



Magensa Decrypt Data Protection with Key Management

Easily Handle Encrypted Data

Magensa Decrypt allows VARs and ISOs to bring encrypted data from remote points of interaction to a central location for secure exchange of encrypted to decrypted data. It also allows for the secure storage, management, and application of encryption keys. Encrypted data travels through existing systems “masked” as unencrypted data, allowing encrypted data to travel in older transaction systems. When the data reaches the central location, the central location exchanges

encrypted data for decrypted data through Magensa, at the same time, Magensa provides card and device authentication and tokenization of data. The central host can then do with the data all it needs to and sends the necessary details out for processing or other transaction types. This allows VARs and ISOs to help bring their customers up to PCI regulations by passing encrypted data through their transaction environment and limiting the scope of their PCI audit.

Centralized Focus

This central location approach limits the locations where an in-depth PCI audit is necessary. In the remote locations, where the data is always encrypted, the PCI scope is greatly reduced because the data is never in the clear. The data is only decrypted in one central location where an in-depth PCI audit will be required. The central host decides what data is returned to the POS app and out for processing and other transaction processes.

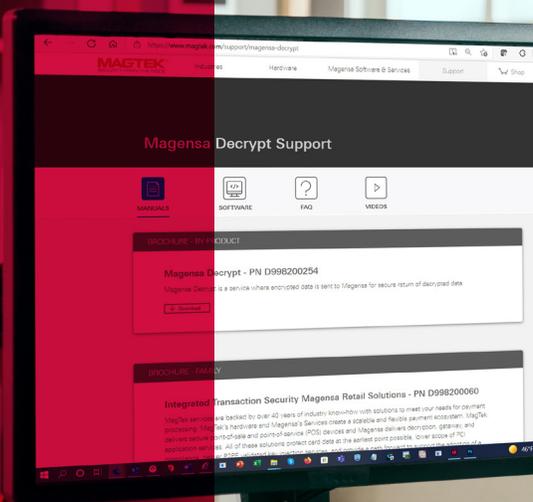
Recommended for

Magensa Decrypt Services are recommended for the most sophisticated user. The greater the challenge and the more development you can handle, the better Magensa Decrypt is suited for your needs.

Security

Magensa Decrypt Services include encryption and decryption that deliver practical solutions for data protection and exceed current PCI DSS regulations. Magensa uses open standard and industry proven Triple DES encryption and DUKPT (derived unique key per transaction) key management to provide a comprehensive security solution that protects cardholder data.

- Limit PCI Scope
- Support Loyalty and Reward Programs
- Include Other Types of Personally Identifiable Information (PII)
- Support Magstripe, Barcode, Chip and NFC
- Key Generation and Management



To get started contact:
retail.solutions@magtek.com

Open Platform

Its open platform does not require you to invest in costly, untested, proprietary solutions that can limit your long-term flexibility and options.

Secure Hardware

MagTek secure card reader authenticators and PIN PEDs deliver instant encryption inside the hardware, which is more secure than software. This places only encrypted data into the transaction environment and secures the data while in the system under test.

Key Benefits

Magensa Decrypt uses tested and proven encryption methods and key management schemes.

1. Reduce the span of your payment environment that requires the highest level of security.
2. Deliver device authentication that checks for rogue devices and verifies the host to the device.
3. Reduce PCI scope to centralized locations.

Magensa Decrypt delivers an easier path to taking and using encrypted card data in your transaction environment.



Use Case

The Challenge

A major vehicle rental company wanted to limit their PCI Scope at all of its various locations nationwide, but still needed to be able to access loyalty and transactional information.

The Solution

By using Magensa Decrypt Services and MagTek secure card reader authentication devices, we were able to instantly encrypt the cardholder data at the first point of interaction, and send the encrypted data to a central host location. The central host location communicated with Magensa Decrypt Services and the data was sent over secure lines for decryption. Unencrypted data was returned via secure lines and used for loyalty programs and other transactional details. The host was the only location where unencrypted data was held and became the main focus for security measures and audits.

The Result

The result is a reduced PCI audit that allows focus on one main location. The data everywhere else is encrypted and secured using triple DES encryption with DUKPT key management. This limits replay attempts and man in the middle attacks, since each encrypted transaction can only be used once.

1. Card Reader/POS app
Sends encrypted data

2. POS app/Host
Sends encrypted data

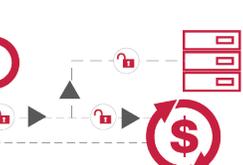
3. Host /Magensa
Host sends encrypted data to Magensa

4. Host/Processor/other
Host sends to other/processing

Magensa returns decrypted data and device & card authentication

Other/processor send response back to host

5. Host/POS app
Host forwards response
Host sends card auth & device auth



Card Reader
Contactless

POS application
Countertop or
Mobile Device

Central Host
Networked

Magensa Web Service
Decrypt

Processor/Other

MAGTEK
SECURITY FROM THE INSIDE

Founded in 1972, MagTek is a leading manufacturer of electronic systems for the reliable issuance, reading, transmission, and security of cards, barcodes, checks, PINs, and identification documents. Leading with innovation and engineering excellence, MagTek is known for quality and dependability. Our hardware products include secure card reader/authenticators, Owantum secure cards, token generators; EMV Contact Chip, EMV Contactless, barcode and NFC reading devices; encrypting check scanners, PIN pads, and credential personalization systems. These products all connect to Magensa, a MagTek owned gateway that offers businesses the ability to securely process transactions using authentication, encryption, tokenization, and non-static data. MagTek is headquartered in Seal Beach, CA, please visit www.magtek.com to learn more.

MagTek Inc. | www.magtek.com |

Registered to ISO 9001:2015 © Copyright 2023 MagTek, Inc. PN D998200254 v200 12/23
The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by MagTek is under license.