Tunnista varmasti

– IDcontrol tunnistautumisopas

IDcontrol Oy | Lars Sonckin kaari 10, 02600 Espoo | 020 734 3225 | myynti@idcontrol.fi

Tunnistautuminen

IDcontrol Oy on tunnistautumisen teknologioiden edelläkävijä kehittämisessä, maahantuonnissa ja jälleenmyynnissä. Asiantuntijamme ovat koonneet tämän oppaan auttamaan oikean tunnistautumisteknologian valinnassa.

Tunnistautumista tarvitaan niin kuluvalvonnassa kuin logistiikassa. Tässä esitteessä käsittelemme kulunvalvonnan tunnistautumisen teknologioita.

Kulunvalvonnassa tunnistautumisen tarve on kasvanut jatkuvasti tiukentuvien turvamääräysten sekä toisaalta teknologian kehittymisen myötä. Markkinoilla onkin monia erilaisia teknisiä vaihtoehtoja tunnistautumisen toteuttamiseen. Jokaiseen kiinteistöön ja käyttötarkoitukseen löytyy oikea teknologia!

Tässä oppaassa käsittelemme seuraavia tunnistautumisen teknologioita:

- RFID-tunnistautuminen
- UHF-tunnistautuminen
- NFC/BLE-tunnistautuminen
- Biometriset tunnisteet (sormenjälki, kasvot, ääni, kämmen, retina)
- Magneettiraitatunnistautuminen
- Viivakooditunnistautuminen
- PIN-kooditunnistautuminen
- Yhdistelmätunnistautuminen

Sisällys

1

Turvallisuustasot

Tunnistautumista suunniteltaessa ensimmäisiä kysymyksiä on päättää tavoiteltu turvallisuuden taso. Korkeaa turvallisuuden tasoa tavoiteltaessa osa tunnistatumisen teknologioista putoaa pois vaihtoehtojen joukosta, joten on tärkeä määritellä ensin turvallisuuden vaatimukset.

Turvallisuustasot

Turvallisuustaso

Korkea

Matala

Tunnistautumisteknologiat

- Yhdistelmätunnistautuminen
- Biometriset tunnisteet (sormenjälki, kasvot, ääni, kämmen, retina)
- Mobiilitunnistautuminen (NFC+BLE)
- RFID-tunnistautuminen
- UHF-tunnistautuminen
- PIN-kooditunnistautuminen
- Magneettiraitatunnistautuminen
- Viivakooditunnistautuminen

RFID-tunnistautuminen

RFID-tunnistautumista voidaan pitää nykyisin yleisimpänä tunnistautumisen muotona. Se onkin luotettava ja edullinen, jo vuosikymmeniä käytössä ollut tunnistautumisen muoto. Itse asiassa se on niin yleinen ja käytössä niin monessa muodossa, että välttämättä kaikki käyttäjät eivät tiedä käyttävänsä RFID-tunnistautumista. RFID-tunnisteita ovat esimerkiksi erilaiset avaimenperät, muovikortit, rannekkeet ja uusimpana vaihtoehtona paperista valmistetut kortit ja rannekkeet.

Turvallisuuden näkökulmasta ei ole merkityksetöntä millainen RFID-tunniste valitaan käyttöön. Avaimenperä on esimerkiksi pieni ja anonyymi ja siten toisaalta turvallinen, mutta ulkopuolisen silmin mahdotonta on erottaa, onko tunnisteen haltija sama henkilö kuin kenelle tunniste on alun perin myönnetty. Tätä uhkaa voidaan pienentää esimerkiksi kuvallisilla henkilökorteilla, tai henkilökunnan ja vierailijat erottavan kortin tekemisellä. Nykyään kortteihin voidaan liittää myös esimerkiksi uv-valossa näkyviä vesileimoja, jolloin väärentäminen käy vaikeaksi.

Korkein turvallisuustaso saavutetaan yhdistelmätunnistautumisella, josta kerromme lisää omassa luvussaan.

RFID-tunnistautuminen on helpoin ja joustavin markkinoilla oleva tunnistautumisen teknologia ja se voidaan tehdä turvalliseksi. Esimerkiksi viivakooditunnisteen kopiointiin tarvitaan vain valokuva koodista, mutta varsinkin uudempien 13,56 MHz:n RFID-tunnisteiden, kuten SeoS- tai Desfire- muuttuva-avaimisten tunnisteiden, kopiointi on vaikeaa, jos ei aivan mahdotonta. Kun yrityksessä tai kiinteistössä tavoitellaan korkeaa turvallisuutta tunnistaumisessa, suosittelemme joko SeoS- tai Desfire- tunnisteiden käyttöä. Matalan taajuuden vanhempaa RFID-standardia ei puolestaan suositella turvatunnistautumista vaativiin kohteisiin, koska se on helposti kopioitavissa. Oikean turvallisuustason saavuttaminen RFID-tekniikalla edellyttääkin selkeää ymmärrystä tekniikan rajoitteista ja mahdollisuuksista yhdistelmätunnistautumiseen.

RFID-tunnistautuminen sopii hyvin lyhyillä matkoilla tapahtuvaan tunnistautumiseen, mutta pidempiä, muutaman metrin etäisyydellä tunnistautumisia varten tulee käyttää UHF-tunnistautumista.

RFID-tunnistautuminen toimii yhtä hyvin verkkoyhteyksiä hyödyntävissä kuin offline-kohteissa, vaikka tietysti verkon yli erilaiset ylläpitoon ja päivityksiin liittyvät tehtävät on helpompi suorittaa.

UHF-tunnistautuminen

UHF (Ultra High Frequency) kuuluu RFID-tunnistautumiseen. UHF-tunnistaumisen etuna on muita RFID-teknologioita pidempi toimintamatka. Kuitenkin UHF-tunnisteiden toiminta täytyy varmistaa asennuspaikkakohtaisesti, sillä UHF-signaali ei esimerkiksi aina kulje taskussa tai laukussa olevasta tunnisteesta lukijaan. UHF-tunnisteiden etuna on, että yhdistettynä oviautomatiikkaan niiden avulla voidaan rakentaa kontaktiton kulkeminen helposti.

UHF-tunnistautuminen voidaan jakaa useampaan luokkaan. Ensimmäinen erottava tekijä on se, käytetäänkö **aktiivisia** vai **passiivisia** tunnisteita. Näiden erona on, että aktiivisessa tunnisteessa on oma virtalähteensä, kuten pieni paristo. Passiivinen tunniste saa virtansa lukijan lähettämästä signaalista. Kulunvalvonnassa yleisemmin käytetään passiivisia tunnisteita. Näitä tunnisteita käytetään usein siten, että luetaan vain tunnisteen avointa sarjanumeroa, joka on kopioitavissa. Jotta UHF-tunnistautuminen on turvallisempaa, tulee käyttää lukija–tunniste-yhdistelmää, jossa lukija lukee tunnisteen muistista salatun avaimen. Tämä lisää turvallisuutta merkittävästi, ja samalla estetään lukijan reagointi avoimiin EPC-tunnisteisiin, joita käytetään tuotemerkkauksessa.

UHF-tunnisteita löytyy erilaisia, aivan kuten 13,56 Mhz tai 125 Khz RFID-tunnisteissa, kortteja, avaimenperiä, rannekkeita ja tuulilasintarroja ajoneuvoihin. Myös UHF-tunnisteiden kanssa voidaan käyttää yhdistelmätunnistautumista.

Kontaktittomassa kulkemisessa henkilön ei tarvitse koskea lukijalaitteisiin tai ovenkahvoihin. UHF-tekniikalla toteutettuna lukuetäisyys voi olla metrejä ja oviautomatiikkaan yhdistettynä voidaan ovi avata automaattisesti, kun siitä pääsyyn oikeudet omaava henkilö tulee esimerkiksi muutaman metrin etäisyydelle ovesta. Tämä toimii hyvin myös esimerkiksi varastoissa, ajoneuvoporteissa ja autotalleissa.

4

Mobiilitunnistautuminen (NFC+BLE)

Viime vuosina yleistynyt NFC/BLE-tunnistautuminen on useimmiten erittäin turvallinen tapa tunnistautua. Erilaisia mobiilitunnisteita löytyy markkinoilta kymmenittäin. Osa hyödyntää ainoastaan älypuhelimien NFC-ominaisuutta, mutta tämä rajoittaa käytön vain Android-laitteisiin (myös Apple on alkanut avaamaan NFC-ominaisuuksia). Ratkaisut, joissa hyödynnetään sekä NFC- ja BLE-ominaisuutta älypuhelimissa, tarjoavat luotettavimman toiminnallisuuden. Itse toiminnallisuuden lisäksi on hyvä huomioida, että mobiilitunnisteista, aivan kuten RFID-tunnisteissa, on eri tasoisia ratkaisua. Kaikki NFC/BLE-tunnisteet eivät välttämättä sovellun korkean turvallisuuden tunnisteiksi.

Helpon jakamisen kautta yritykset ja yhteisöt saavat merkittäviä säästöjä, kun itse tunniste voidaan jakaa digitaalisesti. On kuitenkin hyvä muistaa, että helppo tunnisteiden jakaminen ei tarkoita sitä, että tunnisteiden hallinta ei vaatisi työtä. Aivan kuten avainten hallinta, on myös tunnisteiden hallinta osa yrityksen turvallisuutta. Nykyään löytyy useita eri vaihtoehtoja tunnisteiden hallintaan, ja suosittelemme niiden käyttöä yhdessä kulunvalvonnan ja tunnisteiden hallinnan kanssa.

Useimmissa NFC/BLE-tunnisteapplikaatioissa on mahdollista liittää tunniste osaksi kolmannen osapuolen applikaatiota. Monissa mobiilitunnisteapplikaatiossa voi yleisesti avata lähimmän oven applikaatiosta nappia painamalla tai lisäämällä applikaation älypuhelimen pikavalikkoihin/widgetteihin.

NFC/BLE-tunnisteiden toinen etu on niiden monimuotoiset luennan toteutukset. Joissakin ratkaisuissa riittää, kun älypuhelinta taputtaa tai kääntää, niin lukija tunnistaa laitteen. Joidenkin toimittajien ratkaisuissa seinälukija tunnistaa, kun mobiilitunniste on lähettyvillä, ja kun kulkija peittää kädellä lukijan tai vie käden sen yli, järjestelmä tunnistaa kulkijan.

Mobiilitunnisteen pidemmän lukuetäisyyden ominaisuutta voi hyödyntää yhdessä UHF -tunnisteiden kanssa. Toki on hyvä muistaa, että lukijoiden ollessa hyvin lähekkäin viereisissä kuluissa on vaarana, että viereinen lukija kommunikoi tunnisteen oikean lukijan sijasta. Tällöin tulee lukijoiden lukuetäisyyksiä säätää lyhyemmiksi, jotta kulku on jouhevampaa.

Mobiilitunnisteiden käyttömukavuuteen vaikuttaa erilaisten luennan toteutusten lisäksi se, mitkä ovat puhelimen asetukset. Suurin osa mobiilitunnisteista toimii parhaiten, kun puhelimessa on päällä NFC+BLE-toiminnot sekä paikannus sallittu. On myös hyvä huomioida, että Android-puhelimia ja -alustoja löytyy niin moninaisia, että eri puhelinmallien toiminallisuukissa on suuria keskinäisiä eroja, mitä tulee mobiilitunnistautumiseen.

5

Biometriset tunnisteet

Biometrisistä tunnisteista monille tutuin on sormenjälkitunnistus, mutta biometrisen tunnistautumisen kenttä elää tällä hetkellä nopean kehityksen vaiheessa ja esimerkiksi kasvojen-, äänen, verkkokalvon- ja kämmenentunnistus ovat nopeasti valtaamassa alaa perinteiseltä sormenjälkitunnistukselta.

Biometrisen tunnistautumisen osa, **sormenjälkitunnistus**, myös kehittyy ja tarjolla on erilaisia vaihtoehtoja niin hinnaltaan kuin teknisiltä ominaisuuksiltaan. Yleisesti ottaen paras laatu ja toimivuus sormenjälkitunnistautumisessa saadaan, kun käytetään lukijaa, joka lukee sormenjälkeä pintaa syvemmältä. Kuluneiden sormenjälkien lukeminen on siis myös mahdollista oikealla lukijalla. Sormenjälkitunnistautumisesta tulee lisäksi muistaa, että kuiva ihotyyppi ei toimi yhteen lukijoiden kanssa, joten noin 10 prosenttia väestötasolla ei pysty hyödyntämään sormenjälkitunnistusta.

Biometriseen tunnistautumiseen liittyy merkittävä lakisääteinen rajoitus: kaikki biometriset tunnisteet, kuten esimerkiksi sormenjäljet, katsotaan kuuluvaksi GDPR-regulaatiossa erityisiin henkilötietoryhmiin, eli niiden käsittely on lähtökohtaisesti kiellettyä! Tämä on syytä huomioida tarkasti, sillä tämä tarkoittaa esimerkiksi sitä, että työnantaja ei saa pakottaa työntekijää käyttämään biometristä tunnistautumista. Lisäksi vastuukysymykset tiedon säilyttämisestä ja siitä, missä maassa tietoa varastoidaan ovat hyvin olennaisia.

Toinen biometrisen tunnistautumisen haaste on hygienia. Kuinka usein ja millä tavalla esimerkiksi sormenjälkilukija puhdistetaan? Toisaalta nykyään on saatavilla **kämmenenlukijoita**, jotka lukevat muutaman sentin etäisyydeltä kämmenkuvion ja ovat siten kosketusvapaita.

Mobiilitunnistautuminen on monesti biometristä tunnistautumista edullisempi ja riskittömämpi toteuttaa, ja turvallisuudeltaan sitä voidaan pitää vastaavantasoisena, kun siihen yhdistetään jokin toinen tunnistautumisen keino.

Kasvojen tunnistus on edennyt viime aikoina vauhdilla, mihin ovat osittain vaikuttaneet Covid 19:n aiheuttamat kosketuspintojen puhdistamisen vaatimukset. Aivan kuten sormenjälkilukijoiden kanssa, on kasvojen tunnistamisessa tarjolla kirjava joukko ratkaisuja. Osa järjestelmistä sopii paremmin kasvojen seurantaan kuin tunnistamiseen. Kasvojen piirteiden luotettava tunnistaminen perustuu 3D-kameroihin, ja halvimmat ratkaisut tarjoavat ainoastaan 2D-pohjaisia ratkaisuja. Jälkimmäisiä lukijoita on mahdollista huijata jopa valokuvalla. Kun haetaan korkean turvallisuuden kasvojen tunnistamista, kannattaa ehdottomasti tukeutua 3D-pohjaisiin ratkaisuihin. Osa valmistajista hyödyntää kasvojen tunnistamisessa itse asiassa verkkokalvon tunnistusta, ja tällöin lukijalaitteissa on kaksi pientä kameraa, jotka tunnistavat henkilön retinan. Käyttö on yhtä vaivatonta kuin kasvojen tunnistuksessa, mutta tunnistaminen ja turvallisuus saadaan korkeaksi.

Silmän verkkokalvon käyttäminen tunnisteena on vielä harvinaisempaa kuin sormenjälkien tai kasvojen tunnistaminen, vaikka tekniikka on hyödynnetty jo pitkään. Loppuvuodesta 2020 on odotettavissa uusia ratkaisuja retinan tunnistamisessa.

Ääntä pidetään yhtenä kaikkein yksilöllisimmistä tunnistamisen muodoista, ja sen saralla myös suomalaiset ovat tehneet tutkimus- ja kehitystyötä, mistä on syntynyt patentoituja ratkaisuja. Haasteena on ollut luotettavan äänitunnisteen eli mallikirjaston luominen – millaisissa olosuhteissa ääni on tallennettu ja millaisissa äänitunniste annetaan. Uudet ja kehittyneet mikrofonit ja järjestelmät ovat tuomassa erittäin mielenkiintoisia ratkaisuja äänen käyttämiseksi tunnistautumisessa.

6

Magneettiraitatunnistautuminen

Magneettiraitatunnistautuminen on aiemmin ollut yleistä, mutta nykyään on moneen käyttötarkoitukseen parempiakin tunnistautumisen vaihtoehtoja. Magneettiraitatunnistautumisen etuina ovat edullisuus ja helppokäyttöisyys, huonoina puolina helppo kopioitavuus ja vaurioherkkyys. Monessa tapauksessa esimerkiksi RFID-tunnistautuminen on kestävämpi ja turvallisempi tapa.

Magneettiraitatunnistautumisen etuina ovat edullisuus ja helppokäyttöisyys, huonoina puolina helppo kopioitavuus ja vaurioherkkyys. Yleisimmin magneettiraitatunnistautumista näkee enää kanta-asiakkuusohjelmien, kirjastokorttien ja kuntosalikorttien yhteydessä, mutta näissäkin käyttökohteissa RFID-tunnisteet ovat korvanneet vanhat tunnisteet. Kulunvalvonnassa emme suosittele magneettiraitakorttien käyttöä.

Viivakooditunnistautuminen

Viivakooditunnistautuminen on suhteellisen vanha tapa kulkemisen tunnistamisessa ja erittäin helposti kopioitavissa. Vielä näkee perinteistä viivakoodia hyödynnettävän kirjastoissa, joissa kirjastokortissa on se valmiiksi. Uusimpana toteutuksena näkee 2D-viivakooditunnisteita, varsinkin sisäänpääsylipuissa tai kertakulkuoikeuksina vieraille. 2D-viivakoodin käyttö asettaa itse taustajärjestelmälle suuremmat vaatimukset, jotta tunnisteen kopiointi ei muodostu turvallisuusriskiksi. Ei ole suositeltavaa käyttää 2D- tai 1D-viivakoodia jatkuvana tunnisteena, sillä tunnisteen kopioiminen on helppoa.

Viivakoodi on helppo tunniste jakaa sähköisesti tai tulosteena, ja se sopiikin parhaiten matalamman turvallisuuden kohteiseen ja kaupallisiin käyttöihin kuten lippusisäänpääsyihin.

Viivakoodin jakelu on helppoa kuten Mobiilitunnisteen, kun sen voi toimittaa käyttäjälle digitaalisesti. Itse viivakoodin luominen ja aktivointi on usein helpompaa kuin Mobiilitunnisteen. On hyvä huomioida, että viivakoodeja on lukuisia erilaisia ja kaikki kulunvalvonnan lukijat eivät tue kaikkia viivakoodityyppejä. Onkin mahdollista, että viivakoodiluennassa joudutaan käyttämään muita kuin kulunvalvonnan lukijoita, jolloin kaapelointi tapahtuu usein miten joko RS232- tai USB-väylän kautta.

Aivan kuten muiden tunnistatumistekniikoiden kohdalla myös viivakoodilukijoita on laadullisesti hyvin erilaisia. Tärkeintä on toki huomioida, että lukija tukee valittua viivakoodimuotoa, mutta yhtä tärkeää on nykyään huomioida, että lukija pystyy lukemaan myös kännykän ruudulla olevan tunnisteen. Suuri osa viivakoodeista jaetaan digitaalisesti, eivätkä käyttäjät enää tulosta lippuja/tunnisteita vaan näyttävät viivakoodinsa suoraan puhelimen ruudulta. Näin sanottuna 2D-viivakoodia voidaan pitää jopa yhtenä mobiilitunnistaumisen muotona.

8

PIN-kooditunnistautuminen

Useissa rakennuksissa käytetään edelleen yhtä ja samaa PIN-koodia ulko-oven tai porttikongin oven avaukseen. Lisäksi koodia jaetaan hyvin huolettomasti ystäville, sukulaisille, läheteille ja remonttimiehille. On hyvä huomioida, mihin kaikkialle PIN-koodilla suojatusta ovesta pääsee ja tulisiko sen käyttöä ohjeistaa. Osassa vanhemmista PIN-koodilukijoista voi arvata koodin näppäimistön käytöstä, sekä joissain malleissa saa PIN-koodin selville lukijan avaamalla.

PIN koodi käy myös kertakäyttötunnisteesta viivakoodin tavoin. Näin voidaan sallia asiakkaille kertakäyttöinen pääsy tiloihin kuten kuntosaleille tai julkisiin käymälöihin. Näissäkin käyttökohteissa on suositeltavaa käyttää pidempää, esimerkiksi 6-numeroista PIN-koodia, jotta voimassa olevien koodien arvaaminen olisi vaikeampaa. PIN-koodia käytettäessä sen turvallisuutta voidaan parhaiten parantaa merkin pituutta lisäämällä, antamalla henkilökohtaiset PIN-koodit ja vaihtamalla niitä säännöllisesti.

PIN-koodi on hyvä lisä yhdistettynä johonkin toiseen tunnistautumistapaan kuten RFID-tunnisteisiin.

Suosittelemme, että PIN-koodi aina annetaan henkilölle eikä sitä saa valita itse. Lisäksi PIN-koodin tulisi mieluiten olla pidempi kuin 4-numeroinen.

9

Yhdistelmätunnistautuminen

Yhdistelmätunnistautumista suositellaan käytettäväksi kuluissa, joissa vaaditaan korkeampaa turvallisuutta. Esimerkiksi toimiston ulkokuoren suojaukseen on suositeltavaa käyttää yhdistelmätunnistetta, jolloin ei pääovesta päästä suoraan tiloihin pelkällä yhdellä tunnisteella. Tämä käytäntö voi olla käytössä joko 24/7 tai toimistoaikojen ulkopuolella.

Mobiilitunnisteet sopivat myös yhdistelmätunnistautumiseen, kun mobiiliapplikaation käytöltä vaaditaan puhelimen lukituksen avausta. Näin saadaan yhdistettyä PIN-koodi tai biometrinen tunniste BLE-tunnistautumiseen. Yhdistämällä korkeamman turvallisuuden RFID-tunnisteeseen SeoS-teknologian kortti ja sormenjälkitunnistautuminen, saavutetaan jo korkeamman turvallisuuden tunnistautuminen.

Jopa UHF- ja ajoneuvotunnistautumiseen on hyvä ajatella kahdennettua tunnistautumista. Näistä helpoimpia on mobiilitunnisteen käyttö ajoneuvoporteissa sekä UHF-tunnistautumisen yhdistäminen ajoradan alla olevaan silmukkatunnistamiseen. Jälkimmäisellä ratkaisulla saavutetaan se, että ajoporttia ei voi avata, jos sen edessä ei ole ajoneuvoa. Tällöin pelkän tunnisteen avulla ei voida tulla sisään portista.

Yleisten kulunvalvonnan tunnistautumisten rinnalla voidaan käyttää myös sijaintia. Tämä voidaan toteuttaa useamalla tavalla. Yksi tapa on liittää kulkutunnisteisiin BLE-tunniste ja paikantaa henkilöitä BLE-vastaanottimien kautta tai tunnistaa henkilön läsnäolo WiFi-tukiasemien kautta. Molemmissa tekniikoissa yhdistetään henkilön läsnäolo alueeseen, ja sitä tietoa verrataan järjestelmässä lukijan antamaan sijaintiin, minkä perusteella tehdään päätökset tunnistautumisesta. Kolmas tapa on yhdistää UHF-tunniste henkilöön, jonka paikannus tehdään kulkuaukoittain UHF-lukijoilla.

Yhdistelmätunnistautuminen voi myös tarkoittaa kahden eri henkilön antamien tunnistetietojen yhdistämistä esimerkiksi ohjelmiston käynnistämisessä tai turvatilojen ovien avaamisessa. Näin varmistetaan, että kukaan ei voi yksin avata turvaluokitellun tilan ovea. Esimerkiksi kassakaapeissa tai holveissa on ollut kahden PIN-koodin käyttöominaisuus jo pitkän aikaa.

IDcontrol Oy

ESPOO:
Stella Business Park, Nova talo
Lars Sonckin kaari 10
02600 Espoo
SUOMI

VALENCIA:
Av. d'Aragó 30
46021 Valencia
SPAIN

Myynti (SUOMI):
020 734 3225
myynti@idcontrol.fi

KAPKAUPUNKI:
Advanced ID Solutions PTY
Manhattan Street 55
Cape Town 7490
ETELÄ-AFRIKKA

UUSI-SEELANTI:
+64 9 437 4006
admin@base42.co.nz
http://base42.co.nz

Myynti (ETELÄ-AFRIKKA):
+27 79 881 8230
sales@advancedidsolutions.co.za
www.advancedidsolutions.co.za