



## Loogisen ja fyysisen tietoturvallisuuden yhdistäminen

### Fyysinen ja looginen tunnistus

Fyysisellä tunnistuksella tarkoitetaan kulun- ja pääsynvalvontaa tiloihin ja rakennuksiin. Sen avulla varmistutaan siitä, että vain oikeutetut henkilöt voivat liikkua organisaation tiloissa. Loogisella tunnistuksella tarkoitetaan pääsynvalvontaa eri tietojärjestelmiin ja sen avulla varmistutaan siitä, että vain oikeutetut käyttäjät voivat päästä sisään organisaation tietoverkkoihin ja tietojärjestelmiin. Perinteisesti nämä kaksi tunnistamisen osa-aluetta ovat olleet toisistaan erillään johtuen erialaisista toiminnallisista ja hallinnollisista tarpeista sekä toimintatavoista.

Loogisesta ja fyysisestä pääsynvalvonnasta vastaavien yksiköiden keskeinen tehtävä on yrityksen luottamuksellisen tiedon suojaaminen. Rajoitetut budjetit ja tekniset päällekkäisyydet luovat paineita näiden molempien toiminnallisuuksien yhdistämiseksi. Loogisen ja fyysisen turvallisuuden järjestelmien yhteistyö ei aina ole saumatonta, vaikka niiden tavoite onkin yhteinen.

Nyt uudet tekniset ja sovellukselliset ratkaisut mahdollistavat kaikkien eri tunnistustoimintojen älykkään ja joustavan yhdistämisen toisiinsa. Tämä auttaa parantamaan turvallisten toimintatapojen käytettävyyttä ja hallinnoitavuutta sekä nostamaan organisaation turvallisuustasoa edullisesti ja nopeasti koska jo tehtyjä turvainvestointeja voidaan hyödyntää joustavasti, jolloin suurilta lisäinvestoinneilta voidaan välttyä.

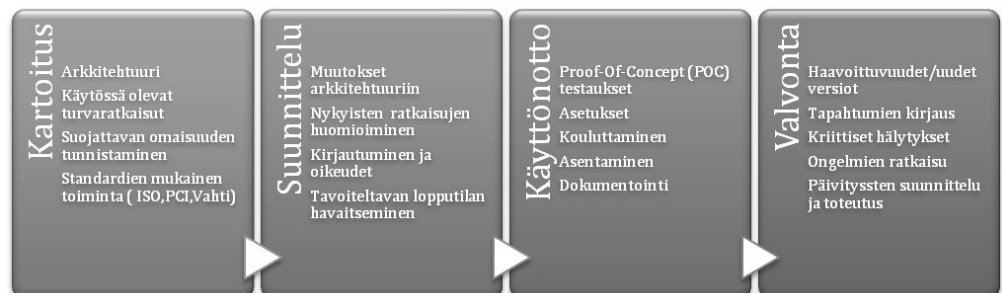
### Lisää turvallisuutta

Fyysisten ja loogisten käyttäjätilien hallinnoinnin ja käytön yhdistäminen samaan järjestelmään lisää tietoturvallisuuden hallittavuutta ja toimivuutta sekä pienentää pääsynvalvonnan aiheuttamia kuluja. Myös tietoturvallisuuden valvonta ja seuranta parantuvat. Yhdistetyt valvontamonitoirinnit mahdollistavat edistyneen käyttäjätilien käytön seurannan ja mahdollisten tietovuotojen tutkimisen jälkikäteen.

### Turvallinen kehityspolku

Useat viimeaikoina toteutetut tutkimukset, sekä käyttöönotetut standardit ohjaavat organisaatioita turvallisempaan käyttäjien identiteettien hallintaan. Tärkeimpiä vaiheita standardien mukaisen identiteettihallinnan saavuttamiseksi ovat uusien käyttäjien luominen, kadonneiden tunnusten muuttaminen/poistaminen, sekä poistuvien käyttäjien poistaminen. Hajautetussa järjestelmässä kyseinen prosessi tulee toteuttaa useaan otteeseen, mutta keskitetysti hallittu järjestelmä mahdollistaa käyttäjän keskitetyn poistamisen organisaation pääsynvalvonnasta.

Kun looginen ja fyysinen pääsynvalvonta yhdistetään, keskeinen edellytys on, että samaa ID-korttia hyödynnetään molemmissa tarkoituksissa.





Tyypillisesti fyysinen pääsynvalvonta on toteutettu käyttäen edullisia tallennusvälineitä (RFID), kun taas looginen pääsynvalvonta perustuu varmennepohjaiseen älykorttitekologiaan, joka on monesti kalliimpaa kuin RFID. Varmenne toimii käyttäjillä eräänlaisena sähköisenä passina, jolla pääsy organisaation tietojärjestelmiin voidaan toteuttaa varmistetusti ja luotettavasti.

Organisaatiot tukeutuvat ja luottavat usein edelleen vaikeasti hallittaviin ja jatkuvia ylläpitokustannuksia aiheuttaviin käyttäjätunnus/salasanaperusteisiin tunnistukseen, jonka turvallisuuden ja käytettävyyden rajoitukset ovat alati kasvava haaste ja kustannuspaikka. Salasanoihin pohjautuvien järjestelmien päivittäminen nykyaikaisiin varmennepohjaisiin ratkaisuihin voi olla kuitenkin liian suuri kerta harppaus jolloin myös väliportaan ratkaisuja tarvitaan. Julkisen avaimen varmennemenetelmään pohjautuvat pääsynvalvonnan järjestelmät mahdollistavat organisaatiolle standardien mukaisen ja luotettavan käyttäjätunnusten pysyvän ja/tai väliaikaisen eston.

### **Ratkaisu yhdistelmäkortissa**

Yhtenäinen järjestelmä voidaan ottaa käyttöön erilaisten yhdistelmäkorttien avulla. Suurin osa markkinoilla toimivista korttivalmistajista toimittavat yhdistelmäkoritteja. Yhdistelmäkortin avulla käyttäjä tunnistautuu ovelta saapuessaan työpaikalleen. Tämän jälkeen käyttäjä hyödyntää samaa ID-korttia kirjautuessaan työasemaltaan organisaation tietoverkkoon, sekä mahdollisesti myös useisiin taustajärjestelmiin käyttäen turvallista kertakirjautumista.

Poistuessaan työasemaltaan työntekijä tarvitsee ID-korttiaan ovien aukaisemiseen ja näin ollen hän ottaa

korttinsa pois työaseman kortinlukijasta jolloin työasema lukkiutuu käyttäjän poistuessa työpisteeltään. Palattuun työpisteelle käyttäjä avaa taas työpöytänsä ja ohjelmistojensa lukituksen omalla kortillaan. Edistykselliseen yhdistelmäkorttiin voidaan tarvittaessa liittää myös muita tarvittavia sovelluksia. Tällaisia ovat esimerkiksi työajanseuranta, työpaikkaruokailun maksaminen, sekä muut tunnistusta vaativat maksu- tai muut palvelut. Eri palveluiden ja sovellusten yhdistäminen yhdelle ID-kortille helpottaa palvelujen käyttöä, lisää organisaation tietoturva sekä alentaa hallinnasta ja käytöstä aiheutuvia kuluja samalla kertaa.

### **Toimiva kokonaisratkaisu**

Fyysisen ja loogisen pääsynvalvonnan yhdistäminen on muutakin kuin tekniikkaa - mukana on oltava myös liiketoimintaprosessien ja identiteetinhallinnan prosessien kehittämistä. Organisaatiokortin hyödyntäminen on turhaa jos rekisteröintiprosessiin, käytettävyyteen ja vaikuttavuuteen ei ole kiinnitetty riittävä huomiota. Secure Link Oy:n sertifioidut tietoturva-ammattilaiset auttavat toteuttamaan pääsynvalvonnan ja identiteetinhallinnan hankkeet erilaisissa ympäristöissä. Asiantuntijamme auttavat organisaatiota edistyksellisen pääsynvalvonnan toteutuksessa kaikissa eri vaiheissa.

***Tutustu palveluihimme osoitteessa [www.securelink.fi](http://www.securelink.fi) ja ota yhteyttä niin kerromme miten organisaatiosi voi kehittää tietoturvasuutta nopeasti ja kustannustehokkaasti.***