StorMagic

DATA SHEET

StorMagic SvKMS
ENCRYPTION KEY MANAGEMENT

STORMAGIC SvKMS

StorMagic SvKMS is an encryption key management solution that can be deployed in any environment. It simplifies complex security and key management infrastructure by providing centralized management and, illustrated in fig. 1, the ability to deploy a KMS to wherever it is needed. This makes it perfect not only for the datacenter, but for the cloud and edge computing environments as well.

Whether on-prem, cloud or multi-cloud, SvKMS offers organizations the flexibility to locate their key management resources where required. It eliminates the need for hardware security modules (HSMs) and uses a REST API for easy integrations into any workflow with custom key imports facilitating an easy transition from legacy solutions.

StorMagic SvKMS is FIPS 140-2 certified, allows advanced identification and access management through SAML 2.0, and can be configured as a single- or multi-tenanted solution, making it an ideal choice for managed security solution providers.

This data sheet is broken down into four sections, covering the features in SvKMS, its requirements, hardware and software compatibility, and finally support levels.

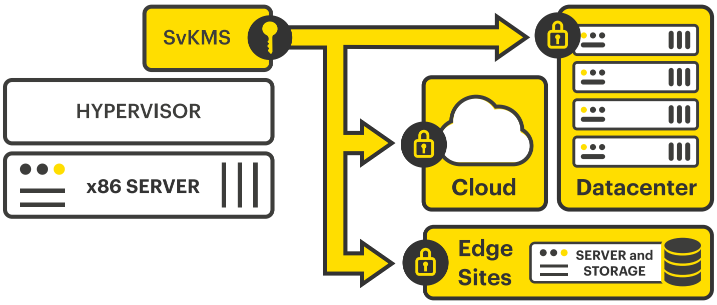

Fig. 1: A typical SvKMS deployment serving keys remotely to any environment or workflow.

SvKMS FEATURES

StorMagic SvKMS includes a comprehensive suite of features allowing control of the full key management lifecycle. All of these features are detailed in the table at the end of this document.

KMIP

SvKMS has been built around maximizing the KMIP open standard to enable organizations to leverage it as part of their key management operations. With SvKMS you can centrally manage, store, and consolidate encryption key management tasks across cloud, SaaS, on-premise systems, and endpoint devices like mobile and IoT.

BYOK/CSEK

Bring Your Own Key (BYOK), or Customer Supplied Encryption Keys (CSEK), ensures encryption keys remain in the hands of the business, regardless of location. This gives business users control for data held off-premise - if the content owner disables access to the keys, it becomes impossible for the information to be decrypted by any third party.

Custom key import

Over time, an organization may have anything from hundreds to millions of keys being used within a complex cryptographic environment. SvKMS's custom key import feature allows users to import keys that may have created by another key manager in a common format, or through a custom algorithm – including PGP, GPG, DES, CAST and Blowfish.

REST API integration and automation

Manually addressing all key management functions at the application level is time-consuming and inefficient, and old-style key managers are driven by complex, error-prone command line interfaces. StorMagic SvKMS has a flexible and robust REST API, allowing organizations to automate key management functions and create streamlined workflows.

Licensing and pricing

SvKMS is licensed on a per-node basis, with a Master Node license required, and subsequent Additional Node licenses depending on the size of the cluster. The base license grants the organization the use of up to 250 keys within the cluster, at no additional cost. If more than 250 keys are required for the cluster, these are charged individually per key.

A support contract of a minimum of 1 year must also be purchased with each SvKMS license. Customers can choose either Gold or Platinum levels of support over 1, 3 or 5 year terms. More information on these levels can be found in the Support section of this data sheet. Master Nodes and Additional Nodes must have the same level of support - the support levels cannot be mixed.

The SvKMS licenses are perpetual - they require just a single one-time payment and have full enterprise functionality included. The only ongoing payment that the customer must consider is the support contract, which must be renewed to retain functionality, support, patches and bug fixes.

A free, fully functional evaluation of SvKMS is available to download, enabling organizations to trial and experience the features and benefits of SvKMS, before purchasing.

For more information and to download an evaluation copy, visit: **stormagic.com/trial**

SYSTEM REQUIREMENTS

StorMagic SvKMS has the following minimum hardware requirements:

CPU	Intel quad core or higher
Memory	6GB RAM [1]
Disk	20GB HDD [2]

[1] 6GB RAM minimum requirement. For optimal performance, 16GB RAM recommended.

[2] 20GB HDD minimum requirement. For optimal performance, 40GB HDD recommended.

HARDWARE AND SOFTWARE COMPATIBILITY

StorMagic SvKMS is compatible with any x86 server, providing it meets the minimum requirements listed above. Furthermore, it can be run in any cloud and on any hypervisor, and has numerous integrations with other software solutions. Further details of these can be found in the tables below.

Cloud Platform Compatibility

Four major cloud providers - Amazon, Microsoft, Google and OpenStack - are supported by SvKMS and the solution can be deployed across one, or multiple providers, as required.

Cloud Platform	SvKMS version
	2.3
Google Cloud	●
Amazon EC2	●
Microsoft Azure	●
OpenStack **- Version 15 (Train)**	●

Hypervisor Compatibility

SvKMS supports many different hypervisors, including VMware vSphere, Microsoft Hyper-V, Linux KVM, Nutanix AHV and Oracle VirtualBox.

It is installed as a VM on top of the hypervisor, allowing advanced hypervisor features to be leveraged such as high availability and fault tolerance. The table below outlines SvKMS' compatibility with different hypervisor versions.

Hypervisor		SvKMS Version
		2.3
VMware	vSphere 6.7 & updates	●
	vSphere 6.5 & updates	●
Microsoft	Windows Server 2016	●
	Hyper-V Server 2016	●
Linux KVM	CentOS 8.0	●
	CentOS 7.6	●
	RHEL 8.0	●
	RHEL 7.6	●
	Ubuntu 18.04 LTS	●
Oracle	VirtualBox 6.1	●
	VirtualBox 6.0	●
	VirtualBox 5.2	●
Nutanix	AHV 5.10	●

Additional Integrations

There are a number of additional storage and database integrations for SvKMS that allow it to simplify the key management of an organization's infrastructure. These are generally achieved through the use of KMIP. The integrations are listed below:

Integration	Explanation
VMware vSAN	Enables vSphere hypervisor encryption features to be used, via KMIP integration
Nutanix	Enables the use of self encrypting drives (SEDs), via KMIP integration
IBM DB2	SvKMS can create a centralized key store when using DB2 native encryption
MongoDB	Enables data-at-rest encryption through storage-based symmetric key encryption, via KMIP
NetApp ONTAP	SvKMS can act as a key management server for volume encryption, via KMIP
Veritas	SvKMS can act as the key management server for Veritas Netbackup encryption, via KMIP

Further details on these integrations and how they can be implemented can be found within the SvKMS Manual.

	GOLD SUPPORT	PLATINUM SUPPORT
Hours of operation	8 hours a day[1] (Mon – Fri)	24 hours a day[2] (7 days a week)
Length of service	1, 3 or 5 years	1, 3 or 5 years
Product updates	Yes	Yes
Product upgrades	Yes	Yes
Access method	Email	Email + Telephone
Response method	Email + Telephone	Email + Telephone
Remote support / WebEx	Yes	Yes
Maximum number of support administrators per contract	2	4

[1] Gold Support is only available within the timezones of UTC -08:00 to UTC +02:00. If you fall outside of this range, you must purchase Platinum Support.

[2] Global, 24x7 support for Severity 1 - Critical Down issues

SvKMS MAINTENANCE AND SUPPORT

SvKMS Maintenance & Support provides organizations with access to StorMagic support resources, including product updates, knowledgebase access and email support with our technical support staff.

Two levels are available. A summary of each is shown in the table above.

StorMagic
Unit 4, Eastgate
Office Centre
Eastgate Road
Bristol
BS5 6XX
United Kingdom

+44 (0) 117 952 7396
sales@stormagic.com

www.stormagic.com

SvKMS FEATURES	SvKMS 2.3
REST API - web page with more information • Applications can connect, interact and integrate directly with SvKMS • A common interface for key management operations (get, fetch, rotate, etc) • Build automation workflows and integrate with use cases limited by previous standards like PKCS#11	●
BYOK/CSEK - web page with more information • Encrypt data and retain control and management of encryption keys even in the cloud • Generate strong keys and control secure export of keys to the cloud, strengthening key management practices • Separate the lock (encryption) from the key (encryption key)	●
CONFORMS TO KMIP SERVER SPECIFICATIONS - web page with more information • Only one key management service is necessary to facilitate all key encryption requirements • Deploy as a KMIP server in a virtual environment in minutes, for a fraction of the cost and effort of an HSM • Reduce overheads/administration related to managing encrypted data, such as tape drives, databases, storage array and software, through centralized management	●
CLUSTER MANAGEMENT AND HIGH AVAILABILITY (HA) • Easily activate a new key management installation • Simple KMS setup for both a single instance and a complex HA cluster • Supports both two and 2N+1 configurations	●
FULL KEY MANAGEMENT LIFECYCLE • Ensure compliance and enact robust key policies	●
ROBUST KEY MANAGEMENT OPERATIONS • Ensure key management requests are restricted to specific IP addresses so only authorized personnel and systems can access keys • Automate rotations to improve security and meet policy guidelines, as well as reduce administrative overhead • Perform key management functions (create, delete, rotate etc.) in bulk to increase efficiency	●
PAINLESS BACKUP AND RESTORE • Saves and stores the current SvKMS state for future restoration • Set on-demand and scheduled backups to an external location, restoring them when required	●
HYBRID ON-PREMISE/CLOUD CONFIGURATION • Generate, store and provision keys on-premise, in the datacenter and/or in private, public or multi-clouds	●
PROACTIVE INSIGHTS (MANAGE NOTIFICATIONS AND ALERTS) • Audits all activity related to key data that can include anything from key creation, to rotation and compromise • Provides alerts on activity in a cryptographic system that requires further investigation in order to detect and prevent breaches or other issues	●
ROLE-BASED ACCESS CONTROL (RBAC) • Allows the administrator to segment and control access to encrypted systems • Allows groups to handle who may access a key. For example, a group for databases may allow certain key users access to unencrypt certain data but may exclude other key users within the storage group	●
CUSTOM KEY IMPORT AND HSM EXTENSION - web page with more information • Manage old key types and secrets - such as PGP, DES, CAST and Blowfish - from one centralized key manager • Consolidate key management into a single pane of glass, while extending the life of in-house hardware security modules (HSMs) • Can serve as an abstraction in front of an HSM, provisioning keys out through the key manager which can then perform many key management lifecycle functions	●
SOPHISTICATED, SINGLE USER INTERFACE (UI) • Simplifies the encryption process through an easy-to-use and modern UI • Provides both a UI and API to manage many key management functions and use cases, all from one interface	●
DETAILED AUDITING AND LOGGING, EXPORTABLE TO POPULAR SIEMs • Analyze and report on key management activities to uncover potential threats • Collects data through the use of the syslog format, which can then be exported to external SIEM tools	●
FIPS 140-2 LEVEL 1 COMPLIANCE • Meets the highest levels of NIST compliance for a key management software product.	●
ADVANCED IDENTITY AND ACCESS CONTROL • Supports certificate authority functions including signing, revocation, time and date • Supports version 2 of the Security Assertion Markup Language (SAML) standard • Integrates with any SAML-standard identity providers including ADFS and OKTA	●