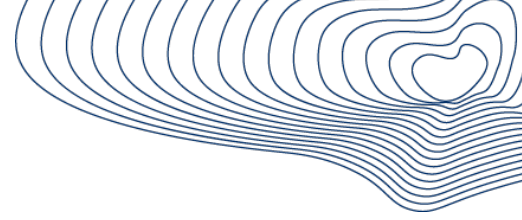




IDENTITEETINHALLINTA

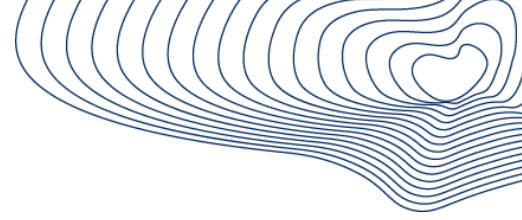
2025

Trivoren pikaopas



IDENTITEETINHALLINTA VUONNA 2025

Digitaalisen identiteetin merkitys kasvaa jatkuvasti. Kun organisaatiot siirtyvät yhä vahvemmin pilvipohjaisiin ja hajautettuihin toimintaympäristöihin, tulee identiteetinhallinnasta yhä keskeisempi osa digitaalista turvallisuutta. Samalla kyberuhkien kehittyminen pakottaa organisaatiot uudistamaan lähestymistapojaan identiteetinhallintaan.



Sisältö

Identiteetinhallinta vuonna 2025.....	1
Trendit, jotka muovaavat yritysten digitaalista turvallisuutta	3
Integraatiot ja Identity Fabric	3
Uudet teknologiat: Passwordless ja tekoäly	4
Hajautetut identiteetit ja lisääntynyt tietosuojatietoisuus	5
Sääntelyvaatimukset muokkaavat identiteetinhallintaa	6
Mitä tulevaisuus tuo tullessaan?	7
Trivore tekee trendeistä totta.....	8



Trendit, jotka muovaavat yritysten digitaalista turvallisuutta

Nostimme tähän oppaaseen alkaneen vuoden identiteetinhallinnan trendejä, jotka muovaavat yritysten digitaalista turvallisuutta.

Integraatiot ja Identity Fabric

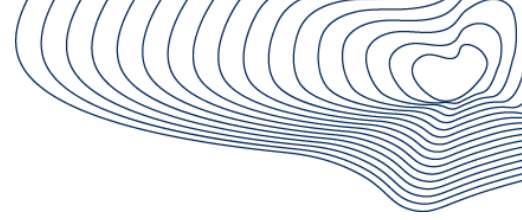
Identity Fabric -ajattelu on viime vuosina noussut keskeiseksi trendiksi identiteetinhallinnassa. Tällaiset ratkaisut mahdollistavat identiteettien yhtenäisen hallinnan hajautetuissa ympäristöissä. Ne yhdistävät liiketoimintaprosessit, IAM-työkalut ja käyttäjätiedot API-rajapintojen ja standardoitujen protokollien avulla. Tämä luo perustan paremmalle skaalautuvuudelle ja säädöstenmukaisuudelle. Kyse ei siis ole vain teknologiasta, vaan kyvystä yhdistää eri järjestelmät ja prosessit saumattomaksi kokonaisuudeksi. Tämä on erityisen tärkeää Suomen kaltaisilla markkinoilla, joissa organisaatioilla on usein käytössään lukuisia eri-ikäisiä järjestelmiä.

Modernissa Identity Fabric -arkkitehtuurissa integraatiot toteutetaan mikropalvelupohjaisesti ja kontitetusti. Tämä mahdollistaa joustavan käyttöönoton ja päivitykset sekä tehokkaan skaalautumisen tarpeen mukaan. Erityisen tärkeää on kyky integroida sekä pilvipalvelut että organisaation omat järjestelmät samaan kokonaisuuteen.

Integraatioiden keskeisiä ominaisuuksia ovat:

- Kattava API-kerros, joka mahdollistaa identiteettipalveluiden joustavan hyödyntämisen
- Vahva tuki standardeille kuten SAML, OAuth ja OIDC
- Kyky yhdistää vanhemmat järjestelmät moderniin IAM-infrastruktuuriin
- Joustava orkestrointi eri identiteettilähteiden ja -palveluiden välillä
- Skaalautuva arkkitehtuuri, joka tukee sekä pieniä että suuria käyttäjämääriä

Identity Fabric ei edellytä kaikkien järjestelmien välitöntä uusimista. Sen sijaan organisaatiot voivat edetä vaiheittain, integroiden uusia ja vanhoja järjestelmiä hallitusti kokonaisuuteen. Tämä mahdollistaa investointien järkevän ajoituksen ja riskienhallinnan.



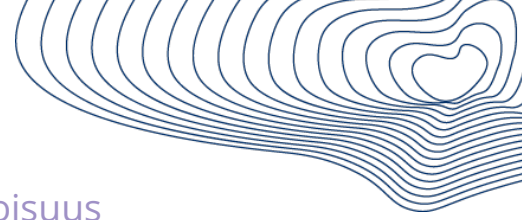
Uudet teknologiat: Passwordless ja tekoäly

Perinteisten salasanojen aika on loppumassa. Passwordless tarkoittaa teknologiaa tai menetelmää, jolla käyttäjien todennus tapahtuu ilman salasanojen käyttöä. Se on laajempi konsepti, joka tarkoittaa kirjautumista ja pääsynhallintaa käyttäen vaihtoehtoisia todennusmenetelmiä, kuten:

- **Biometria**, eli sormenjäljet, kasvotunnistus tai äänen tunnistus.
- **Kertakäyttöiset koodit (OTP)**, jotka lähetetään esimerkiksi sähköpostitse tai tekstiviestillä.
- **Push-ilmoitukset**, eli käyttäjän mobiililaitteelle lähetettävä hyväksymispyyntö.
- **Linkkikirjautuminen**, eli käyttäjälle sähköpostitse lähetettävä suora linkki, joka ei vaadi salasanaa.

Näiden käyttö tulee kasvamaan vuoden 2025 aikana. Nämä menetelmät eivät pelkästään paranna turvallisuutta, vaan myös käyttäjäkokemusta, poistamalla salasanojen muistamisen ja hallinnan tarpeen.

Samalla tekoäly tehostaa identiteetinhallintaa. Sen avulla voidaan tunnistaa poikkeavia käyttäytymismalleja, automatisoida päätöksentekoa ja suojautua uhkilta, kuten AI-aikakaudella yleistyviltä deepfake-tekniikoita käyttäviltä hyökkäyksiltä.



Hajautetut identiteetit ja lisääntynyt tietosuojatietoisuus

Hajautetut identiteettijärjestelmät (DID) ja lohkoketjuteknologiaan perustuvat ratkaisut muuttavat perustavanlaatuisesti tapaamme hallita digitaalisia identiteettejä. Ne antavat käyttäjille aiempaa paremman kontrollin omiin tietoihinsa, mikä on linjassa sekä GDPR:n vaatimusten että yleisen tietosuojatietoisuuden kasvun kanssa.

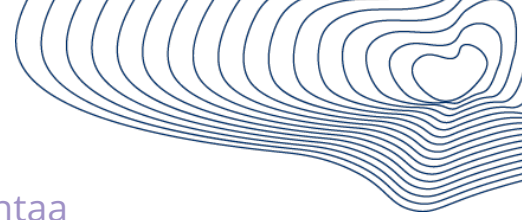
Tämän kehityksen merkitys korostuu jatkossa erityisesti monimutkaisissa B2B- ja kumppaniverkostoissa. Organisaatiot voivat hyödyntää hajautettuja identiteettejä rakentaessaan luottamusverkostoja, joissa identiteettitietoa voidaan jakaa turvallisesti ja läpinäkyvästi. Samalla käyttäjille voidaan antaa todellinen mahdollisuus hallita omien tietojensa käyttöä ja jakamista.

Keskeisiä kehityssuuntia ovat:

- Identiteettilompakoiden (identity wallets) yleistyminen
- Itse hallitut identiteetit (SSI; self-sovereign identity), jotka ovat olennainen osa EU:n digitaalisten lompakoiden (EU Digital Wallets) käsitettä
- Hajautetut luottamusverkostot
- Organisaatorajat ylittävä identiteettien federaatio
- Vahvistettujen tietojen (verified credentials) hyödyntäminen

Tämä kehitys tukee myös kasvavaa tarvetta skaalautuviin ratkaisuihin suurille käyttäjämäärille. Hajautetut järjestelmät mahdollistavat identiteettien turvallisen hallinnan ilman keskitettyjä pullonkauloja tai yksittäisiä haavoittuvuuspisteitä.

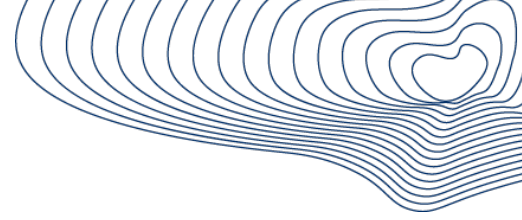
Organisaatioiden kannattaa seurata tätä kehitystä tarkasti ja arvioida, miten hajautetut identiteetit voivat tehostaa niiden toimintaa ja parantaa tietosuojaa. Erityisen tärkeää on varmistaa, että identiteetinhallintaratkaisut tukevat näitä uusia teknologioita ja standardeja.



Säätelyvaatimukset muokkaavat identiteetinhallintaa

Identiteetinhallinnasta on tullut keskeinen osa säädöstenmukaisuutta. EU:n NIS2-direktiivi asettaa uusia vaatimuksia kriittisen infrastruktuurin kyberturvallisuudelle, ja DSA (Digital Services Act) tuo lisävelvoitteita digitaalisten palvelujen tarjoajille. Finanssisektorilla PSD2-direktiivi on jo muuttanut vahvan tunnistautumisen vaatimuksia, ja tulevat EU:n AI-regulaatiot tulevat vaikuttamaan tekoälyn käyttöön identiteetinhallinnassa. Finanssisektoriin vaikuttavat myös vuoden 2023 DORA-säädökset (Digital Operations Resilience Act), jotka tulivat voimaan vuoden 2025 tammikuussa.

Nämä säädökset eivät ole vain vaatimuksia, vaan ne ohjaavat kehitystä kohti turvallisempaa ja läpinäkyvämpää digitaalista ympäristöä. Samalla säädösten noudattamisesta on tullut merkittävä kilpailuetu, kun organisaatiot haluavat varmistaa digitaalisten palvelujensa jatkuvuuden.



Mitä tulevaisuus tuo tullessaan?

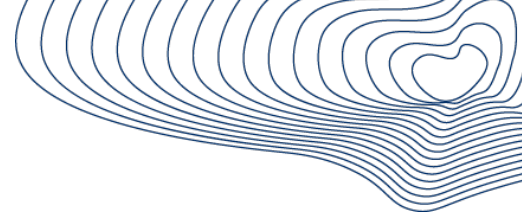
Identiteetinhallinnan tulevaisuus rakentuu siis vahvasti integraatioiden, automaation ja älykkään teknologian varaan. Keskeistä on löytää tasapaino kolmen kriittisen tekijän välillä: tietoturvan, käytettävyyden ja kustannustehokkuuden.

Organisaatioiden toimintaympäristö muuttuu jatkuvasti monimutkaisemmaksi. Pilvipalvelujen lisääntyminen, hajautetut työympäristöt ja kasvavat sääntelyvaatimukset edellyttävät uudenlaista lähestymistapaa identiteetinhallintaan. Identity Fabric tarjoaa tähän käytännönläheisen ratkaisun.

Samalla on selvää, että identiteetinhallinta ei ole enää pelkkä tukitoiminto vaan strateginen voimavara, joka:

- Mahdollistaa liiketoiminnan digitalisaation
- Tehostaa organisaation toimintaa
- Parantaa tietoturvaa
- Tukee organisaation kasvua ja muuntautumiskykyä

Onnistunut identiteetinhallinta edellyttää siis jatkossakin selkeää näkemystä, vahvaa arkkitehtuuria ja kykyä toteuttaa muutokset hallitusti.



Trivore tekee trendeistä totta

Trivore on jo vuosia ollut eturintamassa rakentamassa vaativille organisaatioille moderneja identiteetinhallinnan ratkaisuja. Identity Fabric -ajattelutapa on meille tuttu – olemmehan toteuttaneet lukuisia monimutkaisia IAM-integraatioita, joissa vanhat ja uudet järjestelmät on tuotu saumattomasti yhteen. Mikropalvelupohjainen arkkitehtuurimme ja vahva API-osaamisemme mahdollistavat juuri sellaisen joustavuuden, jota organisaatiot tarvitsevat muuttuvassa toimintaympäristössä.

Haluatko sinäkin varmistaa, että organisaatiosi identiteetinhallinta vastaa tulevaisuuden haasteisiin? Ota yhteyttä, niin keskustellaan, miten voimme auttaa juuri teidän organisaatiotanne rakentamaan kestävän pohjan digitaaliselle kasvulle.