nCipher AN ENTRUST DATACARD COMPANY

www.ncipher.com

Enhanced tokenization and compliance with nShield HSMs

- Protect sensitive data at rest, in use and in motion
- Reduce the scope and cost of compliance audits
- Avoid disruption to applications using format preserving tokenization
- Safeguard encryption keys in a tamper-resistant FIPS 140-2 Level 3-certified security module
- Generate random numbers with a certified, compliant source of entropy

NFINITY STRATEGIC TECHNOLOGY PARTNER PROGRAM

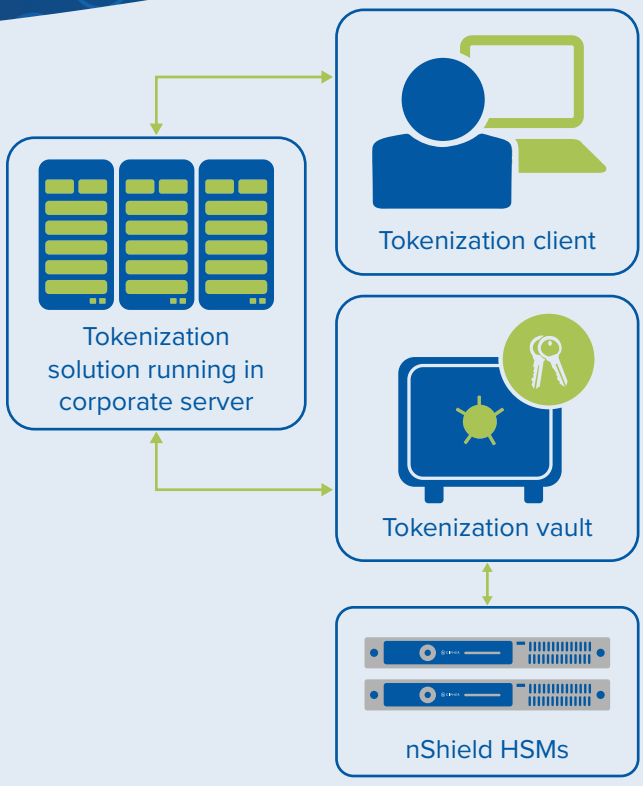
nCipher and tokenization providers enhance enterprise data security and compliance

THE CHALLENGE:

Across industries, enterprises are accumulating and transmitting more sensitive information than ever before, increasing the potential for attack by cybercriminals seeking to monetize private data. The availability of secondary markets for this data makes personally identifiable information, payment card numbers and medical records particularly vulnerable.

In response, organizations have turned to tokenization to reduce the risk of data exposure. Tokenization substitutes a real value with a random token that maintains the same format and type as the original data. This allows existing applications and databases to recognize and process the token in the same way as the original information. For example, as a customer service representative adds to a customer's record, specific fields can be immediately tokenized so they are safeguarded against unauthorized access. Depending on the architecture, the real values are encrypted and stored in a separate vault or, using a vaultless approach, the token is generated via an algorithm, thus obviating the need to store the actual information.

Because the data is devalued, tokenization improves its security while reducing the risk of theft. This can also enhance compliance with mandates such as the PCI Data Security Standard, which notes that organizations can effectively reduce their PCI DSS scope through the use of a compliant tokenization system.



nShield hosts the master root key for the tokenization function and may also perform critical functions within its secure boundary using CodeSafe secure code execution.

nCipher and tokenization providers enhance enterprise data security and compliance

When implementing a tokenization system, an enterprise must ensure that it is designed to prevent the reversal of tokens to reveal the original data. This is essential to ensure that sensitive data remains secure and the organization maintains compliance with data privacy mandates.

THE SOLUTION: TOKENIZATION INTEGRATED WITH NSHIELD HSMs

A strong tokenization solution starts with the token generation process. Recognized best practices for token generation call for either random tokenization or tokenization by encryption, coupled with secure storage of the encryption keys. The PCI Tokenization Guidelines specify that, "Cryptographic keys must be managed and protected in accordance with PCI DSS requirements...Cryptographic keys used for token generation and de-tokenization should therefore not be available to any application, system, user, or process outside of the secure tokenization system."[1]

nCipher nShield HSMs are integrated with leading tokenization solutions. They establish reference tables of highly random, highly secure cryptographic keys, which are used in the token generation process. The nShield's random number generator has been certified as a FIPS-compliant source of entropy. This allows organizations to create highly secure tokens that cannot be reversed by unauthorized users. The nShield HSM also generates and protects the keys used to encrypt reference tables.

When the tokenization architecture incorporates a separate vault of original data, the encryption keys that help protect the vault data are generated by and secured in an nShield HSM.

THE NSHIELD DIFFERENCE

nShield HSMs protect encryption keys in a certified, tamper-resistant environment. Keys handled outside the cryptographic boundary of nShield HSMs are significantly more vulnerable to attacks, which can lead to disclosure of confidential information. HSMs are the only proven and auditable way to secure valuable cryptographic material. nShield HSMs:

- Protect keys and certificates within carefully designed cryptographic boundaries
- Use robust access control mechanisms so keys are only used for their authorized purpose
- Ensure availability by using sophisticated key management, storage, and redundancy features to guarantee keys are always accessible when needed
- Deliver high performance to support high volumes of tokenization
- Comply with regulatory requirements and industry mandates governing financial services, retail and other industries

MICRO FOCUS Voltage

PrimeFactors™ — Applied Data Protection —

1. https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

Search: nCipherSecurity

www.ncipher.com

nCIPHER AN ENTRUST DATACARD COMPANY