

Sicherer E-Mail-Dienst

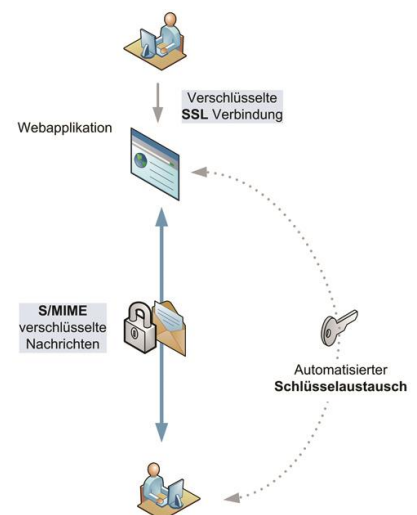
E-Mail hat sich in den vergangenen Jahren zu dem elektronischen Kommunikationsmittel schlechthin entwickelt. Den Ansprüchen an Sicherheit und Privatsphäre vermag E-Mail allerdings nicht gerecht zu werden. Obwohl diese Aspekte zentrale Bedürfnisse der Menschen sind, wird dies bei der Kommunikation mit E-Mail oft akzeptiert. Täglich versenden wir vertrauliche und sensitive Daten per E-Mail. Im Wissen oder auch im Unwissen darüber, dass diese während dem Transport durch das Internet von fremden Personen gelesen und sogar verändert werden können.

Nur durch zusätzliche Sicherheitsmassnahmen wie Verschlüsselung oder Signierung von E-Mails kann diesem Problem entgegen getreten werden. Die Massnahmen scheitern jedoch oft an der Praxistauglichkeit. Wie unsere Umfrage aufzeigt, verzichten viele E-Mail Benutzer auf den Einsatz solcher Technologien, da deren Anwendung zu komplex ist oder notwendiges Vorwissen fehlt. Weil das Bedürfnis nach einfachen Lösungen demnach gross ist, sind alternative Lösungsansätze gefragt. Diese Diplomarbeit befasst sich mit der Konzeption und der Entwicklung einer webbasierten Applikation um den genannten Problemen zu begegnen. Aufbauend auf den zuvor erarbeiteten Grundlagen werden die sicherheitsrelevanten Prozesse einer Webmailapplikation identifiziert, beschrieben und verschiedene Realisierungsmöglichkeiten evaluiert. Anschliessend beschreiben wir eine mögliche Architektur unserer Applikation. Einige Aspekte aus der vorgangigen Planung werden in Form eines Prototypen verwirklicht. Dieser basiert auf dem weit verbreiteten S/MIME Verschlüsselungsstandard, wodurch die Interoperabilität mit externen Kommunikationsteilnehmern gewährleistet ist. Durch die komplette Automatisierung sonst komplexer Prozesse erreichen wir, dass die Webapplikation auch von Benutzern mit geringem Vorwissen benutzt werden kann. Dieser Prototyp zeigt, dass die theoretisch modellierten Prozesse in die Realität umsetzbar sind. Mit unserer Applikation bieten wir einem breiten Publikum eine intuitive Lösung, mit dem die Sicherheitsprobleme von E-Mail der Vergangenheit angehören.



Diplomierende
Christian Felder
Daniel Muhlebach

Dozent
Eduard Mumprecht



Die Webapplikation bietet durchgehende Nachrichtenverschlüsselung mit S/MIME. Der Schlüsselaustausch erfolgt automatisiert und ist vollkommen vom Webmailbenutzer losgelöst.