MyEID 4.5 PKI Smart Card

Introduction

Aventra's MyEID PKI Smart Card has evolved into version 4.5, adding support for 4096 bit RSA keys, faster operation and more storage space. MyEID 4.5 is based on NXP's SmartMX2 SECID P60 microcontroller, with JCOP3 Java Card Operating System. This microcontroller replaces NXP's older JCOP2 based modules.

New in MyEID 4.5

EEPROM storage space is increased to 144 kilobytes. RSA keys are supported up to 4096 bit key length. MyEID 4.5 is faster than earlier versions in performing Elliptic curve cryptography and RSA operations with keys up to 2048 bit. 4096 bit operations are fast as well, with on card key generation taking around one minute and digital signature calculation around 3000-4000 milliseconds. MyEID 4.5 contains some new features for securely transferring symmetric keys between the card and outside world (key wrapping/unwrapping).

Security Certifications

Aventra's MyEID Applet utilises security features of the certified JCOP3 platform for all key storage and cryptographic functionality. The modules of the P60 SmartMX2 family have passed the following security certifications:

- FIPS 140-2
- J2H145 chips (contact interface): Common Criteria EAL 6+
- J3H145 chips (dual interface): Common Criteria EAL 5+

Certified for Windows

MyEID card and MyEID Minidriver have been certified by Microsoft as compatible with Windows 10.

Card body

MyEID cards are available in two form factors: standard and SIM sized. The card material is PVC, making it suitable for visual personalisation using thermal transfer or dye sublimation printers. Other

materials are available on request. Customer specific layouts can be delivered in offset and silk screen printing. Optional features include magnetic stripe, signature panel, holograms, security printing, etc.

Backwards compatibility

MyEID 4.5 is backwards compatible with the earlier MyEID versions.

Additional tools and services

Aventra has developed an extensive portfolio of software products to facilitate the use and maintenance of the MyEID card, including:

- MyEID Minidriver: a Microsoft Certified Windows Smart Card Minidriver
- MyEID Miniriver Utility: a tool for initialising and managing MyEID cards
- MyEID Editor, a versatile card manipulation tool for advanced users
- Active Process Manager, a fully configurable PKI enabled card issuing software
- ActiveCMS, a web based IAM and card management system with a configurable work flow

MyEID Minidriver and MyEID Minidriver Utility are available to download for free on Aventra's web site.

PKCS#11 interface is available using the open source OpenSC middleware/toolkit. Aventra participates in development and testing of OpenSC, keeping MyEID support up to date with new MyEID versions.

Aventra can also offer professional personalisation services. MyEID cards can be personalised both visually and electrically according to customer specifications.

Technical details

Windows 10 Compatible

Common features

- 512 - 4096 bit RSA cryptographic operations with on card key generation
- 192 - 521 bit ECC operations with on card key generation
- Secure random number generator (FIPS 140-2)
- DES, 3DES, AES128, AES256 symmetric encryption algorithms
- SHA-256, SHA-1 and MD5 one way hash algorithms

Supported standards and specifications

- ISO/IEC 7816-1 to 7816-9, 7816-15
- PKCS#7, #11, #12, and #15
- FINEID S4-1 and S4-2
- Smart Card Minidriver Specification v7.07

Other features

- 144K EEPROM memory Dual Interface version supports ISO/IEC 14443 T=CL and Mifare™ Flex

Platform

- JavaCard™ 3.0.4 with Global Platform 2.2.1
- NXP JCOP 3, SmartMX2 P60 Family

Wireless technology (optional)

- ISO 14443 A + B (Mifare® DESFire, Mifare® Classic, Sony Felica)
- ISO 15693, I.Code, Legic
- EM41xx, EM4550, Hitag
- More options upon request

Compatible 3rd party software

- Fujitsu mPollux DigiSign™
- Cross-platform smart card library OpenSC https://github.com/OpenSC/OpenSC/wiki
- Versasec vSEC:CMS
- Citrix™
- Cisco VPN Client
- Large number of software products that support Microsoft™ CryptoAPI, Microsoft Cryptography API: Next Genration (CNG) or PKCS#11 Token Interface.

Version 2