÄÄSYNHALLINNAN MERKITYS 32
6.1 Tietoturva 32
6.2 Operatiivinen tehokkuus 33
6.3 Lainsäädäntö 34

7 VAIHTOEHTOJEN KARTOITTAMINEN 37
7.1 Organisaation tarpeet 37
7.2 Tarkoitukseen soveltuvia vaihtoehtoja 39
7.2.1 Efecte Identity Governance and Administration 39
7.2.2 Imprivata Identity Governance 40
7.2.3 Enter Ruutuvihko 40
7.2.4 One Identity Manager 41
7.3 Valintapäätös 41

8 JÄRJESTELMÄN KÄYTTÖÖNOTTO 43
8.1 Tavoite 43
8.2 Valmistelut 44
8.3 Testausmenetelmät 45
8.4 Testatut tilanteet 46
8.5 Testauksen lopputulos 47
8.6 Jatkosuunnitelmat 48

9 YHTEENVETO 50

LÄHTEET 53

KUVAT

Kuva 1. Kertakirjautuminen. 11
Kuva 2. IAAA-kehys. 15
Kuva 3. Kirjautuminen OpenID-vaihtoehdoilla. 21
Kuva 4. Identiteetin elinkaari. 26

KÄYTETYT LYHENTEET JA SANASTO

2FA	Two-Factor Authentication – kaksivaiheinen todennus
ABAC	Attribute-Based Access Control – attribuuttipohjainen pääsynvalvonta
AD	Microsoft Active Directory – Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu
AM	Access Management – pääsynhallinta
DAC	Discretionary Access Control – harkinnanvarainen pääsynvalvonta
eSSO	Enterprise Single Sign-On – asiakasohjelmaan perustuva kertakirjautuminen
FIM	Federated Identity Management – yhdistetty identiteetinhallinta
GDPR	General Data Protection Regulation – EU:n yleinen tietosuoja-asetus
HR	Human Resources – henkilöstöhallinto
IAM	Identity and Access Management – identiteetin- ja pääsynhallinta
IdM	Identity Management – identiteetinhallinta
LDAP	Lightweight Directory Access Protocol – hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla
MAC	Mandatory Access Control – pakollinen pääsynvalvonta
MFA	Multi-Factor Authentication – monivaiheinen todennus
PoLP	The Principle of Least Privilege – vähimpien oikeuksien periaate
RBAC	Role-Based Access Control – roolipohjainen pääsynvalvonta
SAML	Security Assertion Markup Language – XML-pohjainen tunnistetietojen yhdistämiskielistandardi
SSH	Secure Shell – tietoliikenteen salaamiseen käytettävä verkkoprotokolla
SSO	Single Sign-On – kertakirjautuminen
Web SSO	Selainpohjainen kertakirjatuminen
XML	Extensible Markup Language – merkintäkielen standardi, jolla kuvataan tietoa ja/tai sen rakennetta

1 JOHDANTO

Yrityksissä tapahtuva tietojenkäsittely on nykyisin suurimmilta osin sähköistä. Monia yrityksen toiminnan kannalta tärkeitä tietoja käsitellään ja tallennetaan tietotekniikan sekä erilaisten sähköisten tietojärjestelmien avulla. Tämä on mahdollistanut tiedon helpon muokkaamisen ja jaettavuuden, mutta tietoja tulisi silti suojella samalla tavoin kuin fyysisessäkin muodossa olevia dokumentteja. Digitaalisten tietojen näkyvyyttä ja saatavuutta voidaan säädellä muun muassa tietojärjestelmiin sisältyvien käyttäjähallintaportaalien sekä erilaisten käyttöoikeuksien avulla. Näiden hallinta ja säätely saattavat työllistää yrityksen IT-osastoa runsaasti, mikäli työntekijöitä ja käyttöoikeuksia on paljon. Käyttäjätilien ja käyttöoikeuksien manuaalinen käsittely saattaa lisäksi aiheuttaa virheitä, jotka pahimmillaan johtavat moninkertaiseen työhön. Tätä tehtävää voidaan kuitenkin helpottaa identiteetin- ja pääsynhallinnan järjestelmillä, joiden merkitykseen ja hyödynnettävyyteen tässä opinnäytetyössä keskitytään.

Uusien työsuhteiden alkaessa työntekijöille useimmiten tarvitaan yrityksen sähköpostiosoite sekä käyttäjätunnukset yrityksen verkkoon ja muihin työtehtävissä tarvittaviin tietojärjestelmiin. Tällöin työntekijälle luodaan sähköinen identiteetti, jota hallinnoidaan identiteetin luomisesta aina sulkemiseen asti. Identiteetin elinkaari koostuu lisäksi sen käytöstä, hallinnoinnista ja päivittämisestä. Monesti pidemmissä työsuhteissa identiteetin tietoja tarvitseekin päivittää ja muokata esimerkiksi sukunimen tai työtehtävien muuttuessa. Ajan myötä työntekijöille usein myös myönnetään lisää vastuuta, jolloin käyttäjät tarvitsevat uusia käyttöoikeuksia. Lisäksi tietojärjestelmät kehittyvät ja niiden vaihtuminen luonnollisesti aiheuttaa monenlaisia muutoksia myös identiteetinhallintaan.

Identiteetin- ja pääsynhallinnan avulla suoritetaan käyttäjien todentamista ja valtuuttamista, jotta he voivat käyttää yrityksen tietojärjestelmiä ja resursseja. Todentaminen liittyy olennaisesti identiteetinhallintaan, koska sen avulla varmistetaan, että käyttäjä todella vastaa järjestelmään luotua identiteettiä. Todennuksessa voidaan hyödyntää erilaisia suojamekanismeja, kuten salasanoja, digitaalisia varmenteita ja erilaisia kertakirjautumisratkaisuja. Käyttäjän valtuuttaminen puolestaan liittyy pääsynhallintaan ja sen avulla säädellään, mitä resursseja kyseinen identiteetti saa käyttää. Pääsynhallinnassa voidaan hyödyntää mekanismeja, joiden ansiosta työntekijän tarvitsemat käyttöoikeudet voidaan myöntää esimerkiksi työnimikkeen tai roolin perusteella. Todennuksen ja valtuutuksen lisäksi identiteetin- ja pääsynhallinta mahdollistaa identiteetteihin ja niiden

käyttäytymiseen liittyvän tilastoinnin ja raportoinnin. Näiden avulla kerättyä tietoa voitaisiin hyödyntää muun muassa tietoturvaa uhkaavien tilanteiden selvittämisessä.

Nykyaikaisiin identiteetin- ja pääsynhallinnan järjestelmiin liittyy monia hyötyjä. Niiden avulla voidaan parantaa yrityksen tietoturvaa, operatiivista tehokkuutta sekä varmistaa tietosuojaan liittyvän lainsäädännön noudattaminen. Identiteetin- ja pääsynhallinta mahdollistaa tietoturvan kehittämisen muun muassa aiempaa tarkemman ja johdonmukaisemman käyttöoikeuksien hallinnoinnin avulla. Tietoturvan kannalta onkin olennaista, että yrityksen tietoja voivat hyödyntää ainoastaan ne henkilöt, joilla on voimassa oleva lupa kyseisten tietojen käyttämiseen. Identiteetin- ja pääsynhallinnan avulla on myös mahdollista vähentää IT-osaston kuormittuneisuutta ja parantaa työntekijöiden käyttökokemusta muun muassa kertakirjautumisen ja itsepalveluportaalien avulla. Oikeiden salasanojen etsintään ja unohduksiin kuluva aika voidaan siis hyödyntää itse työntekoon, jolloin yrityksen tehokkuus kasvaa. Lisäksi järjestelmät sisältävät tärkeitä työkaluja, jotka helpottavat tietosuojaan liittyvän lainsäädännön noudattamista.

Opinnäytetyön tarkoituksena on löytää toimeksiantajan tarpeisiin soveltuva identiteetinhallinnan ratkaisu ja perehtyä sen testaamiseen. Uuden järjestelmän avulla on tarkoitus korjata nykyisiin menettelyihin liittyviä ongelmia sekä kehittää organisaation tietoturvaa ja käyttövaltuushallinnan tehokkuutta. Opinnäytetyön käytännön osuudessa tutustutaan erilaisiin identiteetin- ja pääsynhallinnan tuotteisiin sekä perehdytään valittavan järjestelmän käyttöönottoon liittyviin valmisteluihin. Järjestelmän valintaan liittyen selvitetään organisaation tarpeita, tutustutaan soveltuviin vaihtoehtoihin sekä valmistellaan valittavan järjestelmän käyttöönottoa testaamisen kautta.

2 IDENTITEETIN- JA PÄÄSYNHALLINTA

Yritystietotekniikassa identiteetin- ja pääsynhallinnalla tarkoitetaan käyttäjäroolien sekä käyttöoikeuksien määrittelyä ja hallintaa yksittäisille verkon käyttäjille. Sen avulla hallitaan tilanteita, joissa käyttäjille joko myönnetään tai evätään oikeuksia tiettyihin yrityksen resursseihin ja järjestelmiin. Hallittavat identiteetit ovat tavallisesti organisaation työntekijöitä, liikekumppaneita tai asiakkaita, jotka jollakin tapaa ovat tekemisissä yrityksen laitteiden ja tietojärjestelmien kanssa. Identiteetin- ja pääsynhallinnan keskeisenä ajatuksena olisikin, että aina yhdelle todelliselle henkilölle luotaisiin yksi sähköinen identiteetti. Kun se on luotu, sitä on ylläpidettävä, muokattava ja seurattava kunkin käyttäjän käyttöiän ajan. (Martin & Waters 2018.)

Organisaatioissa käytettävien tietojärjestelmien ja muiden tietoteknisten ratkaisujen määrä on kasvanut tietojenkäsittelyn sähköistymisen myötä varsin suureksi. Ne sisältävät runsaasti tietosuojan ja yrityksen toiminnan kannalta luottamuksellista tietoa, jota ei haluta kaikkien työntekijöidenkään saataville. Yritysten johdolla ja IT-osastoilla onkin yhä suurempi tarve säädellä yrityksen resurssien saatavuutta sekä käyttäjien pääsyä kriittisiin tietoihin. Tämän vuoksi organisaatioissa ei voida enää luottaa pelkästään manuaalisiin ja virhealttiisiin prosesseihin käyttöoikeuksia määritettäessä. Identiteetin- ja pääsynhallinnan avulla näitä tehtäviä voidaan automatisoida sekä mahdollistaa yrityksen omaisuuden tarkka valvonta niin yrityksen omien palveluiden kuin pilvipalveluidenkin osalta. Parhaimmillaan se voi mahdollistaa kaikkien käyttöoikeuksien hallitsemisen yhdestä keskitetystä järjestelmästä. (Rouse ym. 2020.)

Identiteetin- ja pääsynhallinnan avulla järjestelmänvalvojat pystyvät muokkaamaan sekä yksittäisten käyttäjien että käyttäjäryhmien rooleja ja oikeuksia. Roolien perusteella käyttäjälle pystytään kerralla myöntämään tarvittavat käyttöoikeudet moniin eri tietojärjestelmiin esimerkiksi työnimikkeen perusteella. Identiteettien provisiointia ja deprovisiointia on myös mahdollista automatisoida muista järjestelmistä tuotavan datan avulla. Sen ansiosta uudet työntekijät voivat heti työsuhteen alkaessa saada käyttöönsä tarvitsemansa käyttöoikeudet ja resurssit. Identiteetin- ja pääsynhallinnan avulla pystytään lisäksi jäljittämään käyttäjien toimintaa sekä luomaan näihin liittyviä raportteja. Sen avulla järjestelmänvalvojat ja organisaation johto pystyvät yhdessä valvomaan yrityksen omien käytäntöjen sekä lainsäädännön noudattamista. (Martin & Waters 2018.)

Identiteetin- ja pääsynhallinta voidaan jakaa kahteen osaan: identiteetinhallintaan ja pääsynhallintaan. Näiden lisäksi tässä luvussa tutustutaan sähköisen identiteetin

määritelmään sekä identiteetin- ja pääsynhallinnan tyypillisiin ominaisuuksiin, joita ovat kertakirjautuminen, yhdistetty identiteetinhallinta ja itsepalveluportaali.

2.1 Sähköinen identiteetti

Tietotekniikassa sähköisellä identiteetillä tarkoitetaan kokoelmaa, jossa kohdetta kuvataan erilaisilla attribuuteilla. Identiteettejä voivat olla niin ihmiset, laitteet kuin yhteistyöyrityksenkin työntekijät. Ihmiseen liitettäviä attribuutteja voivat olla muun muassa nimi, käyttäjätunnus sekä mahdolliset käyttövaltuudet eri tietojärjestelmien käyttämiseksi. Laitteiden, esimerkiksi tietokoneiden osalta attribuutteina voivat toimia muun muassa domainnimi sekä IP-osoite. Identiteetin- ja pääsynhallinnassa keskitytään kuitenkin pääasiassa ihmisten sähköiseen identiteettiin, sillä yrityksessä tai yrityksen nimissä työskennellessään ihmiset usein tarvitsevat käyttövaltuuksia moniin erilaisiin tietojärjestelmiin. (Linden 2015, 10; ISO / IEC 24760-1:2019.)

Sähköinen identiteetti voidaan ajatella todellisen henkilön abstraktiona tietojärjestelmässä. Identiteetin ja siihen liittyvien yksilöivien attribuuttien avulla pystytäänkin tyypillisesti tunnistamaan, kenelle tosielämän henkilölle kyseinen identiteetti kuuluu. Henkilöllisyys-käsitteestä poiketen yhdellä ihmisellä on kuitenkin mahdollista olla useampia sähköisiä identiteettejä. Henkilöllä voi esimerkiksi olla yksi identiteetti yrityksen työntekijänä ja toinen identiteetti saman organisaation asiakkaana. Useimmiten on kuitenkin tarkoituksenmukaista välttää moninkertaisten identiteettien luomista samalle henkilölle yhden järjestelmän sisällä. (Linden 2015, 10.)

2.2 Identiteetinhallinta (IdM)

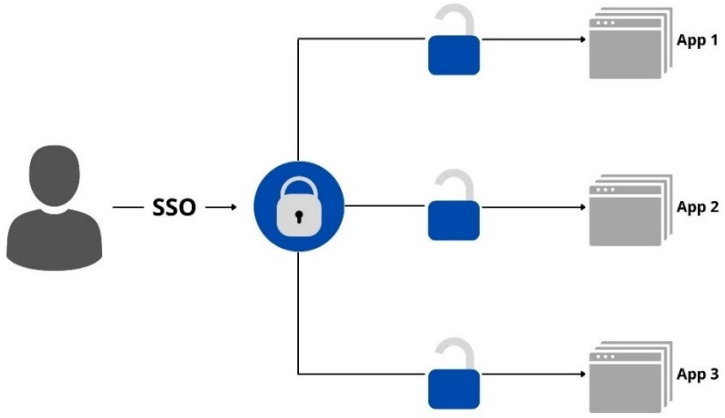
Identiteetinhallinnalla tarkoitetaan sähköisten identiteettien ja niihin liittyvien attribuuttien hallintaa. Identiteetit ja niihin liittyvät merkinnät muodostavat tietokannan, josta käyttäjien sähköisiä identiteettejä voidaan yksilöllisesti hallita. Sen avulla yritysverkkoon kuuluvia sähköisiä identiteettejä voidaan luoda, ylläpitää, seurata ja poistaa. Identiteetinhallinnan ansiosta yritykset voivat myös varmistaa, että käyttäjillä on tarvittavat käyttöoikeudet työtehtäviensä suorittamiseen ja toisaalta varmistaa, ettei työntekijöillä ole pääsyä tarpeettomiin resursseihin. Identiteetin- ja pääsynhallinnassa identiteetinhallinta toteuttaa käyttäjien autentikoinnin eli todennuksen sekä mahdollisesti toimittaa käyttäjästä tietoja pääsynhallinnan prosesseihin. (Canner 2020.)

2.3 Pääsynhallinta (AM)

Pääsynhallinta ohjaa päätöksiä siitä, sallitaanko vai estetäänkö käyttäjän pääsy valittuun tietojärjestelmään tai muuhun yrityksen resurssiin. Päätös perustuu ensisijaisesti käyttäjän identiteettitiedoissa oleviin attribuutteihin. Kun käyttäjän identiteetti on identiteetinhallinnan avulla todennettu, pääsynhallintajärjestelmä voi käyttäjästä toimitettujen attribuuttien perusteella tehdä joko myöntävän tai kieltävän päätöksen kohteen avaamisesta. Pääsynhallinnan tehtävänä olisikin valvoa, että identiteetinhallinnassa määriteltyjä rooleja ja käyttövaltuuksia toteutetaan käytännössä. Pääsynhallinta toteuttaa siis käyttäjien auktorisointia eli valtuuttamista. (Ihalainen 2016.)

2.4 Kertakirjautuminen (SSO)

Kertakirjautuminen on mekanismi, jossa käyttäjälle valtuutetaan pääsy useisiin eri tietojärjestelmiin yhdellä todennustoimenpiteellä. Sen avulla käyttäjän ei tarvitse erikseen kirjautua moniin eri järjestelmiin saman istunnon aikana. Tämä mahdollistaa helpon ja nopean liikkuvuuden palveluiden välillä, kun tarve manuaaliselle kirjautumiselle pienenee. Kertakirjautuminen ei kuitenkaan tarkoita sitä, että kaikissa palveluissa ja tietojärjestelmissä olisi samat ja yhteneväiset tunnistetiedot. Se ennemminkin piilottaa useat tunnistetiedot yhdelle tilille, jota käyttämällä käyttäjä voi kirjautua useisiin eri palveluihin. Kertakirjautumisen ansiosta käyttäjien ei myöskään tarvitse muistaa ulkoa useita erilaisia salasanoja. Lisäksi tämä helpottaa IT-tuen tehtäviä, kun unohtuneiden ja resetoitavien salasanojen määrä pienenee. Kuva 1 havainnollistaa kertakirjautumistapahtuman toimintaa. (Radha & Reddy 2012.)



Kuva 1. Kertakirjautuminen.

Kertakirjautumisratkaisut voidaan jakaa kahteen pääkategoriaan: selainpohjaiseen kertakirjautumiseen (Web SSO) ja asiakasohjelmaan perustuvaan kertakirjautumiseen (eSSO). Kertakirjautuminen voidaan mahdollistaa myös näiden yhdistelmällä.

2.4.1 Selainpohjainen kertakirjautuminen (Web SSO)

Selainpohjaista kertakirjautumista voidaan nimensä mukaisesti hyödyntää vain erilaisten verkkosovellusten kanssa. Siinä käyttöoikeuksiin liittyvät käytännöt luodaan keskeiselle käytäntöpalvelimelle, jossa voidaan määritellä, kenellä on pääsy mihinkin verkkosovellukseen. Valvonta-agenttina toimii tavallisesti käänteinen verkonvälityspalvelin tai verkkopalvelimen laajennus, joka otetaan käyttöön verkkoliikenteen sieppaamiseksi. Valvonta-agentin tehtävänä on todentaa käyttäjä käyttäjätietovaraston, tavallisesti LDAP-hakemiston avulla ja sen jälkeen tarkistaa käyttäjälle asetetut käyttöoikeudet käytäntöpalvelimelta. Mikäli käyttöoikeus on olemassa, välitetään pyyntö verkkopalvelimelle käyttäjän sisään kirjaamiseksi. Kun käyttäjä on kirjautuneena yhteen palveluun, voi hän saman istunnon aikana käyttää useita sivustoja ilman uudelleentodentamista. (PathMaker Group.)

Selainpohjainen kertakirjautuminen on erittäin hyödyllinen ympäristöissä, joissa käytetään runsaasti erilaisia verkkosovelluksia. Käyttäjien lisäksi se tuo hyötyä myös verkkosovellusten kehittäjille, koska sen ansiosta he voivat oman tietoturvansa rakentamisen sijaan hyödyntää kertakirjautumisen suojauskehystä. Sen myötä käyttäjätunnus saadaan helposti HTTP-otsikkomuuttujana. Tällä tavoin käyttäjällä on vain yksi salasana Web SSO -tuotteessa tunnistautumiseksi, eikä yksittäisten sovellusten tarvitse tallentaa salasanatietoja käyttäjälle. (PathMaker Group.)

2.4.2 Asiakasohjelmaan perustuva kertakirjautuminen (eSSO)

Asiakasohjelmaan perustuva kertakirjautuminen tuo kertakirjautumisen käytännössä kaikkiin loppukäyttäjän tarvitsemiin sovelluksiin. Se toimii niin web-sovelluksissa kuin muissakin työasemalla käytettävissä ohjelmistoissa. Asiakasohjelmaan perustuvan SSO:n toiminta perustuu siihen, että se tallentaa muistiinsa sovellusten käyttäjätunnukset ja salasanat silloin, kun käyttäjä kirjautuu sisään. Seuraavan kerran kun sovellus käynnistetään, eSSO tunnistaa tilanteen ja syöttää automaattisesti tunnistetiedot kirjautuen samalla sisään. Asiakasohjelmaan perustuvaan kertakirjautumiseen kuuluu

luonnollisesti myös loppukäyttäjän työpöydälle asennettava ohjelmatiedosto, jonka profiilit luodaan tunnistamaan kaikki tarvittavat kirjautumistilanteet. Lisäksi se voidaan ohjelmoida käsittelemään salasananvaihtoja, muun muassa sellaisia tilanteita varten, joissa salasana olisi vanhenemassa. Koska sovelluksiin ei tehdä muutoksia, asiakasohjelmaan perustuva SSO tarjoaa suhteellisen helposti toteutettavan kertakirjautumisratkaisun useimmille käyttäjän tarvitsemille sovelluksille. (PathMaker Group.)

2.5 Yhdistetty identiteetinhallinta (FIM)

Yhdistetyllä identiteetinhallinnalla (engl. federated identity management) tarkoitetaan järjestelyä, jossa kahden tai useamman toimialueen (engl. domain) välillä käytetään samaa sähköistä identiteettiä. Sen avulla käyttäjät voivat hyödyntää eri toimialueiden alla suoritettavia sovelluksia ja palveluita samoilla käyttäjätunnuksilla. Päätoimialueen ohella, niin sanottuina luotettuina toimialueina voivat olla esimerkiksi yhteistyöyritysten tai tytäryhtiöiden toimialueet. Identiteettien yhdistäminen mahdollistetaan identiteetin- ja pääsynhallintajärjestelmiin kuuluvien identiteetinvälittäjien avulla. Identiteetinvälittäjät ovat palveluntarjoajia, jotka mahdollistavat pääsynhallinnan välittämisen useampien palveluntarjoajien välillä. Yhdistetyssä identiteetinhallinnassa järjestely toteutetaan käytännössä kahden tai useamman identiteetinvälittäjän avulla. (Nallathamby 2018.)

2.6 Itsepalveluportaali

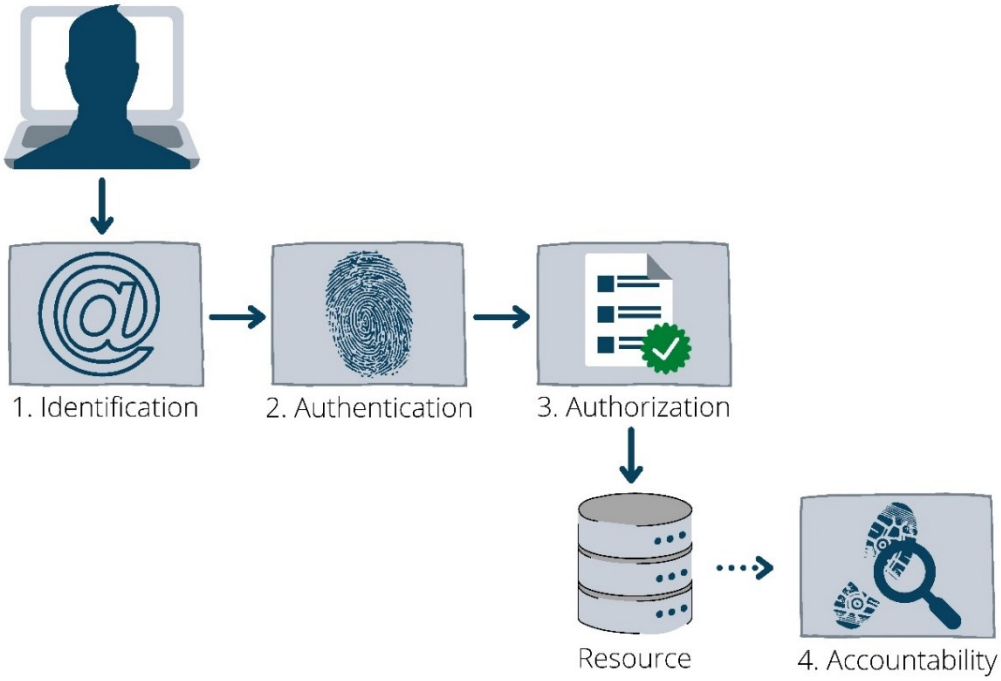
Identiteetin- ja pääsynhallintajärjestelmiin sisältyvien itsepalvelutoimintojen avulla käyttäjät voivat tehdä identiteettiinsä liittyviä muutoksia ilman yhteydenottoa IT-tukeen. Itsepalveluportaalin kautta käyttäjä voi muun muassa vaihtaa salasanansa helposti ja turvallisesti useampiin kokonaisuuteen liitettyihin järjestelmiin yhdellä salasananvaihdolla. Itsepalveluportaalin avulla käyttäjän on lisäksi mahdollista resetoida salasanansa tilanteissa, joissa salasana on joko unohtunut tai vanhentunut. Tavallisesti näissä tilanteissa käyttäjä joutuisi ottamaan yhteyttä IT-tukeen salasanansa resetoimiseksi. Tämä tuo käyttäjien lisäksi suuren hyödyn myös IT-tuelle, sillä salasanojen resetointipyynnöt tavallisesti kuormittavat IT-tukea suhteellisen paljon. Salasanan resetointi voitaisiin itsepalveluportaalissa toteuttaa esimerkiksi turvakysymysten tai tekstiviestillä lähetettävien kertakäyttöisten salasanojen avulla. (Friedensburg 2018.)

Itsepalveluportaalissa käyttäjien on myös mahdollista muokata omia yhteystietojaan. Tavallisesti yhteystiedot rekisteröidään vain käyttäjätilin luomisen yhteydessä. Osa tiedoista voi kuitenkin muuttua ajan myötä, ja usein nämä muutokset jäävät tekemättä käyttäjän profiiliin. Itsepalveluportaalin ansiosta tietoja olisi kuitenkin helpompi muokata ja pitää ajan tasalla. Tällaisia muutoksia voisivat olla esimerkiksi puhelinnumeron tai osoitteen vaihtuminen. Osa tiedoista ei kuitenkaan välttämättä ole käyttäjien itsensä muokattavissa, sillä jotkin muutokset saattavat vaatia vielä tarkistuksen tai muun manuaalisen käsittelyn. (Friedensburg 2018.)

Tietojensa muokkaamisen lisäksi käyttäjien olisi mahdollista pyytää itsepalveluportaalin kautta pääsy- ja käyttöoikeuksia saatavuudeltaan rajoitettuihin palveluihin ja resursseihin. Oikeus resurssin käyttämiseen myönnetään tavallisesti vasta hyväksymisen jälkeen. Järjestelmän avulla hyväksymispyyntöjä on kuitenkin mahdollista ohjata kulkemaan automaattisesti organisaation käytänteiden mukaisesti esimerkiksi esimiehen tai resurssin omistajan kautta, jolloin pyyntöjen käsittelystä saadaan entistä tehokkaampaa. Näiden lisäksi kaikki muutoksiin liittyvät toimet luovat muutoshistoriaa, mikä helpottaa mahdollisten väärinkäytösten selvittämistä. (Friedensburg 2018.)

3 IDENTITEETIN- JA PÄÄSYNHALLINNAN TEHTÄVÄT

Identiteetin- ja pääsynhallinnan vaiheita voidaan tarkastella IAAA-kehyksen avulla. IAAA tulee sanoista: identification (tunnistaminen), authentication (todennus), authorization (valtuutus) ja accounting (tilastointi). Kyseiset vaiheet suoritetaan kuvan 2 mukaisessa järjestyksessä. Tunnistaminen ja todentaminen liittyvät käyttäjän identiteetin varmistamiseen. Kun identiteetti on onnistuneesti vahvistettu, valtuutus tarkistaa myönnetyt käyttöoikeudet ja tekee päätöksen halutun resurssin avaamisesta. Edellisiin vaiheisiin liittyviä toimia voidaan selvittää ja tarkastella jälkikäteen tilastoinnin avulla.



Kuva 2. IAAA-kehys.

3.1 Tunnistus

Tunnistaminen (engl. identification) on pääsynvalvonnan ensimmäinen vaihe. Sillä tarkoitetaan toimenpidettä, jossa käyttäjä ilmoittaa identiteettinsä. Tosielämässä tämä vastaisi tilannetta, jossa vieras henkilö tavataan ensimmäistä kertaa ja esittäydytään nimellä. Digitaalisessa maailmassa tunnistautuminen tapahtuu useimmiten käyttäjänimellä tai sähköpostiosoitteella, jonka käyttäjä syöttää sille tarkoitettuun tekstikenttään. Tunnistaminen ei kuitenkaan takaa väitetyn identiteetin oikeellisuutta, sillä kuka tahansa saattaisi esittäytyä toisen nimissä. (Vitale 2019.)

3.2 Todennus

Todennus (engl. authentication) on toimenpide, jossa vahvistetaan käyttäjältä saadun syötteen oikeellisuus. Sen tarkoituksena on vahvistaa käyttäjän identiteetti, jotta kohteelle voitaisiin myöhemmässä vaiheessa valtuuttaa pääsy juuri hänen identiteetillensä myönnettyihin resursseihin. Todennus voi tilanteesta riippuen olla joko yksi- tai kaksisuuntaista. Kaksisuuntainen eli keskinäinen todennus on tarpeellista tilanteissa, joissa tarvitaan luottamuksellisuutta molempien osapuolten välillä. Esimerkkinä tällaisesta voidaan pitää digitaalisesti allekirjoitettua ja salattua sähköpostia, jossa molempien osapuolten identiteetit vahvistetaan digitaalisten varmenteiden avulla. (Busso 2018.)

Todentamiskeinot voidaan jakaa viiteen kategoriaan: staattiset salasanat, kertakäyttöiset salasanat, digitaaliset varmenteet, biometriset tunnisteet sekä fyysiset tunnistevälineet. Todentamiskeinona käytetään hyvin usein staattista salasanaa, jolla käyttäjä kirjautuu esimerkiksi nettipalveluun monia kertoja. Todentamisessa käytettävä salasana voi tällöin pysyä pitkiäkin aikoja samana, ellei käyttäjä itse vaihda salasanaansa tai jos salasanan vanhenemiselle on määritelty kesto. Kertakäyttöiset salasanat puolestaan ovat usein kirjeellä, sähköpostilla tai tekstiviestillä lähetettäviä PIN-koodeja, joilla todentaminen onnistuu vain yhden kerran. Digitaalisissa varmenteissa todennus puolestaan perustuu sähköisiin salausavaimiin, joita käytetään muun muassa tietojen salaamisessa ja digitaalisissa allekirjoituksissa. Todennus on mahdollista suorittaa myös biometrisilla tunnisteilla, esimerkiksi sormenjäljellä, kasvojentunnistuksella tai iiristunnistuksella. Identiteetin todentamisessa voidaan lisäksi hyödyntää fyysisiä esineitä, kuten vaikkapa kulkuavaimena käytettävää henkilökorttia. (Busso 2018.)

Kun tarvitaan luotettavampaa todennusta, on mahdollista käyttää kaksivaiheista (2FA) tai monivaiheista todennusta (MFA). Niiden tarkoituksena on estää ja hankaloittaa toisen henkilön nimissä todentautumista. Tällaisessa tilanteessa väärinkäytöstä yrittävä henkilö on voinut saada tietoonsa vieraan henkilön salasanan, mutta ei kuitenkaan pääse kirjautumaan, koska ei tiedä esimerkiksi kyseisen henkilön puhelimeen lähetettyä kertakäyttöistä PIN-koodia. Monivaiheinen todennus perustuukin erityyppisiin tunnistetietoihin, jotka voidaan jakaa seuraavasti: mikä tiedetään (kuten salasana), mikä omistetaan (esim. henkilökortti tai matkapuhelin) ja mitä olet (mm. sormenjälki, kasvot tai silmät). Kahden eri salasanan käyttäminen ei siis täytä kriteerejä, vaan tunnistetietojen tulisi olla keskenään erityyppisiä. (Busso 2018.)

3.3 Valtuutus

Valtuutus (engl. authorization) on toimenpide, jossa käyttäjälle myönnetään lupa tietyn resurssin lukemiseen, muokkaamiseen, käyttämiseen tai siihen liittyvien toimintojen suorittamiseen. Kun käyttäjän sähköinen identiteetti on todennettu, tulee hänen valtuutusvaiheessa läpäistä valtuutussääntö päästäkseen käsiksi järjestelmiin, palveluihin ja tietoihin. Valtuutuksella voidaan tarkasti määrittää, mitä identiteetti voi käyttää ja mitä se ei voi käyttää. Onnistuneesta todennuksesta huolimatta käyttäjän pääsy voidaan siis evätä kielteisen valtuutuspäätöksen tuloksena. (Busso 2018.)

Yrityksen resursseja halutaan tietoturvasyistä suojata, ja sen vuoksi niiden saatavuutta rajoitetaan monilla tavoin. Pääsynhallinnan ja siihen liittyvän valtuutuksen tarkoituksena onkin säädellä resurssien saatavuutta sekä valvoa sääntelyn toteutumista. Yleisenä suuntauksena on ollut vähimpien oikeuksien periaate (PoLP), jossa käyttäjille annetaan pääsyoikeudet vain pakollisten työtehtäviensä suorittamiseen. Periaatteen perusteluna on se, että jokainen ylimääräinen valtuus voisi johtaa tahattomiin tai haitallisiin tietoturvakäytäntöjen rikkomuksiin. (Busso 2018.)

3.4 Tilastointi

Tilastointi (engl. accounting) on IAAA-kehyksen viimeinen osuus. Sillä tarkoitetaan prosessia, jolla seurataan käyttäjän toimintaa niissä järjestelmissä, jotka ovat liitettynä identiteetin- ja pääsynhallinnan järjestelmään. Se tallentaa dataa muun muassa resurssien käyttökerroista, niissä vietetystä ajasta sekä siirretyn datan määrästä ja laadusta. Tilastoinnilla kerättyä dataa voidaan käyttää esimerkiksi erilaisten trendien analysointiin sekä mahdollisten rikkomusten havaitsemiseen ja tutkintaan. Tilastointi voikin osoittautua erittäin arvokkaaksi välineeksi esimerkiksi tapahtuneiden tietoturvarikkeiden jäljittämisessä. (Busso 2018.)

4 TODENNUS- JA VALTUUTUSMEKANISMIT

Todennus ja valtuutus liittyvät olennaisesti identiteetin- ja pääsynhallintaan. Todennuksen ja valtuutuksen toteuttamiseen on olemassa erilaisia menetelmiä, joita esitellään tarkemmin tässä luvussa.

4.1 Todennusmekanismit

Todennukseen käytettäviä mekanismeja on monentyyppisiä. Ne voidaan jakaa kahteen pääkategoriaan: fyysisiin ja digitaalisiin suojausmekanismeihin. Niiden merkittävimpänä erona on se, että fyysiset suojausmekanismit tarvitsevat aina jonkinlaisen konkreettisen tuotteen tai henkilöä yksilöivän piirteen todennusta varten. Digitaaliset suojausmekanismit puolestaan perustuvat usein käyttäjillä olevaan tietoon. Todennus on kuitenkin mahdollista toteuttaa myös erilaisten mekanismien yhdistelmillä. Näin on mahdollista toteuttaa omia tarpeita vastaava suojauksen taso.

4.1.1 Fyysiset suojausmekanismit

Fyysisten suojausmekanismien tarkoituksena on suojata resurssien saatavuutta identiteettiin liittyvien fyysisten ominaisuuksien sekä todentamiseen soveltuvien esineiden avulla. Todennuksessa voidaan hyödyntää muun muassa työntekijän hallussa olevia ammatti- ja kulkukortteja, työpuhelimessa toimivaa mobiilivarmennetta sekä erilaisia biometrisiä tunnisteita, kuten kasvojen-, sormenjälki- ja iiristunnistusta. Fyysisiä suojausmekanismeja käytetään useimmiten rinnakkain digitaalisten suojausmekanismien kanssa, jolloin esimerkiksi sormenjäljen kuluminen ei estä kirjautumista eikä toisaalta ammattikortin joutuminen vääriin käsiin mahdollistaisi kirjautumista ilman PIN-koodia tai salasanaa. (Indu, Rubesh Anand & Bhaskar 2018.)

4.1.2 Digitaaliset suojausmekanismit

Digitaalisia suojausmekanismeja on monia. Ne voidaan luokitella kredentiaaleihin, SSH-avainmekanismeihin, sirun ja PIN-koodin yhdistelmiin sekä monivaiheiseen

todentamiseen. Yleisesti tunnettuja digitaalisia suojausmekanismeja ovat lisäksi aiemmin esitelty kertakirjautuminen sekä avoimet standardit: OpenID, OAuth ja SAML.

Kredentiaalit

Kredentiaalit ovat todisteita valtuuksista, asemasta, käyttöoikeuksista ja etuoikeuksista. Ne osoittavat, että käyttäjä ansaitsee käyttää tiettyjä resursseja ja palveluita. Kredentiaalien, kuten staattisten ja kertaluonteisten salasanojen, kuvioiden ja kuvavarmennuksien (CAPTCHA) tarkoituksena on suojata järjestelmää haitallisilta toimilta. Yrityksen verkossa ja pilviympäristössä toimivien resurssien saatavuutta hallinnoidaankin useimmiten LDAP- ja *Microsoft Active Directory* (AD) -tekniikoiden avulla. Niitä käyttämällä on välttämätöntä lisätä, muokata, sulkea ja tarvittaessa poistaa käyttäjätilejä. Niiden avulla hallitaan samalla myös kredentiaaleja, joiden hallinnan turvallisuuteen tulee kiinnittää erityistä huomiota. Heikosti toimivat salasanan palauttamismekanismit ja kredentiaalien vääränlainen käsittely voivatkin aiheuttaa järjestelmiin suuria haavoittuvuuksia. Kredentiaalien päätyminen vääriin käsiin voisi pahimmassa tapauksessa aiheuttaa suurta haittaa organisaation toiminnalle, mikäli henkilötietoja tai muuta luottamuksellista ja salaista tietoa päätyy ulkopuolisille. (Indu, Rubesh Anand & Bhaskar 2018.)

Monivaiheinen todennus

Kredentiaalien suojaustasoa voidaan tarvittaessa parantaa monivaiheisen todennuksen avulla. Perinteisen staattisen salasanan ohella käytetään usein esimerkiksi kertakäyttöisiä salasanoja. Tämä voidaan toimittaa käyttäjälle vaikkapa ennalta ilmoitettuun puhelinnumeroon tai sähköpostiosoitteeseen. Kertakäyttöistä salasanaa voidaan käyttää vain yhden kerran ja sen kelpoisuuteen voi liittyä aikaraja. Usein nämä ovat 4- tai 6-numeroisia PIN-koodeja. Monivaiheisen todennuksen avulla voidaan myös suojella järjestelmää ohjelmallisesti toteutetuilta hyökkäyksiltä. Tätä voidaan toteuttaa esimerkiksi kuvavarmennuksen (CAPTCHA) avulla, jolloin käyttäjää pyydetään ratkaisemaan jonkinlainen tehtävä tunnistetietojen syöttämisen yhteydessä. Käyttäjän tehtävänä voi olla esimerkiksi kirjaimien tunnistaminen, matemaattisen yhtälön ratkaiseminen tai kuvien tunnistaminen. Tehtävien tarkoituksena on varmistaa, että palvelun käyttäjä on todellinen ihminen eikä tietokone. Monivaiheista todennusta voidaan lisäksi käyttää pääsyn turvaamiseen. Salasanan unohtumisen seurauksena käyttäjä voi esimerkiksi vastata tilin

luomisen yhteydessä määritettyihin turvakysymyksiin tai tilata uuden tilapäisen salasanan tekstiviestillä toimitettuna. (Indu, Rubesh Anand & Bhaskar 2018.)

SSH-avainmekanismit

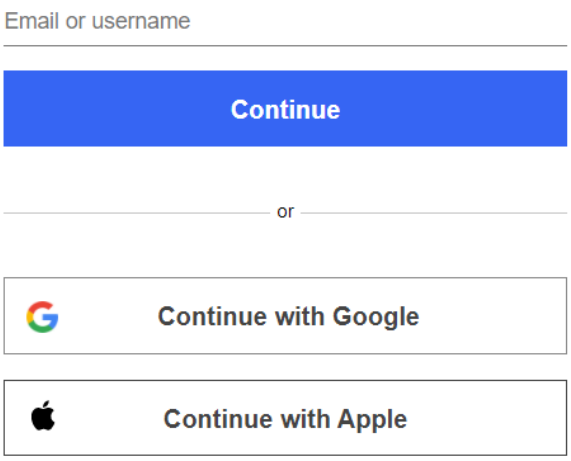
SSH-avaimet (engl. Secure Shell keys) ovat yksi digitaalisista suojausmenetelmistä. Ne auttavat tunnistamaan SSH-palvelimen julkisen avaimen salauksen tai pyyntö-vastaus -todennuksen avulla. Merkittävimpänä etuna on, että todennus palvelimelle suoritetaan ilman salasanan kuljettamista verkon yli. Sen ansiosta salasanoja ei pystytä sieppaamaan siirron aikana tai murtamaan väsytyshyökkäyksillä. Lisäksi se helpottaa käyttäjiä, kun heidän ei tarvitse muistaa pitkiä ja monimutkaisia salasanoja. Käytännössä todennus suoritetaan SSH-avainagentin avulla, joka tallettaa yksityiset avaimet ja toimittaa ne SSH-asiakasohjelmille. Yksityiset avaimet salataan tunnuslauseilla (engl. passphrases) eli pitkillä salasanoilla ja ne välitetään palvelimelle jokaisen yhteyden muodostamisen yhteydessä. Näitä tunnuslauseita käytetään salausten purkamiseen ennen todennusvaiheeseen siirtymistä, kun yksityinen avain lisätään agentin varastoon. SSH-agentti on käynnissä automaattisesti, kun sisäänkirjautuminen aloitetaan ja jatkuu koko istunnon ajan. Siten se mahdollistaa myös kertakirjautumisen SSH-palvelimissa, joihin yhteys on muodostettuna. SSH-avainmekanismit ja staattiset kredentiaalit ovatkin yleisesti käytettyjä todentamismenetelmiä verkkopalveluissa. (Indu, Rubesh Anand & Bhaskar 2018.)

Siru ja PIN

Sirun ja PIN-koodin yhdistelmä on digitaalinen suojausmekanismi, jota käytetään yleisesti esimerkiksi pankkien tarjoamissa maksukorteissa. Samaa mekanismia voidaan hyödyntää myös organisaatioissa sen verkkoon kuuluviin koneisiin sekä palveluihin kirjautumisessa. Mikroprosessorisirut sisältävät käyttäjätietoja ja suojausavaimia, joiden avulla luodaan yksilöllisiä tapahtumatietoja. PIN-koodia käytetään käyttäjän todentamiseen, jotta sirulle tallentuneita käyttäjätietoja ja suojausavaimia voitaisiin hyödyntää. Todennuspalvelimen ja asiakaspäätteen välinen tiedonsiirto salataan ja allekirjoitetaan sirulle tallennetun suojausavaimen avulla. Palvelin tarkistaa allekirjoituksen ja purkaa vastaanotetun tapahtumatiedon palvelimeen tallennettujen pariliitosavainten avulla. Tämän jälkeen palvelin voi palauttaa vastauksen päätteelle. (Indu, Rubesh Anand & Bhaskar 2018.)

OpenID

OpenID on avoimen standardin todennusmenetelmä, joka mahdollistaa käyttäjän todentamisen kolmansien osapuolten palveluilla. Sen avulla voidaan kirjautua verkkosivustolle jo olemassa olevan tilin avulla ilman, että tarvitsee luoda uusia salasanoja. Käyttäjä kirjautuu vain entuudestaan tutulle identiteetin välittävälle sivustolle ja se toimittaa tarvittavia identiteettitietoja avattavalle verkkosivustolle. OpenID:tä käyttämällä voidaan myös valita, kuinka paljon tietoja avattavalle verkkosivustolle halutaan välittää. Verkkosivustolle ei kuitenkaan missään vaiheessa välitetä salasanaa, jolloin tietoturva ei tarpeettomasti vaarannu. Se ei kuitenkaan poista riskiä siitä, etteikö sivusto voisi ohjata käyttäjän salasanatietoja kalastelevalle sivustolle. Tunnettuja identiteetin välittäviä palveluita ovat esimerkiksi *Google Account* ja *Apple ID*, kuten kuvassa 3 on esitetty. (Indu, Rubesh Anand & Bhaskar 2018; OpenID.)



Kuva 3. Kirjautuminen OpenID-vaihtoehdoilla.

OAuth

OAuth on avoimen standardin valtuutusmenetelmä, jonka avulla kolmansien osapuolten sovellukset voivat saada rajoitetun pääsyn henkilön käyttäjätiliin. Sen avulla luodaan siis eräänlaisia valtuuksia sovellusten käyttämiseen ilman tunnistetietojen jakamista. Kolmannen osapuolen sovellus voisi esimerkiksi luoda Facebookiin julkaisuja käyttäjätiliä hyödyntämällä tai Facebookin käyttäjätiliä voitaisiin käyttää kommenttien kirjoittamiseen uutis- ja blogisivustoilla. Se siis mahdollistaa niin yksisuuntaisen kuin keskinäisenkin todennuksen palveluiden välillä. (Raittius 2018.)

Kolmannen osapuolen sovellukselle myönnetään tarvittavat valtuudet identiteettiä jakavan palvelun avulla. Tällöin käyttäjä kirjautuu palveluun ja hyväksyy sovellusten välisen vuorovaikutuksen. Sen jälkeen identiteettiä jakava sovellus luovuttaa OAuth-käyttöoikeustunnuksen yhteydessä päivitystunnuksen, asiakastunnuksen ja asiakassalaisuuden (engl. client secret). Näiden avulla kolmas osapuoli voi hakea tietoja käyttövaltuuden päätepisteestä sekä uudistaa käyttöoikeustunnusten voimassaolon. Käyttäjä voi myös itse tarvittaessa hallinnoida valtuuksia identiteettiä jakavasta palvelusta. Esimerkiksi Facebook-tunnusta hyödyntävien palveluiden käyttöoikeuksia voidaan rajata, hallinnoida ja poistaa Facebook-profiilin asetuksista. (Indu, Rubesh Anand & Bhaskar 2018.)

SAML

SAML on avoin standardi, jonka avulla käyttöoikeustietoja voidaan välittää identiteetintarjoajalta palveluntarjoajille. Se mahdollistaa turvallisen kommunikaation sovellusten välillä sekä antaa käyttäjille pääsyn toisiin sovelluksiin yksillä tunnistetiedoilla. Identiteetintarjoajan ja palveluntarjoajan välisessä kommunikoinnissa hyödynnetään XML-merkintäkieltä. Sitä käyttämällä identiteetintarjoaja (esimerkiksi *Microsoft AD*) lähettää palveluntarjoajalle SAML-vahvistuksen, joka sisältää todennus- ja valtuutustiedot sekä tietoa käyttäjästä. Todennustiedot ilmoittavat käyttäjän identiteetin, kirjautumisajan sekä hänen käyttämänsä todennusmenetelmän ilman salasanatietojen välittämistä. Valtuutustiedot puolestaan vahvistavat, onko käyttäjällä oikeus käyttää kyseistä palvelua ja minkä asteiset valtuudet hänellä on. Näiden perusteella palveluntarjoaja joko mahdollistaa tai hylkää sovellukseen pääsyn. SAML:n ansiosta käyttäjän ei myöskään tarvitse syöttää tunnistetietojaan uudestaan palveluiden välillä siirtyessään. Lisäksi SAML mahdollistaa käyttäjienhallinnan keskittämistä, jolloin useamman järjestelmän sijasta hallintaa voidaan toteuttaa yhdessä järjestelmässä. (Shepherd 2020.)

4.2 Valtuutusmekanismit

Identiteetin- ja pääsynhallinnan järjestelmissä käyttöoikeuksia hallitaan useimmiten roolitai attribuuttipohjaisen pääsynvalvontamekanismin avulla. Näiden lisäksi on olemassa muita valtuutuksen mekanismeja. Mekanismeja ovat

- pakollinen pääsynvalvonta (MAC)
- harkinnanvarainen pääsynvalvonta (DAC)

- käyttöoikeus-/tehtäväpohjainen pääsynvalvonta
- roolipohjainen pääsynvalvonta (RBAC)
- attribuuttipohjainen pääsynvalvonta (ABAC).

4.2.1 Roolipohjainen pääsynvalvonta (RBAC)

Roolipohjainen pääsynvalvonta (RBAC) on pääsynhallinnan mekanismi, jossa käyttöoikeudet perustuvat käyttäjien rooleihin ja asemaan. Käyttöoikeudet myönnetään erilaisten parametrien, kuten käyttäjäroolien, rooliin liittyvien lupien ja rooli-rooli -suhteiden avulla. Roolit voidaan luokitella kahteen kategoriaan: sovellusrooleihin ja organisaatiorooleihin. Sovellusrooli sisältää yhdistelmän erilaisia sovelluskohtaisia oikeuksia tai tehtäviin perustuvia käyttölupia, mutta sen soveltamisala rajoittuu vain tiettyyn sovellukseen. Organisaatiorooli taas muodostetaan työntekijälle kohdennetun työnkuvan ja käyttöoikeuksien perusteella. Organisaatiorooli onkin usein yhdistelmä erilaisia sovellusrooleja. (Indu, Rubesh Anand & Bhaskar 2018.)

Roolipohjainen pääsynvalvonta tarjoaa turvallisen käyttövaltuushallinnan organisaatioissa, joissa on paljon käyttäjiä ja runsaasti käyttöoikeuksia. Käyttöoikeuksien myöntäminen käyttäjälle koostuu käytännössä kolmesta säännöstä: roolin määrittäminen, roolin valtuuttaminen sekä käyttöoikeuksien valtuuttaminen. Käyttöoikeudet resursseihin ansaitaan siis näiden sääntöjen perusteella. Tämän ansiosta roolipohjainen pääsynvalvonta mahdollistaa hyvin suojatun ympäristön käyttöoikeuksien myöntämiselle. Roolit voivat kuitenkin ajoittain muuttua, minkä vuoksi muutokset tulee tarkistuttaa ja vahvistaa todellisessa ympäristössä. (Indu, Rubesh Anand & Bhaskar 2018.)

4.2.2 Attribuuttipohjainen pääsynvalvonta (ABAC)

Attribuuttipohjainen pääsynvalvonta (ABAC) on mekanismi, jossa käyttövaltuuksia hallitaan käytäntöjen perusteella. Roolien sijasta käyttöoikeuksien määritteleminen perustuu erilaisten attribuuttien arviointiin. Nämä attribuutit voivat olla subjekti-, objekti-, resurssi- ja ympäristöattribuutteja. Niihin liittyvät käytännöt voivat määritellä kullekin käyttäjälle erilaisen joukon käyttöoikeuksia. Käyttöoikeuksien määrään ja laatuun voivat vaikuttaa käyttäjän ominaisuudet, jolloin esimerkiksi esimiestason työntekijälle voidaan myöntää tiedostoihin muokkausoikeudet ja heidän alaisilleen vain lukuoikeudet. Roolipohjaiseen pääsynvalvontaan verrattuna attribuuttipohjainen pääsynvalvonta pystyy siis

käsittelemään useampia ulottuvuuksia. Käyttöoikeudet voidaan määrittää IF- ja THEN-lausekkeiden avulla siten, että useammat roolit voidaan korvata yhdellä käyttövaltuusryhmällä. Sen avulla saavutetaan lisäksi tehokas käytäntöjen noudattaminen ja saadaan lisää joustavuutta pääsynhallinnan toteuttamiseen. (Indu, Rubesh Anand & Bhaskar 2018; Casey 2020.)

4.2.3 Pakollinen pääsynvalvonta (MAC)

Pakollinen pääsynvalvonta (MAC) on perinteinen käyttöoikeuksien määrittämiseen käytetty mekanismi, jolla voidaan rajoittaa tiedostojen omistajien kykyä myöntää tai evätä käyttöoikeuksia tiedostojärjestelmässä. Järjestelmänvalvoja asettaa kaikki pääsynvalvonnan oikeudet, joiden mukaan käyttöjärjestelmä tai suojausydin (engl. security kernel) säätelee tiedostojen saatavuutta. Tavallisilla käyttäjillä ei siis ole oikeutta hallita käyttöoikeuksia. Pakollisessa pääsynvalvonnassa jokaiselle tiedostojärjestelmässä sijaitsevalle objektille on asetettu luokitustaso, kuten 'salainen', 'erittäin salainen' tai 'luottamuksellinen'. Vastaavasti myös jokaiselle käyttäjälle on määritetty luokitustaso. Näiden perusteella käyttöjärjestelmä tai suojausydin tarkistaa tunnistetiedot ja säätelee resurssien saatavuutta. Vaikka pakollinen pääsynvalvonta mahdollistaa resurssien vahvan suojaamisen, se vaatii kuitenkin huolellista suunnittelua ja säännöllistä valvontaa, jotta kaikki luokitustasot pysyvät ajan tasalla. (Indu, Rubesh Anand & Bhaskar 2018.)

4.2.4 Harkinnanvarainen pääsynvalvonta (DAC)

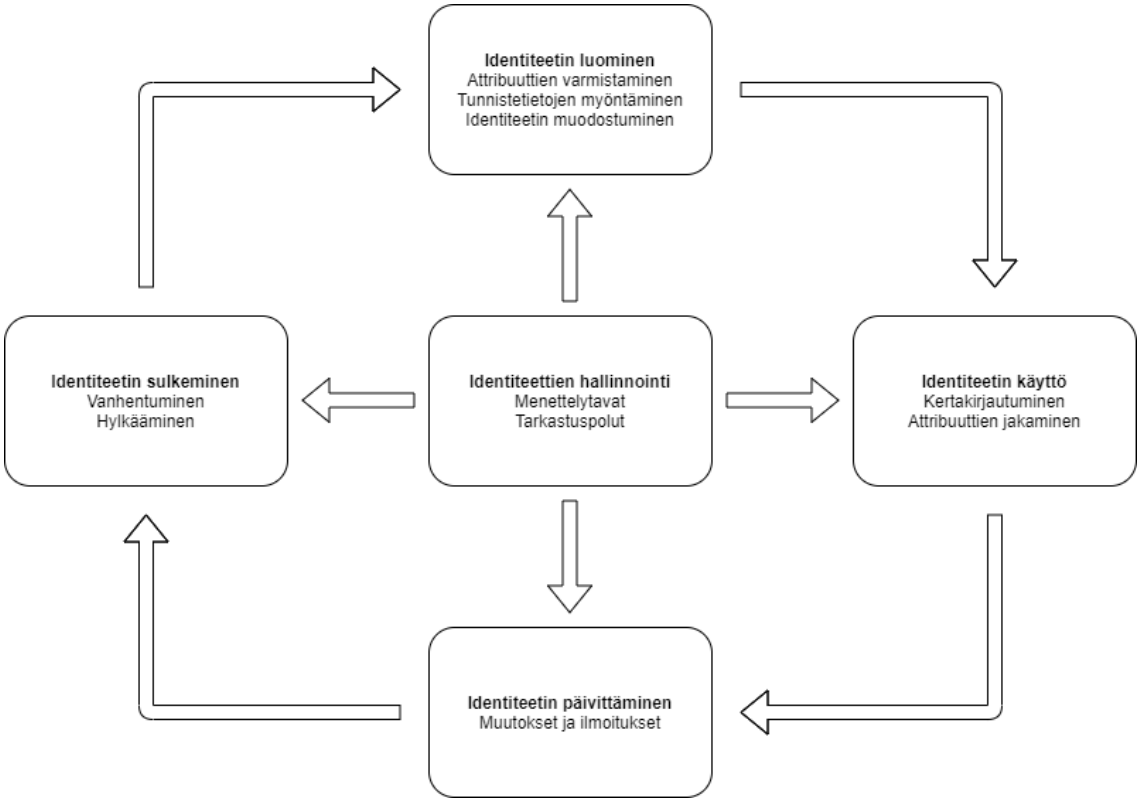
Harkinnanvarainen pääsynvalvonta (DAC) on pääsynhallinnan mekanismi, jossa resurssien omistajat hallitsevat käyttöoikeuksia. Harkinnanvarainen pääsynvalvonta on harkinnanvaraista, koska resurssien omistaja saa itse määritellä käyttöoikeuksia parhaaksi katsomallaan tavalla. Käyttäjän pääsyoikeus tarkistetaan ja vahvistetaan useimmiten todennuksen yhteydessä, kun käyttäjä kirjautuu laitteelle. Harkinnanvarainen pääsynvalvonta tarjoaa enemmän joustavuutta kuin pakollinen pääsynvalvonta, mutta toisaalta se voi johtaa resurssien heikompaan suojaukseen. (Indu, Rubesh Anand & Bhaskar 2018.)

4.2.5 Käyttöoikeus-/tehtäväpohjainen pääsynvalvonta

Käyttöoikeuteen tai tehtävään perustuva pääsynvalvonta (engl. entitlement / task based access control) on mekanismi, jossa jokaiselle tehtävälle, toiminnolle tai prosessille vaaditaan tarkoin määrätty käyttöoikeus. Tämän pääsynvalvontamallin avulla pystytään käsittelemään monimutkaisia käyttöehtoja, jotka määrittelevät tarkasti joko käyttövaltuuksien myöntämisen tai epäämisen. Se vaatii kuitenkin paljon työtä ja ylläpitoa, kun käyttöoikeuksia on suuria määriä. Käyttäjien on myös esitettävä erillisiä pyyntöjä ja saatava hyväksyntä jokaiselle käyttöoikeudelle. Käyttöoikeuteen tai tehtävään perustuvalla pääsynvalvonnalla on kuitenkin kyky toteuttaa muita hierarkkisia pääsynvalvontamalleja, kuten roolipohjaista tai attribuuttipohjaista pääsynvalvontaa. (Indu, Rubesh Anand & Bhaskar 2018.)

5 IDENTITEETIN ELINKAARI

Identiteettejä tulee ylläpitää niiden elinkaaren aikana monilla tavoin. Identiteetinhallinta ei tarkoita ainoastaan käyttäjälle näkyvien toiminnallisuuksien muuttamista, vaan se koskee kaikkia identiteetin vaiheita aina luomisesta sulkemiseen saakka. Identiteetin elinkaari koostuu tyypillisesti neljästä vaiheesta: luominen, käyttö, päivittäminen ja sulkeminen. Identiteettien elinkaareen liittyviä osia ovat myös provisiointi ja deprovisiointi. Identiteettien hallinnoinnin tulisi olla johdonmukaista kaikissa elinkaaren vaiheissa. Kuva 4 esittää identiteetin elinkaaren vaiheiden välisiä yhteyksiä ja niiden tapahtumajärjestystä.



Kuva 4. Identiteetin elinkaari (Bertino & Takahashi 2010, 30).

5.1 Luominen

Identiteetin luominen koostuu kolmesta alavaiheesta: attribuuttien varmistaminen, tunnistetietojen myöntäminen sekä identiteetin muodostuminen. Attribuuttien varmistamisella tarkoitetaan määritteiden oikeellisuuden tarkistamista esimerkiksi viranomaisen myöntämän asiakirjan avulla. Tietyissä tilanteissa onkin tarpeellista varmistaa

rekisteröitävän työntekijän henkilöllisyys, sillä joissakin tehtävissä on välttämätöntä varmistaa esimerkiksi ammattioikeuksien voimassaolo. Vähemmän säädellyissä palveluissa voidaan kuitenkin luottaa pelkästään käyttäjän syöttämien tietojen oikeellisuuteen. Hyvänä esimerkkinä tästä on internetin blogisivustot, joissa käyttäjien henkilöllisyyttä tai syötettyjen tietojen oikeellisuutta harvemmin tarkistetaan. (Bertino & Takahashi 2010, 30.)

Kun attribuutit on varmistettu, siirrytään tunnistetietojen myöntämiseen. Tunnistetiedoista riippuen ne voivat olla joko auktoriteetin tai kohteen itsensä luovuttamia. Tällaisia voivat olla esimerkiksi organisaation myöntämä digitaalinen varmenne tai vastaavasti käyttäjän itsensä valitsema salasana. Tunnistetiedot voivat esiintyä monessa muodossa, kuten digitaalisina varmenteina, salasanoina ja sormenjälkinä. Kukin näistä mahdollistaa erilaisen varmuuden tason. Attribuuttien varmistamisen ja tunnistetietojen myöntämisen lisäksi kohde tarvitsee oman yksilöivän tunnisteen, esimerkiksi henkilönumeron, jotta identiteetti voidaan muodostaa. (Bertino & Takahashi 2010, 31.)

5.2 Provisiointi

Provisioinnilla tarkoitetaan prosessia, jolla valmistellaan tietojärjestelmä palvelemaan käyttäjää. Sähköistä identiteettiä ajatellen provisioinnissa muodostetaan identiteettitietue, joka sisältää käyttäjän kannalta oikeanlaiset attribuutit. Nämä attribuutit voivat olla perustietojen (kuten nimi, osoite ja puhelinnumero) lisäksi järjestelmän käyttämisen kannalta tarkempia määritteitä, kuten käyttöoikeuksia tiettyjen toimintojen käyttämiseen. (Windley 2005.)

Provisiointia voidaan toteuttaa manuaalisesti järjestelmänvalvojan tekemillä toimilla tai käyttäjän suorittamana itsepalveluna esimerkiksi sähköisen lomakkeen kautta. Itsepalvelujen tarjoaminen onkin nykyaikana erittäin yleistä etenkin internetissä käytettävien palvelujen osalta. Provisiointia voidaan lisäksi automatisoida toimimaan esimerkiksi henkilöstöhallintojärjestelmästä saatujen tietojen perusteella siten, että käyttäjälle luodaan automaattisesti tunnukset vaikkapa yrityksen verkkoon. Yksi yritystietotekniikan trendeistä onkin, että käyttäjällä olisi tarvittavat työvälineet, tunnukset ja käyttöoikeudet käytettävissään jo ensimmäisen työpäivän alkaessa. (Windley 2005.)

Järjestelmän luonteesta riippuen identiteettitietue voidaan tarvittaessa välittää myös muihin tietojärjestelmiin käyttöoikeuksien luomista varten. Yksinkertaisimmillaan

identiteettitietueet voidaan vain johtaa tiedostojärjestelmään tai paikalliseen tietokantaan. Monipuolisemmat järjestelmät saattavat kuitenkin tarjota mahdollisuuden myös jaettuun identiteettihakemistoon, jolloin yhdessä paikassa luotua identiteettiä voidaan käyttää useammissa eri tietojärjestelmissä. Jotta identiteettitietueiden välittäminen olisi tarkoituksenmukaista, tietueiden välittämisen tulisi tapahtua jokaisen tehdyn muutoksen jälkeen. Tällöin identiteettitiedot pysyvät ajan tasalla kaikissa järjestelmissä. (Windley 2005.)

5.3 Käyttö

Sähköisiä identiteettejä voidaan hyödyntää palvelujen mahdollistamiseen monilla tavoin. Identiteettejä on kuitenkin aina käsiteltävä turvallisella ja yksityisyydensuojaa noudattavalla tavalla. Kolme yleisimmin käytettyä identiteettipalvelujen mahdollistamaa toimintoa ovat luotettu viestintä, kertakirjautuminen ja attribuuttien jakaminen.

Identiteettien luotettavuus on olennaista luotettavan viestinnän mahdollistamisessa. Luotetussa viestinnässä viestien lähettäjien tulisi pystyä tunnistamaan, erottamaan ja todentamaan vastapuolen identiteetti luotettavalla tavalla. Viesteissä on esimerkiksi mahdollista hyödyntää digitaalista allekirjoitusta, jossa viestin lähettäjän henkilöllisyys voidaan todentaa varmenteiden ja julkisten avainten avulla. Lisäksi viestit voidaan salata, jos halutaan varmistaa viestien luottamuksellisuus. Keskinäinen todennus on tarpeellista myös phishing- ja pharming-hyökkäysten estämisessä. (Bertino & Takahashi 2010, 32.)

Identiteettiä voidaan käyttää kertakirjautumiseen, jossa yhdellä identiteetin todennuksella voidaan päästä useampaan kuin yhteen palveluun. Todentamistulokset välitetään saatavilla oleviin palveluihin, jolloin kirjautumistietoja ei tarvitse syöttää manuaalisesti jokaiseen palveluun. Tämä vähentää käyttäjien tarvetta muistaa useita erilaisia käyttäjätunnus-salasana -pareja sekä nopeuttaa palveluihin pääsemistä. Käyttäjät ovat myös saattaneet pitää manuaalista kirjautumista hieman työläänä prosessina, joka laskennallisestikin kuluttaa työaikaa. Kertakirjautumisen ansiosta palveluiden käyttötiheydet saattavat jopa kasvaa, kun kirjautumiset eivät työllistä käyttäjiä niin paljoa. (Bertino & Takahashi 2010, 32–33.)

Attribuuttien jakaminen on tapahtuma, jossa luotettavat osapuolet ja identiteettipalvelut jakavat tiettyjä attribuutteja keskenään. Tästä esimerkkinä voisi olla uuden verkkopalvelun käyttöönotto, jossa identiteettipalvelu välittää tarvittavat yhteystiedot käyttäjästä

kyseiseen palveluun. Attribuuttien jakaminen vähentää siis tarvetta tietojen manuaaliselle syöttämiselle ja toisaalta myös ylläpitää samojen attribuuttien eheyttä verkon yli hajautuneissa palveluissa. Parhaassa tapauksessa tiedot päivittyisivät yhdestä järjestelmästä kaikkiin palveluihin, jolloin tietoja ei tarvitsisi manuaalisesti muuttaa jokaiseen palveluun. Lisäksi tämä minimoi vanhentuneista tiedoista aiheutuvia väärinkäsityksiä. (Bertino & Takahashi 2010, 33–34.)

5.4 Päivittäminen

Identiteettitietoja on monesti tarpeellista päivittää identiteetin elinkaaren aikana. Työntekijöiden yhteystiedot, työyksiköt, työtehtävät ja monet muut attribuutit usein muuttuvat työsuhteiden aikana. Välillä työntekijöille tulee tarve lisätä uusia käyttöoikeuksia ja toisaalta poistaa vanhoja tarpeettomia oikeuksia. Digitaalisten varmenteiden muodossa olevat tunnistetiedot voivat lisäksi vanhentua, jolloin niitä on tarve uusia. Identiteettitietoja olisikin tärkeää pitää ajan tasalla, jotta tieto pysyy eheänä ja sitä voidaan hyödyntää halutulla tavalla. Vaikka attribuuttien osalta saattaa joskus tapahtua suuriakin muutoksia, tulisi avaintunnisteiden kuitenkin aina pysyä samoina ja yksilöllisinä. Tämä varmistaa hyvän jäljitettävyyden, kun historiatiedot muutoksista säilyvät tallessa. (Bertino & Takahashi 2010, 34–35.)

5.5 Sulkeminen

Identiteettejä ja niihin liittyviä käyttäjätunnuksia tulisi sulkea johdonmukaisella tavalla. Se on erittäin tärkeää identiteettitietoihin perustuvan todennuksen ja valtuutuksen pätevyyden varmistamiseksi. Syitä sulkemiselle voivat olla esimerkiksi käyttäjätilin vanheneminen, tunnistetietojen varkaudet sekä työsuhteen päättyminen. Identiteetin sulkeminen mahdollistaa kuitenkin vielä sen, että se voidaan ottaa uudestaan käyttöön, kun tilanne selviää. Identiteetin sulkemisesta on toki hyvä tiedottaa ajoissa asianomaisille. (Bertino & Takahashi 2010, 35.)

5.6 Deprovisiointi

Identiteetin deprovisioinnilla tarkoitetaan identiteettien poistamista järjestelmästä, kun ne ovat elinkaarensa lopussa. Deprovisiointi on yhtä tärkeä vaihe identiteetin elinkaarta kuin

provisiointikin. On tärkeää poistaa identiteetti ja siihen liittyvät käyttöoikeudet työsuhteen päättyessä. Jos identiteettiä ei deprovisioida, se voi aiheuttaa sekaannuksia sekä mahdollistaa ulkopuolisten pääsyn kriittisiin tietoihin, mikä puolestaan voi johtaa varkauksiin ja petoksiin. Vanhat aktiiviseksi jääneet tilit ovatkin yksi suurimmista turvallisuusaukoista, joita yritykset kohtaavat. Työntekijä saattaa lopettamisensa jälkeen jatkaa yrityksen resurssien käyttöä, mutta sen lisäksi nämä ovat hakkereille suotuisia kanavia murtautua yrityksen järjestelmiin. Tällaisten tilien käyttöä harvemmin valvotaan, eikä murtautuminen välttämättä herättäisi huomiota epätavallisena toimintana. (Windley 2005.)

5.7 Hallinnointi

Edellä mainittuja identiteetin elinkaaren vaiheita ja niihin liittyviä tapahtumia tulisi ohjata kattavien käytänteiden avulla. Identiteettien hallinta on olennainen osa organisaation sisäistä valvontaa ja sen toteuttamista tulisi suunnitella ja tarkastella säännöllisin väliajoin. Tällä tavoin varmistettaisiin käytänteiden ajantasaisuus sekä vaatimustenmukaisuus. Identiteetteihin liittyviä käytänteitä ja tapahtumia tulisi myös kirjata vastuullisella tavalla, jotta voidaan varmistaa hallintoon liittyvien säädösten noudattaminen. (Bertino & Takahashi 2010, 36.)

Identiteettipolitiikka (engl. identity policies) sisältää pääosin identiteettien todennukseen ja valtuutukseen liittyviä käytäntöjä. Todennuskäytännöt määrittelevät tietyn vaatimustason identiteetin varmistamiseen. Valtuutuskäytännöt taas määrittelevät olosuhteet palveluiden ja tiedon saatavuudelle. Käytäntönä voi olla muun muassa roolipohjainen pääsynvalvonta, jossa käyttäjille annetaan ennalta määritetty joukko käyttöoikeuksia vaikkapa työnimikkeen perusteella. Resursseilla ja palveluilla voi lisäksi olla omia käytäntöjä, jolloin pääsy on sallittu esimerkiksi vain tiettyinä aikoina ja tietyistä verkoista. Identiteettipolitiikkaa käytetään hallinnollisten tarkoitusten lisäksi myös yksityisyyden suojaamiseen. Sen avulla voidaan asettaa yksityisyyteen liittyviä käytäntöjä muun muassa käyttäjien ja palvelutarjoajien välille. (Bertino & Takahashi 2010, 36.)

Käytäntöjen lisäksi olisi tärkeää merkitä kirjausketjuihin (engl. audit trails) kaikki identiteettien elinkaaren aikana tapahtuneet muutokset ja toiminnot. Kirjausketju sisältää yksityiskohtaista tietoa kustakin identiteettiin liittyvästä tapahtumasta luotettavalla ja todistettavalla tavalla, jotta kyseenalaisia tilanteita voidaan sen avulla selvittää ja ennaltaehkäistä. Tapahtumia voidaan siis myöhemmässä vaiheessa jäljittää ja tutkia niiden yksityiskohtia. Esimerkiksi henkilötietojen muutoksesta voitaisiin saada selville seuraavat

tiedot: kuka muutosta on pyytänyt, milloin se on tapahtunut ja mikä on ollut muutoksen tarkoitus. Kirjausketjut itsessään ovat tärkeää identiteettitietoa ja niiden tulisi olla suojattu turvallisella ja yksityisyyttä kunnioittavalla tavalla. (Bertino & Takahashi 2010, 37.)

6 IDENTITEETIN- JA PÄÄSYNHALLINNAN MERKITYS

Tässä luvussa käsitellään identiteetin- ja pääsynhallinnan merkitystä sekä siihen liittyviä hyötyjä ja haasteita. Nykyaikaisten IAM-järjestelmien avulla voidaan parantaa organisaatioiden tietoturvaa ja operatiivista tehokkuutta sekä varmistaa tietosuojaan liittyvän lainsäädännön noudattaminen.

6.1 Tietoturva

Identiteetin- ja pääsynhallinnalla on kriittinen rooli yritysten tietoturvan järjestämisessä. Nykyaikana arkaluonteisia tietoja tallennetaan yhä useammin sähköisesti ja näiden saatavuutta tulee hallita turvallisella tavalla. Erilaisten tietojen ja palveluiden saatavuutta onkin tarpeellista rajoittaa, jotta riskit tietojen leviämisestä saataisiin minimoitua. Digitaaliseen maailmaan siirtyminen ja työvoiman hallinnan kehittyminen ovat lisäksi luoneet tarpeen järjestelyille, joissa pääsy yrityksen järjestelmiin mahdollistetaan myös yrityksen ulkopuolisille työntekijöille, yhteistyökumppaneille ja toimittajille. Tällaisissa tilanteissa käyttöoikeuksien ja pääsyn rajoittaminen on vielä tärkeämpää. Nykyisin monissa yrityksissä hyödynnetään paikallisten järjestelmäratkaisujen (on-premise) sijasta myös erilaisia pilvi- ja hybridiratkaisuja, jotka mahdollistavat järjestelmien käytön jopa työntekijöiden omilta kotikoneilta. Tästäkin syystä käyttöoikeuksien hallinnan tulisi olla aiempaa tarkempaa ja johdonmukaisempaa, jotta käyttöoikeudet eivät jäisi aktiivisiksi työsuhteiden päätyttyä. Kriittisten tietojen päätyminen kilpailijoiden tai muiden ulkopuolisten käsiin voisi pahimmassa tilanteessa aiheuttaa suurta tuhoa yrityksen menestymiselle ja maineelle. (Rathod 2019.)

Nykyaikaisilla identiteetin- ja pääsynhallinnan ratkaisuilla voidaan yhdistää useiden eri tietojärjestelmien käyttäjienhallinta yhdelle keskitetylle alustalle. Parhaimmillaan sen avulla pystyttäisiin hallitsemaan kaikkia käyttäjälle kuuluvia pääsyoikeuksia yhdestä paikasta sujuvalla ja yhdenmukaisella tavalla. Tämä helpottaa merkittävästi järjestelmänvalvojien työtä sekä vähentää manuaalisesta hallinnasta aiheutuvia virheitä. Keskitetyn identiteetin- ja pääsynhallinnan avulla järjestelmänvalvojat pystyvät esimerkiksi yhdellä kertaa sulkemaan kaikki käyttäjälle kuuluvat pääsyoikeudet niissä järjestelmissä, jotka ovat integroituna kyseiseen ratkaisuun. Kun työntekijän työsuhde organisaatiossa päättyy, järjestelmänvalvojien on helppo sulkea identiteetti ja varmistua, etteivät käyttöoikeudet jää voimaan. Muussa tapauksessa järjestelmänvalvoja saattaisi joutua manuaalisesti

sulkemaan käyttöoikeuksia useista eri järjestelmistä, mikä helposti johtaa unohduksiin. Aktiivisiksi unohtuneet käyttäjätilit ovatkin yksi merkittävimmistä haasteista ja haavoittuvuuksista yritysten tietoturvan kannalta. (Rathod 2019.)

Vähimpien oikeuksien periaate on hyvä käytäntö resurssien ja järjestelmien suojaamisessa. Se on tietoturvakäytäntö, jossa käyttäjien käyttöoikeudet rajoitetaan vähimpiin mahdollisiin oikeuksiin, joita he tarvitsevat työtehtäviensä suorittamisessa. Organisaatioissa on varsin yleistä, että työntekijöiden roolit ja työtehtävät muuttuvat ajan myötä. Tällaisissa tilanteissa aiemmat käyttöoikeudet jäävät helposti voimaan, mikäli niitä ei työtehtävien muuttuessa huomata poistaa. Ylimääräisten oikeuksien kertyminen lisää tietoturvaan liittyviä riskejä, sillä liialliset oikeudet tekevät käyttäjästä helpomman kohteen hakkereille. Toisaalta se muodostaa myös sisäpiiriuhkan, koska henkilöllä on mahdollisuus tehdä tietovarkauksia. Kasautuneita oikeuksia saattaisi pahimmassa tapauksessa jäädä voimaan myös työsuhteiden päätyttyä, ellei käyttövaltuushallinta ole johdonmukaista. Hyvin suunnitellulla ja keskitetyllä identiteetin- ja pääsynhallinnan järjestelmällä vähimpien oikeuksien periaatteen toteuttaminen on kuitenkin merkittävästi helpompaa. Järjestelmän avulla käyttöoikeuksia voitaisiin helposti muuttaa esimerkiksi roolien perusteella, jolloin roolin vaihtaminen poistaisi käyttäjältä automaattisesti aiemmissa työtehtävissä tarvittuja oikeuksia. (Rathod 2019.)

6.2 Operatiivinen tehokkuus

Identiteetin- ja pääsynhallinta tehostaa organisaatioiden toimintaa monilla tavoin. Sen avulla voidaan parantaa työntekijöiden käyttökokemusta, helpottaa IT-osaston työtaakkaa sekä vähentää ylimääräisiä kustannuksia. Näiden avulla toiminnasta saadaan tehtyä entistä tehokkaampaa ja samalla luotua mahdollisuuksia myös yritystoiminnan kehittämiselle ja laajentamiselle. Identiteetin- ja pääsynhallinnan tärkeys korostuukin erityisesti suurissa ja keskisuurissa yrityksissä, joilla on käytössään paljon erilaisia järjestelmiä ja resursseja. Merkitystä voi korostaa myös käytettävien järjestelmien toteuttamistapa, sillä pilvipalveluiden osalta käyttäjienhallinnan tulisi olla entistä johdonmukaisempaa. (Niemi; Bozicevic 2020.)

Työntekijöiden käyttökokemukset voivat merkittävästi parantua identiteetin- ja pääsynhallintaan liittyvien kertakirjautumisratkaisujen avulla. Nykyisin työntekijät joutuvat työpäivän aikana kirjautumaan moniin erilaisiin järjestelmiin jopa useita kertoja päivässä. Kirjautumiseen kuluvan ajan lisäksi se rasittaa myös työntekijöiden muistia, ja voi johtaa

siihen, että salasanoja kirjoitetaan muistilapuilla tietokoneen viereen. Se ei missään nimessä ole tietoturvankaan kannalta hyvä asia. Kertakirjautumisen avulla käyttäjien ei kuitenkaan enää tarvitsisi kirjautua jokaiseen palveluun erikseen, vaan pääsy voidaan valtuuttaa yhdellä todentamisella useampiin järjestelmiin. Tämä säästää merkittävästi aikaa ja vaivaa sekä vapauttaa työntekijät useiden erilaisten salasanojen muistamiselta. Sen ansiosta työntekijät pystyvät tehokkaammin suorittamaan työtehtäviään ja yrityksen tuottavuuskin voi parantua. (Bozicevic 2020.)

Identiteetin- ja pääsynhallinta mahdollistaa johdonmukaisen ja skaalautuvan tavan käyttäjienhallinnan toteuttamiseen. Sen avulla käyttäjienhallinnasta saadaan tehtyä sekä tietoturvallisempaa että helpompaa. Identiteetin- ja pääsynhallinnan avulla on helppo edistää käyttöoikeuksiin liittyvien käytäntöjen noudattamista ja toteuttaa hallintaa isommillekin joukoille erilaisten roolien ja käyttöoikeusryhmien avulla. Identiteetinhallintaan kuuluvat itsepalveluportaalit voivat myös helpottaa IT-osaston kuormittuneisuutta, sillä jatkuvat salasanojen resetointipyynnöt ovat tavallisesti hidastaneet muiden työtehtävien suorittamista. Identiteetin- ja pääsynhallinnan avulla pystytään lisäksi automatisoimaan muitakin käyttäjienhallintaan liittyviä pyyntöjä ja tunnusten provisiointia. Sen myötä IT-osasto pystyy tehokkaammin keskittymään muihin tärkeisiin työtehtäviin. (Bozicevic 2020.)

Identiteetin- ja pääsynhallinnan avulla voidaan alentaa järjestelmien ylläpitoon ja käyttämättömiin lisensseihin kuluvia kustannuksia. Yhdistetyn identiteetinhallinnan ansiosta ei ole myöskään tarvetta luoda uusia paikallisia identiteettejä, vaan yhtä ja samaa identiteettiä voidaan hyödyntää useammissa eri järjestelmissä. Tällöin ylläpito ei enää vaadi moninkertaista työtä. Pääsynhallintaan liittyvien tilastointiominaisuuksien avulla pystytään lisäksi selvittämään maksullisten lisenssien käyttöä ja sen myötä niiden tarpeellisuutta. Mikäli maksulliselle tuotteelle ei ole enää käyttöä, voidaan sen sulkemisella saada aikaan kustannussäästöjä. (Bozicevic 2020.)

6.3 Lainsäädäntö

Vuonna 2018 voimaan tullut yleinen tietosuoja-asetus (GDPR) on muuttanut EU:n alueella tapaa, jolla organisaatiot käsittelevät työntekijöidensä ja asiakkaidensa henkilökohtaisia tietoja. On olennaista suojata kaikkia sellaisia tietoja, joista henkilöitä voitaisiin tunnistaa. Henkilötiedoiksi lasketaankin kaikki sellaiset tiedot, joista henkilö voidaan suoraan tai välillisesti tunnistaa. Tällaisia ovat kaikki henkilöiden yhteys- ja osoitetiedoista aina potilastietoihin asti. Joidenkin henkilötietojen käsittely voi lisäksi olla lähtökohtaisesti

kiellettyä. Sellaisia ovat etnisyyteen, politiikkaan, uskonnollisuuteen, geneettisyyteen ja seksuaalisuuteen liittyvien tietojen käsitteleminen. Näiden säädösten keskeisenä tavoitteena on estää erityisesti tietosuojarikkomuksia ja henkilötietojen väärinkäytöksiä. GDPR:n myötä säädösten noudattamattomuudesta rankaistaan myös aiempaa suuremmilla sakkorangaistuksilla. (OpenText 2018; Tietosuojavaltuutetun toimisto.)

Identiteetin- ja pääsynhallinnan järjestelmät ja strategiat ovat tulleet välttämättömiksi GDPR:n vaatimusten noudattamisen kannalta. Ennaltaehkäisemisen lisäksi on tärkeää panostaa ongelmien havaitsemiseen ja kunnostamiseen. Kyberturvallisuusuhkien laajuus ja moninaisuus kasvavat jatkuvasti ja samalla riskit tietosuojarikkomuksien suhteen lisääntyvät. Tämä onkin kasvattanut tarvetta suojata henkilötietoja yhä paremmin. (OpenText 2018.)

GDPR asettaa tiukat vaatimukset henkilötietojen käsittelylle. Identiteetin- ja pääsynhallinnan avulla henkilötietoja suojataan luvattomalta ja laittomalta käsittelyltä luotettavan todennuksen ja käyttöoikeuksien hallinnoimisen avulla. Järjestelmät tarjoavat mahdollisuuden monivaiheiseen todennukseen, jolloin todennus on entistä varmempaa. Käyttöoikeuksien hallinnalla puolestaan varmistetaan se, että käyttäjät voivat käyttää ainoastaan heille tarkoitettuja resursseja. Identiteetin- ja pääsynhallinnan avulla pystytään lisäksi jäljittämään mahdollisia rikkomuksia sekä kartoittamaan rikkomuksen aiheuttamia seurauksia. Se tarjoaa korvaamatonta tietoa siitä, miten työntekijät ovat päässeet sovelluksiin, kuten tiedot siitä: kuka kirjautui sisään, milloin ja mitä tietoja he käyttivät. (OpenText 2018.)

GDPR:n mukaisesti käyttäjällä eli rekisteröidyllä on oikeus saada tietoa henkilötietojensa käytöstä. Identiteetin- ja pääsynhallintajärjestelmän avulla pystytäänkin selvittämään, kenellä käyttäjällä on tunnukset missäkin järjestelmässä. Yksi GDPR:n perustavanlaatuisista näkökohdista on lisäksi minimoida käsiteltävien tietojen määrää. Identiteetin- ja pääsynhallinnan avulla on helppoa määritellä se, miten pitkäksi ajaksi käyttöoikeuksia myönnetään ja miten pitkään poistuneen käyttäjän tietoja säilytetään. Tämä mahdollistaa tilitietojen oikea-aikaisen ja käytäntöjen mukaisen poistamisen. Identiteetinhallinnan avulla on myös mahdollista päästä eroon niin sanotuista haamutileistä, jotka aiheuttavat merkittäviä haavoittuvuuksia organisaatioiden tietoturvaan. (OpenText 2018.)

GDPR on lisäksi muuttanut yhteistyötä pilvipalveluiden tarjoajien kanssa. Pilvipalveluiden tarjoajilla on nykyisin isompi vastuu siitä, että henkilötietoja käsitellään GDPR:n mukaisilla tavoilla. Jokaisen pilvipalvelun tuleekin saada käyttäjältä suostumus tietojensa käsittelyyn ja usein tämä hoidetaan palvelussa olevan käyttäjäprofiilin kautta. Tämä tuo

merkittäviä vaikutuksia myös identiteetin- ja pääsynhallintaan, sillä järjestelmien on tarjottava keskitetty rekisteri annetuista suostumuksista. Niiden on lisäksi mahdollistettava suostumusten peruuttaminen joko käyttäjän itse tekemillä toimilla tai pyynnöstä. Järjestelmien välisten integrointien ehtona on, että käyttäjien henkilökohtaiset tiedot jaetaan turvallisesti ja yhteensopivasti valitun pilvialustan kanssa. GDPR ehdottaakin, että uusien sopimussuhteiden olisi tuettava pilvipalveluita, mutta se vaatii identiteetin- ja pääsynhallinnan varmistamaan, että näitä järjestelyjä pannaan asianmukaisesti täytäntöön. (OpenText 2018.)

7 VAIHTOEHTOJEN KARTOITTAMINEN

Opinnäytetyön käytännön osuudessa keskityttiin löytämään toimeksiantajan tarpeita vastaava identiteetinhallintajärjestelmä sekä perehdyttiin sen käyttöönottoon. Työn toteuttamiseen sisältyi tarpeiden määrittelyä, vaihtoehtojen selvittämistä ja vertailemista sekä järjestelmän käyttöönottoon liittyviä toimenpiteitä ja testaamista. Tavoitteena oli löytää ratkaisu, jolla kehitettäisiin käyttäjätunnusten hallintaa sekä parannettaisiin organisaation tietoturvaa.

Opinnäytetyön toimeksiantajana on toiminut pieni varsinaissuomalainen kaupunki, joka työllistää yhteensä noin 600 työntekijää sen eri toimialoilla. Työ toteutettiin yhteistyössä kaupungin tietohallinnon kanssa, jonka tarpeita kyseinen järjestelmä tulisi ensisijaisesti palvelemaan. Tietohallinnon yhtenä tehtävänä on hallinnoida erilaisten tietoteknisten resurssien saatavuutta sekä toteuttaa käyttäjienhallintaa monissa erilaisissa tietojärjestelmissä. Identiteetinhallintajärjestelmällä halutaan selkeyttää tätä käyttövaltuuksien hallintaa sekä ratkaista nykyisiin menettelyihin liittyviä haasteita.

Nykyisten käytäntöjen mukaan käyttäjätunnuksia luodaan, muokataan ja suljetaan esimiesten lähettämien pyyntöjen perusteella. Uusien työntekijöiden osalta esimiehet toimittavat tietohallintoon työntekijän täyttämän käyttöoikeussitoumuksen, joka sisältää tarvittavat tiedot tunnusten tekemistä varten. Niiden perusteella tietohallinto luo uudelle työntekijälle verkkotunnukset ja sähköpostilaatikon sekä lisää hänelle tarvittavat käyttöoikeudet ja jakelulistat. Tietohallinto tekee esimiehiltä saatujen pyyntöjen perusteella tunnuksia myös muihin tietojärjestelmiin, kuten kaupungilla käytössä olevaan asiakas- ja potilastietojärjestelmään sekä sähköiseen asianhallintajärjestelmään. Käyttäjätunnuksiin liittyen tehdään myös monenlaisia muutoksia, kun työntekijän työnkuva tai esimerkiksi työyksikkö muuttuu. Esimiesten tehtävänä on lisäksi ilmoittaa työsuhteiden päättymisestä, jotta identiteetit saadaan suljettua asianmukaisesti.

7.1 Organisaation tarpeet

Kaupungilla on käytössä jopa yli sata erilaista tietojärjestelmää. Näiden kaikkien liittäminen yhden keskitetyn pääsynhallintaratkaisun alle saattaisi olla melko kestämätön ja epäkustannustehokas ratkaisu. Lukumäärän ohella isoksi haasteeksi nousisi myös järjestelmien vaihtuvuus sekä muutokset palveluiden tuottamistyypissä. Kertakirjautumiseen liittyvät toiminnallisuudet eivät myöskään olisi välttämättömiä, sillä suurimmalle

osalle työntekijöistä siitä ei olisi merkittävää etua. Projektissa keskityttiinkin ensisijaisesti toimivan identiteetinhallinnan järjestämiseen.

Nykyisten käytäntöjen mukaan tietohallinto saa tiedon uusista työntekijöistä ja työsuhteiden päättymisestä käytännössä vain esimiesten kautta. Unohduksia kuitenkin tapahtuu usein ja ne johtavat erilaisiin virheisiin. Käyttäjätunnusten puute huomataan usein vasta samana päivänä, kun työntekijä aloittaa työt. Identiteettejä jää myös helposti aktiivisiksi, mikäli työsuhteiden päättymisistä ei muisteta ilmoittaa tietohallinnolle. Tämä aiheuttaa merkittäviä haavoittuvuuksia tietoturvaan, sillä resurssit voivat olla pitkiäkin aikoja käytettävissä työntekijöiden lähdettyä. Lisäksi työnantajan luovuttamat työvälineet, kuten työpuhelimet ja jopa kulkuavaimet, saattavat jäädä lopettaneiden työntekijöiden haltuun ja käyttöön. Tietoturvan kannalta olisikin olennaista saada luotettavasti tietoa siitä, ketkä organisaatiossa työskentelevät ja keiden työsuhteet ovat päättymässä.

Tiedonkulkuun liittyviä haasteita voitaisiin ratkaista tuomalla työsuhteisiin liittyviä tietoja suoraan HR-järjestelmästä identiteetinhallintajärjestelmään. Integraation avulla saataisiin ajantasaista tietoa työsuhteiden voimassaoloista sekä monenlaista muuta identiteettien kannalta olennaista tietoa, kuten työntekijän työyksikkö ja -nimike. Datan avulla voitaisiin myös automatisoida identiteettien hallintaa, jolloin esimerkiksi määräaikaisten työsuhteiden jatkaminen ei aiheuttaisi käyttäjätunnusten osalta manuaalista työtä. Sen avulla voitaisiin lisäksi automatisoida identiteettien deprovisiointia, jolloin niin kutsutut haamutilit saataisiin suljettua. Tämä toisi merkittäviä parannuksia tietoturvaan, kun epämääräiset identiteetit saataisiin asianmukaisesti poistettua. Tiedonkulkuun liittyvien haasteiden ratkaisemiseksi hankittavan identiteetinhallintajärjestelmän olikin tärkeää tukea integraatiota nykyisin käytössä olevan HR-järjestelmän kanssa.

Hyvin toimivan identiteetinhallintajärjestelmän avulla olisi mahdollista kehittää tietohallinnon palveluita entistä paremmaksi. Ajantasaisen tiedon avulla identiteetinhallintaa saataisiin toteutettua aiempaa selkeämmin ja luotettavammin. Automatisoitujen toimintojen avulla voitaisiin lisäksi välttyä tahattomilta virheiltä ja säästää aikaa muille tärkeille työtehtäville. Käyttäjätunnuksiin liittyvien pyyntöjen käsittely olisi myös entistä helpompaa ja nopeampaa, kun tarvittavat lisätiedot olisivat valmiiksi saatavilla. Identiteetinhallintajärjestelmään liittyvät raportointiominaisuudet mahdollistaisivat lisäksi identiteetteihin liittyvän muutoshistorian tarkastelemisen, mikä voisi helpottaa mahdollisten väärinkäytösten selvittämistä.

7.2 Tarkoitukseen soveltuvia vaihtoehtoja

Soveltuvan järjestelmän hankintaan liittyen on tarkasteltu neljää erilaista vaihtoehtoa: *Efecte IGA*, *Imprivata IdG*, *Enter Ruutuvihko* sekä *One Identity Manager*. Järjestelmiä ja niiden ominaisuuksia on esitelty seuraavissa alaluvuissa.

7.2.1 Efecte Identity Governance and Administration

Efecte IGA on pilvipohjainen ratkaisu, jolla voidaan automatisoida identiteettien ja käyttöoikeuksien hallintaa. Järjestelmään kuuluvan itsepalveluportaalin avulla esimiehet voivat lähettää identiteettien provisiointiin liittyviä pyyntöjä sekä myöhemmässä vaiheessa hallinnoida työntekijöidensä käyttäjätunnusten voimassaoloja. Itsepalveluportaalia käyttämällä myös työntekijät voivat tarvittaessa täyttää käyttöoikeuspyyntöjä, joiden käsittelemistä voidaan automatisoida erilaisten hyväksyntäketjujen avulla. Hyväksyntäketjun ansiosta käyttöoikeuden myöntämiseen liittyvä prosessi voidaan suorittaa täysin automatisoidusti, jolloin järjestelmä voi kerätä käyttöoikeuden myöntämiseen vaadittavat hyväksynnät ketjuun merkityiltä henkilöiltä sekä lisätä vastausten perusteella oikeudet. Hyväksyntäketjut voivat tarvittaessa sisältää useampia vaiheita ja tasoja, jolloin myöntäminen voi vaatia useamman eri johtohenkilön hyväksynnän. Esimiehet pystyisivät lisäksi tekemään käyttöoikeuspyyntöjä useille työntekijöille yhdellä kertaa sekä asettamaan tarvittaessa käyttöoikeuksiin liittyviä voimassaoloaikoja. (Efecte 2020.)

Efecte IGA on mahdollista integroida muiden järjestelmien kanssa, jolloin esimerkiksi HR-järjestelmästä saatava tieto voidaan yhdistää identiteetinhallintajärjestelmään. Lisäksi siihen voidaan yhdistää muun muassa attribuuttipohjainen pääsynvalvonta saatavilla olevan lisäosan avulla. Järjestelmä sisältää lisäksi ominaisuuksia, joilla helpotetaan käyttöoikeuksiin liittyvää raportointia ja tarkastelua. Näiden avulla voidaan muun muassa seurata pyyntöjen käsittelyn etenemistä sekä tunnistaa epätavalliselta vaikuttavia käyttäjätilejä. Tietoja voidaan tarkastella luettelojen lisäksi erilaisten kaavioiden, kuvaajien ja visuaalisten analysointityökalujen muodossa. (Efecte 2020.)

7.2.2 Imprivata Identity Governance

Imprivata IdG on alun perin terveydenhuollon tarpeisiin kehitetty identiteetinhallintajärjestelmä, joka mahdollistaa identiteettien automatisoidun provisioinnin ja deprovisioinnin. Provisiointia on mahdollista toteuttaa muun muassa HR-järjestelmästä tuotavan datan avulla, jolloin identiteetti voi olla käytettävissä heti ensimmäisestä työpäivästä alkaen. Käyttöoikeuksien sulkeminen olisi myös helppoa työsuhteiden päätyttyä. Identiteetille kuuluvia käyttöoikeuksia voitaisiin lisäksi määrittää automaattisesti roolipohjaisen pääsynvalvonnan avulla, jolloin myönnettävät käyttöoikeudet ovat helposti hallittavissa. Näiden avulla voidaan vähentää identiteettien luomiseen kuluvaa aikaa sekä kustannuksia. IT-tuen työtä helpottaa lisäksi itsepalveluportaali, jonka avulla työntekijät voivat itse resetoida ja vaihtaa salasanojaan. (Imprivata.)

Järjestelmä sisältää hyödyllisiä tarkastelu-, raportointi- ja analysointityökaluja, jotka helpottavat uhkien arviointia ja korjaamista. Sisäänrakennettujen raportointiominaisuuksien avulla voidaan tarkastella muun muassa käyttäjä-, käyttöoikeus- ja käyttäytymistietoja, jolloin tietoturvaa uhkaaviin tilanteisiin on nopeampaa puuttua. Järjestelmän avulla voidaan siten varmistaa vaatimustenmukaisuus sekä valvoa käytäntöjen noudattamista. (Imprivata.)

7.2.3 Enter Ruutuvihko

Enter SystemSolutions Oy:n kehittämä *Ruutuvihko* on alun perin koulupuolen käyttöön kehitetty ratkaisu, jonka avulla voidaan automatisoidusti luoda, päivittää ja sulkea oppilaiden tarvitsemia käyttäjätunnuksia oppilastietojärjestelmästä tuotavan datan avulla. Kyseinen tuote on jatkokehitetty soveltumaan myös julkishallinnon ja yritysten HR-osaston tarpeisiin, jolloin identiteetinhallinta voi perustua oppilastietojärjestelmän sijasta esimerkiksi HR-järjestelmästä tuotavaan dataan. Datan perusteella käyttäjätunnukset voidaan luoda niin paikallisiin järjestelmiin kuin pilvipalveluihinkin esimerkiksi kustannuspaikkoihin perustuvien ryhmien perusteella. Järjestelmän avulla voidaan hallita käyttäjätietoja koko elinkaaren ajan, ja tiedot pysyisivät ajan tasalla myös järjestelmien välillä. (Enter SystemSolutions.)

Perinteisiin identiteetinhallintajärjestelmiin verraten *Ruutuvihko* on kevyempi ja kustannustehokkaampi vaihtoehto, ja sitä voidaan räätälöidä tarpeiden mukaan. *Ruutuvihko* vähentää käyttäjätietojen hallintaan kuluvaa työaikaa, jolloin aikaa jää enemmän muiden

tärkeiden työtehtävien suorittamiseen. Ratkaisu sisältää myös hyödyllisiä raportointiominaisuuksia, joiden avulla voidaan tarkastella käyttäjätietoihin ja -tunnuksiin liittyviä muutoksia. Näiden avulla voidaan lisäksi tunnistaa virhetilanteita, jolloin mahdollisiin ongelmatilanteisiin voidaan nopeasti reagoida. (Enter SystemSolutions.)

7.2.4 One Identity Manager

One Identity Manager on identiteetin- ja pääsynhallinnan ratkaisu, jolla voidaan hallita identiteettejä ja niihin liittyviä käyttöoikeuksia. Järjestelmän ansiosta käyttäjille voidaan tarjota tarkasti ja luotettavasti ne käyttöoikeudet, joita he tarvitsevat työtehtäviensä suorittamiseen. Tarvittaessa käyttäjät voivat pyytää lisää käyttöoikeuksia itsepalveluportaalin kautta, ja näiden pyyntöjen käsittelyä on mahdollista automatisoida ennalta määriteltävien hyväksyntämenettelyjen avulla. Järjestelmän avulla pystytään automatisoimaan myös käyttöoikeuksiin liittyvät valmistelut, jolloin vältytään monilta manuaalisen käsittelyn aiheuttamilta virheiltä. Tämä nopeuttaa käyttöoikeuspyyntöjen käsittelyä sekä vähentää niiden käsittelyyn kuluvaa työaikaa. (One Identity.)

HR-järjestelmästä saatavat työnsuhdetiedot on myös mahdollista tuoda *Identity Manager* -ratkaisuun. Tämä mahdollistaa identiteettien provisioinnin sekä parantaa samalla käyttövaltuushallinnan turvallisuutta. Lisäksi järjestelmä mahdollistaa identiteettien kaksivaiheisen todennuksen, jota voidaan hyödyntää monissa yrityksen ympäristöön kuuluvissa sovelluksissa. Sillä voidaan vähentää väärinkäytöksien riskiä sekä nostaa tietoturvan tasoa. Järjestelmä sisältää myös raportointityökaluja, joiden avulla saadaan yksityiskohtaisia tietoja siitä, kenellä on ollut pääsy mihinkin resurssiin, milloin ja mistä syystä. (One Identity.)

7.3 Valintapäätös

Vertailun perusteella soveltuvimmaksi vaihtoehdoksi valikoitui *Enter SystemSolutions Oy*:n julkishallinnon tarpeisiin suunnattu *Ruutuvihko*. Valintaan vaikuttivat kustannusten kohtuullisuus, riittävät ominaisuudet sekä soveltuvuus nykyiseen ympäristöön. Järjestelmän hankinnalla saataisiin kehitettyä kaupungin identiteetinhallintaa aiempaa tietoturvallisempaan ja sujuvampaan suuntaan. *Ruutuvihkon* ominaisuudet helpottaisivat käyttäjätunnusten hallintaa monella tapaa ja sen ansiosta aikaa jäisi myös muihin tärkeisiin työtehtäviin. Järjestelmä mukautuu nykyiseen ympäristöön ilman merkittäviä muutoksia ja

sen toimintoja voidaan myöhemmässä vaiheessa laajentaa. *Ruutuvihkon* valintaa helpottivat myös aiemmat hyvät kokemukset koulupuolen *Ruutuvihkosta* sekä hyvin toimivat tukipalvelut.

8 JÄRJESTELMÄN KÄYTTÖÖNOTTO

Opinnäytetyön aikana päästiin tutustumaan hankittavan järjestelmän käyttöönottoon liittyviin valmisteluihin sekä varmistamaan sen toimivuutta testaamisella. Käyttöönotettavana järjestelmänä on *Enter SystemSolutions Oy*:n *Ruutuvihko*, joka toteuttaisi työntekijöihin liittyvää identiteetinhallintaa HR-järjestelmästä tuotavan datan perusteella. Sieltä saatujen tietojen perusteella pystytään automatisoimaan työntekijöiden verkkotunnusten luomista, päivittämistä ja sulkemista. Järjestelmän avulla pystytään lisäksi synkronoimaan käyttäjien nimi- ja voimassaolotiedot valittuihin pilvipalveluihin. Nämä vähentävät merkittävästi manuaalisen työn määrää sekä edistävät tietoturvan toteuttamista.

Ruutuvihko mahdollistaa verkkotunnusten luomisen myös lomakkeen kautta. Tämä helpottaa tilanteita, joissa työntekijän tietoja ei ole vielä ehditty lisäämään HR-järjestelmään. Tunnuksia pystytään tarvittaessa luomaan myös organisaation ulkopuolisille työntekijöille ja yhteistyökumppaneille. HR-datan ulkopuolella olevien henkilöiden tunnusten voimassaoloja ja tietojen muutoksia tulisi kuitenkin yhä toteuttaa manuaalisilla toimenpiteillä.

Järjestelmä otettaisiin virallisesti käyttöön myöhemmässä vaiheessa. Testattavalla versiolla ei vielä tehdä muutoksia olemassa oleviin tunnuksiin, vaan sen avulla on tarkoitus kokeilla järjestelmän käyttäytymistä yleisesti sekä etsiä ongelmia ja löytää mahdollisia kehityskohteita. Järjestelmä muokattaisiin soveltumaan nykyiseen ympäristöön ja sen toimintoja räätälöitäisiin tarpeita vastaaviksi.

8.1 Tavoite

Ruutuvihkon toimivuutta ja soveltuvuutta olisi tarkoitus tutkia testaamisen kautta. Järjestelmän tulisi toimia loogisella ja järkevällä tavalla kaikissa yleisimmissä tilanteissa, joita identiteetinhallinnassa kohdataan. Sen tulisi kyetä toteuttamaan määriteltyjä tehtäviä itsenäisesti ja ilmoittamaan mahdollisista virhetilanteista ymmärrettävällä tavalla. Testaamisen tavoitteena olisi lisäksi tunnistaa mahdollisia kehityskohteita ja muutosideoita. Lopulta järjestelmän tulisi toimia siten, että se voitaisiin ottaa laajemmin käyttöön.

Testaamisella olisi tarkoitus kokeilla Ruutuvihkoon kuuluvien toiminnallisuuksien toimivuutta erilaisten testimenetelmien avulla. Testattavia toimintoja olisivat muun muassa tunnusten provisiointi ja sulkeminen, käyttäjien vienti pilvipalvelujen käyttäjienhallintaan,

tietojen päivittäminen järjestelmien välillä sekä virhetilanteita koskeva raportointi. Tulevaisuudessa identiteetit luotaisiin käytännössä säännöllisesti toimitettavan HR-datan perusteella ja tarvittaessa erikseen täytettävän lomakkeen kautta. Testausvaiheessa järjestelmää voidaan kuitenkin testata myös HR-dataa edustavaa tiedostoa muokkaamalla. Käyttöönoton myöhemmässä vaiheessa testattaisiin vielä järjestelmään lisättäviä uusia toimintoja, kuten käyttäjätunnusten toimittamista esimiehille sähköpostilla.

Järjestelmän tulisi kyetä käsittelemään muun muassa työntekijöiden nimissä esiintyviä harvinaisempia kirjaimia ja merkkejä, henkilöiden samannimisyyttä sekä mahdollisia nimenmuutoksia. Testaamisella varmistettaisiin myös, että tunnukset avataan ja suljetaan oikea-aikaisesti, tiedot ja voimassaolot päivittyvät järjestelmien välillä oikein, ja että käyttöoikeudet poistuvat työsuhteen päätyttyä. Testattavia tilanteita voisivat lisäksi olla päällekkäiset työsuhteet sekä järjestelmän reagointi erilaisiin manuaalisiin muutoksiin.

8.2 Valmistelut

HR-järjestelmästä tuotava data on tärkeässä roolissa kyseisessä kokonaisuudessa. HR-datassa esiintyvät työsuhdetiedot tuotaisiin järjestelmään päivittäin toimitettavana csv-tiedostona. Ruutuvihko poimisi tästä tiedostosta muun muassa nimitiedot, kustannuspaikan, työnimikkeen sekä työsuhteen voimassaolopäivämäärät. Niiden perusteella järjestelmä voisi automaattisesti luoda uusille työntekijöille verkkotunnukset, päivittää nykyisten käyttäjäprofiilien tietoja sekä sulkea poistuvien työntekijöiden käyttäjätunnukset. HR-datan automatisoitu toimittaminen viivästyi lopulta käyttöönoton myöhempään vaiheeseen. Järjestelmää päästiin kuitenkin testaamaan HR-datan muotoa vastaavalla esimerkkitiedostolla, johon voitiin manuaalisesti lisätä työsuhdetietoja kuvaavia rivejä.

Ruutuvihkon asennus toimitettiin uudelle virtualisoidusti toteutetulle palvelinkoneelle. Järjestelmän toimittamista varten oli tehty tarvittavat valmistelut sekä yhteysavaukset. Tässä vaiheessa palvelimelle toimitettu versio oli toiminnallisuuksiltaan hieman lopullista kevyempi, mutta sen avulla päästiin testaamaan järjestelmän keskeisimpiä toimintoja. Järjestelmään liittyviä määrityksiä oli myös mahdollista muokata ini-tiedostoilla ja kokeilla tapahtuvia toimenpiteitä ajamalla järjestelmään kuuluvia ohjelmatiedostoja. Käyttäjien lisääminen ja muokkaaminen tapahtui tässä vaiheessa vain HR-dataa esittävää csv-tiedostoa muokkaamalla. Ensimmäisten testausten jälkeen ja käyttöönoton edetessä järjestelmän toimintoja kehitettäisiin ja kokonaisuuteen lisättäisiin mahdollisesti uusia toimintoja.

8.3 Testausmenetelmät

Järjestelmää testattiin kuvitteellisilla työsuhdetiedoilla ja keksityillä työntekijöiden nimillä. Testaaminen tapahtui pääasiassa HR-dataa esittävää csv-tiedostoa muokkaamalla. Testauksen aikana dataan lisättiin yli 60 työsuhdetta kuvaavaa riviä, joilla muodostettiin yhteensä 35 verkkotunnusta. Riveillä simuloitiin erilaisia työsuhteissa esiintyviä tilanteita sekä testattiin eripituisia ja erilaisia kirjaimia sisältäviä työntekijöiden nimiä. Näillä oli tarkoitus varmistaa, että järjestelmä käyttäytyisi oikealla tavalla kaikissa tulevaisuudessa esiintyvissä tilanteissa.

Järjestelmän tehtävänä olisi suodattaa HR-datassa esiintyviä päällekkäisyyksiä muun muassa nimitietojen, voimassaolopäivämäärien ja työnimikkeiden suhteen. Suodatuksen toimivuutta testattiin erilaisilla ja jopa todellisuudessa mahdottomilla tilanteilla. Dataan lisättiin päättyneiden työsuhteiden tietoja, päällekkäisiä työsuhdetietoja sekä erilaisia nimen- ja työnimikkeenmuutoksia. Järjestelmän tehtävänä oli valita näistä voimassa olevat ja tuoreimmat tiedot.

Tapahtuvia toimenpiteitä voitiin kokeilla niin simuloidusti kuin todellisestikin. Simulaatiotilan avulla pystyttiin varmistamaan, etteivät HR-dataan tehdyt muutokset vaikuttaneet virheellisesti olemassa oleviin tunnuksiin. Testauksen aikana hyödynnettiin molempia tiloja, jotta varmistettiin simulaatiotilassa esitettyjen toimenpiteiden toteutettavuus. Todellisilla muutoksilla saatiin testattua myös tunnusten toimivuutta käytännössä sekä varmistettua käyttöoikeuksien poistuminen työsuhteiden päätyttyä. Simulaatiotilasta olisi merkittäviä hyötyjä myös tulevaisuudessa, kun testattaisiin todellisella datalla suoritettavia muutoksia.

Järjestelmään kuuluvia toimintoja pystyttiin muuttamaan ini-tiedostoja muokkaamalla. Niiden kautta toimintoja voitiin ottaa käyttöön tai tarvittaessa poistaa käytöstä. Ini-tiedostojen avulla voitiin esimerkiksi asettaa edellä mainittu simulaatiotila päälle tai valita, mistä HR-datatiedoston sarakkeista jokin arvo luetaan.

Järjestelmällä suoritettavia toimenpiteitä testattiin paikallisen ympäristön lisäksi pilviympäristöön synkronoiduilla käyttäjillä. Käyttäjiä vietiin pilviympäristöön, testattiin nimenmuutosten päivittymistä sekä tarkistettiin käyttöoikeuksien sulkeutuminen työsuhteen päätyttyä. Synkronoinnin tulisi toimia luotettavasti, sillä Ruutuvihko tulee automatisoimaan myös pilviympäristöjä koskevaa käyttäjienhallintaa.

8.4 Testatut tilanteet

Testausvaiheessa käytiin lävitse kymmeniä erilaisia testitapauksia ja -tilanteita. Ennen testien suorittamista kuvitelluille testihenkilöille määriteltiin erilaiset nimet sekä olettamuksia siitä, miten järjestelmän tulisi kussakin tilanteessa toimia. Testihenkilöiden tietoja lisättiin csv-tiedostoon monessa erässä ja niihin liittyviä toimenpiteitä toteutettiin niin simulaatiotilassa kuin todellisesti. Järjestelmän suorittamat muutokset kirjattiin ylös jokaisen tilanteen osalta ja annettiin palaute hyväksynnästä. Järjestelmän tuli suoriutua tilanteista odotetulla tai muutoin loogisella ja järkevällä tavalla. Tarvittaessa ehdotettiin mahdollista korjausta.

Testitilanteiden tarkastelu toteutettiin lisäämällä työsuhteita kuvaavia rivejä HR-dataa edustavaan csv-tiedostoon. Kuviteltuina henkilöinä oli sekä vakituisia että määräaikaisia työntekijöitä, joiden työsuhteet alkoivat ja päättyivät eri ajankohtina. Rivien perusteella järjestelmän tuli luoda kullekin henkilölle verkkotunnus *Microsoft AD* -hakemistopalveluun. Verkkotunnusten luomista ja aktivointia testattiin henkilöillä, joiden työsuhde olisi alkanut muun muassa vuoden päästä, kahden viikon päästä tai yksittäisten päivien päästä. Niiden osalta katsottiin, loiko järjestelmä tunnukset aktiivisessa vai passiivisessa tilassa. Tunnusten luomista testattiin myös työsuhteen alkamispäivänä sekä jälkikäteen seuraavina päivinä tai kuukauden ja jopa vuoden päästä työsuhteen alkamisesta.

Verkkotunnusten sulkeutumistakin testattiin erilaisilla ajankohdilla. Tilanteita edustivat testihenkilöt, joiden työsuhde oli merkitty päättymään kyseisenä päivänä, edellisenä päivänä sekä viikko, kuukausi tai jopa vuosi sitten. Järjestelmän toimintaa testattiin lisäksi erilaisilla työsuhteissa esiintyvillä tilanteilla, kuten vakituisten työntekijöiden siirtymisellä uuteen työtehtävään tai määräaikaisten työnsuhteiden jatkamisella eripituisten taukojen jälkeen. Vakituisten työntekijöiden osalta seurattiin erityisesti työnimikkeiden päivittymistä ja määräaikaisten osalta tunnusten voimassaoloa. Toivottua oli, että samat tunnukset säilyivät tallessa lyhyiden työsuhteissa esiintyvien katkosten ajan. Pidemmissä katkoksissa tunnukset voitaisiin tarvittaessa sulkea joksikin aikaa. Tunnusten etukäteen suoritettava aktivoiminen ja jälkikäteen tapahtuva sulkeutuminen pystyttiin sallimaan initiedostoja muokkaamalla.

Työsuhdetietojen suodattamista testattiin siten, että yksittäisille henkilöille lisättiin useampia työsuhderivejä. Järjestelmän tuli valikoida näistä voimassa olevat ja tuoreimmat tiedot. Siitä syystä HR-dataan lisättiin rivejä, joissa työntekijällä oli aiemmin ollut eri työnimikkeitä sekä erilaisia nimi- ja yhteystietoja. Suodattamista testattiin myös

päällekkäisillä työsuhteilla, sillä joissain olosuhteissa tällainenkin tilanne voisi olla mahdollinen. Päällekkäisistä työsuhteista huolimatta työntekijällä tuli olla kuitenkin vain yksi verkkotunnus.

Kuvitteellisten työntekijöiden nimiin lisättiin harvinaisempia kirjaimia, jotta selvitettiin päätyvätkö nämä käyttäjänimeen. Näiden tuli suodattua tavallisiksi kirjaimiksi, kuten esimerkiksi ä → a ja é → e. Käyttäjänimeen päätyvät erikoismerkit saattaisivat myöhemmässä vaiheessa aiheuttaa haasteita muiden tietojärjestelmien kanssa. Nimien osalta testattiin käyttää myös väliviivallisia etu- ja sukunimiä sekä pidempiä nimiä. Tällaiset nimet ovat melko yleisiä ja tarvittaessa niitä on tärkeää lyhentää, jotta käyttäjänimi mahtuu järjestelmissä määriteltyihin merkkijonoihin. Nimien osalta testattiin lisäksi kahden samannimisen henkilön luomista. Tällaisissa tilanteissa järjestelmän tuli lisätä henkilöiden käyttäjänimeen erottava tekijä, jotta verkkotunnusten luominen onnistui.

Muutamien testihenkilöiden osalta testattiin erilaisten nimenmuutosten toteuttamista. Muutoksia tehtiin niin HR-datan kuin AD:nkin kautta. Järjestelmän tuli palauttaa AD:ssa tehdyt muutokset, sillä HR-data olisi jatkossa dominoiva tietolähde. Nimi- ja voimassaolotiedot siirtyisivät tulevaisuudessa HR-järjestelmästä AD:hen ja lisäksi määriteltyihin pilvipalveluihin. Tähän liittyen testattiin verkkotunnuksen sulkemista AD:n kautta, jolloin järjestelmä palautti tunnuksen aktiiviseen tilaan seuraavassa ajossa. Tietojen synkronoitumista pilvipalveluihin testattiin *Microsoft Azure AD*:n kanssa, jolloin mahdolliset nimenmuutokset ja voimassaolon päättymiset toteutuivat myös siellä.

Testauksen aikana selvitettiin myös raportointiominaisuuksien toimintaa. Niiden avulla voitiin kokeilla tapahtuvia toimenpiteitä simulaatiotilassa sekä tarkistaa todellisessa tilassa tehtyjä muutoksia ja niiden ajankohtia. Simulaatiotilasta olisi suurta hyötyä käyttöönoton edetessä ja järjestelmän määrityksiä muuttaessa. Raportointiominaisuudet tuovat merkittäviä hyötyjä myös virhetilanteiden selvittämiseen, sillä järjestelmä osaa selkeällä ja ymmärrettävällä tavalla kuvata virheen aiheuttanutta olosuhdetta.

8.5 Testauksen lopputulos

Testausvaiheessa päästiin tutustumaan Ruutuvihkon toimintaan perustoimintoja testaamalla. Järjestelmä toimi varsin luotettavasti jo tässä vaiheessa ja se kykeni käsittelemään haastaviakin tilanteita. Testauksen aikana havaittiin kuitenkin muutamia virheitä, jotka olisivat saattaneet myöhemmässä vaiheessa aiheuttaa haasteita.

Toimeksiantajalle laaditussa testausdokumentaatiossa ongelmien vakavuutta kuvattiin kolmiportaisella asteikolla sekä ehdotettiin mahdollista korjausta. Nämä asiat saataisiin todennäköisesti pienillä muutoksilla korjattua seuraavaan versioon.

Testauksen aikana havaittiin lisäksi järjestelmän määrityksiin liittyviä muutosideoita sekä tunnistettiin uusia tarpeita. Uusilla määrityksillä olisi tarkoitus edistää järjestelmän toimintaa ja joustavuutta. Kokonaisuuteen lisättäisiin myöhemmässä vaiheessa myös uusia toimintoja, jotka toisivat uutta lisäarvoa identiteetinhallinnan toteuttamiseen. Järjestelmä saataisiin hyvin mukautumaan toimeksiantajan ympäristöön ja sen ominaisuudet palvelisivat toimeksiantajan tarpeita.

Testauksessa käytettiin fiktiivistä ja käsin tuotettua HR-dataa. Tästä johtuen testitilanteissa saattoi esiintyä virheellisiä tietoja ja jopa mahdottomia tilanteita. Todellinen HR-järjestelmän tuottama data olisi ollut monilta osin puhtaampaa ja vakaampaa. Käsin tuotetulla datalla pystyttiin kuitenkin testaamaan harvinaisempiakin tilanteita suhteellisen nopeasti. Ruutuvihkon tuottamat virheilmoitukset auttoivat tarvittaessa testidatassa esiintyneiden virheiden ratkaisemisessa.

8.6 Jatkosuunnitelmat

Ensimmäisen testauskierroksen jälkeen järjestelmään tehtäisiin parannuksia ja korjauksia havaittujen ongelmakohtien perusteella. Samalla muutettaisiin järjestelmään liittyviä määrityksiä, jotta järjestelmä toimisi uusimpien ja tarkentuneiden toiveiden mukaisesti. Näiden muutosten vaikutuksia testattaisiin tulevilla testauskierroksilla.

Seuraavissa vaiheissa keskityttäisiin lisäksi HR-järjestelmästä tuotavan csv-tiedoston siirron automatisointiin ja siihen kuuluviin määrityksiin. Ruutuvihkon määritykset muutettaisiin sen jälkeen vastaamaan uusinta taulukkomallia. Käyttöönoton edetessä järjestelmällä voitaisiin myös käsitellä nykyisten jo olemassa olevien verkkotunnusten tietoja ja voimassaoloja.

Lähempänä käyttöönottoa kokonaisuuteen lisättäisiin uusia ominaisuuksia ja toimintoja, kuten verkkotunnusten luonti lomakkeella HR-datan ohi sekä uusien käyttäjätunnusten lähettäminen esimiehelle sähköpostilla. Käyttäjille voitaisiin myös jatkossa lisätä tavallisimmat käyttöoikeudet kustannuspaikkojen perusteella sekä siirtää verkkotunnukset automaattisesti oikeiden yksiköiden alle AD:ssa. Nämä helpottaisivat paljon manuaalista työtä.

Ruutuvihkoa kehitetään jatkuvasti ja käyttöönotettavaan kokonaisuuteen voitaisiin mahdollisesti lisätä uusia toimintoja vielä myöhemminkin. Myöhemmässä vaiheessa järjestelmään voitaisiin esimerkiksi integroida muita pilvipalveluita sekä parantaa käyttäjien käyttökokemusta vaikkapa kertakirjautumisratkaisulla.

9 YHTEENVETO

Opinnäytetyön tarkoituksena oli löytää toimeksiantajana toimineen kaupungin tarpeita vastaava identiteetinhallinnan ratkaisu, jolla tulevaisuudessa helpotettaisiin työntekijöihin liittyvää käyttäjienhallintaa. Järjestelmän tavoitteena oli ratkaista nykyisiin menettelyihin liittyneitä haasteita sekä vähentää käyttäjienhallintaan kuluvaa työaikaa. Tarpeita vastaavan järjestelmän löytämiseksi määriteltiin toimeksiantajan tarpeita sekä etsittiin, tutkittiin ja vertailtiin soveltuvia vaihtoehtoja. Kartoituksen jälkeen löydettiin neljä soveltuvaa vaihtoehtoa, jotka olivat Efecte IGA, Imprivata IdG, Enter Ruutuvihko sekä One Identity Manager. Hankittavaksi järjestelmäksi valikoitui Enter SystemsSolutions Oy:n julkisen hallinnon tarpeisiin kehitetty Ruutuvihko. Valintaan johtivat kustannusten kohtuullisuus, riittävät ominaisuudet sekä soveltuvuus nykyiseen ympäristöön.

Opinnäytetyön aikana perehdyttiin myös hankittavan järjestelmän käyttöönottoon liittyviin valmisteluihin sekä testaamiseen. Testaamisella selvitettiin järjestelmän toimivuutta ja soveltuvuutta toimeksiantajan ympäristössä. Järjestelmää testattiin pääasiassa HR-dataan lisättyjen testihenkilöiden avulla, jotka edustivat erilaisia työsuhteissa mahdollisia tilanteita. Testihenkilöillä kokeiltiin myös järjestelmän kykyä käsitellä eripituisia sekä erilaisia kirjaimia ja merkkejä sisältäviä nimiä. Lisäksi testattiin muun muassa nimenmuutosten toteuttamista sekä käyttöoikeuksien päättämistä työsuhteen loputtua. Tietojen synkronoitumista testattiin kokonaisuuteen integroidulla pilvipalvelulla, jolloin mahdolliset nimenmuutokset ja voimassaolon päättymiset toteutuivat myös pilviympäristössä. Testaamisen tuloksena löydettiin muutamia virheitä ja kehitysideoita, joihin kiinnitettäisiin huomiota käyttöönoton seuraavissa vaiheissa. Myöhemmässä vaiheessa järjestelmä otettaisiin laajemmin käyttöön, jolloin sen avulla voitaisiin luoda, päivittää ja sulkea työntekijöiden verkkotunnuksia suurilta osin automatisoidusti. Samalla järjestelmä tuo merkittäviä parannuksia kaupungin tietoturvaan sekä vähentää käyttäjienhallintaan kuluvaa työaikaa.

Identiteetin- ja pääsynhallinnan järjestelmät helpottavat käyttäjätilien luomista, päivittämistä ja sulkemista sekä mahdollistavat johdonmukaisen tavan hallita yrityksen resurssien saatavuutta. Nämä tehtävät ovat tavallisesti työllistäneet IT-osastoja runsaasti, mutta nykyaikaisten järjestelmien avulla prosessit voidaan automatisoida siten, että työaikaa jää enemmän myös muiden tärkeiden työtehtävien suorittamiseen. Toisaalta ne edistävät myös yrityksen laajentamista, sillä ratkaisuista saatavat hyödyt vain kasvavat työntekijöiden määrän ja erilaisten käyttöoikeuksien lisääntyessä. Tietotekniikan

trendien mukaisesti organisaatioissa ollaan lisäksi siirtymässä yhä enemmän pilvipohjaisten tietojärjestelmien ja palvelujen käyttöön, mikä johtaa siihen, että identiteettejä ja käyttöoikeuksia olisi hallinnoitava yhä johdonmukaisemmin. Virheet ja unohdukset voisivat helposti mahdollistaa sen, että työsuhteiden päätyttyä henkilöt jatkavat yrityksen resurssien ja luottamuksellisten tietojen hyödyntämistä omilta kotikoneiltaan. Aktiivisiksi unohtuneet käyttäjätilit ovat myös hakkereille suotuisia kanavia yrityksen järjestelmiin. Identiteetin- ja pääsynhallinnan järjestelmillä pystytään kuitenkin minimoimaan tämänkaltaisia riskejä.

Todennus ja valtuutus ovat identiteetin- ja pääsynhallinnalla suoritettavia tehtäviä. Todennuksen avulla selvitetään, mitä järjestelmään luotua sähköistä identiteettiä työasemalle tai tietojärjestelmään kirjautuva henkilö vastaa. Kun henkilön sähköinen identiteetti on varmistettu, valtuutuksella säädellään hänen käytettävissä olevia resursseja erilaisten käyttöoikeuksien avulla. Sekä todennukseen että valtuutukseen on olemassa erilaisia mekanismeja. Todennusmekanismit voivat olla fyysisiä suojausmekanismeja, jolloin todennuksessa voidaan hyödyntää muun muassa kulkukorttia tai sormenjäljen- ja kasvojentunnistusta. Todennukseen käytettävät suojausmekanismit voivat myös olla digitaalisia, jolloin todennuksessa voidaan hyödyntää muun muassa staattisia ja kertakäyttöisiä salasanoja, digitaalisia varmenteita tai erilaisia kertakirjautumisratkaisuja. Valtuutukseen käytettäviä mekanismeja voivat puolestaan olla esimerkiksi roolipohjainen tai attribuuttipohjainen pääsynvalvonta. Näiden avulla työntekijälle voidaan lisätä työssä tarvittavat käyttöoikeudet ennalta määritettyjen kokoelmien ja sääntöjen mukaan. Identiteetin- ja pääsynhallinnan järjestelmät mahdollistavat myös todennukseen ja valtuutukseen liittyvien tapahtumien tilastoinnin, minkä ansiosta mahdollisiin virheisiin ja väärinkäytöksiin on nopeampaa reagoida.

Identiteetin elinkaarta tulee hallita johdonmukaisesti koko elinkaaren ajan. Kun uusi työntekijä aloittaa työt yrityksessä, hänelle muodostetaan sähköinen identiteetti. Identiteetin luomiseen liittyy attribuuttien varmistaminen, identiteetin muodostaminen sekä tunnistetietojen myöntäminen. Identiteetin luomisen yhteydessä suoritetaan lisäksi provisiointi, jolla valmistellaan tietojärjestelmät käyttäjän palvelemista varten. Siihen liittyen identiteettitietueeseen lisätään käyttäjän kannalta oikeanlaiset attribuutit aina nimi- ja yhteystiedoista käyttöoikeuksiin saakka. Kun identiteetti on luotu ja provisioitu, voidaan sitä palvelujen mahdollistamisen lisäksi käyttää muun muassa luotetun viestinnän, kertakirjautumisen tai määritteiden jakamisen mahdollistamiseen. Identiteetin elinkaaren vaiheisiin kuuluu myös päivittäminen, jolloin identiteetin tietoja voidaan muuttaa esimerkiksi

sukunimen tai työtehtävien muuttumisen takia. Päivittäminen on kuitenkin toteutettava siten, että yksilöivät avaintunnisteet pysyvät samoina. Sen avulla varmistetaan jäljitettävyys, sillä identiteetin historiatiedot pysyvät tällä tavoin tallessa. Jossakin vaiheessa identiteetin elinkaarta tai sen lopulla identiteetti voi olla tarpeellista sulkea. Siihen voi olla useita syitä, kuten käyttäjätilin vanheneminen, tunnistetietojen varkaudet tai työsuhteen päättyminen. Mikäli identiteettiä ei ole tarvetta ottaa uudestaan käyttöön, voidaan se deprovisioida, jolloin identiteetti poistetaan yrityksen järjestelmistä.

Identiteetin- ja pääsynhallinnan järjestelmät ovat tärkeitä tietoturvan, operatiivisen tehokkuuden sekä tietosuojaan liittyvien lainsäädäntöjen noudattamisen kannalta. Järjestelmien avulla on helpompi hallita identiteettien voimassaoloa sekä resurssien saatavuutta. Ne mahdollistavat identiteettiin liittyvien attribuuttien ja käyttöoikeuksien hallinnan parhaimmillaan yhdestä keskitetystä järjestelmästä, jolloin muutokset voidaan toteuttaa samalla kertaa useisiin eri järjestelmiin. Tämän ansiosta tiedot pysyvät paremmin ajan tasalla ja identiteettien luominen ja poistaminen on helpompaa. Tämä vähentää myös manuaalisesta käsittelystä aiheutuvia virheitä ja estää ulkopuolisia pääsemästä yrityksen resursseihin, kun käyttäjätilit eivät unohdu aktiivisiksi. Johdonmukaiset käyttöoikeuksien hallintaan käytettävät työkalut edistät myös vähimpien oikeuksien periaatteen toteutumista. Identiteetin- ja pääsynhallinnan järjestelmillä voidaan lisäksi vähentää IT-osaston kuormittuneisuutta muun muassa käyttäjienhallintaa keskittämällä ja identiteetinhallinnan prosesseja automatisoimalla. Käyttäjien tehokkuutta ja käyttökokemusta voidaan myös parantaa vaikkapa kertakirjautumisen ja itsepalveluportaalien avulla. Järjestelmät sisältävät lisäksi ominaisuuksia, joilla voidaan tukea tietosuojaan liittyvän lainsäädännön noudattamista. Tällaisia ominaisuuksia ovat muun muassa monivaiheinen todennus, raportointi sekä pilvipalveluita koskevien suostumusten hallintaan käytettävät työkalut.

LÄHTEET

Bertino, Elisa & Takahashi, Kenji 2010. Identity Management: Concepts, Technologies, and Systems. Artech House. Viitattu 15.2.2021 https://ebookcentral.proquest.com/lib/turkuamk-ebooks/detail.action?docID=634511

Bozicevic, Vedran 2020. What is Identity and Access Management and Why It's Important for Modern Companies. GlobalDots. Viitattu 28.3.2021 https://www.globaldots.com/blog/what-is-identity-and-access-management-and-why-its-important-for-modern-companies1

Busso, John 2018. Authentication, Authorization, Accounting and Identity Management. CCSI. Viitattu 1.3.2021 https://www.ccsinet.com/blog/aaa-identity-management/

Canner, Ben 2020. Identity management vs. Access management: The difference. Solutions Review. Viitattu 1.2.2021 https://solutionsreview.com/identity-management/identity-management-vs-access-management-the-difference/

Casey, Keith 2020. What is Attribute-Based Access Control (ABAC)? Okta. Viitattu 13.4.2021 https://www.okta.com/blog/2020/09/attribute-based-access-control-abac/

Efecte. Efecte Identity Governance and Administration - Solution Description. Viitattu 5.4.2021 https://www.efecte.com/iam

Enter SystemSolutions. Enter Ruutuvihko nopeuttaa ja yksinkertaistaa käyttäjienhallintaa. Viitattu 6.4.2021 https://www.enter.fi/fi/ruutuvihko-kayttajahallinta/

Enter SystemSolutions. Ruutuvihko tuo joustavuutta tietohallintoon. Viitattu 6.4.2021 https://www.enter.fi/fi/hameenlinnan-kaupunki/

Friedensburg, Alexander 2018. Five recommended self-service functions in an IAM solution. Cloudworks AS. Viitattu 21.3.2021 https://cloudworks.no/en/five-recommended-self-service-functions-in-an-iam-solution/

Ihalainen, Petteri 2016. Difference between identity management and access management. GlobalSign Blog. Viitattu 1.2.2021 https://www.globalsign.com/en/blog/identity-management-vs-access-management

Imprivata. Imprivata Identity Governance. Viitattu 6.4.2021 https://www.imprivata.com/imprivata-identity-governance

Indu, I., Rubesh Anand, P. M. & Bhaskar, V. 2018. Identity and access management in cloud environment: Mechanisms and challenges. Elsevier. Viitattu 9.3.2021 https://www.sciencedirect.com/science/article/pii/S2215098617316750

ISO / IEC 24760-1:2019(E). IT Security and Privacy – A framefork for identity management – Part 1: Terminology and concepts.

Linden, Mikael 2015. Identiteetin- ja pääsynhallinta. Tampere University of Technology. Department of Pervasive Computing. Report, Vuosikerta 6. Viitattu 31.1.2021 http://URN.fi/URN:ISBN:978-952-15-3568-0

Martin, James A. & Waters, John K. 2018. What is IAM? Identity and access management explained. CSO. Viitattu 23.1.2021 https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html?page=1

Nallathamby, Johann 2018. What is Federated Identity Management? WSO2. Viitattu 21.3.2021 https://wso2.com/articles/2018/06/what-is-federated-identity-management/

Niemi, Kalle. Identiteetin- ja pääsynhallinta (IAM). Itewiki. Viitattu 28.3.2021 https://www.ite-wiki.fi/opas/kayttajahallinta-iam/

One Identity. Identity Manager. Viitattu 6.4.2021 https://www.oneidentity.com/products/identity-manager/

OpenID. What is OpenID? Viitattu 14.3.2021 https://openid.net/what-is-openid/

OpenText 2018. How Identity and Access Management helps meet the data protection requirements of GDPR. Viitattu 23.3.2021 https://blogs.opentext.com/how-identity-and-access-management-helps-meet-the-data-protection-requirements-of-gdpr/

PathMaker Group. Web SSO vs. Enterprise SSO – What do I need? Viitattu 7.2.2021 http://www.pathmaker-group.com/web-sso-vs-enterprise-sso-what-do-i-need/

Radha, Vedala & Reddy, D. Hitha 2012. A Survey on Single Sign-On Techniques. Elsevier. Viitattu 7.2.2021 https://www.researchgate.net/publication/257743941_A_Survey_on_Single_Sign-On_Techniques

Raittius, Rob 2018. What is OAuth? Definition and How it works. Varonis. Viitattu 14.3.2021 https://www.varonis.com/blog/what-is-oauth/

Rathod, Bhavdip 2019. Role of Identity and Access Management (IAM) in Cyber Security. Cyber Defense Magazine. Viitattu 27.3.2021 https://www.cyberdefensemagazine.com/role-of-identity-and-access-management-iam-in-cyber-security/

Rouse, Margaret; Gittlen, Sandra & Rosencrance, Linda 2020. What is identity and access management? Guide to IAM. TechTarget. Viitattu 24.1.2021 https://searchsecurity.tech-target.com/definition/identity-access-management-IAM-system

Shepherd, Jack 2020. What is SAML and How does it work? Okta. Viitattu 13.4.2021 https://www.okta.com/blog/2020/09/what-is-saml/

Tietosuojavaltuutetun toimisto. Henkilötietojen käsittely. Viitattu 23.3.2021 https://tieto-suoja.fi/henkilotietojen-kasittely

Vitale, Thomas 2019. Access Control: Identification, Authentication, and Authorization. Viitattu 2.3.2021 https://www.thomasvitale.com/access-control-authentication-authorization/

Windley, Phillip J. 2005. Digital Identity. USA: O'Reilly Media, Inc. ISBN 9780596008789