aspectra
hosting your future

KEY AND SECRET MANAGEMENT AS A SERVICE

Das Key Management System (KMS) verwaltet zentral die unternehmensweiten IT-Secrets. Auf Secrets muss der Zugriff streng kontrolliert werden: zum Beispiel auf API-Schlüssel, Kennwörter oder Zertifikate. Das KMS gewährleistet kontrollierten Zugang zu den verschlüsselten Daten – durchgehend gesteuert durch Authentifizierungs- und Autorisierungsmethoden. Der Zugriff auf die Secrets via KMS erfolgt per Kommandozeile, HTTP API oder Browseroberfläche. Jeder Zugriff wird dabei aufgezeichnet und bleibt so nachvollziehbar.

aspectras KMS basiert auf dem Produkt HashiCorp Vault Enterprise.
Es stellt die folgenden Kernfunktionen zur Verfügung:

SECURE SECRET STORAGE

Geheimnisse werden verschlüsselt, bevor sie in den permanenten Speicher geschrieben werden. Das verunmöglicht den Zugriff auf Geheimnisse via Dateisystem.

DYNAMIC SECRETS

Zum Beispiel für SQL-Datenbanken oder S3-Buckets. Greift eine Anwendung beispielsweise auf einen S3-Bucket, bittet sie das KMS um Anmeldeinformationen. Das KMS generiert ein Schlüsselpaar mit gültigen Berechtigungen. Nach Ablauf der Nutzungsdauer und nachdem die dynamischen Schlüssel erstellt sind, widerruft das KMS diese automatisch.

DATA ENCYRPTION

Das KMS verschlüsselt und entschlüsselt Daten, ohne sie zu speichern. So können Sicherheitsteams Verschlüsselungsparameter definieren. Entwickler können so verschlüsselte Daten an einem Ort wie einer SQL-Datenbank speichern, ohne eigene Verschlüsselungsmethoden entwickeln zu müssen.

LEASING AND RENEWAL

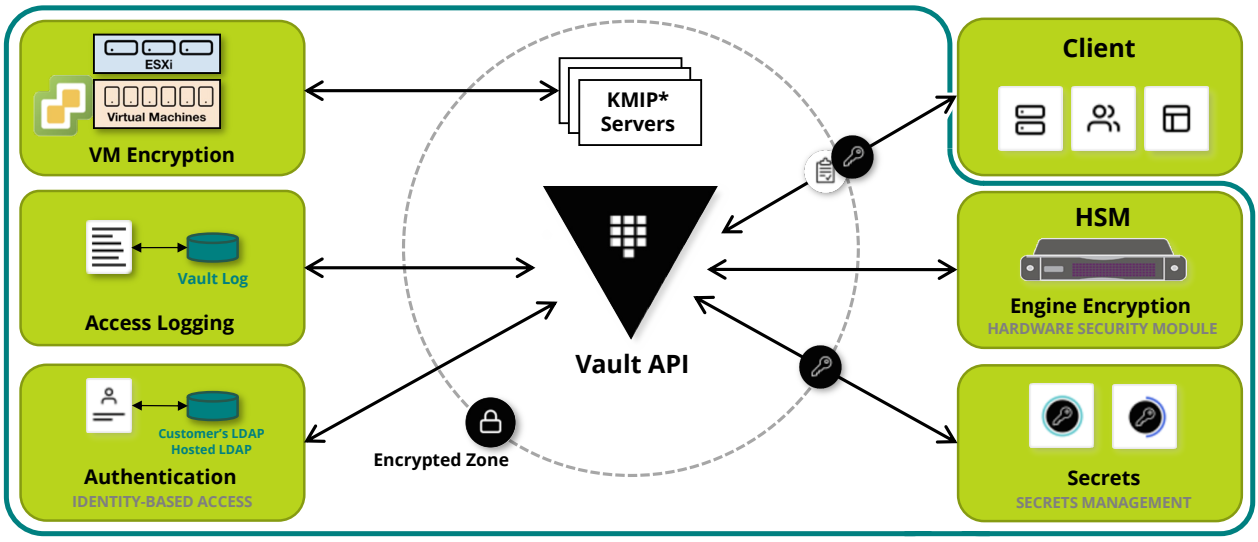
Alle Geheimnisse im KMS haben eine Gültigkeitsdauer. Nach Ablauf widerruft das KMS das Geheimnis automatisch. Anwendungen können die Laufzeit über integrierte Renew-APIs erneuern.

REVOCATION

Das KMS verfügt über eine integrierte Unterstützung für den Widerruf von Geheimnissen. Das KMS kann nicht nur einzelne Geheimnisse widerrufen, sondern auch eine Reihe von ihnen — etwa jene eines bestimmten Typs oder wenn sie von einem bestimmten Benutzer gelesen werden. Der Entzug von Geheimnissen hilft bei der Weitergabe von Schlüsseln und bei der Sperrung von Systemen im Falle eines Ereignisses.

aspectra AG
Weberstrasse 4
CH-8004 Zürich

+41 44 296 56 56
info@aspectra.ch
www.aspectra.ch



*Key Management Interoperability Protocol

ASPECTRA KEY AND SECRET MANAGEMENT

18'000

Ungefähre Anzahl Secrets, welche auf unseren Systemen im Umlauf sind. Auf jedem System sind 5-10 Secrets für Authentifizierungs- und Autorisierungsprozesse im Einsatz.

HARDWARE: HSM

Das aspectra KMS ist durch ein Hardware Security Modul (HSM) abgesichert. Das HSM verwaltet die Schlüssel, die nötig sind, um das KMS zu betreiben. Das HSM-Modul stammt von der Firma *Securosys SA*, einem Schweizer Hersteller von Sicherheitssystemen.

HOCHVERFÜGBAR

Sowohl das Key Management System (KMS) wie auch das Hardware Security Modul (HSM) werden von aspectra hochverfügbar und georedundant zur Verfügung gestellt.

aspectra AG
Weberstrasse 4
CH-8004 Zürich

+41 44 296 56 56
info@aspectra.ch
www.aspectra.ch