Entrust nShield HSMs secure Verifone's VeriShield Total Protect solution

How a leader in secure electronic POS solutions ensures protection of cardholder data from acceptance to processing in a demanding environment.

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

As a leader in trusted and secure payment solutions, Verifone understood that retailers needed a better way to secure credit card transactions and reduce the risk of compromise of their customers' data. Major, well-publicized data breaches have continued to cost retailers millions of dollars each year in damage to reputation and depressed sales. But any solution that provides increased protection for cardholder data needs to do so while maintaining the highest levels of performance – up to millions of transactions per day – for users like processors and retailers.

THE SOLUTION: END-TO-END ENCRYPTION POWERED BY ENTRUST NSHIELD HSMs

Verifone looked to Entrust nShield® hardware security modules (HSMs) to provide high assurance encryption and key management functionality as a critical component of its VeriShield Total Protect solution. VeriShield encrypts cardholder data from the precise moment of acceptance on through to the point of processing, where transactions are decrypted and sent to the payment networks. Entrust nShield HSMs are used to perform secure key exchanges and secure key derivations that produce a unique key to protect each and every payment transaction.

Taking advantage of capabilities unique to the Entrust nShield Security World architecture, Verifone built redundancy so that multiple servers and multiple HSMs, deployed at multiple data centers, can combine seamlessly to service very high transaction volumes with automated load balancing and failover. Additionally, Entrust provides Verifone the ability to offer their customers the option to host their HSMs either on site (the typical choice) or as part of a managed service hosted by Verifone.

LEARN MORE AT ENTRUST.COM/HSM

With this solution, Verifone provides a unique combination of strong security and risk mitigation against malicious capture of cardholder data, while at the same time ensuring performance and availability for transactions – a win-win for retailers. Additionally, by deploying end-to-end encryption (sometimes referred to as point-to-point encryption or P2PE), intermediate systems that sit between the POS (point of acceptance) and the point of decryption at the processor are removed from the scope of most PCI DSS compliance requirements, since the data passing through them is encrypted. The Verifone solution is specifically designed to enable retailers to provide security that goes well beyond the requirements of PCI DSS.

ABOUT THE SOLUTION

Entrust nShield HSMs

Entrust nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With these devices you can deploy high assurance security solutions that satisfy widely established and emerging standards of due care for cryptographic systems and practices – while also maintaining high levels of operational efficiency.

Entrust nShield Connect HSMs isolate and secure cryptographic operations and associated keys for an organization's most critical applications. Entrust nShield Connect HSMs perform encryption, digital signing and key management on behalf of an extensive range of commercial and custom-built applications including public key infrastructures (PKIs), identity management systems, application-level encryption and tokenization, SSL/TLS and code signing. A high assurance alternative to software-based cryptography libraries, Entrust nShield Connect HSMs feature certified implementations of all leading algorithms, as well as the world's fastest ECC performance.

With Entrust nShield HSMs you can:

- Deliver certified protection for cryptographic keys and operations within tamper-resistant hardware to significantly enhance security for critical applications.

- Achieve cost-effective cryptographic acceleration and unmatched operational flexibility in traditional data center and cloud environments.

- Overcome the security vulnerabilities and performance challenges of software-only cryptography.

- Reduce the cost of regulatory compliance and day-to-day key management tasks including backup and remote management. With Entrust nShield HSMs, you buy only the capacity you need and can scale your solution easily as your requirements evolve.

Verifone

WHY ENTRUST?

Verifone evaluated six different HSM models offered by three different vendors before choosing the Entrust nShield Connect HSM. That choice was based on the following:

- **Interoperability and integration**. Entrust offered multiple interfaces (standard PKCS #11 as well as a lower-level interface) which allowed Verifone developers the flexibility to integrate the HSM to maximum advantage in the VeriShield architecture.

- **Ease of use**. Verifone found Entrust nShield HSMs to be easy to use, and significantly more flexible than other HSMs in architecting the system to maximize performance and to minimize key persistence.

- **Performance**. The throughput of Entrust nShield HSMs was significantly higher than competing products, and enabled Verifone to assure retailers that the VeriShield solution would not degrade performance.

- **Support**. Verifone valued the close working relationships with the Entrust team and the help that Entrust specialists were able to provide to developers as they worked to incorporate the nShield HSMs.

- **Entrust nShield Security World**. Entrust nShield Security World architecture enabled the Verifone team to set up a system that provides appropriate load balancing, high availability and reliability. With it, VeriShield-protected transactions are capable of being serviced synchronously across multiple sites and multiple HSMs.

Verifone

KEY BENEFITS

- Perform high assurance encryption of critical data and ensure full lifecycle key management without sacrificing performance or availability

- Service high transaction volumes with automated balancing and failover

- Provide security that goes well beyond PCI DSS requirements

- Reduce operational and compliance reporting costs with a powerful key management architecture

- Automate burdensome and risk-prone administrative tasks and eliminate single points of failure and expensive, manually-intensive backup processes

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com