thalescpl.com

THALES

Payment credential issuing using payShield HSMs

payShield 10K supports issuing for a wide range of payment instruments:

- Magnetic stripe cards
- Contact and contactless chip cards
- Secure Elements in devices
- Host card emulation applications
- IoT and wearable technology

Overview

payShield from Thales is the world's leading payment HSM, helping to secure an estimated 80% of global point of sale (POS) transactions. Thales HSMs have also been used for many years to prepare data for EMV chip cards, personalize the cards and help manage the complete lifecycle of the cryptographic keys and associated payment application credentials. payShield continues to evolve and over the past few years, significant new functionality has been added to support the data preparation and provisioning of mobile devices, wearables and connected devices used to make payments. This document provides an overview of the payShield issuance functionality.

The challenges as payment methods continue to evolve

Any issuer of payment instruments knows that complexity has increased significantly since the days of just having to support plastic magnetic stripe or chip-based credit and debit cards. The card world is still tightly controlled by the issuing banks and corresponding card brands—in contrast, the evolving mobile/IoT world has effectively put the consumer in control where often user experience and convenience are balanced with security, introducing new risks and threats. Some of the top challenges that issuers face today include:

- Keeping up to date with the latest approaches, specifications and security requirements which is time consuming
- Managing different risks associated with payment solutions involving Secure Elements, host card emulation, trusted execution environment or software running on consumer devices
- Ensuring their staff are trained in complex new skills to support a broader range of in-house and outsourced solutions

It is essential for issuers to have a flexible, secure, trusted foundation that can evolve as their needs change.

payShield provides a comprehensive functionality platform for issuers

The off-the-shelf payment credential issuing functionality offers issuers a one-stop-shop to meeting all their issuing needs. Integrated with leading in-house and service provider solutions, payShield has the depth of functionality to support all the major components required for the overall issuance process of a payment instrument. payShield software has helped many issuers simplify their integration efforts and lower their operating costs for:

- Cardholder management
- PIN management
- Key and certificate management
- Application data preparation
- Card and device provisioning
- Lifecycle management for cards and mobile wallets

Key benefits of using payShield for payment credential issuing

payShield continues to evolve, delivering a wide range of immediate benefits including:

- **Early support for all major card, mobile, IoT and emerging applications—**getting you to market faster
- **Proven integration with leading commercial issuing solutions—**reducing your testing time
- **Robust, scalable solution proven in service provider environments—**supporting your business growth
- **Cryptographic isolation for multiple applications and tenants—**delivering extra privacy where demanded
- **Certified to global and regional payment industry security standards—**helping you pass your security audits

Supporting requirements of cardholder management systems

Linked to nearly all payment credentials is a customer or cardholder account, normally associated with a primary account number (PAN). Issuers have expanded their cardholder management systems (CMS) over time to cover more than just payment cards. They now also address the security management needs of mobile devices, wearables and connected devices. payShield has a broad range of functionality supporting all major card scheme activities in all of these areas, providing a fast track approach for:

- Protecting core account data held on master databases for each customer
- Supporting interfaces to card scheme services relating to card digitization and tokenization services
- Generating and distributing PINs and secure passcodes used for authentication of the credential holder
- Securing the transfer of keys and data between the various issuing, personalization/provisioning and transaction processing systems

Managing keys and certificates

The lifecycle management of strong, random, hardware-generated cryptographic keys and associated trusted certificates is a core capability in which payShield excels. Issuers have easy access to secure functions for:

- Certifying the issuer key set
- Facilitating the creation of issuer certificates signed by the relevant global scheme Certification Authority (CA) or a National CA scheme if required
- Generating issuer master keys and sharing with trusted third parties where necessary

Preparing data for payment applications

payShield offers issuers the option to keep control of the keys and secure data destined for the customer card or mobile device rather than outsourcing everything to a third party service provider or bureau. The same core data preparation functionality can be used for cards, mobile secure elements, wearables, connected devices and host card emulation applications.

The functions included as part of standard software can be used for:

- Deriving card/device unique keys then encrypting the keys for transportation to a personalization or provisioning system
- Generating data authentication signatures, device specific keys and certificates
- Creating the data for EMV tags requiring cryptographic processing using the HSM

Provisioning cards and other payment devices

payShield has a set of card personalization and mobile application provisioning functions that can be used for:

- Establishing a secure session with a chip card or device (including mobile, IoT and connected devices)
- Exchanging secure messages with chip cards or devices after a secure session has been established
- Validating an authentication code from a mobile user when requesting a provisioning service
- Generating digitized card single use keys and securely delivering them to the mobile or connected device

payShield: a flexible, secure platform for all your issuance needs

- Securing critical assets at all times
- Supporting multiple integration approaches
- Helping to reduce operating costs

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 amount 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.

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalescpl.com <