cpl.thalesgroup.com

payShield 9000 / payShield 10K compatibility guide

Contents

payShield 10K

payShield 9000

payShield 10K HSMs are fully backwards compatible with payShield 9000 HSMs at the host application programming interface (API) level. This means that you can deploy any payShield 10K model with minimal impact on existing applications and without costly integration work. A consistent approach has been adopted across both product lines for both local and remote management, although you will find that some payShield Manager capabilities have been enhanced to reflect additional capabilities of the newer product.

Category	Specific area
Software	Host application Operating system independence Custom software availability
Configuration and management	Key management Local Master Keys (LMKs) Remote management Cryptographic isolation
Compliance	Audit compliance Testing procedure Existing HSM utilization

Check out the sections below for more details of how we have made it easy for you to introduce payShield 10K HSMs to your existing Thales payment HSM estate.

Host application

As an existing payShield 9000 user you can add a payShield 10K to your system without making any changes to your host application.Any application which makes function calls on the host interface of a payShield 9000 is able to make identical calls on the payShield 10K which is fully backwards compatible from a host API perspective. The responses and error codes returned by payShield 10K are identical to those produced by payShield 9000 running the same functions.

Operating system independence

Just like all Thales payment HSMs that have preceded it, payShield 10K requires no client software to be loaded on the host platform and therefore is compatible with all host operating systems. All of the cryptographic functionality required to manage and operate the HSM is contained within the HSM itself. This has the distinct advantage of being isolated from enforced host operating system upgrades or security patches, providing your HSMs with much higher uptime while also simplifying security audit compliance.

Custom software availability

The optional software customization service provided for payShield 9000 is also available on payShield 10K for new (or modified) customization requests and porting of existing customizations to the newer payShield 10K platform. The command/response host API and the associated error codes are identical between the HSM platforms. Existing payShield 9000 custom code requires recompilation and testing by Thales before it can be used on payShield 10K due to the different hardware and operating system environments. There is no impact on your host application.

Key management

You can continue to store your cryptographic keys in encrypted form (encrypted under an LMK variant or as a Key Block) on your host database rather than in tamper-resistant memory inside the HSM. payShield 10K uses identical LMK variant and Key Block structures to payShield 9000 and therefore all existing encrypted keys are compatible with a payShield 10K configured with the appropriate LMK.

You benefit from not having to generate new keys, translate existing keys or maintain two separate key databases when you are using a mixture of payShield 9000 and payShield 10K HSMs. Likewise a decision to simply replace all your existing payShield 9000s with payShield 10Ks, also means there is no need to generate any new keys or make any changes to your host application.

Local Master Keys (LMKs)

All Local Master Key (LMK) component smart cards generated and in use on any of your payShield 9000s are fully compatible with payShield 10K and will allow any of the newer payShield 10K devices to be configured with the same LMK as the payShield 9000 devices already installed. This allows you to introduce a new payShield 10K device to a system deploying one or more payShield 9000 devices and for each device to have the ability to utilize the same LMK and security officers if desired.

Remote management

Both payShield 9000 and payShield 10K are compatible with the Thales payShield Manager browser-based solution for remote management of HSMs. The functionality supported by the browser is built into each of the HSM types in question and therefore you will benefit from still being able to use payShield Manaager with all HSMs in a mixed estate of payShield 9000 and payShield 10K devices. The browser interface for payShield 10K contains some additional options and status information to reflect the enhanced features supported by the new device.

Cryptographic isolation

The ability to provide secure segregation of tenants or applications is maintained for payShield 10K. You can currently deploy a maximum of 20 LMKs per HSM that can be based on either the variant or Key Block LMK scheme. The smart cards that you currently use to hold the LMK components for payShield 9000 devices can be reused to support the same groups of LMKs on the payShield 10K devices.

Audit compliance

payShield 10K, like its predecessor payShield 9000, will be certified on an ongoing basis under both the FIPS 140-2 and PCI HSM approval schemes. The security engine (known as the Thales Advanced Security Platform or TASP) will be certified to FIPS 140-2 Level 3, whereas the overall HSM (including hardware, software, manufacturing process and secure shipping method) will be certified to v3 of the PCI HSM standard. In addition, the device management procedures, the key management methods, the algorithms and key lengths deployed are fully compatible with payShield 9000, ensuring that the HSM will be accepted as a compliant HSM by the various payment brand or other third party security audits that you need to comply with today.

Testing procedure

Test scripts that you have generated for use on payShield 9000 to test the operation of the host interface are expected to work on payShield 10K without modification. Likewise any test procedures you developed for the console interface are also expected to be compatible. Slight modifications may be required in some cases to support new or enhanced features supported by payShield 10K.

Existing HSM utilization

Existing payShield 9000 devices in live environments can still be used after the introduction of payShield 10K devices. The LMK formats are compatible and both types of device can run compatible base and custom code and be part of a cluster linked to a common host application. payShield 10K delivers exceptionally high levels of backwards compatibility with payShield 9000 to allow you to maximize your past investment in Thales HSM hardware while enabling a smooth migration to payShield 10K and without any fundamental change to proven security procedures and audit compliance.

payShield 10K enhancements—helping to improve your business

Thales has made some changes to payShield 10K compared to payShield 9000 to help you launch new services, lower your operating costs and prepare for future security needs.

payShield 10K enhancement	How you benefit
Latest application support	Taking advantage of the broader cryptographic support in payShield 10K compared to payShield 9000 enables you to launch new product options that depend on the latest payment brand applications and security standards for card, mobile and IoT platforms
Higher performance, lower power consumption	The significant performance increases in both symmetric and asymmetric algorithms on the top-end model means that you can support growth in transaction volumes more easily and potentially explore reducing the overall number of HSMs required in your estate – in addition power consumption is on average 40% lower than payShield 9000
Slimmer form factor	The ability to stack twice as many units into a data center rack enables you to save money on storage or rental fees
User-replaceable PSUs and fans	You no longer need to return the unit to Thales for repair in the event of a PSU or fan failure – you can now replace both items yourself without taking the HSM out of the rack
Clearer visual indicators	The uncluttered front panel design enables your staff who make periodic visual inspections of equipment in the data center to quickly identify any issues with any of your payShield HSMs via alerts such as large red warning triangles or red illuminated handles which are considerably easier to monitor than small multipurpose LEDs
Rapid HSM identification	Your remote team using payShield Manager can instantly light up the maintenance lights on the front and rear of the device making it simple for data center staff to pinpoint quickly the HSM or HSMs requiring attention without having to match serial numbers or identify sticker numbers
Faster firmware updates	The firmware loading process for payShield 10K is on average 10 times faster than that of its predecessor and more robust, reducing your device downtime and minimizing the impact of an unintended event such as a power failure during the update
Key erasure confirmation	A dedicated confirmation light on the rear panel stays illuminated for a sufficient time period after the key erase button is pressed, thereby providing you with assurance that the device is now safe to decommission or move outside a secure production environment if required
Enhanced base packages	payShield 10K includes more functionality in each of its base packages which reduces the overall number of optional licenses required and helps lower the overall cost of your software investment
Superior deployment flexibility	Additional design effort has been employed to make payShield 10K better equipped to handle a range of private and public cloud installation scenarios which helps future proof your investment in Thales payment HSM technology as you explore new service provider options

Next steps

Please contact your local Thales Account Manager or Reseller to plan your migration to payShield 10K. We are experienced in assisting existing payShield 9000 customers in quickly adding payShield 10K to established infrastructures.

What we can assist with

- payShield 10K installation and training
- Recompiling or updating of custom software
- Supporting your critical HSM infrastructure 24 x 7

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

Contact us

For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <