White Paper **01 / 2016**

Eetu Niemi

IAM haltuun ymmärtämällä kokonaisuus

COALA

Hyvin toimiva käyttäjä- ja pääsynhallinta (Identity and Access Management, IAM) on välttämätön tietoturvan ja digitalisaation kannalta. Käyttöoikeuksien tulee olla asianmukaiset ja tietoturva ei saa vaarantua, vaikka organisaation tietojärjestelmillä olisi paljon erilaisia käyttäjiä (joista kaikki eivät välttämättä ole edes työntekijöitä tai asiakkaita) ja käyttäjien muutostahti kova (mm. työtehtävien muutokset ja poistuvat henkilöt).

Toisaalta prosessien digitalisoinnista ei tule mitään, jos käytettävien tietojärjestelmien kirjautumistavat ja käyttöoikeushallinnat ovat hyvin kirjavia - käyttäjää esimerkiksi kiusataan useilla muistettavilla käyttäjätunnuksilla ja salasanoilla, toistuvilla uudelleenkirjautumisilla sekä käyttöoikeuksilla, joiden tilaaminen ja muuttaminen on hankalaa.

Nämä haasteet voidaan ratkaista oikein suunnitellulla IAM:lla. IAM on kuitenkin laaja ja monimutkainen alue, joten vaadittavien teknisten ratkaisujen saati niiden riippuvuuksien hahmottaminen ei yleensä ole yksikertaista.

Tässä Coalan White Paperissa on kuvattu, miten pääset alkuun IAM-kokonaisuuden suunnittelussa kuvaamalla systemaattisesti IAM:in tavoitteet ja laajuus.

***Coala Oy** on kokonaisarkkitehtuuri-, IT-arkkitehtuuri- sekä prosessikehityskonsultointiin sekä niihin liittyvään koulutukseen ja valmennukseen erikoistunut yritys. Tarjoamme myös IT-projektipalveluita kuten määrittelyä, projektihallintaa ja systeemityön kehittämistä. Olemme työskennelleet sekä toimittajan että asiakkaan puolella, joten tunnemme kehitysprojektit molemmin puolin pöytää, sekä tilaajan että tekijän näkökulmasta. Asiakassuhteissa tähtäämme pitkään kumppanuuteen, sillä kokemuksesta tiedämme, että asiakasymmärrys kertyy vain ajan kuluessa.*

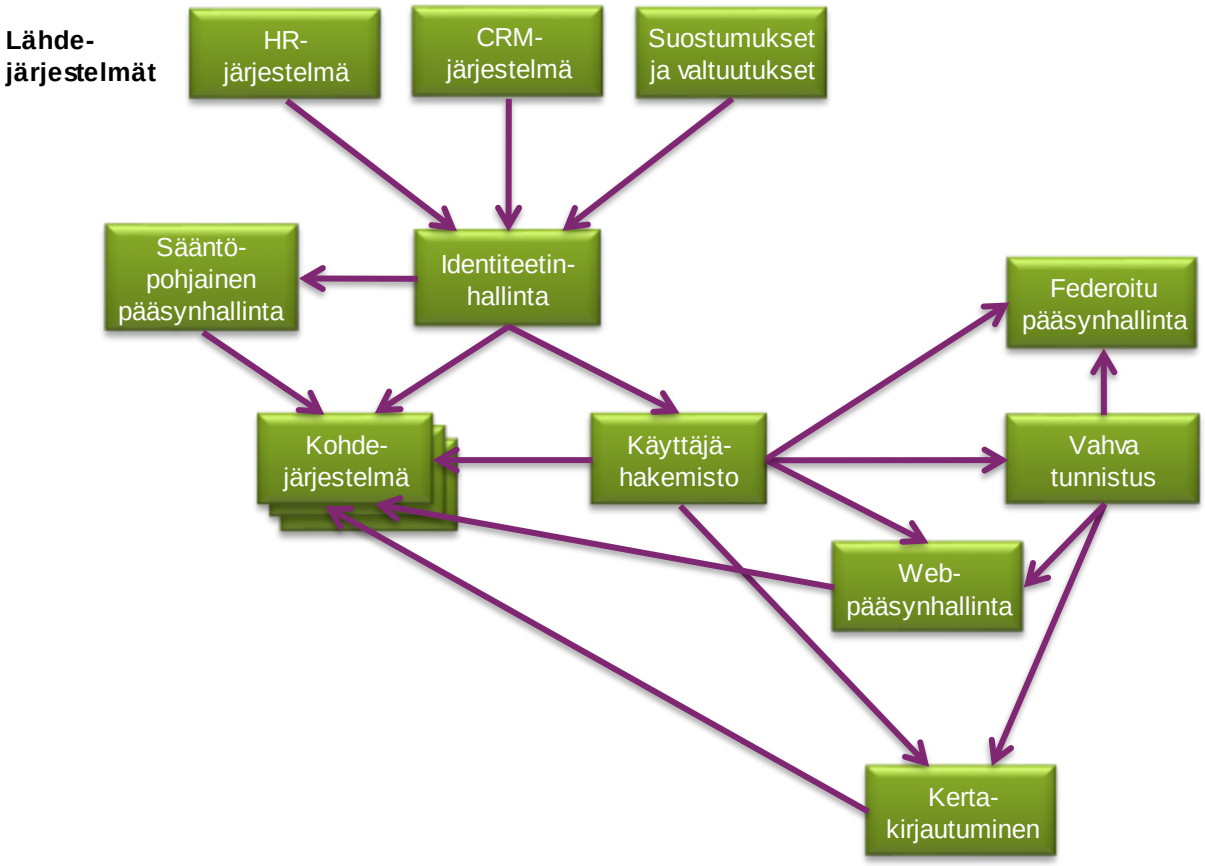
Coala Oy
Pasilanraitio 5
00240 Helsinki

Y-tunnus: 2403281-6

IAM koostuu monesta osasta

IAM:iin kuuluvat seuraavat osat (ks. myös alla oleva kuva):

- Käyttäjien tunnistaminen
- Käyttäjien (identiteettien) hallinta
- Käyttöoikeuksien hallinta
- Kertakirjautuminen (Single Sign-On, SSO)
- Pääsynhallinta (kontrollien asettaminen tietojärjestelmiin siten, että käyttöoikeudet toteutuvat)
- Käyttäjä- ja/tai käyttöoikeustietojen välittäminen (provisiointi) tietojärjestelmiin
- Käyttäjä- ja käyttöoikeustietojen jakaminen (federointi) organisaatioiden kesken



Kohdejärjestelmät ovat niitä tietojärjestelmiä, joiden käyttöoikeuksia halutaan hallinnoida IAM:in kautta. Näihin voi sisältyä myös käyttäjähakemisto (esim. Active Directory). Lähdejärjestelmät taas ovat niitä järjestelmiä, joiden tietoihin IAM:in käyttäjä- ja mahdollisesti myös käyttöoikeustiedot perustuvat.

Luonnollisesti näillä osilla on riippuvuuksia niin keskenään, kuin myös olemassa oleviin tietojärjestelmiin ja prosesseihin. Tarvittavat IAM-komponentit riippuvat ennen kaikkea IAM:ille asetetuista tavoitteista.

Yleensä huomio kiinnittyy IAM-tuotteisiin. Eri toimittajilla on omat tapansa toteuttaa IAM-kokonaisuus. Tuotteet kattavat eri osia IAM-kokonaisuudesta, eivätkä välttämättä toteuta esimerkiksi tässä kuvattuja IAM:in osia yksi yhteen.

Tavoitteiden ja laajuuden määrittely

Kokemuksemme mukaan IAM-ratkaisun käyttöönoton suunnittelu tulee aloittaa tavoitteiden ja laajuuden määrittelyllä. Sen tulee olla ensimmäinen vaihe IAM-käyttöönottoprojektissa tai -hankkeessa (projektin muun sisällön hahmottamiseksi katso Coalan White Paper *Näin onnistut IAM:in käyttöönotossa*).

Tavoitteiden ja laajuuden selkeä linjaaminen on kriittistä koko IAM-hankkeen onnistumiselle. Koko organisaation kattavana asiana IAM vaikuttaa ”kaikkeen” ja vaatii siten laajan hyväksynnän. Jos linjauksia ei alun perin ole tehty, dokumentoitu selkeästi ja niille ei ole avainhenkilöiden tukea, voidaan niistä päätyä kiistelemään jopa vuosien ajaksi. IAM:in aiheuttamat muutokset muun muassa tietojärjestelmiin ja prosesseihin tulee kuvata.

Kattavasta tavoitteiden ja laajuuden määrittelystä saadaan myös suoraan vaatimuksia valittaville IAM-tuotteille – mitä tuotteita tarvitaan ja minkälaiset ominaisuudet niissä tulee olla. Muutoin voidaan päätyä hankkimaan joukko IAM-tuotteita, jotka eivät sovi organisaation tietojärjestelmäympäristöön tai toimi kunnolla yhteen edes toistensa kanssa. Tarpeiden täyttäminen IAM-tuotteita räätälöimällä tulee kalliiksi ja hankaloittaa tulevia ohjelmistopäivityksiä – huolellinen tuotevalinta IAM:in tavoitteet ja laajuus huomioiden on parempi vaihtoehto.

Luonnollisesti tavoitteet ja laajuus toimivat pohjana myös IAM-käyttöönottoprojektin suunnittelulle. Kun ymmärretään muun muassa tarvittavat IAM-komponentit ja integraatiot, voidaan projekti vaiheistaa ja aikatauluttaa asianmukaisesti. Laajojen IAM-toteutusten jako aliprojekteihin helpottuu myös. Myöhemmin käyttöönoton aikana voi tulla ikäviä yllätyksiä ja lisäkustannuksia, jos laajuus ja riippuvuudet eivät ole alusta asti selvillä. Esimerkiksi integraatioiden toteutukseen on varattava resurssit, huomioitava mahdolliset tekniset rajoitukset ja niistä johtuvat kustannukset.

IAM-kokonaisuuden hahmottaminen helpottuu huomattavasti, jos käytettävissä ovat sopivat kokonaisarkkitehtuurikuvaukset. Esimerkiksi sidosryhmäkuvauksia voidaan käyttää IAM:in piiriin tuotavien käyttäjäryhmien suunnittelun pohjana. Prosessikuvauksista voidaan selvittää eri käyttäjäryhmien tarpeita käyttöoikeuksille, erityisesti käyttöoikeusmallien kehittämistä varten. Järjestelmäarkkitehtuurista taas saadaan pohja lähde- ja kohdejärjestelmien valinnalle ja tarvittavien tietovirtojen suunnittelulle. Luonnollisesti IAM-käyttöönoton jälkeen kokonaisarkkitehtuurikuvauksiin on tehtävä tarvittavat päivitykset.

Määriteltävät asiat

Seuraavassa on kuvattu tärkeimmät asiat, jotka tulee olla kuvattuina, ennen kuin IAM-projektissa siirrytään tarkempaan määrittelyyn ja tuotevalintoihin. Suunnittelun ei tarvitse olla tehty detaljitasolla, mutta laajuuden ja ylätason vaatimusten tulee olla suurin piirtein selvillä. IAM-käyttöönotto toteutetaan iteratiivisesti, joten suunnitelmia on luonnollista tarkentaa projektin edetessä. Toisaalta kuitenkin jokaisesta edellä mainitusta alueesta tulee olla olemassa tarkan tason määrittely ennen toteutukseen siirtymistä. Kokemus on osoittanut, että IAM:in käyttöönoton aikana on usein jatkuvasti tarvetta palata tehtyihin linjauksiin

Käyttäjäryhmät

Minkä tyyppisten käyttäjien tietoja halutaan hallita IAM:ssa? Omien työntekijöiden ja/tai asiakkaan edustajien? Entä harmaammalla alueella olevat käyttäjäryhmät, kuten väliaikainen työvoima, konsultit ja

kertakäyttötunnukset? Mitä tietoja käyttäjistä saadaan ja mitä tietoja tarvitaan? Miten eri käyttäjäryhmien käyttäjät tunnistetaan luotettavasti?

Nämä linjaukset eivät aina ole aivan yksinkertaisia. Käyttäjien jako ulkoisiin ja sisäisiin alkaa nykypäivänä olla jo turhan karkea yleistys – harmaalle alueelle jää monia käyttäjäryhmiä. Myös rajanvedot eri käyttäjätyyppien välillä voivat olla haastavia. Linjauksia tehdessä on huomioitava myös käytännön realiteetit, esimerkiksi miten käyttäjät voidaan yksikäsitteisesti tunnistaa, mistä käyttäjäryhmien hallinnassa tarvittavat käyttäjä- ja käyttöoikeustiedot saadaan, sekä onko niiden laatu riittävää. Saadaanko kaikki tarvittavat käyttäjän tiedot, ovatko tiedot yhtenäisiä (ts. sama tieto on kirjoitettu aina samassa muodossa) ja oikeassa muodossa? Tässä vaiheessa on hyvä hahmottaa ainakin karkealla tasolla, mitä käyttäjäattribuutteja eri tyyppisistä käyttäjistä tarvitaan, jotta IAM toimisi halutulla tavalla.

Käyttäjien tunnistaminen on kriittisimpiä huomioitavia asioita. Omien työntekijöiden osalta tämä voi olla melko triviaalia ja kertakäyttötunnusten osalta sitä ei välttämättä tarvita, mutta asiakkaiden ja yhteistyökumppaneiden osalta asia on monimutkaisempi. Heikkoa tunnistusta (ts. käyttäjätunnus ja salasana) pidetään yllättävän usein riittävänä. Tässä kriittistä on käyttäjän riittävä tunnistaminen tunnuksen luontivaiheessa. Vahvaa tunnistusta (esim. verkkopankkitunnukset, mobiilivarmenne) vaaditaan aina vain useammin. IAM:in lisäksi tunnistamista tarvitaan myös sähköisissä allekirjoituspalveluissa. Tunnistamisessa voidaan käyttää omassa ylläpidossa olevia IAM-komponentteja tai ostettua tunnistuspalvelua. Federointitilanteissa toinen organisaatio voi olla jo tunnistanut käyttäjän ja kysymys on, millä ehdoilla tähän tunnistukseen luotetaan.

Lähdejärjestelmät

Mistä tietojärjestelmistä yllä mainittujen käyttäjien tiedot saadaan ja mitä tietovirtoja tarvitaan, että homma saadaan toimimaan? IAM-ratkaisu harvoin on ensisijainen tietolähde (ns. master) esimerkiksi työntekijä- tai asiakastiedoille – vaikka se voi tarvittaessa olla sitäkin. Tyypillisesti käyttäjätiedot perustuvat HR tai CRM-järjestelmän tietoihin. Jos käyttäjäryhmän tietojen master on toisessa organisaatiossa, tarvitaan käyttäjien ja mahdollisesti myös käyttöoikeuksien federointia. Attribuutti- ja sääntöpohjainen pääsynhallinta (ABAC) voi käyttää dynaamisesti useita erilaisia tietolähteitä ja ennalta määriteltyjä sääntöjä käyttöoikeuden myöntämiseen ajonaikaisesti.

Käytettävät lähdejärjestelmät on hyvä nimetä jo tässä vaiheessa, ja samalla voi karkealla tasolla selvittää, millä tavoin IAM:ssa tarvittavat tiedot saadaan järjestelmästä ulos. Tämä tuottaa suoraan vaatimuksia IAM-tuotevalinnalle. Samalla tulee hahmottaa, mitä muutoksia esimerkiksi HR tai CRM-tietojen käsittelyprosesseihin vaaditaan, että IAM saadaan toimimaan. Voi olla, että esimerkiksi syötteen tarkastussääntöjä tulee tiukentaa tai arvojen valintalistoja yhtenäistää, että tiedon laatu saadaan riittäväksi IAM:in tarpeisiin. Organisaatiorakenteen määrittely yhtenäisesti ja riittävän yksinkertaisesti on tyypillinen haaste, joka on vain selvitettävä, jos halutaan antaa käyttäjille tietyt käyttöoikeudet automaattisesti käyttäjän organisaatiotietoon perustuen.

Kohdejärjestelmät

Minkä tietojärjestelmien käyttöoikeuksia halutaan hallita keskitetysti IAM:ssa? Mihin järjestelmiin halutaan toteuttaa kertakirjautuminen? Miten käyttöoikeudet ja käyttäjätiedot välitetään (provisioidaan) järjestelmään?

Järjestelmien valinnassa eräs hyvä lähtökohta (tietoturvatavoitteiden lisäksi) on työn vähentäminen. Esimerkiksi minkä järjestelmien käyttäjähallinnan keskittämisestä olisi eniten hyötyä käyttöoikeuksien

hallintaan kuluvan työmäärän vähentämisen suhteen, ja minkä järjestelmien käyttäjät hyötyisivät eniten kertakirjautumisesta. Järjestelmän käyttäjämäärä ja järjestelmässä käytettävä käyttöoikeusmalli ovat tärkeimpiä huomioitavia tekijöitä. Lisäksi on huomioitava, miten järjestelmän pääsynhallinta on toteutettu. Onko järjestelmässä oma sisäinen käyttöoikeus- ja pääsynhallinta, vai voidaanko käyttöoikeudet välittää IAM:ista reaaliaikaisesti kirjautumisen yhteydessä?

Kohdejärjestelmien valintaan liittyy kiinteästi myös tapa, miten käyttöoikeudet ja tarvittaessa myös käyttäjät välitetään (provisioidaan) kohdejärjestelmiin. Kohdejärjestelmästä riippuen käyttäjä- ja käyttöoikeustiedot voidaan provisioida samaan tai eri aikaan, ja näiden provisiointiin voidaan tarvittaessa käyttää eri tapoja. Provisiointitapoja on karkeasti kaksi: automaattinen ja manuaalinen.

- Manuaalinen provisiointi tarkoittaa käytännössä työjonoa, jossa olevien tehtävien perusteella järjestelmän pääkäyttäjä antaa tai poistaa käyttöoikeuksia ko. järjestelmän omilla hallintatyökaluilla.
- Automaattinen provisiointi tarkoittaa käyttäjä- ja käyttöoikeustietojen välittämistä kohdejärjestelmään joko reaaliaikaisesti kirjautumisen yhteydessä tai eräajotyyppisesti tietyin väliajoin. Se on huomattavasti parempi työmäärän vähentämisen kannalta, mutta luonnollisesti siinä IAM tulee jollakin tavalla integroida kohdejärjestelmään. Tähän vaikuttavat keskeisesti tekniset seikat, eli käytännössä millä työmäärällä järjestelmä saadaan integroitumaan IAM:iin.

Käyttäjätietovarasto (esim. Active Directory) ja web-portaalit ovat yleensä helposti IAM:iin integroitavia tapauksia, mutta entä vanhemmat legacy-järjestelmät ja käytössä olevat pilvipalvelut? Näiden käyttäjähallinta kyseisen järjestelmän omilla työkaluilla voi syödä paljon työaikaa, joten automaattiprovisioinnista olisi hyötyä. Tässä tulee kuitenkin usein vastaan teknisiä rajoituksia – tarvittavien tietojen provisiointi automaattisesti voi osoittautua haastavaksi tai jopa mahdottomaksi.

Kohdejärjestelmät on hyvä nimetä tässä vaiheessa ainakin IAM-toteutuksen ensimmäisten vaiheiden osalta. Yleensä ensimmäisiin kohteisiin kuuluu käyttäjähakemisto, koska sitä usein käyttää jo valmiiksi joukko järjestelmiä (esim. työasemat, verkko, SharePoint, yms.) käyttöoikeuksien hallinnassa. Myöhemmissäkin vaiheissa IAM:in piiriin tuotavista järjestelmistä on hyvä olla selvillä ainakin jonkinlainen priorisointi. Niistä järjestelmistä, jotka ainakin olisi saatava automaattisen provisioinnin piiriin, tulee selvittää IAM-integraatiomahdollisuudet ja -rajoitukset. Tästä saadaan suoraan vaatimuksia IAM-tuotevalinnan pohjaksi ja pohjaa käyttöönottoprojektin suunnitteluun. IAM:in myötä järjestelmien käyttäjähallintaan tulevat muutokset tulee hahmottaa myöhemmän ohjeistuksen ja koulutusten pohjaksi.

Kohdejärjestelmiin liittyen on hyvä myös hahmottaa, miten räätälöityjen (custom) sovellusten kehitys huomioidaan IAM:issa, ja toisinpäin. IAM-tuotteet tarjoavat erilaisia mahdollisuuksia toteuttaa esimerkiksi käyttäjä- ja käyttöoikeustietojen provisiointi. On hyvä hahmottaa, mitkä olemassa olevat custom-sovellukset halutaan IAM:in piiriin ja mitä teknisiä mahdollisuuksia tähän on sovellusten puolella. Jatkossa on olennaista ohjeistaa yhteisten IAM-palveluiden hyödyntäminen ohjelmistokehitykselle.

Käyttöoikeudet

Mitkä ovat IAM:ssa hallittavat käyttöoikeudet, eli millainen käyttöoikeusmallin tulee olla? Tämä riippuu käyttäjäryhmistä ja kohdejärjestelmistä. Kohdejärjestelmissä on usein valmiiksi oma käyttöoikeusmallinsa, jonka sovittaminen keskitettyyn IAM:iin voi vaatia työtä. Käyttöoikeuksien tarkkuustaso voi olla myös hyvinkin erilainen eri järjestelmissä. Toisissa on alle kymmenen erilaista käyttöoikeustasoa, toisissa taas pitäisi pystyä antamaan esimerkiksi asiakas-, tuote-, ja henkilökohtaisia käyttöoikeuksia – jolloin tarvittavien käyttöoikeuselementtien määrä voi nousta tuhansiin, jopa miljooniin. IAM-tuotteissakin on usein rajoituksia sille, mitä elementtejä käyttöoikeusmallissa voi olla, miten elementit voivat liittyä toisiinsa ja kuinka ”syvä” malli voi olla.

Yksinkertaisimmillaan malli voi olla, että tiettyyn kohdejärjestelmään liittyy joukko käyttöoikeuksia (rooleja) joita voidaan myöntää käyttäjille. Tällä pääsee jo yllättävän pitkälle. Toki rooleihin voidaan vaatia hierarkkisuutta, jotta niiden hallinta helpottuu (käyttäjälle voidaan esimerkiksi myöntää ”koontirooli” usean yksittäisen roolin sijasta). Mahdollisuus määritellä toisensa pois sulkevia rooleja on tyypillinen vaatimus, jota läheskään kaikki IAM-tuotteet eivät mahdollista.

Roolien määrä tulee kaikissa tapauksissa pitää hallittavana. Jos tiettyyn järjestelmään olisi luotava esimerkiksi tuhansia rooleja, jotta käyttöoikeudet saadaan määriteltyä tarvittavalla tasolla, tulee harkita attribuuttipohjaisen pääsynhallinnan tai ainakin automaattisesti myönnettävien roolien käyttöönottoa.

Tässä vaiheessa on hyvä varmistaa, että ainakin kriittisimpien kohdejärjestelmien käyttöoikeusmallit on huomioitu, ja varmistettu että niitä voidaan hallita IAM:in kautta. Keskitetyn IAM:in käyttöönotto on myös hyvä mahdollisuus kehittää kohdejärjestelmien käyttöoikeusmalleja. Keskustelut järjestelmien omistajien kanssa kannattaa aloittaa myös tästä aiheesta.

Käyttöoikeuksien hallinnan automatisointi on toinen mietittävä kokonaisuus. Miten käyttöoikeuksien myöntämistä ja poistamista halutaan automatisoida? Käyttöoikeuksien automaattinen hallinta perustuu saatavilla oleviin lähdejärjestelmien tietoihin – siis jos tietyllä käyttäjän attribuutilla on tietty ennalta määritelty arvo, myönnetään kyseiselle käyttäjälle tietyt roolit. Siten erityisesti saatavilla oleva käyttäjätieto ja sen laatu on tärkeä tähän vaikuttava tekijä. Jos esimerkiksi halutaan myöntää käyttöoikeuksia käyttäjän työnkuvan perusteella, pitää selvittää onko tätä tietoa ylipäätään saatavilla lähdejärjestelmästä, onko sen tarkkuus riittävä ja onko attribuutin eri arvojen määrä hallittavissa. Tästä johtuen saatetaan päätyä päivittämään esimerkiksi HR-järjestelmässä olevia attribuuttien valintalistoja tai luomaan kokonaan uusia attribuutteja.

Sääntöjä, joiden mukaan käyttöoikeuksia myönnetään, voi jo alustavasti hahmotella tässä vaiheessa. Ainakin tulisi olla selvillä, minkä lähdejärjestelmien mihinkin attribuuttien arvoihin käyttöoikeuksien automaattinen hallinta perustuu, ja mitä käyttöoikeuksia näiden tietojen perusteella hallitaan.

Itsepalvelutoiminnot

Mitä loppukäyttäjien itsepalvelutoiminnallisuuksia otetaan käyttöön? Voiko käyttäjä itse hakea tarvitsemiaan käyttöoikeuksia, vai onko käyttöoikeuksien haku keskitetty esim. esimiehille? Voiko käyttäjä resetoida salasanansa itsepalvelun kautta?

Itsepalvelutoiminnallisuudet tuovat joustavuutta ja ketteryyttä käyttöoikeuksien hallintaan. Ne voivat myös tuoda kustannussäästöjä, jos itsepalvelun kautta käyttäjätuen ja järjestelmien pääkäyttäjien työkuorma pienenee.

Lopuksi

Oikein toteutettuna IAM:lla voidaan vähentää manuaalityötä, parantaa käyttäjä- ja käyttöoikeustiedon laatua ja helpottaa järjestelmien käyttöä. IAM välttämätön riittävän tietoturvan ja digitalisaation kannalta. Toisaalta IAM on monimutkainen kokonaisuus, jonka laajuus, riippuvuudet ja tavoitteet on kuvattava, jotta sen käyttöönotto voidaan tehdä onnistuneesti. Edellä kuvattiin, mitä asioita kokemuksemme mukaan tulee olla määriteltyinä, jotta IAM-käyttöönotossa pääsee alkuun.

Tässä White Paperissa on kuvattu IAM-kokonaisuutta melko perinteisistä lähtökohdista. Tulevaisuudessa yleistyvä attribuutti- ja sääntöpohjainen pääsynhallinta (Attribute-Based Access Control, ABAC) tulee muuttamaan IAM-kokonaisuutta jo lähtökohdista lähtien. Esimerkiksi välillä suhteettomankin tärkeiksi nousevat roolipohjaiset käyttöoikeudet ovat vain yksi ABAC:in lähdetieto, jonka perusteella käyttöoikeudet muodostetaan reaaliajassa.

Coala White Paper: IAM haltuun ymmärtämällä kokonaisuus