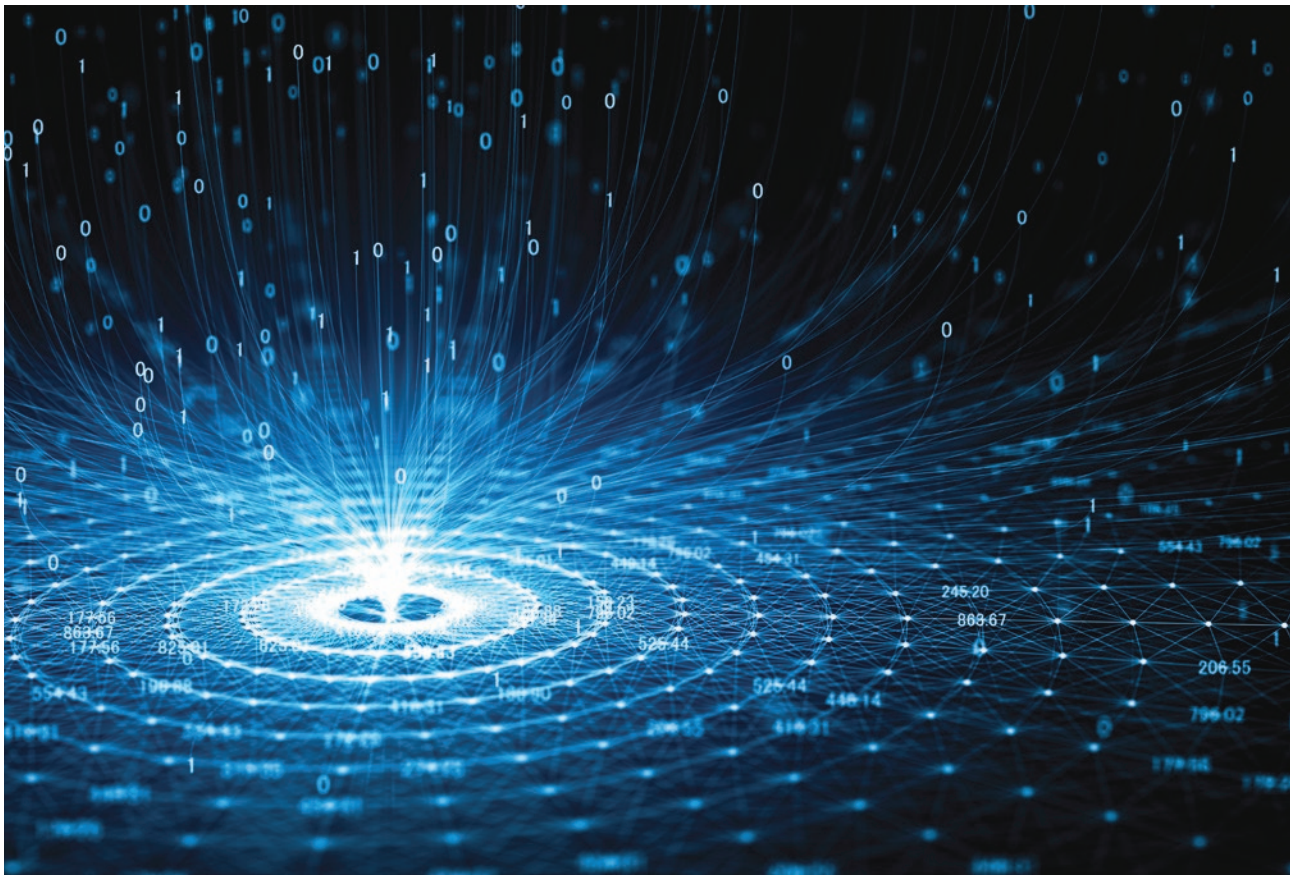
Product Brochure

PCI DSS and TokenBRIDGE™ Solution



Unique tokenization with highest data security standard and high availability

GEOBRIDGE by utimaco®

Introduction

As more and more financial data is both transferred and stored electronically, the communication networks over which it travels and the databases which store it become an irresistible target for criminals. The spate of announcements detailing the retail and banking community victims of the latest attack are almost routine. In response, the payment industry has struggled to protect the data it has to manage, with varied success. PCI-DSS is an industry standard which attempts to articulate best practices for how merchants, processors and financial institutions should protect their cardholder data.

Tokenization *(replacing a sensitive data element with one that has no financial value)* can reduce the complexity of the data protection solution, because the cryptography and key management required to implement a tokenization solution is hidden behind the Token Vault.

When people consider how to protect the data with which their organizations are entrusted, many think of encryption. But encryption just transfers the potential risk from the data itself to the keys encrypting the data, and the complexities of effective key management tax the skills and expertise of many entities struggling to implement cryptographically correct and cost-effective data protection.

TokenBRIDGE licensed on the KeyBRIDGE appliance, implements a secure, easy-to-manage Token Vault, the core of any tokenization solution. This white paper provides both a high-level description of tokenization, and why the TokenBRIDGE appliance is an ideal solution to the Token Vault requirement and how it assists in achieving PCI DSS compliance.

PCI Security Standards

In 2006 American Express, Discover, JCB International, MasterCard and Visa Inc. formed the Payment Card Industry Security Standards Council (PCI SSC). The SSC publishes Payment Card Industry (PCI) standards to help payment systems actors protect cardholder data worldwide. These actors include merchants, banks, payment processors, service providers, and technology providers.

What is the PCI DSS?

The PCI DSS (Payment Card Industry Data Security Standard) is a set of holistic requirements and corresponding testing and evaluation tools. It is designed to promote secure, standardized and interoperable implementations for all entities that handle financial cardholder data globally.

There are 12 high-level requirements[1]:

General Requirement	Specific Requirements
User Profiles Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

Tokenization is frequently sought after for the purposes of satisfying requirement 3:

protect stored cardholder data. However, a thorough and effective tokenization solution will also augment the satisfaction of additional control objectives. After all, the totality these 12 primary requirements are assembled with interdependency for the purposes of protecting the PAN.

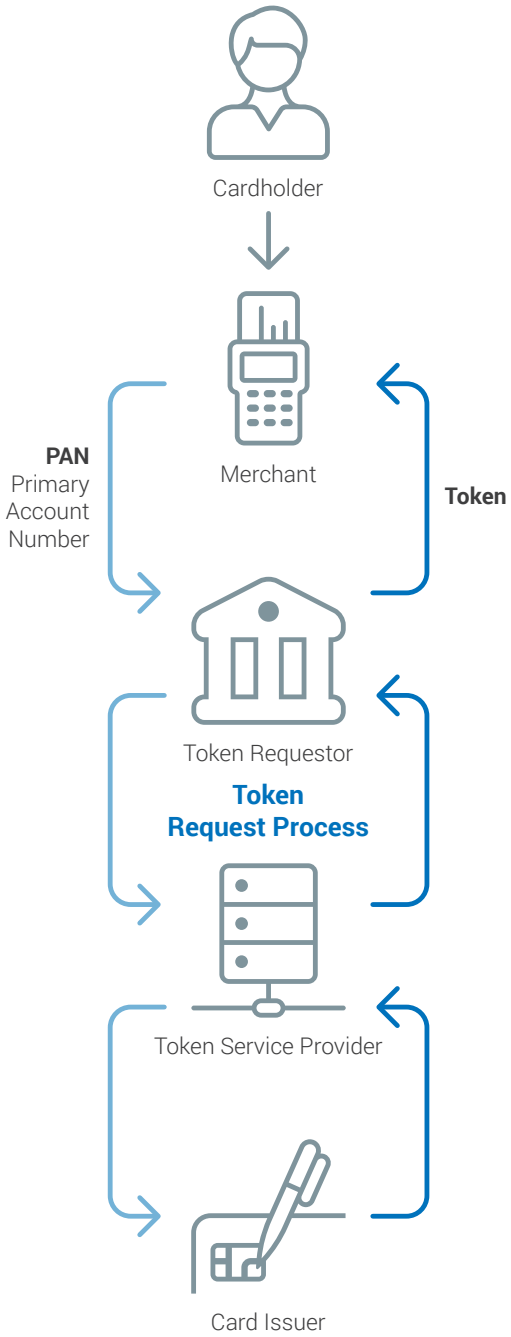
1 Source: Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures, Version 3.2, April 2016

EMV Payment Tokens

In addition to the general DSS requirements, EMVCo defined an interoperable "Payment Token"[2]. An EMV payment token is a Primary Account Number (PAN) replacement value. Payment Tokens (PT) are issued by Token Service Providers (TSP). The following diagram[3] shows how the token is issued and used:

The PT is a reversible token, meaning that the merchant calls the TSP with the PAN and receives the PT, which it then uses in lieu of the PAN for the transaction. When the Card Issuer receives an authorization request with the PT, it then supplies the PT to the TSP, which "detokenizes" it, returns the PAN to the Issuer and deletes the PT from its database. Assuming proper authorization mechanisms at the TSP, an attacker cannot subsequently use the PT to initiate a fraudulent transaction.

PCI issued a set of requirements specific to TSPs[4]. These requirements are intended to apply in addition to applicable PCI DSS requirements to the token data environment (TDE). As a Token Vault, TokenBRIDGE meets these additional PCI requirements.



TokenBRIDGE Features

TokenBRIDGE is a standalone appliance providing a rich set of tokenization services. Tokens may be generated in a wide variety of pre-defined formats, or a client can specify custom token formats. TokenBRIDGE implements a truly unique token vault, leveraging hardware-based encryption with FIPS 140-2 Level 3 security under AES 256-bit encryption allowing a client to submit a sensitive value and optionally receiving a token with either the same length and format, or an alternative length and format, which can be transparently substituted for the original value. Then, on request a TokenBRIDGE user can recover the original sensitive value.

TokenBRIDGE also offers a High Availability (HA) option, which permits multiple appliances to be integrated into a self-replicating network. Appliances may be separated geographically, allowing tokens issued by one appliance to be recovered on another.

TokenBRIDGE leverages the GEOBRIDGE KeyBRIDGE™ platform, and inherits from it a physically secure package, an easy to use graphical interface and rich automated audit features. Built as a TRSM, leveraging an internal FIPS 140-2 Level 3 HSM, TokenBRIDGE utilizes true hardware-based random number generation and stringent dual control features to establish a secure and compliant tokenization solution.

2 EMV® Payment Tokenisation Specification-Technical Framework, Version 2.0, September 2017
3 EMV® Payment Tokenisation Specification-Technical Framework, Figure 3.1
4 Payment Card Industry (PCI) Token Service Providers: Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens), Version 1.0, December 2015

Key Features

- Highly Scalable.
- Flexible and customizable token formats.
- Simple JSON Schema RESTful API driven functionality. No clients to deploy or manage.
- Provides random tokens, based on a true hardware-based, FIPS-certified Random Number Generator.
- Hierarchical user administration. Dual-control required for all sensitive operations.
- Remote communications protected by TLSv1.2 with only high strength cipher suites, utilizing mutual-authentication with client profile connections authenticated by their certificates.
- Extensive audit logging tracks all functional activities and access.
- Configurable network settings enable access to shared network storage for secure file storage and access.
- Configurable automated daily backup function.

Compliance at the Highest Level

- **NIST SP 800-90A Rev. 1:** Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- **ANSI X9.119-2017:** Requirements for Protection of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenization Systems
- **ANS/X9.TR.39-2009:** TG-3 Retail Financial Services Compliance Guideline Part 1: PIN Security and Key Management
- **ANS X9.97-2009:** Financial Services – Secure Cryptographic Devices (Retail) Part 1: Concepts, Requirements and Evaluation Methods
- **NIST SP 800-67:** Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
- **ISO 13491-1:** Banking – Secure Cryptographic Devices (Retail), Part 1 Concepts, Requirements and Evaluation methods.
- **Payment Card Industry PIN 2.0 Security Requirements**
- **FIPS 140-2:** Security Requirements for Cryptographic Modules, Security Level 3
- **FIPS 197:** Advanced Encryption Standard (AES), November 26, 2001

Product Benefits

- Enables secure storage of and access to tokens and their corresponding sensitive data within a single, centralized location.
- The HA option allows multiple appliances to automatically synchronize token databases, creating a reliable, geographically distributed network.
- Organize tokens by creating a logical relationship structure for more compliant handling.
- Offers built-in dual control functions and backup and recovery tools that in the event of a disaster, allow an entire system to be restored in minutes.
- Automates activity tracking within the system, capturing token activity details and user activity, as well as comprehensive audit logging of all sensitive functions.
- Physically secure enclosure – opening or penetrating the enclosure automatically erases the System Master Key (SMK), preventing access to the entire token database.

How TokenBRIDGE Helps to Meet PCI-DSS Requirements

Requirement 3: 'Protect Cardholder Data' and the Capabilities of TokenBRIDGE

The purpose and intent of Requirement 3 is to set standards for protecting cardholder data in storage. Clearly, the best solution is not to store cardholder data unless absolutely necessary, and for the shortest possible time. But if an attacker manages to breach all other safeguards and does get access to stored data, that data should be in a form useless to him. By replacing the data with a token, the attacker cannot use the token to create fraudulent transactions.

TokenBRIDGE Stands Apart

While most other tokenization solutions rely upon software-based encryption and software-based random number generation, these solutions remain susceptible to the same types of attacks that a nefarious actor would employ to breach other safeguards. By using a FIPS certified Random Number Generator and a FIPS certified hardware solution, an attack is far more likely to be thwarted.

The table on the next page lists the relevant Requirement 3 subsections, and how TokenBRIDGE helps to satisfy the requirements.

Glossary

Abbreviation	Explanation
EMV	EuroPay/MasterCard/Visa
HA	High Availability
HSM	Host Security Module
PAN	Primary Account Number
PCI-DSS	Payment Card Industry – Data Security Standard

Abbreviation	Explanation
PCI SSC	Payment Card Industry Security Standards Council
PT	Payment Token
SMK	System Master Key
TDE	Token Data Environment
TSP	Token Service Provider

Requirement		TokenBRIDGE Solution
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.	TokenBRIDGE can create a PAN token that is either entirely random, or an EMV payment token that uses a different BIN. In either case, the stored token is useless to an attacker.
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs).	Once tokenized, the original PAN is only recoverable by authorized entities. Consequently, any database backups that include the token are likewise protected.
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	Because the token is a random number and not the encrypted PAN, no complex key management procedures are required, simplifying the implementation.
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	Substituting random tokens for cardholder data obviates the need for keys. Consequently, TokenBRIDGE installation and ongoing maintenance is significantly simplified.
6.4.3	Production data (live PANs) are not used for testing or development.	Utilizing a token, in lieu of a live PAN will assist in supporting this requirement, particularly that TokenBRIDGE can produce tokens that will satisfy Luhn and Reserved Luhn checks.
6.5.3	Insecure cryptographic storage.	TokenBRIDGE stores all data utilizing FIPS 140-2 Level 3 hardware while leveraging AES 256-bit encryption.
8.2.1	8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	TokenBRIDGE allows for user-definable formats to produce any type of token. TokenBRIDGE stores all data utilizing FIPS 140-2 Level 3 hardware while leveraging AES 256-bit encryption.
9.5	Physically secure all media.	TokenBRIDGE allows for the storage and subsequent encrypted back up of any data. TokenBRIDGE stores all data utilizing FIPS 140-2 Level 3 hardware while leveraging AES 256-bit encryption.
10.1	Implement audit trails to link all access to system components to each individual user. Including all 10.3 requirements • User ID • Type of Event • Date/Time • Success/Failure • Origination event • Identity of affected data, component or resource.	TokenBRIDGE is equipped with audit log functionality beyond repudiation, logging all token distribution and de-tokenization requests to an individual end-point.
12.3.3	A list of all such devices and personnel with access.	TokenBRIDGE utilizes unique connection profiles for each endpoint while enforcing TLS 1.2 mutual authentication requirements.

Technical Specifications

KeyBRIDGE 4100

Physical Dimensions

- **Height:** 1.75 inches (4.4 cm)
- **Width:** 17.2 inches (43.8 cm)
- **Depth:** 21.3 inches (54.2 cm)
- **Weight:** 25 pounds (11.3 kg)
- **Controls:** Power on/off switch, unit ID switch

Connectivity

- **Communications Ethernet:** TCP/IP, TLS 1.2 (only)
- **LAN Connection:** 10/100/1000BASE-T (RJ45) auto-sensing

Electrical

- **Rated input voltage:** 100 to 240 VAC
- **Rated input current:** 5 A at 100 VAC 3 A at 240 VAC
- **Rated input frequency:** 50 Hz to 60 Hz
- **Rated input power:** 300 W

Operating Environment

- **Temperature:** 10°C to 35°C (50°F to 95°F)
- **Relative humidity:** 5% to 80% Non-condensing

Certification/Compliance

- **Safety:** UL62368-1 + CB62368-1/60950-1, BIS
- **Emissions:** CE/FCC, RCM #1 Australia

In 1997, GEOBRIDGE emerged as one of the first information security solutions providers to support cryptography and payment applications for payment processors, financial institutions and retail organizations. Guided by the credo that information security solutions should support, rather than dictate, business requirements, GEOBRIDGE continues to find new mechanisms that leverage our customers' security measures to better meet their business needs. Today, GEOBRIDGE is a leading information security solutions and compliance provider that supports a diverse global client base in retail, financial services, manufacturing and key injection facilities.

GEOBRIDGE brings together a team of highly skilled and highly experienced Network Security Architects, Application Developers, Cryptographic Key Management Experts and Project Management professionals who are fully invested in satisfying the security and compliance requirements of our customers.

Contact

GEOBRIDGE Corporation

20110 Ashbrook Place,
Suite #125, Ashburn,
Virginia 20147

For more information about GEOBRIDGE products, please visit:

geobridge.net