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.

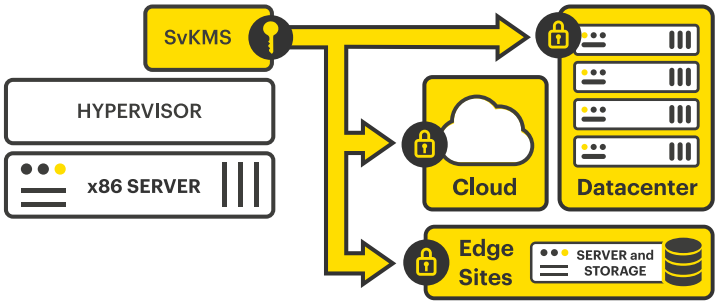

Abb. 1: Eine typische SvKMS-Bereitstellung, bei der Schlüssel remote in einer beliebigen Umgebung oder einem beliebigen Workflow bereitgestellt werden.

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 wird pro Knoten lizenziert, wobei eine Hauptknotenlizenz benötigt wird. Weitere Lizenzen für zusätzliche Knoten hängen von der Größe des Clusters ab. Die Grundlizenz ermöglicht dem Unternehmen die Verwendung von bis zu 250 Schlüssel im Cluster, ohne zusätzliche Kosten. Sind mehr als 250 Schlüssel für den Cluster erforderlich, werden diese einzeln pro Schlüssel in Rechnung gestellt.

Ein Supportvertrag für mindestens 1 Jahr muss ebenfalls gemeinsam mit jeder SvKMS-Lizenz erworben werden. Die Kunden können sich zwischen den Supportstufen Gold oder Platin mit Laufzeiten von 1, 2 oder 5 Jahren entscheiden. Weitere Informationen zu diesen Stufen finden Sie im Abschnitt „Support“ in diesem Datenblatt. Hauptknoten und zusätzliche Knoten müssen dieselben Supportstufen besitzen – die Supportstufen können nicht gemischt werden.

Die SvKMS-Lizenzen sind unbefristet – sie erfordern nur eine einmalige Zahlung und beinhalten die volle Unternehmensfunktionalität. Die einzige laufende Zahlung, die der Kunde in Betracht ziehen muss, ist der Supportvertrag, der erneuert werden muss, damit Funktionalität, Support, Patches und Fehlerbehebungen erhalten bleiben.

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 Softwarelösungen. 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
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
VMware	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.

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

Integration	Explanation	SvKMS Version	
		2.4	2.5
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	●	●
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	●	●

	GOLD-SUPPORT	PLATIN-SUPPORT
Öffnungs-zeiten	8 Stunden pro Tag[1] (Mo - Fr)	24 Stunden am Tag[2] (7 Tage in der Woche)
Dauer des Dienstes	1, 3 oder 5 Jahre	1, 3 oder 5 Jahre
Produkt-Aktualisierungen	Ja	Ja
Produkt-Upgrades	Ja	Ja
Zugriffs-methode	E-Mail	E-Mail + Telefon (über das Platin-Anfragenformular auf support.stormagic.com)
Antwort-methode	E-Mail + WebEx	E-Mail + Telefon + WebEx
Maximale Anzahl von Support-Administratoren pro Vertrag	2	4
Reaktionszeit	4 Stunden	1 Stunde

[1] Der Gold-Support ist nur von 07:00 UTC/DST bis 01:00 UTC/DST verfügbar. Wenn Ihre Geschäftszeiten außerhalb von diesem Zeitfenster liegen, müssen Sie den Platin-Support erwerben
[2] Weltweiter, 24x7-Support für Schweregrad 1 – Kritischer Betriebsausfall & Schweregrad 2 Probleme mit Funktionsverschlechterung

werden. Weitere Informationen über die Integration von SvKMS mit HSMs finden Sie auf der **HSM-Erweiterungsseite** der StorMagic-Website.

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

SvKMS MAINTENANCE AND SUPPORT

SvKMS Wartung & Support bietet Unternehmen Zugang zu StorMagic-Supportressourcen, einschließlich Produkt-Aktualisierungen und dem Zugang zur Wissensdatenbank sowie E-Mail-Support mit unseren Mitarbeitern des technischen Supports. Es stehen zwei Stufen zur Verfügung. Eine Zusammenfassung ist in der obigen Tabelle aufgeführt.

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

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

www.stormagic.com

SVKMS-FUNKTIONEN

	SvKMS 2.5
REST-API - *Webseite mit weiteren Informationen* • 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	●
BYOK/CSEK - *Webseite mit weiteren Informationen* • 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)	●
ENTSPRICHT DEN SPEZIFIKATIONEN DES KMIP-SERVERS - *Webseite mit weiteren Informationen* • 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 verschlüs selter 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 • Unterstützt sowohl Zweier- als auch 2N+1-Konfigurationen	●
VOLLSTÄNDIGER LEBENSZYKLUS DER SCHLÜSSELVERWALTUNG • Gewährleistung der Einhaltung und Verabschiedung robuster Schlüsselrichtlinien	●
ROBUSTE SCHLÜSSELVERWALTUNGSOPERATIONEN • Stellen Sie sicher, dass Anfragen zum Key Management auf bestimmte IP-Adressen beschränkt sind, so dass nur autorisiertes Personal und Systeme auf Schlüssel zugreifen können • Automatisieren von Rotationen zur Verbesserung der Sicherheit und zur Einhaltung von Richtlinien sowie zur Verrin gerung des Verwaltungsaufwands. • Durchführen wichtiger Verwaltungsfunktionen (Erstellen, Löschen, Rotieren usw.) in großen Mengen zur Steigerung der Effizienz	●
SCHMERZLOSE 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 wie derhergestellt werden	●
HYBRIDE VOR-ORT-/CLOUD-KONFIGURATION • Generate, store and provision keys on-premise, in the datacenter and/or in private, public or multi-clouds	●
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 er fordern, 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 Daten banken es bestimmten Schlüsselbenutzern gestatten, bestimmte Daten zu entschlüsseln, aber eventuell andere Schlüsselbenutzer in der Gruppe ausschließe	●
BENUTZERDEFINIERTER SCHLÜSSEL-IMPORT UND HSM-ERWEITERUNG - *Webseite mit weiteren Informationen* • Verwalten alter Schlüsseltypen und Interna – wie PGP, DES, CAST und Blowfish – von einem zentralen Schlüsselmanager aus • Konsolidieren Sie die Schlüsselverwaltung an einer einzigen Stelle und verlängern Sie gleichzeitig die Lebensdauer der hauseigenen Hardware-Sicherheitsmodule (HSMs) • Kann als Abstraktion vor einem HSM dienen, indem es Schlüssel über den Schlüsselmanager bereitstellt, der dann viele Funktionen im Lebenszyklus des Schlüsselmanagements ausführen kann	●
AUSGEREIFTE, 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, AUSFÜHRBAR FÜR BELIEBTE 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 SIEM-Tools exportiert werden können	●
FIPS 140-2 EINHALTUNG DER STUFE 1 • Erfüllt die höchsten Stufen der NIST-Konformität für ein Softwareprodukt zur Schlüsselverwaltung	●
ERWEITERTE IDENTITÄTS- UND ZUGANGSKONTROLLE • Unterstützt Zertifizierungsstellenfunktionen einschließlich Signierung, Widerruf, Zeit und Datum • Unterstützt Version 2 des SAML-Standards (Security Assertion Markup Language) • Integration mit allen SAML-Standardidentitätsanbietern einschließlich ADFS und OKTA	●