MyEID PKI Smart Card

Version 5.0.0
Technical Datasheet

Introduction

Aventra's MyEID PKI Smart Card is designed for strong authentication, digital signing and protecting sensitive data. MyEID is based on JavaCard technology and has versatile PKI and symmetric encryption functionality. Having been in the market since 2004, MyEID has evolved into version 5.

The new version has been certified to Common Criteria EAL4+ level. During the certification, security experts have analysed the JavaCard applet, our production process and facilities thoroughly, helping us to eliminate any potential vulnerabilities.

MyEID 5 is delivered on NXP JCOP4 P71 platform and SmartMX3 security microcontroller with 150kB -200kB of EEPROM memory. SmartMX3 microcontrollers are designed to counter the newest security threats and provide the strongest protection for your private keys.

New in MyEID 5

MyEID 5 includes the following new key features:

- Secure Messaging, compliant with ISO 7816-4 and PIV Card Specifications:
    - NIST SP 800-73-5 Interfaces for Personal Identity Verification: Part 1 – PIV Card Application Namespace, Data Model and Representation
    - NIST SP 800-73-5 Interfaces for Personal Identity Verification: Part 2 – PIV Card Application Card Command Interface
- On-card PSS and OAEP padding in RSA operations
- Cryptographic card genuineness verification – verify that the card originates from Aventra using a cryptographic mechanism.
- Extended length APDU commands
- AES challenge/response PINs.

Security Certifications

MyEID PKI Smart Card

- The composite product, consisting of Aventra's MyEID JavaCard applet and NXP's JCOP4 P71 platform is certified to Common Criteria EAL4+ level
- MyEID 5 is an eIDAS-compliant Qualified Signature Creation Device and Qualified Seal Creation Device.

Platform

- JCOP4 P71 platform and SmartMX3 microcontrollers are certified to Common Criterial EAL6+ level and as FIPS 140-2 compliant.
- Aventra's MyEID Applet utilises the security features of the certified JCOP4 P71 platform for all key storage and cryptographic functionality.

Certified for Windows

MyEID card and MyEID Minidriver have been certified by Microsoft as compatible with Windows 11.

Card body

MyEID cards are available in two form factors: standard and SIM sized. The card is available in PVC, polycarbonate and composite materials, all 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 signature panel, holograms, security printing, etc.

Backwards compatibility

With minor exceptions, MyEID 5 is backwards compatible with the earlier MyEID versions. The exceptions include deprecation of insecure algorithms and key lengths (DES, 3DES, RSA with smaller than 2048 bit keys), and slight changes in the command interface, which have been made to improve security. The differences do not cause compatibility issues in most scenarios, and if they do, they can be addressed with compatibility mode or software updates.

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 issuinca 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.

Aventra Ltd.
Kutomotie 16
00380 Helsinki
Finland

VAT number: FI8940682
www.aventra.fi
Tel. +358 9 4251 1251
sales@aventra.fi

Technical details

Common features

- 2048 - 4096 bit RSA cryptographic operations with on card key generation
- 256 - 521 bit ECC operations with on card key generation on NIST P and Brainpool curves.
- Secure random number generator (FIPS 140-3)
- AES symmetric encryption algorithms with 128, 192 and 256 bit key lengths
- PKCS#1 1.5, PSS and OAEP padding 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

- 150 – 200 kB EEPROM memory
- Dual Interface version supports ISO/IEC 14443 T=CL with optional Mifare™ DESFire EV2 or Mifare™ Plus emulation.

Platform

- JavaCard™ 3.0.5 with Global Platform 2.3
- NXP JCOP 4 P71, SmartMX3 Family

Wireless technology (optional)

- ISO 14443 A + B (Mifare® DESFire, Mifare® Classic)
- ISO 15693, ICode, Legic
- More options upon request

Compatible 3rd party software

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