Alliance Key Manager for VMware
Solution Brief

Encryption Key Management for Virtualized Environments

Server virtualization has been a game-changing technology for IT, providing efficiencies and capabilities that have previously been impossible for organizations constrained within a physical world. Using the same FIPS 140-2 compliant technology that is in Townsend Security's hardware security module (HSM) and in use by over 3,000 customers, Alliance Key Manager for VMware enables enterprises to lower operational costs, meet compliance requirements, deploy encryption key management in the cloud, and accelerate deployment of mission critical security technology through a virtualized encryption key manager.

VMware Technology Alliance Partner

Townsend Security is a VMware Technology Alliance Partner (TAP) and Alliance Key Manager for VMware has achieved VMware Ready status. This designation indicates that after a detailed validation process Alliance Key Manager for VMware has achieved VMware's highest level of endorsement.

vmware READY APPLICATION SOFTWARE

Townsend SECURITY

Cost-Effective
Affordable key management solution for any size organization. Leverages current investment in encryption technologies via vendor-neutral solution.

Compliant
Validated for PCI DSS by Coalfire, a PCI-qualified QSA assessor and independent IT and audit firm.

Compatible
Accessible from any Enterprise platform including Windows, Linux, IBM i, IBM z, and others.

OASIS KMIP (Key Management Interoperability Protocol) compliant.

Easy to Use
Ready-to-use client software speeds deployment and reduces IT costs.

Secure Administration
Protects against key loss through secure and authenticated administration.

Partner Friendly
Extensive partner program insures successful and compliant results for your end customers.

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360 357 9047

Alliance Key Manager for VMware

Alliance Key Manager generates symmetric encryption keys for all AES key sizes including 128-bit, 192-bit, and 256-bit encryption keys. Encryption keys are generated using a cryptographically secure pseudo-random number generator (CSPRNG), and are stored in a secure database. All encryption keys are protected by two layers of encryption as well as SHA-256 hash verification to prevent key corruption and key substitution.

Encryption keys can be either expiring or non-expiring to enforce key use policies as defined by the security administrator. Additionally, encryption keys can be created in advance of use and only available at a pre-determined future date. Encryption key management is restricted to the security administrator and all key management activity is logged to the system log audit trail.

Alliance Key Manager in vCloud

As enterprises adopt Public and Private clouds, they bring their sensitive data with them – customer names, email addresses and other personally identifiable information (PII). While compliance regulations require protecting this information, encrypting this data has been a challenge for organizations who want the flexibility and security of a native VMware solution. By deploying Alliance Key Manager for VMware as a vCloud instance, customers can achieve their security and efficiency goals in a cloud environment.

On-Device Encryption Service

Alliance Key Manager supports a NIST-compliant on-device encryption service so that encryption keys never have to leave the device. This is an attractive option for Internet-facing web applications that process sensitive data. When there is more risk of exposure of encryption keys, you can use on-device encryption which never exposes encryption keys in the user application environment.

Simplified Central Administration

An intuitive GUI application allows Security Administrators to easily create and manage encryption keys and access policies on Alliance Key Manager for VMware. All access to security administration is authenticated using SSL/TLS client and server authentication, enabling multiple security administrators to log in and meet compliance regulations for dual control.

User and Group Control for Key Access

Security administrators can enforce user and group level controls over access to encryption keys. Encryption keys can be restricted to a specific list of users, a specific list of groups, or specific users within a group. Alliance Key Manager uses the distinguished name in certificates to enforce user and group controls which reduces administrative time and cost.

Sample Code and SDKs

Binary key retrieval and encryption libraries are provided for all major operating systems to enable rapid deployment of encryption key retrieval or on-device encryption applications. Sample source code is also provided for Java, .NET (C#), PHP, Perl, RPG, COBOL and more.

Client Side Applications

Available at no extra charge, Townsend Security includes ready-to-use security applications for Microsoft SQL Server Transparent Data Encryption (TDE) and Cell Level Encryption, Drupal, and other applications. There are never extra fees for deploying client-side applications.

Supported Versions of VMware

Alliance Key Manager for VMware supports:

- VMware ESX
- VMware vSphere (ESXi)
- vCloud

Townsend Security

Townsend Security is a VMware Technology Alliance Partner. The company provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, Linux, and UNIX. The company can be reached at www.townsendsecurity.com or (800) 357-1019.