

KEY MANAGEMENT DEVICE FOR THALES E-SECURITY 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



«Thales e-Security»

KEY MANAGEMENT DEVICE

Secure, Flexible and Efficient Key
Management for Payment HSMs



KEY MANAGEMENT DEVICE (KMD)

Technical Specifications

The Key Management Device (KMD) from Thales e-Security 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.thalesecurity.com to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.

Follow us on:

