Data Sheet

THALES
CYBERSECURITY

Top 10 Reasons to Use the Bank Card Security System (BCSS) with the Thales payShield 10K HSM

cpl.thalesgroup.com

THALES

CYBERSECURITY

Built on decades of real-world payment security expertise, the Bank Card Security System (BCSS) simplifies the design, deployment, and management of secure payment card applications that integrate with Thales payShield 10K HSMs. BCSS reduces complexity, cost, and time to market with PCI-proven security functionality, helping organizations stay audit-ready while adapting to new payment requirements.

The following Top 10 reasons highlight why BCSS provides a faster, more reliable way to modernize your payment security operations.

1. Accelerate time to revenue with out-of-the-box payment security functionality

BCSS is built to take care of complex payment security so your developers don't have to. The software helps organizations generate revenue faster by enabling the rapid launch of secure, compliant payment applications with out-of-the-box security features, cutting development timelines by up to 80%. Instead of requiring developers to be cryptography experts or understand traditional HSM host commands, BCSS provides all the essential elements needed for a compliant payment application to meet regulatory requirements.

2. Simplify load management and integration with payShield 10K HSMs

A high-level API with secure communications enables faster, easier integration across multiple payShield 10K HSMs. Hundreds of streamlined, pre-built workflows help developers quickly connect to HSMs in any common programming language without specialized expertise. BCSS also provides robust load balancing and redundancy to ensure all payment functions are handled appropriately and routed to the correct hardware.

3. Centralize and automate payment key lifecycle management

BCSS simplifies development with secure payment key lifecycle management to generate, rotate, assign, and retire keys. A secure key vault protects payment keys, EMV certificates, and additional parameters for credential issuing and processing. With BCSS, developers don't need to design or program key management, allowing them to focus more on core application functionality and needs.

4. Enforce separation of duties with built-in role-based access controls

Built-in, role-based access controls enable key control enforcement, key quorums, dual sign-on, and separations of duties. Traditionally, programmers must incorporate this functionality into their payment applications, manually configure access, and assign role permissions. BCSS manages all of these aspects in compliance with PCI standards, ensuring only authorized users can control payment keys and components as specified. These protections integrate seamlessly with built-in audit-logging features to support PCI-PIN and PCI-DSS compliance.

5. Minimize risk and ensure compliance with proven PCI-ready controls

Secure payment applications must consistently demonstrate compliance with PCI standards. While companies often need to include audit logs and reports in their systems, BCSS minimizes risk through tamper-proof, forensic-level audit logging and comprehensive reporting with Syslog integration. Each event is documented by date, time, user ID, and action taken. All audit logs are hashed and encrypted, and clear keys and PINs never appear in trace files.

6. Deploy however and wherever you need

Whether an organization uses two payShield 10K HSMs or dozens, BCSS supports flexible deployment across on-premises, cloud, and hybrid environments in most common operating systems and programming languages. Companies can easily scale their deployments up or down as needed.

7. Improve visibility across your payment security infrastructure

Transaction Analytics offers comprehensive real-time reporting of payment functions, keys, and parameters to maximize visibility across your payments infrastructure. BCSS provides visibility into critical information on HSM utilization and capacity, including how applications interact with HSMs, the types of calls received, HSM location(s), length of HSM utilization, and HSM failure codes.

8. Reduce complexity and programming

Managing multiple key types and payment processes is inherently complex, and selecting the wrong key, command, or hardware can disrupt payments. BCSS provides strong cryptographic lifecycle management for keys and certificates through a unique architectural approach called a Network Profile Record (NPR), which dramatically simplifies handling payment functions across HSMs. The NPR organizes the keys, certificates, parameters, and associated hardware needed to execute specific payment functions into a single security partition.

9. Easily adapt to evolving payment standards

BCSS stays updated with industry trends and hardware upgrades. When new standards emerge and market trends change, organizations can quickly adjust to shifting business needs, payment schemes, and compliance demands without complex redevelopment. Companies can modify their payment infrastructure as needed, including automatic Local Master Key rotation and seamless migration from variants to Key Blocks.

10. Migrate payments to the cloud at your own pace

Legacy systems are built on outdated languages and complex architectures that most modern-day developers aren't familiar with, forcing companies to adopt risky, complex "rip and replace" strategies for cloud migrations or to hire expensive, specialized developers. BCSS delivers the tools programmers need to manage cloud migration at their own pace, with built-in HSM subroutines for seamless integration with payShield Cloud HSMs and robust load balancing. Migrate payment infrastructure to the cloud at a pace that is right for your business, while reducing risk, minimizing costs, and ensuring resiliency.

Key Benefits

- **Faster time to market:** Launch secure, compliant card payment applications in months rather than years.
- **Lower development and operational costs:** Eliminate the need for custom cryptography, HSM command coding, and manual controls.
- **Reduced compliance risk:** Incorporate embedded PCI-proven controls, audit logging, and separation of duties.
- **Operational resilience:** Achieve load balancing, redundancy, and resiliency across payShield 10K HSMs.
- **Future-ready payments:** Adapt rapidly to new standards, key management models, and deployment models.
- **Cloud-ready by design:** Migrate payment workloads securely with less risk, lower cost, and more control.

A trusted foundation for secure, compliant payments

BCSS, powered by payShield 10K HSMs, provides a reliable, secure foundation for modern payment card applications. By including PCI-compliant controls, simplifying HSM integration, and automating key management and auditing, BCSS lowers risk, accelerates deployment, and helps organizations easily evolve their payment infrastructure now and in the future.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us