Zertifikate-Management in virtualisierten Docker-Umgebungen

Docker-Images benötigen für ihre Betriebsfähigkeit Geheimnisse wie Kennwörter und Schlüsselmaterial. Der Artikel zeigt Möglichkeiten auf, wie der sichere und effiziente Umgang mit Schlüsseln in Containerplattformen gelingt.

Von Werner Zügel, essendi it GmbH

Anwendungskomponenten in Docker-Images müssen notwendige Vorkehrungen für die IT-Sicherheit, Authentifizierung und Autorisierung mitbringen, beispielsweise Signaturzertifikate für Webservices oder Dokumente, Private-Keys, Datenbank-Kennwörter und andere Geheimnisse. Der Umgang mit sicherheitsrelevanten Artefakten wie Schlüsselpaaren stellt dabei eine spezielle Herausforderung dar. Deswegen werden die Entwicklungsstufen voneinander getrennt und für jede Umgebung ein eigenes Docker-Image für eine jeweils eigene Test-Umgebung angelegt. Insofern sind in jedem Stage wieder andere, passende Zertifikate, Schlüssel oder Kennwörter notwendig, die verwaltet werden müssen. Zudem ist die Speicherung von Sicherheitsartefakten direkt in den Docker-Images kein sicherer Ablageplatz.

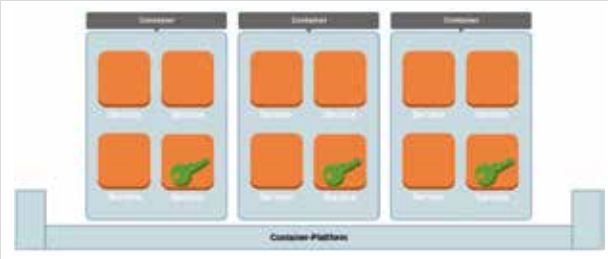
Hier entsteht zudem ein nicht unerheblicher administrativer und logistischer Aufwand. Für agile Softwareprozesse sind daher intelligente Lösungen mit hohem Automationsgrad bei gleichzeitig hohen Sicherheitsanforderungen erforderlich. Abhilfe schafft hier ein Bundle, bestehend aus einer Docker-Plattform, dem „essendi xc“-Zertifikatemanager in Kombination mit Hardware-Security-Modulen (HSM).

Management von Zertifikaten mit essendi xc

Mit essendi xc wird das Management von Zertifikaten wesentlich vereinfacht und automatisiert. DevOps-Teams sollen alle Aufgaben – auch administrative Dinge wie die Anforderung von Zertifikaten – innerhalb des Lösungsteams erledigen können. Dabei unterstützt essendi xc diese agilen Teams: Durch die Self-Service-Funktion von essendi xc wird der Bediener mittels vorkonfigurierter Zertifikatsprofile und dem Rollen- und Rechtekonzept vom System geführt. Gleichzeitig wird gewährleistet, dass die Regeln und Konventionen des Unternehmens, wie beispielsweise die Belegung von CN-Namen oder Schlüsselalgorithmen, eingehalten werden.

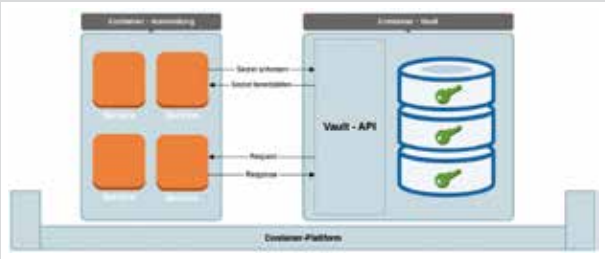
Die Key-Generierung, Anforderung und Beglaubigung bis hin zum Enrolment von Zertifikaten durch interne oder öffentliche Zertifizierungsstellen wird damit weitgehend automatisiert und standardisiert. Über Interfaces können die Vault-Stores der Containerplattformen an den „essendi xc“-Zertifikatemanager direkt angebunden werden. Damit wird bereits ein hoher Grad an Standardisierung

Geheimnisse und Schlüsselmaterial für Container im Überblick



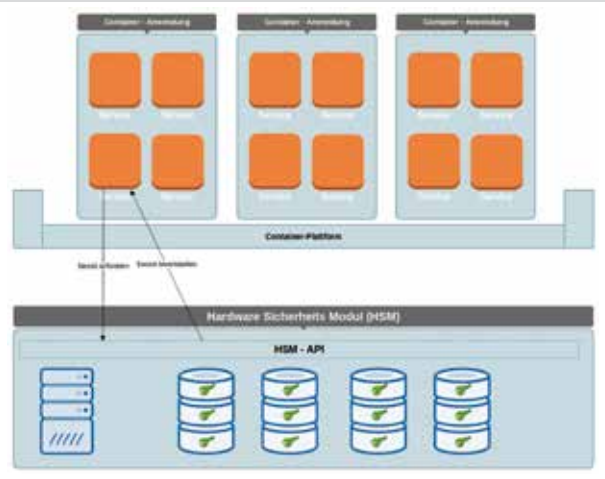
Stufe 0 – Schlüsselmaterial im Container

- Geheimnisse sind Bestandteil der Docker-Images
- Bestandteile des Quellcodes oder in Java-Keystores
- Schlüsselmaterial incl. Private Keys einfach zugänglich
- Transport / Deployment der Schlüssel über unsichere Kanäle
- Images sind über die Entwicklungsstufen hinweg nicht gleich



Stufe 1 – Schlüsselmaterial im Vault der Plattform

- Geheimnisse liegen in sicherem Vault-Speicher der Containerplattform
- geregelter, sicherer Zugang zum Vault über Multifaktor-Authentifikation
- stufenweises Autorisierungskonzept
- Transport der Schlüssel über unsichere Kanäle
- Images sind über die Entwicklungsstufen hinweg identisch



Stufe 2 – Schlüsselmaterial im HSM

- Geheimnisse liegen ausgelagert in sicherem Hardware-Speicher
- performante und umfangreiche Krypto-Algorithmen
- geregelter, sicherer Zugang zum HSM über Multifaktor-Authentifikation
- Mandanten- oder anwendungsbezogene Segmentierung der Speicherorte im HSM
- Autorisierungskonzept passend zur Segmentierung des HSM
- kein Transport der Schlüssel über unsichere Kanäle
- Schlüssel werden im HSM erzeugt, private Schlüssel und andere Geheimnisse müssen das HSM nicht verlassen, da z. B. die Signatur von Webservice-Nachrichten direkt im HSM erfolgt
- Images sind über die Entwicklungsstufen hinweg identisch

und Vereinfachung der Prozesse des Zertifikatsmanagements im Zusammenspiel mit Docker-Plattformen erreicht. essendi xc kann zudem über das JCA-Interface ein HSM direkt ansprechen und Schlüsselmaterial darin erzeugen beziehungsweise ablegen.

Management sensibler Daten in HSMs

Die beste Variante zur Verwaltung von Geheimnissen ist der Einsatz von HSMs. Denn eine solche Infrastruktur ist sicherer als ein bloßer Schutzmechanismus über die Software, da sie schwerer angreifbar ist. Eine gute Integration mit der Verwaltungsapplikation essendi xc ist mit HSM-Geräten der Firma Securosys gegeben. Mit essendi xc werden Zertifikate auf sehr einfache Art und Weise, teilweise hoch automatisiert, angefordert und direkt im HSM hinterlegt. Die Schlüssel werden dort erzeugt und verlassen das HSM niemals. HSMs liefern eine umfangreiche und breite Palette an leistungsfähigen Verschlüsselungsalgorithmen und Funktionen für Krypto-Infrastrukturen. ■

Messestand: Halle 10.0, Stand 10.0-520

Vorträge von essendi it auf der it-sa

Dienstag, 09.10., 14:45 bis 15:00 Uhr, Technik Forum (Forum Blau)
Sicheres Zertifikatsmanagement in Docker-Betriebsumgebungen

Donnerstag, 11.10. von 13.15 bis 13.30 Uhr, Management Forum (Forum Rot)
360° Zertifikatsmanagement
(Gemeinschaftsvortrag mit Partner SwissSign)