

Aventra RuudukkoPIN



PIN-lukua turvallisempi uusi tunnistusmenetelmä

Parempaa turvallisuutta

Aventra esittelee uudenlaisen autentikointiratkaisun, jolla voidaan korvata salasanat ja PIN-luvut. Uusi menetelmä ei vaadi mitään lisälaitteistoa eikä -välineitä. Se soveltuu käytettäväksi sellaisenaan esim. verkkopalveluiden käyttäjien tunnistamiseen, sekä sirukorttien turvallisuuden parantamiseen.

Salasanojen riskit

Tietotekniikan järjestelmissä eräs keskeinen alue on käyttäjän autentikointi, eli sen varmistaminen että palvelun tai tuotteen käyttäjä on se joka väittää olevansa. Yleinen tapa ratkaista tämä ongelma on käyttää ns. jaettua salaisuutta, jonka vain käyttäjä ja järjestelmä tietävät, esimerkiksi salasanaa. Käyttäjä tunnistautuu antamalla käyttäjätunnuksen, ja antamalla salasanan hän osoittaa järjestelmälle olevansa kyseinen käyttäjä, koska vain hän ja järjestelmä tietävät salasanan.

Salasanaan perustuva autentikointi on edullinen toteuttaa, mutta sen suurin heikkous on että kiinteä salasana voi helposti vuotaa asiattomien tietoon. Riski on suuri esimerkiksi salasanaa annettaessa, koska se näkyy tällöin aina selväkielisessä muodossa. Saattaa olla mahdotonta varmistua siitä että paikalla ei ole salakatselijoita tai vaikkapa tallentavaa kameraa.

Sirukortilla voidaan toteuttaa turvallisempi autentikointi, jossa kortti ja järjestelmä voivat matemaattisin menetelmin varmistua toistensa aitoudesta ilman että niiden jaettu salaisuus välittyy selväkielisenä. Käyttämällä PKI-menetelmää ei edes tarvita jaettua salaisuutta, mikä yksinkertaistaa järjestelmän hallintaa, varsinkin jos käyttäjiä on paljon. PKI-kortilla suoritettu autentikointi on huipputurvallinen, sitä ei voi käytännössä murtaa.

Jos autentikointi suoritetaan sirukortilla, on tietysti jollain tavalla todennettava se että varsinaisella käyttäjällä on oikeus käyttää kyseistä korttia autentikointiin. Tarvitaan siis käyttäjän autentikointia kortille. Yleisin tapa toteuttaa tämä on käyttää jaettua salaisuutta kuten PIN-lukua. PIN-lukuun liittyvät kuitenkin täysin samat riskit kuin muihinkin salasanoihin. Kuka tahansa joka saa kortin haltuunsa voi käyttää sitä kuin omaansa, jos hän tietää sen PIN-luvun.

Uusi autentikointiratkaisu

Aventra on kehittänyt turvallisen menetelmän jaetun salaisuuden välittämiseksi epäsuorasti. Ratkaisu perustuu englantilaisen GrIDsure Ltd:n patenttiin. Aventran kehittämä ratkaisu soveltuu sekä yksinomaiseksi autentikointimenetelmäksi korvaten salasanan, että korvaamaan kiinteän PIN-luvun sirukorteissa. Aventra on toistaiseksi ainoa korttivalmistaja maailmassa joka on tuonut PKI-korttiin tämän menetelmän PIN-luvun rinnalle.

Menetelmän kuvaus

Menetelmä perustuu jaetun salaisuuden epäsuoraan välittämiseen. Numerosarjan sijasta käyttäjä valitsee 5x5 ruudukosta neljä mieleistään ruutua ja painaa niiden sijainnin ja järjestyksen mieleensä. Tieto näistä ruuduista välitetään myös järjestelmälle. PIN-luvun kyselyn yhteydessä käyttäjälle näytetään 5x5 ruudukko, jossa kaikkiin ruutuihin on täytetty satunnainen numero. Käyttäjä muodostaa nyt kertakäyttöisen PIN-luvun poimimalla numerot ennalta valitsemistaan ruuduista.

Koska vain käyttäjä ja järjestelmä tietävät käyttäjän valitsemien ruutujen paikan, kukaan muu ei voi muodostaa PIN-lukua annetun täytetyn ruudukon pohjalta. PIN-luvun antamista seuraava sivullinen ei voi päätellä mistä kohtaa ruudukkoa numerot on poimittu, koska kaikki numerot esiintyvät ruudukossa useampaan kertaan. Joka kerta kun PIN-lukua kysytään, ruudukko täytetään eri numeroilla täysin satunnaisesti. Haluttaessa ruudukon kokoa ja valittavien ruutujen lukumäärää voidaan kasvattaa.



Näytettävän ruudukon täyttämät satunnaisnumerot luodaan turvallisuussyistä kortilla. Käyttäjän valitseman kuvion on oltava ennalta arvaamaton, jotta mahdolliset sivulliset eivät arvaisi kuviota kun PIN-lukua annetaan. Tämän varmistamiseksi MyEID-kortin mukana tuleva ohjelmisto opastaa käyttäjää valintatilanteessa havainnollisella mittarilla, joka näyttää valitun kuvion turvatason. Ohjelmisto mahdollistaa myös RuudukkoPINin hallinnoinnin. Valinnaisena ominaisuutena on mahdollista estää liian huonojen kuvioiden valinta.

RuudukkoPIN MyEID-kortilla

RuudukkoPIN on saatavana Aventran MyEID-kortille lisätoimintona. Tuote voidaan myös esiladata MyEID-korteille ja ottaa käyttöön tarvittaessa. Kortilla voi olla sekä tavallisia että RuudukkoPINejä, ja minkä tahansa PINin tyyppiä voidaan myös halutessa vaihtaa. Periaatteessa RuudukkoPINin kuvio voi olla kortilla esivalittuna, kuten tavallinenkin PIN, mutta varsinaisesti RuudukkoPIN on tarkoitettu itsevalittavaksi. MyEID-korttiin liittyvä apuohjelmisto auttaa käyttäjää valitsemaan itselleen kuvion, jonka mukaan PIN-luku muodostetaan autentikoinnissa. Kuviota voi myös tarvittaessa vaihtaa. Kortti voidaan alustaa siten että



käyttäjän on valittava itselleen kuvio (tai tavallinen PIN) ennenkuin korttia voidaan varsinaisesti käyttää. Näin PIN-kuoria ei tarvita lainkaan.

RuudukkoPIN ohjelmallisena ratkaisuna

RuudukkoPINin toiminnallisuus ilman käyttöliittymää on myös saatavana kirjastona, jonka avulla se voidaan liittää mitä erilaisimpiin järjestelmiin. RuudukkoPIN soveltuu myös ainoaksi autentikointimenetelmäksi korvaamaan salasanoja esimerkiksi verkko- tai mobiilipalveluissa. Näin voidaan helposti toteuttaa kertakäyttöisiin salasanoihin perustuva autentikointi ilman että käyttäjien tarvitsisi kuljettaa mukanaan mitään salasanalista tai generointilaitetta.

RuudukkoPIN vs. biometria

Kun tarvitaan korkeampaa turvatasoa kuin mitä PIN-luku pystyy tarjoamaan, on perinteisesti turvaututtu biometriaan. Biometrian suurin etu on että se on aidosti henkilökohtainen. Biometristä ominaisuutta on vaikea siirtää toiselle. Biometria voi parhaimmillaan olla myös nopea ja helppo käyttää. Korkeat kustannukset ja erillisen lisälaitteiston tarve ovat kuitenkin esteenä monissa tapauksissa. Biometria soveltuukin parhaiten tilanteisiin joissa turvavaatimukset ovat erittäin korkeita, kuten huipputurvallisten tilojen pääsynvalvontaan, tai sovelluksiin joissa käyttäjien määrä on riittävän suuri yhtä laitteistoa kohti, kuten esimerkiksi pankkiautomaateissa.

RuudukkoPIN tarjoaa uudenlaisen vaihtoehdon tavallisen salasanan tai PIN-luvun ja biometrian väliin. Turvallisuus on merkittävästi parempi kuin salasanoja käytettäessä, koska aivan kuten biometriassakin, sivullisen on mahdotonta toistaa autentikointia näkemänsä perusteella. Menetelmä ei kuitenkaan vaadi mitään ylimääräistä laitteistoa eikä käyttäjän tarvitse pitää mukanaan mitään laitetta tai numerolistaa. Kustannuksiltaan RuudukkoPIN on vain murto-osa biometriasta, koska kyseessä on ohjelmallinen ratkaisu.

Aventra Oy

Aventra on tietotekniikan turvallisuustuotteisiin ja –palveluihin erikoistunut teknologiayritys. Keskitymme erityisesti PKI-ratkaisuihin (PKI = julkisen avaimen menetelmä). Olemme kehittäneet useimmat tuotteemme itse.

Aventra tarjoaa täyden tuotevalikoiman yksikertaisista muovikorteista aina huipputurvallisiin toimikortteihin. Uusin tuoteperheemme käsittää mobiiliturvaratkaisut.

© Copyright Aventra Oy, 2010. Kaikki oikeudet pidätetään. Tämän esitteen tiedot ovat tekijänoikeuslain alaisia. Kaikki muutokset ja lisäykset vaativat Aventran kirjallisen hyväksymisen. Jäljentäminen on sallittu vain jos tämä ehto säilyy dokumentissa. Julkistaminen tai kääntäminen vaatii Aventran suostumuksen etukäteen. Tuotemerkit ovat haltijoidensa omaisuutta.
Versio 6