

# ActiveSecurity MyEID -toimikortit



## Johdanto

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

## ActiveSecurity™ MyEID -toimikortit

MyEID-toimikortteja on kolmea tyyppiä: normaali luottokorttikoko, SIM-koko sekä microSD. Aventran toimikortit perustuvat JavaCard™ -teknologiaan, joka mahdollistaa toiminnallisuuden päivittämisen ohjelmamoduleja eli appletteja lisäämällä tai poistamalla. Java™ on avoin teknologia, jota monet johtavat toimikorttien valmistajat tukevat. Aventura tai kolmannet osapuolet voivat kehittää myös asiakaskohtaisia appletteja. Aventran kehittämä MyEID-appletti on MyEID-toimikorttien toiminnallisuuden perusta.

### *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™ patentoima RuudukkoPIN 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 MyClient Suiten kanssa.

### *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. Toinen vaihtoehto RFID-teknologian hyödyntämiseksi on varustaa tavallinen MyEID-kortti jollain RFID-sirulla, jolloin saadaan ns. hybridikortti.

Hybridikortti on erittäin monipuolinen työkalu joka sopii kulunvalvontaan, työasemakirjautumiseen sekä muiden sähköisten palvelujen hyödyntämiseen. Erillisten kulunvalvontatunnisteiden ja useiden salasanojen sijaan tarvitaan vain yksi kortti. Tämä säästää organisaation kustannuksia sekä fyysisen että loogisen turvallisuuden hallinnassa.

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.

## 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-tekniologiaa, mikä lisää turvallisuutta merkittävästi. Varsinaista toimikorttilukijaa ei tarvita, mikä säästää tilaa erityisesti pienissä laitteissa.

## Teknisiä tietoja

### Yleiset ominaisuudet

- 512 - 2048 bitin RSA-operaatiot, avainten luonti kortilla
- Turvallinen satunnaisluku (FIPS 140-2)
- Symmetriset algoritmit: 3DES ja AES256
- SHA-1 ja MD5 -algoritmit

### Tuetut standardit ja määrittelyt

- ISO/IEC 7816-1...9 ja 7816-15
- PKCS#7, #11, #12, ja #15
- FINEID S4-1 ja S4-2

### Muut ominaisuudet

- 80K EEPROM-muisti
- Dual Interface –versio: ISO/IEC 14443 T=CL ja Mifare® tuettu
- microSD on yhteensopiva kaikkien Windows ja Windows Mobile -laitteiden kanssa joissa on SD™, miniSD™ tai microSD™ -paikka

### Alusta

- JavaCard™ 2.2.1, Global Platform 2.1.1
- NXP SmartMX -prosessorisirut

### Kontaktiton teknologia

- ISO 14443 A + B (Mifare®, Sony Felica)
- ISO 15693, I.Code, Legic
- EM41xx, EM4550, Hitag
- Valikoima laajenee koko ajan

### Yhteensopivia ohjelmistotuotteita

- Aventra ActiveSecurity™ MyClient Suite
- Fujitsu mPollux DigiSign™ middleware
- Usealla alustalla toimiva toimikorttikirjasto OpenSC ([www.opensc-project.org](http://www.opensc-project.org))
- Laaja valikoima kolmansien osapuolten tuotteita jotka ovat CSP- tai PKCS#11-yhteensopivia

Täydelliset tekniset tiedot toimitetaan pyydettyä.

© Copyright Aventra Oy, 2010. 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 14