

Aventra MyEID -toimikortit



Johdanto

Sähköisen tunnistamisen merkitys kasvaa nopeasti nykyaikaisessa yhteiskunnassamme. Turvallinen sähköposti, kirjautuminen tietokoneille ja sovelluksiin, sekä sähköiset allekirjoitukset ovat tästä esimerkkinä. Aventran PKI-toimikortit vastaavat näihin haasteisiin.

Aventra MyEID -toimikortit

Aventran MyEID-toimikortteja valmistetaan kahta tyyppiä: normaali luottokorttikokoinen toimikortti, sekä microSD. Aventran toimikortit perustuvat viimeisimpään JavaCard™ teknologiaan, mikä mahdollistaa toiminnallisuuden päivittämisen ohjelmamoduleja, eli appletteja lisäämällä tai poistamalla. Java™ on avoin teknologia, jota monet johtavat toimikorttien valmistajat tukevat. Aventra tai kolmannet osapuolet voivat kehittää myös asiakaskohtaisia appletteja. Aventran kehittämä MyEID-appletti on Aventran MyEID –toimikorttien toiminnallisuuden perusta.

Aventra MyEID-appletti

MyEID-appletti toteuttaa yleisimpien PKI-standardien (Public Key Infrastructure), kuten PKCS#15, määrittelemän toiminnallisuuden. Käyttäjille voidaan tarjota mahdollisuus valita haluamansa tunnistautumismenetelmä. Normaalin PIN-luvun lisäksi valittavissa on kaksi muuta menetelmää. Gridsuren™ lisensoima ruudukko-PIN perustuu näytölle ilmestyvään ruudukkoon, josta PIN-luku poimitaan turvallisesti vaikka sivulliset näkisivät toimenpiteen. MyEID-toimikortit ovat myös yhteensopivia PalmSecure™-teknologian kanssa. Siinä kämmenen verisuonista otettava kuva korvaa PIN-luvun. MyEID-appletti on yhteensopiva Aventran ActiveSecurity Suiten kanssa.

Aventra MyEID-kortti

Aventran MyEID PKI-kortti on asymmetrisellä salausalgoritmilla varustettu toimikortti, joka on yhteensopiva ISO7816 ja PKCS#15 standardien kanssa. Sitä voidaan käyttää erilaisissa vahvaa salausta vaativissa sovelluksissa, kuten turvallinen kirjautuminen Windowsiin, sähköpostin salaus, vahva tunnistaminen ja sähköiset allekirjoitukset. Korttia toimitetaan myös Dual Interface –versiona, joka on T=CL ja Mifare™ yhteensopiva.

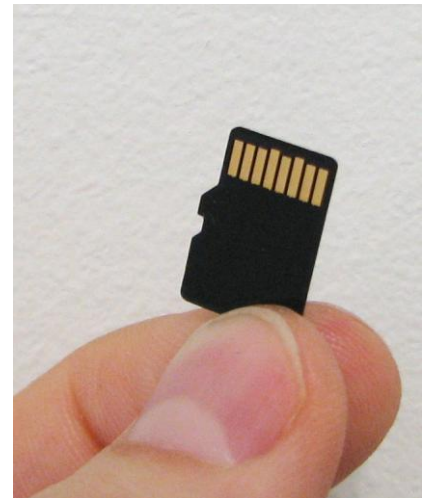
Kortin materiaali on PVC, joka soveltuu lämpösiirto- ja sublimaatiotulostimiin. Asiakaskohtaisia esipainatuksia voidaan toteuttaa offset- ja silkkipainomenetelmillä. Korttiin voidaan myös lisätä magneettiraita tai allekirjoituspaneli. Lisäksi on saatavana monia turvaominaisuuksia, kuten hologrammi tai erilaisia painettuja turvaelementtejä.

Aventra voi tarvittaessa yksilöidä kortit sekä sähköisesti että visuaalisesti asiakkaan määrittelyn mukaan, tai asiakas voi yksilöidä kortit itse käyttämällä Aventran ActivePerso Manager –työkalua, tai kolmansien osapuolien tuotteita.

Aventran MyEID microSD

MyEID microSD-kortti on laskentaväline pienoiskoossa. Sen avulla PKI-toiminnot voidaan tuoda käytännössä mihin tahansa Windows Mobile –laitteeseen jossa on microSD-paikka. Kortilla on myös normaali flash-muisti johon voi tallentaa sovelluksia tai dataa. MyEID microSD-kortilla on sama toiminnallisuus kuin normaalilla MyEID-kortillakin.

Käyttämällä MyEID microSD -korttia mobiilit sovellukset voivat hyödyntää standardoitua PKI-teknologiaa, mikä lisää turvallisuutta merkittävästi. Varsinaista toimikorttilukijaa ei tarvita, mikä säästää tilaa erityisesti pienissä laitteissa.



Aventra ActiveSecurity Client -ohjelmisto

ActiveSecurity Client -ohjelmisto liittyy Aventran toimikortit Windows XP ja Vista -ympäristöihin. Siinä on laaja valikoima kortin ja PIN-luvun hallintaan liittyviä toimintoja, kuten valinnainen GrIDSure™ -teknologia. Ohjelmisto sisältää sekä CSP:n (Crypto Service Provider for Microsoft™ CryptAPI) että PKCS#11 Token Interfacen. ActiveSecurity Wizard on helppokäyttöinen työkalu mm. kortin PIN-toimintojen ja varmenteiden hallintaan.

Teknisiä tietoja

Aventra MyEID-kortti

Alusta

- JavaCard™ 2.2.1, Global Platform 2.1.1

Tuetut standardit ja määrittelyt

- ISO/IEC 7816-4 to 7816-9
- ISO/IEC 14443 T=CL ja Mifare™
- PKCS#15
- FINEID S4-1 ja S4-2

Muita ominaisuuksia

- 512 - 2048 bitin RSA-operaatiot, avainten luonti kortilla
- Turvallinen satunnaislukugeneraattori (FIPS 140-2)
- Symmetriset algoritmit: DES, 3DES, AES128 ja AES256
- 72K EEPROM-muistia

Yhteensopivia ohjelmistotuotteita

- Aventra ActiveSecurity Suite
- Fujitsu mPollux DigiSign™ middleware
- Laaja valikoima kolmansien osapuolten tuotteita jotka ovat CSP- tai PKCS#11-yhteensopivia

Aventra MyEID microSD

Alusta

- JavaCard™ 2.2.1, Global Platform 2.1.1

Tuetut standardit ja määrittelyt

- ISO/IEC 7816-4 to 7816-9
- PKCS#15
- FINEID S4-1 ja S4-2

Muita ominaisuuksia

- 512 - 2048 bitin RSA-operaatiot, avainten luonti kortilla
- Turvallinen satunnaislukugeneraattori (FIPS 140-2)
- Symmetriset algoritmit: DES, 3DES, AES128 ja AES256
- Yhteensopiva kaikkien Windows ja Windows Mobile –laitteiden kanssa joissa on SD™, miniSD™ tai microSD™ -paikka

Täydelliset tekniset tiedot toimitetaan pyydettäessä.

Aventra yrityksenä

Aventra on teknologiayritys joka on erikoistunut sähköisen tunnistamisen tuotteisiin ja palveluihin. Olemme erityisesti keskittyneet PKI-tekno- logiaan. Useimmat tuotteemme ovat itse kehitettyjä.

Aventra tarjoaa täyden valikoiman tuotteita aina yksinkertaisesta muovikortista huipputurvallisiin toimikortteihin. Uusin tuoteperheemme liittyy mobiiliin turvallisuuteen. Tarjoamme myös täyden palvelun ja järjestelmät korttien yksilöintiin ja hallintaan, mukaanlukien laitteet ja materiaalit.

© Copyright Aventra Oy, 2009. Kaikki oikeudet pidätetään. Tämän dokumentin sisältö on tekijänoikeuslain piirissä. Kaikki muutokset ja lisäykset vaativat Aventra Oy:n kirjallisen hyväksynnän. Tämän dokumentin jäljentäminen on sallittu mikäli tämä tekijänoikeuslausunto säilyy osana dokumenttia. Julkaiseminen tai kääntäminen vaativat Aventra Oy:n kirjallisen hyväksynnän. Tavaramerkit ovat haltijoidensa omaisuutta.
Versio 6