Patented Data Security by CardConnect

CardConnect has been awarded two United States Patents for securing confidential information through tokenization.

There is a critical need to secure payment card information, personally-identifiable information (PII), and other types of confidential information that a business collects related to their customers, patients, and employees. To ensure that this need is met, all computer systems a business uses to process unencrypted confidential information, and possibly an entire corporate data center, must be compliant with a variety of regulations. The cost of compliance, as well as the cost of verifying compliance, can be substantial, both operationally and financially.

During the past 20 years, CardConnect has become quite familiar with these regulations when architecting enterprise-level payment solutions for dozens of corporations. CardConnect has worked to develop solutions that minimize the exposure and risk a business has when handling confidential information. The end result is a patented system that uses tokenization in regards to the introduction, storage and use of confidential information in corporate enterprise systems.

What is tokenization?

Before confidential information can enter a business system, application or computer, the information is captured and stored within a tokenizer. The tokenizer then returns a random string of data called a token. The token has no algorithmic relationship with the original piece of data (such as a credit card number), meaning the token is irreversible, and cannot be unlocked with a decryption algorithm. The only application that contains the token's corresponding confidential information is the tokenizer, which is securely hosted and protected by CardConnect.

Due to the irreversible nature of the token, tokens can be used in any application without the application, business system, or network having to comply with regulatory standards, such as the Payment Card Industry Data Security Standard (PCI DSS).

Official Definitions

Cardholder data:

PCI DSS standards define cardholder data as any clear or encrypted primary account number (PAN), and declare any system that "processes, stores or transmits" cardholder data, as well as any system on the same network segment, must comply with the DSS standards.

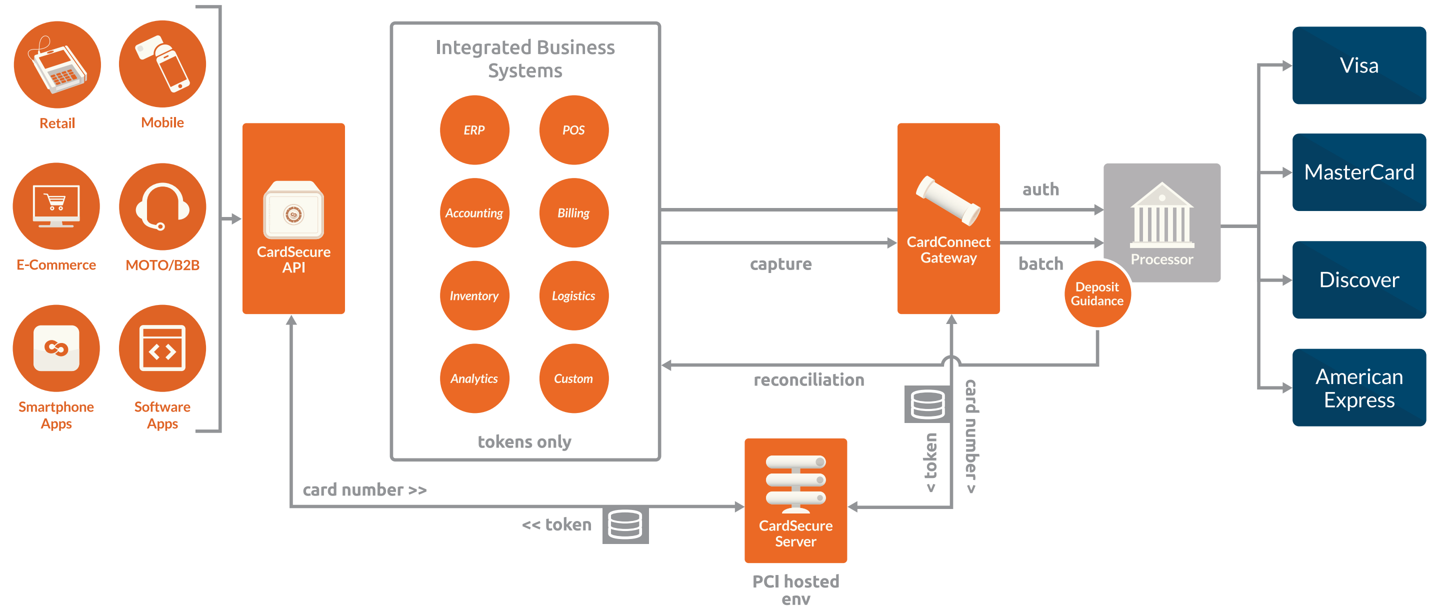
Personally-identifiable information (PII):

Government agencies describe PII as information which can be used to distinguish or trace an individual's identity (name, social security number, biometric records) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (date and place of birth, mother's maiden name).

cardconnect™

How CardConnect’s Patented Tokenization Stacks Up

		Industry Standard
Token Security	**Random Token (Irreversible)**	Derivative Token (could potentially be hacked)
Token Intelligence	**Luhn Test; BIN Recognition**	Unrelated to 16-digit card number
Merchant Specific Security	**Single use, intelligent token – unique to each merchant**	Multi-use token – Using the same token for multiple merchants is a security risk
“High-Value” Token	**Persistent Token – Merchant can reference a token without reissuing it for recurring payments**	Individually Administered Token – a new token is issued for every transaction
PCI Scope Reduction	**A combination of CardConnect's tokenization and integrated hardware (PANpad and P2PE terminals) help take a business out of PCI scope, greatly reducing requirements and cost of compliance.**	Even with a quality tokenization solution, workstations and POS systems remain in scope of PCI compliance and potentially susceptible to catastrophic data breaches.
Keyed-in Card-Not-Present transactions	**PANpad device encrypts and tokenizes card number immediately, removing customer service workstation from PCI scope**	Card number entered via standard keyboard, leaving the customer service workstation subject to PCI regulations
Card Present Transactions	**EMV-compatible P2PE devices resistant to malware**	Standard swipe terminal potentially susceptible to malware attacks
E-Commerce	**AJAX Tokenizer, iFrame, and Hosted Payment Page options**	Basic encryption solutions that leave website or e-commerce application in PCI scope
Integration Capabilities	**Developer friendly API that brings secure payment acceptance to most software applications**	Integration requires costly customization
History of Protecting Payments	**Launched in 2006 and used today by multiple Fortune 500 corporations without one security issue or leak of confidential information.**	


Retail
Mobile
E-Commerce
MOTO/B2B
Smartphone Apps
Software Apps
CardSecure API
Integrated Business Systems
ERP
POS
Accounting
Billing
Inventory
Logistics
Analytics
Custom
tokens only
capture
reconciliation
CardConnect Gateway
auth
batch
Processor
Deposit Guidance
Visa
MasterCard
Discover
American Express
< token
card number >
card number >>
<< token
CardSecure Server
PCI hosted env