StorMagic

FICHA TÉCNICA

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2021

StorMagic SvKMS

GESTIÓN DE CLAVES DE CIFRADO

STORMAGIC SvKMS

StorMagic SVKMS es una solución de gestión de claves de cifrado que se puede implementar en cualquier entorno. Simplifica la seguridad compleja y la infraestructura de gestión de claves al ofrecer administración centralizada y, como se ilustra en la fig. 1, la capacidad de implementar un KMS donde sea necesario. Esto lo hace perfecto no solamente para el centro de datos, sino también para los entornos de nube y de edge computing.

Ya sea localmente, en la nube o en varias nubes, SvKMS ofrece a las organizaciones la flexibilidad de ubicar sus recursos de gestión de claves donde son necesarios. Elimina la necesidad de módulos de seguridad de hardware (HSM) y utiliza una REST API para integraciones sencillas en cualquier flujo de trabajo con importaciones de claves a la medida que facilitan la transición desde soluciones heredadas.

StorMagic SvKMS cuenta con la certificación FIPS 140-2, lo que permite la identificación avanzada y la gestión de acceso a través de SAML 2.0, y se puede configurar como una solución única o multi-tenant, lo que la convierte en una opción ideal para los proveedores de soluciones de seguridad administrada.

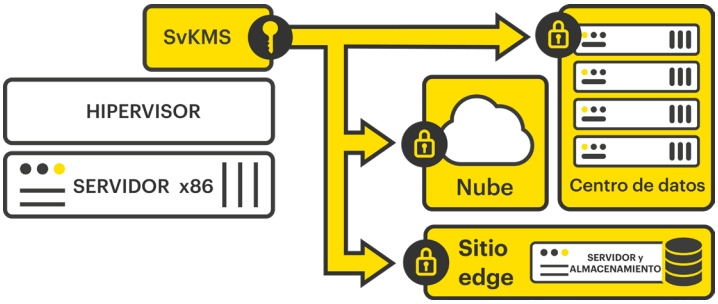

Fig. 1: Una implementación típica de SvKMS que proporciona claves de forma remota a cualquier entorno o flujo de trabajo.

Esta ficha técnica se divide en cuatro secciones, las cuales cubre las características de SvKMS, sus requisitos, compatibilidad de hardware y software, y finalmente los niveles de soporte.

CARACTERÍSTICAS DE SvKMS

StorMagic SvKMS incluye un conjunto completo de características que permiten controlar todo el ciclo de vida de la gestión de claves. Todas estas características se detallan en la tabla al final de este documento.

KMIP

SvKMS se ha creado para maximizar el estándar abierto KMIP a fin de permitir que las organizaciones lo aprovechen como parte de sus operaciones de gestión de claves. Con SvKMS, usted puede gestionar, almacenar y consolidar de forma centralizada las tareas de gestión de claves de cifrado en la nube, SaaS, sistemas locales y dispositivos endpoint, como móviles y de IoT.

BYOK/CSEK

Bring Your Own Key (BYOK), o Customer Supplied Encryption Keys (CSEK), garantiza que las claves de cifrado permanezcan en manos del negocio, independientemente de su ubicación. Esto le da a los usuarios empresariales el control de los datos que se mantienen fuera de las instalaciones: si el propietario del contenido deshabilita el acceso a las claves, se vuelve imposible que la información sea descifrada por terceros.

Importación de claves a la medida

Con el tiempo, una organización puede tener de cientos a millones de claves que se utilizan dentro de un entorno criptográfico complejo. La función de importación de claves a la medida de SvKMS permite a los usuarios importar claves que pudieron haber sido creadas por otro administrador de claves en un formato común, o a través de un algoritmo, incluidos PGP, GPG, DES, CAST y Blowfish.

Integración y automatización de REST API

Abordar manualmente todas las funciones de gestión de claves al nivel de aplicaciones requiere mucho tiempo y es ineficiente, y los administradores de claves de la vieja escuela se rigen por interfaces complejas de línea de comandos que son propensas a errores. StorMagic SvKMS tiene una REST API flexible y robusta que permite a las organizaciones automatizar las funciones de gestión de claves y crear flujos de trabajo optimizados.

Licenciamiento y precios
SvKMS está disponible en tres niveles, conocidos como 'Ediciones': Essentials, Professional y Enterprise. Cada edición determina el tipo de caso de uso y la escala de la solución de gestión de claves requerida. Dependiendo de la Edición, SvKM se puede implementar como una local o como un servicio de suscripción basado en la nube le conoce como Key Management-as-a-Service (KMaaS). Los detalles de las características incluidas en cada SvKMS Edition se explican en la tabla de características al final de la ficha técnica. Puede consultar más información sobre el licenciamiento y los precios de SvKMS en la **página web de SvKMS Pricing.**

Todas las suscripciones a StorMagic SvKMS incluyen nuestro **servicio Platinum Enterprise Support**, que proporciona mantenimiento y asistencia 24 horas al día, 7 días a la semana.

Una evaluación gratuita y completamente funcional de SvKMS está disponible para descargarse, lo que permite a las organizaciones probar y experimentar las características y beneficios de SvKMS antes de adquirirlo.

Para obtener más información y descargar una copia de evaluación, visite **stormagic.com/trial**.

REQUISITOS DEL SISTEMA

StorMagic SvKMS es compatible con cualquier servidor x86, siempre que cumpla con los requisitos mínimos que se enumeran a continuación. StorMagic SvKMS tiene los siguientes requisitos mínimos de hardware:

CPU	4x vCPUs
Memoria	8GB RAM [1]
Disco	20GB HDD [2]

[1] Se requiere mínimo 8GB de RAM, se recomiendan 16GB para entornos grandes.

[2] Requisito mínimo HDD de 20GB. Para un rendimiento óptimo, se recomienda un disco duro de 40GB.

REQUISITOS DEL SOFTWARE

StorMagic SvKMS se pueden ejecutar en cualquier nube y en cualquier hipervisor, y tiene numerosas integraciones con otras soluciones de software. Se pueden encontrar más detalles sobre estas en las siguientes tablas.

Compatibilidad con Plataformas de Nube
Cuatro de los principales proveedores de nube, Amazon, Microsoft, Google y OpenStack, son compatibles con SvKMS y la solución se puede implementar en uno o varios proveedores, según sea necesario.

Plataforma de Nube	Versión de SvKMS		
	2.4	2.5	2.6
Google Cloud	●	●	●
Amazon Web Services	●	●	●
Microsoft Azure	●	●	●
OpenStack - Versión 15 (Train)	●	●	●

Compatibilidad con Hipervisores
SvKMS soporta a muchos hipervisores diferentes, incluidos VMware vSphere, Microsoft Hyper-V, Linux KVM, Nutanix AHV y Oracle VirtualBox. Se instala como una VM sobre el hipervisor, lo que permite aprovechar las características avanzadas del hipervisor, como la alta disponibilidad y tolerancia a fallas. La siguiente tabla describe la compatibilidad de SvKMS con diferentes versiones de hipervisores.

Hipervisor		Versión de SvKMS		
		2.4	2.5	2.6
VMware	vSphere 7.0 y actualizaciones			●
	vSphere 6.7 y actualizaciones	●	●	●
	vSphere 6.5 y actualizaciones	●	●	●
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	●	●	●

INTEGRACIONES Y CARGAS DE TRABAJO SOPORTADAS

Una vez que se ha implementado SvKMS, se puede conectar e integrar en muchos servicios y cargas de trabajo diferentes. La siguiente tabla enumera las integraciones disponibles y documentadas actuales; sin embargo, gracias a la REST API incluida dentro de SvKMS, también puede integrarse fácilmente con aplicaciones propietarias dentro de una organización. Al incorporar todas estas cargas de trabajo a un administrador de claves centralizado, la operación de gestión de claves se simplifica drásticamente y es mucho más segura.

Integración	Explicación	Versión de SvKMS		
		2.4	2.5	2.6
AWS EC2 y S3	Soporte para la gestión de claves externas usando BYOK	●	●	●
Azure Key Vault Managed HSM	SvKMS se puede utilizar como interfaz entre Key Vault y el HSM de terceros		●	●
Azure Storage	Soporte para la gestión de claves externas usando BYOK	●	●	●
BitLocker	Utilice SvKMS para brindar protección externa y segura a las claves AES para el cifrado y descifrado de unidades de Windows		●	●
Commvault	SvKMS es un administrador de claves certificado por Commvault y utiliza KMIP para proteger las claves de cifrado del software de Commvault almacenadas en una base de datos CommServe.	●	●	●
Google Cloud EKM	Utilice SvKMS como administrador de claves externas para proteger los datos en Google Cloud, lo que proporciona un mayor control que BYOK		●	●
IBM DB2	SvKMS puede crear un almacén de claves centralizado cuando se utiliza el cifrado nativo DB2	●	●	●
IBM Informix	Utilice KMIP para la gestión de claves de terceros para cifrar el espacio de almacenamiento (dbspaces, blobspaces y blobspaces inteligentes)			●
MariaDB	SvKMS actúa como un almacén de claves centralizado para el cifrado nativo de MariaDB, a través de la REST API	●	●	●
MongoDB	Permite el cifrado de datos en reposo a través delo cifrado de claves simétricas basado en almacenamiento, a través de KMIP	●	●	●
MySQL	Utilice SvKMS como almacén centralizado de claves para el cifrado de MySQL, a través de KMIP	●	●	●
NetApp ONTAP	SvKMS puede actuar como un servidor de gestión de claves para el cifrado de volúmenes, a través de KMIP	●	●	●
Nutanix Prism	Permite el uso de unidades de autocifrado (SEDs), a través de la integración de KMIP	●	●	●
Salesforce Shield	Proteja los datos cifrados de Salesforce mediante el uso de SvKMS como administrador de claves con BYOK		●	●
Veritas NetBackup	SvKMS puede actuar como el servidor de gestión de claves para el cifrado de Veritas NetBackup, a través de KMIP	●	●	●
VMware vSphere y vSAN	Habilita el cifrado de vSphere VM mediante la integración de KMIP	●	●	●

Para obtener información más detallada sobre cada una de estas integraciones, junto con muchas otras, visite la **página de integraciones de SvKMS** del sitio web de StorMagic. Se detalla la integración de cada solución, con guías de integración disponibles para cada una, las cuales pueden descargarse.

Proveedor	Modelo	Versión de SvKMS		
		2.4	2.5	2.6
Utimaco	CryptoServer CP5	●	●	●
Entrust	nShield Connect 5000+	●	●	●
	nShield Connect 6000+			●
Thales	Luna 7.0		●	●

Integraciones con HSM

SvKMS también se integra con muchos proveedores líderes de HSM para brindar gestión centralizada y capacidades avanzadas de gestión de claves a estas soluciones de hardware que generalmente son favorecidas por las organizaciones por su confiabilidad y capacidad para proporcionar una raíz de confianza. Para consultar más información sobre cómo SVKMS se integra con HSM, visite la **página de extensiones HSM** del sitio web de StorMagic.

StorMagic
The Quadrant
2430/2440
Aztec West
Almondsbury
Bristol
BS32 4AQ
United Kingdom

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

www.stormagic.com

CARACTERÍSTICAS DE SvKMS

	ENTERPRISE	PROFESSIONAL	ESSENTIALS
REST API - página web con más información • Permite que otras aplicaciones se conecten, interactúen y se integren directamente con SvKMS • Define una interfaz común para las operaciones de gestión de claves (obtener, recuperar, rotar, crear, eliminar, etc.) • Cree flujos de trabajo de automatización e intégrelos con muchos casos de uso limitados con estándares anteriores como PKCS #11	●	●	
CASOS DE USO	Ilimitados	5	1
CLAVES DE CIFRADO ILIMITADAS	●	Hasta 250	Hasta 50
BYOK/CSEK - página web con más información • Cifre sus datos y mantenga el control y la gestión de las claves de cifrado incluso en entornos de cómputo en la nube • Genere claves robustas y controle la exportación segura de claves a la nube, fortaleciendo así las prácticas de gestión de claves • Separe el candado (cifrado) de la llave (clave de cifrado)	●	●	
SERVIDOR KMIP - página web con más información • Una solución rentable donde solo se necesita un servicio de gestión de claves para facilitar todos los requisitos de cifrado de las claves • SvKMS se puede implementar como un Servidor KMIP en un entorno virtual en minutos, por una fracción del costo y esfuerzo de un HSM • Reduce los gastos generales y la gestión relacionados con la administración de datos cifrados, como unidades de cinta, bases de datos, arreglos de almacenamiento de información y software, a través de la gestión centralizada	●	●	
GESTIÓN DE CLÚSTERS Y ALTA DISPONIBILIDAD • Active fácilmente una nueva instalación de la gestión de claves • Configuración sencilla de KMS tanto para una sola instancia como para un clúster complejo de alta disponibilidad	●	●	●
CICLO DE VIDA COMPLETO DE LA GESTIÓN DE CLAVES • Garantice el cumplimiento y establezca políticas de claves sólidas durante todo el ciclo de vida de las claves, desde la creación y el almacenamiento, hasta el archivado y la eliminación	●	●	●
OPERACIONES ROBUSTAS DE LA GESTIÓN DE CLAVES	●	●	●
RESPALDO Y RECUPERACIÓN SIN DOLOR • Guarda y almacena el estado actual de SvKMS para futuras recuperaciones • Realice respaldos bajo demanda y programados en una ubicación externa, recuperando estas copias de seguridad cuando sea necesario	●	●	●
CONFIGURACIÓN HÍBRIDA LOCAL/NUBE • Genere, almacene y aprovisione claves en el sitio/localmente, en el centro de datos y/o en las nubes privadas, públicas o híbridas	N/A	N/A	N/A
INSIGHTS PROACTIVOS (GESTIONE NOTIFICACIONES Y ALERTAS) • Audita toda la actividad relacionada con datos de las claves que pueden incluir desde la creación de claves, hasta la rotación y el compromiso • Emite alertas sobre la actividad en un sistema criptográfico que requiere más investigación para detectar y prevenir brechas u otros problemas	●	●	●
CONTROL DE ACCESO BASADO EN ROLES (RBAC) • Permite al administrador segmentar y controlar de manera efectiva quién tiene acceso a varios sistemas cifrados • Permite a los grupos manejar quién puede acceder a una clave. Por ejemplo, un grupo para bases de datos puede permitir el acceso de usuarios específicos para descifrar ciertos datos, pero puede excluir a otros usuarios dentro del grupo de almacenamiento	●	●	●
EXTENSION DE HSM - página web con más información • Soporta la especificación PKCS #11, lo que permite la integración con HSMs • Consolida la gestión de claves en un solo panel, a la vez que extiende la vida útil de los HSMs internos • Puede servir como una abstracción frente a un HSM, aprovisionando claves a través del administrador de claves que luego puede realizar varias funciones del ciclo de vida de la gestión de claves	●		
PROTECCIÓN TPM	●		
IMPORTACIÓN DE CLAVE A LA MEDIDA - página web con más información • Administre los antiguos tipos de claves y secretos, como PGP, DES, CAST y Blowfish, desde el mismo administrador de claves centralizado	●	●	
SOFISTICADA INTERFAZ DE USUARIO ÚNICO (UI) • Un administrador de claves soporta muchos casos de uso de la gestión de claves diferentes, todo desde una interfaz, lo que reduce el tiempo y los costos	●	●	●
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	●	●	●
CUMPLIMIENTO DE FIPS 140-2 NIVEL 1 • Cumple con los más altos niveles de cumplimiento de NIST para un producto de software de gestión de claves	●	●	●
AUTENTIFICACIÓN ÚNICA	●	●	