

Mainframe encryption and key management with PKWARE and Thales



Organizations face a daily challenge to make data available to their customers and employees while also ensuring that this data is secure from internal and external threats. Add layers of regulations and the need to maximize returns on investments made in the datacenter, and organizations suddenly face a tough balancing act. Fortunately, PKWARE and Thales have a solution that keeps data secure and available, all while reducing strains on datacenter resources.

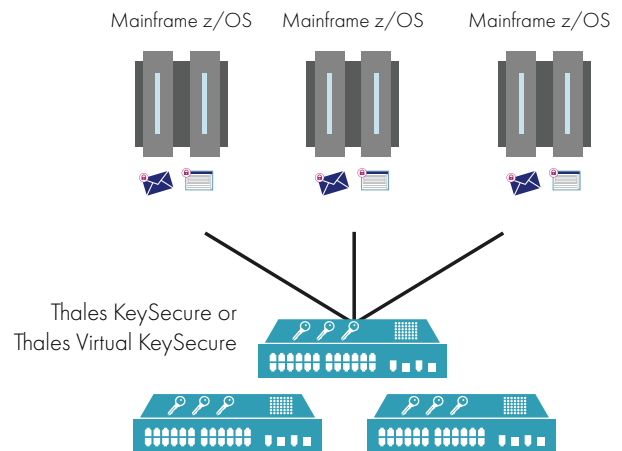
Solution

PKWARE mainframe encryption couples with Thales' KeySecure key management appliance to offer an enterprise class security solution for IBM Mainframe z/OS operating environments. Thales ProtectApp encryption SDK links PKWARE's Smartcrypt Platform to Thales' key management appliance for a complete solution that ties security directly to sensitive data while offering administrators granular controls to further secure data from insider threats.

PKWARE Smartcrypt Platform

PKWARE Smartcrypt Platform for z/OS offers organizations an encryption solution for mainframes using z/OS. Smartcrypt for z/OS is flexible; customers can embed encryption directly into their applications, or secure mainframe databases with field-level, length-preserving encryption. In any of its deployment scenarios,

end-users see no change to their experience while organizations escape needing significant changes to their underlying infrastructure. As a bonus, the ability to compress data reduces strains on bandwidth and allows customers to derive greater return on storage investments.

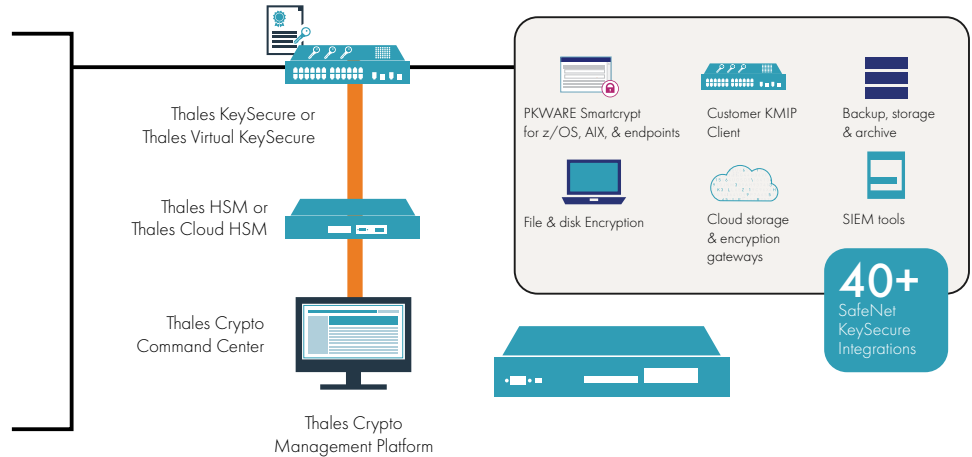


Use Case: Mainframe Encryption: z/OS Platform for z/OS,
Products Concerned: PKWARE Smartcrypt Platform for z/OS, Thales ProtectApp and Thales KeySecure

Data encryption solutions by Thales



Thales's key management ecosystem



Benefits

Persistent data security for z/OS

Encryption secures data wherever it resides while keys are stored in purpose-built hardware security modules on z Systems' hardware.

Hardware crypto processing for better performance

With ICSF integration in Smartcrypt for z/OS, applications are enabled to leverage z Systems hardware crypto.

Simplified compliance

Centralized, efficient auditing of key management practices saves time and simplifies meeting compliance mandates.

Secure all forms of data

PKWARE encryption is flexible enough to secure both structured and unstructured data.

constraining access to specific keys according to job responsibility. Ongoing storage and backup management occur normally; however, storage administrators cannot access data unless they are entrusted by policy with encryption keys.

Centralized encryption key management

Smartcrypt for z/OS may be one of many encryption solutions used in a datacenter. Disparate solutions lead to key management silos, each with its own discrete enforcement policy. KeySecure centralizes and simplifies key management for Smartcrypt along with a broad ecosystem of third-party KMIP-compatible encryption solutions. Consolidating these solutions simplifies their management and auditability.

High availability and intelligent key sharing

Thales KeySecure deploys in flexible high availability (HA) configurations within an operations-center or across geographically dispersed centers using an active-active mode of clustering. Key information automatically replicates to other Thales KeySecure appliances within the cluster across multiple datacenters or clouds to ensure that keys are persistently available in the event of site disruptions.

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.





Thales KeySecure

Thales KeySecure is an encryption and key management appliance that secures and centralizes the administration of Smartcrypt keys and certificates. Consolidating policy and key management simplifies administration to reduce the risk of errors and blindspots, while also freeing time for personnel to tackle other tasks. It makes key surveillance, rotation, and deletion easier which improves security.

Key features

Separated administrative duties improves security

Smartcrypt for z/OS attaches security directly to the data so that it will remain secure wherever it goes. Thales KeySecure's granular authorization controls limit risk posed by privileged insiders by

> cpl.thalesgroup.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@thalessec.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: apacsales.cpl@thalesgroup.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com