

Certified Security OS

with CrypToken M2048



ITSEC E6 high certified

CrypToken® M2048 and MULTOS

USB Token with the most secure smart card operating system



CrypToken
Compact and extremely
durable in a metal case
(actual size)

MULTOS is the first, open, high security, multi-application operating system for smart cards. The beauty of this system is that diverse parties can develop applications that run on the same card and they all co-reside both independently and securely.

Furthermore MULTOS allows to add applications in the field over unsecure channels, utilizing the PKI of the MULTOS scheme. Any modification of the card requires an appropriate certificate. The loading process guarantees data integrity, authenticity and confidentiality. This is beneficial for both, the cardholder and the card issuer.

MULTOS

- First, open, high security, multi-application operating system
- MULTOS achieved ITSEC E6 high security evaluation
- Up to 2048-bit RSA encryption
- Fully defined lifecycle management
- Tens of millions of chips deployed
- Your MULTOS applications run unmodified on the CrypToken

CrypToken

- CrypToken M2048 with Infineon Smart Card Chip (ITSEC E4 high)
- Integrated OMNIKEY Smart Card Reader (PC/SC standard)
- Driverless on CCID enabled OS
- Mobile and secure certificate storage
- Designer metal case
- Cryptographic interfaces: PKCS#11 and MS-CAPI
- Windows (Vista, XP, 2000, CE), Linux, Mac OS X, SUN Solaris

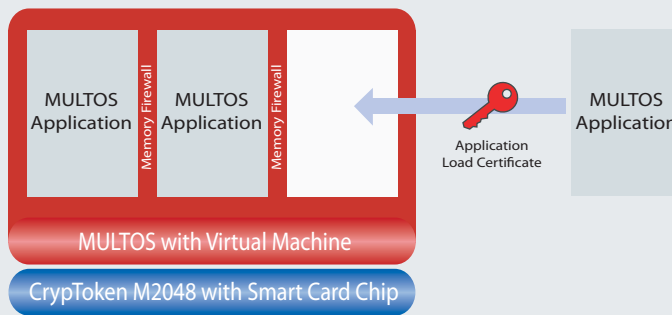
How is this high security level achieved?

The security of MULTOS is ensured by a requirement in the MULTOS implementation license. All MULTOS silicon providers have to undergo a rigorous testing and evaluation process to prove interoperability, security and tamper resistance. No other available smart card platform can claim a similar level of security.

MULTOS applications run on a virtual machine. Therefore MULTOS provides a platform independent way to develop applications. Commonly used chips are manufactured by Infineon, Hitachi and Samsung. The virtual machine guarantees that an application developed on one card can be deployed on another.

A system of memory firewalls ensures that applications cannot access data without proper authorization. Card issuers and application providers establish their trust relation through certificates. Application providers can rely on MULTOS that no application can tamper with code of another application.

MULTOS Smart Card OS on the CryptToken



For additional information visit www.cryptoken.com/multos or www.multos.com

Securing the Digital World™

www.cryptoken.com

MARX Data Security GmbH
Vohburger Strasse 68
D-85104 Wackerstein, GERMANY
Tel. +49 (0) 8403-92 95-14
Fax +49 (0) 8403-92 95-29
contact@cryptoken.com

MARX CryptoTech LP
4485 Tench Rd. #310, Peachtree Commons Office Park
Suwanee, GA 30024, U.S.A.
Tel. +1 770 904 0369
Fax +1 770 904 3893
contact@cryptotech.com

MARX[®]
Data Security