

Keskitetty identiteetinhallinta

Referenssiarkkitehtuuri

Hannu Kasanen, Secproof Finland



Sisältö

1. JOHDANTO	1
2. MISTÄ ON KYSE?.....	1
3. IDENTITEETINHALLINNAN KOMPONENTIT.....	3
3.1. IDENTITEETINHALLINNAN YDIN.....	3
3.2. IDENTITEETTITIEDON VARASTO	3
3.3. LÄHDETTIEDON VÄLITYSRAJAPINTA	3
3.4. IDENTITEETTITIEDON VÄLITYSRAJAPINTA.....	4
3.5. LOPPUKÄYTTÄJÄN KÄYTTÖLIITTYMÄ	5
3.6. HALLINTAKÄYTTÖLIITTYMÄ	6
3.7. SOVELLUSRAJAPINNAT	6
4. SECPROOF IDENTITEETINHALLINNAN ASIANTUNTIJANA	7

LIITE: ESIMERKKI KESKITETYSTÄ IDM-PALVELUSTA



Kirjoittajasta

Hannu Kasanen vastaa Secproofin identiteetin- ja pääsynhallintaan sekä yritysarkkitehtuurien kehittämiseen liittyvistä palveluista. Kirjoittajalla on takanaan mittava käytännön kokemus identiteetin hallinnan kehityshankkeista – alkaen pienimuotoisista selvityksistä ja päätyen laajoihin, aidosti kansainvälisiin IdM-palveluiden käyttöönottoihin. Tyypillisesti kirjoittajan toimenkuvaan kuuluu identiteetin hallinnan tarpeiden selvittely yhdessä asiakkaan IT-organisaation ja liiketoiminnan edustajien kanssa (=mitä tehdään) sekä toteutuksen suunnittelu yhdessä IT-organisaation ja toimittajien kanssa (=miten tehdään).

Trademarks

All trademarks, product names and registered trademarks are the property of their respective owners. Any third-party trademarks, service marks and logos are the property of their respective owners.

Terms of use

This document can be freely copied and printed for an offline internal use. The content of this document may not be sold, reproduced, or distributed without prior written permission from Secproof Finland. Any further rights not specifically granted herein are reserved.

1. Johdanto

Tässä dokumentissa on esitelty Secproofin näkemys keskitetyn identiteetinhallinnan (engl. *identity management, IdM*) referenssiarkkitehtuurista. Lisäksi dokumentissa pyritään avaamaan identiteetinhallintaan liittyviä käsitteitä mahdollisimman yleistajuisesti.

Referenssiarkkitehtuuri tarjoaa yleisen ratkaisumallin keskitetyille identiteetinhallinnan palvelulle ottamatta tarkemmin kantaa tapauskohtaisiin liiketoimintatarpeisiin. Se kuvaa identiteetinhallinnassa tyypillisesti käytettävät komponentit abstraktilla tasolla. Referenssiarkkitehtuuri voi toimia mallina ja suunnittelun apuvälineenä yksittäisille projekteille tai kehityshankkeille.

Huomaa, että identiteetinhallinnan tuotteiden ja teknologioiden kirjo sisältää paljon toimintoja, joita ei ole tässä yhteydessä käsitelty. Tässä kuvattu referenssiarkkitehtuuri sisältää ainoastaan tietyt perusasiat, jotka löytyvät – tai ainakin pitäisi löytyä – jokaisesta keskitetystä identiteetinhallinnan palvelusta.

2. Mistä on kyse?

Identiteetinhallinnalla tarkoitetaan tässä yhteydessä käyttäjän sähköisen identiteetin sekä siihen liitettyjen käyttövaltuuksien hallintaa, sekä tämän identiteetti- ja käyttövaltuustiedon välittämistä sitä tarvitseville tahoille.

Identiteetinhallinnan perimmäisenä tarkoituksena on taata, että **oikeilla käyttäjillä on pääsy oikeisiin resursseihin oikeaan aikaan** – ja kaikki tämä mahdollisimman helposti ja tehokkaasti. Käyttäjä voi tässä tapauksessa olla luonnollinen henkilö (esim. yrityksen työntekijä, kumppani, asiakas tms.), kuvitteellinen henkilö (esim. testikäyttäjä), tietojärjestelmä tai prosessi. Resurssi voi puolestaan olla esimerkiksi tietty (liiketoiminnan kannalta olennainen) tieto, tietojärjestelmä tai sen osa, tai vaikkapa yrityksen toimipiste siihen liittyvine kulkuoikeuksineen.

Identiteetinhallinnan keinoin organisaatio pystyy tehokkaasti vastaamaan mm. seuraaviin kysymyksiin:

- Millaisia käyttäjiä organisaatiossa on olemassa?
- Mihin tietoon, sovelluksiin tai palveluihin em. käyttäjillä on (ollut) oikeus päästä? Miksi?
- Kenellä organisaatiossa on oikeus hyväksyä pääsy em. tietoon, sovelluksiin tai palveluihin?

Identiteetinhallinta ei ole pelkkiä tietojärjestelmiä tai teknologiaa. Siihen liittyy myös erinäinen joukko ihmisiä, prosesseja ja sääntöjä, joita identiteetinhallinnan tehtävänä on tukea, tehostaa ja toimeenpanna.



Identiteetinhallinta vs. pääsynhallinta

Mitä eroa identiteetinhallinnalla ja pääsynhallinnalla (engl. *access management*) on? Tässä yhteydessä edellisellä tarkoitetaan käyttäjä- ja käyttövaltuustiedon hallintaa ennalta määriteltyjen prosessien ja sääntöjen mukaisesti, jälkimmäisellä puolestaan identiteetinhallinnan keinoin myönnettyjen käyttövaltuuksien ajonaikaista (engl. *runtime*) täytäntöönpanoa.

Uudelle työntekijälle voidaan identiteetinhallinnan palvelussa esimerkiksi luoda käyttäjätilit ja myöntää oletuskäyttövaltuudet ennalta määriteltyihin tietojärjestelmiin. Pääsynhallinta astuu kuvaan mukaan vasta, kun kyseinen työntekijä yrittää ensi kertaa käyttää edellä mainittuja tietojärjestelmiä.

Identiteetinhallinnalla ja pääsynhallinnalla on vahvasti symbioottinen suhde. Konkreetista hyötyä saavuttaakseen organisaation tulee hallita riittävässä määrin molemmat osa-alueet.

Identiteetinhallinnan palvelu sisältää tyypillisesti seuraavia **toiminnallisuuksia**:

- Identiteetin elinkaaren hallinta (ml. identiteetin luonti, päivitykset, poisto, arkistointi jne.)
- Attribuuttien generointi (ml. ID-numerot, käyttäjätunnukset, sähköpostiosoitteet jne.)
- Käyttövaltuuksien mallintaminen (ml. roolit, ryhmät, resurssit, säännöt, rajoitteet jne.)
- Käyttövaltuuspyyntöjen sekä niihin liittyvien työkulkujen hallinta ja automatisointi (ml. seuranta, hyväksynät, delegointi jne.)
- Raportointi ja auditointi
- Identiteettitiedon välittäminen ja/tai tarjoaminen sitä tarvitseville tahoille (provisiointi)

Keskitetyllä identiteetinhallinnalla tarkoitetaan edellä mainittujen toiminnallisuuksien tarjoamista koko organisaatiolle keskitetysti yhdestä paikasta. Tämä mahdollistaa paitsi kustannustehokkaan toteutuksen, myös kattavan kokonaiskuvan hahmottamisen ja hallinnan – yli yksittäisten organisaatioyksiköiden ja tietojärjestelmien.

Keskitetyn identiteetinhallinnan **hyödyt** voidaan jakaa kolmeen kategoriaan:

1. Parempi kontrolli

- Identiteetin koko elinkaaren hallinta
- Näkyvyys käyttäjän kaikkiin käyttövaltuuksiin
- Käyttövaltuuksien kumuloitumisen sekä vaarallisten työyhdistelmien ehkäisy
- Selkeät vastuut ja jäljitettävät hyväksymiskäytännöt
- Manuaaliseen työhön liittyvien virheiden väheneminen

2. Parempi kustannustehokkuus

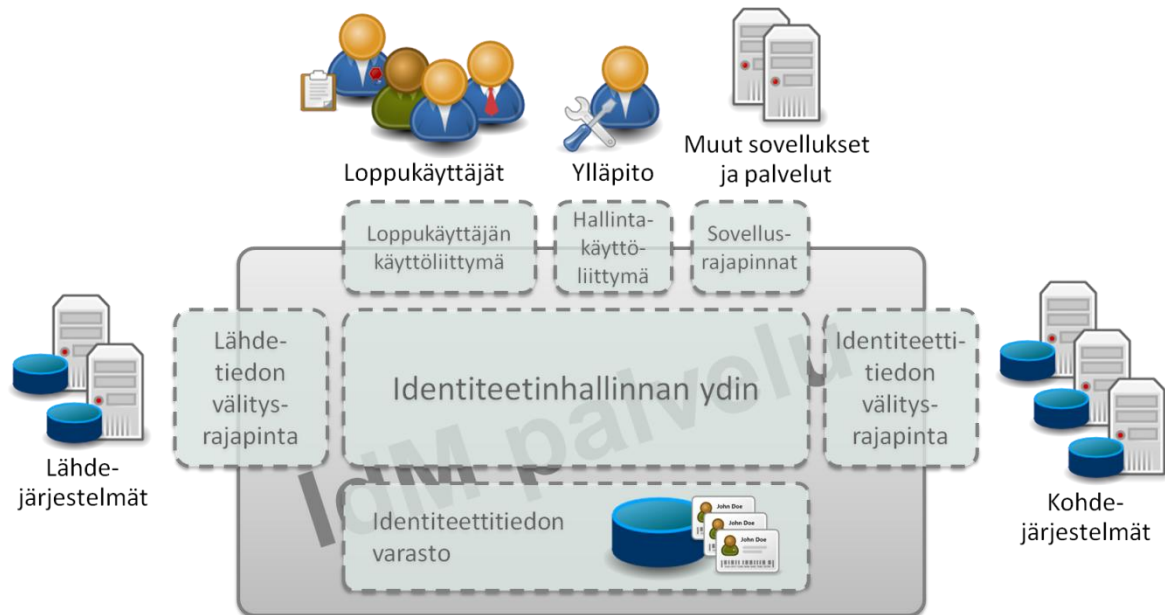
- Vähemmän manuaalista työtä käyttövaltuuksien hallinnassa
- Nopeampi pääsy tuottavaan työhön
- Parempi kyky hallita organisaatiomuutoksia
- Nopeampi ja helpompi käyttövaltuuksien auditointi sekä vaatimustenmukaisuuden (engl. *compliance*) osoittaminen
- Nopeampi ja helpompi sovelluskehitys

3. Parempi loppukäyttäjäkokemus

- Salasanojen vaihto itsepalveluna ja keskitetysti yhdestä paikasta
- Käyttövaltuuksien myöntäminen nopeasti ja/tai automaattisesti
- Käyttövaltuuksien hallinta itsepalveluna
- Mahdollisuus seurata reaaliajassa käyttövaltuuspyyntöjen etenemistä

3. Identiteetinhallinnan komponentit

Alla oleva kuva havainnollistaa keskitetyn identiteetinhallinnan tyypilliset komponentit ja käyttäjäryhmät. Kukin komponentti on tarkemmin kuvattu myöhemmissä kappaleissa.



Kuva 1 IdM-palvelun referenssiarkkitehtuuri

3.1. Identiteetinhallinnan ydin

Identiteetinhallinnan palvelun keskiössä on "moottori", joka toteuttaa identiteetinhallinnassa käytettävät liittyvät säännöt, prosessit ja työnkulut. Tämä "moottori" voidaan konfiguroida käyttäjäorganisaation tarpeita vastaavaksi hallintakäyttöliittymän (ks. kappale 3.6) avulla.

3.2. Identiteettitiedon varasto

Identiteetinhallinnan palvelun taustalta löytyy yksi tai useampi tietovarasto, johon kaikki identiteettitieto (ml. käyttäjät, käyttövaltuudet ja resurssit) talletetaan. Tapauksesta riippuen samaa tietovarastoa voidaan käyttää myös palvelun konfiguraation säilyttämiseen. Tyypillisesti tietovarastona toimii relaatio-tietokanta tai hakemisto.

Tietovarastoon talletettua dataa käsitellään identiteetinhallinnan ytimessä olevien palveluiden välityksellä, ts. suorat yhteydet identiteetinhallinnan palvelun ulkopuolelta on tyypillisesti estetty.

3.3. Lähdetiedon välitysräjäpinta

Identiteetinhallinnan palvelu integroidaan useimmiten yhteen tai useampaan **auktoritatiiviseen lähdejärjestelmään** (engl. *authoritative source*). Tyypillisin esimerkki on henkilöstöhallinnan (HR) tietojärjestelmä, josta saadaan perustiedot yrityksen organisaatorakenteesta sekä yrityksen omista työntekijöistä ja heidän työsuhteestaan. Muita tyypillisiä esimerkkejä lähdejärjestelmistä ovat asiakas-, kumppani-, alihankkija- ja sopimustietokannat.

Lähdejärjestelmistä saatava tieto tuodaan identiteetinhallinnan palveluun lähdetiedon välitysrajapinnan kautta. Rajapinnan toteutuksessa käytetään tyypillisesti tuote- tai teknologiakohtaisia liittimiä (engl. *connectors*) sekä erillisiä tietovarastoja (esim. erillinen yhteys- tai välitaulu lähdejärjestelmän tai IdM-palvelun tietokannassa). Myös csv- tai xml-muotoisten tiedostojen käyttö tiedon välityksessä on varsin tavallista.

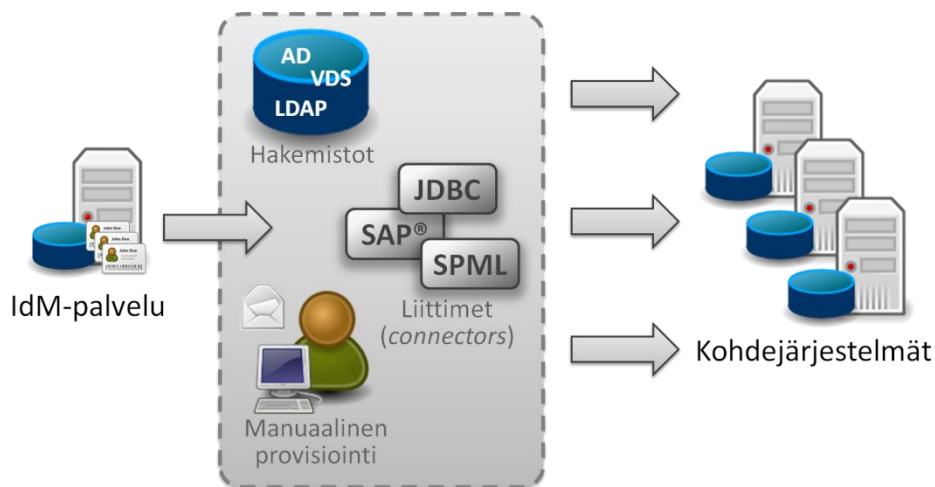
Identiteetinhallinnan ydin sisältää tyypillisesti logiikkaa, joka mahdollistaa identiteettien ja käyttövaltuuksien automaattisen hallinnoinnin lähdejärjestelmistä saatavan tiedon perusteella. Esimerkiksi jokaiselle HR-järjestelmään lisätylle (uudelle) työntekijälle voidaan myöntää hänen työnkuvansa edellyttämät käyttövaltuudet (ml. käyttäjätunnukset, sähköpostiosoitteet, käyttöoikeudet) automaattisesti, ilman manuaalista työtä. Vastaavasti työ- tai sopimussuhteen päättyminen tyypillisesti johtaa olemassa olevien käyttövaltuuksien välittömään poistamiseen.

3.4. Identiteettitiedon välitysrajapinta

Identiteetinhallinnan palvelu välittää identiteetti- ja käyttövaltuustietoa sitä tarvitseville kohdejärjestelmille. Käytännössä tämä tarkoittaa identiteetteihin tai käyttövaltuuksiin tehtyjen muutosten viemistä – tavalla tai toisella – niihin tietojärjestelmiin, sovelluksiin tai muihin resursseihin, joissa em. identiteetti- tai käyttövaltuustietoa viime kädessä käytetään. Tätä toimenpidettä kutsutaan yleisesti **provisioinniksi** (engl. *provisioning*). Onnistuneesti suoritettu provisiointi on edellytys sille, että identiteetinhallinnan palvelussa tehdyt muutokset oikeasti vaikuttavat käyttäjien käyttövaltuuksiin yksittäisissä kohdejärjestelmissä.

Provisiointin toteutuksessa käytetään joko kohdejärjestelmän tarpeisiin räätälöityjä liittimiä tai yleiskäyttöisiä provisiointimekanismeja. Jälkimmäisestä tyypillisin esimerkki on keskitetty käyttäjähakemisto (esim. Microsoft® Active Directory®), johon yksittäiset kohdejärjestelmät voivat tukeutua valtuutus-päätöksiä (engl. *authorization decisions*) tehdessään. Palvelukeskeisten arkkitehtuurien (engl. *service-oriented architecture, SOA*) yleistyessä voi olettaa, että provisiointi pohjautuu jatkossa yhä useammin SOA-maailmaan suunniteltuihin standardeihin. Näistä esimerkkeinä mainittakoon SPML (*Service Provisioning Markup Language*) ja XACML (*eXtensible Access Control Markup Language*).

Usein käyttäjätietojen ja käyttövaltuuksien välittämistä kaikkiin kohdejärjestelmiin on kuitenkin varsin hankala – ellei jopa mahdotonta – automatisoida. Näissä tapauksissa provisiointimekanismina voidaan käyttää sähköpostia tai muita työnohjauksen välineitä. Tällöin provisiointin toteutuksesta vastaa viime kädessä kyseisen kohdejärjestelmän ylläpidosta vastaava taho (ihminen). Manuaalisesta työvaiheesta huolimatta tässäkin tapauksessa on mahdollista saavuttaa valtaosa kappaleessa 2 mainituista keskitetyn identiteetinhallinnan hyödyistä.



Kuva 2 Identiteettitiedon välitysrajapinnassa käytettyjä teknologioita

Joissakin tapauksissa identiteettitiedon välitysrajapinnan kautta voidaan myös tuoda kohdejärjestelmiin suoraan tehtyjä muutoksia takaisin identiteetinhallinnan palveluun. Tätä kutsutaan **rekonsilioinniksi** (engl. *reconciliation*). Sen tarkoituksena on pitää keskitetyssä IdM-palvelussa sekä kohdejärjestelmissä oleva tieto mahdollisimman yhdenmukaisena. Tyypillisesti identiteettitiedon auktoritatiivisena lähteenä pidetään IdM-palvelua, jolloin kaikki sen ohi tehdyt muutokset kohdejärjestelmissä olevaan identiteettitietoon pyritään estämään tai peruuttamaan. Toisaalta osa käyttäjän identiteettiin liittyvistä attribuuteista, esimerkiksi puhelinnumero, saatetaan hallita toisaalla. Tässä tapauksessa rekonsilointiprosessin tehtävänä voi olla ajantasaisten puhelinnumeroiden välittäminen IdM-palveluun.

3.5. Loppukäyttäjän käyttöliittymä

Identiteetinhallinnan palvelu tarjoaa loppukäyttäjäkunnalle vähintäänkin mahdollisuuden nähdä ja hallita omia tietojaan. Tyypillisesti esimiesasemassa olevat henkilöt voivat niinkään nähdä ja hallita alaistensa tietoja. Käytännössä tämä useimmiten tarkoittaa henkilötietojen sekä voimassaolevien käyttövaltuuksien katselua ja/tai raportointia, uusien käyttövaltuuksien pyytämistä, sekä käyttövaltuuspyyntöjen seuranta ja hyväksymistä.

Osa identiteetinhallinnan palveluista tarjoaa loppukäyttäjille myös mahdollisuuden mallintaa ja hallita palvelun piirissä olevia käyttövaltuusrakenteita, sekä niihin liittyviä sääntöjä, rajoitteita ja työnkuluja. Tällöin – ja vain tällöin – identiteetinhallinta voidaan aidosti delegoida käyttäjäorganisaatioon, eikä erillistä ”käyttöoikeustoimistoa” tai muita käyttövaltuuksien hallintaan omistautuneita resursseja välttämättä tarvita. Roolipohjaisissa (engl. *role-based*) IdM-palveluissa tämä käytännössä tarkoittaa roolimallin ylläpitoa. Esimerkiksi sovelluksen omistaja voi itse hallita kyseiseen sovellukseen käyttämiä järjestelmärooleja sekä niihin liittyviä käyttövaltuuksia.

Loppukäyttäjillä tarkoitetaan tässä yhteydessä vähintäänkin organisaation omia työntekijöitä, mutta yhä useammin myös erilaisia ”ulkoisia käyttäjiä”, kuten alihankkijoita, kumppaneita, asiakkaita tai vaikkapa ulkopuolisia auditoijia. Tyypillisesti oman organisaation ulkopuolisille käyttäjille tarjotaan vain rajattu joukko toiminnallisuksia.

Haku	Tiedot	Käyttäjätunnukset	Alaiset	Käyttäjärühmät	Käyttöoikeudet	Hallinnoitavat palvelut	Raportit
KÄYTTÄJÄTILI							
«« »» Cardassian Steven (Tuotantojohtaja)							
Käyttäjätilin käyttöoikeudet							
		<< Edelliset		Tulokset 1-10		Seuraavat >>	
						Hakutuloksia sivulle: 10	
Palvelu	Järjestelmärooli/Rooliryhmä(*)	Käyttäjärühmä	Voimassa alkaen	Voimassa saakka	Tila		
Asiakashallintapalvelu	CRM bonus	Henkilöstöjohtajat			Aktiivinen		
Asiakashallintapalvelu	CRM peruskäyttäjä	Henkilöstöjohtajat			Aktiivinen		
HR Palvelu	HR esimies	Henkilöstöjohtajat			Aktiivinen		
HR Palvelu	HR omistaja	Henkilöstöjohtajat			Aktiivinen		
HR Palvelu	HR osasto	Henkilöstöjohtajat			Aktiivinen		
HR Palvelu	HR työntekijä	Henkilöstöjohtajat			Aktiivinen		
ERP palvelu	ERP peruskäyttäjä	Henkilöstöjohtajat			Aktiivinen		
Laskentatoimipalvelu	FA peruskäyttäjä	Henkilöstöjohtajat			Aktiivinen		
Toimistoautomaatiopalvelu	OA peruskäyttäjä	Henkilöstöjohtajat			Aktiivinen		
Business Intelligence palvelu	BI peruskäyttäjä	Henkilöstöjohtajat			Aktiivinen		
Lisää käyttöoikeus							

Kuva 3 Esimerkki loppukäyttäjän käyttöliittymästä

Identiteetinhallinnan käytännön toimivuuden kannalta loppukäyttäjän käyttöliittymän **helppokäyttöisyys** (engl. *usability*) on ensiarvoisen tärkeä seikka. Identiteetinhallinnan delegointi loppukäyttäjille on mahdollista vain, mikäli heille tarjottava käyttöliittymä on riittävän selkeä ja intuitiivinen. Loppukäyttäjän käyttöliittymä voidaan myös integroida osaksi yritysportaalia tai sähköistä työpöytää mahdollisimman saumattoman käyttökokemuksen saavuttamiseksi.

3.6. Hallintakäyttöliittymä

IdM-palvelun ylläpitohenkilöstölle tarjotaan tyypillisesti erillinen käyttöliittymä palveluun liittyvän konfiguraation hallitsemiseksi. Toisin kuin loppukäyttäjän käyttöliittymä, hallintakäyttöliittymä edellyttää useimmiten perehtyneisyyttä palvelun taustalla oleviin tuotteisiin ja teknologioihin.

3.7. Sovellusrajapinnat

Identiteetinhallinnan palveluita on joskus tarpeen käyttää myös muista sovelluksista tai palveluista käsin. Keskitetty IdM-palvelu voi näin ollen tarjota erilaisia sovellusrajapintoja (engl. *application programming interface, API*) muiden sovellusten ja palveluiden käyttöön.

Sovellusrajapinta saattaa esimerkiksi tarjota samoja, käyttäjien ja käyttövaltuuksien hallintaan tarkoitettuja toimintoja kuin loppukäyttäjän käyttöliittymä. Sovellusrajapinnan käyttö tässä tarkoituksessa mahdollistaa esimerkiksi GRC-ratkaisun¹ liittämisen IdM-palveluun.

Toisaalta sovellusrajapinta voi tarjota mahdollisuuden valtuutus päätösten ulkoistamiseen yksittäisistä kohdejärjestelmistä. Esimerkiksi asiakkuudenhallintajärjestelmä voi rajapinnan kautta tiedustella onko käyttäjällä "X" oikeus nähdä asiakkaan "Y" tiedot. Tällöin IdM-palvelu vastaa keskitetysti valtuutus päätösten tekemisestä – noudattaen organisaatiossa määriteltyjä menettelytapoja ja sääntöjä. Tällainen ratkaisu laajentaa IdM-palvelun sisältöä pääsynhallinnan (ks. kappale 2) puolelle. Yleisin tämän kaltaisen sovellusrajapinnan toteutuksessa käytetyistä standardeista on XACML (*eXtensible Access Control Markup Language*).

Huomaa, ettei keskitetty identiteetinhallinnan palvelu välttämättä edellytä sovellusrajapintojen tarjoamista, ts. rajapinnat ovat valinnainen komponentti IdM-palvelussa.

¹ GRC-termillä (engl. *governance, risk management and compliance*) viitataan tässä yhteydessä identiteetinhallinnan yläpuolella olevaan "bisneskontrollikerrokseen", joka sanelee miten identiteettejä ja käyttövaltuuksia hallitaan. GRC:n piiriin kuuluu esimerkiksi erilaisten menettelytapojen (engl. *policy*) ja vaarallisten työyhdistelmien (engl. *segregation of duties*) määrittäminen liiketoiminnan näkökulmasta. Tällöin IdM-palvelun tehtävänä on lähinnä toimeenpanna tai soveltaa edellä mainittuja määrittämiä käytännössä.

4. Secproof identiteetinhallinnan asiantuntijana

Onko oma organisaatiosi maksimoinut identiteetinhallinnan kautta saavutettavat hyödyt? Kaipaatko osaavaa kumppania keskitetyn IdM-palvelun kehittämisessä? Ota meihin yhteyttä, kerromme mielellämme lisää. Ohessa vahvuuksiamme:

✓ **Asiantuntemus ja kokemus**

Identiteetinhallinta on ydinosamistamme. Kaikki IdM-asiantuntijamme ovat kokeneita tekijöitä, joilla on takanaan useiden vuosien käytännön kokemus identiteetinhallinnan hankkeista. Tunnetta alan teknologiat ja niiden tarjoamat mahdollisuudet – samoin kuin niiden asettamat rajoitukset. Osaamme myös kertoa, miten kehityshanke kannattaa vaiheistaa, jotta se tuottaa konkreettista hyötyä mahdollisimman nopeasti.

✓ **Rehellisyys ja puolueettomuus**

Olemme riippumattomia yksittäisistä teknologioista tai toimittajista. Emme edusta yksittäisiä tuotteita tai kaupaa lisenssejä. Tehtävämme on varmistaa, että Sinä saat parhaan mahdollisen ratkaisun. Sanomme suoraan mikäli näemme, että joku asia kannattaa tehdä toisin – tai jopa jättää kokonaan tekemättä. Osaamme myös perustella mielipiteemme.

✓ **Käytännönläheisyys**

Akateemisten paperiharjoitusten sijasta pyrimme saavuttamaan konkreettisia tuloksia – nopeasti ja tehokkaasti. Näkemyksemme mukaan toimeksianto on onnistunut vain, jos se johtaa mitattaviin kustannussäästöihin ja/tai pienentää aidosti liiketoiminnan riskejä.

✓ **Monipuolisuus**

Secproof on myös riskienhallinnan, jatkuvuussuunnittelun, tietoturvan sekä arkkitehtuuri-suunnittelun tunnustettu ammattilainen. Yhdessä identiteetinhallinnan osaamisen kanssa voimme tarjota asiakkaillemme kokonaisvaltaisen näkemyksen yhdeltä luukulta.

Yhteystietomme:



Hannu Kasanen

Head of Architecture

Puhelin: 050 531 1144

Sähköposti: hannu.kasanen@secproof.com



Ismo Sillanpää

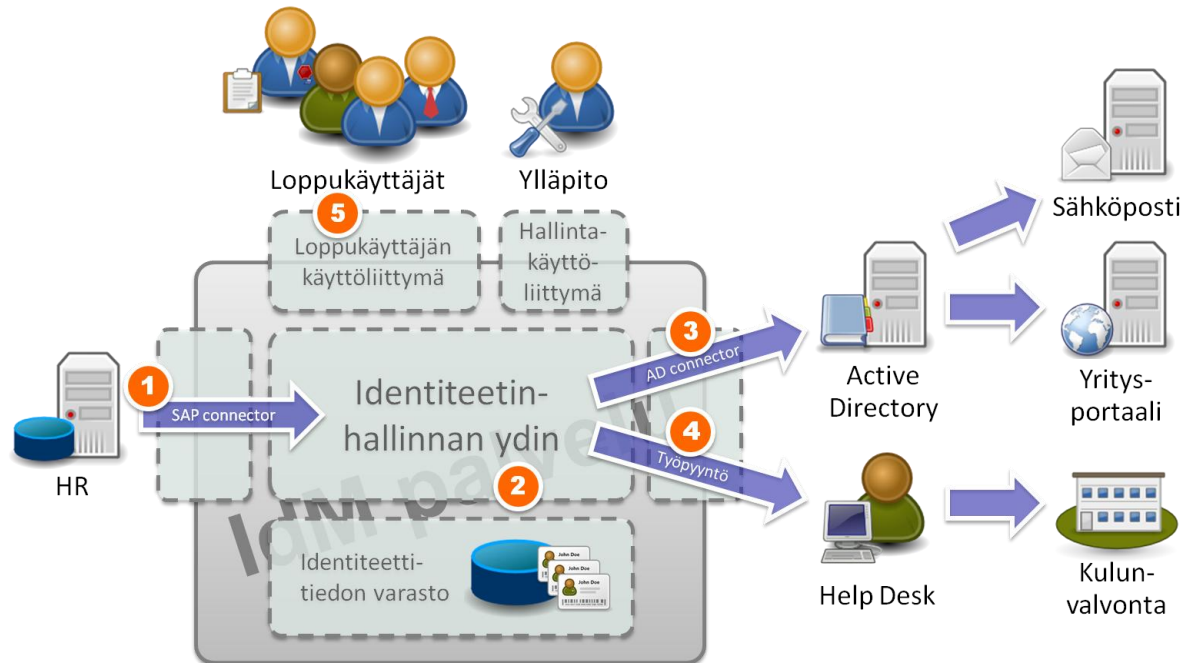
Sales Director

Puhelin: 0500 413 822

Sähköposti: ismo.sillanpaa@secproof.com

Liite: Esimerkki keskitetystä IdM-palvelusta

Tässä liitteessä on kuvattu esimerkin avulla kuinka keskitettyä identiteetinhallinnan palvelua voidaan hyödyntää uusien työntekijöiden käyttövaltuuksien myöntämisessä.



Kuva Esimerkki keskitetystä IdM-palvelusta

Yllä oleva kuva havainnollistaa uuden työntekijän sisäänajoon (engl. *onboarding*) liittyviä prosesseja.

1. Uuden työntekijän tiedot lisätään yrityksen HR-järjestelmään, joka toimii auktoritatiivisena lähdejärjestelmänä IdM-palvelulle. Tässä esimerkissä HR-järjestelmän toteutus perustuu SAP®-teknologiaan, johon identiteetinhallinnan järjestelmä voi kytkeytyä sopivaa liitintä (engl. *connector*) käyttäen. Näin HR-järjestelmään talletetut tiedot henkilöstä ja hänen työsuhteestaan välittyvät automaattisesti IdM-palvelulle.
2. IdM-palvelu luo välittömästi uudelle työntekijälle sähköisen identiteetin – mukaan lukien yksilöllisen käyttäjätunnuksen ja sähköpostiosoitteen – ja tallettaa nämä tiedot IdM-palvelun omaan tietovarastoon. Identiteetin ja siihen liitettävien attribuuttien luonnissa käytetään HR-järjestelmästä saatuja tietoja.
3. IdM-palvelu luo uudelle työntekijälle automaattisesti käyttäjätilin yrityksen keskitettyyn käyttäjähakemistoon, joka tässä esimerkissä on Microsoft® Active Directory®. Lisäksi työntekijä lisätään jäseneksi sopiviin ryhmiin em. hakemistossa. Lopputuloksena uusi työntekijä voi kirjautua omalta työasemaltaan yrityksen sisäverkkossa tarjottaviin palveluihin, kuten sähköpostiin ja yritysportaaliin.
4. IdM-palvelu lähettää yrityksen Help Deskiin työpyynnön kulkuoikeuksien myöntämiseksi uudelle työntekijälle. Help Desk toimittaa työntekijän tarvitseman henkilö- tai kulkukortin sekä lisää pyydetyt kulkuoikeudet (manuaalisesti) yrityksen kulunvalvontajärjestelmään. Kulkuoikeudet myönnetään automaattisesti vain siihen toimipisteeseen, jossa työntekijä pääsääntöisesti työskentelee.
5. Edellä mainittujen, automaattisesti myönnettävien käyttövaltuuksien lisäksi työntekijä voi loppukäyttäjän käyttöliittymän kautta pyytää itselleen muita toimenkuvansa edellyttämiä käyttövaltuuksia. Tällöin pyyntö ohjautuu hyväksyttäväksi työntekijän esimiehelle ja/tai muulle.

työnkulussa määritellylle taholle. Työntekijä voi itse seurata pyynnön etenemistä käyttöliittymän kautta. **Huom:** Yksittäisten käyttövaltuuksien sijasta työntekijä voi pyytää – ja hänelle voidaan myöntää – rooli, jonka seurauksena hän saa kerralla *kaikki* kyseiseen rooliin liitetyt käyttövaltuudet. Esimerkiksi "Controller" roolin omaavalla työntekijällä tulee olla pääsy yrityksen taloushallinnon järjestelmiin ja tilinpäätöstietoihin – riippumatta siitä missä tietojärjestelmissä näitä tietoja säilytetään.

Edellä kuvatun toiminnallisuuden perimmäisenä tarkoituksena on mahdollistaa uuden työntekijän pääsy tuottavaan työhön mahdollisimman nopeasti ja helposti. Tavoitteena on, että työntekijä pääsee käyttämään organisaation tarjoamia peruspalveluita (kuten sähköpostia) heti ensimmäisestä työpäivästä alkaen. Toisaalta identiteetinhallinnan keskittäminen ja automatisointi auttaa välttämään turhia tai virheellisiä käyttövaltuuksia, mikä on omiaan minimoimaan yrityksen riskejä.

