eurodata

IT-Dienstleistungen mit System

Allgemeine Erläuterungen zu

- persönliche Zertifikate
- Wurzelzertifikate
- Zertifikatssperrliste/Widerrufsliste (CRL)
- Public Key Infrastructure (PKI)
- Signierung und Verschlüsselung mit S/MIME

1. Allgemeine Erläuterung zum Thema Zertifikate

Zertifikate bestätigen die Zugehörigkeit eines kryptografischen Schlüssels zu:

- einer Person/Firma/Institution (z.B. bei der PGP-Verschlüsselung von Dateien oder E-Mails).
- einer Maschine (z. B. bei der SSL-Verschlüsselung von Website-Traffic).

Dadurch können Authentizität, Vertraulichkeit und Integrität von Daten gegenüber Dritten garantiert werden.

Die rechtlichen Rahmenbedingungen für die Ausstellung digitaler Zertifikate sind in vielen Staaten durch eigene Gesetze geregelt. In der EU ist eine mit einem qualifizierten Zertifikat erstellte elektronische Signatur weitgehend der handschriftlichen Unterschrift gleichgestellt.

Um beim Einsatz von asymmetrischen Kryptosystemen den Einsatz falscher (z.B. untergeschobener) Schlüssel zu verhindern, wird ein Nachweis benötigt, dass der verwendete öffentliche Schlüssel auch zum designierten Empfänger der verschlüsselten Nachricht bzw. zum Sender einer elektronisch signierten Nachricht gehört. Diesen Nachweis stellt eine vertrauenswürdige Stelle in Form eines digitalen Zertifikates aus.

Man kann sich also ein Zertifikat wie einen Personalausweis in digitaler Form vorstellen: Beim Personalausweis garantiert die vertrauenswürdige Stelle "Meldeamt", dass die Unterschrift, die sich auf dem Ausweis befindet, auch tatsächlich zu der Person gehört, deren Stammdaten und Passbild sich auf dem Ausweis befinden.

Im Gegensatz zum Personalausweis werden Zertifikate aber von vielen verschiedenen Zertifizierungstellen und in vielen verschiedenen Qualitätsstufen ausgegeben. Es ist Sache des Benutzers zu entscheiden, ob er dem Herausgeber des Zertifikates vertraut.

Um die Echtheit des Zertifikates zu garantieren, wird dem Zertifikat eine digitale Signatur einer vertrauenswürdigen Organisation oder Instanz (z.B. eurodata) aufgeprägt. Durch dessen Signatur kann die Integrität und Echtheit des Zertifikates nachgewiesen werden.

2. Signierung/Verschlüsselung von Mails mit S/Mime

eurodata verwendet den Standard S/Mime um E-Mails zu signieren bzw. zu verschlüsseln. Dieser Standard ist bereits in den meisten E-Mail Programmen (Thunderbird, Outlook, Outlook Express) implementiert.

Weitere Informationen zu S/Mime unter: http://www.imc.org/ietf-smime/

S/Mime verwendet Public Key Kryptographie, ein asymmetrisches Verschlüsselungssystem, das mit einem öffentlich bekannten Schlüssel und einem nur dem Inhaber bekannten privaten Schlüssel arbeitet. Im Gegensatz zur symmetrischen Verschlüsselung, bei der ein einziger Schlüssel zum Verschlüsseln und Entschlüsseln benutzt wird, gilt bei dem asymmetrischen Verfahren: „Was mit dem einen Schlüssel verschlüsselt wird, kann nur mit dem anderen Schlüssel entschlüsselt werden und umgekehrt."

Weitere Informationen zu Public Key Kryptographie unter:

http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem

http://www.bsi-fuer-buerger.de/schuetzen/07_0301.htm#asym

3. Begriffserläuterungen

Zertifikate von eurodata/ETL Mitgliedern

Wenn sie den öffentlichen Schlüssel eines Mitarbeiters (eurodata/ETL) kennen, sind Sie in der Lage nachzuprüfen, ob dieser mit seinem geheimen Schlüssel eine E-Mail signiert hat.

Der öffentlichen Schlüssel steckt in dem digitalen Zertifikat des Mitarbeiters und enthält folgende Daten:

- Identität des Inhabers
- Emailadresse des Inhabers
- Ablaufdatum des Zertifikats
- Seriennummer des Zertifikats
- Öffentlicher Schlüssel der Zertifizierungsstelle

Diese Daten sind mit dem privaten Schlüssel der Zertifizierungsstelle unterschrieben und können somit durch den öffentlichen Schlüssel der Zertfizierungsstelle überprüft werden. Dadurch wird sichergestellt, dass das Zertifikat zu einer bestimmten Person gehört.

Erläuterung zur Public Key Infrastructure (PKI)

Jedes Zertifikat ist von einer ausgebenden Stelle beglaubigt, die ihrerseits wieder von höheren Stellen beglaubigt sein kann. Das Vertrauenssystem ist streng hierarchisch. Den gemeinsamen Vertrauensanker bildet ein sog. **Wurzelzertifikat** (Root Certificate).

Microsoft Produkte enthalten bereits verschiedene Wurzel-Zertifikate kommerzieller Zertifikatsanbieter, nicht aber das Wurzelzertifikat der eurodata. Mit dem Import des eurodata Wurzelzertifikates werden dadurch alle Zertifikate, die von eurodata ausgestellt wurden als gültig und vertrauenswürdig eingestuft.

Damit eine signierte E-Mail ohne Warnmeldungen angezeigt wird, muss also das Wurzelzertifikat der eurodata importiert werden. Eine PKI stellt u.a. die Wurzelzertifikate und die CRLs zur Verfügung.

Verwendung des persönlichen Zertifikats

Das persönliche Zertifikat wird in den Zertifikatsspeicher eines Mail-Programms importiert. Danach haben Sie die Möglichkeit eine Mail zu signieren. Möchten Sie eine Mail verschlüsseln, müssen Sie vorher eine signierte Mail des Adressaten empfangen haben, die den öffentlichen Schlüssel enthält. Die Mail wird mit diesem öffentlichen Schlüssel verschlüsselt und kann später nur durch den privaten Schlüssel des Adressaten entschlüsselt werden.
Damit Sie das persönliche Zertifikat auf ihren PC installieren können, benötigen Sie

- Ihre persönliche ***Zertifikatsdatei***. Der Dateiname enthält ihren Namen und besitzt das Dateiformat ***p12*** - z.b *mmustermann.p12* für Max Mustermann.

- Das Passwort (Transportschlüssel) für Ihr Zertifikat. Dieses Passwort dient zur Aktivierung Ihres Zertifikats beim Import in Ihr Mailprogramm.

Zweck des allgemeinen Personenzertifikats

Mit Hilfe von allgemeinen Personenzertifikaten (**personen-soft-ca.cer für eurodata- und etl-personen-ca.crt für ETL Mitarbeiter**) werden die persönlichen Zertifikate unterschrieben. Jedes persönliche Zertifikat enthält somit das jeweilige allgemeine Personenzertifikat. Beim Import in das Mailprogramm werden beide Zertifikate übernommen. Ihr Mailprogramm wird somit allen Zertifikaten vertrauen die aus der gleichen Personengruppe stammen.

Zweck der Widerrufsliste/Zertifikatssperrliste

Personenzertifikate, die vor Ablauf ihrer Gültigkeit als nicht mehr vertrauenswürdig eingestuft werden, werden in einer Zertifikatssperrliste/Widerrufsliste/CRL (**personen-soft-ca.crl für eurodata- und etl-personen-ca.crl für ETL Mitarbeiter**) gepflegt. Widerrufslisten werden von eurodata gepflegt und sind durch das öffentliche Zertifikat der eurodata signiert. Analog zu den bereits erwähnten Zertifikatslisten gibt es die beiden Widerrufslisten personen-soft-ca.crl und etl-personen-ca.crl. Ihr Mailclient wird entsprechend konfiguriert, damit er automatisch diese Widerrufsliste in regelmäßigen Abständen bezieht.

4. Kurze Zusammenfassung der Vorteile

Authentizität

Ihr Mailprogramm wird automatisch alle mit einem eurodata-Zertifikat signierten Mails, die Sie zukünftig erhalten, mit dem öffentlichen Schlüssel der eurodata verifizieren. Auf diese Weise erhalten Sie über die Identität des Absenders einer E-Mail Gewissheit.

Integrität

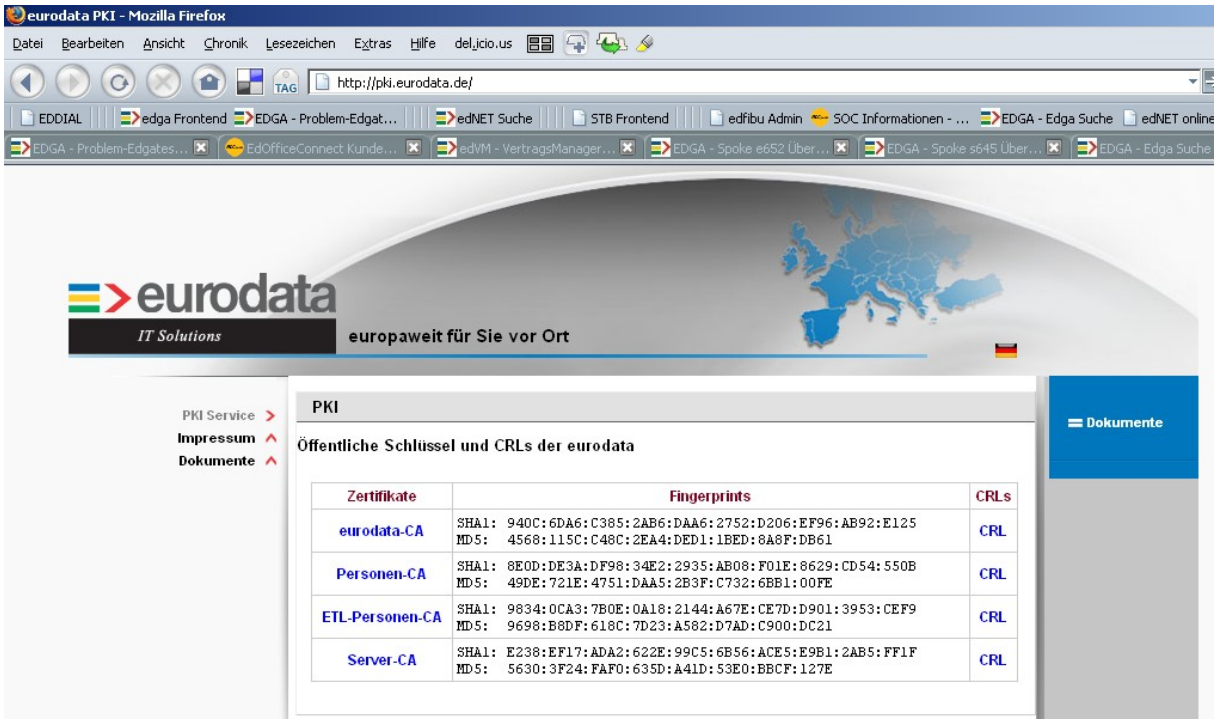
Da die Signatur mit dem Inhalt der Mail "verwoben" ist, kann eine Mail nicht gefälscht oder manipuliert werden. Ihr Mailprogramm verifziert mit Hilfe des öffentlichen Schlüssels des Absenders die Integrität der Mail.

Vertraulichkeit

Ist der Absender im Besitz Ihres öffentlichen Schlüssels (Zertifikat), so hat er die Möglichkeit seine Mails an Sie zu verschlüsseln. Nur Sie können mit Hilfe Ihres privaten Schlüssels die Mail lesen.

5. Beschaffung der eurodata Wurzelzertifikate und Widerrufslisten

Falls Sie noch kein persönliches Zertifkat besitzen, so können Sie trotzdem die übergeordneten allgemeinen Personenzertifikate und Widerrufslisten importieren. Ihr Mailprogramm kann damit alle Zertifikate von eurodata und ETL Mitarbeitern überprüfen. Auf ungültige Zertifikate werden Sie explizit hingewiesen.



Öffnen Sie Ihren Browser und gehen Sie auf **http://pki.eurodata.de**

Jetzt müssen Sie die folgende Zertifikate (CA) und die dazugehörigen Widerrufslisten (CRL) herunterladen. (eurodata-CA, Personen-CA und ETL-Personen-CA)
Rechtsklick auf die jeweilige CA und mit **Ziel speichern unter** auf dem Desktop abspeichern. Anschließend befinden sich folgende Dateien auf dem Desktop die Sie in Ihr Mailprogramm importieren müssen.