nCipher

www.ncipher.com

Secure cardholder data end-to-end with Verifone Verishield total protect and nCipher hardware security modules

Verifone

- Secure cardholder data from swipe or tap to processing
- Provide full lifecycle management of cryptographic keys
- Ensure superior system performance and high availability
- Simplify security auditing and reduce compliance costs
- Provide a FIPS 140-2 Level 3 certified foundation of trust

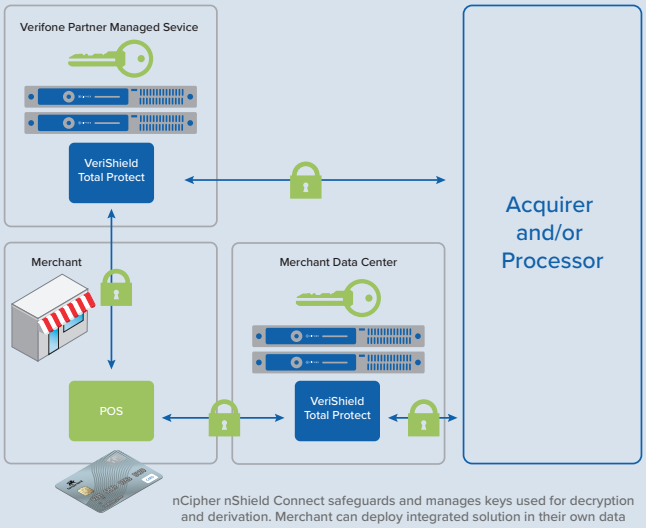
Verifone and nCipher deliver total point of sale protection from card acceptance to processing

THE PROBLEM: RETAILERS NEEDED A BETTER WAY TO SECURE CREDIT CARD TRANSACTIONS AND REDUCE THE RISK OF COMPROMISE OF THEIR CUSTOMER DATA.

- Data breaches continue to make headlines and are costing retailers millions of dollars per year in damaged reputation and depressed sales, not to mention remediation costs and liabilities. While critical cardholder data is typically protected by payment applications using cryptography, the techniques used are not uniformly applied across the transaction chain. This leaves gaps in the process where unprotected data is vulnerable to attack.

THE CHALLENGE: MAXIMIZE SECURITY FOR CREDIT/DEBIT CARD TRANSACTIONS WITHOUT SLOWING PERFORMANCE.

- End to end encryption is required to ensure that critical cardholder data is not exposed and compromised. But encryption can often introduce latencies and slow down processes. Solutions that provide increased protection for cardholder data need to do so while maintaining the highest levels of operational performance, addressing up to millions of transactions per day between retailers and processors. Safeguarding and managing cryptographic keys that underpin the security of the encryption process is vital to provide a foundation of trust for the system.



nCipher nShield Connect safeguards and manages keys used for decryption and derivation. Merchant can deploy integrated solution in their own data center or can choose to use as a Verifone partner managed service.

Verifone and nCipher deliver total point of sale protection from card acceptance to processing

THE SOLUTION: VERIFONE AND NCIPHER TOGETHER DELIVER A UNIQUE COMBINATION OF STRONG SECURITY AND RISK MITIGATION AGAINST MALICIOUS CAPTURE OF CARDHOLDER DATA.

Verifone's VeriShield Total Protect provides merchants with a flexible solution that safeguards plaintext cardholder data by encrypting it from the precise moment of entry and acceptance at the point of sale (POS) device on through to the back end gateway, payment processor, or acquirer. VeriShield Total Protect reduces the risk of merchant data breaches while supporting processing requirements and minimizing the operational impact to existing systems and environments. End-to-end encryption with cryptographic key management powered by nCipher nShield hardware security modules (HSMs) are a critical component of the VeriShield Total Protect solution. HSMs protect and manage large numbers of critical cryptographic keys and ensure they are always available to support the secure transactions.

nCipher nShield Connect and its unique Security World key management architecture enable the VeriShield Total Protect solution to build redundancy to service very high transaction volumes with automated load balancing and failover. Depending on the end customer's need, nShield Connect HSMs can be owned by customers and maintained at their premises, or they can be used as part of a managed service hosted by a Verifone partner. Either way, the end-to-end encryption process is rooted in a protected HSM platform that is certified to FIPS 140-2 Level 3.

WHY USE A NCIPHER NSHIELD CONNECT HSM WITH VERIFONE VERISHIELD TOTAL PROTECT SOLUTION?

Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to disclosure of confidential primary account numbers (PANs). HSMs are the only proven and auditable way to secure valuable cryptographic material such as encryption keys. nCipher nShield Connect HSMs integrate with Verifone's VeriShield Total Protect solution to provide comprehensive logical and physical protection. The combination delivers an auditable method for enforcing security policies that underpin critical components of the data protection infrastructure that goes beyond PCI DSS requirements. End-to-end encryption ensures that intermediate systems that sit between the POS devices have a significant reduction in applicable controls with respect to most PCI DSS compliance requirements.

By providing a mechanism to enforce security policies and a secure tamper resistant environment for back end decryption and key management, customers can demonstrate compliance and minimize the scope of security audits.

NCIPHER NSHIELD CONNECT HSMS ENABLE VERIFONE CUSTOMERS TO:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed to process transactions
- Deliver superior performance to support the highest transaction rates

NCIPHER

nCipher nShield Connect HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With nCipher HSMs you can:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, and CNG)

VERIFONE

VeriShield Total Protect provides a trusted and secure payment solution that protects cardholder data from the point of sale to the processor with complete confidence that unencrypted data will never be exposed. The purpose built solution:

- Uses encryption and tokenization to secure critical PANs and discretionary data
- Minimizes retailer risk and reduces the scope of PCI DSS
- Services transactions across multiple sites for high availability

For more detailed technical specifications, please visit www.ncipher.com or www.verifone.com