

Turvallisuus ja luotettavuus ovat kaikkein tärkeimpiä pääsyoikeuksien myöntämiseen ja jakamiseen – eli lukkoihin ja avaimiin – liittyviä tekijöitä. Niiden merkitys korostuu entisestään lukkoalan muuttuessa yhä digitaalisemmaksi. Suunnitelumme perustana on aina ollut erinomaisen asiakaskokemuksen ja alan parhaan turvallisuuden yhdistäminen sekä fyysisessä että virtuaalisessa maailmassa.

Teknologia-katsaus



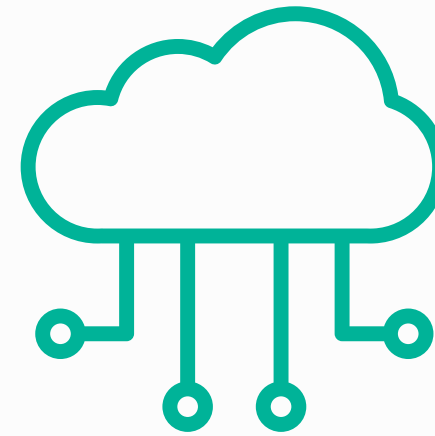
Turvallisuuden varmistaminen digitalisaation edetessä



Pääasiakkaana teknisen infrastruktuurin yritykset

iLOQ S50 oli vuoden 2018 tärkein uusi teknologiajulkistuksemme. Tuote julkistettiin vuoden toisella puoliskolla, ja ensimmäiset asennuskohteet ovat jo täydessä käytössä, kuten esimerkiksi uusi Telia Helsinki Data Center. Lisäksi neuvotteluja käydään useiden muidenkin kiinnostuneiden tahojen kanssa. Ilman avaimia toimiva, mobiilipohjainen pääsynhallintajärjestelmä on nopeasti osoittautumassa suosituksi ratkaisuksi. Se vastaa teknisen infrastruktuurin yritysten käytännön tarpeita, mutta täyttää myös niiden tarkat kyberturvallisuus- ja luotettavuusvaatimukset.

Teknisen infrastruktuurin yritysten kannalta ratkaisumme ytimessä on iLOQin pilvipohjainen ohjelmistoratkaisu. Turvallisen verkkoalustamme kautta voidaan tehokkaasti hallinnoida ja jakaa digitaalisia pääsyoikeuksia erilaisista lukoista koostuviin lukkoverkostoihin. Lisäksi pääsyoikeudet voidaan jakaa reaaliaikaisesti haluttuihin mobiililaitteisiin. Kun ratkaisu otetaan käyttöön, ei enää tarvita suurta joukkoa fyysisiä avaimia, eikä avainten jakamiseen kulu aikaa. Tätä potentiaaliset asiakkaamme arvostavat.



Korkea automatisointiaste ja mahdollisuus integraatioon muiden tietojärjestelmien kanssa on tärkeää monille asiakkaille.

Mobiilipohjainen pääsynhallinta-alustamme on sekä vakaa että joustava. Se mahdollistaa korkean automatisointiasteen ja sen voi integroida muiden tietojärjestelmien kanssa, mikä on tärkeää monille asiakkaille. Asiakkaiden tarpeiden ymmärtäminen ja toteuttaminen on sekä iLOQ S50 -ratkaisun että tuotekehitysosastomme toiminnan ydinajatus.

Kaikki alkaa lukosta

Kaikki mobiilikäyttöisen iLOQ S50 -pääsynhallintaratkaisun yhteydessä toimittamamme fyysiset, NFC-tekniikalla toimivat lukot on testattu perinpohjaisesti, jotta ne vastaisivat teknisen infrastruktuurin asiakkaidemme odotuksia. Ne toimivat ilman paristoja, mikä tekee niistä erittäin luotettavia ja käytännössä huoltovapaita. Kun perinteinen avaimenreikä korvataan NFC-lukijalla, lukkoon eivät vaikuta ika, jää tai muut ulkoiset tai säästä johtuvat tekijät.

iLOQin ohjelmapäällikkö Janne Heusala kertoo, että yksinkertaisuus on ollut pääperiaatteena kaikkien iLOQ-ratkaisujen suunnittelussa. "Kun asiat pidetään yksinkertaisina ja ne tehdään oikein, paljon vähemmän voi mennä pieleen." iLOQ on suunnitellut lukkonsa niin, että ne ovat mekaniikaltaan mahdollisimman yksinkertaisia, ja kaikki tärkeimmät osat on piilotettu lukkosylinterin sisään, mikä lisää turvallisuutta. Riippumatta siitä, etsitkö riippulukkoa, avainsäilön lukkosylinteriä tai oveen asennettavaa lukkosylinteriä, rakenne on pääpiirteittäin aina sama.



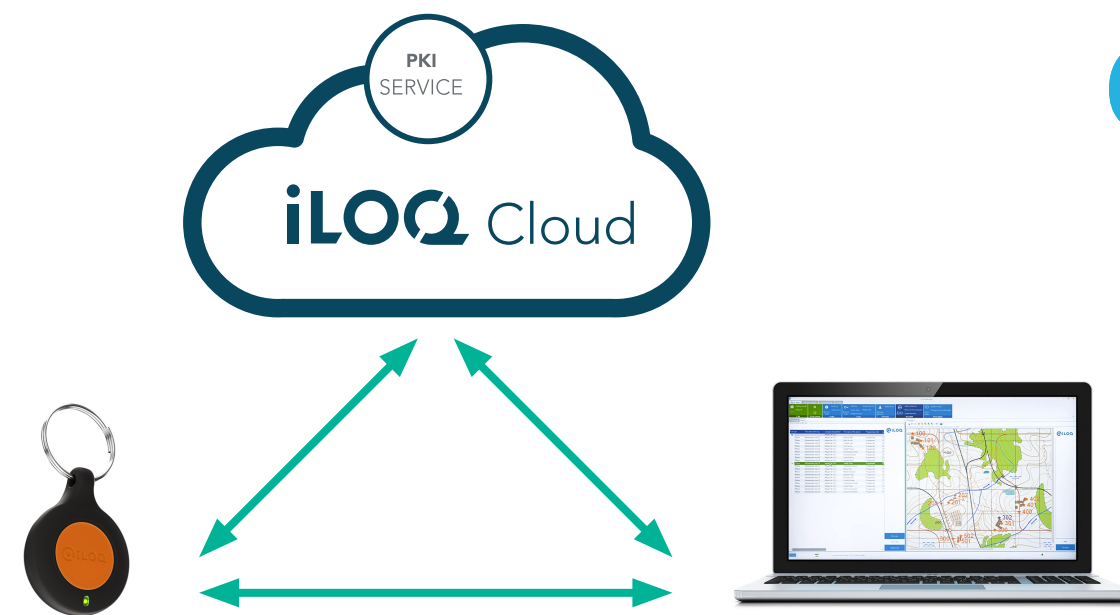
Kun asiat pidetään yksinkertaisina ja ne tehdään oikein, paljon vähemmän voi mennä vikaan."

Janne Heusala, ohjelmapäällikkö, iLOQ

Kyberturvallisuus on nyt kuuma aihe

Digitalisaatio ja automatisaatio valtaavat uusia alueita, ja niiden merkitys kasvaa. Samalla myös kyberturvallisuuteen liittyvistä huolista on käyty tiivistä keskustelua. Huolet ovat perusteltuja, koska digitaaliset ratkaisut ovat tyypillisesti vain niin hyviä kuin niiden takana oleva suunnittelutyö. Huolimatta median tekemistä yleistyksistä turvallisuus on kuitenkin usein yksi digitaalisia ja verkkopohjaisia ratkaisuja kehittävien yritysten pääprioriteeteista. Sitä se on myös iLOQilla.

iLOQ tunnetaan siitä, että se suhtautuu kyberturvallisuuteen tosissaan. Suosittu ja toimivaksi todettu digitaalinen iLOQ S10 -pääsynhallintaratkaisu on ollut markkinoilla jo yli kymmenen vuotta. iLOQ S50:n suunnittelutyö pohjautuu edellisestä mallista saatuihin kokemuksiin ja hyväksi havaittuihin suunnitteluperiaatteisiin. Janne Heusala selittää, miten iLOQ S50 on suojattu etähyökkäyksistä vastaan: "Ratkaisumme pitää sisällään sekä fyysisiä että digitaalisia turvakeinoja. Näin voimme varmistaa parhaan mahdollisen kyberturvallisuustason. Sekä kaapelia pitkin tapahtuvaan että langattomaan tiedonsiirtoon käytetään aina vahvaa AES 256 -salautusta, ja sen lisäksi iLOQ-ohjelmointiavain lisää järjestelmän tietoturvaan fyysisen tekijän. Fyysistä ohjelmointiavainta tarvitaan erityisen tärkeiden tietojen käsittelyyn, jotka sijaitsevat hajautetusti pilvipohjaisella asiakaspalvelimella ja iLOQ Manager -ohjelmistossa."



Ratkaisumme pitää sisällään sekä fyysisiä että digitaalisia turvakeinoja. Näin voimme varmistaa parhaan mahdollisen kyberturvallisuustason."

Janne Heusala, ohjelmapäällikkö, iLOQ

iLOQin tuotekehitysosasto on nähnyt paljon vaivaa luodakseen helpon ja sujuvan käyttäjäkokemuksen, joka palvelee asiakkaan tarpeita. Osastolla on tutkittu yhtä lailla iLOQ S50:n erilaisia käyttötapoja sekä sitä, miten järjestelmää voidaan väärinkäyttää. Mobiilisovellukset ja -laitteet ovat yleensä turvallisia, kunnes joku yrittää peukaloita tai hakkeroida laitetta. Tässä vaiheessa tietoturvaan pitää kiinnittää erityistä huomiota, ja sovelluksen sisäänrakennetut turvamekanismit ovat tärkeitä. "Valitettavasti emme voi laskea sen varaan, että kaikki toimivat rehellisesti. Siksi olemme tehneet paljon taustatyötä ja selvittäneet ja mallintaneet väärinkäyttötavat, jotta ratkaisumme turvallisuus ja toiminnallisuus voidaan varmistaa kaikissa olosuhteissa", Janne Heusala toteaa.

Turvallisuus on jatkuva prosessi

Me iLOQilla tiedämme, että lukkomme toimivat luotettavasti ja säilyttävät tietoturvasonsa pitkään asennuksen jälkeen. Mobiilipohjaisen ja digitaalisen ratkaisun kyberturvallisuuden ylläpito vaatii kuitenkin jatkuvaa työtä. "Digitaalisen teknologian kehitys tapahtuu yhä nopeammissa sykleissä, ja siksi meidän pitää pysyä hereillä ja valppaina", Janne Heusala tiivistää. "Meidän täytyy arvioida kaikkia tietoturvan muuttuvia ja kehittyviä riskejä ja pysyä kehityksen edellä." iLOQin tuotekehitysosasto tutkii kaikki Google- ja Android-ympäristöjen ohjelmistopäivitykset ja uudet ominaisuudet ja varmistaa, että ne eivät laske kyberturvallisuuden tasoa. iLOQ arvostaa sitä, että asiakkaat luottavat ratkaisuihimme ja yrityksemme, ja tavoitteenamme on olla tämän luottamuksen arvoisia joka päivä.



Digitaalisen teknologian kehitys tapahtuu yhä nopeammissa sykleissä, ja siksi meidän pitää pysyä hereillä ja valppaina."

Janne Heusala, ohjelmapäällikkö, iLOQ