Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

InIT Institut für angewandte
Informationstechnologie

Umsetzung eines Zertifikatsdienstes fur die ZHW

Diplomierende
David Eggerschwiler
Alexander Horvath

Dozent
Marc Rennhard

Das Bedurfnis nach Sicherheit fur digitale Daten ist in den letzten Jahren markant gestiegen. Zur Gewahrleistung dieser Sicherheit hat sich dabei der Einsatz von X.509 Zertifikaten etabliert, die auf ein hierarchisches Vertrauensmodell setzen. Um eine reibungslose Nutzung sicher zu stellen, mussen jedoch alle Beteiligten mit einem Zertifikat ausgestattet werden. Ebenso ausschlaggebend ist der einfache Zugriff auf die Zertifikate anderer Benutzer und das Vertrauen zur ausstellenden Certification Authority (CA).

An diesem Punkt setzt vorliegende Diplomarbeit an, mit dem Ziel, einen Zertifikatsdienst fur eine Abteilung der ZHW einzufuhren und den Mitarbeitenden das Versenden von verschlusselten und unterzeichneten E-Mail-Nachrichten zu ermoglichen. Unter Berucksichtigung der Anforderungen der Zielgruppe wurden die verschiedenen Ablaufe und Prozesse definiert.

Entstanden ist die IKT Certification Authority, eine auf EJBCA basierende Open Source CA, welche in die ZHW-Umgebung integriert ist und alle Mitarbeitende der Abteilung IKT mit Zertifikaten ausrustet. Die Zertifikate werden dabei auf sicheren Kryptotoken gespeichert. Diese Token fuhren alle kryptografischen Operationen durch und schutzen den Zugang zu den privaten Schlusseln mit einem Passwort.

Bild klein 1.

Neben der Definition von optimalen Prozessen wurde der Implementierung des Benutzerportals besondere Beachtung geschenkt. Nicht fehlende Technologien, sondern mangelnde Benutzerfreundlichkeit in den Anwendungsablaufen, verhindern oft die Umsetzung von neuen Sicherheitslosungen. Daher wurde der Fokus auf einfache Bedienbarkeit und gut strukturierte Ablaufe gelegt. Aber auch die Attraktivitat des Portals ist von Bedeutung. Dieses schafft Vertrauen und wird durch Wahrung der Corporate Identity erreicht.

Die Autoren erhoffen sich mit dieser Diplomarbeit eine solide Basis fur eine spatere Ausweitung der eingesetzten Anwendungen und des Nutzerkreises auf die ganze ZHW. Damit soll gezeigt werden, dass die Implementierung einer Public Key Infrastruktur nicht nur Grosskonzernen vorbehalten ist und durchaus basierend auf Open Source Software erfolgen kann.