Certificate as a Service

Studiengang: BSc in Informatik
Betreuer: Prof. Hansjürg Wenger
Experte: Dr. Igor Metz (Glue Software Engineering AG)

Mit der Secure Private Cloud EJPD bietet das Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements seinen Kunden eine moderne, Kubernetes basierte On-Premise Cloud Plattform welche höchsten Sicherheitsanforderungen entspricht. In dieser Arbeit wurde ein Service für den automatisierten Bezug und die Verwaltung von TLS-Zertifikaten für die Benutzer der Plattform entwickelt.

Ausgangslage

Für eine sichere und authentisierte Kommunikation der Anwendungen auf der Secure Private Cloud EJPD werden TLS-Zertifikate der Swiss Government PKI verwendet. Bisher wurde über einen existierenden Zertifikatsservice für jeden Kubernetes Namespace automatisch ein Wildcard-Zertifikat ausgestellt, welches von sämtlichen Applikationen innerhalb dieses Namespaces verwendet wird. Somit wird auch der dazugehörende Private Key von mehreren Komponenten benutzt und es ist keine eindeutige Identifikation eines Services möglich.

Ziel

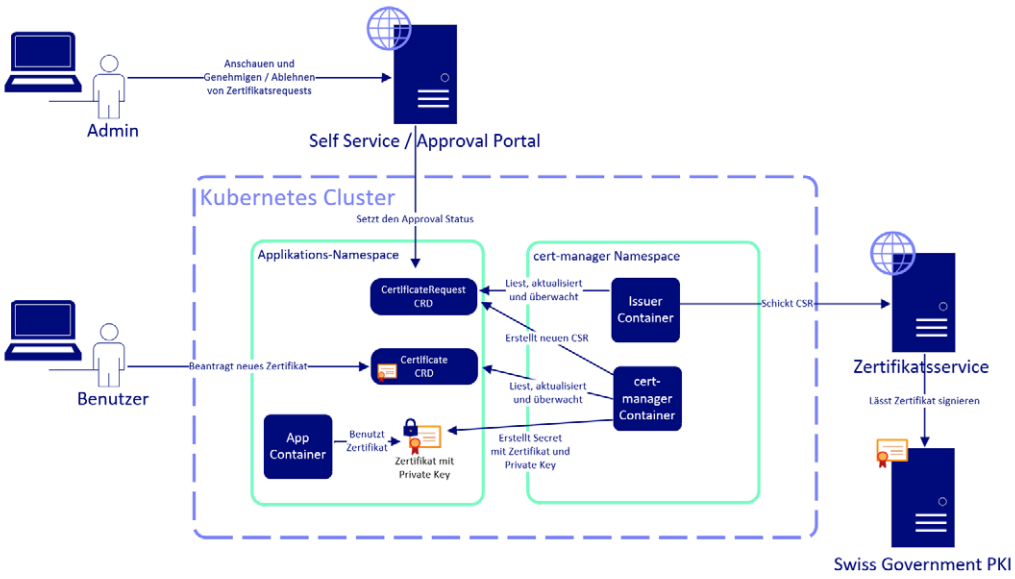
Mit einer neuen, automatisierten Zertifikatsverwaltung soll den Benutzern der Secure Private Cloud EJPD die Möglichkeit geboten werden, selbstständig direkt in Kubernetes Zertifikate verwalten zu können. Somit kann pro Applikation ein eigenes Zertifikat verwendet werden und es ist nicht mehr nötig, Private Keys über mehrere Komponenten hinweg zu teilen.

Um nach wie vor Kontrolle über die ausgestellten Zertifikate zu haben, sollen neue Zertifikatsrequests von Administratoren über ein Portal genehmigt werden müssen.

Realisierung

Die entwickelte Lösung basiert auf dem Open-Source Tool „cert-manager“, welches auf Kubernetes deployed wird und die Verwaltung von Zertifikaten übernimmt. In Form eines sogenannten „Issuers“ wurde eine Schnittstelle zwischen dem cert-manager und dem bestehenden Zertifikatsservice des ISC-EJPD entwickelt. Dieser ist für die Verwaltung von Zertifikatsrequests zuständig. Er prüft eingehende Requests auf ihre Gültigkeit und, sobald diese genehmigt wurden, schickt sie zur Signatur an den Zertifikatsservice. Über das zentrale Approval Portal erhalten Administratoren einen Überblick aller Requests über sämtliche Umgebungen der Secure Private Cloud EJPD und können direkt einzelne Requests genehmigen oder zurückweisen.

Simon Wälchli
IT Security



Übersicht Zertifikatsmanagement