

Magensa Decrypt Service

Magensa Decrypt is a service where encrypted data is sent to Magensa for secure return of decrypted data



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 data for decrypted data with Magensa. 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 with 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 also receives the added benefit of Magensa Web Service features including card authentication, through the Global MagnePrint Exchange; device authentication, with verified devices; and tokenization using either the MagnePrint or encrypted block. The central host decides what data is returned to the POS app and out for processing and other transaction processes.



Security

Magensa Decrypt Services include encryption and decryption that deliver practical solutions for data protection and exceed current PCI DSS regulations. Magensa utilizes 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. Its open platform does not require you to invest in costly, untested, proprietary solutions that can limit your long-term flexibility and options. 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 systems under test.



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.

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.



Benefits of Magensa Decrypt

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. Deliver card authentication of magnetic stripe cards, and check for counterfeit or altered magnetic stripe cards. Even if EMV chips are present on cards, magnetic stripes are used as a back-up method to make transactions. By verifying the magnetic stripe you can verify authenticity of cards.

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



Web Services

Magensa Global MagnePrint® Exchange (card authentication), Magensa Device Authentication, and Tokenization are included with this service at no additional charge.

