



STEALTHKEY™ M-Series 2011



Empowering mobile computing with secure USB solutions.

Portable security redefined.



Encrypted USB flash drives that meet
the strictest security standards.

STEALTHZONE™



STEALTHKEY™ M550



STEALTHHD^{BIO}™



MXI empowers the mobile workforce with its line of fast, affordable and secure portable storage devices. MXI Stealth Key M-Series USB devices enable employees to carry data safely, wherever they travel in the world. By combining the power of strong user authentication, hardware-based data encryption, and portable digital identities, MXI's innovative solutions provide the highest level of protection available against theft or loss of confidential information and systems.

MXI Stealth Key M-Series devices are designed to meet the highest security and privacy standards of even the most demanding clients. Our solutions enable organizations to satisfy multiple security needs with a single device, facilitating greater mobility without compromising security.

MXI Stealth Key M-Series devices are fully portable across all major computing platforms and require no drivers or software to be installed. All feature lifecycle management, and integrated digital identity and cryptographic capabilities. Most offer strong multifactor authentication, very flexible manageability and the ability to carry digital tokens.**



STEALTHKEY^{BIO}™ M700

A man with short, light brown hair, wearing a dark grey suit jacket, a light blue dress shirt, and a purple and white striped tie. He is looking upwards and to the left with a thoughtful expression. The background is a blurred cityscape.

The world's most secure hardware-based encryption

The rugged MXI Stealth Key M-Series offers on-board hardware encryption to transparently protect all content on your device — from data, applications and portable workspaces to digital identities.

The M-Series is powered by the on-board MXI Stealth Processor — the world's first dedicated portable security processor for USB devices and the first to offer FIPS 140-2 Level 3 validation.* The MXI Stealth Processor offers the highest data security and strongest user authentication mechanisms for government and corporate clients.

The innovative, AES-256 hardware encryption features of the MXI Stealth Processor include industry-first NIST SP800-56A secure communication, hardware-accelerated cryptographic function and hardware-based malware protection. Hardware encryption offers more security and portability than software-based encryption since no data is processed on the host computer (where it can be exposed to malicious software). Because this encryption happens on the device transparently, no software needs to be installed and the flash drive is as fully portable as a regular, unencrypted USB storage device.

STRONG MULTIFACTOR AUTHENTICATION

We ensure that your systems know it's really you. Strong user authentication is the best way to prevent unwanted access to data on stolen or lost USB devices.

MXI delivers the strongest authentication technology in the industry to give you the best front-line security. Our portable MXI Stealth Key M-Series devices are capable of multifactor authentication (password, optional biometric and CAC/PIV**) — all within the secure hardware environment of the device — to validate digital identity and protect on-board data. Even a compromised password isn't enough to break in when multifactor authentication is employed.

Since authentication is done completely within the MXI device, it is immune from software-based compromise at the host level. MXI devices are capable of automatic lockdown if too many authentications fail, adding a significant level of security to protect our clients' encrypted information. Optionally, data can be destroyed under these circumstances if the highest level of security is required.

MANAGEABILITY FOR ADMINISTRATORS

MXI Stealth Key M-Series portable security devices feature outstanding manageability systems for IT administrators. ACCESS Enterprise, our industry-leading device and identity-management system, allows administrators to easily deploy, manage and support any number of portable security devices on the network. MXI devices are also manageable through McAfee® ePO™ and the related U.S. DoD Host-Based Security System (HBSS), allowing large-scale organizations to integrate their portable USB storage devices into these standard management systems.***

ACCESS Enterprise also features:

- **Secure Server Policies.** The optional ACCESS Enterprise Server uses industry first, direct-device communication through a NIST SP800-56A certified, authenticated secure channel. The server directly applies policies to devices, bypassing client software on the host, for true security and immunity from malware. AE Server's self-rescue feature ensures that devices remain accessible, even if a user forgets their password or damages their fingerprint. Conversely, device revocation allows compromised devices to be blocked or even have their data erased remotely, preventing data leakage.
- **Streamlined Workflows.** ACCESS Enterprise reduces overhead for administrators while still providing an intuitive and productive experience for users.
- **Tailored to Each User.** Administrators can tailor security policies and portable security device behavior to different user needs. Policies for authentication — such as password complexity rules, biometric security levels and retry limits — can be adjusted to the needs of each group of users.
- **Advanced Reporting.** ACCESS Enterprise gives the option of logging and storing a complete history of administrative activities, security policies and respective state of each individual device. Administrators can accurately log audit and compliance information for increased security.
- **Improved Data Recovery.** Help desk operators can re-establish access to the device or even permanently erase all of the device's data when users fail to authenticate their USB device. Easy to implement password and biometric recovery options are available to rescue blocked users, even if they are away from the corporate network.

OTHER FEATURES OF THE M-SERIES

Digital Identity. Our unique digital identity solutions offer one-time passwords (e.g. RSA SecurID®), dedicated key containers, on-board key generation, secure X.509 certificate storage via PKCS#11 and/or CAPI, and hardware cryptographic acceleration.** MXI's powerful on-board MXI Stealth Processor binds digital identities to users and protects them with up to 3-factor hardware-based authentication — vital for our most security-conscious customers. ACCESS Identity, our identity-management software suite available Q1 2011, allows mission-critical enterprise systems such as single sign-on, remote access, full disk encryption, comprehensive PKI token services, and others to be fully secured while allowing for total portability.***

Powerful Anti-Malware. ACCESS Antivirus Scanner is optionally available on the MXI Stealth Key M-Series. Using powerful McAfee® antivirus technology, it protects the information on your USB drive from viruses, worms, trojans and other malware threats. ACCESS Antivirus Scanner notifies the user immediately if they plug their USB device into an infected host computer. The scanner is always on alert, constantly monitoring data transfers to ensure that malware will not be transferred to the device.

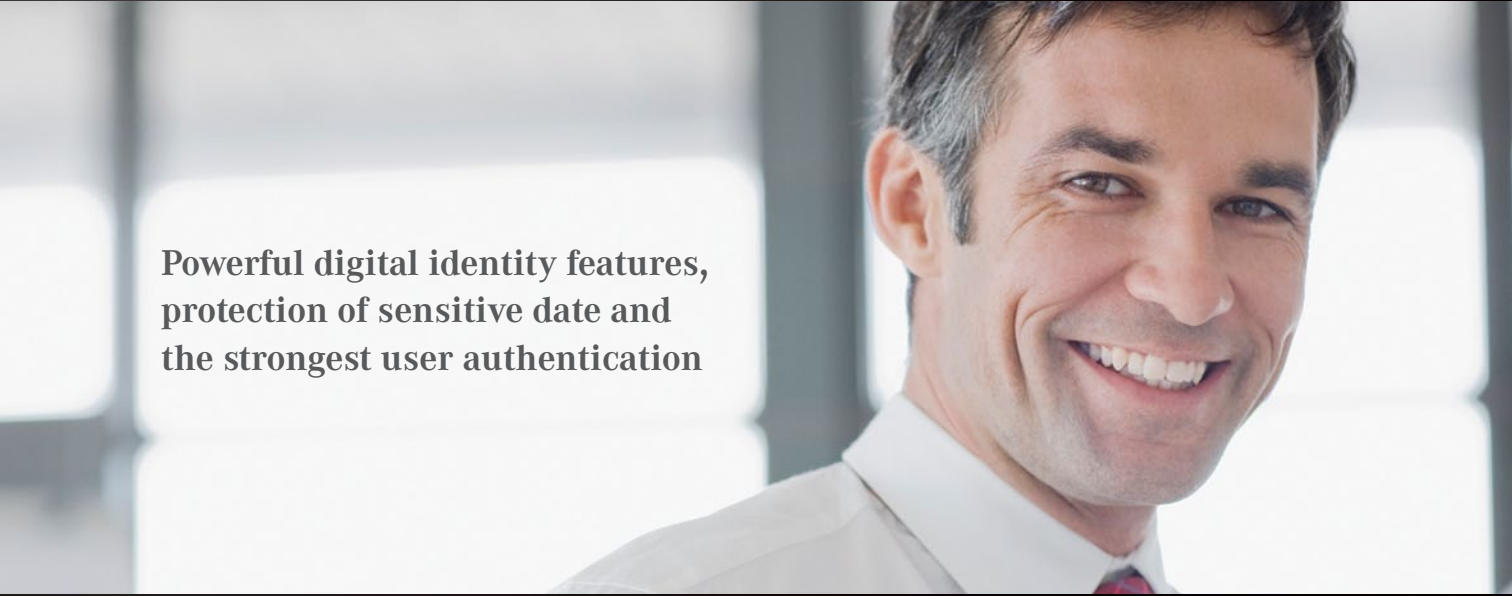
Customizable to Your Enterprise. MXI solutions can be specifically tailored to meet the unique security, compliance and manageability needs of each individual organization. We offer unparalleled customer support to ensure that your expectations are exceeded and future needs anticipated.

Multi-User Support. MXI's SafeShare™ technology, unique in the industry, permits up to 10 users of MXI Stealth Key M-Series devices to collaborate using on-device data without compromising its safety.

STEALTHKEY™ M550



Industry applications



**Powerful digital identity features,
protection of sensitive data and
the strongest user authentication**

CORPORATE

MXI Stealth Key M-Series devices can meet the mobile security and risk-management needs of a wide range of corporate clients, from sole practitioners to large-scale enterprises. All MXI encrypted USB devices enable secure mobile computing and keep on-board data safe, thanks to hardware-based AES-256 encryption, strong multifactor user authentication to protect digital identities, and anti-malware technology. The M-Series features an innovative, tamper-evident enclosure which acts as an integral case, making these devices waterproof and dustproof, and well-suited to very mobile workers.

For employees who need off-site safe access to an IT-managed work environment, MXI Stealth Zone is an innovative platform that transforms shared systems, home computers, or other unsecured computers into fully secure, isolated computing environments. A secure portable desktop — including data, applications and an entire operating system — can be placed directly onto the high-security USB device. After booting from the USB device and authenticating identity, computing happens on the encrypted device, safe from any threats from the unsecured host computer, and no trace of the user is left behind on the host. (MXI Stealth Zone is supported on M500/550 and M700 Bio).

GOVERNMENT / AGENCY

MXI's cryptographically secure devices were the first to receive FIPS 140-2 Level 3 validation, which allows government and military users to meet compliance regulations. Featuring hardware-based AES-256 encryption, strong multifactor user authentication (password, optional biometric and CAC/PIV) to protect digital identities, and anti-malware protection, MXI solutions keep on-board data safe when government employees are working off-site. With secure PKI token functionality and the ability to carry RSA SecurID® soft tokens (requires ACCESS Identity, available Q1 2011), MXI devices integrate seamlessly into your IT infrastructure. They can be managed with MXI ACCESS Enterprise, McAfee® ePO™ or the related DoD Host-Based Security System (HBSS).



HEALTHCARE

Patient confidentiality means private records must be secure. Health care professionals and employees of bio-technology or pharmaceutical companies can't risk leakage of personally identifiable health-care information or confidential research & development data through theft or malware. Offering strong multifactor user authentication (password, optional biometric and CAC/PIV) to protect digital identities, and anti-malware protection, the hardware-encrypted MXI Stealth Key M-Series keeps on-board data safe when health care workers are working off-site.



FINANCIAL SERVICES

Financial firms continue to face a number of challenges in assuring their customers that their identities, assets and transactions are fully safe. MXI offers proven solutions for mobile employees in the financial sector that are expertly designed for security and convenience, while protecting access to and the integrity of customer and financial records.

PROFESSIONAL SERVICES

Solid client relationships are at the foundation of professional services, and the sanctity of trust includes protecting your clients' information. The mobility that is characteristic of professional services practitioners requires a secure means of carrying confidential client data and, frequently, access to a fully secure, managed, off-site work environment through our optional MXI Stealth Zone platform. When using an unsecured computer, MXI Stealth Zone allows employees to boot from the MXI device and work securely within the trusted, encrypted environment of the device.



STEALTHZONE™

A safe, portable desktop solution that secures untrusted computers.



We believe that the future of enterprise computing is having 'anywhere access' to data in the most secure way. MXI continues to engineer better and more feature-rich solutions to enable the most secure mobile computing possible. MXI Stealth Zone — optionally available on most MXI devices — is a groundbreaking platform that enables employees to take their entire desktop with them and compute securely on their USB device.

MXI Stealth Zone's boot-from-USB technology instantly transforms any untrusted computer — shared systems, home computers or public computers — into a safe computing environment. By deploying a Secure USB Desktop (SUD) environment on a high-security device, MXI Stealth Zone instantly transforms any unsecured computer into a standard IT-managed system while maintaining both performance and security. Leveraging MXI's industry-leading strong authentication technologies and hardware-based encryption, MXI Stealth Zone protects the applications, operating system and data on the USB device.

The on-board MXI Stealth Processor brings advanced features to the MXI Stealth Zone platform:

- **Encrypted Storage.** Cryptographically secure lockdown of content shields the desktop from even the worst environments, preventing tampering, intrusion and piracy. FIPS 140-2 Level 3 validated.
- **Secure Preboot Authentication.** Access to the hardware-encrypted desktop requires up to 3-factor authentication, including password, optional biometric and CAC/PIV.
- **Host Isolation.** Insert your MXI USB drive into the host computer, then reboot and authenticate. The computing environment is now fully isolated from both malware and data leakage.
- **Optional Secure Portable Storage.** A separate, secure partition allows exchange of data between the MXI Stealth Zone environment and other computing environments.
- **Optional PKI Token Operation.** Secure key and certificate stores, hardware key generation, digital signing, and a range of other user PKI operations are possible within the USB desktop.

Who benefits from Secure USB Desktops?

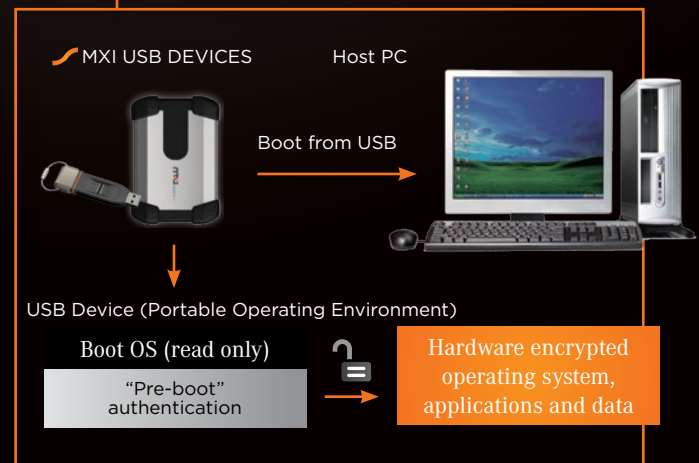
- **Teleworking.** Users can work remotely, whether it's from home, on the road, or the extended offsite of in-theatre soldiers.
- **Disaster Recovery.** When normal systems are inaccessible or potentially destroyed as the result of terrorism, weather conditions or health quarantines, preconfigured portable environments can be distributed as easily as a USB device.
- **Temporary Personnel.** Temporary workers, such as contractors, can be given an environment to use on their own hardware.
- **Separation of Desktop Environments.** When regulatory or security issues demand that users separate work environments for different projects or tasks, MXI Stealth Zone enables deploying of these environments using a single computer.
- **Secure Transactions and Online Banking.** Users can combine a portable web browser with a full-featured PKI token for 'anywhere, anytime' certificate-based authentication.

How It Works

1. *Shut down host computer.*
2. *Insert MXI device enabled with MXI Stealth Zone into USB slot.*
3. *Reboot.*
4. *Authenticate identity.*
5. *You're now in the Zone.*

You now have access to the full operating system and desktop applications on the USB device in a safe, isolated environment where your data remains secure. Cryptographically secure lockdown of content shields the desktop from even the worst environments, preventing tampering, intrusion and piracy.

When you leave, you take your USB desktop with you and no trace of your presence remains behind on the host, meaning you're not left exposed to malicious data miners and other threats.



Products



STEALTHKEY™ M200
STEALTHKEY™ M500

STEALTHKEY™ M550

STEALTHKEY™ M700bio

M200. Affordable, secure encrypted storage

MXI Stealth Key M200 offers the best in affordable, secure portable storage for individuals and smaller, unmanaged deployments. Available in capacities up to 64GB, the M200 can accommodate an entire desktop, giving the mobile employee off-site functionality without sacrificing security.

Unlike the average unencrypted flash drives on the market, the M200 features fast and transparent hardware-based encryption to protect data and digital identity. Strong password authentication, combined with hardware-enforced complexity and usage rules, ensures that your data will remain secure when you are on the move. The optional Antivirus Scanner adds another layer of protection, with on-board malware protection. With no software or drivers to install, this is the perfect zero footprint, secure mobile storage device.

M500. Full-featured, IT-managed USB drive

Cost-effective security is within reach thanks to the MXI Stealth Key M500. Like all our devices, it offers fast and transparent hardware-based encryption and strong user authentication, with added device management systems for administrators and the ability to carry digital identities.

MXI Stealth Key M500 builds on the feature set of our entry-level devices by adding RSA SecurID® technology and PKI features, as well as ACCESS Enterprise, the central-management system that enables administrators to deploy, provision and manage the devices. ACCESS Identity, available Q1 2011, allows the M500's hardware digital identity features to be leveraged by nearly any system in the organization employing certificate-based or RSA SecurID-based security. The ability to carry multiple PKI-based digital identities and/or RSA SecurID® soft tokens – issued with a single click in ACCESS Enterprise – provides strong two-factor authentication to critical systems and information.

The MXI Stealth Key M500 can also accommodate MXI Stealth Zone, an innovative platform that allows you to boot from the USB and transform any untrusted, unsecured computer into a fully secure, managed IT environment.

M550. Rugged, durable design for road warriors

MXI Stealth Key M550 offers the full feature set of the M500 and adds a rugged casing — a lightweight, tamper-evident metal enclosure with steel ring attached. This crush-resistant, thixotropically injected magnesium enclosure was designed for rugged use by road warriors.

M700 Bio Fingerprint authentication confirms identity

MXI Stealth Key M700 Bio is designed for mobile users who need secure, multifactor authentication technology, along with high-capacity storage and protection of data and digital identity. The device features hardware-based encryption thanks to the on-board MXI Stealth Processor (which is FIPS 140-2 Level 3 validated), as well as the strongest multifactor authentication available in the industry.

Unlike common single-factor authentication devices, data on board the MXI Stealth Key M700 Bio is protected with 2-factor authentication. Biometric authentication is made possible through an ergonomic finger-swipe sensor, with hardware-based matching that is fully isolated from PC-based attacks. Coupled with this technology is strong password authentication that offers hardware-enforced complexity and usage rules. In addition, 3-factor authentication protects PKI token and RSA SecurID® operations. The device can accommodate MXI Stealth Zone, an innovative platform that allows you to boot from the USB and transform any untrusted, unsecured computer into a fully secure, managed IT environment.

Specifications



General

Secure portable storage with hardware-based AES-256 CBC mode encryption (FIPS Pub 197)
Encrypted mass storage capacities: 1, 2, 4, 8, 16, 32 and 64GB
Zero software footprint
Secure PKI token functionality**
Ability to carry RSA SecurID® soft tokens**
Manageable with ACCESS Enterprise
Manageable with McAfee® ePO™ and HBSS
One-year warranty

Authentication

Up to 2-factor for secure portable storage:
Strong password
Optional CAC/PIV
Two-factor for RSA SecurID® digital identity applications**

Security

MXI Stealth Processor (FIPS 140-2 Level 3 validated)
Hardware-enforced password complexity and usage rules
Failed authentication threshold with optional data destruction
Anti-malware protection
SafeShare™ technology allows up to 10 independently secured users on a single device
Device administrator role for secure management
Optional user rescue for blocked devices
Anti-MITM, anti-replay secure host-device communications compliant with NIST SP800-56A

Storage

Flash memory mass storage
Private user partition(s), hardware encrypted, size-configurable
Portable application partition, read-only, malware-proof

Standards and Certifications

USB 1.1 and 2.0
FCC
CE
WEEE compliant
RoHS compliant

Physical and Electrical

Compact and portable
Tamper-evident plastic enclosure with removable cap
Waterproof and dustproof enclosure to IEC 60529 IP57
Waterproof enclosure to MIL-STD-810F
LEDs for power, data activity and authentication status
Uses USB bus power

Dimensions, Weights and Environmental

Dimensions, cap on (H x W x L): 12.5 x 21.5 x 76 mm
Dimensions M700 bio (H x W x L): 13 x 26 x 85 mm
Dimensions, cap off (H x W x L): 12.5 x 21.5 x 75 mm
Dimensions M700 bio (H x W x L): 13 x 26 x 84 mm
Weight: 14g M700bio: 29g (approximate)
Operating temperature {0 to 60 °C}
Storage temperature {-20 to 70 °C}
Relative humidity {5 to 95% non-condensing}

Operating Environments

Microsoft Windows® 7, Vista, and XP (64 and 32-bit)
Mac OSX® 10.5 and 10.6 (Intel only)

* Specifications are for MXI Stealth Key M500.

** Requires ACCESS Identity, available Q1 2011.

*** Lightweight, thixotropically injected magnesium enclosure available on MXI Stealth Key M550 and M700 Bio.



SECURITY

MXI facilitates greater worker mobility without compromising security. We provide leading-edge technology for data security, portable enterprise computing and digital identities. For our clients this means peace-of-mind: their data, applications and portable workspaces are protected with the most complete set of security certifications in the industry.

CONTROL

Superior manageability systems give IT administrators flexible control over MXI devices. Our solutions integrate seamlessly into your organization's IT infrastructure, offering centralized, enterprise-class security management and reporting systems. Manageability is transparent to the end user, with no drivers or software for them to install.

INNOVATION

MXI is the industry-leading provider of managed portable security solutions. Our first-to-market technologies address the portable security needs of a wide range of enterprise and government clients globally, offering industry-leading hardware encryption, strong user authentication and innovative software solutions.

Contact us

Technical Support
TECHSUPPORT@MXISEcurity.COM

Sales
SALES@MXISEcurity.COM

GSA GS-35F-0142S

CANADA

2321 Cohen St.
Montreal, Quebec
Canada H4R 2N7
Tel.: (514) 333-5010
Toll free: (888) 422-6726
Fax: (514) 333-5020

USA

1651 E. St. Andrew Place
Santa Ana, CA
USA 92705-4932
Tel.: (714) 258-3000
Toll free: (888) 440-0400
Fax: (714) 258-3040

EUROPE

Saracen House, Swan Street
Old Isleworth
Middlesex, UK TW7 6RJ
Tel.: +44 (0) 208-758-9600
Fax: +44 (0) 208-758-9601

ASIA

201 Tesbury Centre
28 Queen's Rd East
Wan Chai, Hong Kong
Tel: +852-2147 5880
Fax: +852-2147 5881



ISO 9001
ISO 14001

