thalescpl.com

THALES

Key Management Device
for Thales payment HSMs

Secure, flexible and efficient key management for payment HSMs

- Reduces operating costs by streamlining key management tasks
- Complies with ANSI/ISO/PCI key management standards to simplify security audits
- Maximizes flexibility by managing keys for multiple HSMs and their associated LMKs from a single device

Technical specifications

The Key Management Device (KMD) from Thales is a compact, secure cryptographic device (SCD) that enables you to securely form keys from separate components. KMD generates keys in a manner that is compliant with relevant security standards, including X9 TR-39, 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 KMD at a remote location can form keys for multiple payment HSMs distributed across multiple data centers.

Key management functionality

The KMD shares one or more KMD Transport Keys (KTKs) with the HSMs to facilitate secure exchange of key material. This avoids the need for the KMD to require access to the Local Master Keys (LMKs) used by the production HSMs. The KTKs use the same double length variant key structure as the LMKs. Keys generated by the KMD are supplied to the HSMs encrypted under the appropriate KTK where they can be imported. The HSM has a set of console commands to support the management of KTKs for multiple KMDs, enabling highly granular separation of keys if required.

- Up to 20 KTKs supported per KMD
- KMD smart cards used to hold shares of each KTK – 2 minimum, 9 maximum for authorization
- Separate administrator and operator roles managed using KMD smart cards

Administrators

- Administrator roles are created by KTK component holders
- Administrators assign roles to Operators

Operators

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

Cryptographic support

- Triple DES (2-key and 3-key)

Certifications and compliances

- ANSI X9.24-1:2009
- X9 TR-39/TG-3:2009
- PCI PIN Security requirements V2.0:2014

User interface

- 5.6" touch screen color display
- Intuitive graphical user interface

Security

- Flexible role-based access control
- Two-factor authentication using ISO 7816 compliant smart cards
- Tamper-responsive SCD that is derived from PCI PED certified device

Physical characteristics

- Height: 153mm (6.0")
- Width: 192mm (7.5")
- Depth: 57mm (2.24")
- Weight: 0.77kg (1.68lbs)
- DC Voltage: 12 V DC at 1.0 A
- AC Power Pack: 100-240 V, 50/60 Hz @ 0.5 A
- Operating Temperature: 0 to 40°C (32 to 104°F)
- Storage Temperature: -18 to +66°C (0 to 150°F)
- Humidity: 15% to 95% (non-condensing)

Learn more

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

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 number 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.

> thalescpl.com <

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) Lt, 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