Kammer der Schlüssel

Key Management in Public Clouds

Um Daten in der Cloud vor unberechtigtem Zugriff zusätzlich zu schützen, empfiehlt es sich, sie zu verschlüsseln. Ein Hardwaresicherheitsmodul verbessert die sichere Ver- und Entschlüsselung.

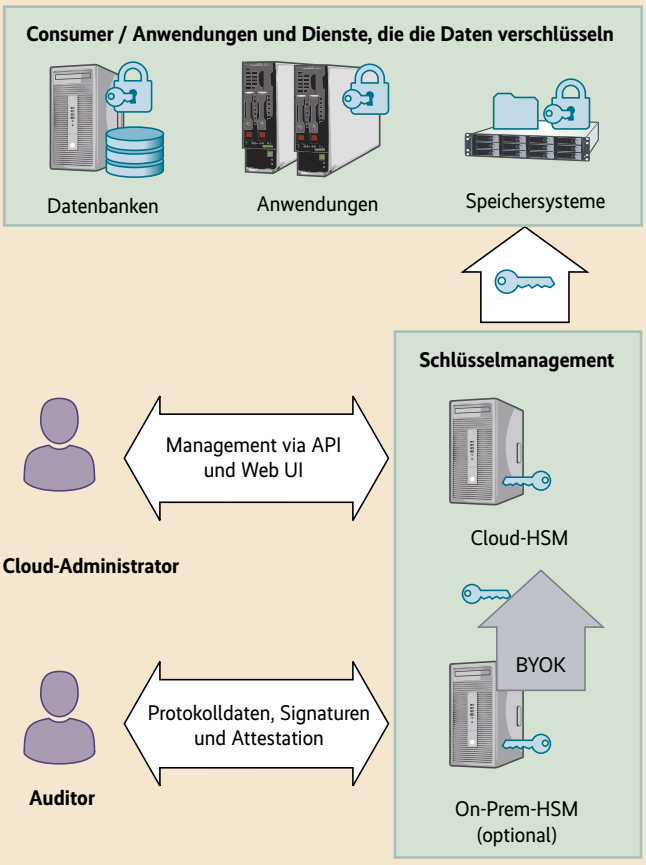
Verschlüsselung ist wie Magie: Richtig angewendet soll sie alles sicher machen – auch in der öffentlichen Cloud. Die Schutzziele Integrität und besonders die Vertraulichkeit sind durch Verschlüsselung zu erreichen. Aber jede Verschlüsselung ist nur so gut wie der Schutz der Schlüssel. Den bestmöglichen Schutz bieten Hardwaresicherheitsmodule (Hardware Security Modules – HSM). Alle großen Public-Cloud-Anbieter stellen daher einen darauf basierten Dienst bereit.

Die wohl wichtigste Grundlage für den richtigen Einsatz von Verschlüsselung ist die Trennung von verschlüsselten Daten und für die Entschlüsselung notwendigen Daten. Liegen beide zusammen, ist der Schutz nicht vorhanden. Wenn zum Zeitpunkt der gewünschten Ver- oder Entschlüsselung der Schlüssel nicht im Zugriff ist, ist die Ver- oder Entschlüsselung nicht möglich. Es gilt also, den Schlüssel nur dann bereitzustellen, wenn ein berechtigter Vorgang ansteht, und den Zugriff auf den Schlüssel zu verwehren, wenn der Vorgang nicht berechtigt ist. Wer hier die richtigen Kriterien findet und technisch umsetzt, kann seine Daten sehr zuverlässig und auch für längere Zeiträume vor unberechtigtem Zugriff oder Veränderung schützen.

Dies ist im eigenen Netzwerk und den Computern vor Ort schon nicht einfach, in der Public Cloud ist es umso schwerer. Ein Ansatz ist, die Schlüssel entweder selbst zu verschlüsseln, sodass vor der Verwendung noch ein Passwort notwendig ist, oder sie zentral zu verwalten und den Zugriff nur nach erfolgreicher Authentifizierung und Autorisierung zu erlauben. In großen Umgebungen kommt man an einer zentralen Verwaltung nicht vorbei. Eine Verschlüsselung der Schlüssel mit einem zusätzlichen symmetrischen Schlüssel kommt meistens nicht zur Anwendung, aber der Transport der Schlüssel erfolgt über authentifizierte und verschlüsselte Verbindungen. Die derzeit höchste Sicherheit für die Schlüssel bieten die HSMs.

Ein HSM kann die Schlüssel schützen, da es in einer separaten Hardware alle sicherheitsrelevanten Funktionen ausführt. Der höchste Schutz gebührt dabei den Schlüsseln, die für die Signatur anderer Schlüssel zum Einsatz kommen. Dabei muss man verhindern, dass diese Schlüssel in fremde Hände gelangen. Andere Aufgaben sind das Erzeugen von Zufallszahlen für Schlüssel, die Verschlüsselung von Daten, die Verwaltung von Schlüsseln und die Bestätigung der Echtheit von Daten über Prüfsummen. Die HSMs sind gegen Missbrauch geschützt (Tamper Resistant) und stellen die Arbeit ein oder warnen, wenn sie Manipulationsversuche an der Hard- oder Software erkennen (Tamper Evident). Manche HSMs sind auch für die Unterstützung von TLS-Verbindungen geeignet und nehmen so den Servern die rechenintensiven Operationen des TLS-Verbindungsaufbaus ab (TLS Offloading). Fast alle HSMs erlauben eine virtuelle Aufteilung der Hardware in eigene Partitionen, die die Daten zertifiziert sicher von den anderen Partitionen trennen. Grundsätzlich ist die Zertifizierung nach den Standards FIPS 140-2 (Federal Information Processing Standard) und Common Criteria üblich sowie die Zulassung für die VS-IT durch das BSI bei diesen Geräten.

Allen Modellen gemeinsam ist die Bereitstellung der Dienste über eine API. Physische Faktoren der Authentifizierung wie Smartcards oder abgetrennte PIN-Pads fallen somit aus. Die Trennung der Netze und die Authentifizierung ist die einzige Absicherung gegen unbefugte Nutzung. Für den Anwender stellt sich die Frage, ob er wirklich mit dem richtigen Schlüsseldienst und HSM redet. Über das Zertifikat des Dienstes lässt sich das einfach nachweisen. Ob der Schlüssel wirklich aus dem HSM ist, erfährt man über die Attestierung. Dabei sendet das HSM eine Prüfsumme des Keys und garantiert so, dass dieser Key wirklich im HSM erzeugt wurde.



Der Kunde verwaltet seine Schlüssel selbst, kann aber auch extern erzeugte Schlüssel importieren (Bring Your Own Key – BYOK).

Schlüsselmanagement in der Cloud

Ein HSM ist eine Hardware und scheint der Idee der Cloud erst einmal zu widersprechen.

Daher offerieren die großen Cloud-Anbieter zwei Optionen. Die erste ist ein allgemeiner Dienst (Key Management Service, KMS), der für die Kunden die Schlüssel verwaltet und innerhalb der Umgebung des Kunden wie ein HSM anzusprechen und zu nutzen ist. Die zweite Option ist, dem Kunden eine Partition auf einem HSM zu reservieren. Damit kann er so auch innerhalb des Netzes des Cloud-Anbieters die physischen und logischen Sicherheitsmechanismen der HSM nutzen.

Daten ver- und entschlüssen

Eine besondere Spielart dieses Betriebsmodells sind die spezialisierten Anbieter von Cloud-HSMs, die nur diesen Dienst und nicht die weiteren typischen Cloud-Dienste im Portfolio haben. Dieser Artikel betrachtet nur die Cloud-Angebote zur Schlüsselverwaltung, unabhängig davon, ob sie Teil eines umfassenden Cloud-Angebotes sind oder von einem spezialisierten Anbieter kommen.

Der Einsatzzweck dieser Angebote ist es, asymmetrische Schlüssel wie RSA, ECC und symmetrische Schlüssel für AES zu erzeugen. Diese kommen für die Verschlüsselung von Daten bei diesem oder einem anderen Cloud-Anbieter zum Einsatz. Die asymmetrischen Schlüssel sind zwar validiert, lassen sich aber nur für einen kurzen Zeitraum einsetzen. Das HSM kann ihre Herkunft auch beweisen. Ver- und entschlüsseln sie Daten wie vorgesehen, erfolgt dies auf den Computern des Cloud-Anbieters. Der Nutzer hat keinen Zugriff auf die Hardware; er kann also nicht verifizieren, dass die Daten dort auch verschlüsselt sind. Auch könnte der Anbieter die Schlüssel speichern und sich oder Dritten Zugriff auf die Daten ermöglichen. Daher stellt sich die Frage, was der Aufwand dann an verifizierbarer und falsifizierbarer Sicherheit bringt.

Bei manchen Datentypen ist die Verifikation möglich. Wer eine Datei oder ein Objekt in einem Cloud-Speicher verschlüsselt und dann die Daten sowie den Key herunterlädt, kann über die Entschlüsselung nachweisen, dass auch wirklich dieser Key die ursprünglichen Daten verschlüsselt hat. Ob die Daten allerdings im Speicher verschlüsselt waren oder erst beim Download verschlüsselt wurden, kann er nicht nachweisen. Wenn der Schlüssel für eine transparente Verschlüsselung von Daten im Einsatz ist, sieht der Kunde nie die verschlüsselten Daten und kann diesen Nachweis nicht führen.

Wie bei vielem in der Cloud ist hier eine Verifikation oder Falsifikation der Angaben des Anbieters nur eingeschränkt möglich. Alle Hersteller bieten Zertifizierungen an, die den Kunden ihrer Dienste zusichern, dass die versprochenen Merkmale auch so umgesetzt sind, wie es beschrieben ist. Man kann hier nur hoffen, dass die Auditoren nach C5 und den anderen Cloud-Sicherheitsstandards auch die Verifikation tatsächlich durchführen und sich nicht nur auf die Angaben der Anbieter verlassen.

Eine Vertrauensbasis schaffen

Für asymmetrische Schlüssel wie RSA kann ein HSM helfen, indem es den zentralen Schlüssel für die Signaturen erzeugt und enthält: den Root einer Zertifizierungsstelle. Es signiert alle Schlüssel für den Alltag und sichert sie so vor unerlaubter Veränderung. Da der öffentliche Schlüssel des Signaturschlüssels vorliegt, ist die Validierung möglich. So kann der Administrator, der Auditor, aber auch jeder Rechner selbst die Echtheit der Schlüssel bestätigen. Diese sind dann für die Übertragung und Validierung der symmetrischen Keys und die Authentifizierung der für die Kommunikation verwendeten Schlüssel im Einsatz. Dieser „Vertrauensanker“ sichert so die gesamte Kette aller Schlüssel. Das HSM erzeugt diesen Signaturschlüssel entweder selbst oder der Anwender überträgt ihn von einem On-Premises-HSM verschlüsselt zum Cloud-HSM (Bring Your Own Key, BYOD). Üblicherweise verlässt er das HSM nicht und kann so auch nicht entwendet werden.

Diese Überlegungen vorangestellt, ist der Einsatz von Verschlüsselung mit eigenen Schlüsseln bei den Cloud-Anbietern eine wesentliche Verbesserung der Sicherheit der Daten. Es ist allerdings notwendig, auch die Methoden, wie den Signaturschlüssel und die Verifikation aller abgeleiteten Schlüssel, anzuwenden und regelmäßig zu kontrollieren.

Die meisten Standards für IT-Sicherheit reduzieren den Schutzbedarf der Daten erheblich, sobald eine ausreichende Verschlüsselung vorliegt, und ermöglichen so den Einsatz auch von Public Clouds für Daten,

Anbieter mit Cloud-HSM oder Software-as-a-Service-Angebot

Hersteller	AWS	Equinix	Google
Produkt	AWS CloudHSM	Equinix SmartKey	GCP
Website	https://aws.amazon.com/cloudhsm/	https://www.equinix.com/services/smartkey/	https://cloud.google.com/hsm/
Kommentar	Amazon hat ein HSM in die AWS-Cloud integriert, bei dem der Kunde einen Mandanten auf der Hardware erhält. Es sind auch mehrere HSM möglich, die sich automatisch synchronisieren. Das HSM ist dabei in AWS Key Management Service (KMS) integriert. Nur die Anwendungen innerhalb des VPC-Netzwerkes haben Zugriff.	Equinix ist ein Anbieter von Rechenzentren, Dienstleistungen und Colocation. Das einzige SaaS-Produkt ist SmartKey; es bietet ein Fortanix SDKMS an. Fortanix kann auch Software auf dem Schlüsselmanagement installieren, um es in eigene Anwendungen zu integrieren.	Auch Google bietet ein HSM als Erweiterung seines Key Management Service (KMS) an. Es ist in die anderen Angebote wie Logging und Storage eingebunden. Der Kunde erhält einen Mandanten auf einem Cavium HSM, das allerdings noch nicht in allen Zonen bereit steht.
Cloud-HSM	ja	SaaS-Angebot	ja
BYOK	ja	ja	ja
Key Management	ja	ja	ja
API	PKCS #11, JCE, Microsoft CryptoNG	RESTful APIs, PKCS #11, CNG, JCE, KMIP	REST API
IAM	IAM von AWS	SAML, OAuth, Active Directory	Cloud IAM
Autorisierung	Quorum ist möglich, optional auch Tokens für die Authentifizierung.	RBAC, Segregation, Quorum	RBAC über Rollen in Projekten
Protokolle	AWS-Log-Service	ja	Cloud-Audit-Logging
Zertifizierung	FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3
Art der Schlüssel	RSA, 3DES, AES, ECC	RSA, AES, ECC	RSA, AES, ECC
Anzahl Schlüssel	3500 pro Cluster, 4 Cluster maximal; Erweiterungen sind möglich	keine spezifischen Angaben	unbegrenzt
TLS-Terminierung	ja	ja	

Angaben ohne Anspruch auf Vollständigkeit

deren Sensibilität dies eigentlich verbieten würde. Es ist dabei zu beachten, dass eine Verarbeitung der Daten in den meisten Fällen eine vorherige Entschlüsselung erfordert. Sonderfälle wie die Verschlüsselungsgateways für beispielsweise Salesforce oder Storage as a Service verschlüsseln die Daten noch im eigenen Netz und übermitteln nur das Chiffrat an die Cloud.

Verschiedene Gesichtspunkte

Die Tabelle beleuchtet die Anbieter nach den folgenden Funktionen und Kriterien (basierend auf den Angaben der Hersteller):

- Cloud-HSM: Gibt an, ob der Dienst es erlaubt, die Schlüssel in einem HSM zu verwalten.
- BYOK – Bring Your Own Key: Der Nutzer kann einen extern erzeugten Key im Cloud-HSM speichern und von dort aus bereitstellen oder ihn im Cloud-HSM für das Erzeugen von Arbeitsschlüsseln oder deren Signierung nutzen. Der Schlüssel kann dabei von einem eigenen HSM verschlüsselt auf das Cloud-HSM wandern und ist nicht für Dritte oder den Cloud-Anbieter sichtbar.
- Key Management: Die Verwaltung der Schlüssel muss es erlauben, diese zu erzeugen, zu löschen, alte Schlüssel durch neue zu ersetzen, zu exportieren, zu importieren und dabei alle Vorgänge gesichert zu protokollieren.
- API: Die Cloud-HSMs sind alle über APIs erreichbar: Public Key Cryptography Standard (PKCS) #11, Microsoft Cryptographic Application Programming Interface (CAPI), Cryptography API: Next Generation (CNG), Java Cryptography Architecture (JCA), Java Cryptography Extension (JCE) und das Key Management Interoperability Protocol (KMIP).
- Identity and Access Management – Authentifizierung: Hier sind Benutzer mit Passwort, Time-based One-Time Password (TOTP), RSA-Token, Zertifikate und API-Keys möglich. In automatisierten Verfahren kommen allerdings nur Zertifikate und API-Keys zum Einsatz.
- Autorisierung: On-Premises-HSMs erlauben neben rollenbasierter Zugriffskontrolle (RBAC) auch das Quorum, in dem mehr als eine Autorisierung für einen Vorgang notwendig ist. Das HSM führt eine Signatur nur dann durch, wenn mehr als eine Person dies genehmigt. Cloud-HSMs erlauben hier zumeist nur das einfache Modell der Autorisierung mit einer Identität und der Vergabe der Berechtigungen über Gruppen.
- Protokolldaten: Die meisten Anbieter haben Protokolldaten, die mit Signaturen vor Veränderungen geschützt sind.
- Zertifizierung: Die meisten Angebote sind nach FIPS 140-2 Level 1, 2 oder 3 und Common Criteria zertifiziert; keines ist zurzeit nach der deutschen VSA zertifiziert.
- Art der Schlüssel: Die Schlüssel können symmetrisch oder asymmetrisch sein. Für die symmetrischen Schlüssel sind neben RSA und DSA auch elliptische Kurven möglich. Manche Anbieter bieten auch Schlüssel nach Methoden an, die auch von Quantencomputern nicht zu brechen sein sollen.
- Anzahl Schlüssel: Welche Anzahl von Schlüsseln der Dienst verwalten kann.

Fazit

Ein Cloud-HSM bietet eine zentrale Stelle für die Verwaltung von Schlüsseln mit klar definierten Prozessen, Audits und Validierung. Es kann eine gute Ergänzung eines Kryptokonzepts sein, doch empfiehlt es sich, darauf zu achten, dass die Authentifizierung für den Zugriff und vor allem die Verwaltung der Schlüssel den Ansprüchen gerecht wird.

(nb@ix.de)

Christoph Puppe
ist Security Consultant bei SVA, Audit-Teamleiter, IS-Revisor, Mitautor des Grundschutzkompendiums und ehemaliger Penetrationstester.

Microsoft	Thales eSecurity	Townsend Security	Utimaco
Azure	CipherTrust Cloud Key Manager	Alliance Key Manager Cloud HSM	Utimaco CryptoServer Cloud
https://azure.microsoft.com/en-us/services/key-vault/	https://www.thalesesecurity.com/products/key-management/ciphertrust-cloud-key-manager	https://www.townsendsecurity.com/product/encryption-key-management-cloud-hsm	https://hsm.utimaco.com/products-hardware-security-modules/form-factor/cloud-hsm-as-a-service/
Das HSM-Angebot von Azure ist in Key Vault integriert. Es erlaubt das Schlüsselmanagement, aber auch das Speichern von Passwörtern. Die API ist nur aus dem VPC des Kunden erreichbar. Wer eine Level-3-Sicherheit benötigt, kann das Dedicated-HSM nutzen. Azure bietet hierbei SafeNet Luna 7 von Gemalto an.	Thales bietet hier den eigenen Vormetric Data Security Manager als SaaS an. Der Dienst ist in Azure, Office 365, AWS und Salesforce und deren private Cloud-Angebote integriert. Andere Clouds sind wohl nicht möglich.	Townsend bietet sein Produkt als HSMaaS mit Hosting in einem PCI-zertifizierten Rechenzentrum, On-Premises-HSM oder in der AWS- und Azure-Cloud betrieben an. Tamper Resistant Hardware ist als Option für das HSM verfügbar, aber nicht für HSMaaS. Die API bietet die Option, die Verschlüsselung mit AES direkt auf dem Gerät durchzuführen.	Utimaco vermietet HSM als HSMaaS jeweils dediziert an einen Kunden; keine virtuelle Trennung oder Partitionierung. Hosting ist ISO-27001-, PCI- und HIPAA-zertifiziert. CryptoServer kann auch Software auf dem Schlüsselmanagement installieren, um es in eigene Anwendungen zu integrieren.
ja	ja	SaaS	ja
ja	ja	ja	ja
ja	ja	ja, über einen Windows-Client	ja, mit der Option, persönlich am Gerät Schlüssel zu bearbeiten, Smartcard als 2FA
REST API	keine spezifischen Angaben	KMIP	Standard-APIs wie PKCS #11, JCE, CNG, OCSP
Azure AD und OAuth2	Integration in das IAM des Cloud-Anbieters über OAuth	über Zertifikate	keine spezifischen Angaben
RBAC	keine spezifischen Angaben	RBAC	RBAC, Multi-Tenancy, Quorum
Über Azure HDInsight und Export in eigene SIEM möglich	ja	syslog	keine spezifischen Angaben
FIPS 140-2 Level 2 (Level 3 mit Dedicated HSM)	FIPS 140-2 Level 1	FIPS 140-2 Level 1	FIPS 104-2 Level 3
RSA, AES, ECC, ECDSA	keine spezifischen Angaben	RSA, AES, ECC	RSA, ECC, ECDSA, ECDH, AES, CMAC, HMAC, SHA2-Family, SHA3
keine spezifischen Angaben	keine spezifischen Angaben	unbegrenzt	keine spezifischen Angaben
nein	nein	keine spezifischen Angaben	keine spezifischen Angaben