Solution Brief

Building More Secure Payment Applications Faster

Leveraging Prime Factors Bank Card Security System and Thales payShield for Better Security, Efficiency, and Agility

THALES
Building a future we can all trust

PrimeFactors™
APPLIED DATA PROTECTION

cpl.thalesgroup.com

Contents

Executive Summary

Developing secure payment applications in-house is costly, complex, and time consuming

Payment security is complex

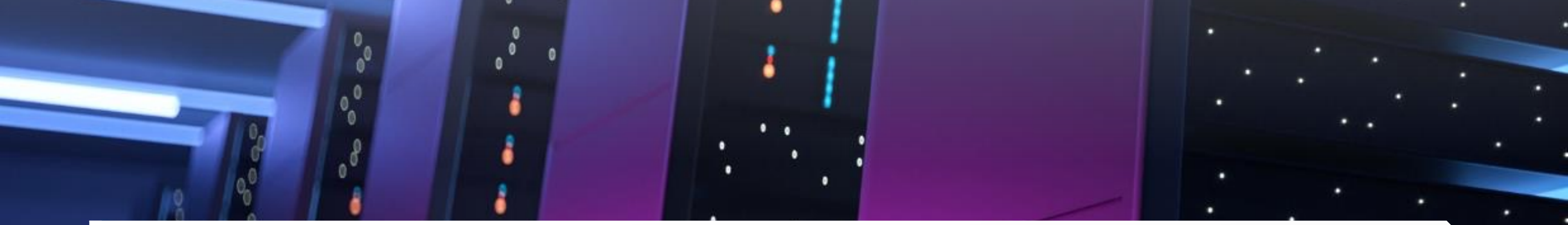
Unique jargon, rules, and cryptographic keys for securing financial information can be complex, posing challenges for organizations developing payment applications to comply with industry standards and regulations for issuing credentials and processing transactions.

Building payment applications is expensive

Creating compliant payment applications can take months or years, incurring significant costs. Re-designs to adapt to evolving payment security specifications can be equally challenging. Knowledge gaps, financial constraints, and compliance issues often limit functionality or increase the risk of audit failures.

There is a better, more cost-effective way

Gain greater visibility and control over your payment security infrastructure with a solution trusted by PCI auditors for over two decades. The Bank Card Security System from Prime Factors, paired with the leading payment HSM from Thales, helps **reduce time to revenue** and **lower costs**, delivering **improved security, efficiency,** and **agility.**



Payment Application Must-Haves

The critically important elements needed in payment applications to meet industry & regulatory compliance

Secure Key Vault

An application must establish a database to securely store and identify encrypted keys generated by the HSM.

Key Management

A key management utility must be developed to generate, assign, rotate, revoke, and manage application keys and exchange them with other parties.

Comprehensive Access Controls

The application must define and enforce users, roles, and duties, establish quorums, and govern dual controls as required by PCI standards to ensure authorized users can control keys and components for their intended purposes.

Audit Logging & Reporting

The application must generate detailed audit logs and reports to track user actions, activities, and the lifecycle of keys and EMV certificates.

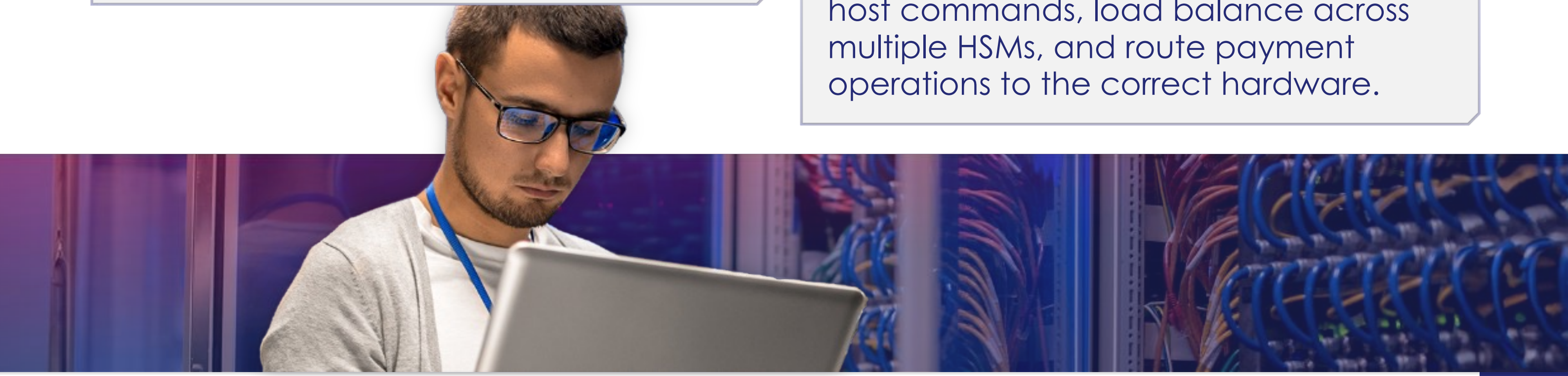
This is crucial to verify key management and security parameters within the payment infrastructure.

Cryptography Command Assembler

Applications must define, identify, and assemble the correct HSM command options, keys, and parameters to execute payment operations.

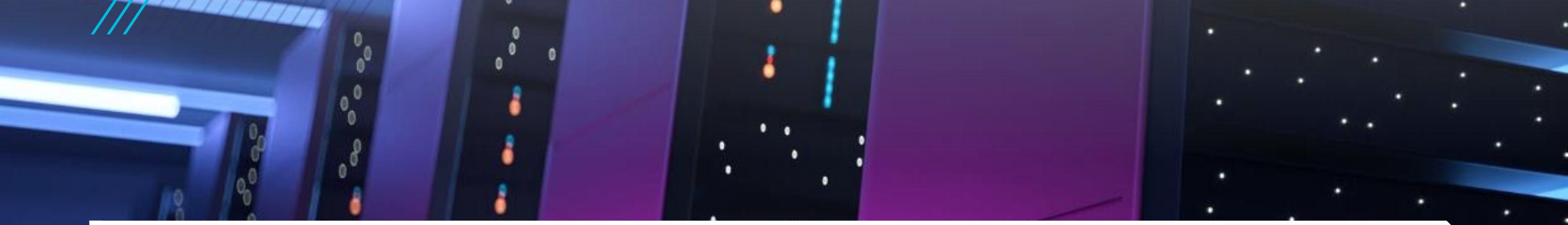
Payment HSM Handler

Applications must integrate with payShield using TCP/IP-based native host commands, load balance across multiple HSMs, and route payment operations to the correct hardware.



PrimeFactors — Applied Data Protection

THALES
Building a future we can all trust



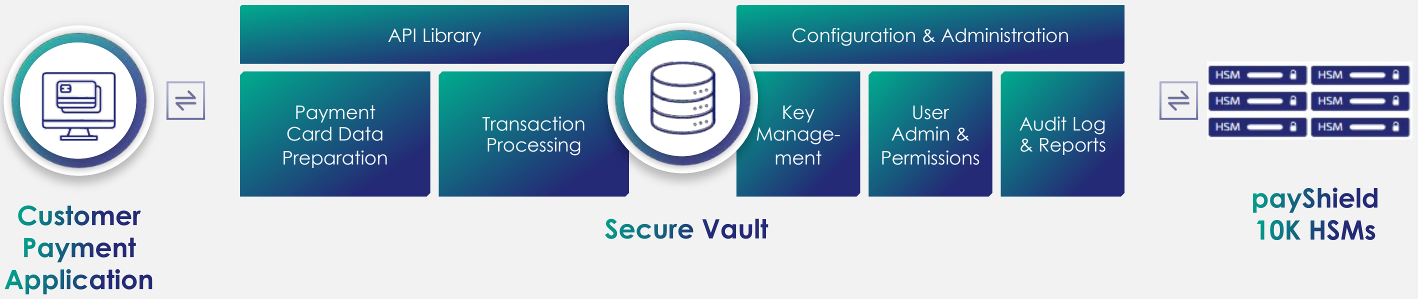
BCSS: Faster, Better, More Agile Apps

Generate revenue faster, reduce costs, and improve security for custom payment applications

BCSS is an application middleware that delivers the critically important elements needed in payment applications to meet industry & regulatory compliance out of the box.

BCSS enforces in-app security and interfaces with payShield HSMs, handling, routing, and load balancing all critical transactions to expedite payment application development and streamline HSM integration.

BCSS Payment Security



Customer Payment Application

API Library

Payment Card Data Preparation

Transaction Processing

Configuration & Administration

Key Management

User Admin & Permissions

Audit Log & Reports

Secure Vault

payShield 10K HSMs

A Fraction of the Work

Reduce costs, time-to-revenue, and complexity with the Bank Card Security System (BCSS)

Costs of Developing Everything Yourself	Out-of-the-Box Features of BCSS
Develop an internal secure database to store cryptographic keys and administrative controls	Secure key vault to organize and protect payment keys, EMV certificates, and other parameters for credential issuing and processing
Learn a new 'programming language' consisting of scores of HSM host commands	Simplified built-in subroutines for interfacing with hundreds of payShield host commands without specific expertise
Build an HSM Command Assembler and Interface Manager to pair correct keys and parameters with appropriate HSM commands and balance the load between HSMs effectively	Pre-built HSM Command Assembler and HSM Handler for managing all HSM interfaces and transactions with redundancy and load balancing
Organizing, managing, and selecting cryptographic keys for specific functions, BINs, or card types as complexity grows	Functional Partitions to organize cryptograms, parameters, and hardware for specific payment operations
Manually set up access and role permissions	Native role-based access controls to enforce responsibility separation, split key material knowledge, dual sign-on, and quorum support, including OpenLDAP and Active Directory integration
Build audit logs and reports	Forensic-level audit logs, Syslog messages, and robust reporting that has passed PCI audits for over two decades
Re-design application whenever changes are needed	Architected for crypto-agility, allowing changes in issuance, acceptance methods, and hardware upgrades without application rework

Better Organization for More Efficiency

Managing payment keys can get complicated

Managing different key types for various purposes can be complex, especially as the number of keys grows.

Using unique keys for different payment operations enhances security, but some keys might be linked to multiple operations.

Selecting the wrong key, command, function, or hardware can halt payments.

Simplifying payments complexity with functional partitioning

BCSS leverages a unique architectural concept - **Network Profile Record (NPR)** to organize the details needed to execute a specific payment operation into a single functional partition.

BCSS Network Profile Records

NPR Name	Device	# of Keys
BANCO-UNO	payShield 10K	14
GOLDCard	payShield 10K	6
FINDATA	ATMnetwork	55

Network Record: GOLDCard **NPR LMK Check:** 9D04A0

Device: payShield 10K **Device LMK Check:** 9D04A0

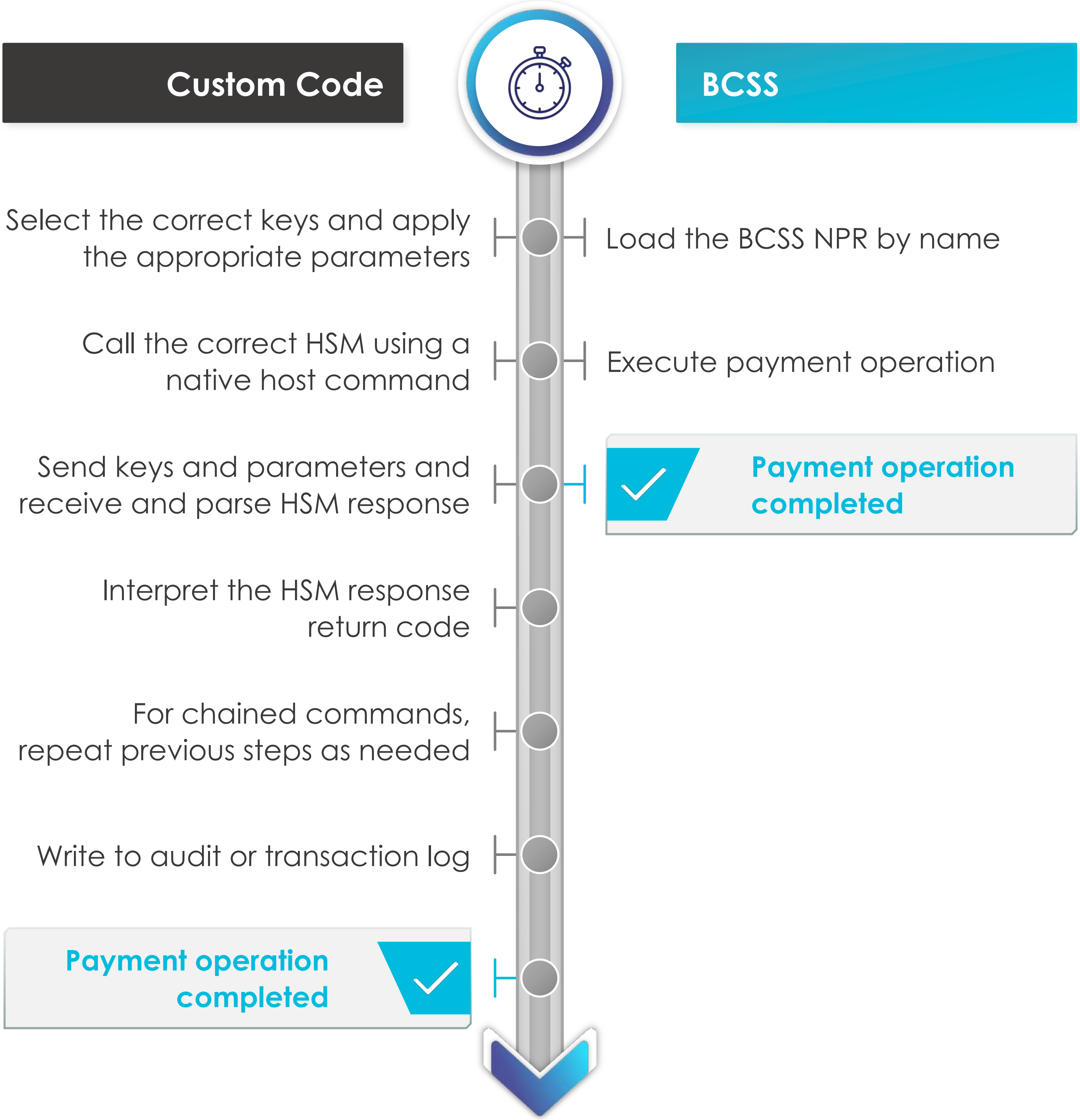
Storage ZMK: *None*

Type	Index	Length	#Vals	Key Check	Date Range
PINK	1	Double	1	DBCDB0	*Never Expires*
PVK	1	Double	2	48934A	*Never Expires*
CVK	1	Double	1	08D7B4	3 Months
CVK2	1	Triple	3	620D5B	*Never Expires*
ZPK	4	Triple	1	B9E6FB	3 Months
TPK	1	Single	1	4D0916	1 Month

The application simply identifies an NPR by name to execute specific payment functions and BCSS will **automatically use the correct keys**, parameters, and associated hardware defined within the NPR.

Efficiency by Example

Comparing the steps needed to execute a payment function in custom code vs. leveraging BCSS NPRs



Custom Code

- Select the correct keys and apply the appropriate parameters
- Call the correct HSM using a native host command
- Send keys and parameters and receive and parse HSM response
- Interpret the HSM response return code
- For chained commands, repeat previous steps as needed
- Write to audit or transaction log
- ✓ **Payment operation completed**

BCSS

- Load the BCSS NPR by name
- Execute payment operation
- ✓ **Payment operation completed**

Better Visibility & Control

Get real time handle on your data security posture

Robust Audit Logging & Reporting:

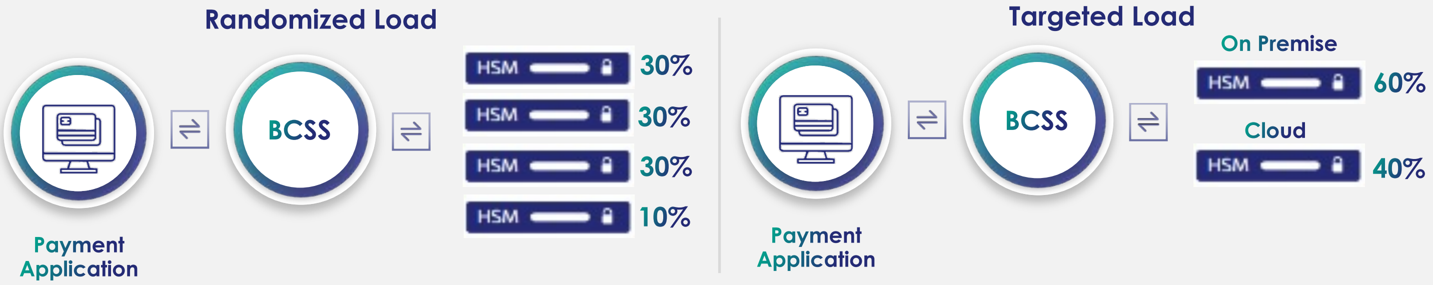
Event Tracking:	BCSS offers comprehensive functionality, tracking each event by date and time, including user ID and action performed.
Security measures recorded:	Each record in the audit log receives a sequence number and is hashed and encrypted.
Sensitive information protected:	While logs show changes, including when and by whom, clear keys and PINs never appear in trace files.
Tamper-proof:	All changes to user IDs and user privileges are recorded in authenticated log records to identify unauthorized tampering.

Transaction Analytics:

Transaction activity:	Gain better visibility into payment transactions, including the NPR used, the specific HSM port and command, and the time consumed.
Allocating transactions:	Verify transaction distribution across payment HSMs over time. Analyze volumes or specific transaction types across large hardware deployments.
Billing:	Verify processed transactions for specific clients or tasks.

Automatic Load Balancing:

BCSS Automatically load balances, spreading transactions evenly, or in a weighted manner, across HSMs, irrespective of their location (on-premises or in the cloud).



Future-Proofing Payment Security

It's only a matter of time until something changes, and the payment application must be reworked

State of the Market – Things Change

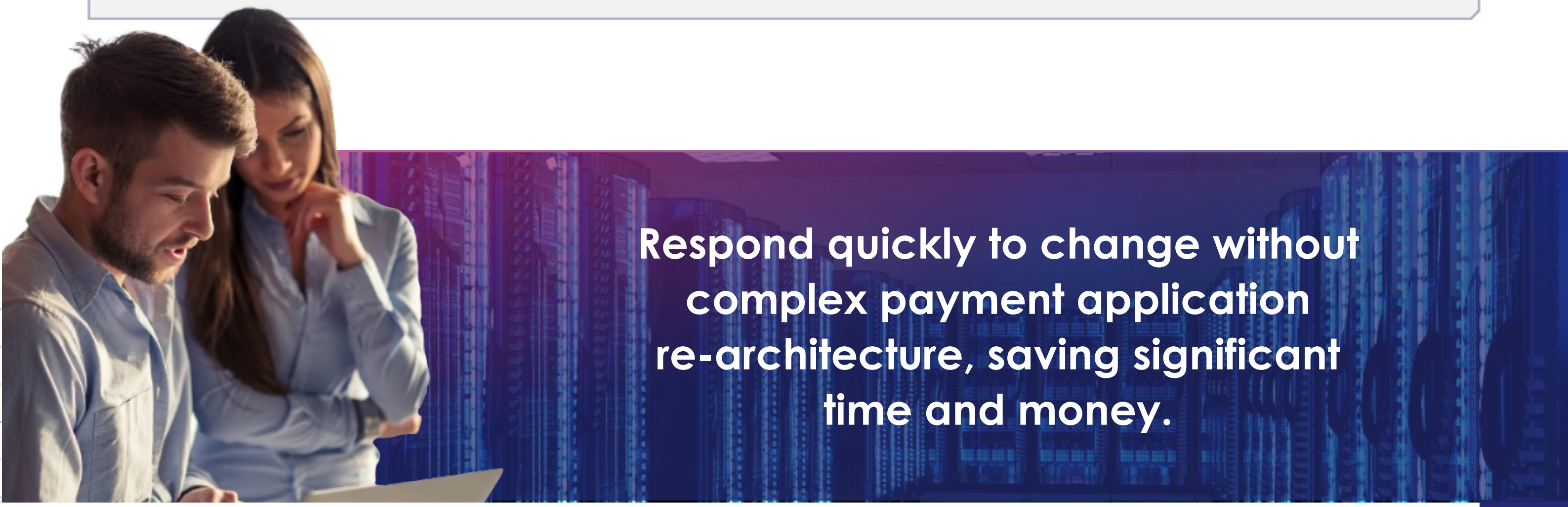
Organizations in the payment industry face constant changes, like **cloud migration, evolutions in cryptographic keys or algorithms, hardware updates, and PCI requirements** (e.g. **Key Blocks**), leading to extensive application re-work and new challenges related to skill gaps.

Crypto-Agility

BCSS is designed for **crypto-agility** – allowing customers to change administrative controls, keys, payment options, and encryption schemes, without re-development. Organizations can easily adapt to market changes at a much lower cost of ownership.

Deployment Flexibility

BCSS supports deployment on-premises, in the cloud, or in hybrid environments, providing **flexibility** and **future-proofing** by **enabling quick responses to industry changes** without complex redevelopment.



Respond quickly to change without complex payment application re-architecture, saving significant time and money.

Key Solution Takeaways

Faster Time to Revenue

BCSS delivers **out-of-the-box security functionality** to build compliant payment applications in a fraction of the time.

Lower Costs

Integrate with payment HSMs faster, without programming to proprietary host commands, and automatically manage hardware **load balancing, redundancy, and failover** with BCSS.

Less Risk

BCSS stays up to date on **industry standards, payment security trends, and deployment models,** so your security posture or environment can evolve over time **without extensive re-development.**

Robust Payment Security

Simplified.

For more than 30 years, Thales and Prime Factors have been collaborating to help enterprises effectively navigate the ever-changing landscape of payment security efficiently and securely. The payShield HSM brings industry-leading functionality for payment security and BCSS adds the application-side controls, organization, and abstraction that helps deliver faster time to revenue for payShield deployments.

Visit the Prime Factors or Thales websites to learn more.