thalesesecurity.com

THALES

Top 10 reasons you can't live without remote HSM management

Improved efficiency

1. Multiple HSMs across all sites can be managed securely from a single central location

The system uses a standard web browser (Internet Explorer, Chrome or Firefox) connecting over a TCP/IP network to the HSM via a secure authenticated session. Strong encryption is employed to protect the data which involves AES 256-bit session keys and ECC 521-bit certificates. HSMs can be logically segregated and grouped as appropriate into separate security domains normally under the control of different security teams. payShield Manager can be used to place any HSM into one of its three permitted states (online, offline and secure) and for transitioning between states – specific smart cards are required during such processes which replace the physical brass keys in face-to-face HSM interactions.

2. Software and license upgrades are much easier to install

Dual smart card control is enforced by payShield Manager to place the HSM into secure state. A single button is clicked to start the software update process when the HSM is in secure state. The user has the option of dragging and dropping the file or navigating to the file location to select the appropriate file to be used. A wizard guides the user through the software upgrade process which takes place over a secure HTTP link. The license upgrade process uses a similar approach after the dedicated 'update licensing' button is pressed. Detailed information on the software version and active licenses is available before and after the software or license upgrade process.

3. Intuitive user interface reduces risk of errors

The legacy console approach to HSM management requires complex data entry in a rigid format associated with the command line interface (CLI). In contrast payShield Manager facilitates rapid navigation via an intuitive menu system using web-based accordion presentation style and simple parameter selection, significantly reducing the risk of incorrect information being entered. Extensive use of check boxes eliminates a lot of typing which is a distinct advantage for example when enabling or disabling host commands as part of a device hardening activity.

4. Travelling to multiple data centers to manage HSMs is no longer necessary

The only pre-requisite for a payShield Manager session to be established is that the HSM is fully locked in the online state in the data center rack – this is a step that is performed during installation and does not normally require security team members to be present. The commissioning of the various smart cards can either be performed securely in the data center or at a remote location. The fact that all HSM management tasks can be performed securely from a location remote from the data center (including the master key installation process) generally eliminates the need for travelling to data centers for routine tasks.

Additional flexibility

5. Freedom to choose the location for remote access simplifies logistics

payShield Manager can be operated from any remote location that meets the operational and security needs of the organization who controls the HSMs. A major advantage is that it is potentially much easier logistically for security team members (especially master key component holders) to meet at such a remote location rather than being constrained to booking a time slot in a data center where there is no flexibility on location.

6. Critical HSM status is remotely accessible to network staff to quickly identify potential issues

Each HSM can be configured to allow staff without payShield Manager smart card credentials to see information on the login screen such as the HSM name/serial number, performance model, software version, online status and the number of error log entries. This is primarily intended for network staff (without security administration rights to change HSM configurations via payShield Manager) to play a role in monitoring HSM basic status and be able to alert the relevant security teams if any potential issues are present.

7. Physical access and time constraints associated with travel to data centers are eliminated

payShield Manager can operate totally independently of any time and access control constraints associated with the data center(s) where the HSMs are located. It only needs a have a valid network connection from any remote location to the data center in question to support the establishment of a secure session using payShield Manager smart cards. This enables any of the HSM management tasks to be performed remotely with the same full functionality available as when face-to-face with the HSM in the data center. The major benefit is that payShield Manager is available 24 x 7.

Greater control

8. Flexibility to control individual tasks based on specific roles improves security

The left and right physical brass keys are replaced by left and right RACC (remote access) smart cards in payShield Manager to support administrator functions. Master key components are stored on RLMK smart cards to support the authorising officer and master key management functions. The RLMK smart cards are based on an 'm of n' share scheme which provides more flexibility in supporting a larger group of security officers. Users restricted to monitoring activities only when the HSM is in online mode are provided with Restricted RACC smart cards. There is flexibility in deciding how many of each type of smart cards are to be created and distributed to support individual security policies.

9. Strong access control based on digital credentials is preferable to reliance on physical keys

All tasks performed using payShield Manager where changes to the HSM configuration are applied require smart cards with user established PINs – the physical brass keys used in some face-to-face HSM interactions are not required. The smart cards provide enhanced security through two-factor authentication (what you have, the card and what you know, the PIN) whereas the physical keys only provide single-factor authentication (what you have, the physical key).

10. Tracking of activities to individual card credentials provides stronger audit control

All login to payShield Manager is via smart card under PIN control. Any action performed using the smart card creates an entry in the audit trail enabling that event to be traced back to the user or users who placed the HSM into online, offline or secure states as appropriate. In contrast the legacy approach (prior to payShield Manager) using master key and authorising officer smart cards in association with physical brass keys does not provide such a detailed entry in the HSM audit log, making traceability at user level not feasible via the HSM audit log.

About Thales eSecurity

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 amount 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.

> thalesesecurity.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • 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