StorMagic

DATENBLATT

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2021

StorMagic SvKMS

ENCRYPTION KEY MANAGEMENT

STORMAGIC SvKMS

StorMagic SvKMS ist eine Lösung für Encryption und Key Management, die in jeder Umgebung eingesetzt werden kann. Es vereinfacht die komplexe Sicherheits- und Schlüsselverwaltungsinfrastruktur durch eine zentralisierte Verwaltung und, wie in Abb. 1, bietet die Fähigkeit, ein KMS überall dort einzusetzen, wo es benötigt wird. Damit eignet es sich nicht nur perfekt für das Rechenzentrum, sondern auch für Cloud- und Edge-Computing-Umgebungen.

Ob vor Ort, in der Cloud oder per Multi-Cloud, SvKMS bietet Unternehmen die Flexibilität, ihre wichtigsten Managementressourcen dort zu platzieren, wo sie benötigt werden. Es macht die Notwendigkeit von Hardware-Sicherheitsmodulen (HSMs) überflüssig und verwendet eine REST-API für die einfache Integration in jeden Arbeitsablauf, wobei der Import von benutzerdefinierten Schlüsseln einen einfachen Übergang von Legacy-Lösungen erleichtert.

StorMagic SvKMS ist FIPS 140-2-zertifiziert, ermöglicht die erweiterte Identifizierung und Zugriffsverwaltung durch SAML 2.0 und kann als Einzel- oder Multi-Tenant-lösung konfiguriert werden. Damit ist sie die ideale Wahl für Anbieter von verwalteten Sicherheitslösungen.

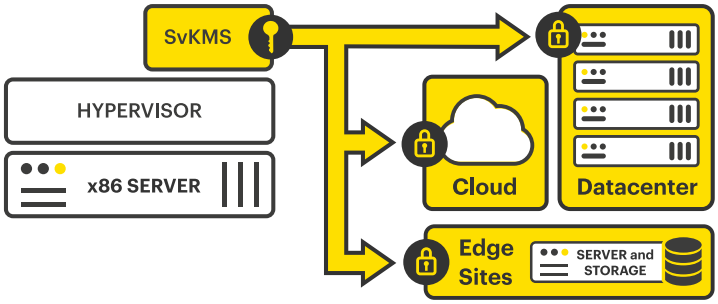

Abb. 1: Eine typische SvKMS-Bereitstellung, bei der Schlüssel remote in einer beliebigen Umgebung oder einem beliebigen Workflow bereitgestellt werden. Dieses Datenblatt ist in vier Abschnitte unterteilt, die die Funktionen von SvKMS, die Anforderungen, die Hardware- und Softwarekompatibilität und schließlich die Supportstufen behandeln.

SvKM-FUNKTIONEN

StorMagic SvKMS enthält eine umfassende Reihe von Funktionen, die die Kontrolle über den gesamten Lebenszyklus der Schlüsselverwaltung ermöglichen. Alle diese Funktionen sind in der Tabelle am Ende dieses Dokuments im Einzelnen aufgeführt.

KMIP

SvKMS wurde um die Maximierung des offenen KMIP-Standards herum aufgebaut, um es Organisationen zu ermöglichen, es als Teil ihrer wichtigsten Managementoperationen zu nutzen. Mit SvKMS können Sie zentral die Verwaltung, Speicherung und Konsolidierung von Aufgaben zur Verwaltung von Encryption Keys über Cloud, SaaS, Systeme vor Ort und Endgeräte wie mobile und IoT-Geräte hinweg durchführen.

BYOK/CSEK

Bring Your Own Key (BYOK) oder vom Kunden bereitgestellte Encryption Keys (CSEK), um sicherzustellen, dass die Encryption Keys unabhängig vom Standort in den Händen des Unternehmens bleiben. Dies gibt Geschäftsanwendern die Kontrolle über Daten, die außerhalb der Geschäftsräume aufbewahrt werden - wenn der Eigentümer des Inhalts den Zugriff auf die Schlüssel deaktiviert, ist es unmöglich, dass die Informationen von Dritten entschlüsselt werden können. Benutzerdefinierter Schlüssel-Import

Custom key import

Im Laufe der Zeit kann eine Organisation Hunderte bis Millionen von Schlüsseln haben, die in einer komplexen kryptographischen Umgebung verwendet werden. Die benutzerdefinierte Schlüssel-Importfunktion von SvKMS ermöglicht es Benutzern, Schlüssel zu importieren, die möglicherweise von einem anderen Schlüsselverwalter in einem gemeinsamen Format erstellt wurden, oder durch einen benutzerdefinierten Algorithmus – einschließlich PGP, GPG, DES, CAST und Blowfish.

REST-API-Integration und -Automation

Die manuelle Verwaltung aller Funktionen des Schlüsselmanagements auf der Anwendungsebene ist zeitaufwendig und ineffizient, und Schlüsselverwaltungen im alten Stil benötigen komplexe Befehlsschnittstellen, die

allerdings auch sehr fehleranfällig sind. StorMagic SvKMS bietet eine flexible und robuste REST API, mit deren Hilfe Unternehmen die Funktionen der Schlüsselverwaltung automatisieren und die Betriebsabläufe optimieren können.

Lizenzierung und Preisgestaltung
SvKMS ist in drei Stufen erhältlich, die als "Editionen" bezeichnet werden - Essentials, Professional und Enterprise. Jede Edition bestimmt die Art des Anwendungsfalls und den Umfang der Schlüssel Management-Lösung. Abhängig der Edition kann SvKMS entweder als eine vor Ort oder als Cloud-basierter Abonnement-Service bekannt als Key Management-asa-Service (KMaaS). Details zu den Funktionen, die in jeder jeder SvKMS-Edition enthalten sind, finden Sie in der Tabelle am Ende des Datenblatts. Weitere Informationen wie SvKMS lizenziert und bepreist wird, finden Sie finden Sie auf der **SvKMS-Preisseite**.

Alle StorMagic SvKMS-Abonnements beinhalten unseren **Platinum Enterprise Support Service**, der 24 Stunden am Tag, 7 Tage die Woche Wartung und Support bietet

Eine kostenlose, voll funktionsfähige Testversion von SvKMS kann heruntergeladen werden, so dass Unternehmen die Funktionen und Vorteile von SvKMS vor dem Kauf testen und ausprobieren können.

Für weitere Informationen und zum Herunterladen eines Testexemplars, besuchen Sie bitte **stormagic.com/trial**

SYSTEMANFORDERUNGEN

StorMagic SvKMS hat die folgenden Hardware-Mindestanforderungen:

CPU	4x vCPUs
Arbeitsspeicher	8 GB ARBEITSSPEICHER [1]
Festplatte	20GB HDD [2]

[1] Mindestens 8 GB RAM erforderlich, 16 GB empfohlen für große Umgebungen.
[2] 20 GB HDD Mindestanforderung. Für optimale Leistung wird eine 40-GB-HDD empfohlen.

HARDWARE- UND SOFTWARE-KOMPATIBILITÄT

StorMagic SvKMS ist mit jedem x86-Server kompatibel, vorausgesetzt, er erfüllt die Mindestanforderungen, wie oben ausgeführt. Darüber hinaus kann es in jeder Cloud und auf jedem Hypervisor ausgeführt werden und verfügt über zahlreiche Integrationen mit anderen Software-lösungen. Weitere Einzelheiten dazu finden Sie in den nachstehenden Tabellen.

Kompatibilität mit der Cloud-Plattform
Vier große Cloud-Anbieter – Amazon, Microsoft, Google und OpenStack – werden von SvKMS unterstützt, und die Lösung kann je nach Bedarf bei einem oder mehreren Anbietern eingesetzt werden.

Cloud-Plattform	SvKMS-Version		
	2.4	2.5	2.6
Google-Cloud	●	●	●
Amazon Web Services	●	●	●
Microsoft Azure	●	●	●
OpenStack - Version 15 (Train)	●	●	●

Hypervisor-Kompatibilität
SvKMS unterstützt viele verschiedene Hypervisoren, einschließlich VMware vSphere, Microsoft Hyper-V, Linux KVM, Nutanix AHV und Oracle VirtualBox. Es wird als VM auf dem Hypervisor installiert, wodurch erweiterte Hypervisor-Funktionen wie Hochverfügbarkeit und Fehlertoleranz genutzt werden können. Die nachstehende Tabelle gibt einen Überblick über die Kompatibilität von SvKMS mit verschiedenen Hypervisor-Versionen.

Hypervisor		SvKMS-Version		
		2.4	2.5	2.6
VMware	vSphere 7.0 & Aktualisierungen			●
	vSphere 6.7 & Aktualisierungen	●	●	●
	vSphere 6.5 & Aktualisierungen	●	●	●
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	●	●	●

ZUSÄTZLICHE INTEGRATIONEN

Es gibt eine Reihe von zusätzlichen Speicher- und Datenbankintegrationen für SvKMS, die es ermöglichen, die Schlüsselverwaltung der Infrastruktur eines Unternehmens zu vereinfachen. Dies wird im Allgemeinen durch den Einsatz von KMIP erreicht. Die Integrationen sind unten aufgeführt:

Weitere Einzelheiten zu diesen Integrationen und wie diese umgesetzt werden können, finden Sie im **SvKMS-Handbuch**.

Integration	Explanation	SvKMS Version		
		2.4	2.5	2.6
AWS EC2 und S3	Unterstützung für externe Schlüsselverwaltung mit BYOK	●	●	●
Azure Key Vault Managed HSM	SvKMS kann als Schnittstelle zwischen Key Vault und HSMs von Drittanbietern verwendet werden		●	●
Azure Storage	Unterstützung für externe Schlüsselverwaltung mit BYOK	●	●	●
BitLocker	Verwenden Sie SvKMS, um einen externen, sicheren AES-Schlüssel für die Ver- und Entschlüsselung von Windows-Laufwerken bereitzustellen		●	●
Commvault	Mit KMIP schützt SvKMS die Verschlüsselungscodes der Commvault-Software, die in einer CommServe-Datenbank gespeichert sind	●	●	●
Google Cloud EKM	Verwenden Sie SvKMS als externen Schlüsselmanager, um Daten in der Google Cloud zu schützen, was eine größere Kontrolle als BYOK ermöglicht		●	●
IBM DB2	SvKMS kann einen zentralisierten Schlüssel-Store erstellen, wenn native DB2-Verschlüsselung verwendet wird	●	●	●
IBM Informix	Verwenden Sie KMIP für die Schlüsselverwaltung von Drittanbietern für die Speicherplatzverschlüsselung (dbspaces, blobspaces und smart blobspaces)			●
MariaDB	SvKMS fungiert als zentraler Schlüsselspeicher für die native MariaDB-Verschlüsselung über die REST-API	●	●	●
MongoDB	Ermöglicht Data-at-Rest-Verschlüsselung durch speicherbasierte symmetrische Verschlüsselungscodes über KMIP	●	●	●
MySQL	Verwendung von SvKMS als zentraler Schlüsselspeicher für MySQL-Verschlüsselung, über KMIP	●	●	●
NetApp ONTAP	SvKMS kann über KMIP als Schlüsselverwaltungsserver zur Volumenverschlüsselung eingesetzt werden	●	●	●
Nutanix Prism	Ermöglicht die Verwendung selbstverschlüsselnder Laufwerke (SED) über die KMIP-Integration	●	●	●
Salesforce Shield	Schützen Sie verschlüsselte Salesforce-Daten durch Verwendung von SvKMS als Schlüsselmanager mit BYOK		●	●
Veritas NetBackup	SvKMS kann über KMIP als Schlüsselverwaltungsserver für die Verschlüsselung von Veritas Netbackup eingesetzt werden	●	●	●
VMware vSphere und vSAN	Ermöglicht die vSphere VM-Verschlüsselung über die KMIP-Integration	●	●	●

Anbieter	Modell	SvKMS-Version		
		2.4	2.5	2.6
Utimaco	CryptoServer CP5	●	●	●
Entrust	nShield Connect 5000+	●	●	●
	nShield Connect 6000+			●
Thales	Luna 7.0		●	●

HSM-Integrationen
SvKMS lässt sich auch mit vielen führenden HSM-Anbietern integrieren, um eine zentralisierte Verwaltung und erweiterte Schlüsselverwaltungsfunktionen für diese Hardware-Lösungen bereitzustellen, die in der Regel von Unternehmen wegen ihrer Zuverlässigkeit und Fähigkeit, Root-of-Trust zu bieten, bevorzugt werden. Weitere Informationen über die Integration von SvKMS mit HSMs finden Sie auf der **HSM-Erweiterungsseite** der StorMagic-Website.

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

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

www.stormagic.com

SvKMS-FUNKTIONEN

	ENTERPRISE	PROFESSIONAL	ESSENTIALS
REST-API - webseite mit weiteren Info • Anwendungen können sich direkt mit SvKMS verbinden, damit interagieren und integrieren • Eine gemeinsame Schnittstelle für Schlüsselverwaltungsoperationen (abrufen, holen, rotieren usw.) • Erstellung von Automatisierungs-Workflows und Integration mit Anwendungsfällen, die durch frühere Standards wie PKCS#11 eingeschränkt sind	●	●	
ANWENDUNGSFÄLLE	Unlimited	5	1
UNBEGRENZTE ENCRYPTION KEYS	●	Up to 250	Up to 50
BYOK/CSEK - webseite mit weiteren Info • Verschlüsseln Sie Daten und behalten Sie sogar in der Cloud die Kontrolle und Verwaltung der Kodierungsschlüssel • Generierung starker Schlüssel und Kontrolle des sicheren Exports von Schlüsseln in die Cloud, Stärkung der • Schlüsselverwaltungspraktiken Trennung von Schloss (Verschlüsselung) und Schlüssel (Verschlüsselungscode)	●	●	
KMIP-SERVERS - webseite mit weiteren Info • Nur ein Key Management System ist erforderlich, um alle Anforderungen bezüglich der Encryption Keys zu erfüllen • Einsatz als KMIP-Server in einer virtuellen Umgebung in Minutenschnelle, für einen Bruchteil der Kosten und des Aufwands eines HSM • Reduzieren Sie die Gemeinkosten und den Verwaltungsaufwand im Zusammenhang mit der Verwaltung verschlüsselter Daten, wie für Bandlaufwerke, Datenbanken, Speicherarrays und Software, durch eine zentralisierte Verwaltung	●	●	
CLUSTER-MANAGEMENT UND HOCHVERFÜGBARKEIT (HA) • Einfaches Aktivieren einer neuen Key Management Installation • Einfache KMS-Einrichtung sowohl für eine einzelne Instanz als auch für einen komplexen HA-Cluster	●	●	●
VOLLSTÄNDIGER LEBENSZYKLUS DER SCHLÜSSELVERWALTUNG • Sicherstellung der Compliance und Umsetzung robuster Schlüsselrichtlinien über den gesamten Lebenszyklus von Schlüsseln, von der Erstellung über Speicherung, Archivierung und Löschung	●	●	●
ROBUSTE SCHLÜSSELVERWALTUNGSOPERATIONEN	●	●	●
EINFACHE SICHERUNG UND WIEDERHERSTELLUNG • Sichert und speichert den aktuellen SvKMS-Zustand für eine zukünftige Wiederherstellung • Einrichten von Backups auf Anforderung und nach Zeitplan an einem externen Standort, wobei sie bei Bedarf wiederhergestellt werden	●	●	●
HYBRIDE VOR-ORT-/CLOUD-KONFIGURATION • Generierung, Speicherung und Bereitstellung von Schlüsseln vor Ort, im Rechenzentrum und/oder in privaten, öffentlichen oder Multi-Clouds	N/A	N/A	N/A
PROAKTIVE EINBLICKE (VERWALTUNG VON BENACHRICHTIGUNGEN UND WARNUNGEN) • Überprüft alle Aktivitäten im Zusammenhang mit Schlüsseldaten, die alles von der Schlüsselherstellung bis hin zu Rotation und Gefährdung umfassen können • Gibt Warnmeldungen über Aktivitäten in einem kryptographischen System aus, die weitere Untersuchungen erfordern, um Verstöße oder andere Probleme zu erkennen und zu verhindern	●	●	●
ROLLENBASIERTE ZUGRIFFSKONTROLLE (RBAC) • Ermöglicht es dem Administrator, den Zugriff auf verschlüsselte Systeme zu segmentieren und zu kontrollieren • Erlaubt es Gruppen zu bestimmen, wer auf einen Schlüssel zugreifen darf. Beispielsweise kann eine Gruppe für Datenbanken es bestimmten Schlüsselbenutzern gestatten, bestimmte Daten zu entschlüsseln, aber eventuell andere Schlüsselbenutzer in der Gruppe ausschließe	●	●	●

FORTSETZUNG AUF DER NÄCHSTEN SEITE

SvKMS-FUNKTIONEN

	ENTERPRISE	PROFESSIONAL	ESSENTIALS
HSM EXTENSION - webseite mit weiteren Info • Unterstützt die PKCS#11-Spezifikation und ermöglicht die Integration mit HSMs • Konsolidiert die Schlüsselverwaltung in einem einzigen Fenster und verlängert gleichzeitig die Lebensdauer der eigenen HSMs • Kann als Abstraktion vor einem HSM dienen, wobei die Bereitstellung von Schlüsseln durch den Schlüsselmanager erfolgt, der dann viele Schlüsselverwaltungs-Lebenszyklusfunktionen ausführen kann	●		
TPM-SCHUTZ	●		
IMPORT VON BENUTZERDEFINIERTEN KEYS - webseite mit weiteren Info • Verwalten Sie alte Schlüsseltypen und Geheimnisse - wie PGP, DES, CAST und Blowfish - über denselben zentralen Schlüsselmanager	●	●	
EINHEITLICHE BENUTZEROBERFLÄCHE (UI) • Vereinfacht den Verschlüsselungsprozess durch eine benutzerfreundliche und moderne Benutzeroberfläche • Bietet sowohl eine Benutzeroberfläche als auch eine API zur Verwaltung vieler wichtiger Verwaltungsfunktionen und Anwendungsfälle, alles über eine einzige Schnittstelle	●	●	●
DETAILLIERTE PRÜFUNG UND PROTOKOLLIERUNG FÜR BEKANNTE SIEM-SYSTEME • Analyse und Berichte über Aktivitäten des Key Managements zur Aufdeckung potenzieller Bedrohungen • Datenerfassung durch die Verwendung des Syslog-Formats, die dann in externe SI EM-Tools exportiert werden können	●	●	●
FIPS 140-2 EINHALTUNG DER STUFE 1 • Erfüllt die höchsten Stufen der NIST-Konformität für ein Softwareprodukt zur Schlüsselver waltung	●	●	●
SINGLE SIGN ON	●	●	