cpl.thalesgroup.com

PrimeFactors™ | THALES
Building a future we can all trust

Prime Factors Bank Card Security System (BCSS) powered by Thales payShield 10K

Get payment system development costs under control with Prime Factors and Thales

Payments security is complex. Understanding the payments ecosystem and abiding by industry standards and regulations for issuing payment credentials and processing transactions requires an immense amount of specialized knowledge. The payments industry has its own jargon, rules and its own types of cryptographic keys and functionality to ensure that the most critical and sensitive information is properly secured.

The complexity can be daunting, forcing some companies to opt for off-the-shelf applications. However, others who want to control their payment applications from top to bottom, make the strategic decision to develop their card issuance or card processing platforms in-house. Once this decision is made, there are additional, important 'make versus buy' decisions related to how all of the logical security requirements (defined by the various payment schemes and network brands) are to be implemented.

Specific functionality linked to payment key management, role-based access controls, separation of duties, audit logging and reporting can be developed from scratch in-house. Internal development teams can learn, implement and manage the broad range of host commands needed to incorporate hardware security modules (HSMs) into their payment card platform. However all of these elements, in addition to requiring specialized expertise, are complex, time-consuming and costly to implement and manage over time. This is where the Prime Factors Bank Card Security System (BCSS) can help.

Simplifying payments security

BCSS was built to simplify payments security. Role-based access controls define and enforce separation of duties. Robust payment key management functionality streamlines cryptographic key management and speeds up issuance and processing. Detailed audit logging and reporting functionality helps to comply with industry requirements and pass PCI audits. Importantly, pre-tested integrations with the Thales payShield 10K payment HSMs allow for easy integration, load-balancing and management.

The solution reduces complexity related to payments security, speeds up application development, and ensures industry and regulatory compliance related to cryptography, without the need for in-house expertise or costly efforts to keep a card issuance or transaction processing system constantly up to date with the latest key management standards, payment schemes, and security certifications.

Solution benefits

- Eliminates complex in-house security-related development activities
- Reduces integration effort and time to market
- Simplifies audit compliance, especially for the newest security standards
- Streamlines generating data for EMV card issuing
- Supports the latest payment applications and security functionality in a timely manner

Support for the latest security standards

BCSS works exclusively with Thales payShield HSM technology to meet the latest logical security requirements of the leading payment brands including American Express, Discover, JCB, Mastercard, UnionPay and Visa. Payment applications can communicate with BCSS in a variety of common programming languages to simplify the implementation and enforcement of robust security controls, without learning the complicated host-commands common to HSMs. With Prime Factors BCSS and Thales payShield HSM technology, payment card issuers, personalization bureaus, and payment processors can get to market faster and respond more quickly to change, whether it's new security requirements or new card applications supported by the HSM firmware. They can be confident that BCSS and Thales technology will help them pass annual card network brand audits with ease.

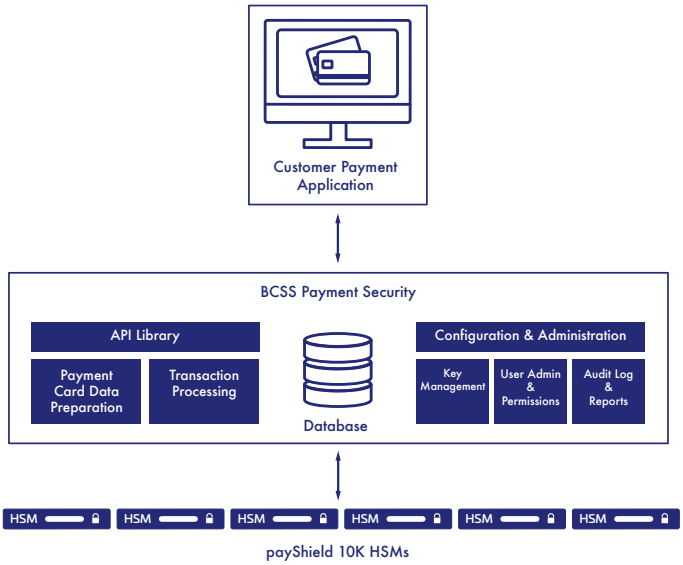
Proven solution for all payment key management and card data preparation needs

Prime Factors BCSS and Thales payShield HSM technology work together to provide complex payment key management and perform sensitive data generation and distribution for card issuance. BCSS utilizes the HSM to generate the cryptographic keys and data required for a wide range of credit and debit card applications. Data preparation and personalization for magnetic stripe cards, EMV chip cards and mobile applications are also supported. All keys and sensitive data are processed according to the latest industry standards, with the Thales payShield 10K HSMs ensuring that no plaintext keys are ever exposed outside the tamper-resistant boundary of its high-performance key generation security engine. The keys and security information generated by payShield 10K are held encrypted in the BCSS key vault database where they are available for secure distribution to other systems and locations, including the bank's own transaction processing and authorization systems. BCSS and the payShield 10K meet all the relevant payment brand security audit standards for card issuance and personalization.

Quicker integrations, better management, and more flexible deployments

BCSS is architected to make it easier to integrate new payShield HSMs and security functionality such as key blocks, without changing in-house payment applications. In addition to simplifying how payment applications can use the HSM, BCSS manages load-balancing of security calls across groups of HSMs and can direct specific workflows to a dedicated HSM or group of HSMs. It can also provide visibility into capacity thresholds that help end users know when additional HSM processing functionality is needed.

BCSS is architected to deploy easily on premises, in the cloud in virtual machines or containers, or in hybrid environments - integrating with the HSMs wherever they reside, making it easier and more flexible than ever to secure payments in any operating environment.



Why BCSS only uses Thales HSMs

- Payment HSMs from Thales are industry-leading and trusted globally
- Thales offers a range of packages optimized for issuing banks and bureaus
- Support for the latest payment brand applications is provided in a timely manner
- The HSMs offer the broadest range of global and regional certifications
- Thales HSM technology is proven in mission critical environments to provide:
  - High performance
  - Resilience
  - Reliability
  - Scalability
  - Remote management

Solution specifications

BCSS provides a high-level API that supports the following functionality:

- Create and verify card security codes (CVV, CVC, CSC, etc.)
- Create and verify user security codes (PINs and PVVs)
- ARQC and ARPC cryptograms compliant with the latest EMV standards
- Transaction switching and verification
- PIN translation and PIN change
- PIN generation and PIN mailer printing support
- RSA key caching
- Management of keys in Key Blocks as required by PCI
- EMV data preparation (Issuer and card certificates, card keys generation, static signatures) including mobile specific keys (single/one-time use)
- Secure Messaging for EMV card updates and PIN change

Underpinned by certified hardware security

payShield 10K integrates out of the box with BCSS – there is no need for any additional host client software. Flexible configuration adapts to individual issuing and processing environments and provides:

A choice of base software packages and optional licenses:
Save costs by just purchasing the functionality needed – secure upgrades can be applied later if necessary

Up-to-date security functionality:
Standards-based key management, security codes and PINs supporting the latest card and mobile applications

Data center friendly features:
Dual redundant power supplies, fans and Ethernet host ports delivering high resilience coupled with remote management to reduce operating costs – ideal for hosted environments

A range of performance levels:
Fast RSA key generation and PIN block translation using key blocks – performance upgrades available without hardware change

Independent security validation:
PCI HSM and FIPS 140-2 Level 3 certified, the recognized security standards for the payments industry

About Prime Factors

For more than 40 years, Prime Factors has served customers across six continents in a variety of industries, including 80% of the top financial institutions in North America, with cryptographic software solutions for payments, information exchange, and general data protection.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.