> PCI Approvals FAQ

THALES

www.thalesesecurity.com

PCI Approvals for payShield 9000 FAQ

We have put together the following FAQ to help answer questions on PCI compliance and the payShield 9000. We hope these answer all the questions you have, but if you require any more information please contact your Thales eSecurity Account Manager or local Thales eSecurity Support Team.

What is PCI All About?

The PCI Security Standards Council is a global forum for security standards for payment card data protection. The Council was founded in 2006 by the following card brands: American Express, Discover, JCB, MasterCard and Visa. They share equally in governance and execution of the Council's work.

The PCI Security Standards Council offers comprehensive standards and supporting materials to enhance payment card data security. This includes a framework of specifications, tools, measurements and support resources to help organizations at every step.

For device vendors and manufacturers, the Council provides the PIN Transaction Security (PTS) requirements. These include requirements for PIN Processing (PCI PIN) and for Hardware Security Modules (PCI HSM). For Point to Point Encryption solutions, a separate set of requirements is provided (PCI P2PE).

What Approvals Are Required for HSMs?

The card brands mandate that organizations processing relevant data must adhere to the following PCI requirements:

- **PCI PIN Security Requirements** – these contain a complete set of requirements for the secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and attended and unattended point-of-sale (POS) terminals.
- **PCI P2PE (Point-to-Point Encryption) Solution Requirements and Testing Procedures** – these facilitate the development, approval, and deployment of PCI-approved P2PE solutions that will increase the protection of account data by encrypting that data.

Both the above sets of PCI requirements themselves contain requirements for HSMs protecting PINs, account data and related cryptographic key operations. These HSMs must be Secure Cryptographic Devices (SCDs) meeting the requirements of ISO 9564 and approved to either:

- **FIPS 140-2 Level 3** or
- **PCI HSM**

Key Point

- ***Either FIPS 140-2 level 3 or PCI HSM approvals satisfy PCI requirements***

Is the payShield 9000 compliant with PCI PIN and PCI P2PE?

Yes - the relevant PCI requirements in PCI PIN and PCI P2PE allow deployment of either PCI HSM or FIPS140-2 Level 3 or higher approved HSMs. payShield 9000 is approved to both these standards, allowing customers to choose which approval to use when demonstrating compliance with PCI PIN or PCI P2PE.

Can You Explain More About FIPS140-2 Level 3?

> What is FIPS 140-2 Level 3?

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard used to validate cryptographic modules.

> How is the payShield 9000 FIPS 140-2 Level 3 Validated?

Validation is handled by third-party laboratories that are accredited by the National Institute of Standards and Technology (NIST). In common with other payment HSM manufacturers the scope of the FIPS 140-2 level 3 validation is restricted to the boundary of the secure cryptographic engine (TSPP) together with implementations of appropriate cryptographic algorithms.

> Is the version of payShield 9000 software important?

To claim compliance with FIPS 140-2 Level 3, all versions of payShield 9000 software from Thales eSecurity are acceptable.

> Where can I find confirmation that the payShield 9000 is FIPS 140-2 Level 3 Validated?

FIPS 140-2 validated devices are listed on the NIST web site, noting that payShield 9000 has certificate number #1322 and is listed under Module Name “TSPP”:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1322

To ensure compliance, it is important to note that the existing FIPS 140-2 Level 3 validation for the TSPP module used in payShield 9000 expires on 29 January 2022.

Can I Have More Information on PCI HSM?

> What is PCI HSM?

The Payment Card Industry Hardware Security Module (PCI HSM) specification defines a set of logical and physical security compliance standards for HSMs specifically for the payments industry. The payShield 9000 HSM from Thales eSecurity was one of the first HSMs to be successfully validated against the PCI HSM standard.

> How is the payShield 9000 PCI HSM Approved?

PCI Recognised Laboratories are organizations that have been approved by the PCI Council to conduct security evaluations on a range of product types, both hardware and software. For device vendors and manufacturers, the labs perform device testing to validate compliance to PCI HSM.

The process checks the following aspects:

- Hardware, including tamper-detection and response mechanisms
- Software
- Supply Chain process, including manufacturing and shipping

> Where can I find confirmation that the payShield 9000 is PCI HSM Approved?

PCI PTS approved devices (including PCI HSM approved devices) are listed on the PCI web site at the following location:

www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

> What other aspects do I need to consider to achieve compliance with PCI HSM?

To achieve compliance it is important to note the following requirements must also be met:

- payShield 9000 must be shipped using a PCI HSM compliant method and deployed within the certificate validation period (currently before the end of April 2019).
- The end user must configure payShield 9000 in a PCI HSM manner as detailed in the documentation supplied.

> Is the version of payShield 9000 software important?

Yes. In order to claim compliance with PCI HSM, each version of software deployed must be PCI HSM approved. The versions of payShield 9000 software validated are listed here:

www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

> Do all versions of PCI HSM meet the requirements of the card brands?

Yes. There are currently 3 versions of PCI HSM. All versions meet the requirements of PCI PIN and PCI P2PE.

What Else Should Be Considered After Initially Deploying the HSM?

PCI HSM addresses the security requirements of the payment industry up to the point of initial deployment.

Other security requirements apply at the point of deployment for the management of HSMs. The end user must consider and implement the relevant requirements in the PCI PIN Security and the PCI P2PE Solution Requirements and Testing Procedures documents. These requirements reflect good security practice, and cover aspects such as*: dual control; physical protection; access controls; procedures to ensure security and integrity; inventory control; tracking of movements; update control.*

Where Can I Find Out Further Information?

Further information can be found as follows:

> payShield 9000 General Information Manual for v3.1 and above, document number 1270A593, Chapter 10.

> PCI web site at the following location: www.pcisecuritystandards.org

Visit us at
www.thalesesecurity.com
to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.

Follow us on:

Americas – 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101-03, 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