White Paper **02 / 2016**

Eetu Niemi

Näin onnistut IAM:in käyttöönotossa

COALA

Oikein toteutettuna käyttäjä- ja pääsynhallinnalla (IAM) voidaan parantaa tietoturvaa, helpottaa järjestelmien käyttöä ja saada kustannussäästöjä esimerkiksi automatisoinnin ja virheiden vähentämisen myötä. IAM-ratkaisun käyttöönoton haastavuus kuitenkin usein yllättää. Usein aikataulu venyy (jopa kaksin- tai kolminkertaiseksi), kustannukset räjähtävät käsiin ja/tai IAM:iin liittyvistä linjauksista päädytään kiistelemään vuosien ajaksi.

Tämä on ymmärrettävää, koska IAM liittyy ”kaikkeen” – prosesseihin, toimintatapoihin, tietojärjestelmiin ja teknologioihin. IAM ei olekaan ”vain” infraa, jonka voi ostaa hyllyltä ja ottaa käyttöön ilman suurempaa hässäkkää. Niin kuin sananlaskukin sanoo, hyvällä suunnittelulla pääsee pitkälle, mutta IAM:in onnistunut käyttöönotto vaatii muutakin.

Tässä Coalan White Paperissa on kuvattu, mitä vaiheita IAM-ratkaisun käyttöönottoon tyypillisesti kuuluu ja mitä niissä on huomioitava, jotta pahimmat sudenkuopat vältettäisiin.

***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:in käyttöönotto

IAM:in käyttöönotto toteutetaan projektissa (yleensä useassa). Pääpiirteissään käyttöönotto on samanlainen kuin muissakin ohjelmistotuotehankinnoissa. IAM:in monet riippuvuudet tuovat kuitenkin hankintaan omat erityispiirteensä. Seuraavissa kohdissa on käyty läpi vaihe vaiheelta, mitä IAM:in onnistunut käyttöönotto edellyttää.

1. Hahmota kokonaisuus
2. Määrittele ratkaisu
3. Ymmärrä markkina
4. Päivitä dokumentaatio
5. Valitse sopivat tuotteet
6. Suunnittele integraatiot ja konfiguraatiot
7. Valitse toteutuskumppanit
8. Suunnittele ja toteuta käyttöönottoprojekti
9. Huolehdi jatkuvista palveluista

1. Hahmota kokonaisuus

IAM-ratkaisun käyttöönottoa suunnitellessa (kuten missä tahansa muussakin ohjelmistohankinnassa) on aluksi ymmärrettävä organisaation tarpeet. Riittävän kuvan kokonaisuudesta saat linjaamalla ainakin seuraavat perusasiat:

- Millaisia käyttäjiä identiteetinhallinnan kautta hallinnoidaan (sisäiset, ulkoiset, väliaikaiset, jne.) ja mistä näiden tiedot saadaan (esim. HR- tai CRM-järjestelmästä)
- Millaisia käyttöoikeuksia hallinnoidaan (esim. on/off -tyyppisiä, roolipohjaisia, vai attribuuttipohjaisia)
- Minkä järjestelmien käyttöoikeushallinta on identiteetinhallinnan piirissä (ja missä vaiheessa)
- Mitä automatisoidaan (esim. tiettyjen käyttöoikeuksien myöntäminen, provisiointi tiettyihin järjestelmiin)
- Mitä itsepalvelutoiminnallisuuksia otetaan käyttöön

Kokonaisuuden hahmottamista on käsitelty aiemmin Coalan White Paperissa *IAM haltuun ymmärtämällä kokonaisuus*.

2. Määrittele ratkaisu

IAM-ratkaisun määrittely on toisaalta saman tyyppistä kuin muissakin ohjelmistohankinnoissa. Toisaalta taas IAM-ratkaisun laajuus ja kattavuus tuovat työhön omat haasteensa. Huolellinen määrittely on välttämätöntä, että IAM-tuotevalinnat saadaan tehtyä informoidusti ja käyttöön saadaan parhaiten soveltuvat tuotteet. Kokemuksemme mukaan arkkitehtuuridokumentaatio voi olla parempi lähtökohta kuin käyttötapaukset ja pitkät vaatimuslistat, kunhan kuvaus on tarpeeksi tarkka. Aikaa säästyy ja olennaisimmat asiat tulevat selvemmin esille. Yleiskuva tarvittavista IAM-komponenteista, niiden välisistä integraatioista sekä liittymistä olemassa oleviin tietojärjestelmiin on hyvin hyödyllinen. Seuraavat määrittelyt ovat tärkeimpiä tässä vaiheessa:

- **Integraatiot ja tietovirrat**. IAM integroituu laajasti lähde- ja kohdejärjestelmiin, joista osa voi olla myös organisaation ulkopuolella. Siksi IAM:in toiminnan kannalta tarvittavat tietovirrat tulee kuvata. Näitä ovat niin provisiointiin kuin pääsynhallintaankin liittyvät tietovirrat. Näihin liittyvien teknisten vaatimusten ja rajoitteiden hahmottaminen on välttämätöntä tässä vaiheessa, jotta

tuotevalinnat voidaan tehdä onnistuneesti. Tiedon laatu on myös varmistettava ja tarvittavat tietomuunnokset huomioitava.

- **Prosessit**. IAM:iin liittyvät prosessit tulee määritellä (tai päivittää olemassa olevia määrittelyitä) ja huomioida niiden riippuvuudet olemassa oleviin prosesseihin. Luonnollisesti käyttäjätunnuksiin ja käyttöoikeuksiin liittyvät prosessit ja toimintatavat menevät ainakin osittain uusiksi IAM-ratkaisun käyttöönoton myötä. Riippuvuuksia on myös (tilanteesta riippuen) HR:n tai asiakkuuden hallinnan prosesseihin. Kaikki käyttäjiin liittyvät tilanteet tulee määritellä ja huomioida niiden vaikutukset käyttöoikeuksiin. Käyttäjäksi tuleminen on yleensä melko yksiselitteistä, mutta haasteet tulevat erilaisista erikoistapauksista: miten hallitaan ja miten käyttöoikeuksiin vaikuttavat esimerkiksi muutokset työnkuvaan, pidemmät poissaolot, sijaisuudet ja työsuhteen päättyminen. Varsinaisten päivittäisten IAM-toimintaan liittyvien prosessien lisäksi on hyvä määritellä myös IAM:in jatkuviin palveluihin liittyvät prosessit (ks. edellä).
- **Käyttäjäskeema**. Käyttäjäskeema määrittelee, mitä tietoa käyttäjistä ylläpidetään IAM-ratkaisussa. Se toimii identiteettien hallinnan pohjana. Luonnollisesti määrittelyssä tulee huomioida, mitä tietoa käyttäjästä ylipäätään tarvitaan, mitä tietoja saadaan lähdejärjestelmistä ja mikä tämän tiedon laatu on. Käyttäjien ja käyttöoikeuksien hallinnan kannalta turhia tietoja (esim. hetu, osa työsuhdetiedoista) ei kannata jo pelkästään tietoturvasyistä välittää IAM:iin. Jokin yksikäsitteinen tunnus käyttäjille kuitenkin tarvitaan – oli tämä sitten henkilönumero tai jokin tietojärjestelmissä käytettävä tekninen tunnus.
- **Käyttöoikeusmalli**. Käyttöoikeusmalli kuvaa, miten käyttöoikeudet muodostuvat. Käyttöoikeusmalli voi olla esimerkiksi hierarkkinen puu, jossa juuressa ovat kohdejärjestelmät, joihin taas voi liittyä käyttöoikeuksia (rooleja)**.** Käyttöoikeudet voivat koostua toisista käyttöoikeuksista. Joissain tapauksissa voi olla järkevää mahdollistaa myös käyttöoikeudet, jotka kokoavat yhteen joukon käyttöoikeuksia useisiin järjestelmiin. Jos käyttöoikeuksien myöntämistä halutaan automatisoida, tulee malliin ottaa mukaan myös attribuutit, joiden perusteella käyttöoikeuksia myönnetään (esim. organisaatioyksikkö), ja määritellä mitä käyttöoikeuksia näiden perusteella hallinnoidaan. Jos taas tarvitaan automaattisesti muodostuvia käyttöoikeusrooleja (tarvitaan esimerkiksi, jos asiakkaalle halutaan antaa tuotekohtaisia käyttöoikeuksia), tulee määritellä rakenne, jonka mukaan roolit muodostetaan. Käyttöoikeusmallin tulee ottaa kantaa myös käyttöoikeuksien nimeämiseen. Mallin tulee lähtökohtaisesti olla yhteensopiva kaikkien kohdejärjestelmien käyttöoikeusmallien kanssa, ellei näitä haluta uudistaa IAM:in mukaisiksi.
- **IAM:in omat käyttöoikeudet**. Ei pidä unohtaa määritellä, millaisia käyttöoikeuksia IAM-ratkaisuun itsessään tarvitaan. Tällä tarkoitetaan esimerkiksi käyttäjien tietojen tarkastelua, käyttöoikeusmallien muokkaamista, käyttöoikeustilausten hoitamista sekä käyttöoikeuksien tilaamista. Eri tyyppisille käyttäjille tarvitaan usein eritasoisia ja/tai laajuisia käyttöoikeuksia. Tässä vaiheessa tuleekin määritellä, minkä tyyppisiä käyttäjiä IAM-ratkaisulla itsessään on (esim. peruskäyttäjä, käyttöoikeustilausten hyväksyjä, admin, jne.) ja mitä eri käyttöoikeuksilla pitäisi pystyä tekemään. Käyttöoikeuksien määrittely on erityisen tärkeää, jos käytössä on itsepalvelutoimintoja ja käyttäjissä on siten muitakin kuin admin-tyyppisiä käyttäjiä ja provisioijia.

3. Ymmärrä markkina

IAM toteutetaan lähes aina valmistuotteilla. Siksi markkinan on syytä selvittää, millaisia IAM-tuotteita markkinoilla on tarjolla, ja miten ne täyttävät organisaation tarpeet. Markkinakatsaus on hyvä keino rajata jo tässä vaiheessa mahdollisen toimittajien ja tuotteiden määrää, niin että varsinainen hankintaprosessi pysyy hallittavana.

Tässä vaiheessa analyysi voi olla melko ylätasolla – tärkeää on lähinnä hahmottaa, minkä toimittajien tuotteet ylipäätään voisivat täyttää tarpeet ja mitä eri tuotteita kultakin

toimittajakandidaatilta suurin piirtein tarvittaisiin. Varsinaisten tuotteisiin liittyvien IAM-vaatimusten lisäksi on hyvä ottaa mukaan myös tärkeimmät toimittajaan liittyvät kriteerit, kuten lisensointimalli ja lokaalin tuen saatavuus. Kevyt RFI-prosessi on toimiva tapa toteuttaa markkinakartoitus.

4. Päivitä dokumentaatio

Kun tarjolla olevat tuotteet ja niiden ominaisuudet ovat karkealla tasolla selvillä, on usein tarpeen päivittää omia vaatimuksia. Laadittua alustavaa IAM-arkkitehtuurikuvaa tulee tarkentaa muun muassa sen perusteella, että tiedetään mitä IAM-tuotteita tarvitaan.

Valmistuotteissa on rajoituksia esimerkiksi konfiguroitavuuden ja integroituvuuden suhteen. Siksi voi olla tarvetta luopua osasta näihin liittyvistä vaatimuksista, tai lieventää niitä. Kuten yleensä, tuotteiden räätälöintiä tulisi välttää tai ainakin se on tehtävä hyvin informoituna.

5. Valitse sopivat tuotteet

IAM-tuotevalinta tapahtuu samalla tavoin kuin muutkin ohjelmistotuotevalinnat – selkeät valintakriteerit arkkitehtuuridokumentaation muodossa ovat kriittisiä. Lisäksi on huomioitava toimittajaan liittyviä tekijöitä, kuten tuki, koulutus, jatkuvuus ja lisensointimalli. Lisämaustetta tuo se, että IAM-kokonaisuus koostuu usein useasta tuotteesta. Voi olla, että tietty toimittaja ei tarjoa kaikkia tarvittavia IAM-komponentteja tuotteina, jolloin voidaan joutua hankkimaan tuotteita useilta toimittajilta. Integraatioiden saaminen toimimaan voi vaatia lisätuotteiden hankkimista. Tavoitteiden ja laajuuden määrittely kertoo, mitä IAM-komponentteja tarvitaan.

IAM-tuotteissa on suuria eroja tuetuissa toiminnoissa, konfigurointimahdollisuuksissa ja integroituvuudessa. Myös teknisissä attribuuteissa kuten saatavuudessa ja skaalautuvuudessa on eroja, puhumattakaan saatavilla olevasta tukidokumentaatiosta ja toimittajan tuesta. Ratkaisun määrittelyn on oltava tuotevalintaa tehdessä kirkkaana mielessä, koska tuotteet eivät vain taivu kaikkeen – ainakaan järkevin kustannuksin.

Erityisen paljon eroja on käyttöoikeusmallien määrittelyssä. Monet tuotteet ovat alun perin olleet lähinnä keskitettyjä käyttäjätietovarastoja, joihin roolipohjaisten käyttöoikeuksien hallinta on lisätty jälkikäteen – enemmän tai vähemmän onnistuneesti. Joissain (tunnetuissakin) tuotteissa yksinkertaisinkin konfiguraatio kuten yhden uuden kohdejärjestelmän lisääminen ja sen roolimallin konfigurointi voi vaatia päivän verran konsulttityötä. Toiset taas mahdollistavat kohtuullisella työllä monimutkaistenkin mallien määrittelyn. Jos käsityötä on paljon ja ympäristö laaja (esim. satoja kohdejärjestelmiä), nousevat kustannukset peruskonfiguraatiostakin satoihin tuhansiin tai jopa miljooniin euroihin.

Myös muissa konfigurointimahdollisuuksissa on eroja. Usein läheskään kaikkea ei saa määriteltyä siististi käyttöliittymässä, vaan vaaditaan koodausta. Vähänkin suuremmat muutokset, kuten integraatiot, voivat vaatia satoja tunteja toimittajan työtä.

Rajattu Proof-of-Concept -toteutus voi olla järkevä tehdä ennen varsinaista hankintaa, jos tuotteen soveltuvuudesta ei olla täysin varmoja. Näin voidaan varmistua esimerkiksi IAM-tuotteiden yhteentoimivuudesta.

6. Suunnittele integraatiot ja konfiguraatiot

Kun tuotteet on valittu, voidaan suunnitella tarkemmin, miten tuotteista muodostetaan arkkitehtuurikuvauksen asettamat vaatimukset toteuttava IAM-ratkaisu. Keskiössä ovat

toteutettavat integraatiot ja konfiguraatiot. Tämä sisältää niin käyttäjäskeeman ja käyttöoikeusmallin konfiguroinnin, provisioinnin vaatimat integraatiot kuin myös pääsynhallinnan ja tunnistuksen komponenttien integroinnit ja konfiguroinnit. Suunnittelulla tarkoitetaan tässä yhteydessä teknistä suunnittelua, joka on sillä tarkkuustasolla, että tuotteen konfiguroija saa sen perusteella tehtyä tarvittavat konfiguraatiot.

Joiltain osin jo tehty arkkitehtuurikuvaus voi ainakin osittain riittää tähän tarpeeseen (esim. käyttäjän tietomallin ja käyttöoikeusmallin osalta). Usein kuitenkin vaaditaan ainakin jonkin verran tarkentamista (esim. mäppäys mitä tuotteessa valmiina olevaa attribuuttia käytetään millekin käyttäjän tietomallin attribuutille ja mitä valmiita attribuutteja poistetaan näkyvistä). Jos tietyn asian toteuttamiseen on tuotteessa useita tapoja, tulee selvittää näiden vahvuudet ja heikkoudet sekä dokumentoida valittu tapa.

Integraatioiden osalta tulee tehdä tarkan tason tekninen määrittely, kattaen muun muassa tiedonsiirtotavat, siirtyvät tiedot, attribuuttien mäppäykset sekä tietomuunnokset ja niiden toteutustavat. Jos käyttöliittymä on tuotteessa konfiguroitavissa, tulee määritellä miltä käyttöliittymän tulee näyttää. Yleensä tuotteissa on mahdollista ainakin poistaa tiettyjä tietoja näkyvistä ja tehdä kevyttä ulkoasun muokkausta.

Toteutettavat integraatiot ja ylipäätään IAM:in toimiminen halutulla tavalla vaatii usein muutoksia myös lähde- ja kohdejärjestelmiin. Myös nämä tulee suunnitella toteutuksen vaatimalla tasolla.

7. Valitse toteutuskumppanit

IAM-tuotteen valmistaja ei useimmiten ole ainoa mahdollinen kumppani ratkaisun käyttöönottoon, vaan tarvittavaa tuoteosaamista on muillakin. Toimituskyvyssä ja laadussa on kuitenkin suuria eroja. Saman kumppanin käyttäminen niin määrittelyyn, suunnitteluun, toteutukseen kuin myös integraattorina toimimiseen ei aina ole viisain valinta. Kannattaa myös huomioida, että ainakin jonkin verran tukea tarvitaan aina ratkaisun valmistajalta.

Sopimusasioilla voidaan vähentää riskejä, mutta lopulta sanktiotkaan eivät korvaa menetettyä työaikaa. Referenssejä vastaavista IAM-toteutuksista kannattaa siis kysyä.

8. Suunnittele ja toteuta käyttöönottoprojekti

IAM-kokonaisuus toteutetaan iteratiivisesti projektissa tai projekteissa. Projektointitapa riippuu muun muassa kokonaisuuden laajuudesta ja siitä, kuinka erillisiä toteutettavat osa-alueet ovat. Ohjelmistotuotteiden käyttöönottoa käsittelevässä kirjallisuudessa on paljon hyviä käytäntöjä käyttöönottoprojektin suunnitteluun ja toteutukseen. IAM:in laajuus ja monet liittymäpinnat tuovat projektiin kuitenkin omat haasteensa.

Tuotteiden asentamisen, konfiguroinnin ja käyttöönoton lisäksi merkittävin työmäärä tulee yleensä integraatioiden toteuttamisesta. Näissä on huomioitava myös lähde- ja kohdejärjestelmiin toteutettavat muutokset.

Konfiguroinnissa yllättävänkin laaja kokonaisuus voi olla kohdejärjestelmien tuonti IAM:in piiriin. Tämä sisältää tarvittavien käyttöoikeusmallien ja provisiointityönkulkujen määrittelyn, unohtamatta mahdollista automaattisen provisioinnin vaatimaa teknistä integraatiota. Jos kohdejärjestelmiä on paljon, voi pelkästään tämän osuuden kesto olla jopa vuosia.

IAM-ratkaisun tulevien käyttäjien kouluttaminen ja ohjeistaminen on kriittinen kokonaisuus. Peruskäyttäjien (jotka ehkä tilaavat käyttöoikeuksia ja mahdollisesti päivittävät omia tietojaan) lisäksi on yleensä huomioitava myös esimiehet (jotka usein hyväksyvät käyttöoikeustilaukset), manuaaliset provisioijat, ohjelmistokehityshenkilöstö (jotta IAM voidaan huomioida uusien järjestelmien kehityksessä alusta asti) sekä admin-käyttäjät. IAM koskettaa useita prosesseja, joten kaikille näissä työskenteleville pitää ohjeistaa ja kouluttaa IAM:in tuomat muutokset toimintatapoihin.

9. Huolehdi jatkuvista palveluista

IAM vaatii yllättävän suuren joukon jatkuvia palveluita toimiakseen. Silti näitä ei aina ole edes suunniteltu ja vastuutettu, tai ainakin ne on resursoitu riittämättömästi. Esimerkiksi ratkaisun ylläpidon sekä uusien konfigurointien ja integraatioiden hallinnan on toimittava. Miten hoidetaan manuaaliset provisioinnit? Miten uusi kohdejärjestelmä lisätään IAM:in piiriin ja kuka määrittelee sen käyttöoikeusmallin? Entä miten hallitaan muutokset lähdejärjestelmien käyttäjätietomalleissa? Miten hallitaan IAM-tuotteiden päivitykset ja niiden vaikutukset tehtyihin konfiguraatioihin? Miten vikojen selvittelyssä edetään? Miten uudet käyttäjät ohjeistetaan ja koulutetaan?

Muun muassa kaikkiin näihin tehtäviin tulee olla määriteltynä toimintatavat ja vastuut (mielellään myös tarkan tason prosessikuvaukset). Selkeiden ohjeiden on oltava saatavilla. Erillinen kehitys- tai testausympäristö on lähes pakollinen muutosten testaamiseksi ennen niiden viemistä tuotantoon.

Lopuksi

IAM-käyttöönotto on laaja ja monimutkainenkin kokonaisuus. Tässä White Paperissa esitetty vaiheistus selkeyttää kuitenkin kokonaisuuden hallintaa. Kuhunkin vaiheeseen on myös annettu konkreettisia vinkkejä, joilla vältät pahimmat sudenkuopat. Myös yleisillä ohjelmistotuotteiden käyttöön liittyvillä hyvillä käytännöillä pääsee pitkälle.

Coala White Paper: Näin onnistut IAM:in käyttöönotossa