STRONGKEY

HIGHLIGHTS

Easily tackle compliance controls

- StrongKey's hardware and application allows you to comply with the most difficult PCI DSS controls:
  - 3.4 – Render PAN unreadable
  - 3.5 – Protect cryptographic keys
  - 3.6 – Implement key-management
  - 4.1 – Use strong cryptography
  - 4.2 – Never send unencrypted PANs

Make audits simple

- We provide detailed documentation on how our solutions meet those requirements.

Stop worrying about keeping up with compliance standards

- Our solutions not only meet but exceed standard PCI DSS requirements today, keeping you ahead of the curve.

PCI DSS Compliance Made Easy

EXCEED COMPLIANCE REGULATIONS WITH STRONGKEY

While the Payment Card Industry Data Security Standard (PCI DSS) has over 150 controls to secure cardholder data, we focus on the 15 most difficult controls to make compliance easy, especially when needing to store that data, like Personal Account Numbers (PANs). We provide all the needed documentation answering those requirements in our Reference Manual, so you have everything you need to submit an audit document to your Qualified Security Assessor.

In the past, some of our customers have breezed through this part of the audit in as little as 15 minutes!

BENEFITS

No modifications needed – through the use of tokenization, StrongKey provides a way to provide applications with encrypted data that fits their fields.

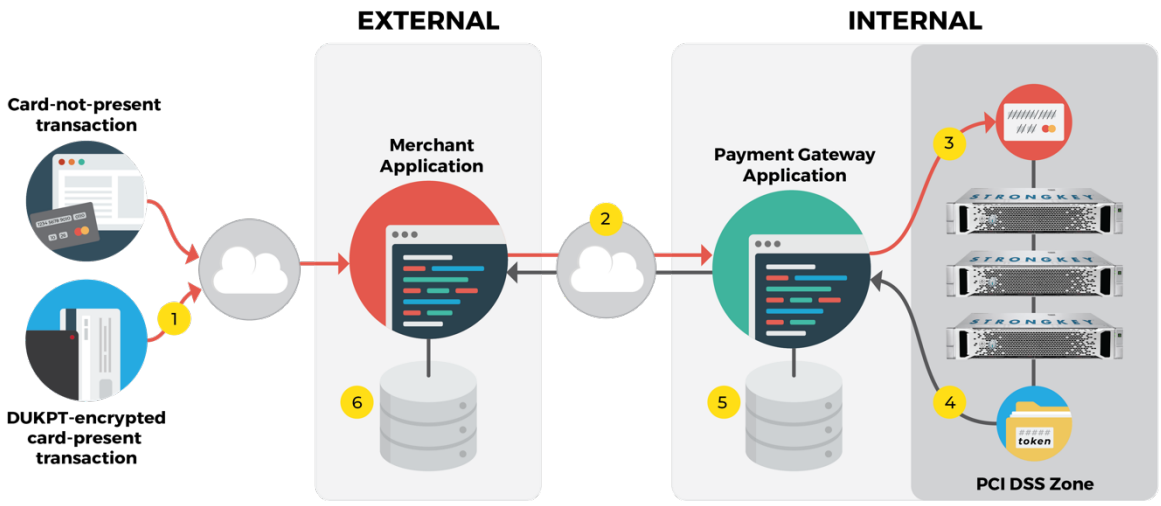
- Payment Gateway's database and applications do not need to be modified for the Token (16 digits, but can be configured up to 64 digits)
- Merchant's database and applications do not need to be modified for the Token (the Token is whatever the Payment Gateway returns to the Merchant and can be customized per Merchant, if desired)

Lower costs – integrates with industry-standard readers, thus eliminating additional cost for patented, proprietary algorithms.

HOW

StrongKey provides a fully integrated suite of solutions to enable PCI DSS compliance:

- **Hardware-based Cryptoprocessor -** industry-leading HSM or TPM configurations with FIPS 140-2 certifications to provide secure environments for master cryptographic keys.
- **Enterprise Key Management Service -** the essential component for creating and managing cryptographic keys
- **Encryption APIs -** simple web services (REST or SOAP) for applications to call for encryption and tokenization
- **Integrated Industry Standards -** StrongKey's Credit Card Crypto Service provides:
  - Base Derivation Key (BDK), Symmetric/Asymmetric Key Management
  - ANSI X9.24-1:2009 Derived Unique Key per Transaction (DUKPT)
    - End-to-End Encryption for "Card Present" Transactions
    - Protect data and Personal Identification Numbers (PIN)
  - Escrow RSA public keys for devices
    - Assumes key-pair was injected in device during manufacturing
  - Generate symmetric keys for devices
    - Enables secure device-key distribution/rotation remotely



1. Magnetic Stripe Reader reads credit card data and encrypts with standard DUKPT algorithm
2. Encrypted DUKPT blob transferred with end-to-end encryption to Merchant Application to Payment Gateway to Payment Gateway Application
3. Payment Gateway Application passes encrypted DUKPT blob to StrongKey's '/tokenize/' REST API endpoint
4. StrongKey decrypts DUKPT blob, re-encrypts & tokenizes PAN, and returns JSON with 16-digit token to Payment Gateway Application; return value looks like:
{"DID":"1","SRID":"14690528407 11","Token":"1000000001121985","ExpiryDate":"0804","ExpiryMonth":"04","ExpiryYear":"08","MaskedPAN":"5452000000007189","Digest":null,"Valid":false,"Exists":true,"AssociationID":"5","IssuerID":"545230","CardholderName":"PAUL HOGAN","Firstname":"PAUL","Lastname":"HOGAN","Notes":null}
5. Payment Gateway Application stores tokenized transaction in database; no modifications are necessary since tokenized data matches existing formatting
6. Payment Gateway Application returns Tokenized transaction to Merchant Application, which stores it in its database; no modifications are necessary for Merchant Application database

CUSTOMER EXPERIENCE:

With over 30 clients on 6 continents, our experience with PCI DSS compliance is tried and true. Our clients' industries include:

- Banking
- Business administration
- E-commerce
- Healthcare
- Payment processing
- Property management
- Retail
- Software
- Technology consulting

ABOUT STRONGKEY

StrongKey makes data breaches irrelevant by redefining how businesses and government agencies secure their information against the inevitability of a breach. While other security companies focus on protecting the perimeter, StrongKey secures the core through strong authentication, encryption, digital signatures and hardware-backed key management—keeping the core safe even with an attacker on the network. Based in Silicon Valley, CA and Durham, NC, StrongKey has provided cryptographic security solutions for over 17 years and is trusted in mission-critical business operations by some of the largest companies in payment processing, e-commerce, healthcare, and finance. Learn more at www.strongkey.com.

StrongKey
Durham, NC & Cupertino, CA
Phone: +1 408-331-2000 | E-mail: getsecure@strongkey.com | Web: strongkey.com