Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

Managed PKI-Lösung mit clientseitiger Schlüsselgenerierung im Browser

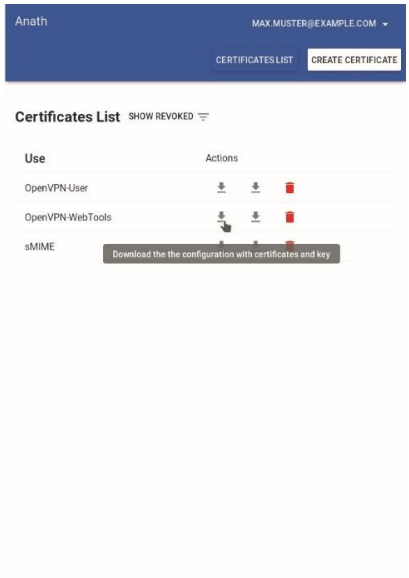
Diplomierende
Rafael Ostertag
Martin Wittwer

Dozierende
Patrick Baumgartner
Andreas Meier

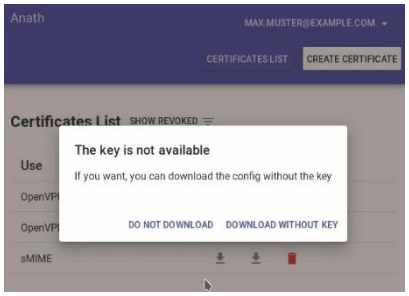
Die vorliegende Bachelorarbeit behandelt die Entwicklung einer PKI-Lösung. Ein wichtiger Teil der Lösung ist hierbei, dass Private-Keys und Certificate-Signing-Requests im Webbrowser der Benutzers erstellt werden, ohne das der Private-Key den Client verlässt. Der Certificate-Signing-Request wird dann direkt nachdem er erstellt wurde an das Backend der Webapplikation geschickt, welches dann ein durch die Certificate-Authority signiertes X.509 Public-Key-Certificate zurück liefert.

Für die Umsetzung der PKI-Lösung wurden zuerst die theoretischen Grundlagen studiert, damit sich die Lösung an anerkannten Standards orientiert und diese einhält. Dazu wurden mehrere RFCs und andere Arbeiten zu Public-Key-Certificates und dem X.509 Standard konsultiert und die wichtigsten Punkte davon zusammengefasst. Anhand der so erlangten Erkenntnisse wurde ein Protokoll für die Kommunikation von Web Client und dem Backend-Server entworfen und definiert, wie der Server das Verwalten von CA und Zertifikaten handhabt. Das Protokoll musste in zwei Applikationen umgesetzt werden. Zum einen ist dies der Web Client, welcher auf AngularJS 1.6 basiert und mit Angular Material gestaltet wurde. Der Client ist die Schnittstelle zwischen dem Endbenutzer und den Funktionen der PKI-Lösung. Auch gehört das Erstellen von Private-Key und Certificate-Signing-Request zu den Hauptaufgaben des Clients. Die andere Applikation ist der Server, welcher die Certificate-Authority beherbergt. Der Server ist in Java 8 geschrieben und als Framework wird Spring Boot 1.5 eingesetzt. Der Server hat verschiedene wichtige Aufgaben. Dazu zählen das Signieren von Certificate-Signing-Request anhand der Certificate-Authority. Der Server unterstützt hierfür zwei verschiedene Modi. Der eine erlaubt das Signieren eines Zertifikats, sofern der Benutzer korrekt authentifiziert ist und ein Zertifikat für seine eigene Mailadresse beantragt. Der andere Modus ist auf mehr Sicherheit ausgelegt und beinhaltet eine zusätzliche Prüfung der Mailadresse, indem eine E-Mailnachricht an den Benutzer geschickt wird, welche ein Bestätigungstoken enthält.

Die Bestandteile der PKI-Lösung sind als Open-Source-Projekte auf GitHub unter https://github.com/AnathPKI verfügbar.



Web Client - Zertifikatsliste



Web Client - Konfigurationsdownload-