



# MULTOS for Embedded Security

## Incorporating MULTOS for USB Token-Enabled Security

### Enterprise Security Suite Offering with the Highest Level of Security and Flexibility

The CrypToken® M2048 provides the centerpiece to MARX's full security offering. The CrypToken M2048 is powered by the MULTOS™ operating system, certified ITSEC Level E6 high, offering 64K memory providing the highest security available for two-factor authentication and embedded AES and RSA encryption. The CrypToken M2048 allows users to add two factor authentication into a wide area of security solutions supporting MS-CAPI or PKCS#11 standard encryption interfaces.

The CrypToken M2048 can run on any operating system with CCID support and no additional drivers, making it ideal for Windows® XP/2000/2003 operating systems as well as Mac OS/X and Linux. The MULTOS operating system loads and runs multiple fire walled applications independently on a single CrypToken providing the same capabilities commonly found on MULTOS-enabled smart cards, but in a standard USB form factor. The capability becomes increasingly important for banking and financial applications that require the breadth of an IT security infrastructure as well as the ability to manage banking and financial applications, including EMV-compliant requirements.

#### The MULTOS Foundation

MULTOS is the first, open, high-security multi-application operating system for smart cards. The elegance of the solution lies in the ability for diverse parties to develop applications that can run on the same card co-residing independently and securely. The capability enables an issuer to add or update applications in the field over un-secure channels utilizing the Secure Trusted Environment Provisioning (STEP™) scheme. Any modification requires a certificate and the STEP process guarantees data integrity, authenticity and confidentiality. This capability benefits both the issuer and the end user.

#### How It Works

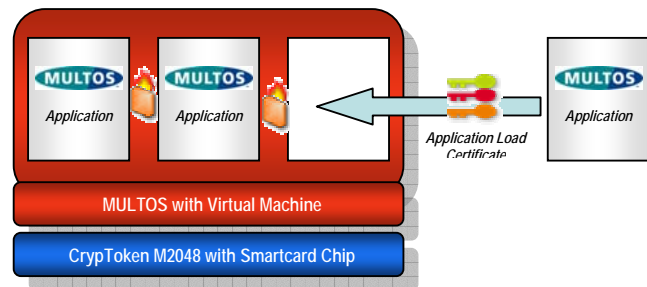
The security of MULTOS is ensured by a requirement for all MULTOS silicon providers to undergo a rigorous testing and evaluation process to prove interoperability, security and tamper resistance. No other available smart card platform can claim the same level of assurance.

MULTOS operates on a virtual machine, providing a hardware independent means to develop applications. This means that applications developed for one chip can be deployed on another. A system of memory firewalls ensures that applications cannot access data without

© 2006 MAOSCO Limited.

MULTOS is a trademark of StepNexus.

proper authorization. Card issuers and application developers establish their trust relationship through certificates. The application providers can rely on MULTOS that no other application can tamper with the code of another application.



*"MULTOS offered the most versatility to support the rigorous security needs required by our customers and to offer the most robust solution that included high security and support for multiple applications", Philipp Marx, President of MARX.*

The MULTOS-based CrypToken M2048 provides the baseline by which a number of enterprise security applications also offered by MARX are built around, including VPN perimeter protection, email encryption, digital signature, Windows logon, SSL client authentication, WLAN access and any security application supporting MS-CAPI or PKCS #11 standard encryption interfaces.

#### VPN Perimeter Protection

How do you know who is accessing your network through your VPN? How can you prevent a customer or business partner from choosing a password that is easily guessed, or prevent them from compromising the password by writing it down someplace easily accessible? Most VPNs manage their passwords and user names. Unfortunately, passwords are secure only if strict guidelines are followed. This is difficult to ensure with employees, and nearly impossible with customers and business partners.

The CrypToken M2048 provides strong, two-factor authentication. This tells you who is accessing your corporate network and prevents access from unauthorized users. The CrypToken M2048 also provides portability, enabling the use of many devices in a variety of locations. MULTOS on-board manages and secures digital certificates and cryptographic data that travel with you on the token.



# MULTOS for Embedded Security



## Email Encryption and Digital Signatures

Emails are like postcards. Everybody can read them as well as change the content on them along the way between sender and receiver. Often, email encryption solutions store your certificate directly on the hard drive – a potential target for eavesdroppers and intruders. If keys are lost or stolen, security is compromised and important information can become inaccessible.

MULTOS on CryptToken offers a highly secure and convenient way to store keys and certificates that can be used for email security. Working together with all common email applications, the CryptToken can encrypt and sign email contents and attachments using the keys stored on the token.

## Windows® Logon

A myth in the IT security arena is that security will improve if password complexity is increased. In most cases, when password complexity is increased, people tend to write down difficult passwords allowing systems and sensitive information to become vulnerable. IT managers also have to spend time resetting and unlocking difficult passwords that are forgotten.

Microsoft has integrated functionality for smart card login and management into the Windows domain servers. Therefore, if you are running Windows 2000 or 2003 Server, you do not have to purchase a separate authentication server to integrate CryptToken. The Public Key Infrastructure (PKI) includes a Certificate Authority (CA) for signing certificates, revocation, integration into Active Directory, and an enrollment system used to personalize the tokens and smart cards for the end user. MULTOS also provides for the secure storage of credentials to support single sign-on which is automatically entered into the Windows Gina logon process.

## SSL Client Authentication

eBusiness solutions, financial transactions and subscription services require reliable user authentication and secure transmission channels. This can be achieved with the combination of certificate-based client authentication and SSL transmission. However, the most difficult aspect of this scenario is ensuring that your certificate is stored in a safe place. To reach the highest security level, it is necessary to have the trusted storage capability that MULTOS on

CrypToken can offer. The solution is proven with X.509 certificates (S/MIME) or PGP keys.

## WLAN Authentication

New standards have been widely adopted by network equipment manufacturers that significantly improve security of Wireless LAN networks. These standards 802.11i and WPA2, including EAP and 802.1x enable the use of a central authentication server, session key rotation and user authentication based on digital certificates and public key cryptography. However, adoption of these standards has been slow due to the complexity of deploying and managing the client security, including keys, certificates and security settings.

The CryptToken M2048 provides a convenient and highly secure method for authenticating to a Wireless LAN. Working with all major Radius vendors, the token is ready to use with an EAP-TLS compatible certificate stored directly with MULTOS on the token. Together with a standard 802.1x compatible access point and an 802.1x compliant authentication server the CryptToken M2048 combined with MULTOS enables a highly secure Wireless LAN implementation.

## Summary

The MULTOS embedded, baseline operating system for MARX Data Security CryptToken M2048 offers unparalleled security and flexibility for applications targeted for protecting personal and enterprise information and content.

**MARX Data Security** has provided the software industry with security products since 1985. First focusing on software security, MARX enhanced their strategy to include the incorporation of USB tokens nearly ten years ago. The company is based in Germany and also has offices in the US, Poland, Italy and Ukraine.

The MARX client base includes a wide variety of companies, including small businesses, medium businesses and Fortune 500 corporations.

For more information about CryptToken M2048 and MARX Security Applications contact:

[www.cryptoken.com](http://www.cryptoken.com)

For more information about MULTOS contact:  
[info@multos.com](mailto:info@multos.com) or [www.multos.com](http://www.multos.com)