MAGENSA™

A MAGTEK COMPANY

Magensa TokenExchange

Encrypting and Manipulating Data

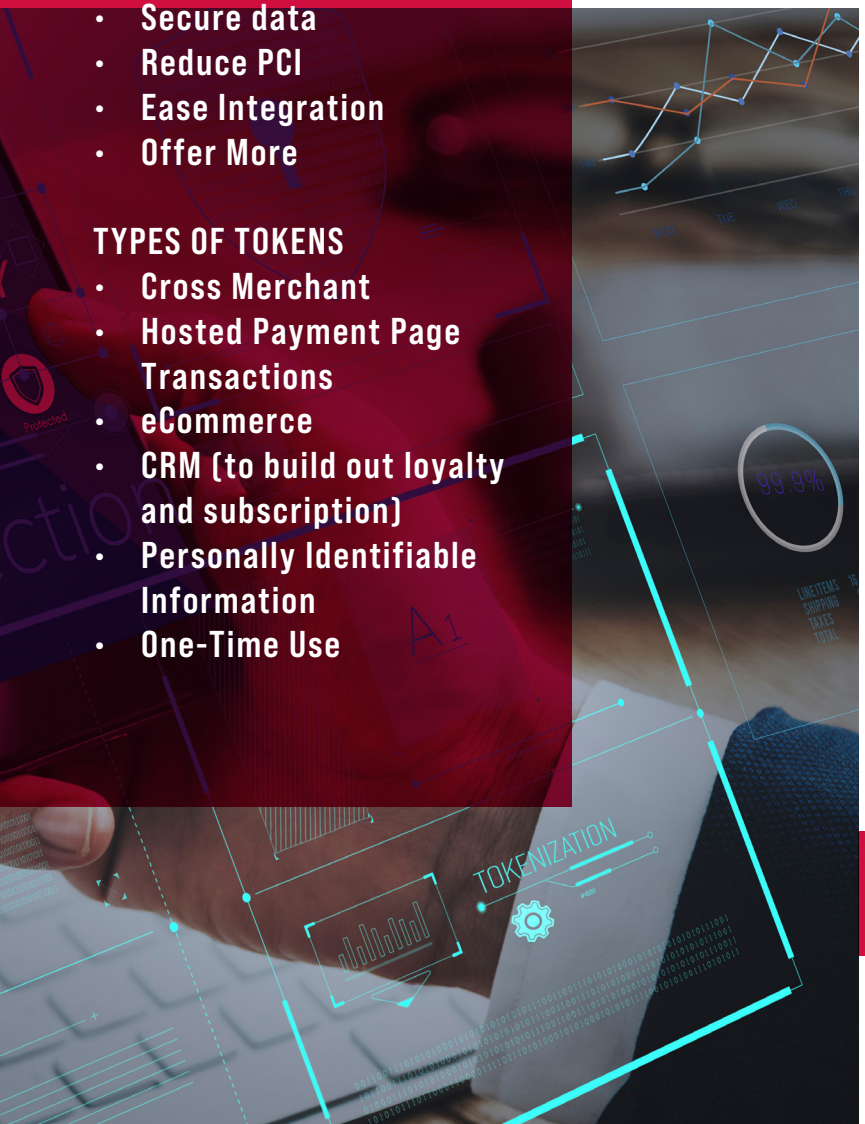
Tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security. Magensa Tokenization Services are cloud-based, data protection services supporting the generation, transport, and redemption of dynamically generated tokens integrated into applications and business processes. Magensa TokenExchange provides a unique way of anonymizing and protecting sensitive information.

KEY BENEFITS

- Secure data
- Reduce PCI
- Ease Integration
- Offer More

TYPES OF TOKENS

- Cross Merchant
- Hosted Payment Page Transactions
- eCommerce
- CRM (to build out loyalty and subscription)
- Personally Identifiable Information
- One-Time Use



Platform-as-a-Service

Magensa's tokenization is delivered as a Platform-as-a-Service (PaaS), a type of cloud computing service that provides a platform that allows customers to develop, run, and manage applications without the complexity of building and maintaining infrastructure typically associated with developing and launching an application. The benefits include faster launch time, less cost, and lower operating expenses.

Security and Key Management

Magensa's encrypted tokens are resilient to quantum computer hacking techniques. Tokens are created by leveraging symmetric key encryption within a hardware security module (HSM) using AES/3DES encryption by a derived unique key per transaction (DUKPT). Merchants never have access to clear-text data. Tokens are securely generated and accessed.

Dynamic Tokenization

Dynamic tokenization means a unique token generates every time using a unique encryption key for each token created. Tokenizing encrypted data is more secure.

Vaultless Tokenization

Vaultless tokens mean the customer maintains custodianship of the data as an encrypted token that they can store or Magensa will store on their behalf.

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

MagTek® Inc. | 1710 Apollo Court, Seal Beach, CA 90740
www.magtek.com | 562.546.6400

Token Generation and Redemption

Privatize All Sensitive Data

Sensitive information should remain private to prevent any harm to the owner.

- Personally Identifiable Information (PII) is any data that can identify a person, i.e., PANs (regulated by PCI-DSS), social security numbers, email, phone, etc.
- Protected Health Information (PHI) is a specialized form of PII data that includes anything used in a medical context that can identify patients.

Sensitive data exists in two forms:

1. **Data in-flight**: Any data being transmitted or transferred between locations, often over a network.
2. **Data at-rest:** For example, vast quantities of information reside in data warehouses and repositories. By replacing sensitive data with tokens, which have no extrinsic or exploitable meaning or value, the content in these databases is protected from compromise. Compared to encryption, tokenization lowers processing and storage requirements, creating the perfect solution for securing large volumes of data.

How Magensa Tokenization Works

Data is anonymized and protected in-flight and at-rest by generating and redeeming dynamic tokens.

1. Customers are onboarded and their payment application connects to the tokenization services through the ***Magensa Payment Protection Gateway Service*** or ***Decrypt and Forward Service***.
2. Sensitive data is sent to Magensa for token generation.
3. Magensa creates tokens, encrypts them, and returns them back to the business to hold.
4. When the tokenized sensitive data needs to be viewed or processed, the business sends the encrypted tokens to Magensa for decryption and return or securely forwards to other endpoints for processing.

Implementations and Applications

Magensa Tokenization Services are implemented in a wide variety of payment and non-payment environments.

Magensa TokenExchange

The token generation and redemption back-end service for a variety of token types where Token storage is available through the Magensa TokenHub to support Magensa TokenExchange requirements or special use cases including format preserving needs.

Magensa TokenExchange Connect

Secure eCommerce Payment Tokens are facilitated with embedded client-side JavaScript enabling direct connection to a Magensa hosted, customer branded, payment iFrame form that enables ISVs to secure sensitive data.

In the payment environment

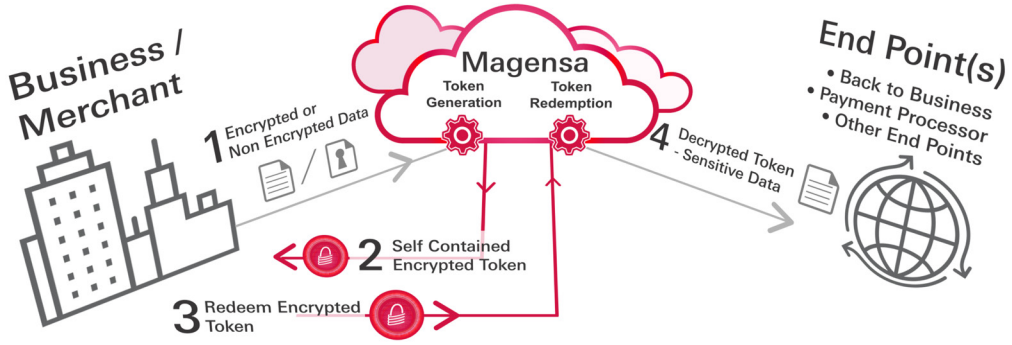
Magensa Tokenization Service are often used in payments.

- **Masking:** Card-on-file, tipping, and authorization and capture data.
- **Reduce PCI Scope:** When cardholder data (PAN and expiration date) is encrypted at the time the card is swiped and then a token is returned for settlement purposes, the merchant significantly reduces PCI-DSS scope since they do not have access to clear-text data.

In non-payment environments

Magensa Token Web Service enables Token Generation and Token Redemption operations.

- **Cloak Sensitive Data for Analytics:** Tokens are an excellent solution to cloak sensitive data while still providing valuable data to analytics tools to provide actionable information.
- **Customer Tracking:** Instead of cardholder data, tokens are an excellent alternative to track the transaction process and use this information to better serve and market to customers.



MAGTEK®
SECURITY FROM THE INSIDE

Magensa provides software developers with a wide range of innovative tools and services for authentication, data security, and identity management. Using Magensa encryption/decryption services, tokenization, payment gateway services and APIs, ISVs and integrators bring their applications to market faster and more securely. Magensa's distributed, end-to-end security and privacy solutions have been trusted by commercial, financial and government enterprises for years, and without compromise. Privatize Sensitive Data with Integrity.