E-Mail Verschlüsselung

Landratsamt Roth

S/MIME Standard

Disclaimer: In der Regel lässt sich die Verschlüsselungsfunktion störungsfrei in den E-Mail-Programmen einrichten. Es wird aber darauf hingewiesen, dass in einigen Fällen das Einrichten der Verschlüsselungsfunktion in E-Mail-Programmen durch nicht vorhergesehene Inkompatibilitäten mit anderen Systemeinstellungen zu Fehlern bis hin zum Programmcrash führen kann. Das Einrichten der Verschlüsselungsfunktion erfolgt deshalb auf Ihr eigenes Risiko.
Das Landratsamt Roth kann hierfür aber auch für etwaige Folgeschäden keine Haftung und keinen Support übernehmen. Bei der Einrichtung gemäß dieser Anleitung erklären Sie sich mit diesem Haftungsausschluss einverstanden. Die Nutzung des Verschlüsselungszertifikats unterliegt den rechtlichen Bedingungen der jeweiligen Länder, die einzuhalten sind.

Landratsamt Roth
Weinbergweg 1
91154 Roth
Internet: www.landratsamt-roth.de

E-Mails werden im Internet offen übertragen. Sie sind mit Postkarten vergleichbar, die von vielen Personen beim Transport gelesen werden können.

Das Problem im Internet:
Mails werden abgefangen und gelesen. Um vertrauliche Inhalte vor fremden Augen zu schützen, gibt es jedoch eine Lösung: **die Verschlüsselung der E-Mails**.
Dabei werden sie so kodiert, dass sie für Unbefugte nicht lesbar sind. Diese Sicherheitsaspekte sind insbesondere bei der internen und externen Geschäftskommunikation wichtig. Doch hier muss man unterscheiden: Intern ist die Bereitstellung der Verschlüsselungsmöglichkeit durch die Verwendung eines einheitlichen E-Mail-Systems einfach. Der Absender aktiviert die Verschlüsselung über die Zustelloptionen.

Ganz anders jedoch in der externen Kommunikation: Die E-Mail-Systeme der Kommunikationspartner sind ausgesprochen vielfältig.

Um auch in diesem Umfeld verschlüsselt kommunizieren zu können, bietet das Landratsamt Roth eine einfache und wirksame Lösung an, die auf dem Internet-Standard **S/MIME** basiert. S/MIME ist ein Verfahren, das von vielen E-Mail-Programmen unterstützt wird. Das heißt: in der Regel verfügen alle externen Kommunikationspartner über die technischen Möglichkeiten, es einzusetzen.

Wie wenig Aufwand es erfordert, verschlüsselt zu kommunizieren, soll die vorliegende Anleitung zeigen: von der Ersteinrichtung bis zum täglichen Gebrauch.

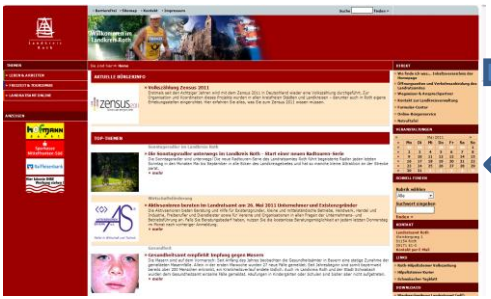
Das Prinzip

Kleiner Aufwand – große Wirkung: Für jeden Teilnehmer wird einmalig ein Schlüsselpaar erzeugt. Das Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel. Nur diese zusammen generierten Schlüssel passen zueinander.

Der öffentliche Schlüssel ermöglicht das Verschlüsseln von Nachrichten, der private Schlüssel das Entschlüsseln. Der öffentliche Schlüssel wird dem Kommunikationspartner übermittelt. Mit dem öffentlichen Schlüssel kann der Kommunikationspartner dem Halter des privaten Schlüssels kodierte E-Mails senden. Und der wiederum macht die verschlüsselte E-Mail mit dem zugehörigen privaten Schlüssel wieder lesbar. Wichtig ist, dass der private Schlüssel nie weitergegeben werden darf. Denn der private Schlüssel garantiert die Sicherheit, dass nur derjenige die E-Mails entschlüsseln kann, an den sie auch gerichtet ist.

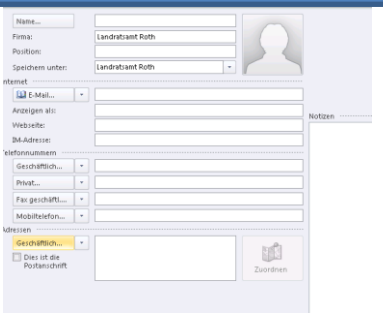
Um die Verschlüsselung auf dem eigenen PC zu ermöglichen, sind eine Reihe von einfachen Schritten nötig. Diese Schritte werden auf interner und externer Seite getrennt vorgenommen. Die internen Schritte sind für Microsoft Outlook dargestellt. Bei anderen Versionen muss die Funktion geprüft werden.

Interner Kommunikationspartner (Landratsamt Roth)



Webseite des Landratsamt Roth laden

Externer Kommunikationspartner



Zertifikat des Landratsamt Roth von der Webseite

und ins Adressbuch integrieren.

Richtung Extern/Intern funktioniert

Mit dem intern generierten öffentlichen Schlüssel ist es nun möglich, dass der externe Kommunikationspartner dem internen Partner (Landratsamt Roth) verschlüsselte E-Mails sendet und dieser die verschlüsselten E-Mails auch lesen kann.

Ablauf:

1. Interner Kommunikationspartner
    a. Schlüsselpaar generieren
    b. Zertifikat im E-Mail-Programm integrieren
    c. Öffentlichen Schlüssel für die Verschlüsselung zur Verfügung stellen.
2. Externer Kommunikationspartner
    a. Öffentlichen Schlüssel im Adressbuch hinterlegen
    b. E-Mail schreiben und vor dem Versenden auf „verschlüsseln“ klicken

Die externen Schritte im Einzelnen

E-Mail-Programme und Systemlandschaften können sehr unterschiedlich sein. Das Landratsamt Roth unterstützt mit dieser Lösung die folgenden Systeme:

Nachfolgend wird zunächst allgemein geschildert, wie der externe Gesprächspartner vorzugehen hat; die Screenshots der unterstützten Systeme können dem Anhang entnommen werden.

Schlüssel im Adressbuch hinterlegen
Wie beim Schritt 1b ist es notwendig, den öffentlichen Schlüssel in das Adressbuch des eigenen E-Mail-Programms zu integrieren.
Die Folge: Neben Name und Adresse befindet sich nun auch der Schlüssel des Kommunikationspartners im Adressbuch.

Verwaltungs-PKI-Zertifikat laden und integrieren
Um bei späteren Mails nicht immer gefragt zu werden, ob der Kommunikationspartner vertrauenswürdig ist, sollte auch das so genannte Wurzelzertifikat der Bayerischen VerwaltungsPKI eingebunden werden.

Zertifizierungsstelle des internen Kommunikationspartners ist der Freistaat Bayern. Das Zertifikat, das aus einer langen Zeichenkette besteht, lässt sich von der Internetseite https://www.bsi.bund.de/DE/Themen/weitereThemen/VerwaltungsPKIVPKI/Wurzelzertifizierungsstelle/Zertifikate/zertifikate_node.html herunterladen und automatisch in das Mailprogramm integrieren.

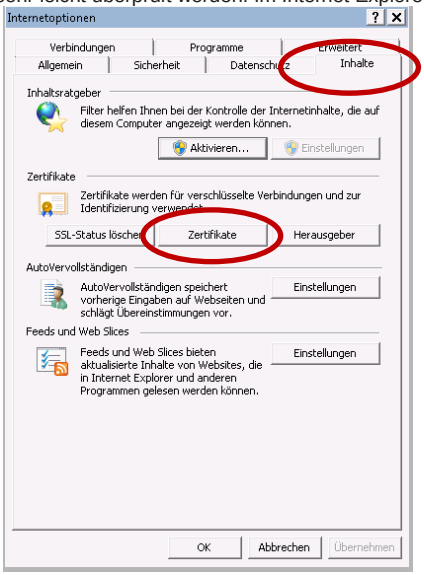
Schlüsselpaar generieren

Falls noch kein Schlüsselpaar existiert, also keine E-Mail-Verschlüsselung genutzt wird, ist auch dieses Schlüsselpaar zu erstellen. Existiert im Unternehmen des externen Kommunikationspartners eine Certification Authority (CA), wird über diese ein Schlüssel generiert. Weitere Informationen hierzu hat Ihr Administrator. Anderenfalls kann das Schlüsselpaar auch im Internet bezogen werden – von einer der Firmen, die Zertifizierungsstellen anbieten und denen zu vertrauen ist.

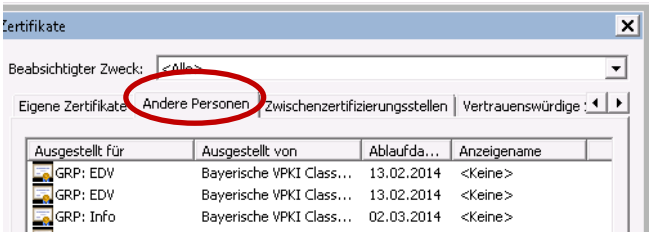
Diese Anleitung für Externe führt Sie Schritt-für-Schritt. Die Generierung des Schlüsselpaares ist im Übrigen unabhängig von E-Mail-Programm und Systemarchitektur

Schlüssel im Adressbuch hinterlegen

Der Schlüssel wird automatisch durch das Beantworten einer signierten Mail in das Adressbuch integriert. Das kann sehr leicht überprüft werden: Im Internet Explorer [Extras] [Internetoptionen] klicken.



In diesem Fenster des Registers [Inhalte] wird mit einem Klick auf [Zertifikate] der Zertifikatsspeicher geöffnet. Hier sind alle eingebundenen Zertifikate abgelegt. Falls das Zertifikat nicht im Zertifikatsspeicher enthalten sein sollte, kann dieser Schritt auch manuell erfolgen: Es genügt ein Rechtsklick mit der Maus auf den Absender der E-Mail und dann [Ins Adressbuch einfügen] wählen.



Verwaltungs-PKI-Zertifikat laden und integrieren

Dieser Schritt ist bei Tests nicht notwendig gewesen. Dennoch ist es möglich, dass die Meldung „nicht vertrauenswürdig“ angezeigt wird. Dann muss das Verwaltungs-PKI-Zertifikat von https://www.bsi.bund.de/DE/Themen/weitereThemen/VerwaltungsPKIVPKI/Wurzelzertifizierungsstelle/Zertifikate/zertifikate_node.html heruntergeladen werden. Ein Doppelklick auf das Zertifikat integriert es automatisch in Microsoft Outlook. Falls dies nicht möglich sein sollte, wird das Zertifikat über das Menü [Zertifikate] und die Funktion [Importieren] eingebunden. In dem sich öffnenden Fenster ist das Zertifikat aus dem Ordner, in dem es gespeichert wurde, einzubinden.