IDENTITEETIN- JA PÄÄSYNHALLINTA PALVELUNA

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Visamäki, Tietojenkäsittelyn koulutusohjelma

Syksy, 2018

Miina Vina

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma
Visamäki

Tekijä Miina Vina **Vuosi** 2018

Työn nimi Identiteetin- ja pääsynhallinta palveluna

Työn ohjaaja/t Erkki Laine, Jyrki Immonen

TIIVISTELMÄ

Opinnäytetyön tarkoitus oli selvittää pilvipalveluna toteutetun identiteetin- ja pääsynhallinnan järjestelmistä käytettävien käsitteiden merkitystä sekä tietoturvan ja tietosuojan kannalta käyttöönoton suunnittelussa huomioitavia asioita valtion viranomaisen näkökulmasta.

Lähdemateriaalina selvitystyössä käytettiin valtiovarainministeriön julkaisemia VAHTI-ohjeita, tietosuojavaltuutetun toimiston tuottamia ohjeita ja esimerkkitapaukseksi valitun pilvipalveluna toteutetun järjestelmän sopimus-, käyttöehto- ja käyttöohjedokumentteja. Lisäksi lähdemateriaalina käytettiin internetissä tarjolla olevia artikkeleita identiteetin- ja pääsynhallinnan pilvipalveluista.

Raporttiin on koostettu eri ohjeista identiteetin- ja pääsynhallinnan tietoturvavaatimuksiin vaikuttavia tekijöitä ja tietosuojan varmistamiseksi vaadittavia toimenpiteitä. Eri palvelun tuottajien ratkaisuista ja aiheesta kirjoitetuista artikkeleista saadun käsityksen perusteella raportissa käytettävällä IDaaS-käsitteellä tarkoitetaan pilvipalvelua, joka mahdollistaa IDaaS-palveluun integroitavien sovellusten ja palveluiden identiteetin- ja pääsynhallinnan.

Keskeiseksi kysymykseksi havaittiin datan sijainti ja sijainnin aiheuttamat tietoturvariskit, varautumisen riskit ja tietosuojan toteutumisen edellyttämät toimenpiteet. Organisaation pitää tietää missä data sijaitsee ja kuka sitä käsittelee sekä arvioida miten kriittistä on palvelun toiminnan jatkuminen myös silloin, kun tietoliikenneyhteydet ulkomaille katkeavat.

Avainsanat IAM, IDaaS, Identiteetin- ja pääsynhallinta, pilvipalvelut

Sivut 33 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Visamäki

Author Miina Vina **Year** 2018

Subject Identity and Access Management as a Service

Supervisors Erkki Laine, Jyrki Immonen

ABSTRACT

The purpose of this thesis was to find out the meaning of terms for cloud based identity and access management systems and to determine what security and data protection regulations the governmental authority has to take into account when planning to use a cloud based identity and access management system.

The VAHTI-instructions published by the Ministry of Finance, articles and guides published by the Office of the Data Protection Ombudsman as well as a data processing agreement, hosting and delivery policy and an administrator guide for a selected service example with cloud based identity and access management solution were used as source materials in the research. The materials also include articles found on Internet about cloud based identity and access management.

Factors that affect security requirements of identity and access management systems and actions needed to ensure the data privacy have been collected in this thesis. The meaning of the term IDaaS is based on articles about the term and solutions provided by different service providers. The term IDaaS is used in this report when referring to a cloud service, which enables identity and access management for services and IDaaS integrated programs.

The important question based on the research is the location of the data and its impacts on security, availability and privacy risks and the required actions for protection of personal data. Organizations must know where the data is and who has access to it. Organizations have to plan how to ensure continuity of operations if the international network connection is lost.

Keywords IAM, IDaaS, Identity and Access Management, Cloud Services

Pages 33 pages

SISÄLLYS

SANASTO

AM	Access Management, pääsynhallinta
GDPR	General Data Protection Requlation, Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisen henkilöiden suojelusta henkilötietojen käsittelystä sekä näiden tietojen vapaasta liikkuvuudesta ja diretiivin 95/46/EY kumoamisesta, EU:n yleinen tietosuoja-asetus
IDaaS	Identity As a Service, identiteetinhallinnan pilvipalvelu
IdM	Identity Management, identiteetinhallinta
IAM	Identity and Access Management, identiteetin- ja pääsynhallinta
IAMaaS	Identity and access management as a service
IdP	Identity provider, federoidussa identiteetinhallinnassa identiteetin tarjoaja, tunnistuspalvelu
IPSec	Internet Protocol Security, joukko protokollia verkkoyhteyden välityksellä siirrettävän tiedon salaamiseen ja turvaamiseen
Käyttövaltuus	Käyttöoikeus, oikeus johonkin toimenpiteeseen tai resurssiin
MFA	Multi Factor Authentication, useaan tunnistetekijään perustuva tunnistus
OAuth 2.0	Avoin standardi, protokolla valtuuttamiseen
OpenID Connect	Avoin standardi, protokolla tunnistamiseen. Protokollaan on integroitu OAuth 2.0-protokollan kyvykkyydet
Provisiointi	Identiteetinhallinnassa uuden sähköisen identiteetin luominen, muokkaaminen tai poistaminen kohdejärjestelmästä identiteetinhallinnan järjestelmään asetettujen sääntöjen perusteella

Pääsynhallinta	Käyttäjän tunnistaminen ja käyttöoikeuksien (valtuuksien) päättely
Pääsynvalvonta	Tunnistetun käyttäjän käyttöoikeuksien (valtuuksien) päättely
SAML	Security Assertion Markup Language, avoin standardi, XML-pohjainen kehys käyttäjän todennus-, oikeus- ja attribuuttitietojen välittämiseksi identiteetin ylläpitäjältä palveluun
SCIM	System for cross-domain Identity Management, avoin standardi pilvipalveluiden ja -sovellusten identieetinhallintaan
SIEM	Security Informationand Event Management, keskitetty lokien ja tapahtumien hallintapalvelu
SP	Service Provider, federoidussa identiteetinhallinnassa tunnistuspalveluun nojaava palvelu
SPML	Simple provisioining markup language, XML-pohjainen protokolla provisiointiin
SSH	Secure Shell, protokolla ja sovellus, jota käytetään verkkoyhteyden salaamiseen
Synkronointi	Tietojen välittäminen lähdejärjestelmästä toiseen siten, että tiedon muuttuessa yhdessä paikassa, muutetaan se myös muihin synkronoinnin piiriin kuuluviin järjestelmiin
TLS	Transport Layer Security protocol, verkkoyhteyden salaamiseen käytetty protokolla
Tunnistaminen	Tapahtuma, jossa tunnistautunut käyttäjä yksilöidään ja henkilöllisyys todennetaan
Tunnistautuminen	Tapahtuma, jossa käyttäjä esittää yksilöivän tunnisteensa tietojärjestelmässä ja todistaa olevansa sen haltija
VAHTI	Valtiovarainministeriön asettama julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

VPN	Virtual Private Network, tekniikka turvallisten verkkoyhteyksien muodostamiseksi

1 JOHDANTO

Tietojärjestelmien toteutustapana ovat yleistyneet pilvipalvelut, joiden toimintamalli tukee palveluiden nopeaa käyttöönottoa, helppoa integroitavuutta ja jatkuvatoimintaisuutta. Pilvipalvelut skaalautuvat ketterästi asiakkaan tarpeiden mukaan. Samoja ominaisuuksia kaivataan identiteetin- ja pääsynhallinnan järjestelmien toimintaan, jotta tunnistamisen ja käyttövaltuushallinnan palvelut olisi helppo ottaa käyttöön organisaation uusissa järjestelmissä. Pilvipalvelun käyttöönoton yhteydessä organisaatiossa mietitään täyttääkö Identity as a Service-toimintamalli (IDaaS) organisaation vaatimat tietoturvan, tietosuojan ja teknisten ominaisuuksien vaatimukset ja voidaanko IDaaS-palvelua hyödyntämällä saada identiteetin- ja pääsynhallintaan kaivattua ketteryyttä ja joustavuutta.

Tässä opinnäytetyössä selvitetään mitä tietoturvaan ja tietosuojaan liittyviä vaatimuksia on huomioitava, jos identiteetin- ja pääsynhallinnan palvelut toteutetaan pilvipalvelussa. Selvitystyötä tehdään valtion viraston näkökulmasta, joten työssä huomioidaan valtion viraston toimintaan kohdistuvat vaatimukset, ohjeet ja lainsäädäntö. Lisäksi tutkitaan Oraclen toteuttaman Identity Cloud Service -tuotteen ominaisuuksia esimerkkinä pilvipalvelussa toteutetusta IAM-ratkaisusta.

Opinnäytetyössä selvitetään, mitä tarkoittaa IDaaS ja Cloud IAM sekä mitä tietoturvaan ja tietosuojaan liittyviä asioita tulee huomioida, kun suunnitellaan identiteetin- ja pääsynhallinnan järjestelmän toteuttamista pilvipalvelussa.

IDENTITEETIN- JA PÄÄSYNHALLINTA

”Tietotekniikassa (sähköinen) identiteetti tarkoittaa kohdetta kuvailevien ominaisuuksien eli attribuuttien kokoelmaa” (Linden 2015, 10). Tyypillinen sähköinen identiteetti on henkilön käyttäjätunnus tietojärjestelmässä. Sähköinen identiteetti voi olla myös esimerkiksi organisaatiolla tai laitteella. Sähköinen identiteetti sisältää tosielämän kohdetta kuvaavia tietoja, attribuutteja. Esimerkiksi työpaikan sähköpostitilin tietoihin tarvitaan henkilön nimi ja sähköpostiosoite, intranetin käyttäjätietoihin voi olla tarpeen lisätä puhelinnumero ja tehtävänimike. (Linden 2015, 10–11.)

Sähköinen identiteetti syntyy, kun on tarpeellista hyödyntää kohteen ominaisuuksia tietojärjestelmissä. Esimerkiksi tiedon turvaamiseksi pääsy rajataan vain käyttäjälle tarpeellisiin resursseihin. Tietojen oikeellisuus ja käsittelyn jäljitettävyys varmistetaan, kun tietojen käsittelystä jää jälki johon tallennetaan tunnistetieto käyttäjästä. Identiteetin tietoja hyödyntämällä tarjotaan hyvä käyttökokemus sähköisessä palvelussa tarjoamalla erilaisia näkymiä perustuen henkilön rooliin ja asemaan organisaatiossa. Korkeakoulun intranetissa voidaan näyttää opiskelijalle ja opettajalle erilaiset näkymät ja uutiset.

Identiteetinhallinta (IdM, Identity Management) on prosessi, jolla sähköisen identiteetin tietoja ylläpidetään sekä välitetään eri tietojärjestelmiin organisaation toimintakäytännön mukaisesti. (Linden 2015, 10–11.) Identiteetinhallinnan järjestelmällä yhdistetään eri tietojärjestelmissä olevat saman kohteen tunnisteet yhteen sähköiseen identiteettiin, jota voidaan hallita yhdessä paikassa. Esimerkiksi henkilöstöhallinnon tekemä nimenmuutos voidaan välittää sähköpostijärjestelmään sähköpostiosoitteen muuttamiseksi. Tieto välitetään sovittujen käytäntöjen mukaisesti muihinkin identiteetinhallintaan kytkettyihin järjestelmiin.

Pääsynhallinnalla (AM, Access Management) tarkoitetaan sitä toimintoa, jossa tietojärjestelmän käyttäjä tunnistetaan ja tunnistuksen perusteella päätetään, onko käyttäjällä käyttövaltuus kirjautua järjestelmään ja suorittaa hänen pyytämänsä toiminto. (Linden 2015, 11.)

1.1 Tunnistaminen ja käyttövaltuuksien hallinta

Jotta pääsy järjestelmään voidaan sallia, pitää tietojärjestelmää käyttävä henkilö tunnistaa. Yksinkertaisimmillaan tunnistamiseen käytetään käyttäjätunnusta ja salasanaa. (Linden 2015, 16.)

Identiteetin todentamiseen käytettävät menetelmät jaetaan kolmeen ryhmään:

1. Jotain, mitä henkilö tietää tai muistaa, kuten salasana

2. Jotain, mitä henkilöllä on hallussaan, kuten toimikortti tai matkapuhelin
3. Jotain, mitä henkilö on tai kuinka hän käyttäytyy, kuten sormenjälki

Kahteen tai useampaan eri ryhmän tekijään perustuvaa tunnistusta pidetään vahvana tunnistamisena. (Linden 2015, 16.)

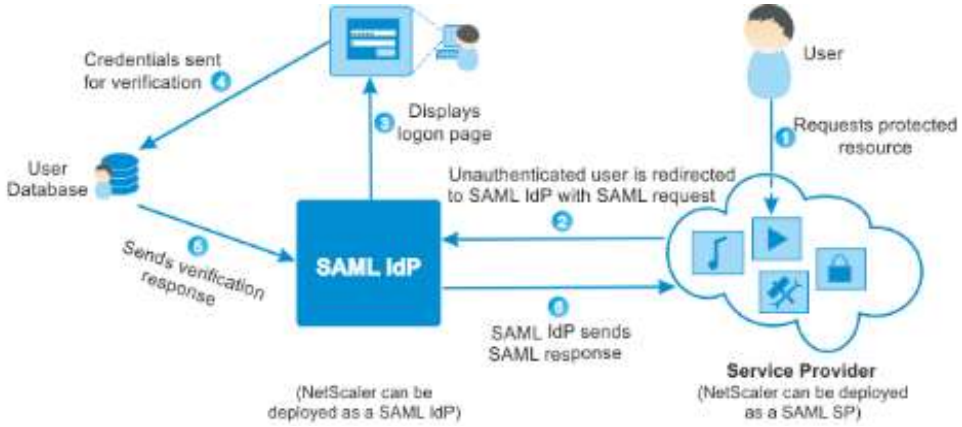
Pelkkä henkilön tunnistaminen ei ole riittävä toimenpide tietojärjestelmän käytön ja tietoturvan näkökulmasta. Käyttäjän tunnistamisen jälkeen tietojärjestelmän toimintojen pitää tietää, onko käyttäjällä oikeus käyttää tietojärjestelmää tai tehdä erilaisia toimenpiteitä järjestelmässä. Jotta tietojärjestelmään tallennettua luottamuksellista aineistoa ei pääse käsittelemään kuka tahansa kirjautunut käyttäjä, tulee kyseisen aineiston käyttöön myöntää käyttövaltuus. (Linden 2015, 31.)

Kertakirjautumisen toteuttavat tekniikat mahdollistavat sen, että käyttäjän ei tarvitse tunnistautua erikseen jokaiseen käyttämäänsä palveluun. Kertakirjautumisen piirissä olevat palvelut ovat käytettävissä ilman käyttäjän toimenpiteitä, kun käyttäjätunnus ja salasana on syötetty ensimmäiseen palveluun. Federoidulla identiteetinhallinnalla toteutetaan usein myös kertakirjautuminen.

1.2 **Federoitu identiteetinhallinta**

Federoitu identiteetinhallinta mahdollistaa saman identiteetin hyödyntämisen identiteettiä hallitsevan organisaation ulkopuolella toteutetussa tietojärjestelmässä tai palvelussa. Federoidussa identiteetinhallinnassa identiteettiä hallitaan yhdessä organisaatiossa ja sen tietoja voidaan hyödyntää muiden organisaatioiden ylläpitämissä palveluissa. Identiteettiä hallinnoiva ja palvelua ylläpitävä organisaatio tekevät luottamussopimuksen, jossa sovitaan identiteetin ja- pääsynhallinnan yhteisistä toimintatavoista ja identiteetin attribuuttien yhdenmukaisuudesta. Identiteettiä hallinnoiva organisaatio vastaa tietojen oikeellisuudesta ja ajantasaisuudesta.

Federoitu identiteetinhallinta mahdollistaa sen, että käyttäjä ei tarvitse erillistä käyttäjätunnusta kirjautuessaan toisen organisaation tarjoamaan palveluun. Palvelu ohjaa käyttäjän tunnistautumaan oman organisaationsa tunnistuspalveluun. Tunnistuspalvelu välittää palvelulle tiedon onnistuneesta tunnistautumisesta. Identiteettiä hyödyntävä palvelu luottaa käyttäjän omassa organisaatiossa tehtyyn tunnistamiseen. Käyttäjän kotiorganisaatio puolestaan luottaa palveluun ja välittää käyttäjän tiedot palvelulle (kuva 1).



Kuva 1. Federoitu kirjautuminen SAML-protokollaa hyödyntäen (Citrix 2017).

2 VALTIONHALLINNON TIETOJENKÄSITTELYN VAATIMUKSET

2.1 Valtion viraston tietoturvan säädökset

Valtion viranomaisen yleistä velvollisuutta huolehtia toimintansa tietoturvasta ohjataan lainsäädännöllä. Velvollisuudesta säädetään viranomaisen toiminnan julkisuudesta annetussa laissa (Julkisuuslaki, 621/1999). Asiakirjojen käsittelyä, asiakirjojen luokittelusta ja luokittelua vastaavista tietoturvavaatimuksista säädetään asetuksessa tietoturvallisuudesta valtionhallinnossa (Tietoturvallisuusasetus, 681/2010).

Valtiovarainministeriä valmistelee uutta lakia julkisen hallinnon tiedonhallinnasta. Lailla uudistettaisiin julkisen hallinnon tiedonhallintaa ja sitä koskevaa ohjausta koskeva sääntely. Laki korvaa Julkisuuslain hyvää tiedonhallintatapaa koskevan sääntelyn. (Kivivasara, n.d.)

Henkilötietojen käsittelystä säädetään 25.5.2016 voimaan tulleessa EU:n yleisessä tietosuoja-asetuksessa. Tietosuoja-asetus tuli sovellettavaksi siirtymäajan jälkeen 25.5.2018. Asetus koskee sekä julkisella että yksityisellä sektorilla tapahtuvaa henkilötietojen käsittelyä. (Eduskunta, 2018) Asetusta sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa. Tietyissä kysymyksissä valtioilla on kutenkin mahdollisuus säätää poikkeuksia ja täsmennyksiä. (Oikeusministeriö, 2018.). Suomessa on voimassa Henkilötietolaki 523/1999. Henkilötietolakia sovelletaan niiltä osin, kuin se ei ole ristiriidassa tietosuoja-asetuksen kanssa. (Tietosuojavaltuutetun toimisto, Henkilötietolaki, n.d.) Hallitus on antanut eduskunnalle esityksen henkilötietolain kumoamisesta ja sen korvaamisesta uudella, EU:n tietosuoja-asetusta täydentävällä ja täsmentävällä tietosuojalailla. Lakia sovellettaisiin rinnakkain tietosuoja-asetuksen kanssa ja sen on tarkoitus kumota henkilötietolaki. (HE 9/2018.)

Valtioneuvoston tekemät periaatepäätökset antavat ohjeita valtionhallinnolle. Periaatepäätökset ovat poliittisia kannanottoja ja luonteeltaan valmistelevia päätöksiä. Kukin hallitus päättää erikseen hallituskautensa alussa, mitkä aiemmin hyväksytyt päätökset ovat voimassa kuluvalla hallituskaudella. Valtionhallinnon tietoturvallisuuden kehittämisestä 26.11.2009 tehdyllä periaatepäätöksellä ohjataan valtionhallinnon tietoturvatoimintaa. (Valtioneuvosto, n.d.)

2.2 VAHTI

VAHTI on valtiovarainministeriön asettama digitaalisen turvallisuuden johtoryhmä, joka toimii julkisen hallinnon tietoturvallisuuden ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatio-

elimenä. VAHTI edistää julkishallinnon digitalisaatiota huolehtimalla turvallisuuden vaatimuskehikon laatimisesta ja ylläpitämisestä. (Valtiovarainministeriö, n.d.)

VAHTI ohjaa valtionhallinnon tietoturvatoimenpiteitä ja käsittelee tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja muut linjaukset (Valtioneuvosto, 2009, 33). Valtioneuvoston periaatepäätöksessä valtionhallinnon tietoturvallisuuden kehittämisestä todetaan, että viranomaisella tulee olla VAHTI-ohjeisiin ja tietoturvatasomäärityksiin ja varautumistoiminnan vaatimuksiin perustuvat suunnitelmat, ohjeet ja menettelyt (Valtioneuvosto, 2009, 10).

VAHTI-ohje 9/2006 ohjeessa käyttövaltuushallinnan tärkeimpiä teknisiä vaatimuksia on jatkuvatoimintaisuus, korkeinta luokkaa oleva sisäinen tietoturvallisuus ja skaalautuvuus. Käyttövaltuushallinnan pitäisi mahdollistaa toimivat varajärjestelyt poikkeustilanteissa. Samassa ohjeessa on vaatimus käyttövaltuuksien hallinnan prosessin jäljitettävyydestä. Jälkikäteen pitää pystyä selvittämään kuka tai ketkä ovat myöntäneet ja muokanneet käyttövaltuuksia ja milloin muutokset käyttövaltuuksiin on tehty. Käyttövaltuushallintajärjestelmän tulee mahdollistaa raportit käyttäjistä ja heidän työrooleistaan, työrooleista ja niihin kytketyistä käyttövaltuuksista, käyttäjistä ja heidän käyttövaltuuksistaan, käyttäjistä tietyllä työroolilla ja käyttäjistä, joilla on oikeudet tiettyyn kohteeseen. (VAHTI 2006, 16,21,29–30.)

2.3 **Tietoturvallisuuden tasot**

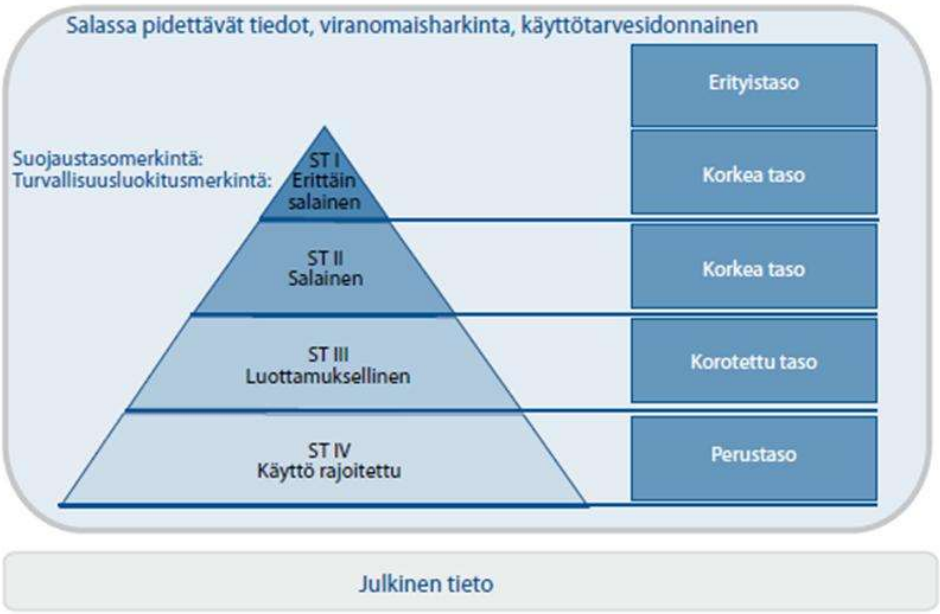
Tietoturvallisuusasetuksessa tietoturvallisuudella tarkoitetaan hallinnollisia, teknisiä ja muita toimenpiteitä, jotka organisaatio toteuttaa tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi. Valtion viranomaisella tarkoitetaan valtion hallintoviranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia. (Asetus tietoturvallisuudesta valtionhallinnossa 681/2010, § 3.)

Viranomaisella on velvollisuus toteuttaa hyvää tiedonhallintatapaa ja siten huolehtia tietojen ja tietojärjestelmien saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja laadusta (Laki viranomaisen toiminnan julkisuudesta, Julkisuuslaki 612/1999, § 18). Tietoturvallisuusasetuksessa säädetään viranomaisen asiakirjojen käsittelyä koskevista yleisistä tietoturvavaatimuksista, asiakirjojen luokittelusta ja luokittelua vastaavista tietoturvavaatimuksista. VAHTI -ohjeessa 2/2010 annetaan ohjeet tietotuvallisuusasetuksen vaatimusten toteuttamiseksi.

Organisaation ja tietojenkäsittely-ympäristön tietoturvavaatimukset määritellään tietoturvallisuustasojen avulla. Tasot kuvaavat hallinnollisia ja teknisiä vaatimuksia, joita organisaatiossa tulee toteuttaa. Tasoja on

kolme: perustaso, korotettu taso ja korkea taso. Valtion viranomaisen tulee toteuttaa vähintään tietoturvallisuuden perustaso. (VAHTI 2012b, 27.) Tietojärjestelmän merkitys, tietojenkäsittely-ympäristössä käsiteltävän aineiston suojausluokitus sekä niihin kohdistuvat riskit ja uhat vaikuttavat ympäristöltä vaadittavaan tietoturvatasoon (kuva 2). (VAHTI 2010. 15–16.)

Asiakirjojen luokittelussa on käytössä neljä tasoa. Asiakirjan suojaustasoon vaikuttaa miten suuri haitta aiheutuu, jos asiakirjan sisältämä tieto paljastuu. Asiakirjojen luokittelua suositellaan käytettäväksi vain salassa pidettäviin asiakirjoihin. (VAHTI 2010, 53-54.)



Kuva 2. Suojaustasoa vastaavat tietoturvatasot (VAHTI 3/2012, 27.)

Yksittäinen korotetulla tasolla oleva tietojärjestelmä edellyttää kaikkien palvelun tuottamiseksi tarvittavien teknisten ratkaisujen ja prosessien toteuttamista korotetulla tasolla. Eri suojaustason järjestelmät eriytetään toisistaan. (VAHTI 2012b, 34–35.)

2.3.1 Tietoturvallisuuden perustaso

Tietoturvallisuuden perustason toteuttavassa ympäristössä voidaan käsitellä salaamattomana enintään suojaustason IV luokiteltua tietoaineistoa (VAHTI 2010, 43). Perustason toteuttamiseksi viranomaisen on huolehdittava, että sen toimintaan liittyvät tietoturvariskit on kartoitettu ja käsiteltävän aineiston tärkeys tunnistettu. Tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu on määritelty ja tehtävien hoitamiseen on riittävä asiantuntemus ja työvoima. Tietoturvan ja ohjeiden noudattamista valvotaan. Tietojen saanti ja käytettävyys turvataan eri tilanteissa. Häiriötilan-

teisiin varaudutaan tärkeiden toimintojen jatkuvuussuunnittelun ja toipumissuunnitelmien avulla. Tietojen salassapito varmistetaan antamalla pääsy vain niille, jotka tarvitsevat tietoja työtehtäviensä hoitamiseksi. Tietojärjestelmiä käyttävien roolien käyttövaltuudet tulee suunnitella ja eri rooleissa toimivat henkilöt pitää pystyä listaamaan rooleittain ja tietojärjestelmittäin. Tietojen eheys varmistetaan estämällä tiedon muuttaminen ja luvaton käsittely käyttövaltuushallinnan ja valvonnan avulla. Tietojen säilytystilat tulee olla riittävästi valvottuja ja suojattuja. Henkilöstön tietoturvaosaaminen varmistetaan säännöllisellä koulutuksella ja ohjeistuksella. Henkilöstön luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn avulla. Myös palvelua tuottavan toimittajan ja sen alihankkijoiden tulee täyttää fyysiseen tietoturvaan kohdistuvat vaatimukset. Palvelua tuottavan toimittajan henkilöstön ja sen alihankkijoiden luotettavuudesta tulee huolehtia. Viranomainen valvoo tietojen käsittelyä myös silloin, kun tietoja käsitellään toimeksiantosopimuksen perusteella jossain toisessa organisaatiossa. (VAHTI 2012b, 19–23.) Palvelun hankintasopimuksessa määritellään tietoturvavaatimukset ja miten tietoturvallisuuden valvonta, seuranta, auditointi ja raportointi toteutetaan. (VAHTI 2010, 109).

Tietojärjestelmien tulee tuottaa sellaista lokitietoa, josta niiden käyttöä voidaan tarvittaessa selvittää ja valvoa. Valvontaan on suositeltavaa ottaa käyttöön keskitetty lokien ja tapahtumien hallintapalvelu (SIEM). Sekä onnistuneet että epäonnistuneet kirjautumiset kirjoitetaan lokiin. Lokin tietojen perusteella yksittäisen käyttäjän kirjautumiset voidaan yhdistää hänen henkilöllisyyteensä luotettavasti. (VAHTI 2012b, 22.)

Organisaatiolla on määritelty salasanapolitiikka ja huonolaatuisten salasanojen käyttö estetään. Tunnistautumiseen käytetään henkilökohtaisia käyttäjätunnuksia. Valtiohallinnon yhteisiä tietojärjestelmiä käytettäessä suositellaan käytettäväksi Virtu-kirjautumista. Virtu on valtionhallinnon organisaatioiden välinen luottamusverkosto, joka toteuttaa federoidun identiteetinhallinnan valtion organisaatioiden välillä. (VAHTI 2010, 75–80.)

Käyttövaltuudet ovat henkilö- tai roolikohtaisia. Yksittäisen käyttäjän käyttövaltuudet voidaan selvittää. Ensitunnistus organisaatiossa aloittavalle käyttäjälle tehdään valokuvallisesta henkilöllisyystodistuksesta tai saman tasoista sähköistä todennusmenetelmää käyttäen. Varmuuskopioita otetaan olennaisista suojattavista kohteista suunnitelman mukaisesti. (VAHTI 2010, 118–122.)

2.3.2 Korotettu ja korkea tietoturvataso

Korotetun tieturvatason ympäristössä on mahdollista käsitellä selväkielisenä tietoa, jonka suojaustaso on III (VAHTI 2010, 43). Tietoaineistojen käyttö organisaation ulkopuolisesta verkosta edellyttää vahvaa tunnistau-

tumista (VAHTI 2012b, 48). Vahva suositus on, että korotetun tason järjestelmässä käytetään vahvaa tunnistautumista. Tietojärjestelmään saadaan asentaa vain omistajan hyväksymiä ohjelmia ja laitteita. Organisaatio on määritellyt sallitut laitteet ja ohjelmat. Organisaatiolla on erilliset, toisiaan täydellisesti vastaavat kehitys- ja tuotantoympäristöt. Erillinen testiympäristö voidaan jättää toteuttamatta riskianalyysin perusteella. (VAHTI 2012b, Liite 3.)

Sopimuksessa määritellään tietoturvataso, jota palvelun tuottajan tai sen alihankkijan tulee noudattaa. Tietoturvavaatimukset määritellään tarjouspyynnössä. (VAHTI 2010, 109.)

Muut, kuin kiireelliset päivitykset tai muutokset tehdään vain etukäteen sovittuna aikana (VAHTI 2010, 109). Virheelliset kirjautumisyritykset tärkeimpiin järjestelmiin tai palveluihin aiheuttavat tunnuksen lukkiutumisen. Jälkikäteen on selvitettävissä, millä perusteella käyttäjän käyttövaltuudet on myönnetty. Laitetiloissa eri suojausluokkaa vaativat osat on eriytetty rajoittamalla kulkua tilojen välillä. Tärkeimmistä järjestelmistä otetaan suojakopioita, joita säilytetään eri palotilassa, kuin varmuuskopioita. Tietojärjestelmän määritykset ja toteutukset on auditoitu tietoturvallisuuden osalta. (VAHTI 2010. 118–125.) Auditoinnista on olemassa kirjallinen raportti ja sen suorittaja ei ole järjestelmän toimittaja tai kehittäjä (VAHTI 2012b, Liite 3).

Korkean tietoturvatason ympäristössä voidaan käsitellä selväkielisenä enintään II -suojaustason luokiteltua aineistoa (VAHTI 2010, 43). Kun korkean tason palveluita käytetään organisaation ulkopuolisesta verkosta, pitää käyttää vahvaa tunnistautumista (VAHTI 2012b. 118–122).

Tunnistuksen epäonnistumista sekä valtuuksien puutteeseen kariutuvia toimenpideyrityksiä tilastoidaan. Laitetiloja ja kulkua tiloissa valvotaan automaattisesti ja valvontamenettely on dokumentoitu. Ulkopuolisten toimintaa laitetiloissa valvotaan. Varmuuskopioiden palautusta testataan säännöllisesti. (VAHTI 2012b. 118–122.) Kulkuoikeudet IT-laitetiloihin tarkastetaan vuosittain. Organisaatiolla on erilliset, toisiaan täydellisesti vastaavat kehitys- ja tuotantoympäristöt. Korkean tason järjestelmässä käytetään vahvaa tunnistautumista. (VAHTI 2012b, Liite 3.)

Jatkuvuussuunnitelmien toimivuutta harjoitellaan keskeisten yhteistyökumppanien kanssa (VAHTI 2010, 105). Ennen sopimuksen solmimista, organisaatio auditoi kumppanin. Sopimuksessa määritellään sanktiot tietoturvapoikkeamista ja -loukkauksista. (VAHTI 2010, 109.)

2.4 **ICT-varautumisen tasot**

Hyvään tiedonhallintatapaan kuuluu varautuminen häiriötilanteisiin (VAHTI 2012a, 12). Varautuminen käsittää hallinnolliset, toiminnalliset ja

tekniset toimenpiteet ja ratkaisut, joilla varmistetaan palveluiden saatavuus ja toiminnan jatkuvuus. ICT-varautumisen tasot ovat avoin taso, perustaso, korotettu ja korkea taso. Tasoille sijoitetaan palvelut niiden tarpeiden ja tärkeyden mukaisesti. Varautumisen taso voi olla matalampi, kuin palvelun tietoturvataso ja päin vastoin (VAHTI 2012a, 20.)

Varautumisen vaatimukset tulee sisällyttää tarjouspyyntöihin ja sopimuksiin. Sopimuksissa tulee varmistua, että vaatimukset toteutuvat koko hankintaketjussa ja että sopimuskumppanit huolehtivat siitä, että kumppanit asettavat varautumisvelvoitteet myös alihankkijoilleen. (VAHTI 2012a, 26.)
Avoin taso on lähtötaso, jolloin organisaation varautumistarpeita ei ole vielä määritelty. Avoimella tasolla voidaan myös harkitusti toteuttaa palveluita. Avoimen tason palvelu voi olla pitkiäkin aikoja poissa käytöstä ilman suurta haittaa tai vastaava palvelu on mahdollista saada jotain muuta kautta. (VAHTI 2012a, 21.)

Perustasolle sijoitetaan palvelut, joiden hetkellinen lamautuminen häiriötilanteissa ei keskeytä organisaation ydintoimintoja. Palveluiden käytön pääpaino on virka-aikana. Vian korjaaminen voidaan aloittaa seuraavana arkipäivänä. Tavoitteellinen toipumisaika häiriöstä voi olla seuraavan työpäivän aikana. (VAHTI 2012a, 22.)

Korotetulle tasolle määritellään organisaation kannalta kriittiset toiminnot. Korotetulle tasolle sijoitetaan yhteiskunnan elintärkeitä toimintoja tukevia tai kansalaiselle häiriötilanteissa keskeisiä palveluja ja tietojärjestelmiä. Tietojärjestelmissä on ympärivuorokautinen valvonta ja vian korjaaminen on mahdollista aloittaa viivytyksettä. Jos palvelu tai järjestelmä on tärkeä yhteiskunnan elintärkeille toiminnoille ja poikkeusolojen toiminnalle, sen on toimittava myös niissä tilanteissa, joissa yhteydet Suomesta ulkomaille ovat lamaantuneet. Korotettu varautumisen taso olisi syytä todentaa ulkopuolisen auditoinnin avulla. (VAHTI 2012a, 22.) Tietoliikennepalvelun priorisointi ja muutokset häiriötilanteessa on suunniteltu ja sovittu palvelutoimittajan kanssa (VAHTI 2012a, 79).

Korkean varautumisen tason tietojärjestelmiä ovat esimerkiksi hallinnon turvallisuusverkko ja turvallisuusviranomaisten operatiiviset järjestelmät. Palveluiden ja tietojärjestelmien tulee toimia ympärivuorokautisesti. Pienetkin palvelukatkokset tietojärjestelmien toiminnassa aiheuttavat vakavia toiminnallisia häiriöitä. Korkean tason palveluiden on toimittava, vaikka tietoliikenneyhteydet ulkomaille olisivat poikki. (VAHTI 2012a, 22–23.) "Kriittisten palveluiden ja sovellusten käyttöoikeudet hallitaan ja valvotaan Suomesta" (VAHTI 2012a, 75). Kriittisten toimintojen, kuten sähkönjakelun ohjausjärjestelmät ja tietoliikenneverkon solmujen kytkentäpisteet, palvelutuotanto on hajautettu vähintään kahteen eri paikkaan Suomessa. Verkot ja tietoliikennepalvelut varmennetaan ja toteutetaan hallinnon turvallisuusverkon vaatimusten mukaisesti. (VAHTI 2012a, 75–79.)

2.5 **Lokit**

VAHTI-ohjeissa on erillinen yleisohjeistus ICT-lokien turvallisesta käsittelystä valtionhallinnossa. Lokien käsittelyllä tarkoitetaan lokien keräämistä, analysointia, säilyttämistä, luovuttamista ja poistamista.

Lokien käsittelyn tulee perustua määritettyyn tarpeeseen, käsittelyn tulee tapahtua määriteltyjen järjestelmien ja toimintatapojen mukaisesti, analysointi tulee määritellä etukäteen ja käyttäjien sekä ylläpitäjien tietosuoja ja oikeusturva tulee huomioida käsittelyssä. Lokitiedon saatavuus, suoja, eheys ja laatu turvataan. Organisaation tulee varmistaa, että lokitiedot ovat turvassa hävittämiseltä, muuttamiselta ja muulta käsittelyltä. Ylläpitolokien kirjaus tulee toteuttaa siten, etteivät ylläpitäjät pääse poistamaan suorittamiensa toimenpiteiden merkintöjä. Lokitiedot, jotka sisältävät tunnistamistietoja tai henkilötietoja muodostavat henkilörekisterin. (VAHTI 2009, 19–21.) Lokitietojen säilytysaika määritellään ja säilytysajan umpeuduttua lokitiedot poistetaan (VAHTI 2009, 24).

Lokiin kirjatun tapahtuman suorittaja tulee tunnistaa henkilö-, järjestelmä-, tai prosessitasolla. Tunnistaminen edellyttää, että lokiin kirjataan epäonnistuneiden ja estettyjen tapahtumien lisäksi sallitut ja onnistuneet tapahtumat. Lokitietojen ja tunnisteiden avulla voidaan osoittaa osapuolet, jotka ovat olleet tekemisissä tietyn tapahtuman kanssa. (VAHTI 2009, 15.)

Tunnistamistietojen käsittelykerroista tulisi tallentaa ainakin aloitus- ja lopetusaika, käsittelijän yksilöivä ja henkilöön yhdistettävä tunnus, mitä tietoja on käsitelty, minkä ajankohdan tietoja on käsitelty, peruste lokin katsomiseen ja käsittelyyn ja mahdollinen kuvaus käsittelystä. Lokien käsittelyn loki on mahdollista toteuttaa esimerkiksi keskitetyllä lokijärjestelmällä, johon kaikki lokit kerätään ja johon kirjaudutaan henkilökohtaisella käyttäjätunnuksella. Tämän edellytyksenä on, että ulkoistetusta palvelusta lokit voidaan siirtää keskitettyyn järjestelmään sen hyväksymässä muodossa. (VAHTI 2009, 39–40.) Asiattomista lokien käsittely-yrityksistä pitää seurata hälytys (VAHTI 2009, 23).

Palvelun hankintaa suunniteltaessa lokien käsittelyyn liittyvät vaatimukset tulee selvittää ja määritellä. Lokien sisältö, sälytysaika, käyttövaltuudet ja saatavuus keskitettyyn lokien hallintajärjestelmään pitää selvittää. Lisäksi palvelun toimittajan osalta on selvitettävä, miten lokien muuttaminen on estetty ja miten lokin muuttaminen ja muuttaja jäljitetään. Toimittajan henkilöstön osalta tulee henkilöstön tekemät toimenpiteet kirjata lokiin samoin, kuin oman organisaation työntekijöiden tekemät toimenpiteet. Palvelusopimuksessa on hyvä määritellä lokien omistaja ja osapuolten oikeudet lokien käsittelyyn. (VAHTI 2009, 53¬–56.)

2.5.1 Pääsynhallintajärjestelmän loki

Lokiin tulee kirjoittaa kaikki onnistuneet ja epäonnistuneet tunnistautumiset ja sovellusten tai palveluiden käytön yritykset. Lisäksi lokiin kirjataan pääsynhallintajärjestelmään suoraan tehdyt tapahtumat ja tieto kohdejärjestelmiin välitetyistä tiedoista. Käyttövaltuuksien myöntäminen, poistaminen ja kyseisten toimintojen suorittaja pitää olla selvitettävissä. Järjestelmästä tulee saada myös raportti identiteeteistä, niiden haltijoista ja niihin liittyvistä käyttövaltuuksista. Lokitietojen perusteella käyttäjätietojen ja käyttövaltuuksien muutoksia voidaan seurata. (VAHTI 2006, 26–27.)

2.6 **Tietosuoja**

Henkilötietoja sisältävää IAM-järjestelmää hallinnoiva organisaatio toimii rekisterinpitäjänä ja sitä koskee tietosuoja-asetuksen asettamat rekisterinpitäjää koskevat velvollisuudet.

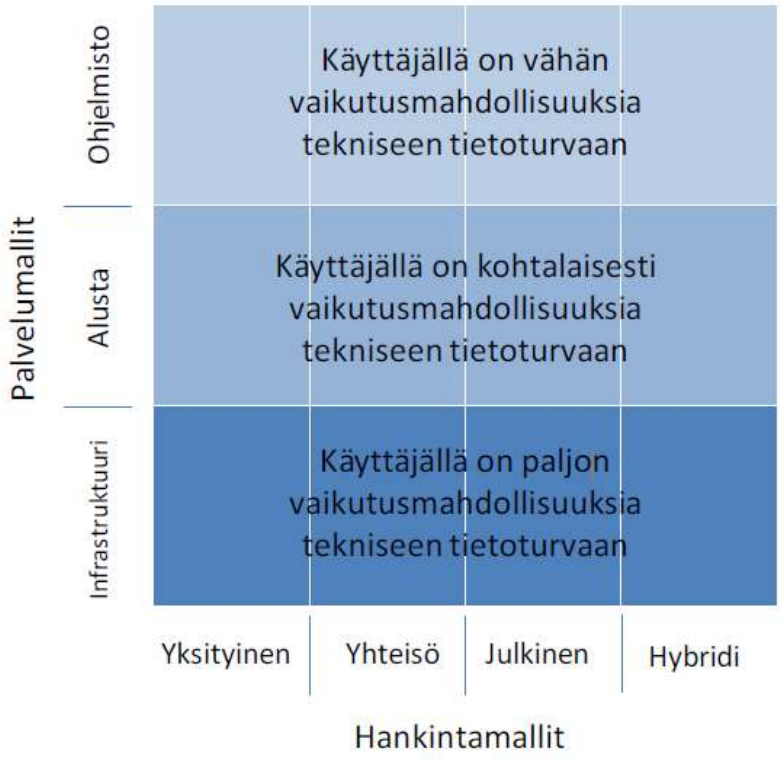
Rekisterinpitäjän tulee huolehtia siitä, että henkilötietojen käsittely perustuu asianmukaiseen perusteeseen. Asianmukaisia perusteita on esimerkiksi rekisteröidyn vapaaehtoinen ja yksiselitteinen suostumus, rekisterinpitäjän oikeutetun edun tai lakisääteisten velvoitteiden toteuttaminen. Rekisterinpitäjän pitää arvioida käsittelyyn liittyvät riskit ja suunniteltava riskien hallinta. Henkilötietoja kerätään vain todetun tarpeen mukaan, niitä säilytetään vain tarvittava aika. Pääsy henkilötietoihin rajataan vain niille, joilla on tarve päästä henkilötietoihin. Henkilötietoja sisältävän järjestelmän tietoturvasta huolehditaan. Rekisterinpitäjä huolehtii siitä, että sen kumppanit ja alihankkijat toteuttavat riittävän tietosuojan tason määrittelemällä tietosuojan toteuttamiseen liittyvät tarkat vaatimukset jo palvelun hankintavaiheessa. Kumppaneilta vaaditaan salassapitosopimukset ja tarvittaessa vaitiolosopimukset. Havaittuaan tietosuojaloukkauksen, rekisterinpitäjä ilmoittaa siitä rekisteröidylle ja valvontaviranomaiselle 72 tunnin sisällä. (VAHTI 2016, 18–30.) Rekisterinpitäjä osoittaa noudattavansa henkilötietolakia erilaisin määrittelyin, dokumentein ja ohjein (Tietosuojavaltuutetun toimisto, n.d.).

3 PILVIPALVELUT

3.1 Pilvipalvelun määritelmä

Pilvipalvelulla tarkoitetaan palvelumallia, jossa jaetusta tietoteknisestä resurssista tarjotaan helposti ja nopeasti käyttöön otettavia ja joustavasti skaalautuvia tietojenkäsittely-, tallennus- tai tietoliikennepalveluita verkon yli. Asiakas voi säätää käytössään olevien resurssien ominaisuuksia tarpeidensa mukaan itse. Palveluiden käyttö on mahdollista ajasta, paikasta ja laitteesta riippumatta. Asiakkaalla ei välttämättä ole tietoa palvelun tarkasta fyysisestä sijainnista, mutta asiakkaalla voi olla mahdollisuus määritellä missä maassa tai datakeskuksessa data sijaitsee. Pilvipalveluiden resurssien käyttöä optimoidaan automaattisesti palveluiden käyttöasteen perusteella. Asiakkaalla on mahdollista seurata, hallita ja raportoida resurssien käyttöä. (NIST 2011, 2.)

Tavanomaisia palvelumalleja ovat Software as a Service (SaaS), eli ohjelmistoresurssi-palvelumalli, Platform as a Service (PaaS) eli alustaresurssipalvelu ja Infrastucture as a Service (IaaS) eli infrastruktuuriresurssipalvelu. Mallit eroavat siinä, miten paljon asiakkaalla on velvollisuuksia loppukäyttäjille suunnatun palvelun tuottamisessa ja toisaalta mahdollisuuksia vaikuttaa palvelun toiminnallisiin ominaisuuksiin (kuva 3). (Viestintävirasto 2014, 5.)



Kuva 3. Palvelu- ja hankintamallit (Viestintävirasto, 2014, 6)

Yksityisessä pilvipalvelussa infrastruktuuri, jolla palvelut tuotetaan, rajataan vain yhden organisaation käyttöön. Palvelun infrastruktuuri voi sijaita organisaation omassa datakeskuksessa tai palvelun tuottajan datakeskuksessa ja ylläpito voi tapahtua organisaation tai ulkopuolisen toimijan toimesta. Yhteisöpilvipalvelussa palvelu tuotetaan määriteltyjen organisaatioiden jakamalla palvelualustalla. Palvelun omistajana voi olla yksi tai useampi organisaatio ja palvelun infrastruktuuri voi sijaita yhden alustaa jakavan organisaation tai palveluntuottajan datakeskuksessa. Julkinen pilvipalvelu tuotetaan jaetulla palvelinalustalla ja data sijaitsee palveluntuottajan datakeskuksessa. Palvelun käyttäjäjoukkoa ei ole rajattu. Hybridimallissa pilvi-infrastruktuuri voi olla yhdistelmä erilaisia hankintamalleja, jotka toimivat standardirajapintojen avulla yhdessä. (NIST 2011, 3.)

3.2 **Identiteetin- ja pääsynhallinta pilvipalveluna**

Pilvipalveluissa toteutetuista identiteetin- ja pääsynhallinnan palvelusta käytetään termejä IDaaS, IAMaaS ja Cloud IAM. Cloud IAM on esimerkiksi Googlen käyttämä tuotenimi pilvessä toteutetulle identiteetin- ja pääsynhallinnan tuotteelle. Kaikilla termeillä tarkoitetaan pilvipalvelumallin mukaisesti toteutettua identiteetin- ja pääsynhallinnan ratkaisua. (Auth0 Inc, 2017; Centrify, n.d.; Fujitsu, 2017; Gartner, n.d.; Google, n.d.; IWelcome, n.d.; Okta, n.d.; Seacat Anna, 2016.)

IDaaS-palveluiden kehitys on lähtenyt tarpeesta helpottaa ja ketteröittää pilvipalveluiden identiteetin- ja pääsynhallintaa. Pääsynhallintaa on helpotettu tarjoamalla kertakirjautuminen SaaS-palveluihin. Perinteiset, organisaation omassa ympäristössä toteutetut identiteetin- ja pääsynhallinnan järjestelmät voivat olla monimutkaisia kokonaisuuksia. Niiden ylläpito vaatii teknistä erikoisosaamista, jota erityisesti pienemmillä organisaatioilla ei aina ole. Pienet ja keskisuuret yritykset tavoittelevat pilviratkaisulla helpotusta identiteetin- ja pääsynhallinnan ja niiden kautta tietoturvan kehittämiseen. (Edwards, 2017; Amazon Web Services, 2018; JumpCloud, n.d.; Seacat Anna, 2016.)

IDaaS-termillä kutsuttavat palvelut sisältävät palveluntuottajasta riippuen erilaisia identiteetin- ja pääsynhallinnan toimintoja. Saatavilla olevat palvelu- ja hankintamallit vaihtelevat toimittajan mukaan. Tyypillisesti IDaaS-palvelut sisältävät vähintään kertakirjautumisen SaaS-palveluihin. Lisäksi tarjolla voi olla muita identiteetin- ja pääsynhallinnan toimintoja, kuten identiteettien provisiointi SaaS-palveluihin, erilaisten käyttöoikeusroolien hallinta ja käyttäjän itsepalvelutoimintoja. Kehittyneemmissä IDaaS-palveluissa voidaan hallita SaaS-palveluiden lisäksi asiakkaan omassa ympäristössä toteutettuja palveluita ja sovelluksia ja niihin voidaan integroida itse kustomoituja sovelluksia. IDaaS-palvelut ja niiden tarjoamat ominaisuudet kehittyvät nopeasti. Palvelut tarjoavat kertakirjautumisen lisäksi muita vastaavia ominaisuuksia, mitä organisaation omassa ympäristössä toteutetut identiteetin- ja pääsynhallinnan ratkaisut. (Edwards, 2017; Amazon Web Services, 2018; JumpCloud, n.d.; Seacat Anna, 2016.)

3.3 Tietosuoja-asetuksen asettamat velvollisuudet pilvipalvelun ylläpitäjälle

Pilvipalvelun toimittaja toimii palvelua tuottaessaan henkilötietojen käsittelijänä asiakkaan lukuun. Toimittajaa koskee EU:n tietosuoja-asetuksen henkilötietojen käsittelijää koskeva sääntely. (Tietosuojavaltuutetun toimisto, Henkilötietojen käsittelijän velvollisuudet, n.d.) Henkilötietojen käsittelyä on esimerkiksi tietojen kerääminen, säilyttäminen, käyttö, siirtäminen ja luovuttaminen.

Henkilötietojen käsittelystä sovitaan rekisterinpitäjän ja käsittelijän välisellä sopimuksella. Sopimuksessa määritellään osapuolten vastuut, velvollisuudet ja oikeudet henkilötietojen käsittelyssä. Palvelun loputtua käsittelijän on tuhottava tai palautettava kaikki sen hallussa olevat tiedot rekisterinpitäjälle ja tuhottava tietojen jäljennökset, ellei siihen ole lakisääteistä estettä. Henkilötietojen käsittelijöiden alaisuudessa toimivien henkilöiden on oltava salassapitovelvollisuuden alaisia. Henkilötietojen käsittelijä tarvitsee rekisterinpitäjältä kirjallisen luvan käyttääkseen alihankkijaa käsittelyssä. Henkilötietojen käsittelijän on varmistuttava sopimuksin, että alihankkija noudattaa samoja velvoitteita, kuin käsittelijä. Alkuperäinen käsittelijä vastaa siitä, että alihankkijatkin noudattavat tietosuoja-asetusta. (Tietosuojavaltuutetun toimisto, Henkilötietojen käsittelijän velvollisuudet, n.d.)

Henkilötietojen käsittelijä auttaa mahdollisuuksien mukaan rekisterinpitäjää vastaamaan rekisteröidyn esittämiin tarkastuspyyntöihin. Henkilötietojen käsittelijän velvollisuus on ilmoittaa välittömästi rekisterinpitäjälle, jos huomaa rekisterinpitäjän ohjeistaman käytännön rikkovan tietosuojaa koskevia sääntöjä ja havaitsemistaan henkilötietojen tietoturvaloukkauksista. (Tietosuojavaltuutetun toimisto, Henkilötietojen käsittelijän velvollisuudet, n.d.)

Käytettävät työkalut, sovellukset tai palvelut mahdollistavat sen, että käsittely rajoittuu vain tarkoituksen kannalta tarpeellisiin henkilötietoihin ja tekniset ratkaisut eivät pakota tallentamaan tarpeettomia tietoja. Käsittelijä sallii rekisterinpitäjän valitseman auditoijan suorittaman auditoinnin ja osallistuu auditointiin. (Tietosuojavaltuutetun toimisto, Henkilötietojen käsittelijän velvollisuudet, n.d.)

4 IDENTITEETIN- JA PÄÄSYNHALLINTA PILVIPALVELUSSA CASE ORACLE

Oracle Identity Cloud Service on PaaS-mallin mukaisesti toimiva identiteetin- ja pääsynhallinnan palvelu. Palvelu toimii pilviperiaatteiden mukaisesti skaalautuen ja mukautuen ketterästi organisaation tarpeisiin ja olemassa olevaan tekniseen ympäristöön. (Oracle, 2016)

4.1 **Ominaisuudet**

Oracle Identity Cloud -palvelun keskeiset ominaisuudet ovat keskitetty identiteetinhallinta, pääsynhallinta ja kertakirjautuminen, sovellusten hallinta, palvelun laajentamista tukevat avoimet ja standardeihin perustuvat rajapinnat sekä pilvipalvelun toimintaperiaatteita tukeva mikropalveluarkkitehtuuri. (Oracle, 2016)

Identiteetinhallinta voidaan tehdä www-portaalin tai REST-rajapinnan kautta. Hybridi-ratkaisussa identiteetit tuodaan ja niiden tiedot synkronoidaan palveluun organisaation omasta käyttäjähakemistosta. Palvelussa voidaan toteuttaa myös käyttäjän itsepalvelutoimintoja, jotka mahdollistavat tunnuksen rekisteröinnin ja salasanan uusimisen itsepalveluna. (Oracle, 2016)

Oracle Identity Cloud -palvelussa voidaan hallinnoida valmiiksi integroituja, eri pilvipalvelutoimittajien toteuttamia sovelluksia ja palveluita. Asiakas voi integroida palveluun omia sovelluksiaan. Palveluun voidaan integroida mobiili-, web- ja työpöytäsovelluksia. (Oracle, 2018a osa 3, Luku 6)

Käyttäjätunnuksia voidaan provisioida ja synkronoida Oracle Identity Cloudissa hallittuihin sovelluksiin (Oracle, 2018a osa 3, Luku 6). Integroiduissa sovelluksissa voidaan ottaa käyttöön federoitu identiteetin- ja pääsynhallinta sekä kertakirjautuminen käyttäen avoimia standardeja OpenID Connect 2.0, OAuth 2.0 ja SAML 2.0. Kertakirjautuminen on mahdollista pilvipalvelussa ja organisaation omassa ympäristössä toteutettuun sovellukseen. (Oracle, 2016)

Identity Cloud -palvelussa hallittujen sovellusten kirjautumiskäytännöissä voidaan sovelluskohtaisesti asettaa vaatimukseksi vahva tunnistautuminen. Vahvan tunnistautumisen vaatimus voidaan asettaa kaikille sovellusta käyttäville käyttäjille kaikissa tilanteissa tai tiettyjen ehtojen toteutuessa. Vahva tunnistautuminen voidaan vaatia esimerkiksi silloin, kun kirjautujalla on järjestelmänvalvojan oikeudet palveluun tai kirjautuminen tapahtuu organisaation oman verkon ulkopuolelta. Käytettävissä olevia todentamistapoja on mobiilitunnistussovellus, tekstiviestinä tai sähköpostilla lähetetty kertakäyttöinen salasana, etukäteen asetetut turvakysymykset tai etukäteen käyttäjän generoima kertakäyttöinen, rajatun ajan voimassa oleva ohituskoodi. Ohituskoodin voi generoida myös järjestelmänvalvoja. (Oracle, 2018a. Osa 5, Luku 24.) Oracle Identity Cloud -palveluun integroituihin sovelluksiin voidaan myöntää pääsy ja käyttövaltuuksia joko käyttäjä- tai ryhmäkohtaisesti (Oracle, 2018a, Osa 3, Luku 6).

Järjestelmänvalvojan roolissa oleva henkilö voi nähdä raportteja, joissa on tietoja käyttäjistä, sovelluksista tai palvelun toiminnasta. Käyttäjistä raportoidaan epäonnistuneet ja onnistuneet kirjautumiset. Sovelluksista

voidaan raportoida käyttäjämääriä ja käyttövaltuuspäätöksiä. Tapahtumat voidaan myös hakea keskitettyyn lokijärjestelmään REST-rajapintojen kautta. Raportteja säilytetään 90 päivää. (Oracle, 2018a, Osa 3, Luku 8.)

Euroopan datakeskukset, joilla Oraclen pilvipalvelut tuotetaan sijaitsevat Iso-Britanniassa, Hollannissa ja Saksassa. Identity Cloud -palvelu on mahdollista sijoittaa Iso-Britannian, Hollannin tai Cloud at Customer -toteutuksessa asiakkaan omaan datakeskukseen. Asiakas määrittelee millä maantieteellisillä alueilla palvelu toteutetaan. (Oracle, n.d.)

4.2 **Toimitusehdot**

Oraclen pilvipalvelut tuotetaan Oraclen hallinnoimassa datakeskuksissa tai palvelu voidaan tuottaa asiakkaan datakeskuksessa. Cloud at Customer -toteutuksessa Oracle toimittaa operointiin tarvitsemansa tietotekniset laitteet asiakkaan datakeskukseen. Asiakkaan velvollisuus on toteuttaa riittävät konesalipuitteet Oraclen tekniikan asentamiseksi ja verkkoyhteyden turvaamiseksi. Oracle vastaa vain omien teknisten laitteidensa ylläpidosta asiakkaan konesalissa. (Oracle 2017a, 3.)

Oracle voi siirtää dataa eri datakeskukseen saman maantieteellisen alueen sisällä tietojen palautuksen yhteydessä. Datakeskusten migraatiosta, joka tapahtuu muusta syystä, kuin datan palauttamiseksi tiedotetaan 30 päivää ennen toimenpidettä. (Oracle 2017a, 10.)

Asiakkaan tulee päivittää Oraclen pilvipalvelusovellukset siten, että käytössä on aina uusin sovellusversio. Oracle ei vastaa pilvipalvelussa esiintyvistä ongelmista, jotka johtuvat sovellusten vanhentuneesta versiosta. Versiopäivitys tulee tehdä ennen, kuin tuki aiemmalle versiolle päättyy. Jos asiakas ei päivitä palvelua, Oracle voi tehdä päivityksen automaattisesti tai keskeyttää palvelun käytön. Jos palvelusta ei tule uutta versiota, Oracle nimeää Oracle-palvelun, johon siirtyä. (Oracle 2017a, 10.)

Asiakkaan tekniset yhteyshenkilöt voivat olla yhteydessä Oraclen pilvipalvelun asiakastukeen. Teknisellä yhteyshenkilöllä tulee olla perusymmärrys ja osaaminen Oraclen pilvipalvelusta, käytössä olevasta pilvisovelluksesta ja sen käytöstä. Teknisen yhteyshenkilön pitää kyetä auttamaan Oraclea ongelmien ratkaisussa. Asiakas toimittaa Oraclelle teknisten yhteyshenkilöiden ajantasaiset yhteystiedot. Oraclen tukeen kuuluu ongelmien diagnosointi, raportoitujen ja todennettavissa olevien vikojen korjaaminen ja muutoksen hallinnan tuki. Tekninen tuki on tavoitettavissa ympäri vuorokauden asiakastukiportaalin kautta ja puhelimitse. Ei-tekninen asiakastuki on käytettävissä kello 8–17. (Oracle 2017a, 11.)

Sekä asiakas että Oracle määrittelee tukipyynnölle kriittisyysluokan. Oracle on luokitellut ja kuvannut neljä luokkaa. Kriittisimmän luokan edellytys on, että ongelma estää työskentelyn ja kriittisen palvelun käyttö on

täysin estynyt. Tällaisissa ongelmissa tyypillisesti esimerkiksi data on korruptoitunut, kriittinen toiminnallisuus ei ole käytettävissä, palvelussa on viiveitä ja palvelu jää jumiin toistuvasti. Oracle lupaa reagoida tällaiseen tukipyyntöön 15 minuutin sisällä ja työskentelee 24/7 kunnes ongelma on ratkaistu tai on löytynyt keino kiertää se. Tänä aikana asiakkaan teknisen yhteyshenkilön tulee olla tavoitettavissa. Tikettien kriittisyysluokitusta voidaan muuttaa tilanteen mukaan korkeammaksi tai alemmaksi. (Oracle 2017a, 11-12.)

Palvelun päättymisen jälkeen asiakkaalla on 60 päivää aikaa siirtää datansa pilvipalvelusta. Tämän jälkeen Oraclella ei ole velvollisuutta säilyttää dataa. Jos datan siirrossa tarvitaan apua, asiakas tekee palvelupyynnön Oraclelle. Sopimuksen ja irtisanomisajan kuluttua Oracle poistaa tai rikkoo datan siten, että sitä ei pystytä enää palauttamaan. Cloud at Customer -vaihtoehdossa asiakkaan on luovutettava Oraclen konesaliin tuomat tekniset laitteet takaisin Oraclelle samassa kunnossa kuin asennettaessa. Kohtuullinen, normaalista käytöstä johtuva kuluminen hyväksytään. (Oracle 2017a, 13.)

Jos Oracle huomaa tai saa tietoonsa, että käyttöehtoja ja palveluehtoja on rikottu, Oracle nimeää asiaa selvittämään tutkijan. Tutkija voi jäädyttää käyttäjätilejä tai pääsyn palveluun, kunnes asia on ratkennut. (Oracle 2017a, 14.)

4.3 **Tietoturva**

Oracle Cloud -palveluiden toimintakäytäntö on ISO/IEC 27002 -standardin tietoturvallisuuden hallintakeinojen menettelyohjeiden mukainen. Oraclen henkilöstö mukaan lukien sopimuskumppanit ja määräaikaiset työntekijät sitoutuvat Oraclen tietoturvakäytäntöön. (Oracle 2017a, 3.)

Asiakas vastaa Oraclen pilvipalveluita hyödyntävistä tai pilvipalveluun integroiduista, omassa hallinnassaan olevasta omaisuudesta. Asiakkaan vastuulla on palvelussa käsitellyn aineiston luokittelu ja asiakas määrittelee, voidaanko asiakkaan tietoaineistoja säilyttää ja käsitellä pilvipalvelussa. Asiakas on myös vastuussa tietojen käsittelyn hyväksynnästä ja muista päätöksistä, joita tarvitaan Oraclen pilvipalvelun tuottamiseksi. (Oracle 2017a, 5.)

PaaS-palveluiden osalta asiakas vastaa sovellusten tietoturvaan liittyvistä asetuksista ja tehtävistä. Oracle suojaa palvelun toimittamiseen tarvittavan globaalin infrastruktuurin kuten tekniset laitteet, verkon ja sovellukset, jolla pilvipalvelut tuotetaan. Oracle suojaa sekä toimistot, että datakeskukset. (Oracle 2017b, 7.)

Asiakkaan velvollisuus on toteuttaa oma kattava tietoturvakäytäntö. Asiakas vastaa loppukäyttäjän selaimen vähimmäisvaatimusten toteutumi-

sesta, vähimmäisvaatimukset täyttävän tietoverkkoyhteyden toteutumisesta, päätelaitteen tietoturvan hallinnasta siten, että palveluun ladattavat tiedostot eivät sisällä haitallista dataa ja omassa hallinnassaan olevien käyttäjätilien hallinnasta hyvän tietoturvakäytännön mukaisesti. Lisäksi, jos palvelu on asiakkaan omassa datakeskuksessa, asiakas vastaa riittävästä fyysisestä ja tietoverkon tietoturvasta. (Oracle 2017a, 6.)

Asiakas voi suorittaa omaan ympäristöönsä haavoittuvuustestejä hankkimalla hyväksynnän ja sopimalla aikataulusta etukäteen Oraclelta. Testien tulokset ja johtopäätökset toimitetaan Oraclelle. (Oracle 2017a, 8.)

Datakeskukset on suojattu betonisilla ajoesteillä, videovalvonnalla, hälytysjärjestelmillä ja miehitetyillä vartiointiasemilla. Pääsy datakeskukseen on rajoitettu vain valtuutetuille työntekijöille. Pääsy valtuutetaan vain, jos työtehtävien hoito sitä edellyttää. Kaikki työntekijät ja vierailijat käyttävät näkyvää virallista tunnistetta. Käynnit datakeskuksessa kirjataan lokiin ja auditoidaan säännöllisesti. Avainten ja pääsykorttien hallintaa ja pääsyä valvotaan. Datakeskuksen sisäänkäynneillä on vartija 24 tuntia päivässä ja 365 päivää vuodessa. Vartija suorittaa datakeskuksessa vierailevien tunnistuksen ja huolehtii vierailijoiden seurannasta. Laitteiston fyysinen siirtely on valvottua. Verkkokaapelit on suojattu ja verkkokaapelien asentamista julkisille alueille vältetään. (Oracle 2017a, 4; Oracle 2017b, 8.)

Oraclen alustan suojauskäytäntöön kuuluu pääsyn rajaaminen protokollatasolla, tarpeettomien sovellusten ja palveluiden poistaminen, tarpeettomien käyttäjätunnusten poistaminen, tietoturvapäivitysten hallinta, tapahtumien kirjaaminen lokiin ja hälytykset. (Oracle 2017b, 11.)

Oraclen pilviverkko on erotettu yhtiön omasta verkosta. Verkon suojauksesta huolehditaan suojauslaittein kuten palomuurein. Verkon tietoturvan toteutumisen seurantaan käytetään valvontatyökaluja. Kuormantasauksella, liikenteenvalvonnalla ja laitteistokapasiteetilla suojataan verkkoa palvelunestohyökkäyksiltä ja epäilyttävältä verkkoliikenteeltä. (Oracle 2017b, 9.)

Asiakkaan yhteys pilveen salataan TLS-protokollalla. Salaus on vähintään 128 bittinen ja yksityinen avain on vähintään 2048 bittiä. Oracle suosittelee uusimpia, vahvempaa salausta tukevia selaimia pilvipalveluiden käytössä. Jos kolmannen osapuolen sovellus ei salli salausta, Oracle tarkastaa, hyväksyy salaamatonta yhteyttä käyttävän sovelluksen ja mahdollistaa yhteyden. Pilvipalveluun voidaan ottaa yhteys myös SSH -yhteydellä tai käyttäen IPsec -protokollia käyttävää VPN -yhteyttä. (Oracle 2017b, 10.)

Oraclen hallinnassa olevien palvelukomponenttien osalta Oraclen pääsy asiakkaan dataan on rajoitettu vain valtuutetuille työntekijöille ja pääsy dataan valtuutetaan vain, jos työtehtävien hoito sitä edellyttää. Oraclen

ylläpitoyhteys pilvipalveluun tapahtuu suojatun VPN-tunnelin kautta erillisin käyttäjätunnuksin. Pääsy edellyttää vahvaa tunnistautumista. Kaikki työntekijöiden tekemät operaatiot näppäimistön näppäilyt mukaan lukien kirjoitetaan lokiin auditointia ja väärinkäytösten selvittämistä varten. (Oracle 2017b, 8; Oracle 2017a, 4.)

Asiakkaan data on eroteltu loogisesti tai fyysisesti muiden asiakkaiden ympäristöistä (Oracle 2017a, 4). Pääsynhallintaa PaaS-palveluun hallitaan jaetun identiteetin- ja pääsynhallinnan avulla. Asiakkaan käyttäjät, ryhmät, data ja hankkimat palvelut sekä sovellukset sidotaan asiakaskohtaiseen identiteettitoimialueeseen. Jaetun identiteetinhallinnan avulla hallitaan sitä, ketkä pääsevät kirjautumaan palveluun ja millaisia oikeuksia heillä palvelussa on. Käyttäjä voidaan tunnistaa joko Oraclen pilvessä tai käytössä voi olla federoitu kirjautuminen, jolloin tunnistaminen tehdään organisaation omassa tunnistuspalvelussa. Federoidussa kirjautumisessa hyödynnetään SAML-protokollaa käyttäjän tietojen välittämisessä organisaation omasta käyttäjätietokannasta Oraclen palveluun.
(Oracle 2017b, 14.)

Oracle varmistaa palvelussa olevan asiakkaan datan säännöllisesti. Varmistukset säilytetään samassa sijainnissa, josta palvelua tarjotaan, mutta ne voidaan tallentaa myös vaihtoehtoiseen paikkaan säilyttämistä varten. Varmistuksia säilytetään vähintään 60 päivää. Oracle ei palauta dataa asiakkaan puolesta. Oracle voi kuitenkin auttaa palautuksessa, jos data on hävinnyt asiakkaan toimien seurauksena. Asiakas vastaa sellaisten palveluiden varmistamisesta, joihin asiakas voi määritellä oman käytäntönsä mukaiset varmistukset ja niiden palveluiden varmistamisesta, joita ei ole tuotettu Oraclen toimesta osana pilvipalvelua. (Oracle 2017a, 6–7.)

Palvelun on suunniteltu olevan käytettävissä 24 tuntia vuoden jokaisena päivänä. Palvelussa voi kuitenkin olla suunniteltuja huoltokatkoksia. Suunnitelluista käyttökatkoksista ja katkoksen aikana tehtävistä toimenpiteistä tiedotetaan etukäteen. Katkosten ajoittamisessa huomioidaan palvelun matalan käyttöasteen ajankohdat ja maantieteelliset vaatimukset. Asiakaskohtaisten muutosten aiheuttamista katkoksista sovitaan asiakkaan kanssa. Oraclen tavoittelema pilvipalvelun käytettävyysaika on 99,5%. Palvelun käytettävyys raportoidaan kuukausittain. Raportoidussa palvelun keskeytysajassa ei huomioida suunniteltuja ylläpitotoimien aiheuttamia katkoksia, Oraclesta riippumattomista syistä aiheutuvia katkoksia ja asiakkaan toimista aiheutuvia katkoksia. (Oracle 2017a, 7–10.)

Ennen työntekijän palkkaamista työntekijöille tehdään turvallisuusselvitys. Työntekijät ja alihankkijat allekirjoittavat salassapitosopimuksen ja osallistuvat säännöllisesti tietoturvakoulutuksiin. (Oracle 2017b, 9.)

Kolmannen osapuolen suorittamien auditointien raportit julkaistaan säännöllisesti. Asiakas voi pyytää viimeisintä raporttia Oraclelta palvelun arviointia varten. (Oracle 2017b, 13.)

Oracle valvoo asiakkaan datan käsittelyä sekä omassa, että yhteistyökumppaninsa ympäristössä. Oraclen tietoturvaorganisaatio valvoo ja käsittelee tietoturvauhkia ympäri vuorokauden. Organisaatiolla on dokumentoitu käytäntö tietoturvapoikkeamien käsittelystä ja toimintatavoista. (Oracle 2017b, 11.)

4.4 **Tietosuoja**

Tietosuojan toteutuminen varmistetaan sopimuksella. Oraclen pilvipalveluiden tietosuojan toteuttamisesta sovitaan datankäsittelysopimuksessa.

Rekisterinpitäjänä asiakas vastaa käsittelyn ja tietojen siirron lainmukaisuudesta. Asiakas informoi käyttäjiä henkilötietojen käsittelystä ja vastaa tarvittavien suostumusten ja hyväksyntöjen hankkimisesta. Oracle on henkilötietojen käsittelijä ja Oraclella on velvollisuus noudattaa henkilötietojen käsittelystä säädettyjä lakeja ja asetuksia. Oracle ja sen alihankkijat ja kumppanit käsittelevät henkilötietoja vain tuottaakseen pilvipalvelun palvelusopimuksen mukaisesti ja noudattaen asiakkaan antamia kirjallisia ohjeita. (Oracle 2018b, 2.)

Oracle ei ole velvollinen antamaan lainopillista neuvontaa ja ohjausta asiakkaalle, mutta informoi asiakasta, jos asiakkaan kirjaama henkilötietojen käsittelyohje on ristiriidassa sovellettavan lainsäädännön kanssa. (Oracle 2018b, 3.)

Oraclen keräämät henkilötiedot, voivat vaihdella riippuen mitä palveluita on käytössä. Henkilötiedot voivat sisältää muun muassa henkilön yhteystiedot, salasanan, tietoja perhetilanteesta, työhön ja työsuhteeseen liittyviä tietoja, yksilöiviä tunnisteita henkilön käyttämistä laitteista ja verkkopalveluiden käytöstä kerättyä dataa. (Oracle 2018b, 2.)

Asiakkaalla on pääsy sähköiseen palveluun, jonka tietojen avulla asiakas voi vastata rekisteröityjen esittämiin tietopyyntöihin henkilötietojen käsittelystä. Niiltä osin, kun tiedot eivät sijaitse tässä palvelussa, asiakas voi tehdä palvelupyynnön Oraclelle tai palvelua ylläpitävälle taholle tietojen saamiseksi. Oracle ei vastaa sille tulleisiin henkilötietoihin kohdistuviin pyyntöihin vaan ohjaa kysymykset rekisterinpitäjälle eli asiakkaalle. Oracle auttaa vastaamisessa tuottamalla asiakkaalle pyyntöä vastaavaa informaatiota hallussaan olevasta datasta. (Oracle 2018b, 3–4.)

Palvelun tuottamiseksi Oracle voi käsitellä henkilötietoja maailmanlaajuisesti. Jos henkilötietojen käsittely sisältää tietojen siirtoa Euroopan talousalueelta sen ulkopuolelle maahan, jonka ei ole Euroopan komission päätöksellä todettu tarjoavan riittävää tietosuojaa, siirtoon sovelletaan Euroopan komission hyväksymien mallilausekkeiden mukaisia tai tietosuoja-asetusta noudattavia ja riittävän tietosuojan takaavia sopimuksia. Mallilausekkeita sovellettaessa asiakas toimii tietojensiirrossa tietojen

viejänä, Oracle tietojen tuojana ja kolmannen osapuolen tietojenkäsittelijä alihankkijana. (Oracle 2018b, 4.)

Oracle ylläpitää listaa niistä kumppaneista, jotka voivat käsitellä henkilötietoja avustaessaan pilvipalvelun ylläpidossa. Lista on nähtävissä Oraclen tukisivulla. Muutoksista voi tilata itselleen ilmoituksen. Kun uusi kumppani lisätään listalle, asiakkaalla on 14 päivää aikaa vastustaa kirjallisesti kumppanin osallistumista henkilötietojen käsittelyyn toimittamalla Oraclelle asiallinen perustelu liittyen alihankkijan kykyyn suojata henkilötietoja lakien, asetusten ja sopimuksen edellyttämällä tavalla. Oracle ja asiakas etsivät yhdessä ratkaisua ongelmaan. Yksi mahdollinen ratkaisu on tuottaa pilvipalvelu ilman kyseisen alihankkijan osallistumista ylläpitoon. Jos yhteisymmärrykseen ei päästä kohtuullisessa ajassa, asiakas voi keskeyttää palvelun käytön. Tällainen keskeytys ei vapauta asiakasta maksuvelvoitteista. Maksuvelvoitteet jatkuvat sopimuskauden loppuun. (Oracle 2018b, 6.)

Kumppaneita vaaditaan noudattamaan samaa tietoturvan ja tietosuojan tasoa, kuin mitä Oraclen sopimuksissa määritellään. Asiakas voi pyytää Oraclelta auditointia asian varmistamiseksi. Asiakkaalla on myös oikeus saada kopio sopimuksista, jotka Oracle on tehnyt henkilötietoja käsittelevän kumppanin kanssa. Oraclen vastuulla on varmistaa, että kumppanit ja alihankkijat noudattavat ehtoja ja tietosuoja-asetusta. Kumppaneita ja alihankkijoita sitoo salassapitovelvollisuus. (Oracle 2018b, 6.)

Asiakas voi auditoida Oraclen velvoitteiden noudattamisen kerran vuodessa. Lisäksi tietosuojavaltuutettu voi asiakkaan mandaatilla tehdä auditoinnin useammin. Oracle avustaa auditoinneissa. Auditoinnin suorittajan hyväksyy sekä asiakas että Oracle. Auditoinnista ilmoitetaan Oraclelle kaksi viikkoa etukäteen ja sille toimitetaan yksityiskohtainen auditointisuunnitelma. Jos vastaava auditointi on suoritettu 12 kuukauden sisällä ja Oracle voi vahvistaa, ettei muutoksia ole tapahtunut edellisen auditoinnin jälkeen, ei uutta auditointia tehdä. Auditointi ei saa häiritä kohtuuttomasti Oraclen toimintaa. Jos laki ei kiellä, auditointiraportit toimitetaan Oraclelle. Raportit ovat luottamuksellista materiaalia. Asiakas kustantaa auditoinnit itse ja maksaa Oraclelta auditoinnin avustamista varten tarvitut ylimääräiset resurssit. (Oracle 2018b, 7.)

Oracle arvioi ja reagoi välittömästi tapahtumiin, jotka viittaavat luvattomaan pääsyyn henkilötietoihin. Havaitessaan tapahtuman, joka vaarantaa henkilötietojen suojan, Oracle informoi asiakkaalle 24 tunnin kuluessa. (Oracle 2018b, 7.)

Pilvipalvelun päättyessä Oracle palauttaa tai järjestää asiakkaan saataville henkilötiedot, jotka ovat sillä hetkellä saatavissa asiakkaan ympäristöstä. Palvelun irtisanomisajan päätyttyä kaikki henkilötiedot poistetaan palvelusta siten, ettei niitä pystytä palauttamaan. (Oracle 2018b, 8.)

5 HUOMIOITA IDAAS-PALVELUSTA

Oraclen IDaaS-palveluun tutustuttiin esimerkkinä yhtenä pilvipalvelussa toteutetuista IAM-järjestelmästä. Tutustumisen lähtökohdaksi otettiin palveluun liittyvät sopimukset. Lisäksi tutustuin hallintaoppaan kautta palvelun teknisiin ominaisuuksiin.

Oracle on huomioinut tietoturvan ja tietosuoja-asetuksen vaatimukset datankäsittelysopimuksessaan. Palvelu on mahdollista toteuttaa yksityisenä pilvenä asiakkaan omassa datakeskuksessa, jolloin data on mahdollista saada Suomeen ja eriyttää muiden asiakkaiden datasta kokonaan. Datan käsittelijät voivat silti olla EU-alueen ulkopuolella. Identity Cloud -palvelun data voidaan säätää olemaan Alankomaissa. Asiakas voi hallita datan sijaintia.

Oraclen palvelu tukee avoimia rajapintoja jotka mahdollistavat palvelun kustomoinnin ja omien sovellusten integroimisen pilvipalveluun.

Jos asiakkaan mielestä Oraclen uusi kumppani ei pysty toimimaan tietosuoja-asetuksen mukaan, asiasta voidaan neuvotella ja etsiä molempia tyydyttävää ratkaisua. Asiakkaan esittämien hyvien syiden perusteella voidaan sopia, että alihankkija ei osallistu palvelun ylläpitoon. Toinen vaihtoehto on lopettaa palvelun käyttö.

Tämän dokumentin kirjoitushetkellä Oraclen Identity Cloud -palvelun tukemat selaimet ovat Mozilla Firefox, Google Chrome Windows-alustalla ja Safari Mobile. Oraclen vanhoissa toimitusehdoissa vuodelta 2015 huoltoikkuna on noin 10 tuntia kerran kuukaudessa (Oracle, 2015; Darrow, 2016; Hopping 2016). Aikaa ei ole mainittu uusimmassa toimitusehdossa. Tieto on ilmeisesti saatavilla kirjautumisen takaa.

5.1 IDaaS-palveluun liittyviä riskejä

Pilvipalvelun maantieteellinen sijainti pitää ottaa huomioon suunnittelussa. Suomen kansainväliset verkkoyhteydet ovat kehittyneet ja kehittyvät. Ehkä tulevaisuudessa datakeskuksia sijaitsee Suomessa. Jos data ja palvelu ovat ulkomailla, valtionhallinnossa pitää kriittisten toimintojen osalta huomioida vaatimus toiminnan jatkuvuudesta, vaikka tietoliikenneyhteydet ulkomaille on katkenneet.

Monimutkaisen identiteetin- ja pääsynhallintalogiikan ja prosessien siirtäminen palvelusta toiseen on mittava projekti. Riippuen siitä, missä määrin kokonaisuus on siirretty pilveen ja mistä osista se koostuu, riskit kasvavat. Mitä monimutkaisempi hallintalogiikka pilveen on rakennettu, sen hankalampi se on siirtää erityisesti silloin, jos lähde- ja kohdepalvelu tarjoavat vain omia sovelluksiaan järjestelmien integrointiin eikä avoimia rajapintoja tueta.

Organisaatio käyttää omia kustomoituja sovelluksia joille ei löydy valmista integraatiota IDaaS-palveluun. IDaaS-palvelun hyödyllisyys riippuu siitä, onko omien sovellusten integroiminen palveluun mahdollista, miten ja kenen toimesta integraatio on mahdollista rakentaa. Jos palvelu ei tue avoimia rajapintoja, palvelun toimittajan toteuttamiin integraatio-työkalujen ominaisuuksiin tutustumalla varmistetaan, että niiden avulla integraatiot onnistuvat organisaation käyttämiin palveluihin ja sovelluksiin.

Pilvipalvelun tuki voi päättyä palvelusta johtuvista syistä. IAM-palvelun siirtämiseen pitää varata aikaa ja resursseja eikä ajankohta palvelun vaihtamiselle ole välttämättä organisaation päätettävissä.

Palvelun tuki ja osaaminen ovat ulkomailla. Jos palvelun ylläpito ja tuki ovat ulkomailla ja ongelman korjaaminen edellyttää pääsyä asiakkaan dataan tai laitteistoon, omaan ympäristöön asennettu yksityinen pilvipalvelu on yhtä riippuvainen tietoliikenneyhteyksistä ulkomaille, kuin ulkomailla sijaitsevaan datakeskuksessa toteutettu pilvipalvelu.

Organisaatio ei voi vaikuttaa palvelussa esiintyviin katkoksiin. Oraclen tapauksessa Oracle varaa sopimuksessa oikeuden ylläpitotoimien aiheuttamiin katkoksiin. Jos palveluiden ajankohdasta ei voida sopia, organisaatio ei voi vaikuttaa omassa toiminnassaan esiintyviin käyttökatkoihin. Ongelmatilanteissa Oracle edellyttää, että asiakkaan yhteyshenkilö on tavoitettavissa ongelman selvittämisen aikana. Vian selvittämiseksi organisaatiolle jää vastuu osallistua ongelman korjaamiseen, vaikka sillä ei olisi osuutta palvelun teknisessä ylläpidossa. Organisaatiossa tulee olla yhteyshenkilö, jolla on tekninen ymmärrys ja osaaminen palvelun toiminnasta, jotta voi toimia Oraclen apuna ongelmien selvittämisessä.

5.2 **IDaaS-palvelun hyötyjä**

Palvelu päivittyy nopeasti ja organisaation kannalta vaivatta. Organisaation käytössä on tuoreimmat ohjelmistoversiot ilman raskasta päivitysprojektia. Mahdollisista päivittämiseen liittyvistä haasteista vastaa palvelun toimittaja.

Palvelu skaalautuu käytön ja tarpeen mukaan. Skaalautuvuus voi tarkoittaa myös joustavuutta laskutuksessa. Palvelusta voi olla mahdollisuus maksaa aktiivisen käytön mukaan tai käyttäjätunnusten määrän mukaan.

Palvelun laajentaminen esimerkiksi uusilla hallittavilla sovelluksilla on nopeaa ja ketterää. Paluihin on integroitu valmiiksi sovelluksia, joten monet sovellukset ja palvelut voidaan ottaa hallintaan ilman omaa kehitystyötä.

Palvelun jatkuvatoimintaisuus on hoidettu palvelun toimittajan puolesta. Organisaation ei tarvitse huolehtia laitteistosta eikä tiloista.

6 SELVITYSTYÖN TULOKSET

6.1 Mitä tarkoittaa IDaaS ja Cloud IAM?

IDaaS, IAMaaS ja Cloud IAM -käsitteillä tarkoitetaan pilvipalveluperiaatteen mukaan toteutettua identiteetin- ja pääsynhallinnan palvelua. Käsitteet ja niiden sisältö ovat muodostuneet sen perusteella kuka asiasta kirjoittaa ja milloin teksti on kirjoitettu. Palveluiden nopea kehittyminen ja uusien ominaisuuksien tuki laajentavat käsitteen merkitystä jatkuvasti. Palvelun tarjoamat ominaisuudet voivat vaihdella eikä käytettävästä käsitteestä voi päätellä millaiset ominaisuudet palvelussa on toteutettu. Yleisimmin käytetty käsite on IDaaS. Jossain tapauksessa IAMaaS-käsitettä käyttämällä on haluttu korostaa, että palvelu on muutakin kuin kertakirjautuminen SaaS-palveluihin.

6.2 Mitä pitää huomioida pilvipalvelun käyttöönoton suunnittelussa?

VAHTI-ohjeessa käyttövaltuushallintajärjestelmän tärkeimpiä teknisiä vaatimuksia on jatkuvatoimintaisuus, korkeinta luokkaa olevaa sisäinen tietoturva ja skaalautuvuus. Järjestelmän tulee olla sellainen, että toiminta on mahdollista varajärjestelyin pitää käynnissä myös poikkeustilanteissa. (VAHTI 2006, 30.) Tietoturvatasojen toteuttamiseksi IAM-järjestelmältä vaaditaan korkeaa käytettävyyttä ja kykyä tuottaa lokitietoa raportointia ja valvontaa varten.

6.2.1 Tietosuoja, tietoturva ja varautuminen

Rekisterinpitäjän tulee varmistaa riittävän tietosuojan toteutuminen ja jos henkilötietoja siirretään EU- ja ETA-alueen ulkopuolelle pitää siirron mahdollistamiseksi huomioida tietosuoja-asetuksen erityisvaatimukset. Tietojen siirto pilvipalveluun on mahdollista, jos data siirretään alueelle, jonka EU:n komissio on päätöksellä todennut toteuttavan riittävän tietosuojan. Riittävä tietosuojan toteutuminen voidaan varmistaa myös EU:n mallilausekkeiden ja tietosuoja-asetuksen mukaisilla sopimuksilla. Tietosuojan toteutuminen varmistetaan auditoimalla palvelu.

IDaaS-palvelun toimittaja ja ylläpitäjät toimivat henkilötietojen käsittelijänä rekisterinpitäjänä toimivan organisaation lukuun, kun heillä on pääsy palvelussa oleviin henkilötietoihin. Rekisterinpitäjän on varmistettava, että palvelua tuotettaessa ja ylläpidettäessä noudatetaan EU:n tietosuoja-asetuksen ja henkilötietolain määräyksiä.

Palvelun osalta pitää olla tiedossa missä data sijaitsee ja kuka sitä käsittelee. Pilvipalvelun ylläpitäjät voivat toimia henkilötietojen käsittelijänä maailmanlaajuisesti. Henkilötietojen käsittelystä on sovittava kirjallisella sopimuksella palvelun toimittajan kanssa. Sopimuksella huolehditaan tietosuoja-asetuksen mukaisesti vastuista ja velvollisuuksista tietosuojan

turvaamiseksi. Tietosuoja-asetuksen noudattaminen pitää varmistaa myös pilvipalvelun ylläpitoon osallistuvien alihankkijoiden osalta, vaikka palvelun toimittaja vastaakin alihankkijoidensa osalta tietosuojan toteutumisesta. Vaikka palvelu päätetään sijoittaa yksityisenä pilvipalveluna organisaation omaan ympäristöön, saattaa henkilötietojen käsittely tapahtua silti maailmanlaajuisesti.

Organisaation IAM-palvelulle määrittelemä tietoturva- ja varautumistason on toteuduttava pilvipalvelussa. Jos pääsynhallintaan kytkettävä sovellus tai palvelu luokitellaan korotetulle tietoturvatasolle, tulee myös muut siihen liittyvien teknisten ratkaisujen toteuttaa korotetulla tasolla.

Pilvipalvelun hankintamalli vaikuttaa organisaation mahdollisuuteen vaikuttaa palvelun tietoturvaan. Jos palvelu asennetaan yksityisenä pilvipalveluna asiakkaan omaan ympäristöön, vastaa asiakas ympäristön fyysisestä tietoturvasta. Muissa hankintamalleissa pitää tutustua palvelun toimittajan tuottamaan dokumentaatioon tietoturvan toteuttamisesta ja luotettavan tahon suorittamiin tietoturvan auditointiraportteihin. Lisäksi voidaan vaatia mahdollisuutta oman auditoinnin teettämiseen.

Jos pääsynhallinta eri järjestelmiin ei toimi, koko organisaation toiminta voi lamaantua. Tietoturvan kannalta on tärkeää, että käyttövaltuudet pääsynhallinnassa ovat ajan tasalla. Käyttövaltuuksien päivittämisessä esiintyvät katkokset ja ongelmat aiheuttavat riskin, että palvelut tai tieto ei ole käyttäjän saatavilla oikealla hetkellä ja toisaalta että ne ovat virheellisesti saatavilla väärille henkilöille.

Pilvipalveluiden toimintaperiaate on olla käytettävissä jatkuvasti. Jos palvelussa voi kuitenkin olla suunniteltuja huoltokatkoksia, selvitetään miten pitkiä huoltokatkokset voivat olla ja miten suunniteltujen huoltokatkosten ajankohdista sovitaan ja tiedotetaan asiakkaalle. Lisäksi selvitetään, onko asiakkaalla mahdollisuus vaikuttaa katkoksen ajankohtaan. Palveluiden ylläpitoaikataulu on tärkeä myös ohjelmistojen ajantasaisuuden ja sitä kautta tietoturvallisuuden ylläpidon kannalta.

Huomioitava on myös pilvipalvelun tekninen tuki ja tuen vasteajat. Vasteaikojen tulee toteuttaa varautumisen tason vaatimukset. Palveluun liittyvää osaamista tulee löytyä Suomesta (VAHTI 2010, 42).

Tietoturvaan ja käytettävyyteen vaikuttavat myös tietoverkkoyhteyksien luotettavuus. Verkkoyhteyksien luotettavuus varmistetaan riittävillä varayhteyksillä ja yhteyksien salaamisella. ICT-varautumisen vaatimukset -ohjeessa yhteiskunnalle kriittisten korotetun varautumisen tason järjestelmien toiminnan tulee jatkua myös silloin, kun tietoliikenneyhteydet ulkomaille on lamaantuneet (VAHTI 2012a, 22).

Palvelun käyttöönoton suunnitellussa organisaation on arvioitava omat tarpeensa palvelulta vaadittavien ominaisuuksien suhteen ja vaatimuksensa datan sijainnin suhteen. Pilvipalvelussa data sijaitsee useimmiten ulkomailla, ellei palvelun tuottaja mahdollista yksityisen pilven toteuttamista organisaation omassa ympäristössä. Sijainti vaikuttaa verkkoyhteyksien tietoturvaan ja palvelun varautumiseen sekä tietosuoja-asetuksen noudattamiseen vaadittaviin toimenpiteisiin.

6.2.2 Palvelun käyttöehdot ja ominaisuudet

Palvelua hankittaessa otetaan huomioon, kuka datan omistaa, miten organisaatio saa datan haltuunsa ja miten data ja toiminnallisuudet saadaan siirrettyä toiseen palveluun. Myös lokeista varmistetaan ja sovitaan niiden omistajuus ja sälytysaika. Organisaation pitää tietää kenellä on oikeus käsitellä lokeja ja miten lokien muuttaminen estetään ja miten lokien käsittelyä valvotaan.

IAM-järjestelmä voi olla helposti kompleksinen kokonaisuus, jota organisaatiossa on kehitetty pitkään. Omassa ympäristössä toteutettu IAM-järjestelmän uudistaminen tai kaikkien toiminnallisuuden siirto järjestelmästä toiseen on mittava projekti. Pilvipalvelun sopimuksen päätyttyä asiakkaalla voi olla suhteellisen lyhyt aika saada datansa pilvestä ja siirtää toiminta uudelle alustalle. Pilvipalveluiden toimintamallin mukaisesti pilvessä toteutetun IAM-palvelun käyttöönoton pitäisi olla ketterää ja nopeaa. Tästä on hyvä varmistua ja varautua siihen, että palvelu voidaan joutua siirtämään nopealla aikataululla eri syistä. Käyttöönotossa voidaan miettiä, onko IAM-kokonaisuudessa osia, joiden siirtäminen on helpompaa ja riskittömämpää ja saavutetaanko sellaisten toimintojen käyttöönottamisella kuitenkin organisaation tavoittelemia hyötyjä.

Eri palveluiden tukemat tekniset ominaisuudet vaihtelevat. Tärkeimmät palvelulta vaaditut ominaisuudet ovat tunnistaminen ja kertakirjautuminen sekä SaaS- että paikallisesti hallittuihin sovelluksiin ja palveluihin, tietojen synkronointi ja provisiointi SaaS- palveluihin ja paikallisesti toteutettuihin sovelluksiin, avoimet rajapinnat sovellusten ja palveluiden integroimiseksi palveluun, yleisesti federoidussa pääsynhallinnassa käytettävien protokollien tuki, mahdollisuus ottaa käyttöön vahva tunnistaminen ja määritellä sovellus-, käyttäjä- ja verkkoaluekohtaisesti missä tilanteissa vahvaa tunnistamista vaaditaan, pääsyvaltuuksien hallinnan automatisointi politiikan mukaisilla säännöillä, mahdollisuus kohdentaa sääntöjä käyttäjä, ryhmä tai rooli-kohtaisesti.

Identiteetinhallintaa varten palvelu pitää pystyä integroimaan lähderekisteriin, kuten henkilöstöhallinnon järjestelmään ja hallinnan automatisointiin pitäisi olla mahdollista tehdä hallintasääntöjä. Hallintasääntöjen avulla tulee tunnuksen syntyä, passivoitua ja poistua organisaation sekä tietojen päivittyä hallintapolitiikan mukaan.

Järjestelmän tulee tuottaa kohdassa 2.5.1 mainitut lokit ja ne pitää saada keskitettyyn järjestelmään säilytystä, valvontaa ja raportointia varten. Käyttövaltuuksien hallintajärjestelmästä pitää saada raportti sen kautta hallituista sovelluksista ja palveluista sekä niihin liittyvistä käyttövaltuuksista.

Palvelun tuottajalla on lista kumppaneista, joilta organisaatio voi saada apua ja kehitystyötä integraatioiden tekemiseen sekä tarvittaessa palvelun ylläpitoapua. Valtion organisaation näkökulmasta pitää tukea ja asiantuntemusta löytyä myös Suomesta.

IDaaS-palveluita on saatavilla eri hankintamalleilla toteutettuina. Sama toimittaja voi tarjota mahdollisuutta eri hankintamalleihin. Palvelu voidaan ottaa käyttöön toimittajasta riippuen julkisesta pilvestä, yksityisenä pilvipalveluna tai hybridi-ratkaisuna, jossa omassa ympäristössä oleva käyttäjähakemisto integroidaan pilvipalveluun ja jolloin identiteetinhallinta tehdään omassa ympäristössä. Eri toimittajat voivat tarjota palveluita SaaS tai PaaS-malleilla.

7 YHTEENVETO

Työn tavoitteena oli tutustua pilvipalveluna toteutetun IAM-järjestelmän käsitteisiin ja ominaisuuksiin. Lisäksi tavoite oli selvittää mitä asioita on huomioitava pilvipalveluna toteutetun IAM-järjestelmän käyttöönotossa erityisesti valtion viranomaisen näkökulmasta.

IDaaS-käsitteen määrittelyn tutkimuksissa valtaosa lähdemateriaaleista oli palvelun toimittajien kaupallista materiaalia. Se vaikutti merkittävästi yhtenäisen määrittelyn puuttumiseen. Palveluiden tarjoajat määrittävät käsitteen sen mukaan, mitkä ominaisuudet heidän tuotteensa pystyy toteuttamaan. Lisäksi nopea palveluiden kehittyminen laajentaa käsitteen määrittelyä jatkuvasti. Toiset palvelut tarjoavat edelleen vain kertakirjautumista SaaS-palveluihin, kun toisissa palveluissa on monipuoliset mahdollisuudet identiteetin- ja pääsynhallintaan myös omassa ympäristössä toteutettuihin palveluihin ja sovelluksiin. Yleisesti voidaan kuitenkin puhua IDaaS-palvelusta, kun tarkoitetaan kertakirjautumista vähintään SaaS-sovelluksiin ja SaaS-sovellusten identiteetin- ja pääsynhallintaa.

VAHTI-ohjeista etsin tietoa siitä, millaisia erityisvaatimuksia valtion viranomaista koskettaa IAM-palvelua tuotettaessa ja hankittaessa. Identiteetin- ja pääsynhallintaan liittyviä vaatimuksia on useassa eri ohjeessa, koska pääsynhallinta sisältyy tietoturvan toteuttamiseen. Suunnittelin löytäväni yksityiskohtaiset tekniset vaatimukset IAM-järjestelmälle. Lopputuloksena avarsin omaa ymmärrystäni tietoturvan toteutumisesta. Tietoturvan toteuttamisessa hallinnolliset toimet ja tietoturvan omaksuminen osaksi organisaation toimintaa on keskeisessä asemassa. Jatkuvasti kehittyvät tekniset välineet tukevat organisaatiota tietoturvan toteuttamisessa.

Selvitystyön aikana opin valtionhallinnon asiakirjojen luokittelusta ja luokitteluun liittyvistä tietoturvavaatimuksista. Lisäksi opin, että tietosuoja-asetus ei aseta esteitä henkilötietojen käsittelylle ja siirtämiselle pilvipalveluun vaan asetuksen vaatimuksia noudattamalla pilvipalvelun käyttöönotto on mahdollista siten, että organisaatio voi turvata rekisteröidyn tietosuojan toteutumisen.

Organisaation on selvitettävä, voidaanko varautumisen vaatimukset huomioiden IAM-palvelu toteuttaa Suomen rajojen ulkopuolella vai pitääkö käytettävä palvelun toimittajat rajata niihin, joilta voidaan hankkia palvelu yksityisenä pilvenä organisaation omassa ympäristössä. Palvelun hyödyllisyyden ja laajennettavuuden kannalta oleellista on myös avointen rajapintojen tuki. Kun organisaatiolla on olemassa oleva IAM-järjestelmä, oma ehdotukseni on, että pilvipalvelun tarjoamia hyötyjä haetaan hybridi-ratkaisulla. Hybridi-ratkaisulla IAM-järjestelmän siirto pilvipalveluun voidaan jakaa pienempiin kokonaisuuksiin ja siten voidaan vähentää riskejä ja työmäärää, jota koko kokonaisuuden siirtäminen kerralla sisältäisi.

LÄHTEET

Amazon Web Services (2018). Haettu 1.8.2018 osoitteesta https://aws.amazon.com/mp/scenarios/security/idaas/

Auth0 Inc (n.d.). Cloud Identity and Access Management(IAM). Haettu 31.7.2018 osoitteesta https://auth0.com/learn/cloud-identity-access-management/

Centrify (n.d.). Identity-as-a-Service (IDaaS) for Cloud and Mobile App Single Sign-on and Security. Haettu 31.7.2018 osoitteesta https://www.centrify.com/solutions/cloud/identity-as-a-service-idaas/

Citrix (2017). SAML Authentication. Haettu 6.8. osoitteesta https://docs.citrix.com/en-us/netscaler/12/aaa-tm/saml-authentication.html

Darrow B. (2016). Sorry, Your Cloud May Be Out for the Next 10 Hours. Haettu 11.8.2018 osoitteesta http://fortune.com/2016/06/24/oracle-cloud-offline-for-10-hours/

Eduskunta (2018). EU:n yleisen tietosuoja-asetuksen (GDPR) täytäntöönpano - Uusi tietosuojalaki. Haettu 11.7.2018 osoitteesta https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/EUn-tietosuojauudistus/Sivut/EUn-yleinen-tietosuoja-asetus.aspx

Edwards, J. (2017). Seven IDaaS Vendors to Watch in 2018*. Identity Management Solutions Review.* Haettu 20.5.2018 osoitteesta https://solutionsreview.com/identity-management/idaas-vendors-to-watch-2018/

Fujitsu (2017). Fujitsun IDaaS-palvelu hallitsee identiteetit reaaliaikaisesti. Haettu 18.7.2018 osoitteesta http://www.fujitsu.com/fi/about/resources/news/press-releases/2017/idaas.html

Gartner (n.d.). IT Glossary, IAM as a Service (IAMaaS). Haettu 18.7.2018 osoitteesta https://www.gartner.com/it-glossary/iam-as-a-service-iamaas

Google (n.d.), Cloud identity & access management. Hattu 31.7.2018 osoitteesta https://cloud.google.com/iam/

HE 9/2018 vp. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Haettu 20.5.2018 osoitteesta https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_9+2018.aspx

Linden, M. (2015). Identiteetin- ja pääsynhallinta. Tampereen teknillinen yliopisto. Tietotekniikan laitos. Raportti 6. Haettu 17.4.2018 osoitteesta https://tutcris.tut.fi/portal/files/3087873/linden_identiteetin_ja_paasynhallinta.pdf

Henkilötietolaki 523/1999. Haettu 17.4.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Hopping C. (2016), Oracle's policies document gives notice of 10-hour outages, haettu 11.8.2018 osoitteesta http://www.cloudpro.co.uk/cloud-essentials/public-cloud/6107/oracles-policies-document-gives-notice-of-10-hour-outages

IWelcome (n.d.). The IDaaS platform for the enterprise. Haettu 31.7.2018 osoitteesta https://www.iwelcome.com/identity-management#all

JumpCloud (n.d.). Haettu 19.7.2018 osoitteesta https://jumpcloud.com/blog/identity-service-saas-identity-provider/

Laki viranomaisen toiminnan julkisuudesta. Julkisuuslaki 612/1999. Haettu 17.4.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Oikeusministeriö (2018). Tietosuojalaki täydentäisi EU:n tietosuoja-asetusta. Haettu 20.5.2018 osoitteesta http://valtioneuvosto.fi/artikkeli/-/asset_publisher/1410853/tietosuojalaki-taydentaisi-eu-n-tietosuoja-asetusta

Okta. (n.d.). What is IDaaS? Understanding Identity as a Service and Its Applications. Haettu 31.7.2018 https://www.okta.com/identity-101/idaas/

Oracle (2018a). Administering Oracle Identity Cloud Service, versio 18.2.4, Haettu 23.5.2018 osoitteesta https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/administering-oracle-identity-cloud-service.pdf

Oracle (2018b). Data Processing Agreement for Oracle Cloud Services. Haettu 2.5.2018 osoitteesta http://www.oracle.com/us/corporate/contracts/data-processing-agreement-011218-4261005.pdf

Oracle (2017a). Oracle Cloud Hosting and Delivery Policies. Haettu 26.4.2018 osoitteesta http://www.oracle.com/us/corporate/contracts/ocloud-hosting-delivery-policies-3089853.pdf

Oracle (2017b). Oracle Cloud Infrastructure Classic and Platform Cloud Services Security. Haettu 30.4.2018 osoitteesta https://cloud.oracle.com/iaas/whitepapers/Oracle_IP_Services_Security_R4.pdf

Oracle (2016). Oracle Identity Cloud Service. Haettu 13.6.2018 osoitteesta https://www.oracle.com/assets/idcs-datasheet-3097388.pdf

Oracle (2015), Oracle Cloud Enterprise Hosting and Delivery Policies, haettu 11.8.2018 osoitteesta http://www.oracle.com/us/corporate/contracts/cloud-ent-hd-pol-soc-1961313.pdf

Oracle (n.d.). Data Regions for Platform and Infrastucture Services. Haettu 23.5.2018 osoitteesta https://cloud.oracle.com/data-regions#country)

NIST, National Institute of Standards and Technology (2011). The NIST Definition of Cloud Computing. Haettu 17.8.2018 osoitteesta https://doi.org/10.6028/NIST.SP.800-145

Seacat Anna (2016). What Is IDaaS? A CISO Clears Up Confusion Around the Definition of Cloud IAM. haettu 18.7.2018 osoitteesta https://securityintelligence.com/what-is-idaas-a-ciso-clears-up-confusion-around-the-definition-of-cloud-iam/

Tietosuojavaltuutetun toimisto (n.d.). Henkilötietolaki. Haettu 11.7. osoitteesta https://tietosuoja.fi/henkilotietolaki

Tietosuojavaltuutetun toimisto (n.d.). Henkilötietojen käsittelijän velvollisuudet. Haettu 24.7.2018 osoitteesta https://tietosuoja.fi/henkilotietojen-kasittelijan-velvollisuudet

Tietosuojavaltuutetun toimisto (n.d.). Osoita noudattavasi tietosuojasäädöksiä. Haettu 24.7.2018 osoitteesta https://tietosuoja.fi/osoitusvelvollisuus

VAHTI (2006). Käyttövaltuushallinnon periaatteet ja hyvät käytännöt. Vahti-ohje 9/2006. Haettu 17.4.2018 osoitteesta https://www.vahtiohje.fi/c/document_library/get_file?uuid=d48cbc58-d7a4-4757-a0a1-78cd860a3912&groupId=10229

VAHTI (2009). Lokiohje. Vahti-ohje 3/2009. Haettu 17.4.2018 osoitteesta https://www.vahtiohje.fi/c/document_library/get_file?uuid=775179cb-6c54-4dfb-b65d-e925d47c61d2&groupId=10229

VAHTI (2010). Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Vahti-ohje 2/2010. Haettu 17.4.2018 osoit-

teesta https://www.vahtiohje.fi/c/document_library/get_file?uuid=b4a90e50-7307-4004-ac8e-b9103220db6a&groupId=10128&groupId=10229

VAHTI (2012a). ICT-varautumisen vaatimukset. Vahti-ohje 2/2012. Haettu 20.5.2018 osoitteesta https://www.vahtiohje.fi/c/document_library/get_file?uuid=c99a95f5-c150-49b6-aa5c-a90a821da13e&groupId=10229

VAHTI (2012b). Teknisen ympäristön tietoturvataso-ohje. Vahti-ohje 3/2012. Haettu 17.4.2018 osoitteesta https://www.vahtiohje.fi/c/document_library/get_file?uuid=5a273c6e-2935-4bbf-a4c6-f00e0f878db5&groupId=10229

VAHTI (2016). EU-tietosuojan kokonaisuudistus. Vahti-raportti 1/2016. Haettu 10.8.2018 osoitteesta https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Valtioneuvosto (2009). Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä 26.11.2009. Haettu 5.7. osoitteesta https://vm.fi/documents/10623/307681/VAHTI+periaatepäätös+2009/24355a33-4042-42fb-9dba-981e6398ee7a/VAHTI+periaatepäätös+2009.pdf

Valtioneuvosto (n.d). Haettu 11.7.2018 osoitteesta https://valtioneuvosto.fi/paatokset/periaatepaatokset

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. Tietoturva-asetus 1.7.2010/618. Haettu 17.4.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2010/20100681

Kivivasara, S. (n.d.). Tiedonhallintalain valmistelu. Haettu 29.8.2018 osoitteesta https://vm.fi/tiedonhallintalain-valmistelu

Valtiovarainministeriö (n.d.). VAHTI-toiminta. Haettu 21.5.2018 osoitteesta http://vm.fi/vahti

Viestintävirasto (2014). Pilvipalveluiden turvallisuus. Haettu 20.5.2018 osoitteesta https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf