THALES

Key Management Device for Thales e-Security Payment HSMs

KEY BENEFITS

- Operates without connecting to production HSMs thereby reducing operating costs
- Complies with ANSI/ISO key management standards to simplify security audits
- Manages keys for multiple HSMs and LMKs to maximize operational flexibility
- Supports software upgrades to satisfy future key management requirements

A flexible and secure approach to key component management for payment HSMs

The Thales e-Security Key Management Device (KMD) for payment HSMs is a compact tamper-resistant security module (TRSM) that enables keys to be formed securely from separate components in a manner that is compliant with relevant security standards including X9 TR-39, ANSI X9.24-1 and PCI PIN Security.

Unlike the traditional approach, this critical key management task can be carried out without any physical connection to a production hardware security module (HSM), providing greater flexibility without any degradation in security. A single KMD can form keys for multiple payment HSMs using different local master keys (LMKs).

With its touch screen graphical user interface, the KMD is simple and intuitive to operate, and is compatible with the full range of Thales payment HSMs including the award-winning payShield 9000. The device configuration and management user interface complies with banking grade security best practices and the installed software is automatically validated for integrity prior to use. Upgrades are supported to meet future functional enhancements and security audit requirements.

> Thales Key Management Device (KMD)

Technical Specifications

Key Management Functionality

- Compatible with variant Local Master Keys (LMKs) used in Thales payment HSMs
  - payShield 9000
  - HSM 8000
  - RG7000
- Compatible with standard HSM LMK smart cards
- Support for multiple LMKs for comprehensive separation of key types, applications or customer data
- Separate administrator and operator roles

Administrators

- Administrator roles are created by LMK 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

Features & Benefits

- Secure component entry (directly into TRSM)
- Standalone key management functionality
- Flexible role-based access control
- Secure software upgrade

Cryptographic Support

- Triple-DES (2 key and 3 key)

Certifications & Compliances

- ANSI X9.24-1:2009
- X9 TR-39/TG-3:2009
- PCI PIN Security Requirements V2.0:2008

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-resistant and responsive hardware 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)

Americas: 2200 North Commerce Parkway, Suite 200, Weston, Florida 33326 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific: Unit 4101, 41/F, 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