ENCRYPTION & TOKENIZAITON

Alliance Token Manager
Data Sheet

Alliance Token Manager

Protect against data loss and simplify compliance for data privacy standards.

What is Tokenization

Alliance Token Manager allows Enterprise customers and payment system vendors to reduce the risks associated with data loss and meet compliance regulations. Tokenization is a recognized data privacy strategy that replaces sensitive data with a token. The generated token maintains the original data characteristics but holds no value, reducing the risks associated with sensitive data loss.

About Townsend Security

Townsend Security provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, Linux, and UNIX. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.

Townsend® SECURITY

Enterprise wide solution, the tokenization server generates millions of tokens and stores terabytes of data effortlessly across the Enterprise

Greatly reduces the risk associated to data loss caused by data moving inside and outside the firewall

Meets regulatory requirements by supporting large number of data types including Credit Card (PAN), SSN, Drivers License, random numbers, random characters, and masked data

Easily manage PCI requirements with a solution that meets VISA encryption best practices

Reduce audit costs, take servers out of scope of compliance

www.townsendsecurity.com

Tokenization Compliments Encryption to Meet Business Needs

Tokenization improves on encryption technology by keeping sensitive information out of the data stream. Encryption securely protects data records stored on a database that may need to be recalled. The use of encryption and decryption ensures data that is flowing within and outside the network stays secure.

Tokenization protects data within the network and is an asset for internal IT department that runs routine systems tests and QA projects. When data is moved from the production environment to a test environment it poses a potential risk of data loss. When the data is tokenized, the tokens simulate the transferred information, ensuring the test system can support the data scheme while providing an extra level of security for employees involved in the project.

The use of tokens ensures sensitive data remains encrypted and secure on its designated database.

Tokenization for the Enterprise

Tokenize data from any application on any platform, and use the token across all Enterprise platforms such as Windows, Linux, Unix, IBM i, and IBM z mainframe. Any application or operating system that supports industry standard SSL/TLS communications can access the tokenization server. The use of authenticated SSL/TLS communications ensures all communications with the tokenization server remain secure.

Reduce Risks Associated to Data Loss

Replace sensitive data (credit cards, social security numbers, etc.), stored on the database with a token value. If the files containing tokens are lost or stolen, the sensitive data is not compromised in any way.

Tokenization can help minimize the impact of regulations such as HIPAA, PCI, HITECH , GLBA and individual state privacy laws.

Take Servers Out of Scope of Compliance

Generate non-recoverable tokens, (when the original data does not need to be recovered) using a separate token server and eliminate the need to store the original data in an encrypted format, taking the server out of scope for regulatory compliance.

Meets VISA Best Practices

Alliance Token Manager meets the technical recommendations set forth by Visa for tokenization implementations.

Tokens to Support Multiple Data Types

Protect a wide variety of information including credit card numbers, driver's licenses, phone numbers, zip codes as well as other types of financial data and any other proprietary or personally identifiable information (PII). You can specify that a token credit card number pass or not pass LUHN check-digit authentication.

Masked Tokens

Alliance Token Manager supports the masking of tokens using the following options - Mask using the last 4 digits, the first 5 digits, the first 6 digits or mask using the first 2 and last 4 digits. This flexibility allows organizations to meet regulatory requirements that allow organizations to retain some parts of the original personally identifiable information.

High Availability Mirroring

Supports real-time, high availability mirroring for data redundancy, network recovery, and load balancing. You can mirror the tokenization database to a remote data center or third party business recovery site using a variety of commercially available mirroring products.

Hardware/Software Requirements

- IBM Power Systems server, any model
- IBM i operating system, V5R2 or later
- IBM Digital Certificate Manager (no charge) licensed program
- IBM 4764 SSL acceleration hardware feature (optional)

Support

Software maintenance
Technical support
24/7/365 support available
Onsite installation
Contract services available

Townsend Security

Townsend Security provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, Linux, and UNIX. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.