MAGENSA™

A MAGTEK COMPANY

Security

Device Authentication

A standard feature of Magensa Web Services is protecting transactions and securing against rogue devices

Beyond just IDs

Magensa provides authentication for personal electronic devices including payment terminals, PIN encrypting devices, card and check readers, and card issuing units. Legitimate devices can be identified and authorized for use while rogue devices can be identified and stopped before they are used to commit fraud.

Know that the devices you are communicating with are legitimate. Device Management goes beyond merchant IDs and terminal IDs and makes it impossible for rogue and tampered devices to communicate with your network. Using a proven mutual authentication technique, secured devices are programmed to generate an encrypted challenge and communicate directly to Magensa using a TLS connection. Magensa in turn responds with a unique, one-time response to arm the device for operation. This mutual authentication allows both the user and the host to validate their identities. If one does not recognize the other as legitimate, the authentication will fail and the device will be disabled.

Digital Signatures:

Protect your data from redirection. Magensa uses Digital Signatures which work much like a hand signature for verification with added security. Redirection becomes impossible since Digital Signatures authenticate the actual sender which provides non-repudiation and verification that incoming messages are coming from the expected source.

Session IDs:

Guard against in transit data attacks. Magensa provides you with the tools you need to help prevent man-in-the-middle attacks using Session IDs. Session IDs deliver time stamp capabilities and limit to the duration on communication sessions securing your transactions in transit.

Remote Services

Device Enablement

Magensa can be programmed to remotely enable and configure your device for operation. After the device and Magensa have been mutually authenticated, a digital certificate is transmitted to the device, enabling the machine to operate for a predetermined period of time which can be defined by the user.

Device Disablement

Magensa can use the same infrastructure described above to configure and disable your device for operation. If you choose to disable a device, then it will remain non-operational until such time it is re-enabled thru Magensa Web Services. This service mitigates your liability and allows you to remotely control any device connected to the network.

Key Injection

Save time and resources with secure remote key injection and key management by Magensa. Magensa's secure infrastructure allows institutions to safely and remotely inject encryption keys, minimizing risk, lowering costs and enhancing overall operations.

Life Cycle Management

Magensa delivers certified and safe key injection and limits device liability. Magensa delivers protection against third party and rogue devices by providing secure initial key injection and life cycle management. Devices can no longer be bought and sold through third party, unverified sources, preventing insidious efforts.

Compliance and Certifications	
MagTek	ISO 9001:2015
	Terminal Quality Management
	TR-39 (TG3) / PCI PIN compliant
	EMVCo
	ROHS
Magensa	PCI DSS
	PCI 3.x PTS | PCI 4.x PTS
	TR-39 (TG3) / PCI PIN compliant

MAGENSA™
A MAGTEK COMPANY

Serving enterprises globally, Magensa provides a wide range of innovative tools and transaction processing services for authentication, cryptographic security, and privatization of sensitive data. Magensa's encryption/decryption services, payment gateway services, tokenization services, remote services, and applications are used by software developers, ISVs and systems integrators to bring their applications to market faster and more securely. Magensa's services and solutions are trusted by commercial, retail, financial and government enterprises without compromise. Magensa, LLC is a subsidiary of MagTek, Inc.