

## DELIVERING CONFIDENCE – EMPOWERING DATA SECURITY FOR CARD ISSUERS

Our physical and logical security solutions include the technologies and best practices you need to pass your security audits. Our solutions also reduce the risk of fraud and theft by safeguarding cardholder data, production data, and access to the card issuance systems, without slowing the issuance process.

When configured properly, the Datacard MX9100™, MX8100™, MX6100™, MX2100™, and MX1100™ card issuance systems meet or exceed PCI-CP 2.0, PCI-DSS 3.0, and other stringent security standards.

**Multiple lines of defense help ensure physical and logical card security.** Entrust understands the critical security concerns within card operations. Our security solutions help card issuers pass security audits and offer multiple lines of defense to safeguard cardholder data, production data, and access to card issuance systems – leading the way in overall security and accountability.

**Data protection starts with software.** Datacard system controller software allows customers to segregate data from operators – and segregate operator and administrator logins to meet or exceed PCI Data Security Standards (PCI-DSS). The Datacard Security Implementation Guide provides recommended security settings, making it easier to achieve the right level of protection. For set-up efficiency, system controller PCs are shipped pre-configured with these settings. In addition, customized or advanced levels of security, auditing, and event logging can be configured easily.

**Patch management maximizes operational efficiencies and security compliance.** Before distribution, Entrust tests all relevant security patches for Microsoft® and other software to help ensure new patches do not interrupt or slow card production. All approved patches are available as part of our Software Maintenance Agreements (SMAs).

**Exceptional levels of physical security.** The design of our system controller cabinet restricts access to hard drives and USB ports. For even greater protection, USB ports and DVD/CD-ROM drives can be disabled logically. Other options include locking tray covers and module hoods to prevent unauthorized access to cards in all stages of production.

**Expert professional services help maintain system security.** Entrust offers professional services to help you prepare for stringent security audits. With extensive industry expertise, Entrust technicians adhere to best practices to ensure the system is returned to its secure state once updates and diagnostics are complete.

**Learn more about the MX Series at [entrust.com](https://www.entrust.com)**

Physical Security of System	Logical Security of System Software	Security Services	Other Solutions
<ul style="list-style-type: none"> <li>• Single system controller PC reduces data files in use</li> <li>• Closed bezel reduces access to sensitive data files</li> <li>• Locked controller PC enclosure limits unauthorized access to USB ports and DVD/CD-ROM</li> <li>• Ability to disable USB ports (and/or DVD/CD-ROM) when needed, while still retaining dongle functionality for service support needs</li> <li>• Topping foil splitting kit</li> <li>• Locking input trays*</li> <li>• Locking output trays*</li> <li>• Locking module hoods*</li> </ul> <p>* Available on the MX9100, MX8100, and MX6100 Card Issuance Systems</p>	<p>Robust options for identity access management (IAM) implementation:</p> <ul style="list-style-type: none"> <li>• Role-based access control (RBAC)</li> <li>• Strong password and Microsoft® Windows® OS domain support</li> <li>• Support for corporate security profiles</li> <li>• Traceability of all operational activities</li> <li>• Advanced security options for database encryption</li> <li>• Data deletion upon job completion</li> <li>• Controller PCs shipped from factory pre-configured with recommended Windows OS security settings</li> <li>• Adaptive Issuance Key Manager Software provides secure access to keys and cryptographic functions during personalization, making sure the keys and sensitive information is protected</li> </ul>	<ul style="list-style-type: none"> <li>• Security Patch Management service in the CIS software provides approved patches, as part of SMA program</li> <li>• Site assessment services relating to security audit preparation</li> <li>• Server relocation and re-hosting services</li> <li>• Secure administrative process for managing customer trace files</li> </ul>	<ul style="list-style-type: none"> <li>• On-demand data fetching to achieve centralized data management</li> <li>• Tight integration of MX Series hardware to your IT infrastructure to remove operator intervention when starting, loading, or removing jobs</li> <li>• Custom audit data handling</li> <li>• Data Security Software software protects both data-in-motion and data-at-rest, provides data confidentiality and secures data access and transactions</li> </ul>

 [Learn more about the MX Series at entrust.com](https://www.entrust.com)

