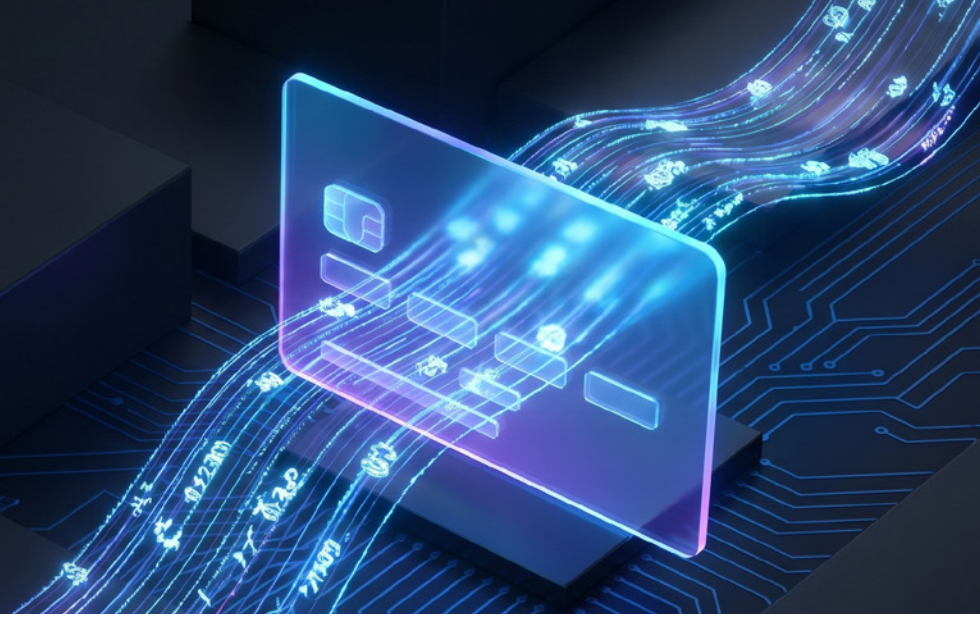


payShield Trusted Management Device (TMD)

Secure, Flexible and
Efficient Key Management
for Payment HSMs



- Encrypts sensitive key information at point of entry via secure touch screen
- Enforces strong role-based authentication for critical tasks
- Supports choice of output formats for keys and components
- Offers use of QR codes to streamline key sharing and reduce data entry errors
- Presents compact, intuitive, self-contained PCI HSM KLD solution for use anywhere

- Separate Administrator, Operator and Auditor roles managed using TMD smart cards
- Flexible range of methods of sharing keys & components securely between the TMD and HSM – QR codes, smart cards, USB tokens & paper components

Administrators

- Administrator roles are created by MZMK component holders
- Administrators assign roles to Operators and Auditors

Operators

- Operators may perform functions according to the role(s) assigned by Administrators
- Dual control enforced for all Operator functions
- Functions include key management & system operations

Typical use cases

- Forming keys from components
- Splitting existing keys into component
- Sharing symmetric KEs internally within an organization or externally with trusted third parties

Overview

The payShield Trusted Management Device (TMD) from Thales is a compact, intuitive, self-contained secure cryptographic device (SCD) that enables you to securely manage symmetric keys. TMD generates keys in a manner that is compliant with relevant security standards, including X9 TR-31, ANSI X9.24-1 and PCI PIN Security. Unlike traditional approaches, this critical key management task can be carried out without any physical connection to a production HSM, providing greater operational flexibility without compromising security. A single TMD can form keys for multiple payShield HSMs distributed across multiple data centers, enabling large payment processors, for example, to create and distribute thousands of symmetric keys in a timely and secure manner while eliminating data entry errors.

Key Management Functionality

The TMD shares one or more keys, known as Master Zone Master Keys or MZMKs, with the HSMs to facilitate secure exchange of key material. This avoids the need for the TMD to require access to the Local Master Keys (LMKs) used by the production HSMs. Keys generated by the TMD are supplied to the HSMs encrypted under the appropriate MZMK where they can be imported.

- Up to 20 MZMKs are supported per TMD : DES (double & triple length) and AES (128, 192 & 256 bits) cryptographic key support
- TMD smart cards used to hold shares of each MZMK – 2 minimum, 9 maximum for authorization



Security Features

- Sensitive data erased immediately in the event of an attack tamper responsive design independently certified by PCI
- Strong role-based authentication (dual control minimum)
- Secure touch screen replaces traditional keyboard – sensitive key information encrypted at point of capture
- Comprehensive audit log

Device Features

- Compact, intuitive, self-contained solution – no accessories to attach
- QR codes simplify key sharing – avoids manual data entry
- Integral printer quickly prints component or cryptogram avoids writing down screen information
- Integrated camera facilitates easy key distribution – no need for manual entry

Product Models and Options

- 7" 1280x800 full color TFT IPS capacitive touch screen display
- Rechargeable & replaceable 5200 mAh Li-Ion battery
- Power supply option packs for US, UK, Europe & Australia
- Integral ISO/IEC 7816-1/2/3 compliant smart card reader
- Integral thermal printer (48mm printing width with tear bar)
- USB cable (type C to type A)

Security Certifications and Compliances

- PCI HSM certified KLD
- PCI PIN Security audit

Physical Characteristics

- Height 72mm
- Width 114mm
- Depth 231mm
- Weight 625g
- Power 5V/2A switching power adapter, Li-Ion battery
- Operating Temperature: 0 to 50C
- Battery Charging Operating Temperature: 0 to 45C
- Storage Temperature: -20 to 60C
- Operating Humidity: 5 to 85% (non-condensing) Safety and Environmental Compliances
- TUV CB, cTUVus, FCC, IC, CE, RCM
- RoHS, REACH, WEEE

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.