cpl.thalesgroup.com

THALES

Top 10 reasons for using the payShield Trusted Management Device

Increasingly the payments industry standards are demanding more secure solutions for the manual entry of key components into hardware security modules (HSMs). The complexity of physically gathering IT resources inside data centers for key ceremonies, so they can access a console or dumb terminal connected to the HSM, is time consuming and costly. The payShield Trusted Management Device (TMD) complements the payShield Manager remote management solution for Thales payment HSMs by offering an efficient, flexible and secure approach to managing and sharing critical keys in locations remote from production HSMs. We have compiled a top 10 reasons for using the device for sensitive key management to help you understand the significant benefits.

Improve efficiency

1 Intuitive self-contained solution
It is fast and easy to train staff on this intuitive touch screen solution. Everything is included in the portable handheld device with no accessories to attach. You should expect to get a full day's work achieved on a single charge. Unlike the legacy console approach, payShield TMD does not implicitly need specialist Key Managers to operate effectively – you can involve a broader range of IT staff.

2 Simplified key management
It is designed explicitly to simplify key management by offering alternatives to the cumbersome approach of manual key entry via a direct HSM connection. Common data entry errors associated with legacy approaches are eliminated. The security policy for key generation and distribution is totally under your control, enabling payShield TMD implementation and procedures tailored to your needs, delivering efficiency without the risk of degrading overall key security.

3 Rapid key sharing options
You can use the integrated printer and camera to quickly share keys using QR codes, a unique and innovative feature offering of the payShield TMD. The printer removes the need to write down screen information and the QR code is a quick and error free method for entering components and keys. The touch screen interface reduces the time needed to complete many tasks through elimination of most historical typing requirements.

Increase flexibility

4 Remote location deployment
The device can be operated in any secure location outside the data center. There is no physical HSM or network connection required, making it more flexible to deploy. It is much easier to organize key ceremonies for key generation and sharing compared to the legacy console approach. Effectively you have 24x7 access to sensitive key management capabilities using a flexible group of security team members with higher availability. Everything you perform using payShield TMD can complement what you already achieve using Remote payShield Manager, thereby reinforcing the value of remote management for your HSM estate.

5 Multiple security teams supported
Every single payShield TMD device can support up to 20 individual cryptographic zones. Each of these zones could be managed by separate security teams if desired to reflect different applications operating in your organization for example. Our solution is highly flexible in offering you the ability to configure the roles available to each team member on an individual basis, underpinned by smart card ownership with PIN control.

6 Wide range of output formats
Traditional approaches to manual key management often were restricted to paper components. payShield TMD broadens the choice and now the keys you generate are in encrypted form under a range of formats – text (screen or printed), QR codes and USB tokens. This facilitates broad coverage of symmetric keys with varying key strengths for the 3DES and AES algorithms. All key types conform to the TR-31 standard - they can be generated and shared, both internal and external to your organization, as needed.

7 Retrospective component creation
An important benefit of using payShield TMD is that it offers you the ability to avoid key component storage after keys have been formed and shared. For any installed key that subsequently needs to be shared, creating new key components retrospectively is available. This delivers significant cost savings and flexibility in implementing your overall key management infrastructure as you no longer have to worry about securely storing key components when not in use or risk operational disruption if a component is lost.

Strengthen security

8 Secure touch screen
Replacing the traditional console or dumb terminal with our secure cryptographic device means that PIN entry and key component data is encrypted at the point of capture. All sensitive data stored inside the device is erased immediately in the event of a tamper attack. The overall hardware and software solution that comprises payShield TMD is independently certified to PCI HSM v3 Key Loading Device (KLD) standards, helping you meet the latest security audits.

9 Strong role-based authentication
All users of the payShield TMD solution require individual smart cards. Dual control is enforced via such smart cards for all key management and device management operations. Each smart card is under PIN control – the cards are proprietary to the device and counterfeit cards will be detected and blocked. Administrators define and manage Operator roles for the cryptographic zones under their control.

10 Comprehensive audit log
Each notable action is recorded together with the smart card serial numbers used during the dual authentication process – any attempt to modify log entries will be detected due to the message authentication deployed. The audit log can be filtered (including by cryptographic zone) to assist with analysis. Strict rules on the reading, exporting and deletion of the log are enforced.

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.

> cpl.thalesgroup.com <

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us