

Taming the PCI Compliance Juggernaut – Tokenization

Background

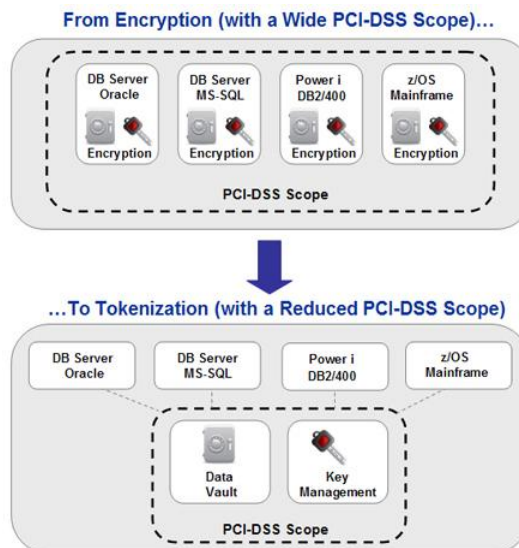
One of the biggest headaches facing merchants today is compliance with the Payment Card Industry Data Security Standard (PCI-DSS). Compliance can add significant cost to the IT budget while slowing down core business development and operations. This complexity is ever increasing with the addition of mobile store fronts such as iPhone and Blackberry. It begs the question, how do merchants tame the compliance juggernaut? As with most things in life, that depends. Fortunately, in the case of PCI, less is more.

Although PCI-DSS has over 250 requirements, each requirement is based on the premise of protecting cardholder data such as the primary account number (PAN). When you remove the card data from your system components – Presto! Your system component is no longer within PCI scope. As far as PCI is concerned, if no PANs, CVVs, or block data are stored on your system component, there is nothing to protect and therefore no PCI compliance issues.

The idea sounds simple enough, but what if you need the credit card data on your system for business reasons such as charge backs? Are you out of luck? Not really. What you can do is substitute a token for the sensitive data. What this means is that in your payment system, a piece of sensitive data such as a PAN can be substituted by a **token** like a transaction ID so that after authorization, only the token is stored. Criminals cannot tie the token back to the corresponding credit card number, and merchant card data storage is reduced.

How Tokenization Works

When properly deployed, tokenization allows merchants to limit storage of cardholder data to within the tokenization system. In the diagram below, tokenization is used to remove card data from 4 servers to just 1 token server and the key management program.



In other words, the PCI requirements for the 4 servers are eliminated.

Taming the PCI Compliance Juggernaut – Tokenization

How Tokenization Works (continued)

Tokenization consists of four parts:

1. **Token Generation** - Process of creating the token
2. **Token Mapping** – Method of associating token to its original value
3. **Card Data Vault** – Central data repository of cardholder information used by token mapping method
4. **Cryptographic Key Management** – Method through which data encryption/decryption keys are managed and how they are implemented to protect cardholder and account data.

"Merchants and processors that use tokens in accordance with best practices are able to limit PAN storage, significantly reducing the risk that sensitive cardholder data may be stolen by data thieves." - **VISA**

Tokenization example in a Retail Environment (Courtesy of AJB Software)

In the following diagram using the CSM tokenization product, card data has been removed from the POS client and the back office RTS server. Card data resides only in the Card Data Vault (CSM database).

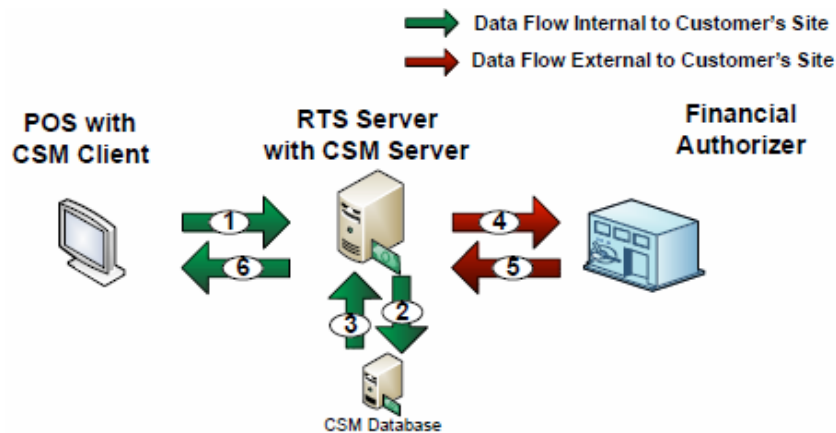


Figure 3.1 Typical Retail Settlement Processing Environment with RTS and CSM

1. POS initiates the settlement by sending store token to CSM server via CSM client.
2. CSM server requests PAN from the CSM database by sending the store token.
3. CSM server receives the PAN and forwards it to RTS server.
4. RTS sends out the settlement request to the financial authorizer.
5. The settlement reply is received by the RTS server from the Financial Authorizer.
6. POS receives settlement confirmation.

Conclusion

No matter how you look at it, there is no “substitution” (no pun intended) for using tokenization. It will help you reduce the scope of PCI compliance to save time and money in your PCI remediation efforts.